Izzat Alsmadi

The NICE Cyber Security Framework

Cyber Security Intelligence and Analytics

Springer

The NICE Cyber Security Framework

Izzat Alsmadi

The NICE Cyber Security Framework

Cyber Security Intelligence and Analytics

Springer

Izzat Alsmadi
Texas A&M University
San Antonio, TX, USA

ISBN 978-3-030-02359-1 ISBN 978-3-030-02360-7 (eBook)
https://doi.org/10.1007/978-3-030-02360-7

Library of Congress Control Number: 2018960944

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

In this book, I tried to cover with essential information US NIST National Initiative for Cybersecurity Education (NICE) framework KSAs in certain areas related to cyber intelligence and analytics in particular. By no means is the information in this book complete or comprehensive due to the extensive information in this area.

This book can serve as an introductory source for those who are planning to adopt the NICE framework in cyber security education. The NICE framework is meant to establish a common ground between the academia and the industry on the different knowledge areas, specialties, and work roles in cyber security. However, in its current format, the framework is abstract. Different institutions can decide their own focuses from this abstract educational model. They can also estimate the course time required to complete each KSA in the framework as clearly each will take different course times to teach by educators or to complete by students.

San Antonio, TX, USA
Izzat Alsmadi

Contents

Chapter 1
Introduction

The job market for cyber security-related jobs is growing and is expected to reach a peak on demand in the next few years. Statistics showed that the USA has an overall national workforce shortage. Additionally, there is a need for education methods in this field in particular to evolve and accommodate market demands. In this path, NICE Cyber security education framework has been introduced recently. In this book, our goal is to present a teaching material based on NICE framework. The NICE framework focus was more jobs oriented than educational oriented. The NICE framework itself extended earlier OPM security framework (https://www.opm.gov/policy-data-oversight/assessment-and-selection/competencies/). Both frameworks adopted KSA competencies (Knowledge, Skills, and Abilities or Experience) as an alternative to classical course or program learning outcomes (CLOs and PLOs). One of the main differences between the two approaches is that KSA competencies explicitly distribute teaching, learning and also assessment activities to three categories: KSAs. This is very necessary for practical-oriented majors such as cyber security where knowledge and lecturing based on slides will not be enough.

NICE framework is evaluated from an education perspective. Issues and challenges related to using such framework to guide future cyber security programs are discussed in details. One of the most significant challenges observed is related to the lack of a unified method to estimate KSAs. Different KSAs vary widely in their level of details. Additionally, the same KSA can interpret in different cyber security classes or programs differently. This means that estimating how much of course time such KSA should be allocated can widely vary from one school or program to another.

In NICE documentation, Knowledge areas have codes up to K0614. Similarly, last skill number in NICE framework is 0359 and last Ability is A0119. Nonetheless, with newer versions/releases of NICE framework, numbering is changed, some merges, updates, or changes occur to all KSAs.

Cyber security jobs are expected to grow vertically or in size in the next few years and also horizontally where many new job security roles are expected to arise.

I. Alsmadi, *The NICE Cyber Security Framework*,
https://doi.org/10.1007/978-3-030-02360-7_1

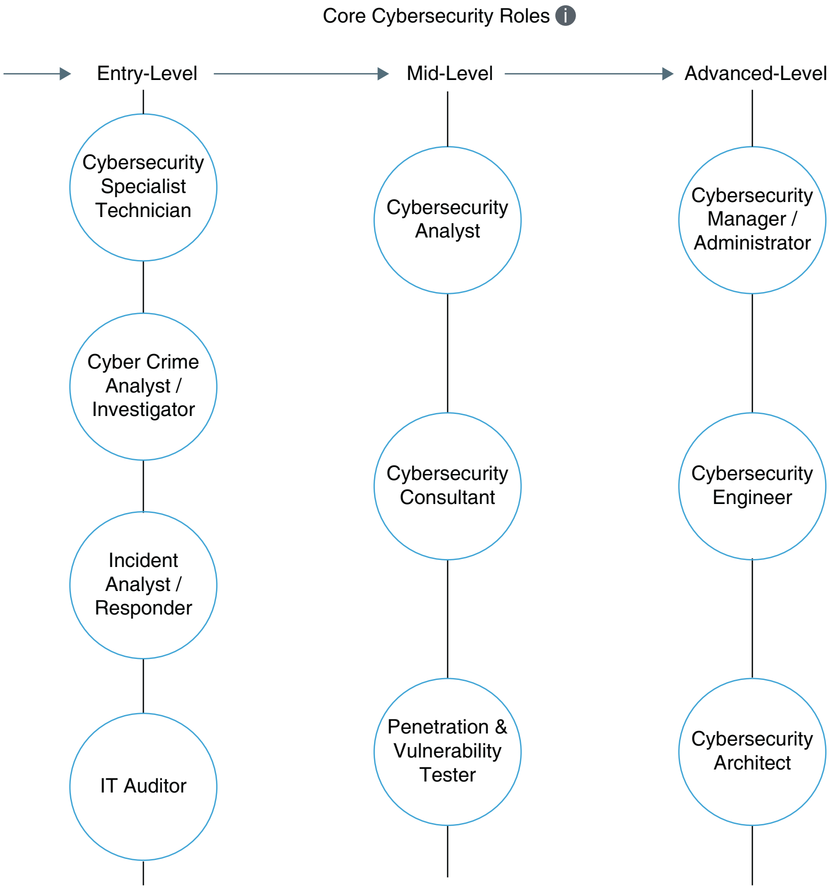

Core Cybersecurity Roles
Entry-Level
Mid-Level
Advanced-Level
Cybersecurity Specialist Technician
Cyber Crime Analyst / Investigator
Incident Analyst / Responder
IT Auditor
Cybersecurity Analyst
Cybersecurity Consultant
Penetration & Vulnerability Tester
Cybersecurity Manager / Administrator
Cybersecurity Engineer
Cybersecurity Architect

Fig. 1.1 Core cyber security roles (Cyberseek.org)

The NICE and OPM frameworks represent collective effort at US national level to envision and show job demands and help fulfill such demand through helping educational institutes match such demand. Figure 1.1 shows core cyber security roles: cyberseek.org.

General Issues with NICE Framework (Applied to August 2017 Version)

The Classification of KSAs Based on NICE Framework

Evaluating how NICE KSAs are used to map with Specialty Areas and Work Role, we can observe the following KSA categories:

Table 1.1 The first six knowledge areas exist in all framework specialties (see footnote 1)

K0001	K0004
K0002	K0005
K0003	K0006

1. **Core KSAs (KSAs listed in all or most cyber security job roles)** (Table 1.1):

   Those are included in all 52 specialty areas (33 main specialty areas, with several sub-specialty areas). Looking at the description of those knowledge competencies, we can see that they are very broad in nature. Each one of them can be covered within a course. This is one of the problems that we will elaborate on further in another section. As those are included in all 52 specialty areas, they should be included separately in an introductory course that will be a prerequisite course to all other program courses.

   We set a cut-off of seven specialty areas and above to consider "core skills and abilities." Tables 1.2 and 1.3 show the core skills and abilities based on our assumption.

   Similar to core knowledge competencies, we can see that *core* skills and abilities are constructed to be broad and generics. This is why they are included in many specialty areas.

   So, the question is then "Is this is the best/optimized set of KSAs to be considered in NICE framework, based on the level of abstraction or details?" Should we decompose some of those core KSAs or not? What will be the advantage or the drawback of doing so? There are many indications that the current set of KSAs is not final. The process is evolutionary however and may not see the term "final set of KSAs" any time soon.

   The framework is designed to find a unified or common language between: companies, job recruiters, students or job seekers, and education providers (Colleges, Universities, etc.). For education providers, KSAs have to map to courses. How many KSAs from the framework to include in each course is the most difficult question to consider. There is no assessment in NICE framework on how broad each KSA can be or how much course time, grading, etc. each KSA should be allocated.
2. **Work role special KSAs: KSAs largely listed for one Work role**

   One of the ideas we are proposing in this chapter is for cyber security programs to consider developing job-oriented courses, one or more courses to be developed explicitly to target one job role. The list in this section can be a good starting point. The NICE framework documentation described different work roles and required KSAs for each one. This can serve companies, job recruiters, or job seekers. However, education course designers are interested to ensure that KSAs are not repeated in the different courses. Current higher institute educations are built around courses as they are the smallest autonomous units. You can ask students to take a course as a prerequisite, but you can't ask them to take a KSA as a prerequisite.

Table 1.2 Core Skills with their occurrence count in specialty areas and description (see footnote 1)

Skill	No.	Skill	No.
S0367	14	S0027	7
S0296	9	S0060	7
S0218	8	S0297	7
S0249	8		

Table 1.3 Core Abilities with their occurrence count in specialty areas and description

Skill	No.	Skill	No.
A0123	15	A0106	9
A0013	14	A0015	8
A0089	13	A0082	7
A0066	12	A0084	7
A0170	11	A0088	7
A0070	9	A0105	7
A0085	9	A0119	7

Table 1.4 KSAs not included in current NICE framework matrix of work roles and specialty areas

Knowledge	Skills	Ability
K0085, K0099, K0141, K0166, K0173	S0099, S0105, S0161, S0163, S0164, S0165, S0180, S0230, S0366, S0368, S0371, S0373	A0075, A0126, A0127, A0131, A0132, A0133, A0134, A0135, A0136, A0137, A0138, A0139, A0140, A0141, A0142, A0143, A0144, A0145, A0146, A0147, A0150, A0151, A0152, A0153 A0154, A0155, A0156, A0157, A0158, A0162, A0169, A0173

They will have to develop core courses (with common or core KSAs) that can fit first- or second-year cyber security students. However, higher level courses should be more focused and hence should include unique KSAs.

3. KSAs that are not included in any work role or specialty area. Table 1.4 below shows the list of KSAs that are currently not included in any work role or specialty area:

Why will NICE includes KSAs in their framework and don't use them at all? Following are some possibilities:

- It is possible that those were removed by mistake or with new releases. For example, for the Knowledge: K0085, we can see it in version Nov. 2016 (800-081), (https://www.careeronestop.org/competencymodel/info_documents/NICE-WorkforceFramework-Nov2016.pdf) in securely provision, risk management, software development, strategic planning and policy development, vulnerability assessment and management (VA) modules or specialty areas but not in the current excel file or august. 2017 (final) version: (http://nvlpubs.nist.gov/

nistpubs/SpecialPublications/NIST.SP.800-181.pdf). Table 1.5 shows the list of KSAs that do not exist anymore in the most recent versions.

Those are removed completely without any notice. Unlike the next list where the new document shows that they were withdrawn and included in other KSAs.

- Ability A0162 is listed in some references and removed in some others.
- Two KSAs with the same number and different descriptions:

A0162: "Ability to ensure information system security, acquisition personnel, legal counsel, and other appropriate advisors and stakeholders are participating in decision making from system concept definition/review and are involved in, or approve of, each milestone decision through the entire system life cycle for systems"[1]
A0162: "Ability to recognize the unique aspects of the communications security (COMSEC) environment and hierarchy"

- There are some KSAs that exist in the most recent documents, but they are not used in any work area or specialty (Table 1.6).
- There are other instances where the removed KSAs from the current version are shown as withdrawn or combined with other KSAs (Table 1.7).

Table 1.5 List of NICE KSAs that are removed completely from recent publications

K0085, K0099, K0166, K0173, S0099, S0105, S0165, A0075, A0169

Table 1.6 KSAs that are not used in any work area or specialty

S0366, S0368, S0371, S0373, A0126, A0127, A0131, A0132, A0133, A0134, A0135, A0136, A0137, A0138, A0139, A0140, A0141, A0142, A0143, A0144, A0145, A0146, A0147, A0150, A0151, A0152, A0153, A0154, A0155, A0156, A0157, A0158, A0162, A0173

Table 1.7 List of withdrawn or updated KSAs/Tasks in NICE framework

Withdrawn	Integrated into	Withdrawn	Integrated into
K0141	K0420	K0337	K0007
T0336	T0228	K0385	K0142
K0223	K0073	K0450	K0036
K0253	K0227	K0490	K0058
K0282	K0200	K0611	K0131
S0161	S0160	S0163	S0060
S0180	S0062	S0230	S0066

[1] William Newhouse, Stephanie Keith, Benjamin Scribner, Greg Witte, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, NIST Special Publication 800-181, August 2017.

Level of Details and Granularity of KSAs

Several papers discussed issues related to the level of details and granularity of NICE KSAs (e.g., CSRC 2016). There are some KSAs that seem to have more details than others. On the other hand, this can be subjective and can vary from one course to another or from one job description to another. While making a unified language between education and the industry is considered as a strength element in NICE framework, however, it has some drawbacks. For example, for the Knowledge K0001: "**Knowledge of computer networking concepts and protocols, and network security methodologies**" (see Bejtlich 2010; Bellovin et al. 2017;Campbell 2003; Cichonski et al. 2012; Gennuso 2012; Incident Response Plan, Document Version: 1.0.0 2018; Information security Technologies to Secure Federal Systems 2004; InfoSec Nirvana 2015; ISO/IEC 27035 2018; Kumari and McPherson 2009; Lewis 1993; Libicki 2017; Mehta 2014; Olson and Blackwell 1990; Sang-Hun 2016; Trivedi 2007; Zhang 2017), clearly the granularity of such statement can vary widely from one scope to another. For the classical computer science education, this statement may be covered within up to three complete courses (i.e., computer networking 1, 2 and network security). How much each cyber security-related work area or specialty require from this KSA can clearly vary from one to another. The NICE framework in its current.

To investigate K0001 in particular, this integrates two large knowledge areas: (1) computer networking concepts and protocols and (2) network security methodologies. If we start with the first one, here are some of the "main subjects" that can be covered under this short statement: Network topologies, LANs, WANs, routing, switching, OSI model, TCP/IP suit, (many networking protocols), wireless, etc. Those can be covered typically in one or two computer networking courses. So, there is no doubt that such single Knowledge component is very large, regardless of how much instructor is going to shorten it. So, there are several issues with this Knowledge competency. For example, let's take **Scope Coverage:** How much content an educator should cover in this competency? All NICE framework KSAs are introduced without any reference to time, effort, or resource estimations. This may make it as a reference rather than a practical framework or model. In other words, the framework requires that you should cover this competency, somehow, without any reference on what to cover or how much effort to spend.

Starting the next chapter, chapters' content will be divided into four components: Tasks, Knowledge, Skills, and Abilities. Codes and descriptions of those tasks and KSAs are all copied from NIST reference documents. We will only present educational materials that can realize such components.

Bibliography

Bejtlich R (2010) CIRT-level response to advanced persistent threat. SANS Forensic Incident Response Summit

Bellovin SM, Landau S, Lin HS (2017) Limiting the undesired impact of cyber weapons: technical requirements and policy implications. J Cybersecur 3(1):59–68. https://doi.org/10.1093/cybsec/tyx001

Campbell T (2003) An introduction to the computer security incident response team (CSIRT) setup and operational considerations. Global information assurance certification paper. giac.org

Cichonski P, Millar T, Grance T (NIST), Scarfone K (Scarfone Cybersecurity) (2012) NIST Special publication 800-61, SP 800-61 Rev. 2. Computer security incident handling guide, August 2012

Gennuso K (2012) Shedding light on security incidents using network flows. SANS. https://www.sans.org/reading-room/whitepapers/incident/shedding-light-security-incidents-network-flows-33935

Incident Response Plan (2018) Document version: 1.0.0. http://www.i-assure.com, www.i-assure.com/wp-content/uploads/dlm.../RMF_Incident-Response-plan.docx

Information security Technologies to Secure Federal Systems (2004) GAO report to congressional requesters. GAO-04-467. www.gao.gov.

InfoSec Nirvana (2015) Part 2, Incident classification, security investigation series. http://infosec-nirvana.com/part-2-incident-classification/

ISO/IEC 27035 (2018) http://www.iso27001security.com/html/27035.html

Kumari W, McPherson D (2009) Remote triggered black hole filtering with unicast reverse path forwarding (uRPF). Network working group, request for comments: 5635

Lewis L (1993) A case-based reasoning approach to the management of faults in communications networks. CAIA

Libicki M (2017) Second acts in cyberspace. J Cybersec 3:29–35

Mehta L (2014) Top 6 SIEM Use Cases—InfoSec Institute. http://resources.infosecinstitute.com/top-6-seim-usecases/. Accessed 6 Sept 2014

Olson L, Blackwell A (1990) Understanding network management with OOA. IEEE network magazine

Sang-Hun C (2016) Computer networks in South Korea are paralyzed in cyberattacks. New York Times. http://www.nytimes.com/2013/03/21/world/asia/southkorea-computer-network-crashes.html. Last Accessed 26 June 2016

Trivedi K (2007) A standards-based approach for offering a managed security service in a multivendor network environment. Internet Protocol J 10(3)

Zhang E (2017) What is event correlation, examples, benefits and more. Digi Guardian, Sep. 12th 2018, digitalguardian.com

Chapter 2
Acquisition Management

The process of acquiring computing resources includes several activities related to planning, budgeting, comparing alternative options, configuration and change management, etc. Our focus in this book is on securing information and computing resources. As such, selected KSAs as well as the content of each KSA will be focused on this subject only.

Why security personnel should have KSAs related to acquisition management? In many cases of acquisition projects, security personnel should be present in the committee to plan and manage the acquisition process. Security goals and functions exist in all business domains and functions. Any new acquisition for information systems, network components, security controls, and hardware or software components can have its impact on security and can possibly create a vulnerability if not selected and integrated properly. At the end, for hackers, all what they need is to discover one vulnerability that they can find and expose to start attacking their targets.

K0126: Knowledge of Secure Acquisitions (e.g., Relevant Contracting Officer's Technical Representative [COTR] Duties, Secure Procurement, Supply Chain Risk Management)

Contracting Officer's Technical Representative (COTR) or Contracting Officer's Representative (COR) should ensure that company will only acquire the right: products, services, and contractors. Procurement of new hardware, software, or information system should not be authorized before ensuring that such procurement went through the right procedures according to business policies and regulation guidelines.

Software or system acquisition includes the following four main steps: (1) planning, (2) contracting, (3) monitoring and acceptance, and (4) follow-up. Proper security measures should be adopted through the whole process where security problems can occur at any stage (Table 2.1).

I. Alsmadi, *The NICE Cyber Security Framework*,
https://doi.org/10.1007/978-3-030-02360-7_2

Table 2.1 Acquisition stages based on different standards (Polydys and Wisseman 2009a, b)

Standard/ stage	Planning	Contracting	Monitoring and acceptance		Follow-up
IEEE 1062	Planning	Contracting	Implementation	Acceptance	Follow-on
PMBOK	Initiating		Monitoring executing	Closing	
NIST SP 800-61	Business planning	Acquisition planning	Contract performance	Contract Closeout	Follow-on
DoD 5000.2	Pre-system acquisition	System acquisition			Sustainment
ISO/IEC 12207	Preparation	Advertisement	Monitoring	Acceptance and Closure	

Securing Communication with Contractors During the Solicitation Process

A company trying to acquire software or systems will send solicitation documents to candidate contractors. COTR or those assigned in the procurement process should be the only contact point with those contractors. Same initial information or any extra provided clarifications should be provided to all candidate contractors/vendors. The acquisition team should act with extreme caution when dealing with contractors/vendors to keep the competitive process open and fair. Details about the selection process should be classified and no contractor or vendor should be given any insider information. Commitment to acquire the final selected system should be only made public after final decision and all candidate contractors should be aware of the selection.

Securing the Acquisition Process

Upon selecting a contractor or vendor, written contract should clearly explain the two-party duties and responsibilities. Details should help in clarifying expectations and limit any possible conflicts or potential problems in future.

Software Acquisition Working Group in U.S. Department of Homeland Security prepared a guidebook that has focused on how to improve the software acquisition and purchasing process. The ultimate goal is to enhance software supply chain management (DHS 2007, Polydys and Wisseman 2009a, b).

Software applications and information systems continuously go through cycles of new fixes, updates, enhancements, etc. Figure 2.1 shows possible software supply chain path (Polydys and Wisseman 2009a, b).

Every software change may introduce possible vulnerabilities. We assume that such vulnerabilities that exist in acquired software are accidentally or carelessly inserted at any time during the software lifecycle. While it is possible that many

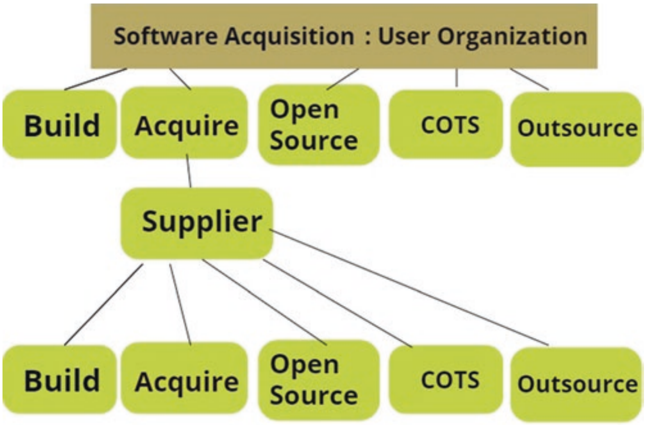


Fig. 2.1 Possible software supply chain path (Polydys and Wisseman 2009a, b)

software systems exist with vulnerabilities that were never exploits or discovered, however, the existence of such vulnerabilities is a serious risk that. If such risks are not accounted for (e.g., in risk avoidance, mitigation or tolerance methods), they can cause catastrophic consequences. Examples of categories of such consequences include: sensitive data exposures that can jeopardize privacy, intellectual property, integrity, etc. Attacks that expose software vulnerabilities may also cause identity thefts and serious financial losses.

Software procurement team should learn how to check with software vendors issues related to software vulnerability. They should know through a series of questions, reading through documentations, interviews with vendors, etc. what vendors have or have not done as part of their secure development process, how they handle vulnerabilities, etc.

K0148: Knowledge of Import/Export Control Regulations and Responsible Agencies for the Purposes of Reducing Supply Chain Risk

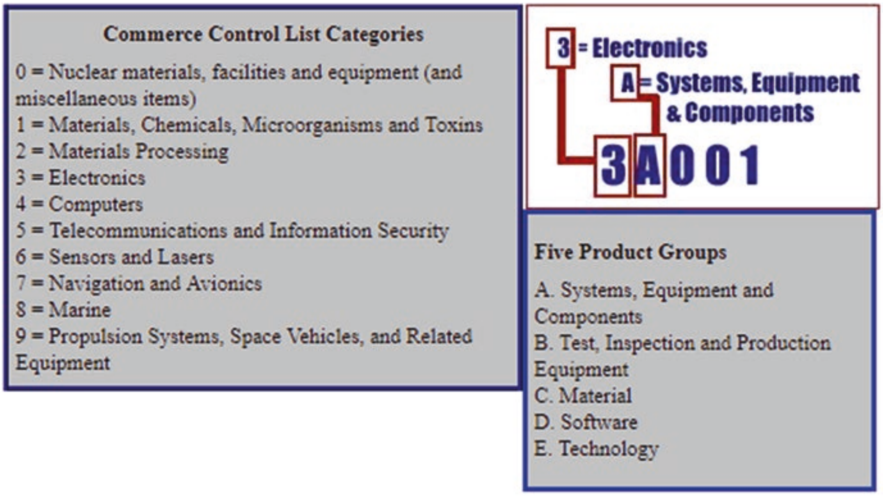
Export Control Classification Numbers (ECCNs) and Harmonized Tariff Schedule (HTS) Numbers and CCATS are standard entries used to identify different items. Those values consist of digits and numbers, Table 2.2.

Each ECN number contains five digits (Fig. 2.2). The first number from the left shows the Commerce Control List (CCL) category. The second digit is a letter and shows one of five possible product groups.

When it comes to software/information system acquisition, many US legislations give precedence to local or national products. For security concerns in particular, more reasons exist to support such choice. In cloud hosting, for example,

Table 2.2 Examples of US HTS and ECCNs

Model #	US HTS	US ECCN
Alienware M17X/M17X10	8471.30.010	5A992
Inspiron 1017	8471.30.010	5A992
Inspiron 1120/1121	8471.30.010	5A992



Commerce Control List Categories

0 = Nuclear materials, facilities and equipment (and miscellaneous items)
1 = Materials, Chemicals, Microorganisms and Toxins
2 = Materials Processing
3 = Electronics
4 = Computers
5 = Telecommunications and Information Security
6 = Sensors and Lasers
7 = Navigation and Avionics
8 = Marine
9 = Propulsion Systems, Space Vehicles, and Related Equipment

Five Product Groups

A. Systems, Equipment and Components
B. Test, Inspection and Production Equipment
C. Material
D. Software
E. Technology

Fig. 2.2 US ECN specifications (www.bis.doc.gov)

US government agencies demand that any contractor or service provider should verify that hosted data/services exist physically in the USA. Similarly, through the Export Administration Act (EAA) and the Arms Export Control Act (AECA), exports of weapons, military-related products or products that can have dual usage: civilian and military are prohibited. Other important regulations related to supply chain and foreign exports include: Trade Expansion Act of 1967:232, Foreign Investment and National Security Act of 2007 (“FINSA”), National Defense Authorization Act of 2011 and the “Wolf Provision” Act 2014.

With the Internet, online social networks, smart phones, and all globalization issues, security concerns are in continuous increase. Many IT companies have their headquarters in the USA, while the majority of their products are developed in other countries. In order to keep a balance, a large and important country such as the USA cannot and should not keep itself isolated from the global economy and the benefits of global ICT supply chain.

With global industry, companies or supply chain, different types of risks may arise. For example, several recent cases showed examples of espionage from foreign countries (especially China and Russia). Reports showed that major global companies and government agencies have frequently discovered malicious code and software and hardware in their ICT networks or equipment, which could facilitate cyber-attacks (US Chamber of Commerce 2016).

K0154: Knowledge of Supply Chain Risk Management Standards, Processes, and Practices

Supply chain risks related to ICT sectors may include insertion of counterfeits, malicious software and hardware, unauthorized production, tampering, theft, or poor manufacturing and development practices in the ICT supply chain (NIST 2015).

Supply chain literature summarizes the following main categories of risks: demand, delay, disruption, inventory, manufacturing and breakdown, physical plant capacity, supply, system, sovereign, transportation risk (Tummala and Schoenherr, 2011). Literature categorizes also those risks into four levels: extreme or very high, high, low, and very low based on four factors: consequence or impact type, consequence severity, risk occurrence frequency, and predictability.

A recent cyber security supply chain standard is developed by: North American Electric

Supply risk mitigation strategies can take different categories also such as: demand management, supply management, product management, and information management (Blos et al. 2009). More specifically, supply risk mitigation can consider one of the following generic risk mitigation strategies: risk postponement, selective, transfer, avoidance, etc.

Reliability Corporation (NERC) based on an initiative from Federal Energy Regulatory Commission (FERC) agency in department of energy (FERC order No. 829).

FERC Order No. 829 directed the electric reliability organization to develop standards that address supply chain risk management for industrial control system hardware, software, and computing and networking services.

The current NERC draft (August 10, 2017) contains three components within Critical Infrastructure Protection (CIP: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx) standard:

- Supply chain risk management Reliability Standards CIP-013-1 (Cyber Security—Supply Chain Risk Management).
- CIP-005-6 (Cyber Security—Electronic Security Perimeter(s)).
- CIP-010-3 (Cyber Security—Configuration Change Management and Vulnerability).

The current standard is not comprehensive and it excludes: Electronic Access Control and Monitoring Systems (EACMS), \5\ Physical Access Control Systems (PACS), and Protected Cyber Assets (PCAs), with the exception of the modifications in proposed Reliability Standard CIP-005-6, which apply to PCAs (https://www.gpo.gov/fdsys/pkg/FR-2018-01-25/html/2018-01247.htm).

BES Cyber Asset

This is a new term used by NERC in (CIP V5 standard) shifting from identifying Critical Cyber Assets to identifying BES Cyber Systems or Assets. In NERC glossary, BES Cyber Asset (BCA), is defined as: “A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 min of its required operation, mis-operation, or non-operation, adversely impact one or more facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System” (Fig. 2.3).

BES cyber systems are classified into three categories: high, medium, and low impact. Focus is on high and medium impact systems. One sub-system with high or

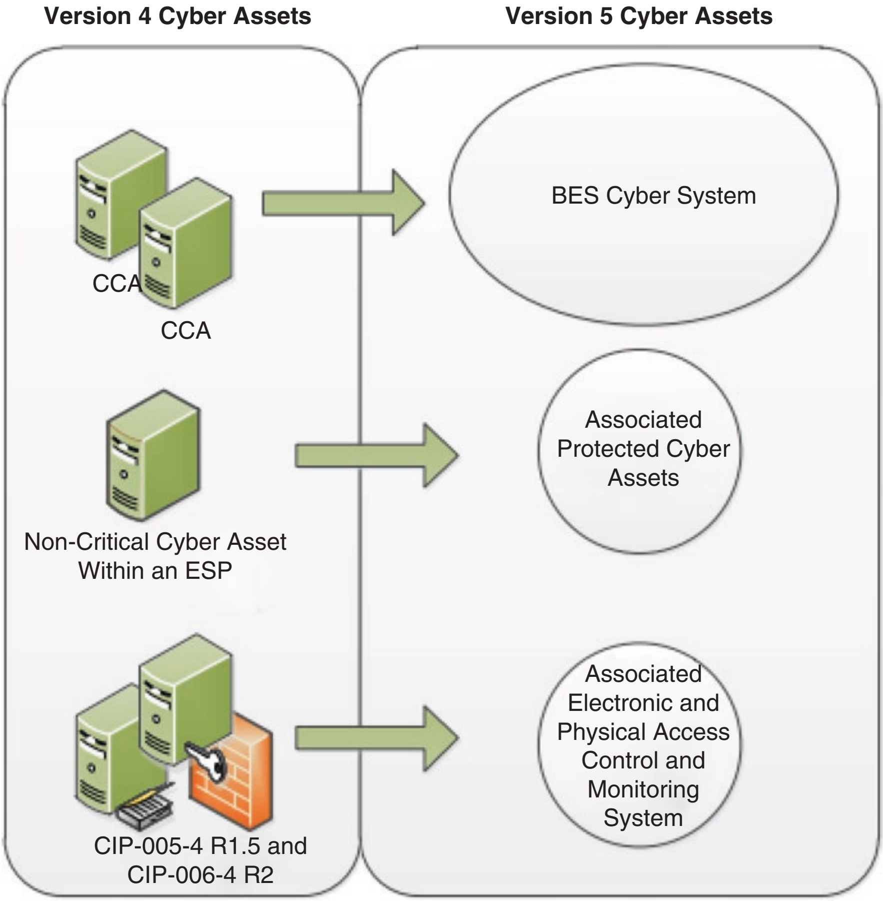

Version 4 Cyber Assets
Version 5 Cyber Assets
CCA
CCA
BES Cyber System
Non-Critical Cyber Asset Within an ESP
Associated Protected Cyber Assets
CIP-005-4 R1.5 and CIP-006-4 R2
Associated Electronic and Physical Access Control and Monitoring System

Fig. 2.3 BES cyber systems (NERC: CIP-002-5.1 standard)

medium impact will cause the whole system to be considered also as high or medium. Currently, cut-off is set to yearly power generation of 1500MW as the lowest for a system to be considered in the low impact category.

US National Institute of Standards and Technology (NIST) developed and instituted supply chain risk management (SCRM) framework: NIST 800-161, 2015, (https://csrc.nist.gov/publications/detail/sp/800-161), (https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management). The framework extends earlier similar or related efforts including:

- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.
- NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments.
- NIST SP 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems.
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System.
- NIST 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.
- NIST SP 800-53A Revision 4, Guide for Assessing the Security Controls in Federal Information Systems and Organizations.
- Department of Defense and Department of Homeland Security Software Assurance Acquisition Working Group, Software Assurance in Acquisition: Mitigating Risks to the Enterprise.
- National Defense Industrial Association (NDIA), Engineering for System Assurance [NDIA].
- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15288—System Life Cycle Processes [ISO/IEC 15288].
- ISO/IEC 27036—Information Technology—Security Techniques—Information Security for Supplier Relationships [ISO/IEC 27036].
- The Open Group's Open Trusted Technology Provider™ Standard (O-TTPS), Version 1.0, Mitigating Maliciously Tainted and Counterfeit Products [O-TTPS].
- Software Assurance Forum for Excellence in Code (SAFECode) Software Integrity Framework, [SAFECode 2] and Software Integrity Best Practices [SAFECode 1].

NIST SCRM focusing on the following main goals (Pillars of ICT SCRM):

- Resilience: Ensuring that ICT supply chain will provide required ICT products and services under stress or failure circumstances.
- Quality: Reducing vulnerabilities that may limit the intended functions of a component, lead to component failure, or provide possibilities for exploitation.
- Security: Provides basic CIA (confidentiality, integrity, and availability) when it comes to the different supply chain activities, services, and members or partners.
- Integrity: Ensuring that the ICT products and services are immune from tampering or alteration. Additionally, SRCM should ensure that the ICT products and

services will perform according to acquirer specifications and without additional unwanted functionality.
- Sustainability and compliance.
- It also focuses on four SCRM strategies: (1) incident management, (2) supplier business continuity planning (BCP), (3) manufacturing and test resilience, and (4) product resilience

ISO/IEC 20243 and 27036

ISO/IEC 20243: Open Trusted Technology Provider Standard (O-TTPS)—Mitigating the Risk of Tainted and Counterfeit Products and the Assessment Procedures for 20243 (latest versions, 2015 and 2018). (https://www.iso.org/standard/74399.html, https://publications.opengroup.org/x1607). The O-TTPS certification program identifies organizations that conform to ISO/IEC 20243.

ISO/IEC 20243 is a process-based standard that focuses on reducing the risk of counterfeit in commercial-off-the-shelf (COTS) products and their supply chains requirements for suppliers throughout their products' lifecycles. The standard contains processes and practices for ICT providers. The standard focuses on product integrity and supply chain security.

ISO/IEC 27036 addresses the general security requirements in suppliers' relationships in any procurement, security guidelines for ICT, and cloud supply chain security. The standard is structured with ISO/IEC 15288: System and Software Engineering, Lifecycle Processes. The standard is also mapped to ISO/IEC 27002.

K0163: Knowledge of Critical Information Technology (IT) Procurement Requirements

IT procurement requirements can be defined as the demand for: information systems, equipment, hardware, software, personnel, services or solutions, or facilities by specified quantities for a specific period of time. Requirements in IT procurements continuously change and evolve as technology, environment, and even security risk continuously and rapidly change.

The amount of planning and effort to spend in IT procurement can vary from one project to another based on several factors such as: overall estimated budget, security risks involved/expected, and criticality of the project.

First step in IT procurement is to identify business needs based on several factors including business mission/objectives, budget, and standards or regulations. Procurements with high budgets should include clear justifications and business values on such investments. They should also include details related to compatibility with existing systems. Decisions should also be made whether such requirements can be fulfilled in-house or a procurement process is necessary.

IT procurement requirements share several commonalities with requirements collection and analysis in other software and IT projects. For example, here is a list of possible problems IT procurement requirements' problems:

- Problems in the requirements collection process: IT equipment can be requested based on three categories: (1) Must have: If core business functions or services are currently down or unavailable waiting for such IT equipment, Similarly if such items are required to handle serious security issues; (2) Necessary to have: For necessary updates or upgrades with less urgency in comparison with the first case; and (3) Good or want to have, enhance, or improve business functions, without core or security urgency. IT procurement requirement needs to be clearly classified under which one of those three previously mentioned categories. Handling requirements for each category will be completely different from the others.
- Requirements feasibility issues: Adopted requirements should be feasible, applicable, or doable. This has to consider several factors related to business goals and mission, environment, users, budget, and many other factors. In many cases, what worked in one business or environment successfully may not work in the same level of success in a different company or environment. Many examples in the different IT sectors include cases where a certain software or information system was requested based on unrealistic or through IT procurement requirements and such systems were a complete failure.
- Fitness issues: In connection with the two previous issues, fitness issues are very critical, especially when acquiring a large equipment or information system that will impact many people and business sectors. The process of large information systems, especially if they are upgrading earlier systems can be very expensive and time-consuming. Acquisition failures can be then catastrophic. This is why some organizations struggle dealing with legacy systems. However, a balance is required here between making the right and proper transition or else having to deal with legacy systems with very painful and expensive maintenance issues.

IT procurement requirements can also be classified into: mandatory, functional, technical, and work or performance.

- Mandatory: Where certain criteria must exist in the candidate supplier.
- Functional: If services, information systems, or applications are requested, requirements can be stated in terms of service requestor needs. Service providers or suppliers will have to come up with their own plan on how to fulfill such functions. The quality, clarity, and completeness of the provided requirements from service requestor can help create a better contract and define at the end of the acquisition process success or failure factors.
- Technical requirements. Usually IT departments from service requestor should detail requirements for such technical needs or support. They can also clarify hardware, network, software, or training expectations.
- Performance requirements: Those are typically regulations or constraints that can be included in addition to one of the earlier options. For example, constraints should be made on project timeline and expected deliverables, qualifications of supplier, etc.

IT Procurement Methods

Several factors decide the proper IT procurement method for a particular procurement project. Constraints on budget, quality, and availability of requested products or services, fair and open competition are examples of main criteria to consider. For seeking offers from contractors, one of the following methods can be used: (1) quick quotes, (2) competitive sealed bidding, (3) competitive negotiation, or (4) public or online auctions. Major factor in picking which one of those alternatives is the project cost or budget. In some exceptional cases (e.g., urgent procurement, informal quotation, exempt procurement), seeking one candidate supplier is possible.

A successful procurement process requires continuous effort throughout the process from different members including: business owners or stakeholders, procurement team, subject matter experts, IT team in addition to supplier teams.

K0164: Knowledge of Functionality, Quality, and Security Requirements and How These Will Apply to Specific Items of Supply (i.e., Elements and Processes)

This knowledge area is related to the previous one; how to handle different aspects of IT procurement requirements, namely: functionality, quality, and security. In addition to procurement requirements, it is important to understand projects' requirements in which supply or procurements are requested.

Functional Requirements

Requirements should be collected and defined by the procurement requester, business owner, or their assigned teams. They should seek help from the procurement personnel and other SCRM team members. One major output of this team effort is to identify the requirements for the procurement and how these requirements will apply to the supply items.

Functional requirements are domain-specific related to the services that requested system or service will provide. It is important to select, from supply options, those that best fit the requested system or service with best budget, time, quality, etc. As we can see, there are many goals or desired attributes that ideally should exist in selected supply item. However, in practical limitations may exist that will force companies to settle with less than ideal choices.

First one is related to the availability of different options from different vendors or suppliers. The popular Porter value chain model (Porter 2008) indicates in one of the five supply forces that the bargaining power of buyers is limited if supply options are limited (Fig. 2.4).

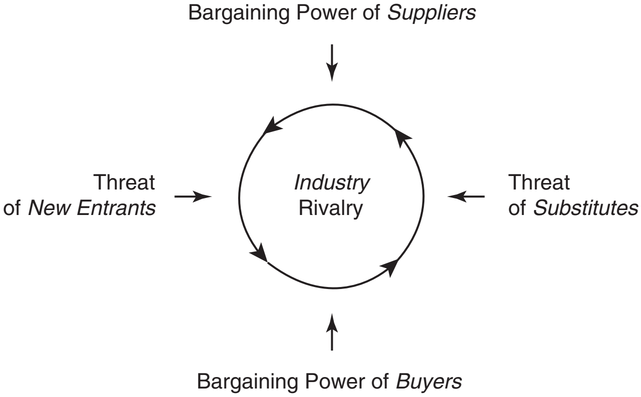


Fig. 2.4 Porter five forces supply model (Porter 2008)

How can we judge that the acquired system is the best fit for the request?

In project or system analysis, it is important to distinguish between two stages:

- Existing system analysis: This analysis focuses on the "problem domain"; what are the existing problems in the current system that triggers this IT procurement project.
- Acquired system specifications: What are the requested/desired features that should exist in the acquired system?

IT procurement systems should ideally include both parts (Existing system analysis and Acquired system specifications; indicating that system in the two terms refers to completely different systems). In some projects, contents from those two parts will be mixed without clearly differentiating between requirements related to what the current system has from requirements from what the solution should have or should impact on the current system.

Quality Requirements

Quality requirements or also called non-functional requirements complement functional requirements. Those are general desired characteristics (e.g., quality, performance, reliability, usability, maintainability, security) that the solution system should have.

Requirement of project requesters should be different between "must have" quality requirements and "desired to have" quality requirements. Making all requirements in one category whether "must have" or "desired to have" is not a wise selection. Those differences in the classification of the requirements can be the main criteria to decide which supplying option to select. While it is desired to have all kinds of high-quality requirements, selection team should be able to make decision related to:

- What functional or non-functional requirements that cannot be compromised and that they should exist in acquired system exactly as described. Alternatively, team should also be able to distinguish what are the requirements that can be compromised to a lower level and what is the accepted level.
- In most cases, different suppliers will offer different detail services. Team should be able to evaluate and judge those different quality attributes and compare them with each other or compare them with offered costs.

Security Requirements

Security requirements can be seen as one major category of quality requirements described earlier. However, in most cases, those security requirements cannot be compromised especially with government contracts or systems required to meet certain standards or regulations.

It is important for selection team to be aware of necessary or “must have” security requirements in the subject system in accordance with accepted standards or regulations. We described in other sections examples of some of those standards and regulations.

K0169: Knowledge of Information Technology (IT) Supply Chain Security and Risk Management Policies, Requirements, and Procedures

Supply Chain Security Policies

Similar to most of other business domains, supply chain security elements include, but not limited to: physical security, access control, employees, users and customers’ security, education and training awareness, procedural and workflow security, information protection and documentation security, partners’ communication and transportation security, risk management and disaster recovery, etc. The value or importance of each one of those elements may vary from one case or business to another. Unlike security policies in other business department, security policies in supply chain should go beyond the business premises to partners and communication or channels with supply chain partners.

Several US entities contribute to creating supply chain security policies such as: the Department of Defense (DOD), Department of Homeland Security, National Institute of Standards and Technology (NIST), Office of Management and Budget, Federal Energy Regulatory Commission, and General Services Administration (GSA). Due to the international nature of supply chain security, international organizations such as: International Organization for Standardization and International Electrotechnical Commission (ISO/IEC), World Customs Organization (WCO), International Civil Aviation Organization (ICAO), International Maritime Organization (IMO), and Universal Postal Union (UPO) contribute also to policies and standards in this area.

One noticed security-related policy in supply chain in the USA and most other countries is the issue of keeping all or most of the supply chain within national borders. In some sensitive government organizations in the USA, this is a must policy in IT procurements. In some other cases, if international suppliers are allowed either preferences are given to certain countries or some countries are excluded in particular (e.g., China, Russia, or India) from the selection.

Another important policy component is related to the vetting process. With different variations based on the nature of the organization and the procurement project and details, vetting can occur at different levels to cover most of the supply chain components. For example, many government organizations require certain levels of security clearance for all those workers, from the contractor or supplier side, in the procurement project. As part of the vetting process, suppliers may receive credits or liabilities based on their compliance or lack of compliance to security policies or requirements or in cases when some security vulnerabilities were discovered within their responsibilities.

US NIST described the following important principles when it comes to supply chain security policies:

- Security breaches are inevitable: Make your supply chain security policies as if security breaches will occur; be proactive rather than responsive.
- Security problems are not only technical or IT related; but also have social, human, training, and management aspects. Training is an important element in any security framework to educate people on security issues, regulations, controls, and protection mechanisms.
- Security is comprehensive; all what it takes is to find one vulnerability or weakness in one component: (e.g., technical, network, management, human, training, and security weaknesses or problems).
- Resilience: Supply chain should provide the required products and/or services under normal and stress or failure circumstances.

Here are few examples of US Supply chain security policies:

- **Supply chain security policies (SAFE Port Act of 2006)**: This act requires testing all US-bound cargo containers and scanning of all containers for radiation at the 22 busiest US ports.
- **Secure Freight Initiative (SFI)**: US Department of Energy and US Customs requires 100% scanning of US-bound cargo at selected ports.

Supply Chain Security Requirements and Procedures

Security problems in the supply chain should not be seen as IT problems only as they can seriously impact different functions in the supply chain. Security requirements should not also be seen as surplus; necessary only with government contracts or when we must comply with certain regulations or standards.

System analysts and team preparing procurement requirements may view security requirements as an extra overhead and time/budget limitations may impact such views. However, enterprise-level security requirements and policies should be developed that can be implemented, easily across all organization projects. In some cases, projects or their components can be classified under several security-related categories (e.g., low, medium, and high). Based on which category such project or component falls, certain security requirements can be pulled and applied from organization existing template.

When it comes to best practices and procedures in supply chain security, sharing information and experience between the different private and public sectors is important. On the other hand, in many cases, for information classification issues, government sectors are reluctant to share or provide such information. There are also several attempts of building national or global digital or online threat intelligence monitoring systems to keep all members informed of latest malwares, hacking attempt, or breaches, etc.

Supply Chain Risk Management Policies

In supply chain activities, several risk categories may occur. Here are few examples or categories of such risks:

- Vetting process problems: Direct or indirect service providers in the supply chain may leak sensitive information of expose some system vulnerabilities.
- Poor or negligent information security practices by contractors or suppliers.
- Vulnerabilities within suppliers' premises, managements, practices, etc.
- Suppliers' usage of unverified or improper third-party software or systems.
- Suppliers have no proper security, access controls, or auditing systems.

Supply chain risk management policies and processes are identified, established, and managed by organizational stakeholders and any assigned employees.

Cross-functional communication or reporting mechanisms: While supply chain is a single business functional component, security and risk management issues are not; they cut across every major function and business area. Team in risk management should have the required technical and functional knowledge to be able to collect and plan for organization-wide risk management requirements. If the different business functions do not communicate and collaborate effectively especially with issues related to security and risk, small problems can eventually grow to be serious ones.

K0257: Knowledge of Information Technology (IT) Acquisition/Procurement Requirements

IT procurement requirements are defined earlier in this chapter as the demand for system, hardware, networks, software, personnel, services, etc. to be integrated in the business that the business currently lacks. Business owner, stakeholders, and their assigned employees or domain experts will have to evaluate current or existing systems to evaluate future demands or needs.

Team who will prepare IT acquisition or procurement requirements should study the problem domain first and understand its current state and environment. The request for proposal (RFP) document usually starts from a domain personnel or expert. Such document typically includes problems with the current or existing domain or business function and solution specifications. Such document is used to trigger the acquisition or procurement process and is considered one of the main reference documents.

Different business functions may have their own custom or unique acquisition/procurement requirements. On the other hand, IT/security requirements support more than one business function or the whole organization. Function or domain experts may not explicitly request IT or security requirements. However, acquisition team should have the right knowledge, skills, or expertise to add/update acquisition or procurements requirements to accommodate those, not requested, but yet necessary IT or security requirements. Acquisition team should also prepare cost-benefit analysis of all procurement requirements.

K0264: Knowledge of Program Protection Planning to Include Information Technology (IT) Supply Chain Security/Risk Management Policies, Anti-tampering Techniques, and Requirements

Program protection planning (PPP) aims to manage the effort of risk management for critical system resources and organization assets and ensure that important organization assets are adequately protected. Risk management team should prepare a deliverable document for this stage or milestone. This document captures Acquisition Information Assurance (IA) strategy, threat and vulnerability information, descriptions of (Critical Program Information) CPI and critical functions/components, etc. (Table 2.3). PPP may also reference many other documents related to procurement requirements, security, or risk management issues.

This document can be further divided into two parts (Acq.osd.mil 2011): (1) Milestone A plan should include an initial criticality analysis, candidate CPI, potential countermeasures, and information assurance strategy. (2) Milestone B plan should be a comprehensive document.

Information should be protected from adversaries and unauthorized personnel. This includes information that by itself is unclassified but if aggregated with other

Table 2.3 Program protection content (Acq.osd.mil 2011)

1. Program protection schedule	4: Horizontal protection
2 CPI and critical functions and components protection (protected items and countermeasures), criticality analysis	5: Threats, vulnerabilities, countermeasures, and assurance
2.1. Configuration Managements (CMs)	6: Other system security-related plans and documents
2.2. Critical Program Information (CPI) and critical components	7: Program protection risks
3: Critical Program Information (CPI) and critical components	8: Foreign involvement
3.1. Identification methodology	9: Processes for management and implementation of PPP
3.2. Inherited CPI and critical components	10: Processes for monitoring and reporting compromises
3.3. Organic CPI and critical components	11: Program protection costs
12. Program protection analysis	12.2: Critical Program iInformation (CPI) analysis
12.1: Information analysis	12.3: Trusted Systems and Networks (TSN) analysis

types of unclassified information, it may allow an adversary to clone, counter, or damage sensitive information.

For many government departments, such plan is required based on certain instructions/policies such as:

- DoDI 5000: https://aida.mitre.org/dodi-5000/
- DoDI 5000.02: Operation of the defense acquisition system
- DoDI 5200.39: Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation
- DoDI 5200.mm: Trusted Systems and Networks
- DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks
- DoDI 4140.67 DoD Counterfeit Prevention Policy
- DoDI 8500.01 Cybersecurity

Organizations may have many databases, datasets, or files that include information. There is a need first to classify such information from sensitivity, importance (to be protected and kept private), or privacy perspectives. Based on information classification, different protection plan mechanisms should be planned.

Information Sensitivity (Alsmadi et al. 2018)

Information must be protected based on its value as well as the likelihood that such information may be targeted for unauthorized disclosure. In general, information can fall in one of three categories based on its sensitivity: confidential information, private information, public information. This classification of information sensitivity is independent of the format and status. The only difference between these categories is the likelihood, duration, and the level of harm incurred in case an unauthorized access occurs.

Confidential information: Confidential information represents information that can result in significant level of risk when unauthorized disclosure, alteration, or destruction of that information occurs. Examples of confidential information include electronic medical records, financial information, and credit card transaction. In most cases, unauthorized access to such information can result in a significant monetary loss for the owner of the information as well as long-term harm. As a result, confidential information should be maintained in a way that allows only authorized people to access it. In such context access controls can be implemented in a way that allows access to data based on roles or on need basis. Keep in mind that the highest level of security controls needs to be applied to confidential information. Restricted information is one of the sensitive categories of confidential data. Restricted information is defined as "information that cannot be disclosed to an unauthorized organization or to one or more individuals" (Sengupta, 2011).

Private information: Private information represents information that can result in a moderate, minor risk in case unauthorized disclosure occurs. In general, all information that is not classified as confidential information or public information is considered private information. A reasonable level of security controls should be applied to private information (Ivancic et al. 2015).

Public information: Public information represents information that can result in a little or no risk in case unauthorized disclosure occurs. In most cases, public information is available to anyone who needs access to it. Examples of public information include but not limited to press release, maps, directories, and research publications.

The PPP document itself should be classified by content (Acq.osd.mil 2011). Threat and vulnerability information is commonly classified as secret or above. The program original classification authority is responsible for determining the appropriate classification of the PPP documents and related information.

Anti-Tamper (AT) is a key protection activity that is intended to prevent and/or delay exploitation of Resident CPIs in system resources. In USAF (Secretary of the Air Force/Special Programs Directorate (SAF/AQL)) unit, AT analysts ensure all CPIs are assessed and threats to CPIs are continually monitored to determine if AT measures are necessary and appropriate. The USAF AT team provides assessment reports of Commercial Off the Shelf products used in the protection of CPIs.

K0266: Knowledge of How to Evaluate the Trustworthiness of the Supplier and/or Product

In procurement analysis, usually procurement team will have to make choices between several possible suppliers and also products. Different criteria should be considered in selecting the final product and supplier. Selection criteria will not only consider the product but also the product supplier. In this section, we will focus on one criterion related to the supplier as well as the product; the trustworthiness. Other words usually connected and related to trustworthiness include: trust, reputation, credibility, confidence, integrity, and the more general word; quality. Mutual trust is an evolutionary process that increases or decreases with time based on companies' previous interactions with each other. Trustworthiness relations can also be inherited or transitive where for example if company A trusts supplier B, and company C trusts company A, company C may trust supplier B. In trust issues, there are also other parts that are transitive. For example, if a company is hiring a supplier for a product or service, not only the supplier should be trustworthy but also the supplier suppliers as well.

In some projects, procurement team may request on-site monitoring and audit for supplier processes and products. An inspection of the supplier's production processes and conformity management system can aid in better understanding of supplier environment and also build a level of trust.

Supplier and their products should work to gain trust from consumers. With the Internet, e-commerce, search engines, and online social networks, positive or negative feedback on service providers or products can quickly spread to a large number of audiences. The credibility of such feedback changes from one case or environment to another, but due to the importance of such feedback, investing on the credibility of such customers' feedback is also key and important for suppliers and their products.

Part of supplier process to show trustworthiness is transparency and opened with clients. They should show their conformance to standards: what is complete and what is not. They need to show summary of their security risk assessments, plans, etc. For companies, it is useful to be able to classify existing and candidate suppliers into three main categories (high trustworthy, medium, and low), based on several criteria that can be defined, evaluated, and updated with each procurement project.

Alves (2012a, b) paper showed that the following factors are important to evaluate the trustworthiness of suppliers:

- **Feedback**

  Feedback about supplier previous interactions with any client can provide valuable information about the organizations behavior in previous or historical transactions [3]. The feedback can be used to measure trustworthiness or credibility but can also help know more details about supplier processes, products, and overall quality issues.

  A similar criterion mentioned in EN50581 standard; historical experience with the supplier. This experience can be direct through the procurement company, some of its partners, or general experience extracted from credible supplier existing clients.

- **Legal bonds**

  Legal bonds or contracts can manage the supplier interactions with other companies.
- **International presence**

  There is no doubt that popularity is related to trust and credibility. Larger companies that have been in business for longer time and have branches in different locations can be seen as more trustworthy in comparison with small or startup-companies. That does not mean of course that this is always true. Additionally, when it comes to international issues, different companies may perceive trust issues differently when we consider the cultural impact or influence.
- **Monitoring**

  Monitoring encourages transparency and responsible behaviors. Monitoring can take different forms. For example, we mentioned in a different section that some contracts may require procurement team or company to conduct audit or monitoring activities with project suppliers.
- **Cooperative norms**

  This is related to the supplier organization values, process maturity, objectives, and principles.

  A similar evaluation factor described by EN50581 standard; results of previous inspections or audits especially when those inspections come from partners or trusted sources.

K0270: Knowledge of the Acquisition/Procurement Lifecycle Process

A generic engineering lifecycle model includes five stages:

- Material Solution Analysis
- Technology Development
- Engineering and Manufacturing Development
- Production and Deployment
- Operations and Support

The majority of engineering projects, processes, or products consider those five stages, either one time or through several cycles. Figure 2.5 shows DoD acquisition process and major stages (Acquisition University Press 2001).

Figure 2.5 shows four major stages in acquisition lifecycle:

- Pre-systems acquisition, concept, and technology development. In some model, this stage is divided into two stages: (1) concept refinement and decision, (2) technology development. Pre-systems acquisition stage is called “NEED” stage in DHS model (DHS 2008). Gaps and needs in existing systems are investigated and validated.

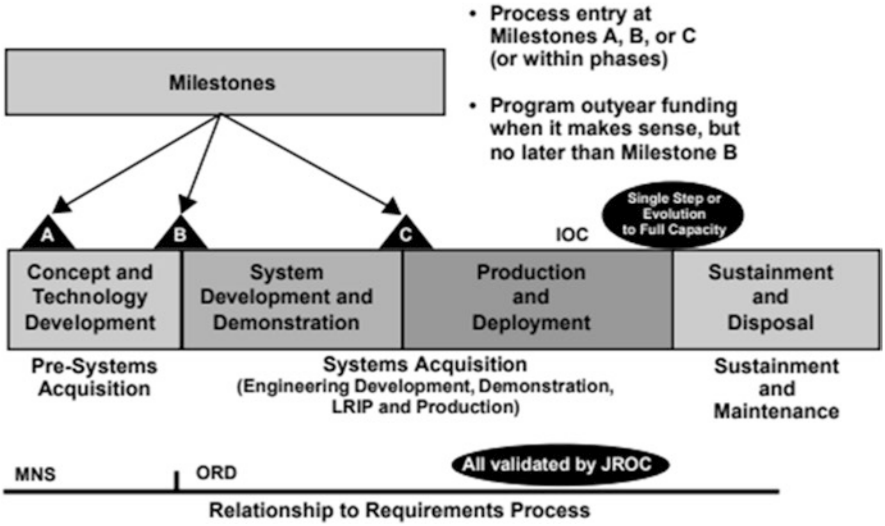

• Process entry at Milestones A, B, or C (or within phases)
• Program outyear funding when it makes sense, but no later than Milestone B
Milestones
A
B
C
IOC
Single Step or Evolution to Full Capacity
Concept and Technology Development
System Development and Demonstration
Production and Deployment
Sustainment and Disposal
Pre-Systems Acquisition
Systems Acquisition (Engineering Development, Demonstration, LRIP and Production)
Sustainment and Maintenance
MNS
ORD
All validated by JROC
Relationship to Requirements Process

Fig. 2.5 DoD acquisition process (Acquisition University Press 2001)

- In concept refinement, several alternative concepts are evaluated and compared that can satisfy project objectives or requirements. Risks associated with each concept are also discussed and analyzed. At the end of this stage, a decision must be made to advance concepts to the next stage.
- System development and demonstration.
- Production and deployment: In this stage, product is deployed and evaluated on its real environment. This stage is divided into two sub-stages in some models: initial deployment or operational capability (IOC) and full; FOC.
- Sustainment and maintenance: This includes all activities after the first deployment cycle. In other models, this same stage is called operations and support. In some DoD or military models, this stage may include the term “Disposal”; in some cases, explicit process/stage is required to dispose or retire the product properly.

US department of Homeland Security (DHS) defines four stages for acquisition lifecycle (Hutton 2010):

- Identify assets needed functional capabilities and how those capabilities can serve requested objectives.
- Capabilities alternative solutions, cost, and schedule estimations.
- Developing, testing, and deploying selected alternatives.
- Evaluate asset after solution deployment to judge if objectives are met and moved, or not to full production.

Federal Aviation Administration proposed an acquisition lifecycle model of the stages: mission analysis, investment analysis, and solution implementation; a cycle of operation: in-service management and service life extension; finally, system disposal stage (Fig. 2.6).

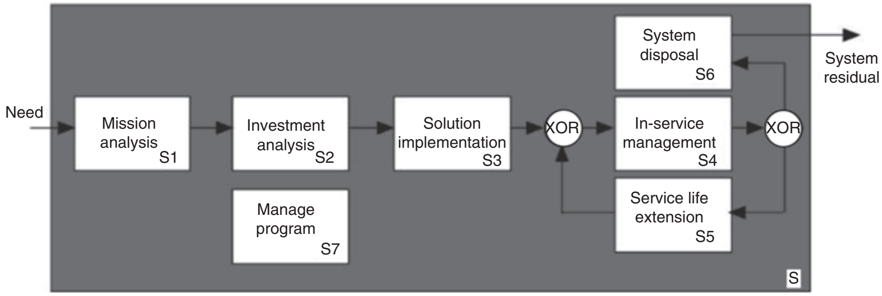


Fig. 2.6 FAA acquisition lifecycle model (Grady 2006)

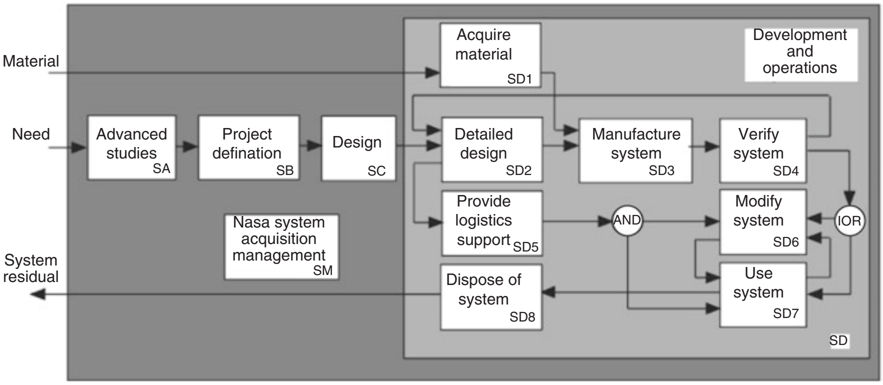


Fig. 2.7 NASA acquisition lifecycle model (Grady 2006)

Similar to FAA, NASA adopts a semi-evolutionary model in development, deployment, and operational stages can go in several increments or cycles (Fig. 2.7).

Defense Acquisition University

Defense Acquisition University (DAU) is a corporate university of the US DoD that focuses on: Acquisition, Technology, and Logistics (AT&L) training to military and federal civilian staff and contractors (https://www.dau.mil/). Many relevant contents to this chapter can be found in the University website. Similarly, DoD directive 5000 is a major reference for government policies on acquiring material systems and infrastructure.

Positions in the acquisition workforce have different acquisition duties that can fall into 15 functional areas. For each area, certification is available at three levels: basic, intermediate, and advanced: Auditing, Business Cost Estimating and Financial Management, Business Cost Estimating, Business Financial Management, Contracting, Facilities Engineering, Industrial/Contract Property Management, Information Technology, Lifecycle Logistics, Production, Quality and Manufacturing, Program Management, Purchasing, Small Business, Systems Planning, Research, Development and Engineering—Program Systems Engineering, Science and Technology Manager, Engineering, Test and Evaluation.

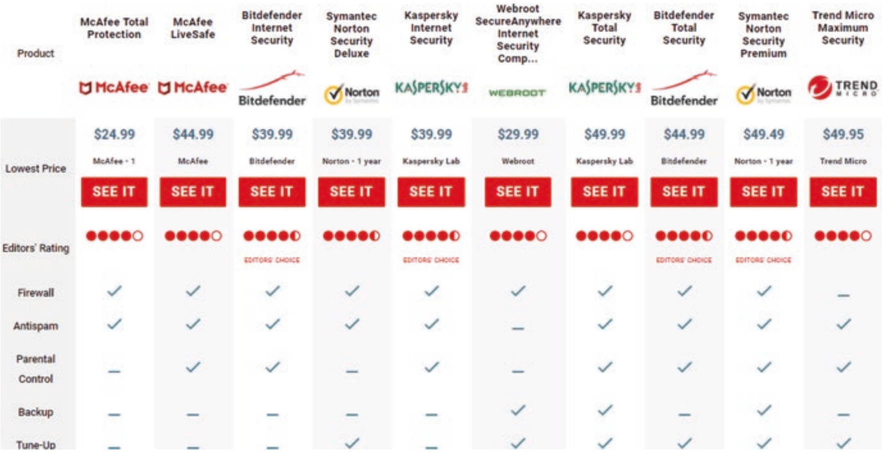
K0523: Knowledge of Products and Nomenclature of Major Vendors (e.g., Security Suites—Trend Micro, Symantec, McAfee, Outpost, Panda, Kaspersky) and How Differences Affect Exploitation/Vulnerabilities

Security suites or anti-malware systems provide full or integrated security control solutions that protect against a large spectrum of malwares or attacks. Earliest versions of such tools were called antiviruses where the only or most popular malwares at the time were viruses. The term malware is now used to refer to all categories of malicious software such as: viruses, worms, Trojan horses, spywares, and ad-wares. Similarly, the term security suites indicate a recent trend in security controls to provide a one-for-all security suite that can provide all categories of security controls or functions. For customers, and IT support this can be more convenient having to deal with and configure one centralized security suite. We can also avoid the issue of conflicts of actions or decisions between the different security controls. For example, we may have a gateway firewall that has a role to block a certain traffic while the same traffic is allowed, and necessary from a viewpoint of another security control. Currently, with many security controls, the role of precedence usually is enforced where if a security control denied a certain traffic and dropped it, there is no way for further security controls to reverse that.

On the other hand, with centralization, the issue of "single point of attack" or "single point of failure" always rises. For a large enterprise, with a large number of assets, databases, etc. can one centralized security control be sufficient? How much confidence we have that this centralized security control is making always the right permit and deny decisions (e.g., consider false-positive and false-negative cases), and how much confidence we have that such centralized security suite is not going to be a target itself (e.g., tampering to change, add/delete some sensitive roles in its role-engine)?

In addition to malwares, there are other categories of security controls such as firewalls and Intrusion Detection/Protection systems: IDS/IPS. Details on those categories can be found in other parts of this book. Major focus in this section is on the major vendors in this area of anti-malwares or integrated security controls. Security suites can be classified and compared according to the list of features they can provide in comparison with cost (Fig. 2.8).

While paid security suites tend, usually to perform better than those that are free or open source, some no-cost options, such as: Avira, Panda, ClamWin, Avast, Microsoft Security Essentials, and AVG, hold up well. The rankings can vary



Product	McAfee Total Protection	McAfee LiveSafe	Bitdefender Internet Security	Symantec Norton Security Deluxe	Kaspersky Internet Security	Webroot SecureAnywhere Internet Security Comp...	Kaspersky Total Security	Bitdefender Total Security	Symantec Norton Security Premium	Trend Micro Maximum Security
	McAfee	McAfee	Bitdefender	Norton	KASPERSKY	WEBROOT	KASPERSKY	Bitdefender	Norton	TREND MICRO
Lowest Price	$24.99 McAfee - 1 SEE IT	$44.99 McAfee SEE IT	$39.99 Bitdefender SEE IT	$39.99 Norton - 1 year SEE IT	$39.99 Kaspersky Lab SEE IT	$29.99 Webroot SEE IT	$49.99 Kaspersky Lab SEE IT	$44.99 Bitdefender SEE IT	$49.49 Norton - 1 year SEE IT	$49.95 Trend Micro SEE IT
Editors' Rating	●●●●○	●●●●○	●●●●◐ EDITORS' CHOICE	●●●●◐	●●●●◐ EDITORS' CHOICE	●●●●○	●●●●○	●●●●◐ EDITORS' CHOICE	●●●●◐ EDITORS' CHOICE	●●●●○
Firewall	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
Antispam	✓	✓	✓	✓	✓	–	✓	✓	✓	✓
Parental Control	–	✓	✓	–	✓	–	✓	✓	✓	✓
Backup	–	–	–	–	–	✓	✓	–	✓	–
Tune-Up	–	–	–	✓	–	✓	✓	✓	✓	✓

Fig. 2.8 The Best Security Suites of 2018 (pcmag.com)

significantly from 1 year to another and even from one evaluator to another (e.g., based on features of interest). The main advantage of buying a security suite from a vendor is the ability to get help and support. With the sensitivity of security problems or breaches and the urge to solve them quickly, one-time effective support can justify avoiding the free or open source option.

In terms of acquisition, there are different models on how security suite services are sold or provided. In addition to the free or open source options, early generations of security controls have the option of one-time payment. However, current commercial security suites offer yearly subscriptions. Additionally, options can vary between costs per user or individual and cost per site or enterprise. Different factors cause the transition to this model:

- **Internet and bandwidth availability**: Early generations of Internet services were limited and slow. With the increase of available bandwidth for users and businesses, it became possible to provide real-time services. Many security suites offer the option to scan your machine without the need to install any software locally (e.g., software as a service—SaaS).
- **The continuous evolution of security threats**: Security threats change daily and new threats, vulnerabilities, or malware are discovered. The need to have real-time or frequent update for security suites is very important. In this scope, the term, zero-day attack is used to refer to attackers taking advantage or recently discovered vulnerabilities. They hope that such vulnerabilities are still valid in some computers, especially those that they did update their security suites (Assuming that security provider already discovered such vulnerability and created a fix/update for it).
- **Different platforms and mobility issues:** Users want to protect their laptops, desktops, smart phones, tablets, etc. They prefer to have one account and subscription that allow them to provide the same protection level from the same provider on their different computing environments.

S0086: Skill in Evaluating the Trustworthiness of the Supplier and/or Product

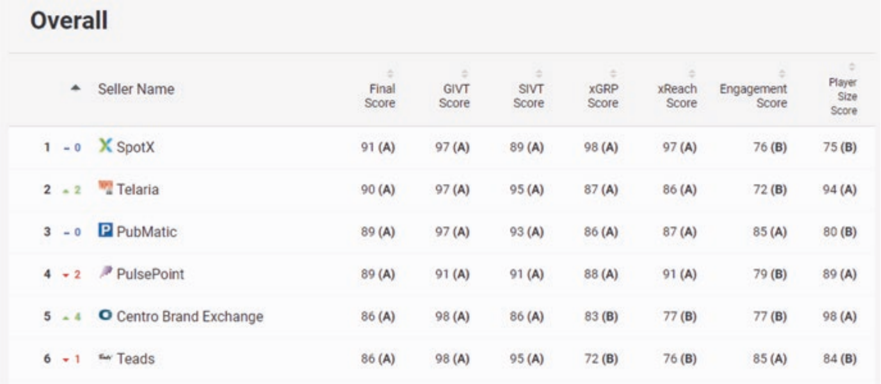
S0086-1: There are examples of websites that provide trust rankings for certain industrial sectors. For example, the website: Pixalate (http://www.pixalate.com) includes Global Seller TrustIndex for digital advertisers (Fig. 2.9). Investigate Pixalate metrics (i.e., columns in Fig. 2.9) from a seller or supplier perspective.

S0086-2: Similar to Pixalate, make your own research to find another website or tool that evaluate the trust of suppliers or sellers. Show the different metrics or attributes used in the tool or website and how it can be utilized to compare between different sellers and suppliers.

A0009: Ability to Apply Supply Chain Risk Management Standards

Government contractors are required to comply for protecting the confidentiality of Controlled Unclassified Information (CUI) with National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-171. It is intended to force contractors to implement reasonably expected security requirements. Non-compliance requirements means lost business and potential fines.

In this Ability, download and use NIST compliance 800-171 compliance template for ITS managed systems: (e.g., https://www.csiac.org/wp-content/uploads/2016/01/SRC-800-171-Requirements-Worksheet.xlsx, or https://www.complianceforge.com/nist-800-171-compliance-criteria-worksheet.html, or https://library.educause.edu/resources/2016/9/nist-sp-800-171-compliance-template, or https://its.uiowa.edu/sites/its.uiowa…/NIST-SP-800-171-Template-ITSManaged.xlsx). Then select your organization and make sure you complete the template for your selected or evaluated organization. Table 2.4 shows a small sample to show the columns that should be included in the evaluation.



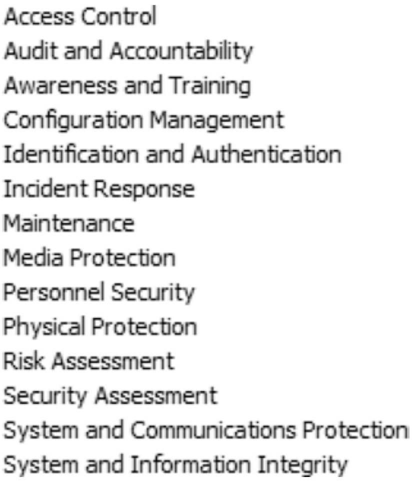
Overall

		Seller Name	Final Score	GIVT Score	SIVT Score	xGRP Score	xReach Score	Engagement Score	Player Size Score
1	- 0	SpotX	91 (A)	97 (A)	89 (A)	98 (A)	97 (A)	76 (B)	75 (B)
2	▲ 2	Telaria	90 (A)	97 (A)	95 (A)	87 (A)	86 (A)	72 (B)	94 (A)
3	- 0	PubMatic	89 (A)	97 (A)	93 (A)	86 (A)	87 (A)	85 (A)	80 (B)
4	▼ 2	PulsePoint	89 (A)	91 (A)	91 (A)	88 (A)	91 (A)	79 (B)	89 (A)
5	▲ 4	Centro Brand Exchange	86 (A)	98 (A)	86 (A)	83 (B)	77 (B)	77 (B)	98 (A)
6	▼ 1	Teads	86 (A)	98 (A)	95 (A)	72 (B)	76 (B)	85 (A)	84 (B)

Fig. 2.9 Pixalate seller TrustIndex and metrics (http://www.pixalate.com)

Table 2.4 NIST 800-171 compliance template (https://its.uiowa.edu/sites/its.uiowa…/NIST-SP-800-171-Template-ITSManaged.xlsx)

NIST 800-171 control number	Control family	Control text	NIST 800-53 mapped control	Requirement	Res. party	Responsible party actions	Notes
3.1.1	**Access Control**	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)	AC-2, AC-3, AC-17	Maintain list of authorized users defining their identity and associated role and sync with system, application, and data layers. Account requests must be authorized before access is granted	ITS	Applies UI Enterprise Active Directory Policy (IT-02), in conjunction with Data Owner approval for individual access requests	ITS performs all authentication actions, but the Data Owner is still responsible for determining who gets added to the ITS-owned OU/group
3.1.2	**Access Control**	Limit information system access to the types of transactions and functions that authorized users are permitted to execute	AC-2, AC-3, AC-17	Utilize access control lists (derived from 3.1.1) to limit access to applications and data based on role and/or identity. Log access as appropriate	ITS	Applies UI Enterprise Active Directory Policy (IT-02); user access requests checked against AD database for authorization. All access requests are logged	



Access Control
Audit and Accountability
Awareness and Training
Configuration Management
Identification and Authentication
Incident Response
Maintenance
Media Protection
Personnel Security
Physical Protection
Risk Assessment
Security Assessment
System and Communications Protection
System and Information Integrity

Fig. 2.10 NIST 800-171 control families

To complete the template, you have to make sure to include all 14 NIST 800-171 control families (Fig. 2.10).

A0031: Ability to Conduct and Implement Market Research to Understand Government and Industry Capabilities and Appropriate Pricing

Market research can be used by service providers as well as service consumers. For example, a person looking for an attorney may use an online market research to see how typically attorneys in their area charge for similar cases. New attorneys, on the other hand, should consider when they decide their services' pricing what other attorneys in the area are asking for those similar services and hence they should do their market search as well.

Before doing a market research, we should first have a good understanding of what we are looking for (e.g., project requirements). Without such knowledge, market research will be very unfocused and not useful at the end.

- Pick a project (e.g., possible software to buy). Then find 3–5 most possible suppliers for this software or information system. Make a comparison between those suppliers using SWOT (Strengths, Weaknesses, Opportunities, and Threats) analysis. For each one of those four categories, rank your 3–5 candidate suppliers from best to worst. Find the final best candidate based on aggregating results from the four categories.
- Market research can be classified into: primary (making your own research from scratch) or secondary (relying on others' information or resources). It can also be classified into: quantitative (based on hard facts and statistical data) or qualitative (e.g., based on surveys, feedbacks from customers).

- Conduct your own research to make a comparison between those four different methods, strengths, and weaknesses of each one of those methods or techniques.
- In the scope of Porter five forces model, describe from a market research and appropriate pricing perspective, how will each force of those five forces can expand or limit the need to conduct market research when acquiring a product or service.
- Study US DoD facilities pricing guide (DOD UNIT COST/AREA COST FACTORS AND FACILITIES PRICING GUIDES: https://www.wbdg.org/FFC/DOD/UFC/ufc_3_701_01_2011_c13.pdf, July 2017). Show some of the factors described in the guide on how to decide or judge proper product pricing.

A0039: Ability to Oversee the Development and Update of the Lifecycle Cost Estimate

For most products or services, there are three main stages related to budgeting and cost:

- Initial cost (e.g., cost to analyze, need, research, design, develop or acquire, deploy)
- Annual or maintenance cost
- Replacement or upgrade costs
- Different models and products can have different percentages of overall cost. Figure 2.11 shows one example and distributed among the three stages (DOE 2018). Pick a project of your selection and evaluate the cost estimate distribution among those three main stages (in percentage).
- For product manufacturing company or supplier, there are four cost categories in DoD 5000.4-M “Cost Analysis Guidance and Procedures”: (1) research and development, (2) investment, (3) operating and support, and (4) disposal.

For cost estimation, several techniques can be used such as: (1) parametric, (2) analogy, (3) engineering estimates, and (4) actual cost.

- Develop or use existing project requirements. Those can be related to a project you are working on or through Internet search. Then use Microsoft project management software to develop Work Breakdown Structure (WBS). Estimate project overall cost based on its WBS.
- The Excel template from US National Park Services (NPS): (Life Cycle Cost Estimate Template 3-2-2011—National Park Service, https://www.nps.gov/dscw/upload/LifeCycleCostEstimateTemplate_3-2-11.xlsx). Use this template to complete all costs associated with a project of your selection (e.g., the project you have selected in the previous section).

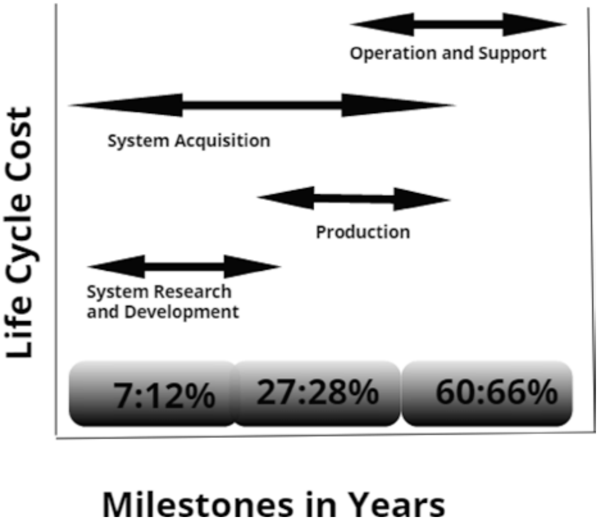


Fig. 2.11 Lifecycle cost distribution (DOE 2018)

A0045: Ability to Evaluate/Ensure the Trustworthiness of the Supplier and/or Product

Figure 2.12 shows a model to evaluate suppliers based on several factors (Alves et al. 2012a, b).

- Pick two suppliers of your choice. Make your own research to find out (estimated values) for all the attributes listed in the figure.

The original paper collected such data based on customers' surveys. Alternatively, you can pick e-commerce websites in which most of those attributes are available publicly. If some attributes are not available, estimate or ignore (make sure to take the same actions for all evaluated suppliers).

- In order to make a quantitative comparison, you can use the equation proposed in the paper:

  TAgS = 0.036*Coop37 + 0.072*Coop38 + 0.013*Benev42 + 0.008*Fb31 + 0.006*Coop32 + 0.156*Vincul26 + 0.003*Credi40 + 0.049*Fb30 + 0.057* Fb29 + 0.116*Monit22 + 0.061*Monit23 + 0.196*Vincul28 + 0.069*Inter7 + 0.022*Inter8 + 0.005*Dim11

  Refer to the original paper to find out exact attributes used in the equation from the proposed model.

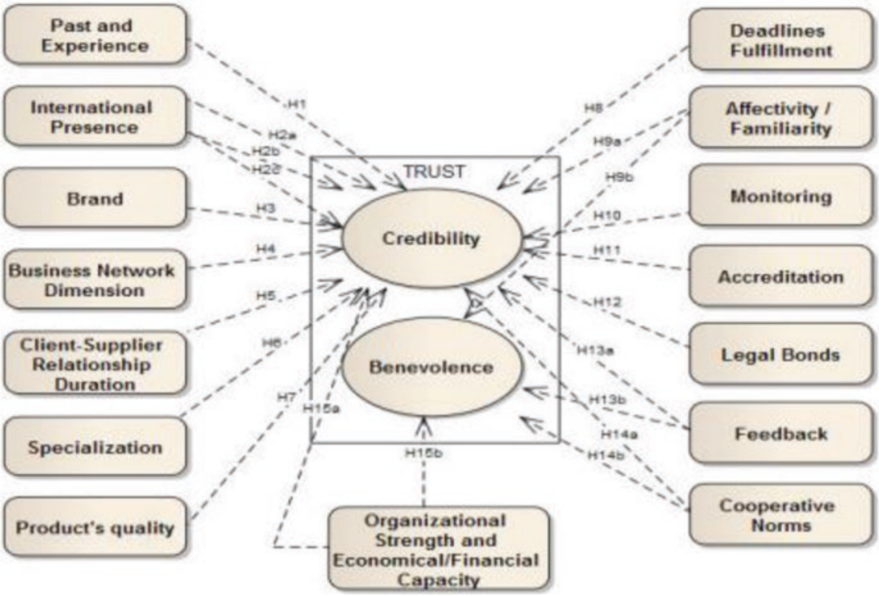


Fig. 2.12 A model to evaluate suppliers' trustworthiness trustworthiness (Alves et al. 2012)

A0056: Ability to Ensure Security Practices Are Followed Throughout the Acquisition Process

We described in previous sections the different stages in the acquisition process based on different models or standards (Please see Figs. 2.5, 2.6, and 2.7 in addition to Fig. 1.3 in dtic.mil document (http://www.dtic.mil/dtic/tr/fulltext/u2/a495389.pdf)).

Each acquisition stage should explicitly include security practice and assessment elements. Select an example of an RFP or acquisition document (either from your organization or from public Internet sources), then make sure it contains the following security-related elements, organized according to the different acquisition stages:

1. Planning stage: The following are security practices or components that should exist at this stage:

    - Initial risk assessment: Based on the nature of the acquisition stage, there is a need to protect the process and the information involved throughout this stage. For example, if the acquisition stage includes research and development, it is important to protect the integrity of the process, copyright materials, etc.

      (Polydys and Wisseman paper 2009a, b) sections 2.1.2 and 3.1.1 include several questions to evaluate acquisition initial risk assessment. Answer all those questions for your selected project.

- Solution alternatives: Several acquisition alternatives exist to acquire a software, information system, service, hardware, etc. Acquisition team will have to pick one alternative.

  (Polydys and Wisseman paper 2009a, b) section 2.1.3 described four steps when considering design or solution alternatives. Answer all those steps for your selected project.

2. Requirements analysis stage: In this stage, project requirements are developed based on initial need study. (Polydys and Wisseman paper 2009a, b) section 2.2 describes examples of software assurance requirements that should be considered at this stage. Answer all those requirements for your selected project.
3. Acquisition strategy

   (Polydys and Wisseman paper 2009a, b) section 2.3 describes examples of security practices that should be considered at this stage. Answer all those security practices for your selected project.
4. Acquisition evaluation

   Questionnaires/surveys can be developed to respond to some of the security concerns related to the acquired product. Use the table described in (Polydys and Wisseman paper 2009a, b) section 2.5.2 SwA Concern Categories to list in detail all security concerns related to the product you are evaluating.
5. Complete the steps described in (Polydys and Wisseman paper 2009a, b) and evaluate your project/product accordingly.

A0056-2

Evaluate SOAR software security assurance model (Software security assurance, State-of-the-Art Report (SOAR)) July 31, 2007, Information Assurance

Technology Analysis Center (IATAC), Data and Analysis Center for Software (DACS), http://www.dtic.mil/dtic/tr/fulltext/u2/a472363.pdf). In particular, focus on section 5: SDLC Processes and Methods and the Security of Software. Evaluate all the elements in section 5 according to the acquisition project you have selected in this chapter.

Evaluate SAF software security assurance model (Christopher Alberts and Carol Woody, Prototype Software Assurance Framework (SAF), from SEI, CMU, April 2017). Evaluate all the elements according to the acquisition project you have selected in this chapter.

A0064: Ability to Interpret and Translate Customer Requirements into Operational Capabilities

Requirements are fulfilled through operational capabilities. We described in an earlier section of this chapter system models that divide project scope into problem and solution domains. Customers' requirements involve the analysis of the problem domain and study its needs. Operational capabilities involve the design, implementation, and deployment of "a solution" for the problem domain "needs." It is important for acquisition team to be able to understand customer project requirements. It is then important to be able to translate those requirements as problems into solution elements or operational capabilities. It is also important to be able to compare between different possible solutions. It is also important to realize the "fitness" of the proposed solution to the problem or the "needs." Acquisition team should also understand all this in the scope of budget and cost estimation and be able to evaluate or assess services based on cost.

- Download a Capability Development Document (CDD) template from Internet sources (e.g., https://www.dau.mil/cop/rqmt/Lists/Tools/AllItems.aspx, or http://acqnotes.com/acqnote/acquisitions/capability-development-document-cdd, or http://www.acqnotes.com/Attachments/CDD%20Writers%20Guide.pdf).

For your selected project, make sure you completed the template sections. The template should include, as minimum the following sections: (1) Capability Discussion, (2) Analysis Summary, (3) Concept of Operations Summary, (4) Threat Summary, (5) Program Summary, (6) System Capabilities Required for the Current Increment, (7) Family of System and System of System Synchronization, (8) Information Technology and National Security Systems (IT and NSS) Supportability, (9) Intelligence Supportability, (10) Electromagnetic Environmental Effects (E3) and Spectrum Supportability, (11) Assets Required to Achieve Initial Operational Capability (IOC), (12) Schedule and IOC/Full Operational Capability (FOC) Definitions, (13) Other Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF) Considerations, (14) Other System Attributes, and (15) Program Affordability.

Capabilities can be developed in different stages or milestones: Initial Capabilities Document (ICD) and Capability Production Document (CPD). Different types of relations may exist between capabilities at those three different levels or stages (e.g., part of, related to). Other important deliverables to consider in CDD include: Key Performance Parameters (KPP) and Key System Attributes (KSA) address performance.

Bibliography

(CSD), NIST Computer Security Division (2010) NISTIR 7622 draft, piloting supply chain risk management practices for federal information systems (DRAFT), pp 1–78

Acq.osd.mil (2011) Program protection plan outline & guidance, Ver. 1.0. Deputy Assistant Secretary of Defense, Systems Engineering. https://www.acq.osd.mil/se/initiatives/init_pp-sse.html

Alsmadi I, Burdwell R, Aleroud A, Wahbeh A, Ali Al-Qudah M, Al-Omari A (2018) Security and access controls: lesson plans. In: Practical information security. Springer, Cham

Alves P, Campos P, Oliveira E (2012a) Modeling the trustworthiness of a supplier agent in a B2B relationship. In: Camarinha-Matos LM, Xu L, Afsarmanesh H (eds) Collaborative networks in the internet of services. PRO-VE 2012. IFIP advances in information and communication technology, vol 380. Springer, Berlin

Alves P, Campos P, Oliveira E (2012b) Modeling the trustworthiness of a supplier agent in a B2B relationship, PRO-VE 2012. International Federation for Information Processing IFIP AICT 380, pp 675–686

Blos MF, Quaddus M, Wee HM, Watanabe K (2009) Supply chain risk management (SCRM): a case study on the automotive and electronic industries in Brazil. Supply Chain Manag 14(4):247–252

Boyens JM, Paulsen C, Moorthy R, Bartol N (2015) Supply chain risk management practices for federal information systems and organizations. https://doi.org/10.6028/nist.sp.800-161

Defense Acquisition University Press (2001) System engineering fundamentals. http://acqnotes.com

Department of Homeland Security Cyber Security Division (2007) Software assurance in acquisition: mitigating risks to the enterprise, Draft Version 1.0

DHS (2008) Acquisition instruction/guidebook, 102-01-001, INTERIM, Version 1.9

DOE (2018) DOE G 430.1-1 Chp 23, life cycle cost estimate. https://www.directives.doe.gov/directives-documents/400-series/0430.1-EGuide-1-Chp23

Grady JO (2006) System requirements analysis. Academic, Cambridge

Hutton JP (2010) United States Government Accountability Office, Deepwater requirements, quantities, and cost require revalidation to reflect knowledge gained, GAO-10-790, https://www.gao.gov/assets/310/307742.html

Ivancic WD, Vaden KR, Jones RE, Roberts AM (2015) Operational concepts for a generic space exploration communication network architecture, Technical report, NASA Glenn Research Center

National Institute of Standards and Technology (NIST) 800-161 (2015), Supply chain risk management practices for federal information systems and organizations. U.S. Department of Commerce, p 9

Polydys ML, Wisseman S (2009a) Software assurance in acquisition: mitigating risks to the enterprise. Technical paper. http://www.dtic.mil/dtic/tr/fulltext/u2/a495389.pdf

Polydys ML, Wisseman S (2009b) Software assurance in acquisition: mitigating risks to the enterprise. Occasional paper, Information Resources Management College. http://www.dtic.mil/dtic/tr/fulltext/u2/a495389.pdf

Porter M (2008) Competitive advantage: creating and sustaining superior performance. Simon and Schuster, New York

Sengupta A (2011) Method for processing documents containing restricted information: Google patents

Swanson M, Bartol N, Moorthy R (2010) Piloting supply change risk management practices for federal information systems. National Institute of Standards and Technology (NIST), U.S. Department of Commerce, p 1

Tummala R, Schoenherr T (2011) Assessing and managing risks using the Supply Chain Risk Management Process (SCRMP). Supply Chain Manag 16(6):474–483

US Chamber of Commerce, International Affairs (2016) Preventing de globalization: an economic and security argument for free trade and investment in ICT. https://www.uschamber.com/sites/default/files/documents/files/preventing_deglobalization_1.pdf

Chapter 3
Continuity Planning and Disaster Recovery

Business continuity planning focuses on making sure that business will continue to run under failures, problems, disasters, etc. Response to problems can take different alternatives from avoidance, preventive or protective measures to backup and recovery measures. This chapter covers all KSAs related to those two concepts in particular.

K0210: Knowledge of Data Backup and Restoration Concepts

Data, information, knowledge, and experience are different terms that indicate data in different processing stages or levels. We use data for simplicity to refer to all those terms. Data represents the main inputs and outputs for any information system. In fact, any information system can be seen as a processor that takes input data in some form and creates output or processed data based on one or more input data along with different processes, algorithms, etc. that make the output data valuable to the business owning that information system. Operational data in servers and databases represent the dynamic form of the data. Data at rest or static data exist in storage devices. Since failures, security problems, natural disasters, etc. are inevitable, data backup is not a surplus task that only companies with serious databases and information systems should consider. Even individuals should always make sure that data in their personal computers have been backed up. Possibly, the frequency of data backup process and the required time to return to earlier versions of a system can vary from personal use to enterprises with larger spectrum of users, but the importance of the backup process is applicable to almost all users.

Restoration is the reverse process of bringing data from backup sources to live systems so that they can replace a main disk or database corrupted data or failures.

I. Alsmadi, *The NICE Cyber Security Framework*,
https://doi.org/10.1007/978-3-030-02360-7_3

Types of Storage Destinations

Storage devices went through several cycles of progress in the last several decades. Two major factors navigated that progress: storage size and speed of access for those storage devices for both backup and restoration. When compared with CPU, memory or network data processing time (i.e., latency), so far data processing time through storage devices is the slowest out of the 4 (Fig. 3.1).

External Hard Drives, Flash Drives, etc.

For individual users and small size companies, USB external hard and flash drives can be a preferred option in many situations. Cost, portability, and convenience are main advantages to consider such option.

USB data transfer standard with no close competition is now the most popular and truly universal standard or bus that is used in a very large number of applications that go even beyond computing environments and applications.

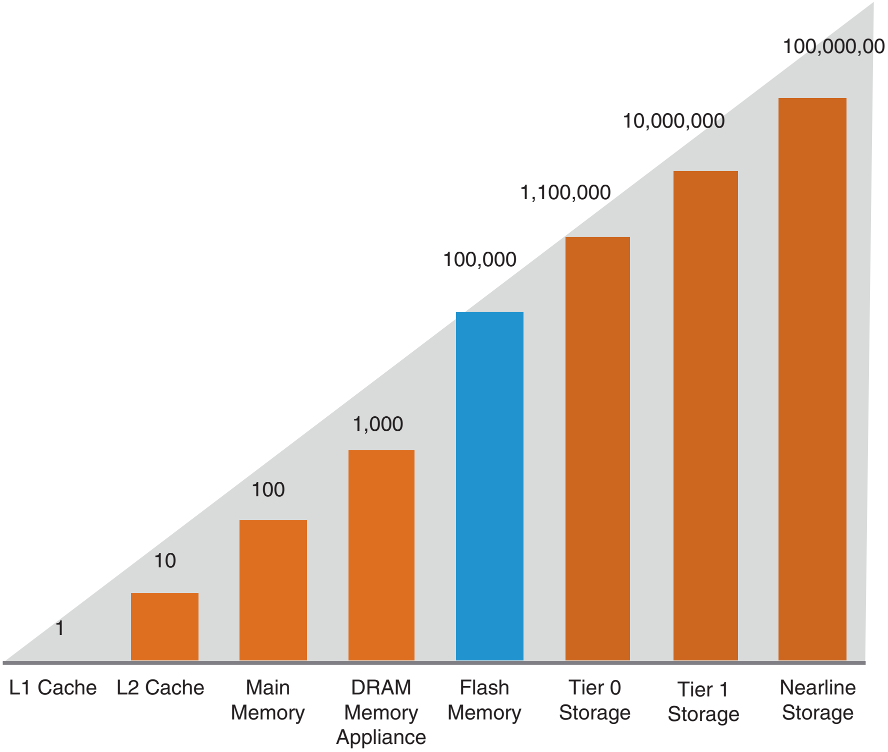


Fig. 3.1 Data processing latency in nano-seconds (Richardson 2012)

USB standard went through three stages of speed. The current highest speed USB3 is fast and can backup and restore a large amount of data in a relatively short amount of time.

In terms of reliability, such external disks have a fair amount of failures that may lead to data lost or corruption. Due to their small sizes, they can be lost or stolen.

Network Attached Storage Systems

Network attached storage (NAS) provides data backups through the network and allows for large amounts of storage. A NAS storage can be a hard drive with an Ethernet port. Other NAS solutions can use WIFI and or multiple hard drives in a RAID system. The benefit, in comparison with an external USB hard drive connected to the server, is that NAS can ease the load on servers through the backup and restoration process.

NAS can be seen as a network-based file server that can authenticate clients to access resource files.

Storage Area Networks

Storage area networks (SAN) utilize Fiber Channel interconnects and connect a set of storage devices for data sharing. SAN can service largely enterprises in comparison with NAS and is typically more expensive. SAN storage can be composed of high performance disk arrays.

While NAS operates on single files, SAN operates on multiple devices. Both storage options typically utilize RAID servers and employ different storage management tasks such as access control and encryption. NAS accesses data as files while SAN accesses data as blocks. This gives SAN a robust feature over SAN when handling interactive systems that support many high-speed file transfers with Giga or terabytes of files.

RAID

RAID (Redundant Array of Independent or Inexpensive Disks) is a disk or storage virtualization method to integrate one or more physical disks to act in a form of an array of logical disks. Redundancy is a key work in RAID as the different disk array needs to work completely independent from each other, if they have to, in backup or failure situations. Seven models or levels of RAID (i.e., RAID0, RAID1, RAID6) exist from which system storage designers can pick from. The different levels try to balance between reliability, size and availability, efficiency and overhead as the major factors that distinguish and decide which RAID level best to use. For example, RAID0 offers striping, with no mirroring, unlike RAID1. As a result, RAID0 does not support reliability and fault tolerance. RAID1 offers redundancy but does not offer striping which will make it less efficient than RAID0.

Remote or Online Storage

With the continuous growth of cloud services, renting storage space from cloud service provider as a viable option for many users and companies. Large files can easily be shared and exchanged between users and partner organizations without the need to have local storage devices or the need to overhead the local network. Cloud service provider is also responsible for the correctness, availability and integrity of data, and the need to have and acquire it whenever required.

Cloud services are expensive in comparison with previous options. They are paid periodically or based on demand. This is a continuous cost and overhead as an alternative to one-time upfront investment in previous options.

Security of data in the cloud is also another drawback and concern. Regardless of how much cloud companies are working to demonstrate and claim the protection of data, from failures and exposures, within their premises, in practical, they can't proof such claims (especially when it comes to possible exposures, rather than corruption). The US government contracts enforce several policies on cloud service providers, if acquired from public companies. For example, cloud service provider should always verify that data is hosted physically in the USA.

Backup vs. Archive

Both backup and archive look similar in terms of storing enterprise data. However, in terms of goals and details the two tasks are different. Unlike backup, archived data do not need to come back operational any time. As a result, the process of archiving may change how data will look like (in the archived version) and need not look like or work as it is in the operational or life version.

K0021: Knowledge of Data Backup, Types of Backups (e.g., Full, Incremental), and Recovery Concepts and Tools

K0365: Knowledge of Basic Back-Up and Recovery Procedures Including Different Types of Backups (e.g., Full, Incremental)

Backup can take different types of levels. The first popular and trivial backup is "**full back-up**" to backup all source data, all data/files types or extensions, applications, logs, etc. The major advantage of this backup is that it is very easy to implement and does not require algorithms to classify or distinguish user from application generated data or distinguish data files from application files, and so on. On the other hand, the disadvantage is that such backup will typically require a large destination storage devices or systems especially with databases from medium to large enterprises. The process to backup large sources of data can also be time-consuming and can impact system resources.

As an alternative to full backup, partial or selective backup methods focus on predefined or user-defined data sources. Applications that can perform backup processes usually include those two options (i.e., predefined data sources: folders, directories, etc. or user-defined data sources in which users can choose folders, directories, etc. from their data sources.)

Incremental backup (which can be implemented for both full and selective backup methods) is implemented through revisiting all destination backup files and folders and do not re-backup those files or folders that are identical between the source and the destination. Only files or folders that are new to the destination or that are different from the source. The major goal of incremental backup is to reduce the amount of time required to complete frequent or periodic backup activities. The amount of reduced time or overhead between the full and incremental backup can vary especially as incremental backup has its own overhead (through the need to investigate destination files and compare them with source files). The restoration process from incremental backup is also different from the restoration process from full backup. To restore from an incremental backup, we need to restore last full backup and every incremental backup that occurs up to the required or failure point.

Full back-up can be combined with incremental backup. For example, a company may plan a policy to conduct backup daily: full back-up once a week and incremental backup the rest of the days. In this case, every other day (than the full backup day) will include changes in that day.

As an alternative to alternative backup, differential backup can be used. In the previous example, it will be similar to incremental backup except that each day backup will have changes from the previous backup rather than changes from the full backup day. In other words, backup and restore times in the differential backup will be shorter than those of the incremental backup.

Another variation from incremental backup is called "synthetic backup." In the attempt to balance between full backup and the advantage of having all data saved, and incremental backup, with more efficiency and less time, synthetic backup creates incremental backups in real time and eventually frequent full backups (e.g., through special services or applications in the backend server).

The frequency of the backup (i.e., hourly, daily, weekly) can also vary from one system or organization to another. Several factors can impact choice such as the size of the organization or its data sources, the volume of data, the freshness/volatility of the data, or how often such data is changing.

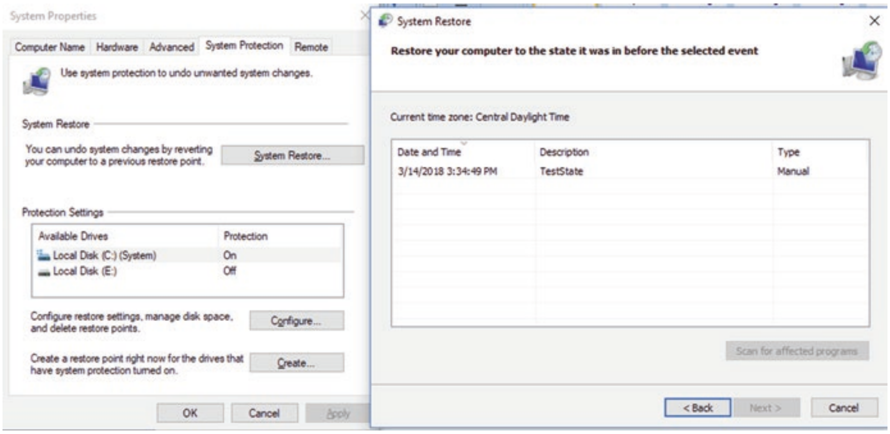
While backup process saves operational data to a backup data or copy, recovery reverses the process by bringing a backed-up data to live or operations in cases where live or operations systems failed and went through data failure or corruption. The quality of the recovery process is measured through how fast, quick, and transparent this standby version can replace the operational system. For interactive and real-time systems with many users and sensitive data, this recovery process should be very quick without being noticed by users.

As a reverse process to the backup process, restoration process can vary based on the backup process. For example, we described some differences between incremental and differential backup largely on how their recovery process is accomplished.

In addition to the previous backup types that direct the recovery process, recovery can be different in what it means for data, programs, users' actions, etc. For example, for data, recovery process involves rolling back to a correct earlier data state. Live or operational data can be missing, corrupted, or having some problems. Each one of those cases may dominate a different decision on how to go from the current missing or corrupted data to this earlier stable data state. For example, if data is missing, there is no choice but to retrieve earlier data state, and eventually lose every data update after the backup date. However, if data is corrupted, we may be able to merge earlier data with current data to minimize the amount of lost data. This is where sometimes restoring process can be distinguished from recovery, where recovery indicates only a surgical operation to restore only corrupted files or data.

Besides data recovery or restoration, when it comes to recovery of workflows (e.g., user actions, applications), the process can be more complex to accommodate not only micro actions or data transactions, but more complex system and data states that should be recovered as one unit (i.e., either all or none). This rolling back concept is very popular, for integrity purposes, in Database Management Systems (DBMSs) and servers where many transactions are observed as related to each other. They may include several sub-activities and all those activities should be completed together to move to another state. A simple example to this will be a person who is trying to withdraw money from an ATM. If the process fails in any intermediate stage, the whole completed steps so far will have to be rolled back. Another example is creating an OS (e.g., Windows) restoration point, (Fig. 3.2). One more difference between data recovery and process or work flow recovery is that some work flow activities are not recoverable. For example, if you created a new file with the same name of an old file and ignored the warning message, such process cannot be recovered and you will not be able to restore the overridden file.

Recovery can be divided into forward and backward recovery. Log files can be used in forward recovery. Transactions that were completed, while the data was lost or corrupted can be rolled forward based on information from the logs (e.g., DBMS, OS, web server logs). If transactions were not completed successfully, rolled back or backward recovery will be triggered to reverse all process partially completed



System Properties

Use system protection to undo unwanted system changes.

System Restore

You can undo system changes by reverting your computer to a previous restore point.

Protection Settings

Available Drives	Protection
Local Disk (C:) (System)	On
Local Disk (E:)	Off

Configure restore settings, manage disk space, and delete restore points.

Create a restore point right now for the drives that have system protection turned on.

System Restore

Restore your computer to the state it was in before the selected event

Current time zone: Central Daylight Time

Date and Time	Description	Type
3/14/2018 3:34:49 PM	TestState	Manual

Fig. 3.2 An example of creating Windows restore

activities. Those two recovery mechanisms are not mutually exclusive. In one system failure, both forward and backward recoveries can be used; try first forward recovery and for those transactions that forward recovery is impossible, use backward recovery. Operating systems employ also “crash recovery” to recover automatically from failures that cause system crashes. Similar to backward recovery, crash recovery rolls back in completed and failed transactions or transactions that caused operating system failure.

K0026: Knowledge of Disaster Recovery Continuity of Operations Plans

A major incident or a disaster can bring a business to a complete bankruptcy if no plans exist to deal with such abnormal situations. Several companies did not survive and went out of business upon experiencing such situations.

Organizations should have disaster recovery plans (DRPs); documented processes or sets of procedures to recover from problems or disasters and protect business assets and infrastructure in the event of a disaster. Disasters are problems at large scales that can occur due to natural causes (e.g., flooding, earthquakes, fire) or human-made problems (e.g., security breaches, large-scale systems’ failures, power or network outage, terrorisms). Most security controls target the goal of preventing disasters and problems from occurring. Nonetheless, plans should also put in place for recovering from disasters once they occurred.

To properly plan for DRP and determine what should be protected, business RTO (recovery time objective; maximum acceptable amount of resource downtime) and RPO (recovery point objective; maximum acceptable amount of data loss) should be determined. They measure how much data and time a system can afford to miss or lose.

RPO measures how much data a system can lose since the last backup. RTO measures how quickly a system needs data or resources to be restored. Accidents can happen, and no support system can guarantee 100% uptime; hence, RPO and RTO metrics set the limit of how much the system critical resources can afford failures.

DRP plan should include details on responsible personnel and how to reach them in urgent cases. It should explicitly describe the roles and duties of the different personnel involved, points of contacts, etc. The plan should be realistic and periodic exercises are necessary to ensure the validity of the plan and also build employees' awareness and training on such plans. Frequent plan exercises can also ensure that planning procedures are current and represent or reflect the most up-to-date system state and resources. Employees and different teams' responses should be studied and feedback should help assess and improve the process. The plan should be visited at least once a year to make sure that it is up-to-date and is aligned with the current business mission, priorities, resources, capabilities, and risks.

In addition to training and exercises, testing a DRP plan can take different forms such as:

- Checklist review: Verify the content of the DRP plan against known standards.
- Tabletop exercise: Scenario-based verification. Team can pick different scenarios of disasters and walk through and evaluate DRP against those scenarios.
- Dry run tests: Test system functions (e.g., fail or interrupt such function), one at a time.

In order to protect critical resources, DRP should consider backups for data and critical system assets off-sites (i.e., in different physical locations from live or operational systems). Different options exist that balance between cost and downtime or availability:

- Complete or hot site: This is an off-site or backup site that can run, instead of the operational site within a very short amount of time. This option is the best in terms of availability but very expensive to acquire and also expensive to maintain.
- Cold site: This represents the opposite option of hot site. Price can be affordable but will take time and extra resources to be able to operate as a main site.
- Warm site: A warm site is an intermediate option between hot and cold site to balance between cost and downtime.
- Mobile site (e.g., on a car or truck).
- Shared site (with some other businesses that have similar goals or business functions).

Business Continuity Plan (BCP) focuses on ensuring that most business functions operate with no interruption. BCP shares many similarities with DRP. Similar to business continuity plan (BCP), DRP targets assets availability and reducing main business functions' downtime and data loss. In the security scope, for both DRP and BCP, human safety and data privacy are also very important goals.

BCP focuses on sustaining business mission and critical functions. DRP focuses on finding alternative locations, operations, or services, once those are interrupted in the main business site or workflow. BCP is more comprehensive than DRP and hence includes DRP, COOP, and business resumption plan.

Both BCP and DRP plans should include alternative details for main infrastructure disruptions. For example, if a disaster occurs that prevents employees from working physically from company locations, how they will communicate if they need to work from home. The plans should also identify critical system assets and functions. They should show how such assets and functions will be protected and how they will be accessed or restored in disaster situations.

A Continuity of Operations Plan; COOP (also called Continuity of Government Plan), as defined by: National Continuity Policy Implementation Plan (NCPIP) and the National Security Presidential Directive51/Homeland Security Presidential Directive20 (NSPD-51/HSPD-20), is "an effort within individual executive departments and agencies to ensure that Primary Mission Essential Functions (PMEFs) continue to be performed during a wide range of emergencies, including localized acts of nature, accidents and technological or attack-related emergencies," Fig. 3.3, (fema.gov).

In the core of COOP: Primary and Mission Essential Functions (PMEFs and MEFs) and National Essential Functions represent the main US government essential functions (fema.gov). Private sector business can define their critical business functions or activities and develop a COOP plan to ensure that functions will not be interrupted by disasters, security problems, etc. COOP plan should also include orders of sessions and delegation of authorities to ensure who will do what in disaster situations. NSPD-51/HSPD-20 standard identifies the following COOP requirements: Essential Functions, Orders of Succession, Delegations of Authority,

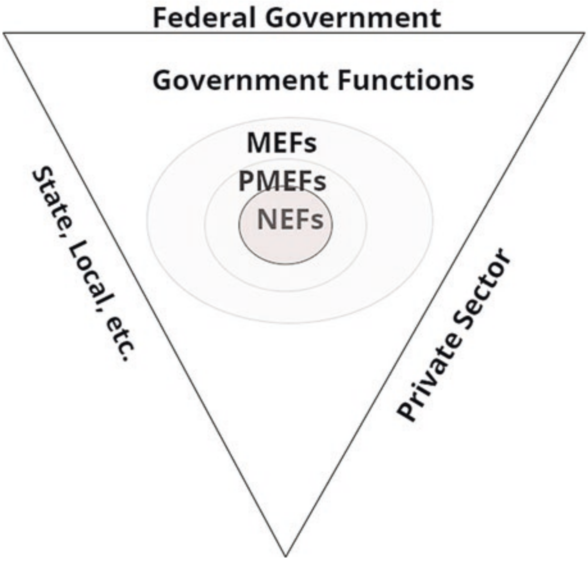


Fig. 3.3 COOP (fema.gov)

Continuity Facilities, Continuity Communications, Vital Records Management, Human Capital, Tests, Training, and Exercises (TT&E), Devolution of Control and Direction, and Reconstitution. COOP plan can be activated whenever it is impossible for employees to reach their working places (e.g., based on a wide range of natural and human-made disasters).

Business Process and Impact Analysis (BPA/BIA)

For DRP, BCP, and COOP, it is important to conduct Business Process Analysis (BPA) and also Business Impact Analysis (BIA). NIST SP 800-34, Rev. 1, defined BIA as "the analysis of an information system's requirements, functions, and interdependencies." BIA identifies the system critical functions and resources and what impact such functions or resources, if they failed, will have on the business.

A BIA is important to correlate information systems with critical business processes. BPA examines and maps the business functional processes, workflows, activities, personnel expertise, systems, data, and facilities to a business function or requirement. BPA analyzes the costs and constraints of individual process activities to identify areas for improvement and increased efficiency.

FCD and CGC

Federal Continuity Directive (FCD) provides direction to Federal government for developing continuity plans and programs. Continuity Guidance Circular (CGC) provides continuity guidance or plan for non-Federal entities and private sector organizations.

S0032: Skill in Developing, Testing, and Implementing Network Infrastructure Contingency and Recovery Plans

S0150: Skill in Implementing and Testing Network Infrastructure Contingency and Recovery Plans

- Use NIST Special Publication 800-34 Rev. 1 template (Appendix B—Sample Business Impact Analysis (BIA) and BIA Template) to develop a BIA document for your business of choice.

- Read NIST Special Publication 800-34 Rev. 1. Then based on the document, use the template (Appendix A—Sample Information System Contingency Plan Templates: select one of the three available templates; low, moderate, and high impact systems) to develop a plan for your business or an organization of your choice.
- You can find through the Internet many references for "disaster recovery (DR) self-assessment tool." Such tools can take several forms such as surveys (to distribute for target employees) or just self-assessment checklist. Some of those are generic to be used in any sectors, while some others are more focused to certain industrial sector. Search and find one of those DR self-assessment, use it in your selected business and summarize output results.
- You can find through the Internet many references for "business continuity (BC) self-assessment tool." Such tools can take several forms such as surveys (to distribute for target employees) or just self-assessment checklist. Some of those are generic to be used in any sectors, while some others are more focused to certain industrial sector. Search and find one of those BC self-assessment, use it in your selected business and summarize output results.

Bibliography

Richardson J (2012) Avoiding "Whack-a-mole" in the data center. http://www.datacenterjournal.com/avoiding-whack-a-mole-in-the-data-center/

Chapter 4
Cyber Defense Analysis and Support

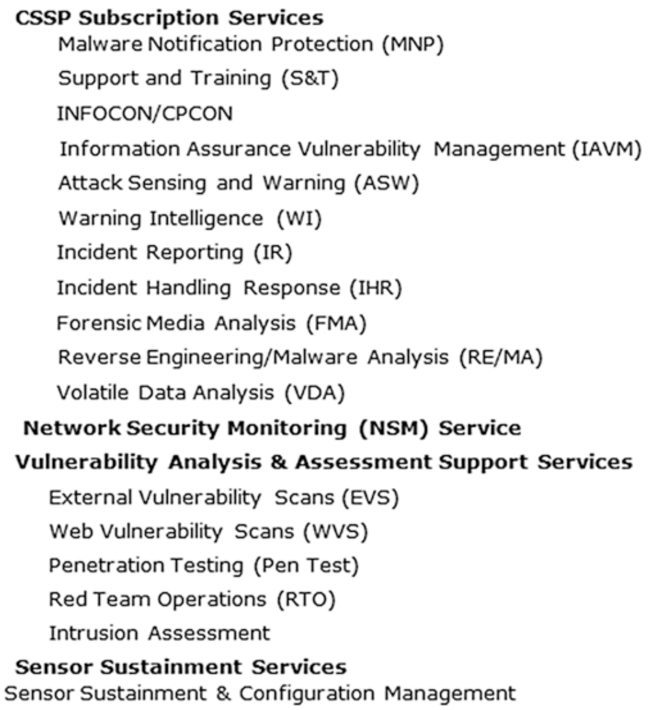
K0098: Knowledge of the Cyber Defense Service Provider Reporting Structure and Processes Within One's Own Organization

Cyber Defense Service Provider; CDSP (also called Computer Network Defense Service Provider; CNDSP in several references, Cyber Security Service Provider (CSSP), even cloud defense service provider) represents an organization responsible for delivering different functions: protection, detection, evaluation, response, and sustainment services to service subscribers. CNDSP team consists of a Computer Emergency Response Team; CERT or Incident Response and Recovery Team (IRRT). The team is also related to Network Operations and Security Center. The team should ensure that service subscribers have extensive anti-malware programs, vulnerability management plan, etc. Figure 4.1 shows overall CSSP tasks according to DISA (https://www.disa.mil).

In NICE framework, this falls also within cyber defense infrastructure support specialty area. In DoD, this falls within (CNDSP) specialty area.

In US DoD, several entities act as Tier II CNDSP such as: Defense Information System Agency (DISA), Navy Cyber Defense Operations Command (NCDOC), Marine Corps Network Operations and Security Center (MCNOSC), and Defense Information Systems Agency (DISA) Global Support Center, recommend DoD-wide Computer Network Defense; CND operational direction and support all DoD Components. Namely, DoD requires those to provide three services: (1) protect; (2) monitor, analyze, and detect; and (3) respond (DoD O-8530.2: Support to Computer Network Defense (CND), reference c). Figure 4.2 shows reporting procedure by CNDSP Tier II once a security incident is detected (CJCSM6510.01B-2013). In this architecture, USCYBERCOM: www.navy.mil/local/USCYBERCOM/, and USSTRATCOM: http://www.stratcom.mil/, are considered Tier I (Directive Authority for Cyberspace Operations).

I. Alsmadi, *The NICE Cyber Security Framework*,
https://doi.org/10.1007/978-3-030-02360-7_4



CSSP Subscription Services

- Malware Notification Protection (MNP)
- Support and Training (S&T)
- INFOCON/CPCON
- Information Assurance Vulnerability Management (IAVM)
- Attack Sensing and Warning (ASW)
- Warning Intelligence (WI)
- Incident Reporting (IR)
- Incident Handling Response (IHR)
- Forensic Media Analysis (FMA)
- Reverse Engineering/Malware Analysis (RE/MA)
- Volatile Data Analysis (VDA)

Network Security Monitoring (NSM) Service

Vulnerability Analysis & Assessment Support Services

- External Vulnerability Scans (EVS)
- Web Vulnerability Scans (WVS)
- Penetration Testing (Pen Test)
- Red Team Operations (RTO)
- Intrusion Assessment

Sensor Sustainment Services

Sensor Sustainment & Configuration Management

Fig. 4.1 CSSP services (https://www.disa.mil)

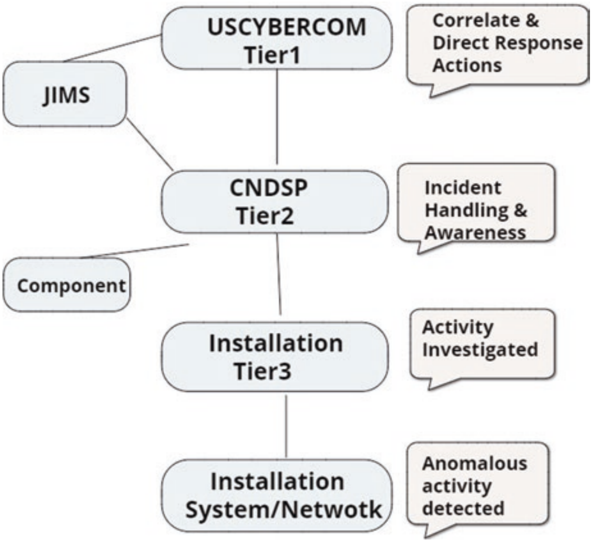

USCYBERCOM Tier1
Correlate & Direct Response Actions
JIMS
CNDSP Tier2
Incident Handling & Awareness
Component
Installation Tier3
Activity Investigated
Installation System/Netwotk
Anomalous activity detected

Fig. 4.2 CNDSP Tier II security incident reporting procedure

Enterprise should provide standardized information to the CNDSP team who will exercise response plans to validate the processes, subscriber documents, contact information, and communication mechanisms. CNDSP is not required for organizations that will only be passing information over the commercial Internet Service Provider (ISP). Non-DOD ISPs connected to the DISN must be covered by accredited CNDS providers IAW DODD O-8530.1 (CJCSI 6211.02D).

DoD identifies different work roles that fall under this specialty area: C11.2.1.1; CNDSP Analyst (CND-A), C11.2.1.2; CNDSP Infrastructure Support (CND-IS), C11.2.1.3; CNDSP Incident Responder (CND-IR), C11.2.1.4; CNDSP Auditor (CND-AU), and C11.2.1.5; CNDSP Manager (CND-SPM). (See DoD 8570.01-M for detail functions for each one of those different work roles).

DOD CNDSP Directives

In CDN-SP DoD issued the following directives: DoDD O-8530.1, Computer Network Defense (CND), and DoDI O-8530.2, Support to Computer Network Defense (CND), DoD O-8530.1-M, Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation Process. These issuances identify security policies, assign responsibilities, and provide procedures essential to support CND initiatives. Those policies are frequently revised and updated. DoD 8530.1-M—Defines a standard process for certifying and accrediting CND Service Providers within DoD.

CJCSI 6510.01D and CJCSI 6510.01E contain detailed procedures for IA and CND that complement the guidance issued in DoD 8500 series directives and instructions in 2004 and 2007 consecutively.

K0107: Knowledge of and Experience in Insider Threat Investigations, Reporting, Investigative Tools and Laws/Regulations

An insider threat is generally defined as "a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems," NCCIC 2014.

The 2015 Vormetric Insider Threat Report (Vormetric 2015) indicates that over 22% of US organizations experienced a data breach in the last 12 months. Additionally, 93% of organizations indicate that they feel vulnerable to insider attacks.

Based on several statistics in the most recent years, insider threats make a significant portion of overall threats. Three main reasons contribute to why insider threats keep showing as serious and significant threats:

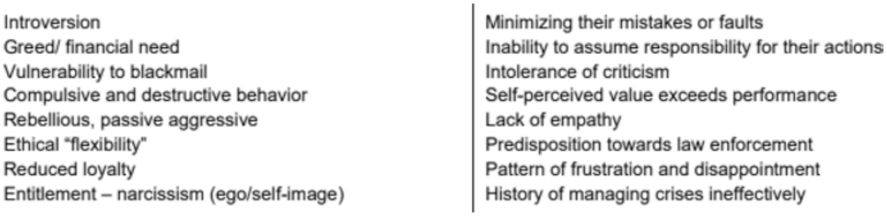
- Insiders, regardless of their position or permissions, have access to sensitive resources and have enough knowledge to make intrusion possible.
- It is usually harder and complex to investigate and track an intrusion from an insider in comparison with outsiders' intrusions. For one reason, most security controls face external interfaces. Additionally, if those insiders have administrative privileges, and those insiders intentionally commit attacks, they have the abilities to hide, tamper, manipulate, and complicate the investigation process. This makes them harder to analyze, defend against, or anticipate.
- On the other side of insiders with intentional attack, insiders can be part of an attack without their consent knowledge. They can be tricked using several mechanisms (e.g., social engineering) to be attackers as well as victims of the same attack. This is why organizations start to allocate resources for security awareness training.

It is important to understand the psychology and causes of insider threats. Why will an employee be a possible target or entrance for attacks? Analysis and statistics showed different reasons that range from careless to malicious (Fig. 4.3, NCCIC 2014). On the other hand, US-CERT conducted an analysis of over 800 malicious insider attacks and found that there was no standard profile of a malicious insider.

Phishing Attacks

Many reports on insider threats showed that data leaks or breaches are on top of the serious and frequent insider threat attacks. This can typically happen when users or employees click on malicious or unsafe links.

For hackers or attackers, phishing attacks are easy to develop; all what it takes is to fake a legitimate website or user account (e.g., a bank, an e-commerce website, an online social network website, a boss email) and then send it through a message or email, typically with a sense of importance or urgency to a mass of victim users. Sometimes those can be just pop-ups or links in websites users are visiting. More recently, online social networks (OSNs) such as Facebook and Twitter as well as smart phones start seeing those types of phishing attacks or links.



Introversion
Greed/ financial need
Vulnerability to blackmail
Compulsive and destructive behavior
Rebellious, passive aggressive
Ethical "flexibility"
Reduced loyalty
Entitlement – narcissism (ego/self-image)

Minimizing their mistakes or faults
Inability to assume responsibility for their actions
Intolerance of criticism
Self-perceived value exceeds performance
Lack of empathy
Predisposition towards law enforcement
Pattern of frustration and disappointment
History of managing crises ineffectively

Fig. 4.3 Examples of reasons why an insider can be an attack target (NCCIC 2014)

Password Attacks

While most security policies and regulations pay attention to the strength and protection of users' passwords, yet many users still, for different purposes, use weak or common passwords or accidentally forward sensitive data to unintended users.

Password roles and guidelines went through different cycles of mechanisms to make passwords stronger and harder to guess by password attackers. For example, different opinions exist on the value for periodically (e.g., 1 month or 3 months) changing passwords. While this was part of NIST standards, many did not see a value of the need to change frequently the password (i.e., either it is strong or it is not, additionally this indicates the existence of methods to store passwords or their hashes). Most recent NIST Special Publication 800-63B (March 2018) revised their stance on password regulations or recommendations. In this newest release, NIST removed the need for periodic change of passwords. The new release also removed the need for password complexity requirements (mixing between the four: capital and small letters, numbers and special characters). A new requirement is added to screen the newly created password against a list of known bad passwords or bad categories of passwords (e.g., passwords obtained from previous breach corpuses, dictionary words, repetitive or sequential characters, context-specific words, such as the name of the service, the username). This is a requirement before accepting the new password. Size also matters, where longer passwords or passphrases are recommended.

Privilege Tampering/Escalation and Abuse

Access controls in operation systems, DBMSs, web servers, routers, etc. include users and their permissions or rights to access different system resources. With middle to large enterprises, this data in access controls can be very large. Administrators may not have the right time and tools to frequently visit access controls to make sure that all users are valid and also those users have the right level of permissions. An attack that starts from a privilege creation or escalation can hence go undetected for a significant time if no proper automatic auditing mechanisms exist to screen for such issues. Privilege tampering can take one of three forms:

- Creating a new account for a user. This means that an attacker may not need an insider account in this case and they will just try to create and use this new account.
- Using an existing account. An employee with proper account and permissions can be a victim of an identity theft where an attacker will try to use their account and permissions. Those are compromised accounts (i.e., internal accounts that have been compromised by external attacks). In this case, the account and permissions are valid but used by a malicious user. It can be very hard in such case

to distinguish the attacker from the victim employee (if they are using their accounts and credentials).

- Privilege escalation: In those cases, valid users (e.g., insiders) are trying to maliciously escalate their privileges to access resources that they are not supposed to and knowingly misuse data and exploit the system.

Challenges in Insider Threats Investigations

- High volume of network activity: Given the continuously increasing volume of traffic in networks, detecting malicious acts in real or short time is a challenge. IT's main goal is to ensure that all business services are running without problems. Digging deeper into traffic with many roles for possible security alerts may cause a significant network overhead. Bottom line, always there is a need to balance between performance, security and efficiency as in terms of resources, those goals may often contradict with each other.
- Lack of IT staff training. IT staff are not trained to be detectives or forensic investigators. Roles of security personnel in organizations are evolving and on the rise. IT staff may lack the skills to handle, from a technical or communication perspective, several types of attacks.
- Growing use of cloud services: For security in general, cloud services create different forms of security risks and concerns. For data, services and possible infrastructure that are provided by a cloud service provider, how could an organization properly conduct insider attacks' investigations?
- Pressure to change IT configurations quickly more so than securely. IT staff are busy with running normal operations and deal with frequent software, system, network, and hardware updates. Such frequent changes create security challenges on making sure that new challenges will not create new vulnerabilities and that our security policies are up-to-date and capable of protecting our most recent software, system, network, and hardware environments.
- Use of Mobile devices and Bring-Your-Own-Device (BYOD) model: Mobile devices and BYOD are inevitable in any organization regardless of how much classified data and systems are in that organization. Whether employees have their own smart devices or use organization devices risks exist in many perspectives. For insider threats in particular, with powerful smart devices, users can access and expose system resources through those devices. As those devices are typically used for dual company and personal usage, isolating the two domains from each other is impossible. Smart devices cannot be connected in the organization domain in the same level of control as desktops and laptops. This keeps a very vague or illusive relation between organization network and those devices which complicates activities such as controlling, monitoring, or investigating such devices, if necessary.

Methods to Counter and Mitigate Insider Threats

We have mentioned earlier that profiles of insiders' attacks can vary. So, with no specific profiles, how do you prevent malicious insider attacks from happening? Followings are methods proposed to mitigate or counter insider threats:

- Security awareness training: With the importance of security controls and mechanisms, the human factor should always be a focus in our security investments. While we build and optimize our firewalls with the best possible protection policies and roles, we should not ignore the "human firewall" where humans are those who create those policies and roles. Users will also use and enforce those policies. As such, policies should be simplified to normal users and help them understand the necessity and importance of enforcing such roles. It is easy to blame employees on being careless or ignorance when tricked into some social engineering or phishing attacks. As the impact of such incident goes beyond the employee, organizations should invest on any methods that can help mitigate such attacks. We can implement safeguards, such as firewalls, strong spam filtering systems, but in the end, it comes down to users, training, and awareness programs.

  Awareness, training, and education are different but related elements in this scope (Table 4.1). Organizations and managers should support such effort and allocate proper resources. Many US government organizations currently employ different security awareness methods for their employees (e.g., periodic exercises, training, gamification).
- Identity and access management: Proper policies should exist on how to create, monitor, and maintain user and access control accounts. Policies can be used also to alert for certain behaviors (i.e., red flags) that can be possibly part of a phishing attack (e.g., new user account, privilege escalation).
- Intrusion detection and prevention systems: an IDS/IPS represents an intelligence security control that can provide real-time monitoring and guard actions. In comparison with firewalls, IDS/IPS is more intelligent and comprehensive.

Table 4.1 Different elements between awareness, training, and education (Whitman and Mattord 2008)

	Awareness	Training	Education
Attribute:	"What"	"How"	"Why"
Level:	Information	Knowledge	Insight
Objective:	Recognition	Skill	Understanding
Teaching method:	Media	Practical Instruction	Theoretical Instruction
	• Videos	• Lecture	• Discussion seminar
	• Newsletters	• Case study workshop	
	• Posters, etc		• Background reading
		• Hands-on practice	
Test measure:	True/False Multiple Choice (identify learning)	Problem solving (apply learning)	Essay (interpret learning)
Impact timeframe:	Short-term	Intermediate	Long-term

- SIEM or log management: Take advantage of data analytics to continuously screen through logs and alert for possible red flags. The quality of such tools depends on the accuracy and efficiency of built-in algorithms as typically such algorithms have to search through a large volume of data in a very short amount of time. Key successful factors include to lower false-positive and false-negative rates as well as causing minimum overhead in overall system performance.
- Web application firewalls. Those are also called Layer 7 or application layer firewalls. In comparison with classical L2–L3 firewalls, web application firewalls can look at different attributes that identify malicious applications, users, or traffic.

Insiders' Investigations: Laws and Regulations

If a company wants to implement technological solutions designed to help detect and investigate insider threats, explicit roles and regulations should exist within the company to regulate the monitoring, detection, investigation, and prosecution processes. These resources will depend on the organizational structure, who to report to, to be part of the investigation, etc.

Conducting private investigations in organizations are possible. However, organizations should make sure to transfer the investigation to a public investigation if they realize that, based on the nature of the crime, they should step out of the case. For companies' sanctions and violations, policies and regulations should be in place first that guide employees to the proper usage of computing resources, the Internet, information privacy, etc. Employees should be trained and educated on how to avoid any liabilities based on improper actions. Auditing and loggings mechanisms can be used to search for evidences. Investigation teams should have the technical skills and the knowledge related to laws and regulations that make them capable of searching for, collecting properly handling and using digital evidences. Due to the evolutionary nature of computing environments, digital related laws evolved and continue to evolve rapidly. How much valid and credible a digital evidence can be? Can we trust a web log that traces a phishing attack to a certain user? Those are examples of open legal issues and concerns when it comes to digital investigations in general.

K0157: Knowledge of Cyber Defense Policies, Procedures, and Regulations

Cyber defense implies taking proactive measures to stop and protect again future or possible attacks. Cyber defense policies include roles and regulations, at either the company or the national levels that are taken to protect organization or nation critical infrastructures, assets, and resources. Those proactive measures may also involve monitoring and intelligence techniques for detecting and obtaining information about possible future intrusions or attacks.

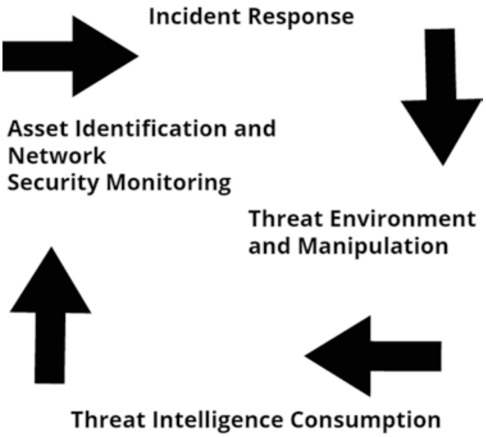
An organization's cyber defense is based on the process of managing and evaluating cyber risks. This should be a periodical process that should be performed whenever the organization's cyber environment is changing; either within the organization (e.g., new systems, technological changes, changes in business functions) or outside the organization (e.g., constant change of cyberspace threats to the organization).

Cyber defense can be divided into passive and active. Passive cyber defense includes security controls such as firewalls and anti-malware systems with consistent protection against possible threats without direct or constant human interaction. Active or proactive cyber defense involved more human or real-time interactive interactions as well as countermeasure activities. The organization will monitor its networks and collect data about cyber threats and coping measures. Those are then translated into ad hoc applicable controls. The organization may also implement a deception array of potential attackers in order to confuse attackers or trap them. Several models are proposed to describe the different tasks in active cyber defense and interactions between those tasks. For example, Radvanovsky and Brodsky 2016 proposed an Active Cyber Defense Cycle based on four tasks (Fig. 4.4): (1) Threat intelligence consumption, (2) asset identification and network security monitoring, (3) incident response, and (4) threat and environment manipulation

In another classification, cyber defense can be classified into:

- Unprotected or open systems
- Static or passive perimeter-based security
- Enhance or active perimeter-based security
- Dynamic moving target defense (DMTD): Defenders continuously try to protect or defend the system through shifting or reducing attack environment, surface, etc. This will hopefully increase the security complexity profile and minimizes the opportunities for successful attacks.

Fig. 4.4 Active cyber defense cycle


Incident Response
Asset Identification and Network Security Monitoring
Threat Environment and Manipulation
Threat Intelligence Consumption

In terms of cyber defense regulations, there has been much public discussions about the security countermeasures that companies can lawfully take to protect their computer assets, networks, and data. For example, recent regulations are discussing the legality and limitations of cyber intelligence gathering. Cyber intelligence gathering may include data collection about hackers, intruders, adversaries, etc. that can help understand their motives, intrusion methods, etc. to ultimately help prevent or deter future attacks. On the other hand, defensive cyber actions can raise a variety of issues (e.g., privacy concerns, and data collection or surveillance), private sector practitioners may consult their lawyers before conducting some types of defensive cyber actions.

Another related term that is evolving is: cyber actions, defensive cyber actions, or active defense that we will describe in the following sections.

K0190: Knowledge of Encryption Methodologies

See (K0019): Knowledge of cryptography and cryptographic key management concepts

K0408: Knowledge of Cyber Actions (i.e., Cyber Defense, Information Gathering, Environment Preparation, Cyber-Attack) Principles, Capabilities, Limitations, and Effects

The term: "Defensive cyber actions or active defense" captures a wide range of activities that can be conducted for the purpose of systems and network defense in response to cyber threats. Those should be differentiated from counter or offensive measures that may occur in response to an actual attack.

Defensive cyber actions include different categories of important tasks:

- Cyber intelligence gathering: This is the process of gathering information about the possible adversaries and their target profiles, tools, infrastructure, tactics, and procedures. This information can then be used to protect against their future activity. This process may also help organizations know some details about their weaknesses, vulnerabilities, or what weaknesses or vulnerabilities that are targeted by the investigated adversaries.

  Software agents such as web bugs or beacons exist since several years and used by some companies for different reasons. Spying on customers using software agents in different forms is not something new, despite the public denials of companies who usually do that. Spying for cyber defense will have different goals, different and more focused categories of "customers." Forensic analysts may also conduct their online investigation after attacks or malware breakouts. In such cases, the goal is to detect and investigate the attack and how it happened, and/or malware eradication rather than trying to spy on attackers or retrieve stolen data.

- Sink holing: This is the process of buying or registering domain names used previously for malware command-and-control servers.
- National and international data sharing: Companies at the national level and government sectors at the international level have common interests to monitor and prevent large-scale attacks that go beyond a company or even a country. Government should implement laws that prosecute and prevent cyber offensives even if they target businesses in other countries.
- Hacking back: Offensive actions such as hack back can be an option in some cyber action situations. Cyber agents in government may conduct such actions, but typically such offensive actions will never be publicly disclosed or admitted.

S0063: Skill in Collecting Data from a Variety of Cyber Defense Resources

For one selected threat of your choice, conduct an adversarial assessment based on the document (Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs 2014, Attachment C: Core Cyber Defense Performance Data and Metrics, Fig. 4.5). The document should contain the following cyber defense resources: Protect, Detect, React, Defense activities, Restore/COOP, and Mission Effects.

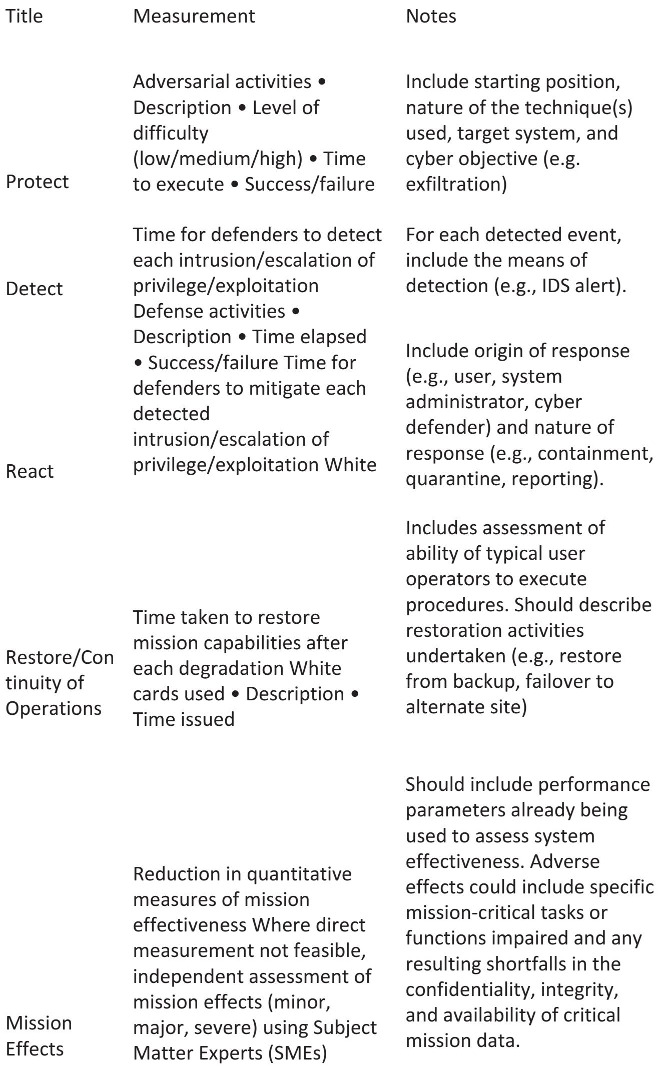
S0096: Skill in Reading and Interpreting Signatures (e.g., Snort)

As an open source IDS/IPS, Snort produce signatures that are classified into different classes based on the detected activity types. Examples of the most commonly reported class types include:

- Trojan-activity
- Policy-violation
- Misc.-activity
- Attempted-admin
- Web-application-attack

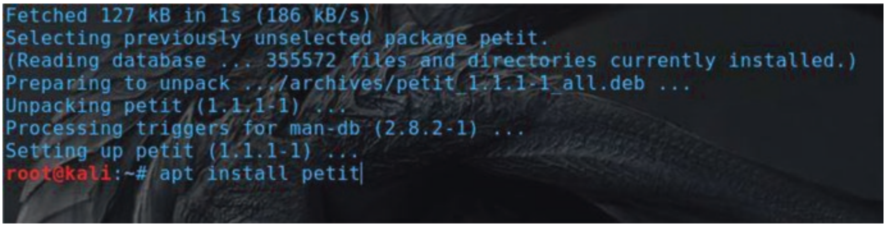
Some of the important attributes in each SNORT log record that can be used in the classification process include: The Generator ID (GID), the Signature ID (SID), and revision number.

Task1: Search through the Internet for “SNORT Log analysis tools” and find a proper tool to analysis the two SNORT log files attached. Show several screenshots from your analysis and any interesting information or knowledge you can get about the SNORT log file you have selected. Below are screenshots of an open source tool (Petit) that can be used to analyze SNORT logs (Figs. 4.6, 4.7, and 4.8):



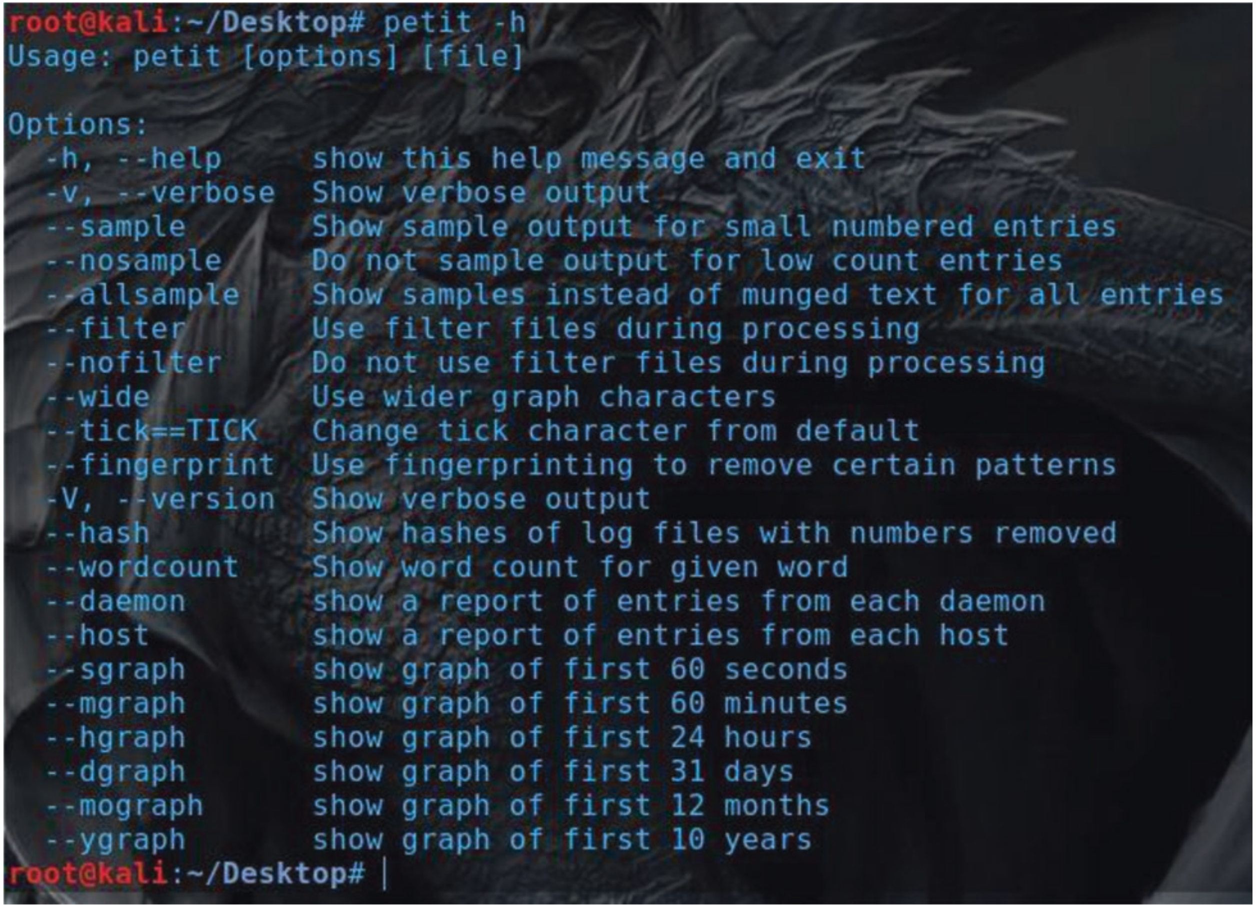
Title	Measurement	Notes
Protect	Adversarial activities • Description • Level of difficulty (low/medium/high) • Time to execute • Success/failure	Include starting position, nature of the technique(s) used, target system, and cyber objective (e.g. exfiltration)
Detect	Time for defenders to detect each intrusion/escalation of privilege/exploitation	For each detected event, include the means of detection (e.g., IDS alert).
React	Defense activities • Description • Time elapsed • Success/failure Time for defenders to mitigate each detected intrusion/escalation of privilege/exploitation White	Include origin of response (e.g., user, system administrator, cyber defender) and nature of response (e.g., containment, quarantine, reporting).
Restore/Continuity of Operations	Time taken to restore mission capabilities after each degradation White cards used • Description • Time issued	Includes assessment of ability of typical user operators to execute procedures. Should describe restoration activities undertaken (e.g., restore from backup, failover to alternate site)
Mission Effects	Reduction in quantitative measures of mission effectiveness Where direct measurement not feasible, independent assessment of mission effects (minor, major, severe) using Subject Matter Experts (SMEs)	Should include performance parameters already being used to assess system effectiveness. Adverse effects could include specific mission-critical tasks or functions impaired and any resulting shortfalls in the confidentiality, integrity, and availability of critical mission data.

Fig. 4.5 Core cyber defense performance data and metrics (dote.osd.mil 2014)



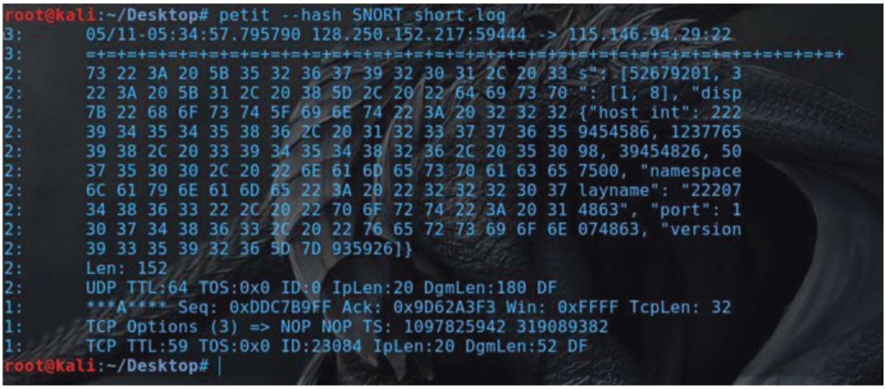
```
Fetched 127 kB in 1s (186 kB/s)
Selecting previously unselected package petit.
(Reading database ... 355572 files and directories currently installed.)
Preparing to unpack .../archives/petit_1.1.1-1_all.deb ...
Unpacking petit (1.1.1-1) ...
Processing triggers for man-db (2.8.2-1) ...
Setting up petit (1.1.1-1) ...
root@kali:~# apt install petit
```

Fig. 4.6 Snort log analysis (Petit installation)



```
root@kali:~/Desktop# petit -h
Usage: petit [options] [file]

Options:
  -h, --help        show this help message and exit
  -v, --verbose     Show verbose output
  --sample          Show sample output for small numbered entries
  --nosample        Do not sample output for low count entries
  --allsample       Show samples instead of munged text for all entries
  --filter          Use filter files during processing
  --nofilter        Do not use filter files during processing
  --wide            Use wider graph characters
  --tick==TICK      Change tick character from default
  --fingerprint     Use fingerprinting to remove certain patterns
  -V, --version     Show verbose output
  --hash            Show hashes of log files with numbers removed
  --wordcount       Show word count for given word
  --daemon          show a report of entries from each daemon
  --host            show a report of entries from each host
  --sgraph          show graph of first 60 seconds
  --mgraph          show graph of first 60 minutes
  --hgraph          show graph of first 24 hours
  --dgraph          show graph of first 31 days
  --mograph         show graph of first 12 months
  --ygraph          show graph of first 10 years
root@kali:~/Desktop# |
```

Fig. 4.7 Snort log analysis (Petit usage)



```
root@kali:~/Desktop# petit --hash SNORT short.log
3:      05/11-05:34:57.795790 128.250.152.217:59444 -> 115.146.94.29:22
3:      =+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
2:      73 22 3A 20 5B 35 32 36 37 39 32 30 31 2C 20 33 s": [52679201, 3
2:      22 3A 20 5B 31 2C 20 38 5D 2C 20 22 64 69 73 70 ": [1, 8], "disp
2:      7B 22 68 6F 73 74 5F 69 6E 74 22 3A 20 32 32 32 {"host_int": 222
2:      39 34 35 34 35 38 36 2C 20 31 32 33 37 37 36 35 9454586, 1237765
2:      39 38 2C 20 33 39 34 35 34 38 32 36 2C 20 35 30 98, 39454826, 50
2:      37 35 30 30 2C 20 22 6E 61 6D 65 73 70 61 63 65 7500, "namespace
2:      6C 61 79 6E 61 6D 65 22 3A 20 22 32 32 32 30 37 layname": "22207
2:      34 38 36 33 22 2C 20 22 70 6F 72 74 22 3A 20 31 4863", "port": 1
2:      30 37 34 38 36 33 2C 20 22 76 65 72 73 69 6F 6E 074863, "version
2:      39 33 35 39 32 36 5D 7D 935926]}
2:      Len: 152
2:      UDP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:180 DF
1:      ***A**** Seq: 0xDDC7B9FF Ack: 0x9D62A3F3 Win: 0xFFFF TcpLen: 32
1:      TCP Options (3) => NOP NOP TS: 1097825942 319089382
1:      TCP TTL:59 TOS:0x0 ID:23084 IpLen:20 DgmLen:52 DF
root@kali:~/Desktop# |
```

Fig. 4.8 Snort log analysis (Petit; data extraction)

Task2: The link (2017 in Snort Signatures, written by Martin Lee and Vanja Svajcer, http://blog.talosintelligence.com/2018/01/2017-in-snort-signatures.html) shows the top five Snort Signatures reported in 2017. Search for the top reported signatures in 2018, or any other year and compare them based on SNORT categories with those reported in 2017, Fig. 4.9 (Lee and Svajcer 2017).

Task3: Many tools and websites create "signatures" to identify attacks, malicious links, acts, sources, etc. For example, the Python script described in this link (https://github.com/jpsenior/threataggregator) can collect malicious sources (e.g., IP addresses) based on signatures from several tools/websites such as:

- http://geolite.maxmind.com/download/geoip/database/GeoLite2-City.mmdb.gz
- https://reputation.alienvault.com/reputation.data
- http://malc0de.com/bl/IP_Blacklist.txt
- http://rules.emergingthreats.net/blockrules/compromised-ips.txt
- http://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt
- https://palevotracker.abuse.ch/blocklists.php?download=ipblocklist
- http://www.binarydefense.com/banlist.txt
- https://sslbl.abuse.ch/blacklist/sslipblacklist.csv
- https://zeustracker.abuse.ch/blocklist.php?download=ipblocklist
- http://www.nothink.org/blacklist/blacklist_ssh_all.txt
- http://www.malwaredomainlist.com/hostslist/ip.txt
- http://www.ciarmy.com/list/ci-badguys.txt
- http://autoshun.org/files/shunlist.csv

Task4: FBI releases a document in 16 April 2014 about Open SSL Heartbeat issue (Fig. 4.10).

Investigate Snort signatures described in the document and prepare one page for each one describing its details.

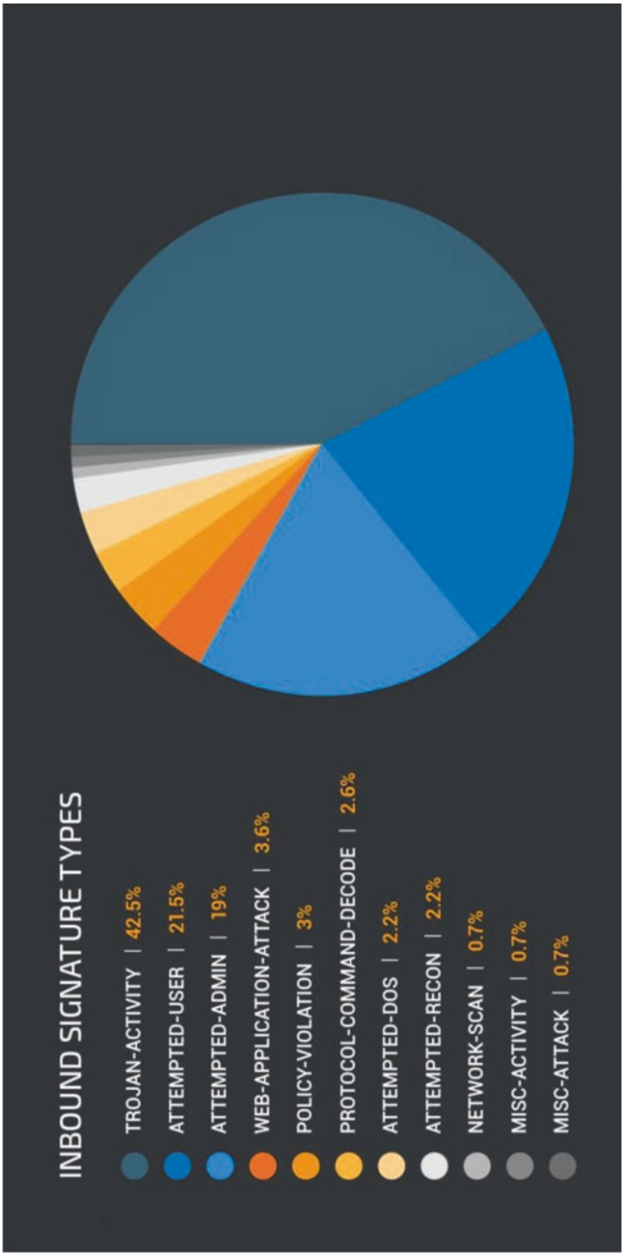
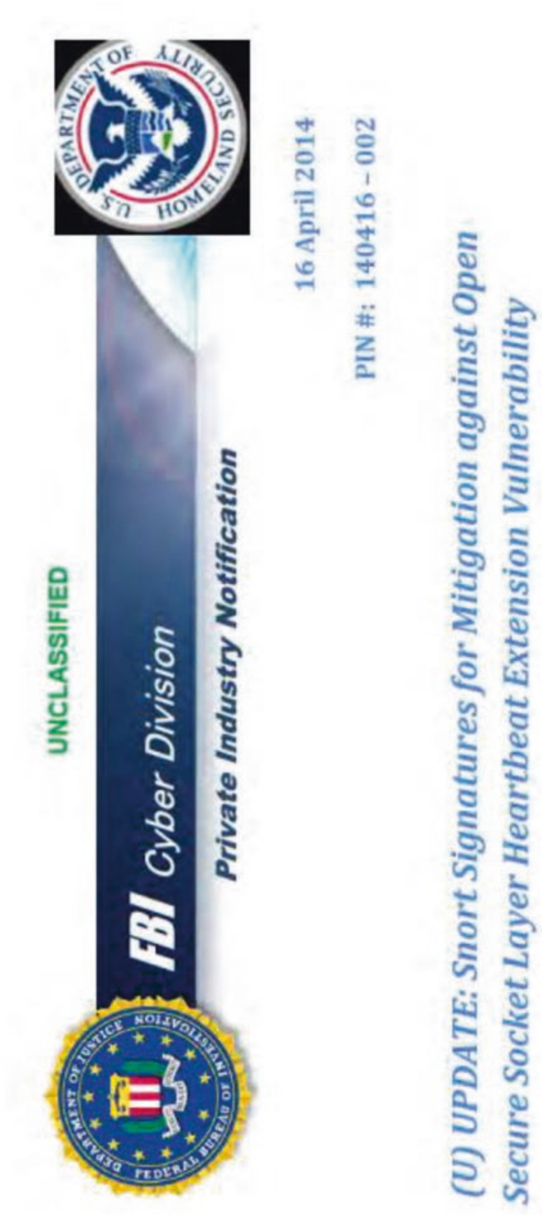


Fig. 4.9 Top SNORT signatures in 2017 (Lee and Svajcer 2017)



UNCLASSIFIED

FBI Cyber Division

Private Industry Notification

16 April 2014

PIN #: 140416 – 002

(U) UPDATE: Snort Signatures for Mitigation against Open Secure Socket Layer Heartbeat Extension Vulnerability

Fig. 4.10 An article on: snort signatures to mitigate OpenSSL heartbeat

Task5: https://packettotal.com can be used to automatically analyze traffic files for possible abnormal behaviors

Pick two of the files that are listed in this link:

https://www.asecuritysite.com/forensics/snort?fname=heart.pcap&rulesname=heart2.rules&fname=heart.pcap&rulesname=heart2.rules, upload those packet files to https://packettotal.com, then summarize the output reports from the website and what kind of malicious activities those are related to real case that you should investigate. For example, read on FBI website about Heartbeat case (heart.pcap) and OpenSSL.

S0124: Skill in Troubleshooting and Diagnosing Cyber Defense Infrastructure Anomalies and Work Through Resolution

Task1: Microsoft provides cloud-based cyber defense through (https://protection.office.com) for Office products. Some of the defense infrastructure controls provided include: Access control and advanced threat protection. MS Office can get security alerts through access to protection.office.com. Create a report on this website and tool and compare available functions with similar ones (e.g., Amazon GuardDuty, Amazon Macie, AWS Trusted Advisor, AWS CloudTrail, Amazon Inspector, AWS Config Rules, Wazuh (wodle), Netflix: SecurityMonkey) provided by other companies under the category of: cyber defense infrastructure. In particular, what kind of anomaly alerts that each system can provide.

Task2: In some cyber defense cases, active and offensive defense can be considered an option (with ethical and legal constraints). In the previous KSA, task3, we used an open source script (threat aggregator) to identify malicious sources or IP addresses using several websites or tools. Those offensive IP sources that are proven malicious according to several sources can be used for testing whether they themselves have vulnerabilities that can be targeted. Use output list from (threat aggregator) that is confirmed according to several sources as an input for vulnerability testing tools such as those that can be found in cyber security images such as Kali, BlackArch, and Parrot (e.g., Metasploit, OpenVAS). Some scripts (e.g., https://github.com/1N3/Sn1per) can also be used to automate the process and aggregate testing though several vulnerability assessment tools. There are also some open source scripts (e.g., https://github.com/hybridus/heartbleedscanner) that can target testing for some of the recent vulnerabilities that can also be used.

Tasks3: Conduct a research on firewalls anomaly detection and removal techniques. Try to find tools that can be used for testing firewalls (either automated or semi-automated). Pick a working or running firewall of your choice and evaluate its rules for possible anomalies (either statically or based on real-time traffic).

Tasks4: Conduct a research on IDS/IPS systems and anomaly detection and removal techniques. Try to find tools that can be used for testing IDS/IPS (either automated or semi-automated). Pick a working or running IDS/IPS of your choice and evaluate its rules for possible anomalies (either statically or based on real-time traffic).

S0170: Skill in Configuring and Utilizing Computer Protection Components (e.g., Hardware Firewalls, Servers, Routers, as Appropriate)

Computer protection components protect information systems against various threats and scan all system objects for possible malwares and vulnerabilities.

Task1: This is a sample task on how to use Snort, as an example of open source IDS/IPS. The goal is not only to familiarize yourself with this IDS/IPS in particular but general IDS/IPS architecture and components (e.g., rules configuration, testing and assessment, which can be extended to other types of IDS/IPS or firewalls).

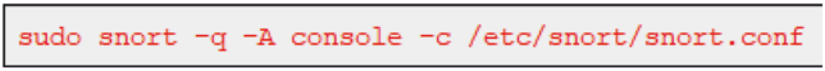
After proper installation of Snort, make sure to run the tool on an IDS/IPS mode (rather than the basic monitoring more), Fig. 4.11.

The file (local.rule) is created for users to add their own rules (as it is empty by default). You can add your experimental rules to this file. Image below, Fig. 4.12, shows an example of two rules added to local.rules.

Create examples of different rules and make sure to test them for conformance with proper action. For example, the second rule in the previous figure can be tested by sending inward or outward Ping messages.

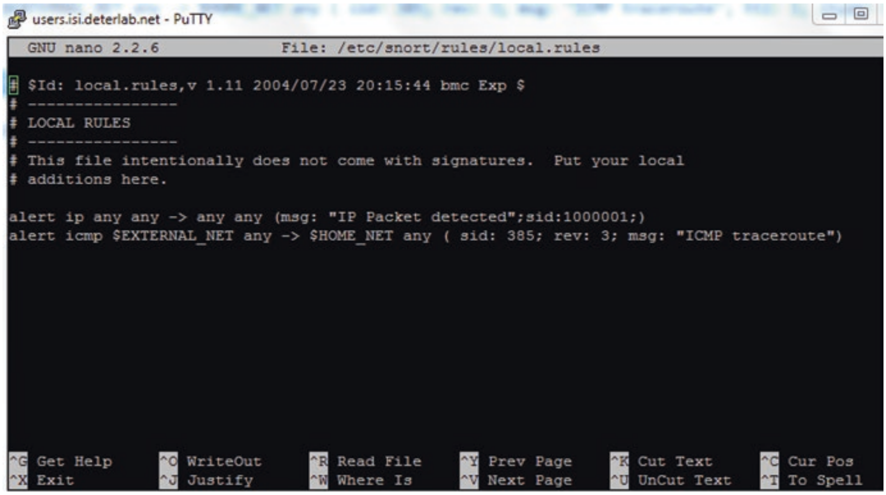
Task2: Servers include security layers or components that contribute to the overall information system security architecture. One important layer is related to access control (e.g., users, groups). Use one server of your choice (e.g., Windows 2012 server, Fig. 4.13). Show through walk-through steps how to create users/groups with different levels of access privileges or permissions.

Task3: GNS3 (https://www.gns3.com) is a popular network simulator. We will use it to simulate a network and evaluate creating access control lists (ACLs) on routers. Using GNS3 create the topology shown in Fig. 4.14.



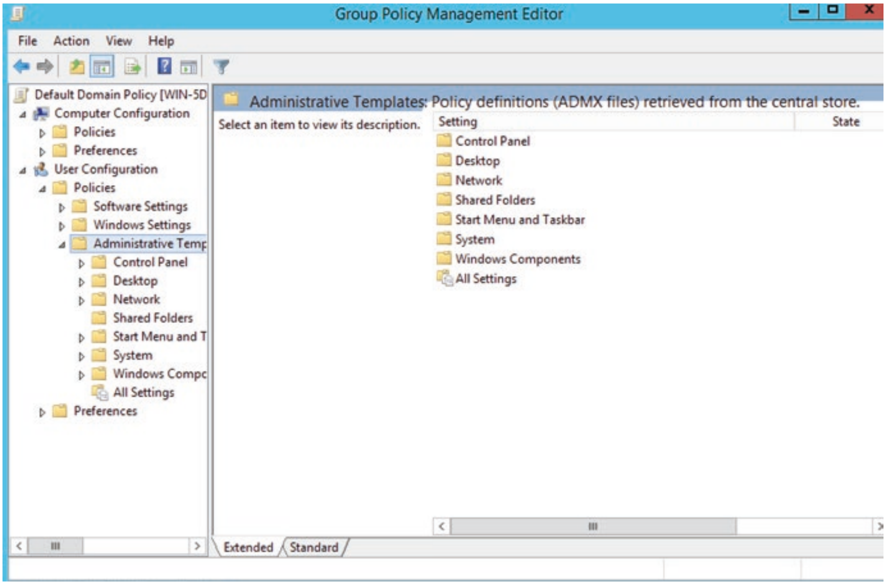
```
sudo snort -q -A console -c /etc/snort/snort.conf
```

Fig. 4.11 Running Snort as an IDS/IPS



```
  GNU nano 2.2.6              File: /etc/snort/rules/local.rules

# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.

alert ip any any -> any any (msg: "IP Packet detected";sid:1000001;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any ( sid: 385; rev: 3; msg: "ICMP traceroute")







^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text  ^T To Spell
```

Fig. 4.12 Examples of custom rules in Snort



Administrative Templates: Policy definitions (ADMX files) retrieved from the central store.

Select an item to view its description.

Fig. 4.13 Windows 2012 server group policy management

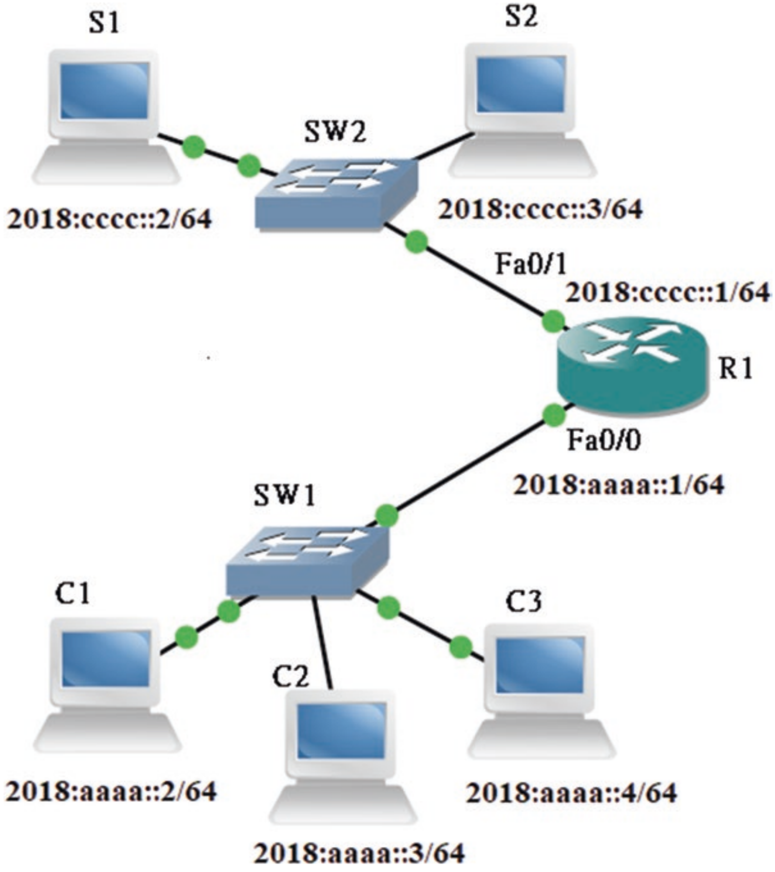
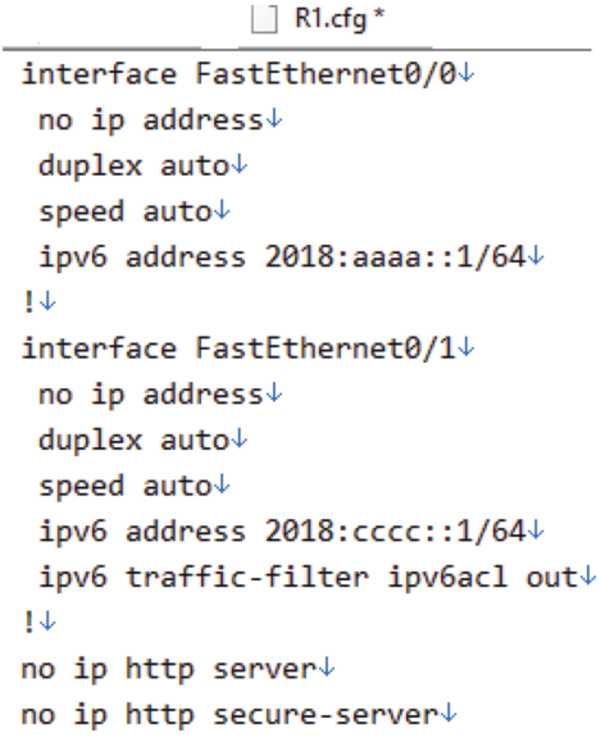


Fig. 4.14 A small network topology simulation using GNS3

You can configure the topology and ACL manually or through uploading a configuration file (Fig. 4.15).

Try different examples of ACLs such as:

- Only permit host C3 (IPv6 address: 2018:aaaa::4/64) access Server S1 user port 80, deny other host access server S1 use port 80, and permit any IPv6 traffic. Use the command (v6acl#show ipv6 access-list ipv6acl) to display added ACLs to the router.
- Then set up configuration for all topology components and show the impact of ACL rules (e.g., how C3 will access servers but not C1 or C2)



```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2018:aaaa::1/64
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2018:cccc::1/64
 ipv6 traffic-filter ipv6acl out
!
no ip http server
no ip http secure-server
```

Fig. 4.15 A sample of GNS3 configuration file

Bibliography

CJCSM6510.01B (2013) http://www.jcs.mil, https://fas.org/irp/doddir/dod/cjcsi6510_01.pdf

Lee M, Svajcer V (2017) Snort signatures. http://blog.talosintelligence.com/2018/01/2017-in-snort-signatures.html

National Cybersecurity and Communication Integration Center (2014) Combating the insider threat. https://www.us-cert.gov

Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs (2014) Attachment C: core cyber defense performance data and metrics. http://www.dote.osd.mil/pub/policies/2014/8-1-14_Procs_for_OTE_of_Cybersec_in_Acq_Progs(7994).pdf

Radvanovsky R, Brodsky J (2016) Handbook of SCADA/control systems security, 2nd edn. CRC Press, Boca Raton

Vormetric Data Solutions (2015) Vormetric insider threat report 2015. http://enterprise-encryption.vormetric.com/rs/vormetric/images/CW_GlobalReport_2015_Insider_threat_Vormetric_Single_Pages_010915.pdf

Whitman ME, Mattord HJ (2008) Principles of information security. Course Technology, Stamford

Chapter 5
Cyber Intelligence

As a subset of cyber security, cyber intelligence, also called: cyber threat intelligence is about information acquisition for tracking, analyzing, and countering of cyber, digital, or information security threats. Cyber intelligence serves as the backbone for integrated security frameworks where the accuracy and credibility of collected information about possible threats can significantly impact the ability to counter or respond to such threats, Fig. 5.1.

Not only cyber intelligence teams; private or public use the Internet and public resources to learn about threats and vulnerabilities but also hackers and attackers. In the year 2016 alone, 135 high threat zero-day exploits in Adobe, 76 in Microsoft products and 50 in Apple products were discovered, (Zero Day Initiative: https://www.zerodayinitiative.com, 2017).

K0409: Knowledge of Cyber Intelligence/Information Collection Capabilities and Repositories

What are some of the major goals for cyber intelligence?

Security frameworks include an important component related to security assessment (i.e., identification, prioritization, mitigation). But how can we identify, mitigate, etc. an organization possible risk? Risks or threats are ranked or prioritized based on their probability of occurrence, impact, etc. Quantitative and qualitative methods can be used, but in all cases, cyber intelligence is an important stage to help in collecting credible threat assessment information.

I. Alsmadi, *The NICE Cyber Security Framework*,
https://doi.org/10.1007/978-3-030-02360-7_5

Smart Data
accurate
actionable
rapid

Fig. 5.1 Smart input data for actionable intelligence (http://aescit.com/cyberintel)

Cyber Intelligence Levels

- Strategic cyber intelligence. Those are high-level goals of the organizations targeting threats or malicious actions. At this level, it's important to identify threats' sources, main goals, and possible consequences.
- Operational cyber intelligence. At this level, more operational information about threats are targeted. For example, cyber intelligence team will try to acquire the following information about each possible threat: capabilities and resources attackers have or will require to have to be able to successfully meet their strategic goals. Cyber intelligence team will try also to predict their entry targets, intrusion and propagation methods, etc. that the cyber attacker will require to carry out the attack to further their strategic goals.
- Tactical or technical cyber intelligence. Knowledge at this level will be related to what kind of real-time methods and tools (e.g., software) they will use and what will be the possible counter or response mechanisms from the defender.

Sources of Cyber Intelligence or Collection Capabilities

Currently, there are several categories or sources of cyber intelligence, also called collection capabilities, or intelligence gathering disciplines. This list continuously grows vertically and horizontally.

- ***Open source intelligence (OSINT)*:** Cyber intelligent team should learn how to gather data points, transform these data points into actionable intelligence that can prevent target attacks. They should learn how to identify, repel, or neutralize targeted intelligence gathering against organizational assets. OSINT includes data collected from publicly available sources, free or subscription-based, online or offline.

- ***OSINT*** can include many sub-categories such as:
  - **Classical media**: Such as newspapers, magazines, radio, and television channels
  - **Online social networks (OSNs) or Social media intelligence (SOCMINT)**: Blogs, discussion groups, Facebook, Twitter, YouTube, etc.
  - Internet public websites and sources
  - Communication Intelligence (COMINT)
  - Measurement and signature intelligence (MASINT)
  - Search engines (e.g., Google, Yahoo)
  - **Deep or dark web intelligence**

    Deep web: Those include web pages, documents, etc. that are not indexed by main search engines and/or that cannot be read or accessed by conventional methods.

    In percentage, the public or visible web is much smaller than deep web. Deep web can include the following categories: Dynamic web pages, Blocked sites, Unlinked sites, Private sites, Non-HTML or Scripted content, and Limited or local access networks or content not publicly accessible through the Internet.

    Dark web or net: Those include web pages, documents, etc. that are accessed by anonymized methods (e.g., TOR browsers) and are often used for criminal activities.

    The dark web has become a port for hacking communities, offering cyber criminals the ability to discuss offer and sell new and emerging exploits (e.g., zero-day vulnerabilities or exploits). Zero-day forum is a popular example of darknet websites (website link continuously varies, e.g., http://qzbkwswfv5k2oj5d.onion.link/, http://msydqstlz2kzerdg.onion/).

    Some of dark web forums are accessible only via the TOR network, while others are accessible via traditional web browsing. Those dark web forums start to have their own strict vetting processes to ensure that they will not be targeted by intelligent teams and face criminal charges and legal consequences. As such, it is common to have some users in those websites who are decoy intelligence personnel, police officers, FBI, etc.

    The website is a market for buying and selling zero-day vulnerabilities. In addition to zero-day vulnerabilities, these forums offer a variety of "services" ranging from illegal drug sales, forged items (e.g., passports, driver licenses, credit cards, bank notes), weapons, identity theft information (e.g., PII; personal identifiable information), or botnet services.

    For security intelligence, one of the main goals to study dark webs is to develop a functioning system for extracting information from those communities and apply machine learning methods to predict cases of considerable threats. The fact that humans heavily depend and use the Internet these days in all life aspects, gives hackers a platform rich of data and resources for hackers to collect data and learn how to hack and attack users and information systems (ACS 2016). Not even dark websites, but public websites can also be

Table 5.1 Examples of darknet marketplaces (Anomali 2017)

Marketplace	URL
Sky-Fraud	http://sky-fraud.ru/
Exploit.in	https://forum.exploit.in
LeakForum	https://leakforums.net
HackForums	http://hackforums.net/
PaypalTheRealDeal	http://trdealmgn4uvm42g.onion
Alphabay	http://pwoah7foa6au2pul.onion

used as effective hacking or attacking tools. For example, websites such as: Shodan: (https://www.shodan.io/), Zomeye: (https://www.zoomeye.org), and https://www.go4expert.com/ can provide a wealth of information for attackers about candidate targets with very good introduction details to start further investigations and analysis. Table 5.1 shows examples of darknet marketplaces or websites (Anomali 2017).

The following link (7839 Awesome Deep Web Links List, https://darkweb-news.com/deep-web-links/) includes a large list of dark websites.

- **SIGINT (signal or electronic mediums such as satellites).** It can also include: GEOINT (geospatial intelligence, e.g., images taken from aircraft, satellite) and MASINT (measurement and signature intelligence; e.g., radar data). For example, Google earth and different mapping and location-based services now provide details and collect geo-related activities and information that possible many governments were or are not able to collect using intelligent resources. High-quality geo-images used to be expensive and have many restrictions where now they can be offered for free. Several references and studies indicated that websites such as Google track users' locations even when data or location-based services are not enabled.

While OSINT information is available largely for free, however several challenges exist related to information overload, the collection, and aggregation process. Additionally, transferring such information into actions is not trivial. Several recent security incidents in the USA showed that significant information was available before many events. The problems were related to making timely proper actions or synchronizing information from the different sources.

The Intelligence Lifecycle or Activities

Cyber intelligence is a cycle process of collection and utilizing data. Followings are the major steps:

- Initial analysis and planning and direction: Similar to any project first stage should include requirements analysis and planning. We should have defined goals or else data analysis and intelligence will be very time-consuming and unfocused. The process can be however evolutionary where initial requirements and plan can be a good start (in the first cycle). Outputs from earlier cycles can be used to improve further analysis and planning in next cycles.

- Data collection stage: Data is collected, manually or through tools from the different sources we have mentioned earlier. Programming and scripting languages such as: Python, R, Ruby, Java, Go, etc. can be used to automate the parsing process. Many websites may resist the parsing or crawling process (especially OSNs). Alternatively, those websites offer their own APIs (largely with limited capabilities) to parse their data (e.g., see: https://developers.facebook.com, https://dev.twitter.com/docs, https://www.npmjs.com/package/google-trends-api). Data can also be collected from logs such as: Honeypots, Firewall logs, Intrusion Detection System logs, and scans of the Internet.
- Data processing: Several data preprocessing techniques are typically employed in the data analysis activities. For example, this stage may include how to prepare data for analysis (e.g., stemming, stop-words' removal), data storage, and retrieval methods. In some cases, data can be stored into text file, small-scale databases, or big data repositories.
- Data analysis and production: This is the main goal and most time-consuming task in the cycle. In this task, knowledge and intelligence, according to the project goal are extracted.
- Data dissemination and usage: In an evolutionary process, this can trigger further data analysis in future cycles. In later cycles, knowledge and intelligence are produced to decision-makers or target audience.

Areas of Cyber Intelligence

- **Cybercrime**
  Cyber intelligence can be part of forensic analysis and investigation for a digital forensic team. They can be related to a single incident or crime or a large-scale national or international malware, hacking, etc.
- **Hacktivism**
  Political, social, or environmental causes may drive some people to participate in hacking activities. A noble cause however does not justify an illegal or unethical mean. As such, Hacktivists utilize similar hacking techniques to avoid detection. Anonymous is an example of a popular international Hacktivism organization, largely for political agenda.
- **Cyber espionage or cyber spying**
  Cyber spying between governments witnessed a significant increase in the last few years especially from countries such as Russia and China on the USA. Government sponsored cyber spying can be persistent with many illusive groups, activities, and targets.
- **Advanced Persistent Threat, APT**
  Some malwares and attacks were persistent. They may come back periodically using different forms or shapes or with slightly different attacking mechanisms, while persistent on similar targets. Table 5.2 shows examples of the noticeable or significant APTs (ISACA2018).

Table 5.2 Examples of significant APTs, (ISACA2018)

APT	Year	APT	Year	APT	Year
The Cuckoo's Egg	1989	Zeus	2007	RSA attack	2011
Moonlight Maze	1989	GhostNet	2009	Duqu	2011
Titan Rain	2003	Operation Aurora	2009	Flame	2012
Sykipot	2006	SpyEye	2009	Red October	2012
Gozi	2007	Stuxnet worm	2010	Eurograbber	2012

K0525: Knowledge of Required Intelligence Planning Products Associated with Cyber Operational Planning

Based on public or private sectors, intelligence planning can produce different products:

- Dynamic threat assessment DTA or threat intelligence assessment (TIA):
  DTA tries to identify the capabilities and intentions of adversaries or threats. A dynamic or automated threat assessment model is expected to provide real time, or near real time threat assessment and whether a subject threat should trigger further serious security measurements.
  The real challenge is that catastrophic events are low in probability and catastrophic in consequences. In order to develop a dynamic or auto threat assessment system, such system can be very complex and expensive to develop, maintain, and continuously train as cyber security threats are very dynamic. Probability of attacks is low, but also probability to stop the attack can also be low. Dynamic threat assessment may or may not stop an attack. In most cases, threat assessments may target reducing the probability of attack occurrence, reducing or mitigating its impact.
  DTAs may include the following main components: indicators of compromise, attack tactics, techniques and procedures, suggested actions and responses, and finally postmortem analysis and findings.
- Intelligence Support Plans. At the national level, NISP support plan shows how intelligent capabilities can be used to meet intelligence requirements. NISP tries also to integrate intelligence knowledge from different national sources.
- Cyber situation awareness: Security awareness programs try to educate users and employees on how to reduce attack occurrences. Many attacks start from social engineering techniques (e.g., phishing links). Users are tricked to click such links or emails which will eventually trigger further security problems. Cyber intelligence can be an affective knowledge source to direct and focus cyber security awareness trainings.
- Cyber operational planning (COP): Using cyber intelligence, COP develops detailed operational security plan for cyberspace operations through collaboration and integrated intelligence efforts across organizations or national borders. In NICE framework, COP includes three specialty areas: Cyber Intel Planner, Cyber Ops Planner, and Partner Integration Planner (Fig. 5.2).

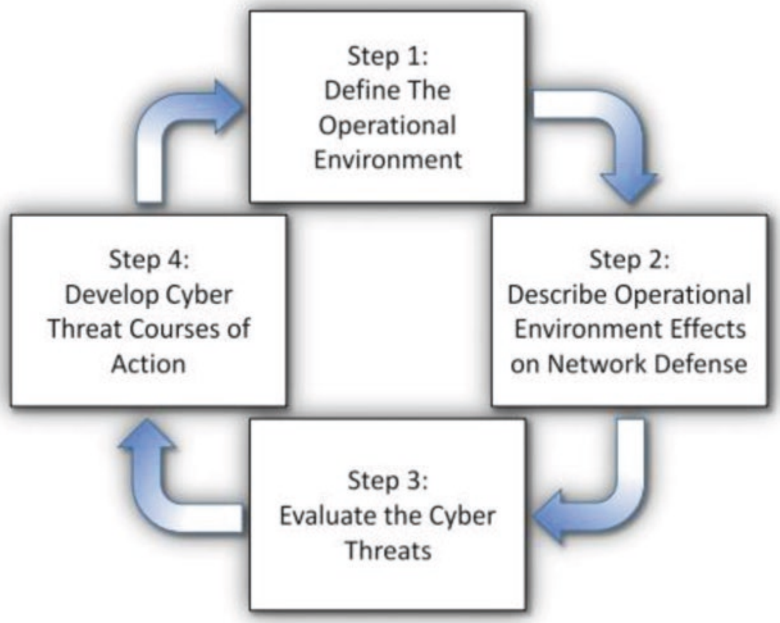

Step 1:
Define The Operational Environment
Step 2:
Describe Operational Environment Effects on Network Defense
Step 3:
Evaluate the Cyber Threats
Step 4:
Develop Cyber Threat Courses of Action

Fig. 5.2 Cyber operational environment (Kime 2016)

K0550: Knowledge of Target, Including Related Current Events, Communication Profile, Actors, and History (Language, Culture) and/or Frame of Reference

In NICE framework, Targets (TGT) can be regions, countries, non-state entities, and/or technologies. As specialty area, TGT has two work roles: target developer (level 1) and target network analysis (level 2).

Knowledge to acquire in those two work roles can be very large, given that Targets can be defined at different levels of complexities and details. Additionally, the amount of knowledge and information to collect about possible targets can be very large and complex and require aggregation of data from many sources including structured and largely unstructured data.

K0553: Knowledge of Tasking Processes for Organic and Subordinate Collection Assets

Team or personnel in cyber intelligence can work with different sources of information including humans, employees, agents, other agencies, services, and allied forces. Communication with different information sources is necessary and should always be effective to ensure passing the right information to the right decision-makers in the right time.

K0554: Knowledge of Tasking, Collection, Processing, Exploitation, and Dissemination

The process of tasking, collection, processing, exploitation, and dissemination functions (TCPED) of intelligence data drives decision-making and intelligent operations at different levels. It represents an intelligence cycle from tasking information intelligence process (e.g., by commander) to disseminating it to end users or proper channels. Acting based on the disseminated information is not part of the TCPED cycle.

The TCPED process utilizes intelligence to support operations at all levels. An effective TCPED process should be able to help operations and intelligence planners to address validated needs and collect data to best address those needs. In some security literature, the term TCPED is replaced with: PCPAD (Planning and Direction, Collection, Processing and Exploitation, Analysis and Production, and Dissemination). The following section describes briefly the TCPED tasks.

Tasking The process by which collection assets are assigned to collect based on an initial request.

Collection Data is collected, based on the task from all possible sources, including humans, employees, agents, other agencies, services, and allied forces. They can also be software agents or bots; small programs that crawl the web searching for certain information.

Processing In processing stage, data analysis activities try to extract knowledge based on requested task. Each intelligence project can require inputs from different sources and also different processing methods and tools. Additionally, this stage can be the most labor-intensive and time-consuming tasks.

Exploitation Exploitation stage extends the processing stage to convert information into intelligence.

Dissemination Dissemination is the process of passing information and findings to end users or decision-makers. Intelligence products are disseminated through all available delivery methods.

K0562: Knowledge of the Capabilities and Limitations of New and Emerging Collection Capabilities, Accesses, and/or Processes

Similar to the sources of data, the tools and applications to collect data are very large, vary between commercial, open source, and free ones. Their capabilities and limitations vary widely. Analysis team should continuously research to stay aware for new and emerging tools and applications. Websites, software tools, and applications continuously change and their capabilities vary rapidly.

We described in a previous KSA (i.e., K0409) examples of new or emerging collection capabilities: HUMINT, SIGIN, OSINT, etc.

K0568: Knowledge of the Definition of Collection Management and Collection Management Authority

K0404: Knowledge of Current Collection Requirements

In collection management, intelligence collection requirements from various resources is managed and organized. Intelligence requirements are converted to collection requirements: observables/data inputs. The collection requirements can also include monitoring social networks, blogs, online forums, news outlets, etc. Other collection management activities are: establishing priorities, tasking or coordinating with appropriate collection sources or agencies, and monitoring results.

Collection management authority: CMA establishes, prioritizes, and validates theater collection requirements, and collection policies.

Collection managers should have management and communication skills to communicate and coordinate with allies and partners. They should report to security decision-makers and production managers with timely, accurate, and concise information in a manner that safeguards sensitive intelligence sources and methods. With the large number of volumes of collection capabilities, it is important for collection manager to focus the collection process and assets based on a specific scope driven by collection requester and their intelligence requirements (IRs).

Joint Management Support Tools or Collection Management Support Tools is used in the USA to support collection managers who work with the government. JMST information system provides integrated capabilities from a variety of sources mentioned earlier in KSA K0409.

K0571: Knowledge of the Feedback Cycle in Collection Processes

Intelligence collection processes typically go through several cycles of: tasking, collection, processing, exploitation, and dissemination functions (TCPEDs). They can start from initial Intelligence requirements and evolve based on real-time collected and processed information.

Feedback or output from the collection process should be actionable. All organizations whose actions affect the status of requirements must cooperate by making status changes available on a timely basis. This near real-time feedback capability will facilitate the task of: dynamic re-tasking.

The re-tasking stage feeds back into the collection process and redirects collection toward high priority targets or goals that are identified based on previous collection cycles and intelligence requirements (e.g., priority intelligence requirements; PIRs).

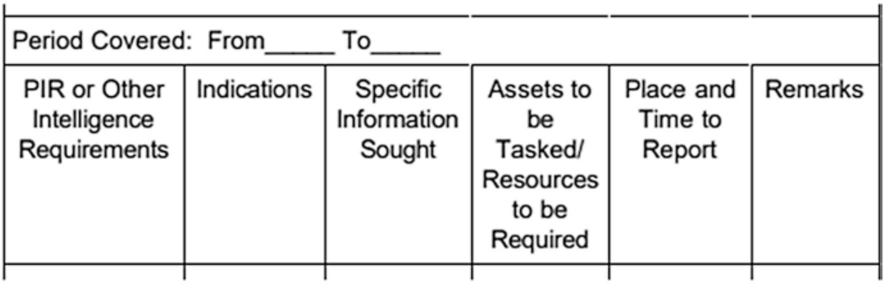
K0578: Knowledge of the Intelligence Requirements Development and Request for Information Processes

Intelligence requirements represent the key activity to guide the whole collection process cycle and focus the collection process on the most important information needs. Several attempts exist to develop intelligence requirement frameworks to integrate efforts from different sources and create unified terminologies. But what can guide the intelligence requirements themselves?

Comprehensive risk assessments that include threat, vulnerability, and consequence are crucial elements in identifying specific intelligence requirements. Those can reveal current or existing information or intelligent gaps that should be filled through intelligent gathering and collection processes. On the other hand, intelligence requirements can be triggered by users seeking some intelligent information about an adversary, their capabilities, intentions, or actions. This information need is then expressed to the appropriate element of the intelligence community as intelligence requirements (e.g., key questions to answer).

K0580: Knowledge of the Organization’s Established Format for Collection Plan

The collection plan establishes guidance for collection activities and tasks’ collection assets. It brings information sources’ list (e.g., humans, OSINT) and intelligent requirements to action, allocating resources and sources to intelligent requirements and objectives. A logical plan is developed for transforming the essential elements of



Period Covered: From_____ To_____					
PIR or Other Intelligence Requirements	Indications	Specific Information Sought	Assets to be Tasked/ Resources to be Required	Place and Time to Report	Remarks

Fig. 5.3 Collection plan format (HSDL 1996 and 2004)

information into orders or requests to sources' list to be accomplished within a required time limit. The collection should include at minimum the PIRs, intelligence indicators, Specific information requirements (SIRs), Specific orders and requests (SORs), and collection agencies or assets available.

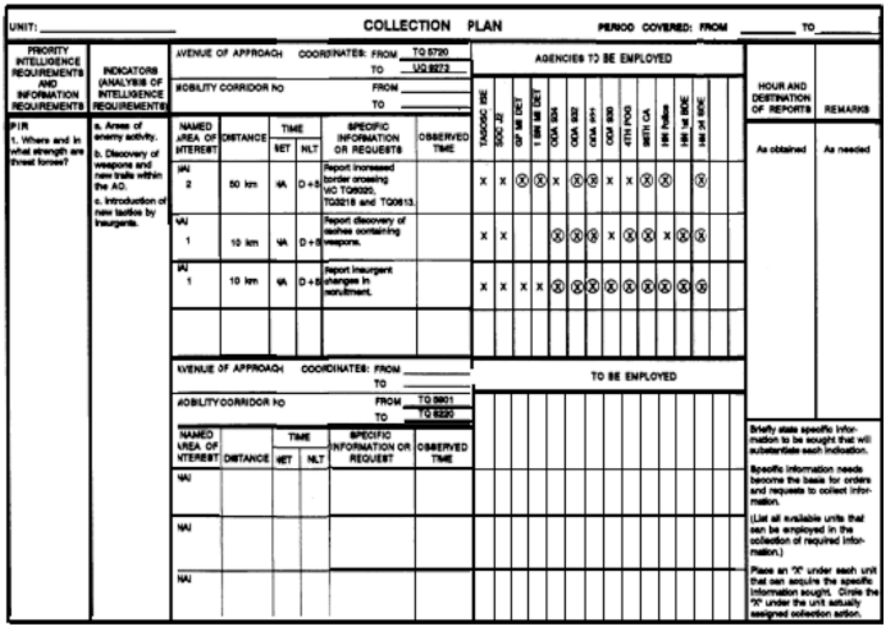
The collection plan can be informally used only by the intelligence staff or can be formal based on a structured template (e.g., Fig. 5.3) that can be communicated among different departments. The collection plan includes intelligence requirements, intelligence indicators, when information is needed, who is to receive the collection intelligence, and how it will be used, Fig. 5.3, (HSDL 1996 and 2004). The template should also be divided into different sections based on the source or category of collection (e.g., OSINT, HUMINT, SIGINT).

Examples of other collection template formats include: Standard collection format and dispersed battlefield collection plan format (FM34-2 and FM34-7, Globalsecurity). Figure 5.4 shows a standard collection format with sample entries (FM34-2 and FM34-7, Globalsecurity).

K0595: Knowledge of the Relationships of Operational Objectives, Intelligence Requirements, and Intelligence Production Tasks

Operational objectives are developed during mission analysis and are typically derived from theater-strategic or national-level guidance. Operational objectives guide and prioritize intelligent requirements (Principle of Timeliness: Intelligence must be available and accessible in the right time to be able to effectively use it.).

Intelligence production converts information into intelligence, according to initial intelligent requirements and produce intelligence that is reliable, valid, current, and relevant. In some cases, analysts perform analysis to create new intelligence and knowledge for further collection and analysis.



UNIT: ______ COLLECTION PLAN PERIOD COVERED: FROM ______ TO ______

AVENUE OF APPROACH COORDINATES: FROM TQ 5720 TO UQ 8273

MOBILITY CORRIDOR NO FROM ______ TO ______

PRIORITY INTELLIGENCE REQUIREMENTS AND INFORMATION REQUIREMENTS	INDICATORS (ANALYSIS OF INTELLIGENCE REQUIREMENTS)	NAMED AREA OF INTEREST	DISTANCE	TIME		SPECIFIC INFORMATION OR REQUESTS	OBSERVED TIME	AGENCIES TO BE EMPLOYED															HOUR AND DESTINATION OF REPORTS	REMARKS
				NET	NLT			TACSOC IDE	SOC J2	GP MI DET	1 BN MI DET	ODA 934	ODA 932	ODA 911	ODM 930	4TH POG	96TH CA	HN Police	HN 1st BDE	HN 2d BDE				
PIR 1. Where and in what strength are threat forces?	a. Areas of enemy activity. b. Discovery of weapons and new trails within the AO. c. Introduction of new tactics by insurgents.	NAI 2	50 km	NA	D+5	Report increased border crossing VIC TQ6020, TQ3218 and TQ0613.		X	X	⊗	⊗	X	⊗	⊗	X	X	⊗	⊗		⊗			As obtained	As needed
		NAI 1	10 km	NA	D+5	Report discovery of caches containing weapons.		X	X			⊗	⊗	⊗	X	⊗	⊗	X	⊗	⊗				
		NAI 1	10 km	NA	D+5	Report insurgent changes in recruitment.		X	X	X	X	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗				

AVENUE OF APPROACH COORDINATES: FROM ______ TO ______

MOBILITY CORRIDOR NO FROM TQ 9901 TO TQ 8220

NAMED AREA OF INTEREST	DISTANCE	TIME		SPECIFIC INFORMATION OR REQUEST	OBSERVED TIME	TO BE EMPLOYED															
		NET	NLT																		Briefly state specific information to be sought that will substantiate each indication. Specific information needs become the basis for orders and requests to collect information. (List all available units that can be employed in the collection of required information.) Place an "X" under each unit that can acquire the specific information sought. Circle the "X" under the unit actually assigned collection action.
NAI																					
NAI																					
NAI																					

Fig. 5.4 A standard collection format with sample entries (FM34-7: Globalsecurity)

In military, primary intelligence production tasks are:

- Intelligence Preparation of the Battlefield (IPB): Threat and environment analysis in a specific geographical area.
- Situation Development: Producing current intelligence about the threat situation in a specific geographical area.
- Target Development: The analysis of a potential adversary (e.g., their capabilities) to determine their significance and relevance to mission defined objectives. Each target's lethal and nonlethal capabilities should be evaluated to develop a prioritized list of targets and the intelligence requirements that support target analysis.
- Battle Damage Assessment (BDA): The timely and accurate estimate of damage from the application of a military force, either lethal or nonlethal, against a predetermined objective.

Cyber Intelligence: K0596 Knowledge of the Request for Information Process

Requirements in general and intelligence requirements in particular generally fall into three categories: critical information requirements (CIRs), priority information requirements (PIRs), and requests for information (RFIs).

Request for information or request for intelligence (RFI) is related to getting directions or guidance about intelligence cycle or process. They can be used to clarify plans, specifications, intelligent requirements, collection objectives, etc.

The request should summarize asked questions. In addition to the request, RFI should include requester, output expectations (e.g., a summary document, presentation), and priority or due date.

A successful outcome of an RFI depends on:

- The existence of structured RFI templates and procedures. The templates and procedures should be simplified to accelerate the process.
- Knowing the right administrative procedures for RFIs. For example, RFI may include a request approval for some deviations from initial requirements that cannot be met for some reasons. RFI may also include queries to obtain directions on how to proceed when there are conflicting input requirements.
- Clarity of RFI queries or questions. This includes providing all supporting or required documents, reasons, etc.
- Citing specific portions of relevant plans, requirements, documents, etc. that are the subject of the request.
- Quoting excerpts from concrete references needed to clarify unclear portions to facilitate answering questions or queries in the RFI. Figure 5.5 shows an example of an RFI process workflow, (Bottari 2014).

Figure 5.6 shows an RFI template showing the major components to be included (VeriSign 2012).

K0602: Knowledge of the Various Collection Disciplines and Capabilities

K0458: Knowledge of Intelligence Disciplines

Intelligence collections may include host nation actors and agencies as well as other allied nations' actors and capabilities. Those capabilities can vary depending on their capabilities and the data and information requested. These capabilities are somewhat related to intelligence collection disciplines (INTs); described in an earlier KSA (i.e., human intelligence (HUMINT); imagery intelligence (IMINT); measurement and signature intelligence (MASINT); open source intelligence (OSINT); and signal intelligence (SIGINT)), Fig. 5.7 (McCarron 2015). There are also multiple intelligence complementary capabilities.

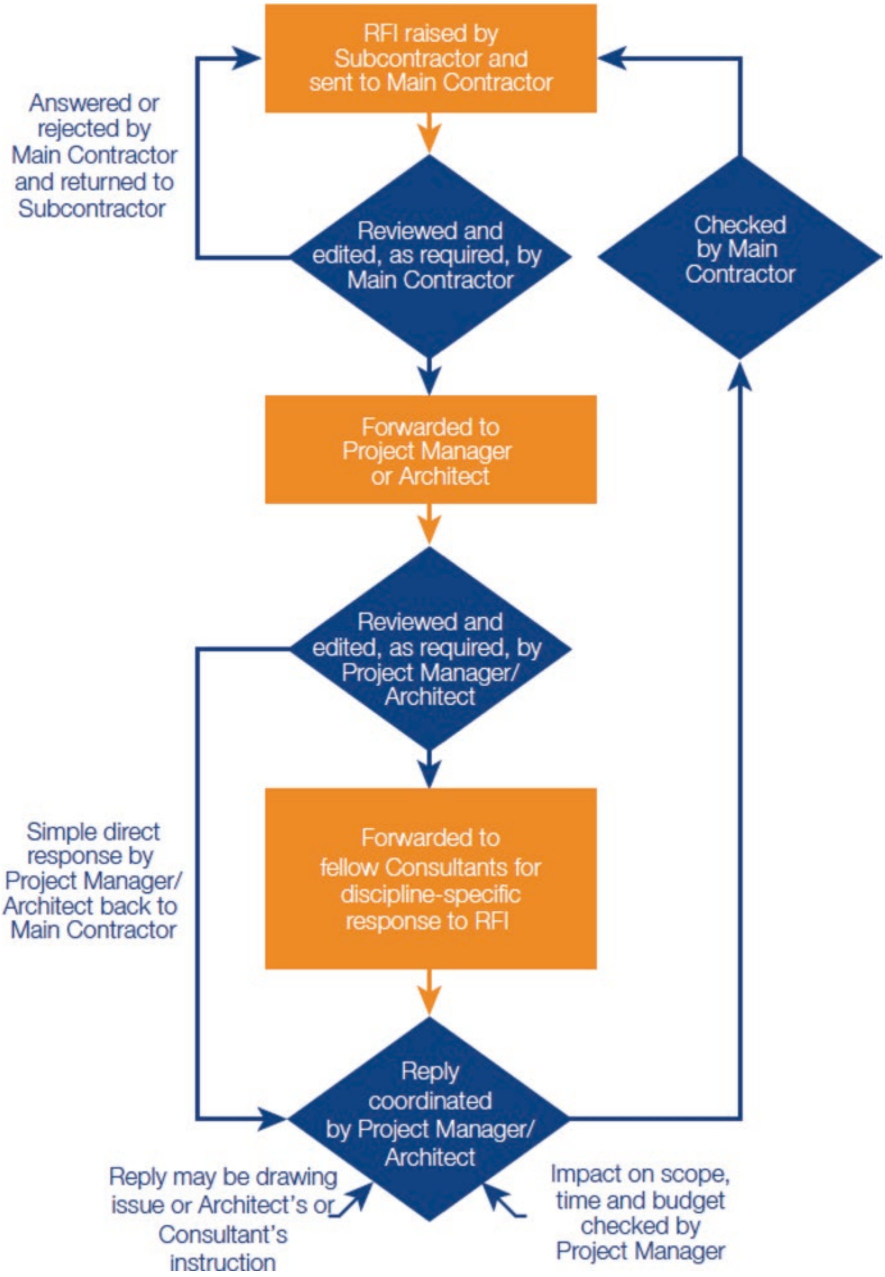
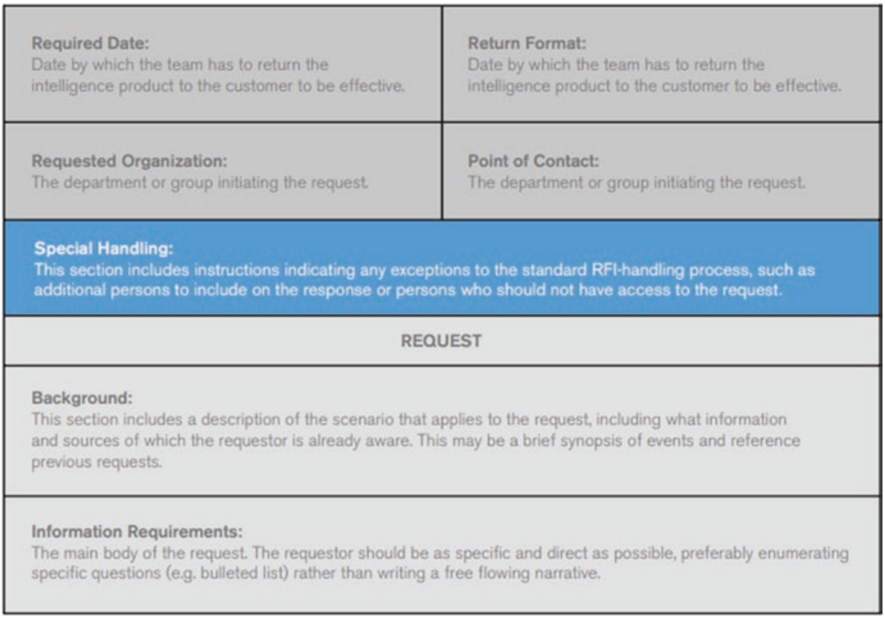

RFI raised by Subcontractor and sent to Main Contractor
Answered or rejected by Main Contractor and returned to Subcontractor
Reviewed and edited, as required, by Main Contractor
Checked by Main Contractor
Forwarded to Project Manager or Architect
Reviewed and edited, as required, by Project Manager/ Architect
Simple direct response by Project Manager/ Architect back to Main Contractor
Forwarded to fellow Consultants for discipline-specific response to RFI
Reply coordinated by Project Manager/ Architect
Reply may be drawing issue or Architect's or Consultant's instruction
Impact on scope, time and budget checked by Project Manager

Fig. 5.5 An example of an RFI process workflow, (Bottari 2014)



Required Date: Date by which the team has to return the intelligence product to the customer to be effective.	**Return Format:** Date by which the team has to return the intelligence product to the customer to be effective.
Requested Organization: The department or group initiating the request.	**Point of Contact:** The department or group initiating the request.

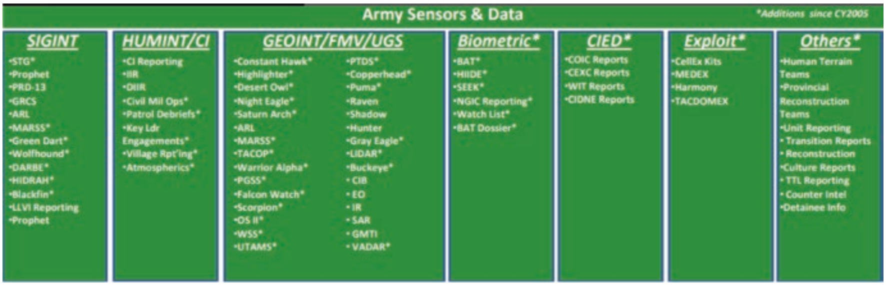
Special Handling:
This section includes instructions indicating any exceptions to the standard RFI-handling process, such as additional persons to include on the response or persons who should not have access to the request.

REQUEST

Background:
This section includes a description of the scenario that applies to the request, including what information and sources of which the requestor is already aware. This may be a brief synopsis of events and reference previous requests.

Information Requirements:
The main body of the request. The requestor should be as specific and direct as possible, preferably enumerating specific questions (e.g. bulleted list) rather than writing a free flowing narrative.

Fig. 5.6 An RFI template from: (VeriSign 2012)



Army Sensors & Data

*Additions since CY2005

SIGINT
•STG*
•Prophet
•PRD-13
•GRCS
•ARL
•MARSS*
•Green Dart*
•Wolfhound*
•DARBE*
•HIDRAH*
•Blackfin*
•LLVI Reporting
•Prophet

HUMINT/CI
•CI Reporting
•IIR
•DIIR
•Civil Mil Ops*
•Patrol Debriefs*
•Key Ldr Engagements*
•Village Rpt'ing*
•Atmospherics*

GEOINT/FMV/UGS
•Constant Hawk*
•Highlighter*
•Desert Owl*
•Night Eagle*
•Saturn Arch*
•ARL
•MARSS*
•TACOP*
•Warrior Alpha*
•PGSS*
•Falcon Watch*
•Scorpion*
•OS II*
•WSS*
•UTAMS*
•PTDS*
•Copperhead*
•Puma*
•Raven
•Shadow
•Hunter
•Gray Eagle*
•LIDAR*
•Buckeye*
• CIB
• EO
• IR
• SAR
• GMTI
• VADAR*

Biometric*
•BAT*
•HIIDE*
•SEEK*
•NGIC Reporting*
•Watch List*
•BAT Dossier*

CIED*
•COIC Reports
•CEXC Reports
•WIT Reports
•CIDNE Reports

Exploit*
•CellEx Kits
•MEDEX
•Harmony
•TACDOMEX

Others*
•Human Terrain Teams
•Provincial Reconstruction Teams
•Unit Reporting
• Transition Reports
• Reconstruction
•Culture Reports
• TTL Reporting
• Counter Intel
•Detainee Info

Fig. 5.7 Multinational intelligence (McCarron 2015)

Bibliography

ACS (2016) Cybersecurity: threats, challenges, opportunities. https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf

Anomali (2017) Medium, shedding some light on the dark web. https://medium.com/@AnomaliDetect/shedding-some-light-on-the-dark-web-9581af0d9600. April 19th 2017

Bottari T (2014) Ten tips on managing RFIs for your construction projects, Oracle Aconex, January, 16, 2014. https://www.aconex.com/blogs/ten-tips-on-managing-rfis-for-your-construction-projects/

Collection plan formats and instructions, FM34-7: globalsecurity. https://www.globalsecurity.org/intell/library/policy/army/fm/34-7/34-7_appd.pdf

Joint Intelligence Support to Military Operations, Homeland Security Digital Library, United States. Joint Chiefs of Staff (1996 and 2004)

Kime B (2016, March 26) Threat intelligence: planning and direction. Unpublished master's thesis, SANS Technology Institute. https://www.sans.org/reading-room/whitepapers/threats/threat-intelligenceplanning-direction-36857

McCarron V (2015) Big data for defense and intelligence, ttcus.com

VeriSign (2012) Establishing a formal cyber intelligence capability, White Paper. https://www.verisigninc.com/assets/whitepaper-idefense-cyber-intel.pdf. Accessed Nov 17 2014

Chapter 6
Cyber Intelligence Analysis

Cyber intelligence (CYBINT) evolves recently as a discipline with major tasks related to cyber intelligence collection, analysis, and dissemination. CYBINT can be related to several categories of INT (e.g., HUMINT, SIGINT, and OSINT). However, in comparison with those, CYBINT deals with very broad and illusive intelligence spectrum that can require daily changes in terms of intelligence collection, analysis, and dissemination. Additionally, CYBINT can easily cross-national borders bypassing all kinds of security controls. For example, a worm that is created somewhere in the world can spread within hours, minutes, or even seconds to thousands of computers all over the world. One more distinction is that with the five main collection disciplines mentioned earlier, key players are typically countries, government agencies, or some medium to large size companies. On the other hand, in CYBINT, a key player can be just an individual (e.g., a professional hacker) who is making a large impact across the world.

The publicity and availability of the Internet and its resources to all people around the world can create both opportunities and challenges for CYBINT; it makes collecting data about any individual or entity around the world possible, while it can also create similar opportunities for hackers and malicious users. They can even use Proxies, Virtual Private Networks (VPNs), Anonymizers, or Spoofing tools to hide or fake their identities. Users around the world, with limited resources, and even skills can make serious worldwide impacts given the availability of a large inventory of free and open source hacking and cyber tools.

I. Alsmadi, *The NICE Cyber Security Framework*,
https://doi.org/10.1007/978-3-030-02360-7_6

K0110: Knowledge of Common Adversary Tactics, Techniques, and Procedures in Assigned Area of Responsibility (i.e., Historical Country-Specific Tactics, Techniques, and Procedures; Emerging Capabilities)

As part of threat intelligence activities (in particular technical and tactical threat intelligence) details about adversaries should be investigated. The main purpose is to inform decision-makers regarding the risks and implications associated with the different threats.

Common adversary tactics (tactical adversary goals during an attack), techniques (how adversaries achieve tactical goals), and procedures (i.e., steps or adversary usage of techniques) (TTPs) can help security intelligence teams better prepare for response and countermeasures. This term, TTPs is used in the military to describe adversary behaviors when committing or executing an attack.

TTPs can also be seen as the behavioral component of adversaries' actions in an ABC model of adversaries' actions that include: atomic, behavioral and computed actions (https://digital-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain/).

Extracting an adversary TTPs is not a trivial task and may need an integration of information from several different sources, structured and unstructured data, etc. (Fig. 6.1: Bianco 2017).

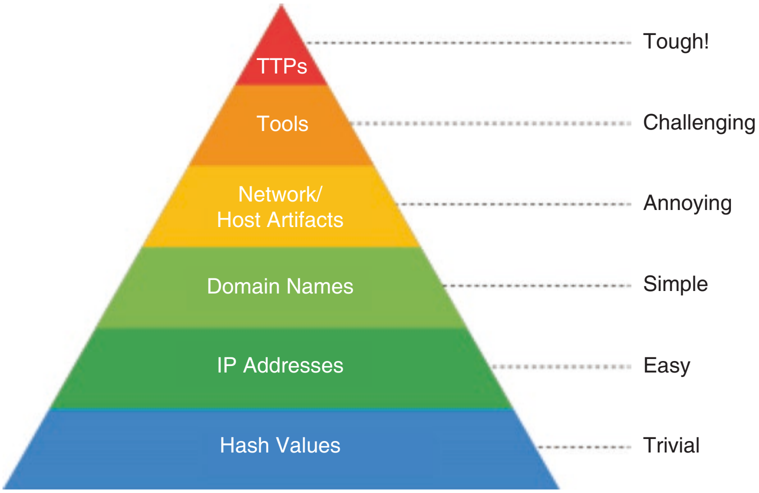


Fig. 6.1 The pyramid of pain (Bianco 2017)

Cyber Kill Chain Models

Kill chain model (https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html) shows the cyber-attack lifecycle and study adversary behaviors as a sequence of attack progression activities (Fig. 6.2); while attack progressing steps may not be sequential in many cases and some activities may occur in parallel.

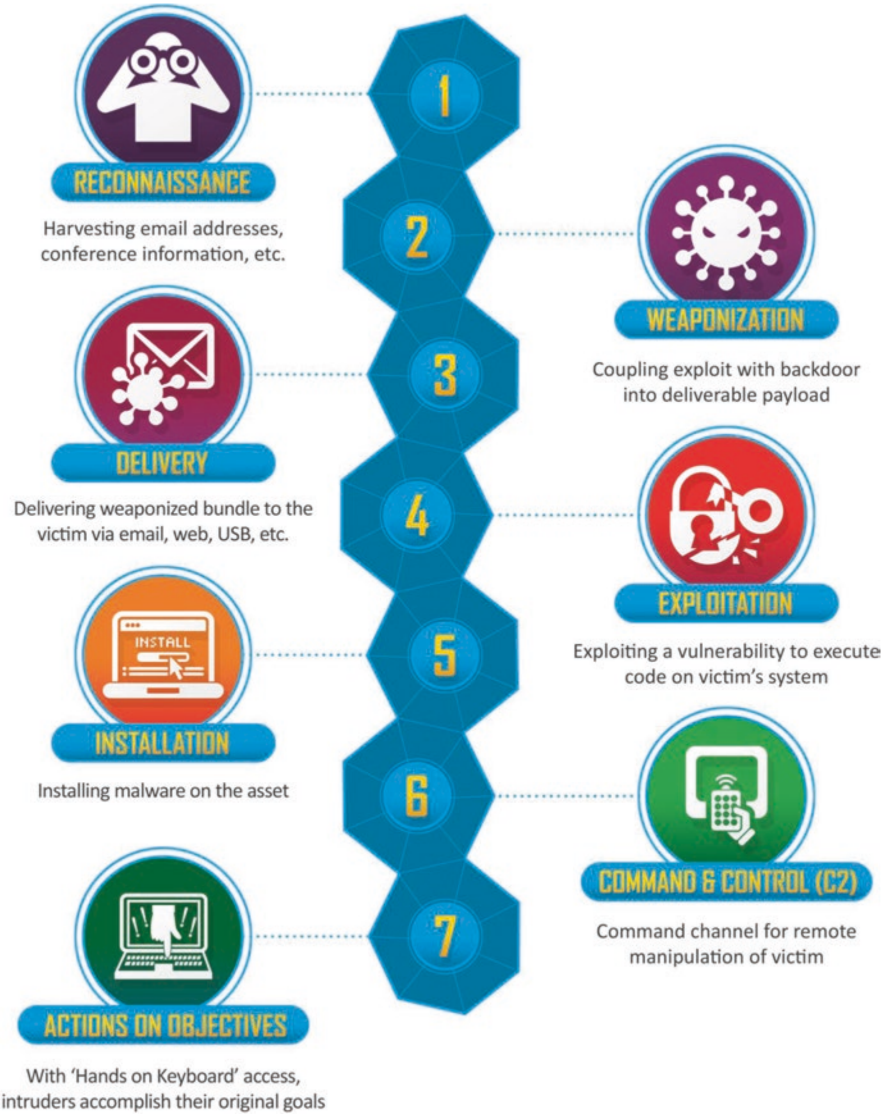

1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Fig. 6.2 Cyber kill chain model (https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html)

Additionally, the time and effort it will take in each attack in each one of those steps may vary. For defense teams (e.g., incident response teams, digital forensic investigators, or malware analysts) understanding the cyber-attack lifecycle or the chain can help them to work in a structured or chained manner. Each phase in the kill chain model in itself is a large research area to investigate and analyze.

Similar to LookheedMartin cyber threat lifecycle, NIST proposed a model for cyber-attack lifecycle: (Fig. 6.3: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf).

By studying cyber-attack lifecycle, we can understand attackers' behaviors, motives, techniques, etc. Additionally, we can evaluate and assess validity and completeness of security controls and protection mechanisms. We can also plan for mitigation activities for gaps in controls, possible existing vulnerabilities, etc.

Cyber Threats' Description Languages and Models

Several structured models exist to describe cyber threats. Here is a list of examples:

- Structured Threat Information Expression: STIX: http://stixproject.github.io/about/. DHS Automated Indicator Sharing (AIS) initiative (https://www.dhs.gov/ais) is utilizing STIX framework.
- Common Attack Pattern Enumeration and Classification schema: CAPEC: https://capec.mitre.org/index.html

MITRE ATT&CK framework behavioral-based threat model

MITRE (https://attack.mitre.org/wiki/Main_Page) is an example model, framework, or suite of threat models to represent TTPs that can be used against information

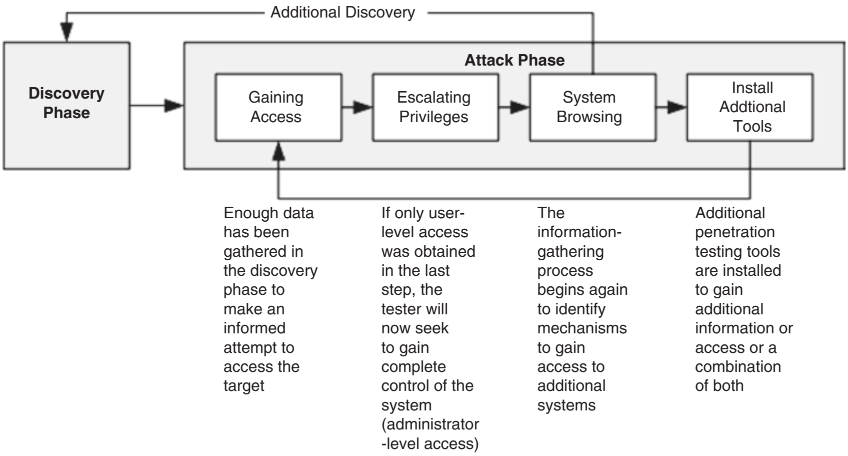
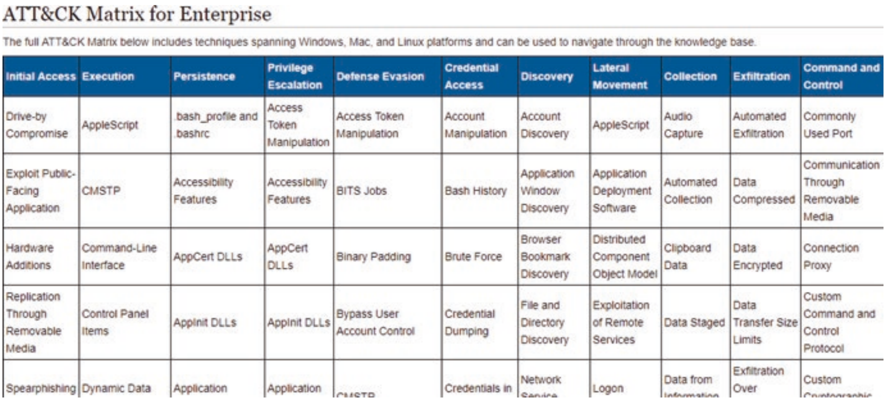

Additional Discovery
Discovery Phase
Attack Phase
Gaining Access
Escalating Privileges
System Browsing
Install Addtional Tools
Enough data has been gathered in the discovery phase to make an informed attempt to access the target
If only user-level access was obtained in the last step, the tester will now seek to gain complete control of the system (administrator -level access)
The information-gathering process begins again to identify mechanisms to gain access to additional systems
Additional penetration testing tools are installed to gain additional information or access or a combination of both

Fig. 6.3 Attack phase steps with loopback to discovery phase (nistspecialpublication800-115)

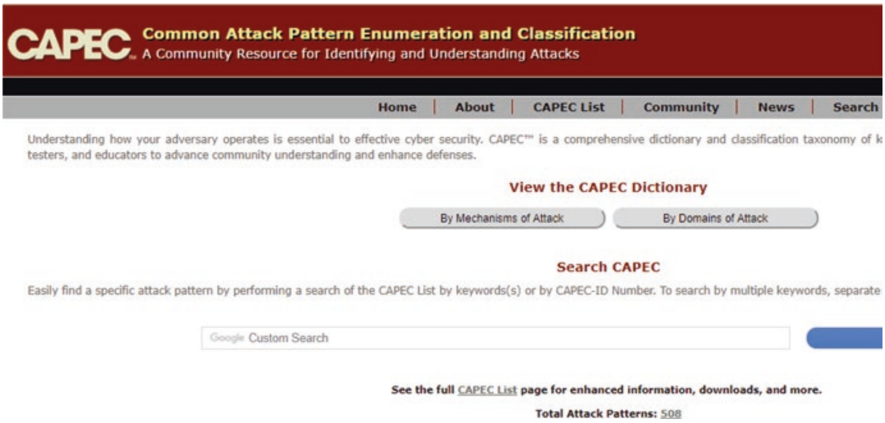


ATT&CK Matrix for Enterprise

The full ATT&CK Matrix below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the knowledge base.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	bash_profile and bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing	Dynamic Data	Application	Application	CMSTP	Credentials in	Network Service	Logon	Data from Information	Exfiltration Over	Custom Cryptographic

Fig. 6.4 A sample of MITRE ATT&CK attack matrix



CAPEC Common Attack Pattern Enumeration and Classification

A Community Resource for Identifying and Understanding Attacks

Home | About | CAPEC List | Community | News | Search

Understanding how your adversary operates is essential to effective cyber security. CAPEC™ is a comprehensive dictionary and classification taxonomy of k testers, and educators to advance community understanding and enhance defenses.

View the CAPEC Dictionary

By Mechanisms of Attack | By Domains of Attack

Search CAPEC

Easily find a specific attack pattern by performing a search of the CAPEC List by keywords(s) or by CAPEC-ID Number. To search by multiple keywords, separate

Google Custom Search

See the full CAPEC List page for enhanced information, downloads, and more.

Total Attack Patterns: 508

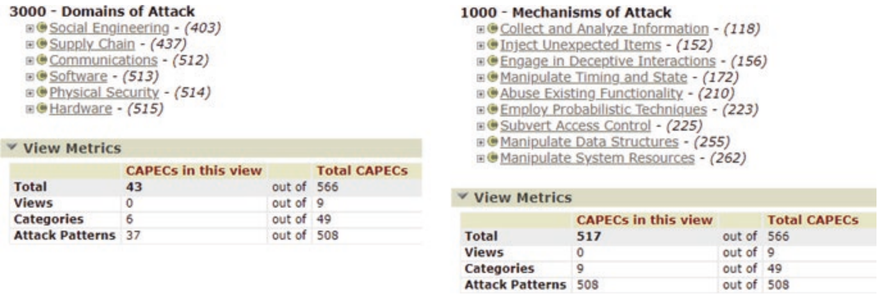
Fig. 6.5 MITRE CAPEC (https://capec.mitre.org/index.html)

systems. The framework starts with focusing on Windows operating systems and later on expands to other operating systems. The framework describes a large matrix of attacks on those different operating systems (Fig. 6.4: https://attack.mitre.org).

MITRE includes CAPEC (Common Attack Pattern Enumeration and Classification) attacks and attack patterns classification model (Fig. 6.5).

CAPEC classifies attacks based on either the domain or the mechanism of the attack into the categories shown in Fig. 6.6.

(ATT&CK) model can be enhanced by adding cyber-D&D TTTPs (tools, tactics, techniques, and procedures) that can be used by defenders to detect and mitigate attacker TTPs (Stech et al. 2016).



3000 - Domains of Attack

- Social Engineering - *(403)*
- Supply Chain - *(437)*
- Communications - *(512)*
- Software - *(513)*
- Physical Security - *(514)*
- Hardware - *(515)*

View Metrics

	CAPECs in this view		Total CAPECs
Total	43	out of	566
Views	0	out of	9
Categories	6	out of	49
Attack Patterns	37	out of	508

1000 - Mechanisms of Attack

- Collect and Analyze Information - *(118)*
- Inject Unexpected Items - *(152)*
- Engage in Deceptive Interactions - *(156)*
- Manipulate Timing and State - *(172)*
- Abuse Existing Functionality - *(210)*
- Employ Probabilistic Techniques - *(223)*
- Subvert Access Control - *(225)*
- Manipulate Data Structures - *(255)*
- Manipulate System Resources - *(262)*

View Metrics

	CAPECs in this view		Total CAPECs
Total	517	out of	566
Views	0	out of	9
Categories	9	out of	49
Attack Patterns	508	out of	508

Fig. 6.6 CAPEC attack domains and mechanism (https://capec.mitre.org/index.html)

K0115: Knowledge of Emerging Computer-Based Technology That Has Potential for Exploitation by Adversaries

This is a very large generic knowledge area. Emerging computing-based technologies can vary from those in the cloud computing, smart or mobile phones, wireless, networking, a large spectrum of software, operating and information systems, Internet of Things (IoT), embedded systems, and many others.

For the least, to cover this knowledge area, readers should frequently visit and read vulnerabilities in public websites such as (https://cve.mitre.org/). CVE: Common vulnerabilities and exposures website is continuously updated with recent discoveries of vulnerabilities and exposures in different information systems, software, etc.

Other websites with similar goals include: https://www.securityfocus.com/vulnerabilities, http://seclists.org/bugtraq, etc.

K0312: Knowledge of Intelligence Principles, Policies, and Procedures Including Legal Authorities and Restrictions

Cyber Security Intelligence Principles

Several cyber security intelligence principles exist to guide the different public and private sectors. We will pick those described in (Information Technology Industry Council: ITI 2011)

1. Leverage public-private partnerships: With the large spectrum of possible threats and the huge amount of information (e.g., that can be collected through the Internet), regardless of the amount of resources and effort government can allocate to cyber security intelligence, this will not be enough, complete, or comprehensive. Different initiatives should exist to integrate intelligence from different sources using proper methods to ensure that information will reach intended audience within the right time.

2. Acknowledge some of cyber security intelligence challenges that have borderless, interconnected, and global nature of today's cyber environment. Attackers can exist anywhere in the world; they can be part of government sponsored agencies, private companies, or even individuals or amateurs.
3. There is a need to adapt, evolve, and respond quickly in this very changing environment. IT, as a general sector, evolves rapidly with many new and emerging techniques, environments, etc. Additionally, cyber security threats and techniques evolve rapidly as well.
4. Understand risk management and the different mitigation options and activities. Security cannot be complete or comprehensive, and what works well today may not work well tomorrow. What works well in some environment may not work well in another. While taking all possible security measures is important, nonetheless, risk should be assisted at different levels and mitigation alternatives should be always planned for.
5. The importance of security awareness: The human factor and dimension in any security framework will always be a key factor. Very strong security measures can be bypassed by tricking untrained or ignorant users. Training should consider and accommodate the different skills' levels of users. Training and awareness programs should be frequent and evaluate feedback from previous experiments to improve future training and awareness plans.

Cyber Security Act 2015

The Act establishes a mechanism for cyber security information sharing among private sector and federal government entities. It also provides protection from liability for private entities that share cyber security information in certain situations.

FISMA

The Federal Information Security Management Act (FISMA) was created to describe minimum controls required to protect federal information and information systems. It also provides a mechanism to improve federal agency information security programs.

Some experts believe that FISMA is not adequate to address federal network cyber security issues as it is mainly a reporting mechanism (Senkowski and Dawson 2009). Other reasons to believe the inefficiency of FISMA include: (1) the lack of widely accepted cyber security metrics, (2) the variations in agency interpretation of the mandates in the act, (3) insufficient means to enforce compliance both within and across agencies, etc. (Fischer 2014). FISMA was reformed in 2014 to tackle some of the earlier mentioned limitations.

Electronic Surveillance and FISA

Foreign Intelligence Surveillance Act (FISA) originally enacted in 1978 authorizes foreign intelligence surveillance activities that are seen as vital to keeping the US safe. It includes sections which concern targeting non-US persons1 abroad for surveillance and sections to provide statutory procedures and protections for surveillance of US persons abroad. "www.dni.gov". Under Title I of the Act, the government can file an application asking the Foreign Intelligence Surveillance Court (FISC) to authorize a foreign electronic surveillance of a facility based on a probable cause. This will eventually allow intelligence team to conduct electronic surveillance, trap and trace devices, or access specified records. CIAs differentiate between US persons and foreign nationals upon disseminations of FISA-acquired information.

The act is revised/updated in 2008 and 2012.

Intelligence Authorization Act

This act authorizes appropriations for intelligence and intelligence-related activities of the US government and authorizes funds for the intelligence and intelligence-related activities.

The Cyber Intelligence Sharing and Protection Act

This act focuses on information sharing (including classified information) and coordination between federal intelligence entities and private sector experts or providers of cyber security services. This includes, for example, information related to cyber threats or attacks.

Freedom of Information Act (FOIA)

This covers the protection from liability for entities sharing information (e.g., intelligence and law enforcement activities) and the exemption from disclosure of that information.

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)

This act discusses issues related to the collection, analysis, and sharing of security-related information.

K0315: Knowledge of the Principal Methods, Procedures, and Techniques of Gathering Information and Producing, Reporting, and Sharing Information

Public and private sectors should increase information sharing and work together in order to create new collaboration platforms and improve existing ones. The type and nature of information to share can vary from one threat type to another. Nonetheless, information sharing can fall in several categories such as those shown in Fig. 6.7 (Vez 2017).

Examples of more specific information to share (Vez 2017):

- Unusual network activity
- Login failures
- Denial of Service attack attempts
- Unusual privileged account user activity
- Counterfeited device identifiers
- Bad IP addresses, DNS attacks, etc. For example, the following websites keep tracking of Bad IP addresses, URLs, etc. for different types of attacks, Fig. 6.8 (https://github.com/stamparm/maltrail)

Attempts are also made to enhance information gathering and sharing using different methods or techniques such as:

- Protection from liabilities, consequences, or legal issues: We listed in an earlier KSA different Acts in the USA exist to protect security intelligence personnel from liabilities. However, careful consideration should be made to privacy issues,

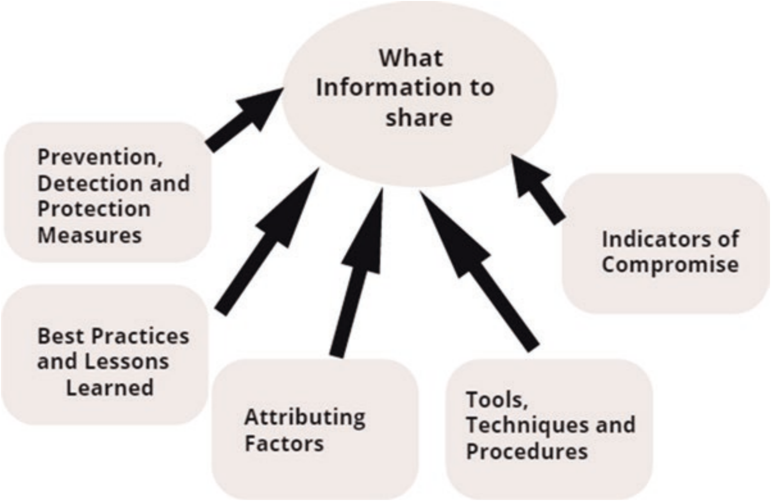
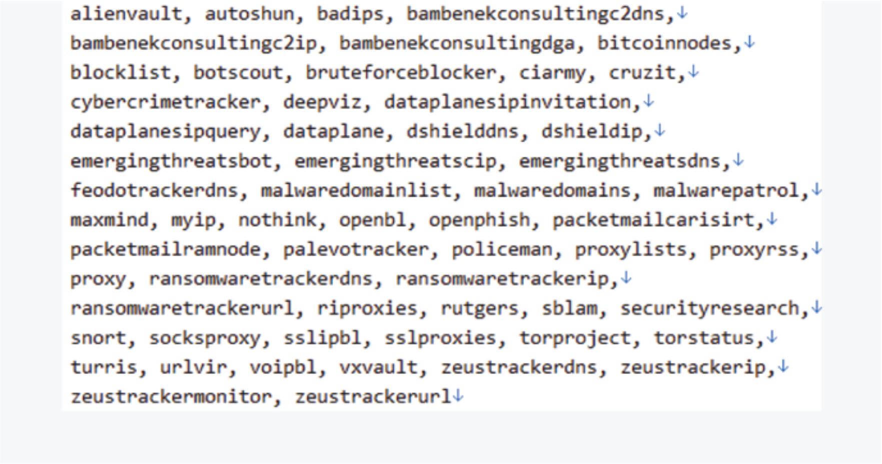

What Information to share
Prevention, Detection and Protection Measures
Best Practices and Lessons Learned
Attributing Factors
Tools, Techniques and Procedures
Indicators of Compromise

Fig. 6.7 Information sharing categories (Vez 2017)



```
alienvault, autoshun, badips, bambenekconsultingc2dns,↓
bambenekconsultingc2ip, bambenekconsultingdga, bitcoinnodes,↓
blocklist, botscout, bruteforceblocker, ciarmy, cruzit,↓
cybercrimetracker, deepviz, dataplanesipinvitation,↓
dataplanesipquery, dataplane, dshielddns, dshieldip,↓
emergingthreatsbot, emergingthreatscip, emergingthreatsdns,↓
feodotrackerdns, malwaredomainlist, malwaredomains, malwarepatrol,↓
maxmind, myip, nothink, openbl, openphish, packetmailcarisirt,↓
packetmailramnode, palevotracker, policeman, proxylists, proxyrss,↓
proxy, ransomwaretrackerdns, ransomwaretrackerip,↓
ransomwaretrackerurl, riproxies, rutgers, sblam, securityresearch,↓
snort, socksproxy, sslipbl, sslproxies, torproject, torstatus,↓
turris, urlvir, voipbl, vxvault, zeustrackerdns, zeustrackerip,↓
zeustrackermonitor, zeustrackerurl↓
```

Fig. 6.8 Websites that track bad IP addresses (https://github.com/stamparm/maltrail)

especially when no probable cause exists to encourage information gathering and sharing.

- Covert methods, channels, and personnel. Many security intelligence channels and personnel work under-cover to protect users' identities and also help them in the information gathering process.
- Encourage information sharing for such information that is not legally prohibited to share. Users may not be willing to share such information, especially when there are no obligations or incentives. Incentives and motivations should also be adopted to encourage two-way information sharing between public and private sectors.

Existing Efforts in Cyber Security Information Sharing

- Several efforts exist at national or organizational levels to integrate and coordinate cyber security intelligence and information sharing. Here are several examples:
- National Cybersecurity and Communications Integration Center (NCCIC): https://www.us-cert.gov/nccic.
- INTERPOL's Cyber Fusion Centre, Global Complex for Innovation (https://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation)
- European Joint Cybercrime Action Taskforce (J-CAT): https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce
- Cyber-security Information Sharing Partnership (CISP): https://www.ncsc.gov.uk/cisp

- National cyber security center: https://www.ncsc.gov.uk/threats
- Japan Cybercrime Control Center: https://www.jc3.or.jp/index.html
- National Cyber-Forensics and Training Alliance: https://www.ncfta.net
- Information Sharing and Analysis Organizations (ISAOs): https://www.dhs.gov/isao
- Information Sharing and Analysis Centers (ISACs): https://www.nationalisacs.org/, http://ctin.us/site/isaos/
- Retail Cyber Intelligence Sharing Center (http://www.r-cisc.org/

K0352: Knowledge of All Forms of Intelligence Support Needs, Topics, and Focus Areas

Cyber intelligence provides support to different elements in cyber defense infrastructure. Effective, correct, and timely intelligence is vital for all types of critical infrastructure threats' assessments, defense mechanisms, and security controls. Cyber intelligence provides also support planning, executing, and assessing of cyber operations.

Intelligence support includes supporting the two major tasks in intelligence: collection and dissemination. We described earlier the importance of having coordinated national or international efforts for both intelligence collection and dissemination tasks. This coordination can make the process more effective and responsive to take proper actions of impacted entities within the right time and actions.

For intelligence support, it is also important to evolve laws and regulations that can target a good balance between individual privacy rights and concerns along with national intelligence needs. The traditional requirements for search and warrants are impractical in the Internet, virtual, and online social networks' world. Many of the large IT companies such as Google and Facebook aggregate a huge volume of information about users, their activities, and behaviors. For pure business and marketing purposes, they already violate many privacy-related regulations. While this may not justify expanding such exposure to the intelligence community, nonetheless it shows the need to evolve laws and regulations in this area.

To proper conduct intelligence activities, intelligence requirements should be properly described and communicated. Intelligence information requester should clarify objectives and expectations and possibly also prioritize requirements (e.g., priority intelligence requirement (PIR)).

On the skills' need, cyber intelligence jobs require a mixture of skills that vary between technical (e.g., cyber security, IT, data science, and intelligence), behavioral or social (e.g., to understand humans' behavior, attackers), and communicational. The NICE framework was an attempt to acknowledge the need for cyber security education to evolve and expand beyond the classical one-for-all cyber security education that does not realize that cyber security jobs' market includes several work roles and specialty areas that may require different categories of KSAs.

K0354: Knowledge of All Relevant Reporting and Dissemination Procedures

K0355: Knowledge of All-Source Reporting and Dissemination Procedures

All-source intelligence information can come from any or all of the intelligence disciplines, including: SIGINT, HUMINT, IMINT, MASINT, OSINT, and GEOINT.

The Intelligence and Information Sharing and Dissemination Capability (IISDC)

IISDC is a national collaboration to the exchange and dissemination of information and intelligence among the different US government and private sectors and get the right information to the right/relevant audience within the right time. It does not only cover cyber security events only but all events that can result in public safety or security issues (DHS 2007).

Suspicious Activity Reporting (SAR) Process

SAR focuses on gathering information to detect and prevent criminal activities; domestic and international associated with terrorism or other criminal activities, Fig. 6.9.

NSA/CSS Policy 5-5, "Reporting of Security Incidents and Criminal Violations: August 2010"

Individuals who suspect an unauthorized disclosure of NSA/CSS information should report it in accordance with NSA/CSS Policy 5-5.

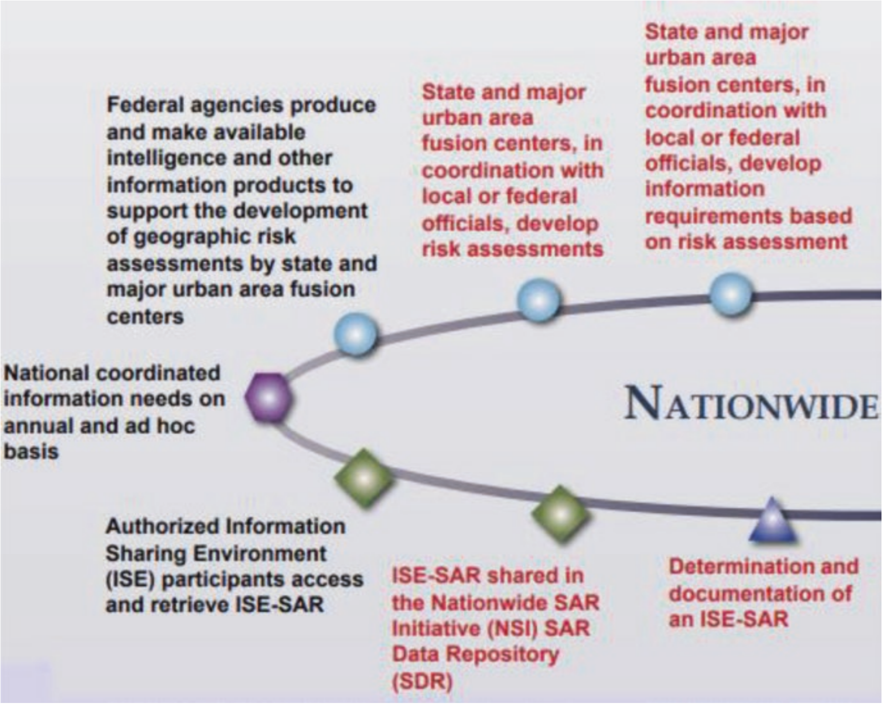

Federal agencies produce and make available intelligence and other information products to support the development of geographic risk assessments by state and major urban area fusion centers
State and major urban area fusion centers, in coordination with local or federal officials, develop risk assessments
State and major urban area fusion centers, in coordination with local or federal officials, develop information requirements based on risk assessment
National coordinated information needs on annual and ad hoc basis
NATIONWIDE
Authorized Information Sharing Environment (ISE) participants access and retrieve ISE-SAR
ISE-SAR shared in the Nationwide SAR Initiative (NSI) SAR Data Repository (SDR)
Determination and documentation of an ISE-SAR

Fig. 6.9 SAR components (NSI.NCIRC.GOV)

Interagency Threat Assessment and Coordination Group (ITACG) Intelligence Guide for First Responders

ITACG is designed to assist government entities and private sectors in accessing and understanding intelligence reporting. ITACG consists of responders and federal intelligence analysts from the DHS and FBI to enhance the sharing of intelligence information.

Unified Crime Reporting System

UCR Program is started in 1929 by the International Association of Chiefs of Police for those who are seeking **information** on crimes in the nation. UCR collects offense information for certain crime categories (e.g., murder, non-negligent manslaughter, rape, aggravated assault).

Production and Dissemination of Serialized Intelligence Reports Derived from Signals Intelligence

Intelligence reports can take one of three forms: raw, serialized, and special.

Raw intelligence (e.g., TDs, DIIRs, IIR, TACREPs, KLs, and CRs) is immediately reported by the collector and serves as the basis for other reports. Serialized intelligence reports focus on one aspect (e.g., time: daily, weekly, monthly, etc. reports) or by subject, geographic location, etc. Special intelligence reports are produced on request or as needed (e.g., National Intelligence Estimates). Both serialized and special reports are often referred to as FINTEL, i.e., processed or finished intelligence reports.

NSA FISA report (see also USSID SP0018 Reporting and Dissemination Team) is limited to an examination of the procedures and practices used to protect acquired US person information disseminated in serialized intelligence reports. By limiting the scope to serialized reports, NSA's privacy officer can avoid the two most problematic means of disseminating US person data: (1) by collecting it through obscured nodes (e.g., Tor) and (2) then deeming it evidence of a crime that can be disseminated in a raw form to FBI.

Intelligence Products Typically Available to First Responders (HSDL 2009)

1. Situational Awareness and Threat Reporting
2. Information Report
3. Intelligence Assessment (IA)
4. Threat Assessment (TA) or Special Assessment (SA)
5. Intelligence Bulletin (IB)
6. Joint Intelligence Assessment (IA) or Intelligence Bulletin (IB)

K0358: Knowledge of Analytical Standards and the Purpose of Intelligence Confidence Levels

In this scope, analytical standards are standards related to intelligence analysis and intelligence evaluation. Two particular events triggered reform in intelligence evaluation acts: 9/11 (lack of proper or enough linkage and coordination between intelligence collection and processing) and Iraq WMD (excessive information linkage and intelligence credibility issues).

DNI ICD 203: Analytic Standards (www.dni.gov)

The following security intelligence analytic standards are listed in DNI ICD 203 (https://www.dni.gov/files/documents/ICD/ICD203_Analytic_Standards.pdf): (Similar standards can be found in Intelligence Reform and Terrorism Prevention (IRTPA, 2004), SEC. 1019.).

- Objectivity: Analysis should not be biased to any human dimensions or factors. It should acknowledge different perspectives and views and not only focus on one narrow mindset.
- Independent of Political Consideration, against or with subject.
- Timeliness: Deliver the right actionable intelligence to the right intended audience on the right time to take proper actions.
- Comprehensive and not limited or narrow focus: Based on all available sources of data/intelligence.
- Exhibits Proper Standard of Analytic Tradecraft, specifically:
  - Properly describes quality and reliability of underlying sources
  - Properly caveats and expresses uncertainties or confidence in analytic
  - Properly distinguishes between underlying intelligence and analysts' assumptions and judgments
  - Incorporates alternative analysis where appropriate
  - Demonstrates relevance to US national security
  - Uses logical argumentation
  - Exhibits consistency of analysis over time
  - Makes accurate judgments and assessments

How Right and How Often? (Lowenthal 2008 and 2012)

An open-ended question in security intelligence analysis is related to the best formula of "how right to collect and disseminate intelligence and how often"?

Probably one of the main reasons why this question is complex and open is related to the fact that each intelligence requirement can have a unique content in terms of: goal, input variable, information sources, time, etc.

K0359: Knowledge of Approved Intelligence Dissemination Processes

Many articles showed some flaws in US intelligence dissemination in terms of, for example, timeliness, integration or coordination between public and private sectors, etc.

Intelligence reports, raw, specific, or serialized, can be delivered or dissemination in face-to-face meetings, structured reports, emails, etc.

Common Forms/Format of Dissemination

The most suitable form and format for intelligence dissemination depends mainly on the needs of the recipient, the urgency of the intelligence information, and the possible means to convey the information (e.g., verbal, electronic, messages, texts).

- Estimates: Intelligence estimates represent usually the first significant intelligence product developed to support initial orientation, and other planning needs.
- Briefings: The initial orientation brief should generally follow the estimate and presents the basic background intelligence.
- Studies: Intelligence studies deliver detailed intelligence on specific aspects of threats.
- Reports: A structured format for a possibly large range of audience.

K0386: Knowledge of Collection Management Tools

K0391: Knowledge of Collection Systems, Capabilities, and Processes

In intelligence collection management, the different activities related to collecting, processing, and reporting or disseminating intelligence collection from various sources are managed. One of the most popular collection management tools (CMTs) in the USA is Joint Collection Management Tools (JCMT), or also known as Collection Management Support Tools (CMST), from DOD Intelligence Information System (DODIIS).

Joint Collection Management Tools (JCMT) (globalsecurity.org)

JCMT is an all-source integrated collection management tool that provides tools for gathering, organizing, and tracking intelligence collection requirements. JCMT integrates the following legacy systems (globalsecurity.org):

- Army's Collection Management Support Tools (CMST)
- DIA's Collection Requirements Management Application (CRMA)
- UNIX-based National Exercise Support Terminal (UNEST)
- Southcom's Intelligence Support Processing Tool (ISPT)
- USAF National Air Intelligence Center's (NAIC) Collection Requirements Management System (CRMS)

ECHELON

ECHELON (also called or part of SHAMROCK and FROSTING programs) is another relatively old US intelligence collection program that started in the 1960s and integrated in some other programs by the year 2001.

UTT: Unified Targeting Tool

UTT is NSA web-based tasking tool (that replaces an earlier telephony targeting system OCTAVE in 2011). UTT was mentioned in NSA PRISM program (Fig. 6.10, Washington post 2013).

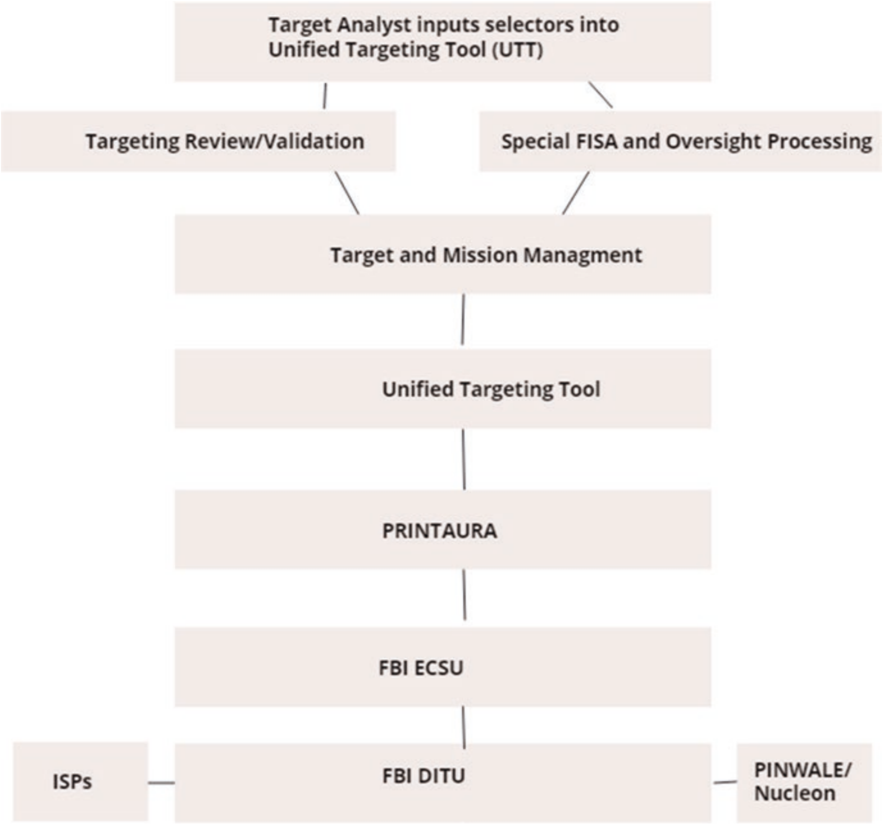

Target Analyst inputs selectors into Unified Targeting Tool (UTT)
Targeting Review/Validation
Special FISA and Oversight Processing
Target and Mission Managment
Unified Targeting Tool
PRINTAURA
FBI ECSU
ISPs
FBI DITU
PINWALE/ Nucleon

Fig. 6.10 PRISM tasking process (Washington post 2013)

NSA XKeyscore Program

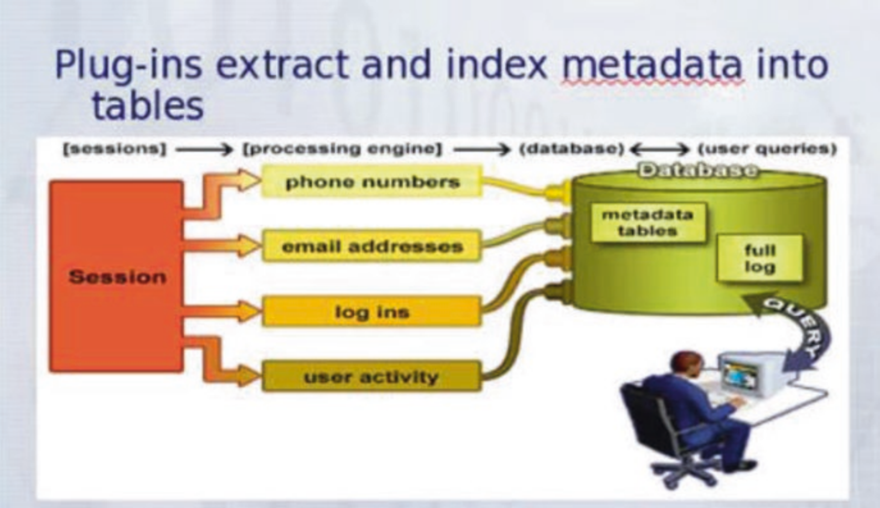
This is also a web-based tool that can collect public and private information (e.g., emails, chats) without the need for authentications. Majority of details on this program is not disclosed but claim the ability to collect a large amount of private information about persons of interests (including email contents, private chats, Internet search terms, Internet browsing history and activities, etc.), Fig. 6.11. Under FISA act, NSA is required to request a warrant if the person of interest is a US citizen.

PRISM Program

PRISM (also called SIGAD US-984XN), started in 2007, is a code name given to an NSA program related to collecting information from Internet and online social networks (Washington post 2013). List of target companies' databases include: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple.

Upstream

Upstream is collection of communications on fiber cables and infrastructure or as data travels on the backbone. Upstream has the following four major surveillance programs: FAIRVIEW, BLARNEY, STORMBREW, and OAKSTAR.



Plug-ins extract and index metadata into tables

Fig. 6.11 NSA XKeyscore (https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data)

Both upstream and PRSIM: downstream surveillance programs operate under Section 702; a law that relaxes constitutional and privacy safeguards under "targeting foreign surveillance."

Cadence

Cadence is a health-related collection management tool (https://www.terumobct.com/cadence). It includes cyber-attack features related to business intelligence collection and goals. It integrates collection management three major tasks: collection, analysis, and reporting.

WebTAS

WebTAS Enterprise (WE) is a suite of tools that supports the integration, visualization, analysis, and production of actionable intelligence across multiple data sources, user communities, and missions (https://www.issinc.com/webtas-enterprise). WebTAS STAKE's is developed for Combined Air and Space Operations (CAOC) ISRD collection management as well as other users in need of ISR support.

K0387: Knowledge of Collection Planning Process and Collection Plan

Collection planning should be guided by collection requirements with appropriate collection capabilities. The process can be evolutionary or adaptive to refine collection plans and strategies and enable the optimum collection capabilities to collection requirements. The plan should contain answers to the four main questions:

- What to collect?
- What collector?
- Where to collect?
- When to collect

Several factors should be considered when developing a collection plan (usacac.army.mil):

- Requirements for collection assets in subsequent missions
- Time available to develop information collection plan
- Insertion and extraction methods
- Reporting and communications plan
- The reconnaissance handover with higher or subordinate echelons

- The sustainment supports
- Legal support requirements

Collection plans should be adaptive; collection requirements may go through several updates to ensure that collection efforts are synchronized with current operations while also supporting future operations planning. The steps in updating the information collection plan are (Information collection: FAS.org 2012):

- Allocate assets to other collection requirements
- Eliminate satisfied requirements
- Develop and add new requirements or change existing ones
- Re-task and allocate assets

The overall ranking scheme for potential intelligence collections should be as follows (RAND 2008):

1. Priority of targets. Higher-priority targets will always be collected over lower ones.
2. Opportunities: Targets with fewer collection opportunities will be opportunities to collect before other targets.
3. Quality: Higher quality information will be collected over lower quality ones.

Internet-Based Collection Planning Process

- Determine collection and search requirements (e.g., PIRs)
- Decide best websites to use and also best search strategies
- Decide the level of information details
- Decide search time constraints

K0389: Knowledge of Collection Sources Including Conventional and Non-conventional Sources

A source can be an individual or group who works outside official status, not formally designed to gather or produce intelligence, but who can provide important information. Raw intelligence can be collected from sources vice security professional agencies.

In a previous section, we described all-source intelligence and the different categories of intelligence sources.

Collection sources can be different based on the different collection categories (e.g., HUMINT, SIGIN, OSINT) between strategic and tactical levels. For example, in HUMINT, the strategic level may look for sources that can provide information on opposing nations mobilization procedures, WMD capabilities, etc. At the tactical level, a potential source would be someone that can provide operational information that can indicate current environments or daily/weekly/monthly, etc. activities about the target or adversary.

SIGADs DNR and DNI Collection Sources

504 separate Internet data (DNI) and telephone metadata (DNR) collection sources were focused targets in NSA PRISM collection program. 2013 reports that showed that top five countries that were targets in this collection are: (1) Iran, 14 billion Boundless Informant reports, (2) Pakistan (13.5 billion), (3) Jordan (12.7 billion), (4) Egypt (7.6 billion), and (5) India (6.3 billion).

K0390: Knowledge of Collection Strategies

Cross-Intelligence Collection Strategies

Cross and all intelligence strategies focus on integrating strategies from different sources whenever necessary or required. That is very typical in most collection plans. Strategies should clarify how to collect, compile, and integrate information from those different sources and what to do in cases of contradictions or conflicts.

Collection strategies should be effective, diverse, and adaptive based on the nature of the current most hard to penetrate targets. Analysts should provide continuous feedback on the validity of collection requirements and resources. The collection process should balance between competing requirements of providing valuable, real time, relevant, comprehensive, etc. requirements.

Collection Coverage Plan

The scope of a collection process can be easily shifted due to the large number of possible sources to collect data from. In order to optimize project resources, it is important to keep project goals focused based on collection requirements or plans.

The complexity and details in the collection plan may vary based on the project scope and requirements. For a simple project, a collection plan can at least specify collection resources, intelligence requirements, or any specific details or constraints related to the collection process.

Collection plans should a balance between near-term goals that target collection requirements or plans and strategic collection strategies that consider evolution in targets, priorities, etc.

Strategic Intelligence

Strategic intelligence is "Intelligence that is required for the formulation of strategy, policy, and military plans and operations at national and theater levels" (CIA.gov).

From business perspectives, strategic intelligence collection should help organizations in future decision-making processes, policies, and ultimately organization success where it should help providing the correct information for the right people in the right time. Part of strategic intelligence is to provide abilities to predict future events and plan for them (e.g., disrupt adversaries or hackers attacking plans).

K0394: Knowledge of Common Reporting Databases and Tools

The term "common reporting" refers to security intelligence reporting mechanisms for security intelligence artifacts (e.g., intelligence, security vulnerabilities, malwares). They should contain the due diligence rules for the different participants to follow to collect and report the information for the automatic exchange of security-related information.

On the software applications' side, many information systems and applications include their own reporting tools and mechanisms.

IBM/Cognos analytics is an example of a business intelligence (BI) web-based analytic system with several reporting mechanisms (http://www.olspsanalytics.com/ibm-cognos/). They can target different types of users and industries. Most reporting is provided Tivoli common reporting. Cognos provides support for open architecture standards such as SOAP, WSDL, and XML. Tableau is another example of popular BI system with reporting and visualization tools.

Other examples of tools include: Microsoft SQL Server-based packages (SSIS and SSRS), Crystal Reports, MS Dynamics GP reporting, Power BI, Oracle reporting, and many others.

K0401: Knowledge of Criteria for Evaluating Collection Products

Security intelligence collection process should be able to product information that can fulfill initial requirements and goals. If requirements are met, then the process output can further feed the requirements to help develop new or deeper requirements that build upon the output intelligence product.

Security intelligence can be categorized into three levels based on vendors' products:

- Cyber threat intelligence
- Threat intelligence: A general category that includes cyber intelligence as well as other intelligence categories.
- Business risk intelligence: Supports not only cyber security but other business functions.

For known or popular intelligence collection tools, evaluation should consider historical records of those products. For example, evaluation should consider how many previous attacks such tools were able to intercept, mitigate, etc. Security intelligence collection tools have different models on how they deal with their known and unknown territories. As most tools may not be comprehensive and may not be able to intercept all possible types of their known attack types, or generally known attack types, we can use tools' behaviors with their unknown attack types as an important quality factor to consider and compare with. This is very important as most attack types will try to make themselves unique in some aspect to avoid detection.

Within the same range of cost, tools with abilities to detect more categories of attacks or threats are better. However, accuracy and timeliness should also be taken into considerations.

As an alternative, recommendation to readjust or realign the collection process is necessary where all or some activities will go through a second collection cycle. The cycle model can be used to establish what the problem was in the first cycle. Examples of such problems can be:

- Were the initial requirements unrealistic?
- Did the collection process use the wrong sources?
- Was the input data correctly contained within the sources but not drawn out properly during analysis?
- Did the final product meet the intelligence goals?

How do we evaluate the collection process or product? In most cases, they will have to be evaluated indirectly after the analysis stage (Fig. 6.12: MWR: Chismon and Ruks, 2015).

If the intelligence collection process was able to intercept, forecast an attack or whether the mitigations recommended by the threat or security intelligence process has mitigated or allowed the detection of particular attacks or mitigate an attack, then the collection process is a successful one. As such tasks are important goals behind most security intelligence activities, they can be used as important success measures as well. In more realistic assessments, especially when attackers use new or unknown attack methods, then it's unlikely that intelligence collection would have been able to provide intelligence to stop the attack. It should help understand the attack and be able to stop future similar ones.

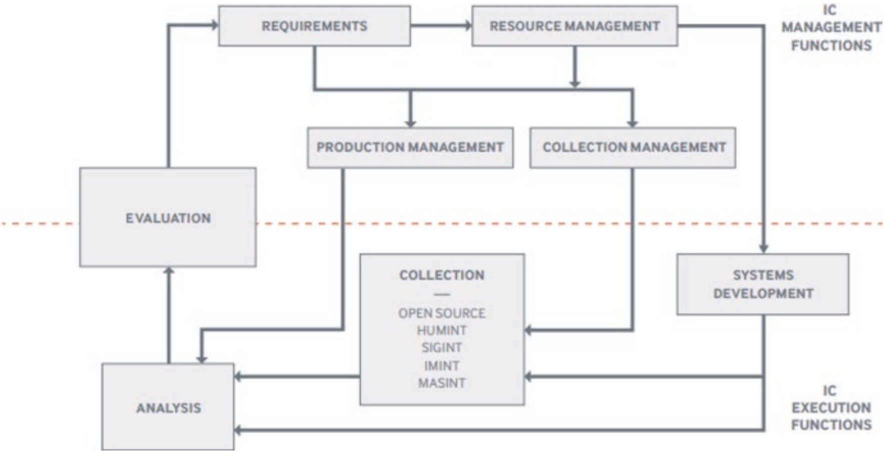


Fig. 6.12 Threat intelligence functional flow (MWR: Chismon and Ruks 2015)

Accuracy and Timeliness

For security intelligence collection products, accuracy and timeliness are key factors to evaluate those products. Accuracy of collected intelligence can be verified later on or through other sources of information that can help increase the credibility or collected intelligence.

Intelligence collection tools and products may face different collection challenges. For example, for privacy, copyright, or data ownership issues, collection tools may not be able to collect all required information (e.g., from deep and dark websites). Beyond the technical limitations, information collection regulations can also limit the ability to collect certain information.

The evaluation of intelligence collection products is a continuous process. The state of a good collection tool may not stay the same without continuous monitoring, tunings, and updates.

K0441: Knowledge of How Collection Requirements and Information Needs Are Translated, Tracked, and Prioritized Across the Extended Enterprise

In military intelligence collection, the requirements are translated into specific mission tasking orders issued to a commander with tactical control of the assets in question (Fig. 6.13: Joint Publication 2-01, 2017).

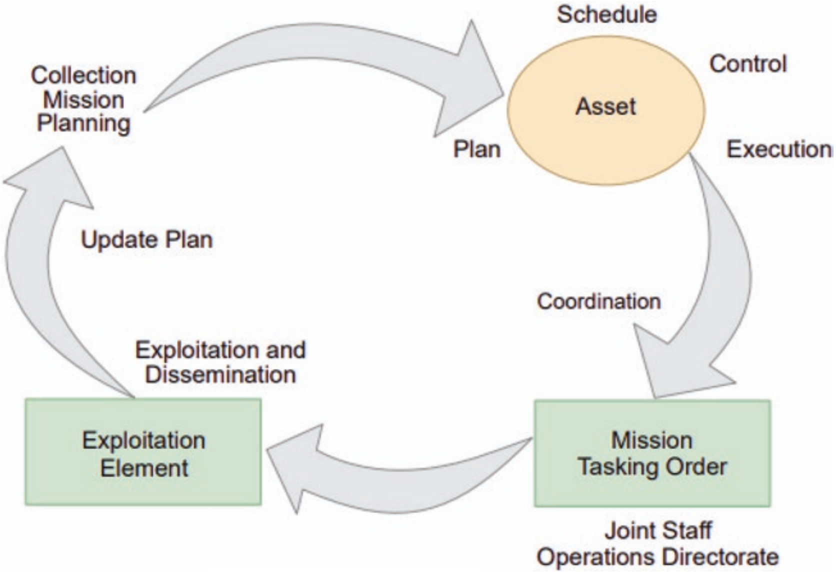


Fig. 6.13 Collection operation management (Joint Publication 2-01, 2017)

Actionable Knowledge

Intelligence information should be transformed into "actionable knowledge." In simple terms, actionable knowledge is the knowledge that is action oriented or that can be used to: directly or indirectly help in decision-making.

In the typical data/information pyramid, data is at the first layer, large in volume, less in value, then (2) Information, (3) Knowledge, and (4) Experience; with less in volume and more in value. While most information systems will produce knowledge, that is eventually actionable, require/advice certain actions, the term "actionable knowledge" is used in some information systems and data analytics to focus knowledge goals. In security controls for example in general, actionable knowledge can be seen in the policies and high-level rules that control the actions of the security controls. This is the difference for example between a network monitoring tool such as Wireshark, that can produce data, information, and even possibly knowledge, but not an actionable knowledge as in Snort or an IDS/IPS system where actions (e.g., permit, deny, etc. traffic) are based on knowledge about that traffic. Monitoring tools can collect data/information and "advice" on certain actions. However, there is a need for human analysts who can analyze generated data and take actions to a system that is actionable (e.g., a firewall).

The term "knowledge" is not symmetric when it comes to different problem domains, threats, collection requirements, etc. The variation can be both at the level of details and complexity. “Actionable knowledge” can also vary in level of details and complexity. A simple action by a firewall or an IDS/IPS to block suspicious traffic can be considered “actionable knowledge.” On the other hand, new security or policy requirements to enforce certain regulations/constraints on passwords can also be considered as “actionable knowledge” taken based on several security incidents, activities, collected data, information, etc.

Additionally, in some cases, it is possible to automate knowledge extraction or production while in some other cases, data/information should be aggregated from different sources to be able to produce the required knowledge.

It is important to differentiate “actionable knowledge” from those simple and low-level security rules, access control lists, etc. that can be seen in firewalls, routers, switches, etc. Such rules are actionable but cannot be considered as knowledge. For example, a firewall that can block traffic based on source or destination: IP, MAC addresses, port numbers, or protocols can take those actions based on “primitive data variables” that are collected directly from network traffic.

Autonomous Security Controls

Ideally, we are eager to have autonomous security controls that can monitor networks for possible malicious or abnormal behaviors and eventually create their own “actionable knowledge” based on that historical and real-time traffic monitoring to accommodate our network and systems’ threats.

Many vendors claim to have systems that are capable to be autonomous security controls. The validity of such claims may need to be clarified and compared with the “actionable knowledge” that their systems can provide. In other words, while some systems are capable of providing “low level” categories of actionable knowledge for specific or categories of abnormal or malicious attacks, no system can realistically claim to provide more complex types of actionable knowledge to a large spectrum of possible threats.

K0456: Knowledge of Intelligence Capabilities and Limitations

It is important for intelligence users to understand each intelligence system or tool capabilities and limitations; what they can and what they cannot do. This will help saving time and resources through all the security intelligence lifecycle through optimizing the usage of those resources and setting the right expectations.

Intelligence Capabilities

Intelligence systems/tools can help in one or more of the following tasks (ITACG 2011):

- Support in the decision-making process (long and short term). This is a major goal in all information and intelligence collection activities. Current decision-making processes require support of information and intelligence at different level of details and sources. The quality and timeliness of the right information can be an invaluable asset to any decision support system.
- Long- and short-term alerts of potential threats. This is also another major goal for most of security intelligence collection and monitoring activities. The types and natures of alerts that intelligence systems can provide should be communicated properly between intelligence providers and consumers to make sure they are on the same levels of expectations. For example, an intelligence collection system can fall from the "can" to the "can't" based on the threat alert level of details, accuracy, timeliness, etc.
- News alerts. Decision-makers may need to be summarized on certain types/categories of news that are happening in some countries, industries, user groups, etc.
- Security and situational awareness. In addition to news' alerts that are directed to a limited category of audience (e.g., decision-makers), security awareness programs target a larger category of audience. For example, recently, phishing attacks (through emails, SMS messages, etc.) showed significant increase in volumes. This triggers many US organizations to conduct security awareness programs to inform employees of how to best deal with such security threats.
- Reports on specific topics: For example, a crime or incident, local, national, or international, may trigger different types of security intelligence collection and analysis activities (See digital forensics, malware analysis, etc.).
- Persons of interest (PoI) intelligence collection. This can be strategic, long term, ongoing based on certain profiles, or can be targeted based on specific national or international incidents.

Intelligence Limitations

Different types of limitations can be discussed about intelligence systems. One important aspect in this regard is to understand each system limitations and communicate such limitations properly with intelligence collection, analysis, and usage teams. For different reasons (e.g., job security, system acquisition problems), miscommunication between those different teams will eventually different types of problems.

Predictive vs Prescriptive Analytics

Intelligence limitations are affected by intelligence collection and analysis challenges. One of the main intelligence challenges is that in many cases expectations are not clear. In other words, evaluating the accuracy and success measures on the intelligence collection and analysis is not trivial. We described, for example, one simple success factor, for most security intelligence systems; the ability to successfully detect/mitigate all security threats. Clearly this is simple to say and unrealistic to expect. The security intelligence process is a continuous and evolutionary process, we continuously learn from the past to improve future responses.

The ability to alert and mitigate for future security threats can be seen as part of a larger scope (the ability to predict future events or activities). Some collection activities target predictive analytics, rather than intelligence.

Intelligence in most of the tasks we described earlier is considered as "Prescriptive analytics": What happened in the past and what is happening now. Predictive analytics (PA) focus on predicting what will happen in the future. Intelligence and PA complements each other; the best models of PA are those who are built on rich levels or prescriptive analytics.

Predicting future events face limitations related to the accuracy of the prediction. We collect certain variables related to those events and in our prediction models, we assume, for practical reasons that only those variables will impact the occurrence of such events. A typical PA model will have a "target, class, label" variable and a number of "predictor" variables. We typically include predictor variables that we can collect. In reality, in most cases, we will have missing variables; variables that influence the occurrence of those events that we can't collect data about, or we can with very low accuracy.

K0457: Knowledge of Intelligence Confidence Levels

Intelligence collection and analysis activities produce results tied with accuracy or confidence levels. Intelligence audience should not look at the intelligence information while ignore its accuracy. Rumors may convey important, serious, or valuable information, but with very low accuracy and hence significance. Intelligence can vary from "facts: with very high confidence" to "rumors, or assumptions: with very low confidence."

Data analysis algorithms (e.g., clustering, classification, prediction) produce different types of performance measures or metrics (e.g., confusion matrix, area under curve, AUC, F-measure, root mean square error, RMSE). For data analytics, it is very important to study all relevant performance metrics to an analytic activity, their implications, meanings, interpretations, etc.

For intelligence users, trying to study and understand such metrics can be very time-consuming and confusing. Hence, it is the job of intelligence collection and analysis teams to create accuracy or confidence levels that are more readable or easier to interpret and understand by users who are typically with no technical background/skills. For example, accuracy of intelligence collection or analysis results can be summarized into three confidence levels:

- **High confidence**. Some aspects that support this selection:
  - Intelligence is correlated from more than one source
  - Intelligence is correlated from more than one system/tool
  - Source of information is trustworthy (e.g., based on previous intelligence)
  - Minimum assumptions and strong logical reasoning/inference
- **Medium confidence.** Some aspects that support this selection:
  - Intelligence is partially collaborated from more than one source.
  - Intelligence source or system is partially tested or has previous accepted levels of confidence.
  - Low contradictions, assumptions, etc.
- **Low confidence**. Some aspects that support this selection:
  - Intelligence system or source is new, unverified, etc.
  - Several assumptions and/or contradictions exist
  - Intelligence comes from difference sources with conflicting information.

Such three levels' categorization of the accuracy makes the assessment simple for users or decision-makers while at the same time help them always correlate intelligence with accuracy or confidence levels. As confidence levels indicate probabilities, a continuous percentage range (i.e., from 100 to 0%) can be used where 100% indicates top or absolute confidence and 0% indicates no confidence. Percentage confidence can also be converted to ranges (e.g., >90% highly likely, 60–90% probable, and 40–60% possible)

It is important as part of showing the right confidence level is to use the right terms when expressing intelligence information. Here is a list of possible terms to use in each level:

- **High confidence**: Certainly, most likely, etc.
- **Medium confidence**: Likely, probably, etc.
- **Low confidence**: Possibly, may or may not, etc.

Different levels of confidence can also be associated to different components of the same intelligence case. Each statement or information can be given its own confidence level and then the overall intelligence case can be given one unified confidence level.

K0459: Knowledge of Intelligence Employment Requirements (i.e., Logistical, Communications Support, Maneuverability, Legal Restrictions)

Working for government intelligence agencies requires special background investigations and security clearance; eligibility for access to classified information. The process considers many factors when granting security clearances, such as: citizenship, loyalty, drug use, personal integrity and conduct, and medical fitness. The subject person can be subjected to different types of investigations (https://fas.org):

- NACLC (National Agency Check with Local Agency Check and Credit Check)
- SSBI—Single Scope Background Investigation
- SSBI-PR—SSBI Periodic Reinvestigation

Other examples of clearance investigations include: ANACI (Advance National Agency Check with Inquiries, only used for civilian employees), MBI—(Moderate Risk Background Investigation), T3, T5, T3R, or T5R.

Security clearance levels can indicate one of the two: (1) Level of access to sensitive information or (2) level of investigations conducted on the person requesting or holding the clearance. In the USA, there are some general security clearance levels as well as departmental (e.g., DoD, DoE, DoJ) clearance levels and terms. Here is one example of general security clearance levels:

- **Top Secret Clearance**, also Top Secret/Sensitive Compartmented Information (TS/SCI). This level will be reinvestigated after 5 years.
- **Secret Clearance**: This level will be reinvestigated after 10 years.
- **Confidential Clearance**: This level will be reinvestigated after 15 years.

K0460: Knowledge of Intelligence Preparation of the Environment and Similar Processes

Intelligence preparation of the environment: IPE is one of the intelligence analysis methods. IPE tries to analyze the environment and threats using graphical means with the goal of introducing useful information to decision-makers. More specifically, the goal is to determine and evaluate the threats or targeted force’s capabilities, intentions, and vulnerabilities. IPE tries also to predict future events/threats through a process of deductions.

Other related terms or activities include: Intelligence preparation of the battlefield or the battlespace (IPB) and intelligence preparation of the operational environment (IPOE). Two significant characters in this method are its flexibility in terms of support for change whenever required and its focus on the location dimension where a major goal in this analysis is to “Go” or “No-go” to a specific target area.

Geospatial IPOE includes four steps (https://www.nga.mil):

1. **Define the Environment**: This step includes gathering basic information needed to outline the exact location of the mission or area of interest.
2. **Describe Influences of the Environment**: For the area of interest from the first step, next provide descriptive information. Consider all details that may affect a potential operation in the area: weather, vegetation, roads, facilities, population, languages, social, ethnic, religious, and political factors.
3. **Assess Threats and Hazards**: For the area of interest, add intelligence and threat data, drawn from multiple intelligence disciplines.
4. **Develop Analytic Conclusions**: Integrate all information to develop analytic conclusions such as adversary's courses of actions; COA.

K0461: Knowledge of Intelligence Production Processes

The intelligence production process includes the following major stages or activities:

- Tasking: This step starts the intelligence activity. It is triggered by an event or order from decision-makers. The input to this task includes initial requirements and collection or analysis goal.
- Researching: Intelligence process starts with initial researching and investigation based on early requirements. This may trigger further sub-cycles, between researching and tasking to verify requirements with intelligence requestor.
- Processing: This is the main and typically most time-consuming task. This task can also be part of a cycle: Tasking-researching-processing, where collected data may trigger frequent queries or clarifications.
- Reporting: Typically, standard reporting procedures exist (e.g., intelligence information report; IIR). Reporting can be responsive, one time in response to a specific request or can be periodic.
- Dissemination: This is the final task to disseminate collected intelligence to requesters or specific intended audience.

K0462: Knowledge of Intelligence Reporting Principles, Policies, Procedures, and Vehicles, Including Report Formats, Report-Ability Criteria (Requirements and Priorities), Dissemination Practices, and Legal Authorities and Restrictions

Intelligence reporting evolves recently to ensure that proper communication in terms of intelligence in general and reporting procedures and formats in particular exists between the different national intelligence agencies. Intelligence that is received or intercepted by one agency should be made available to proper audience in all other agencies within the right time and format.

One major issue in the recent intelligence reporting evolution is related to the speed of reporting and dissemination. In many cases, there was a need to reduce the dissemination time that used to be slower due to some government bureaucratic regulations. For example, FBI enables starting 2009–2010 Intelligence Information Reports (IIRs) to be directly disseminated to all intelligence agents. Thorough reports such as analytic intelligence reports are still centralized and will only be reported through FBI headquarters.

Examples of Intelligence Reporting Formats

- Periodicals: Daily, weekly, or monthly operational reports. For routine intelligence activities, reports are submitted based on known templates on specific periods. Certain events may trigger exceptional reports.
- Intelligence summaries: Incidents, visits, certain events, may trigger special intelligence summary reports to be created.
- Intelligence Information Reports (IIRs).
- Operational narratives: Different intelligence and military activities require their own operational reports based on the targeted missions.
- Intelligence analysis fusion: Developed by operational and theater level security intelligence staff.
- Field and Daily Field Intelligence Report (DFIR).
- The Defense Intelligence Report (DIR)

Intelligence information, by definition and default involves private or secret information that is not available for public or acquired from public sources. Nonetheless, cases may exist where information acquired from public or open sources is valuable/new from the perspectives of intelligence agencies. Other examples that may indicate public information with intelligence values:

- Information that was posted through the Internet and then removed.
- Printed or oral information.
- Information that was exchanged through proprietary or unpopular applications or languages.
- Information that is different from what is reported publicly.
- Information is available only through the dark or deep web.

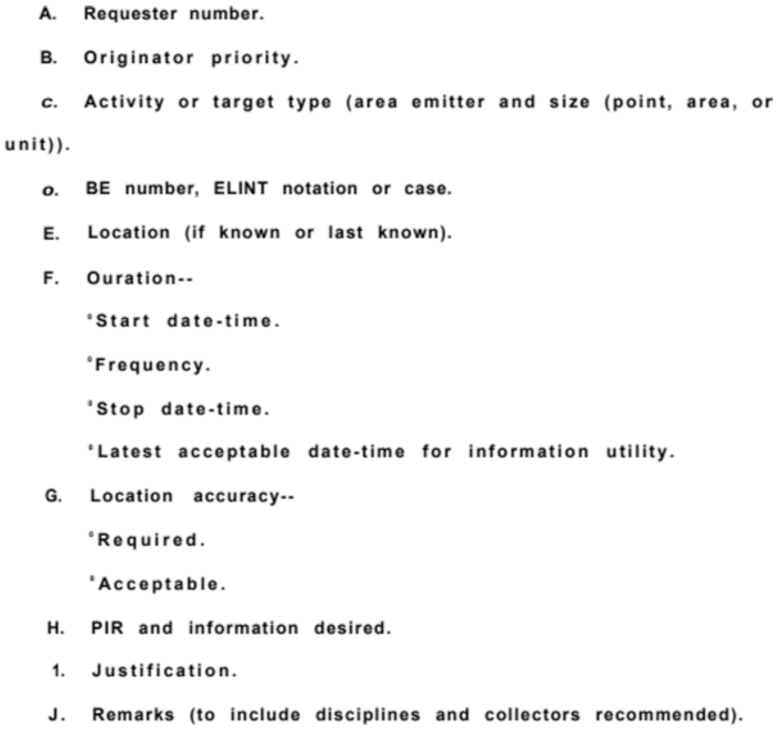
Intelligence is typically disseminated to security decision-makers, intelligence requesters, etc. However, there are cases where adversaries can also be targeted by certain types of information and intelligence.

K0463: Knowledge of Intelligence Requirements Tasking Systems

The goal of intelligence requirements' tasking systems is to provide specific requirements, to create realistic assessments of potential threats and exploits. This system focuses on providing the requirements rather than the instructions to the intelligence team.

Standard Collection Asset Request Format (SCARF)

The standard collection asset request format (SCARF) is used in intelligence requirements tasking. It can also be used to communicate and request information from other departments or agencies, Fig. 6.14.



A. Requester number.

B. Originator priority.

c. Activity or target type (area emitter and size (point, area, or unit)).

o. BE number, ELINT notation or case.

E. Location (if known or last known).

F. Ouration--

°Start date-time.

°Frequency.

°Stop date-time.

°Latest acceptable date-time for information utility.

G. Location accuracy--

°Required.

°Acceptable.

H. PIR and information desired.

1. Justification.

J. Remarks (to include disciplines and collectors recommended).

Fig. 6.14 SCARF format: (FM 34-3-1990)

National Human Intelligence Requirements Tasking Center (NHRTC)

NHRTC is the CIA's National HUMINT Requirements Tasking Center that manage requirements through NHCD. National Human Collection Directives (NHCDs) is developed by NHRTC with major focused on human intelligence collection, requirements, policies, and programs. This requirement system is designed to be active that can change frequently and also community driven. The system is capable of accomplishing intelligence tasks such as: (Lowenthal and Clark 2016):

- Collection accountability
- Standard reporting formats
- Feedback to users
- Retain flexibility to meet urgent needs

K0464 Knowledge of Intelligence Support to Planning, Execution, and Assessment

Security intelligence can provide support to different types of activities where such knowledge or intelligence is one of the key inputs in making decisions. For example, intelligence can support targeting through services such as: target system analysis, audience analysis, and target recommendation. The form and degree of intelligence support can vary from one function to another from full time to periodic or ad hoc intelligence support or products.

For planning, and as one of the key goals of intelligence is to reduce uncertainty and improve our decisions or future actions, intelligence support to planning is highly desirable (Fig. 6.15).

For the different planning activities, intelligence can provide support accordingly (MCC guidebook 2014).

- The analysis of adversary situation: Intelligence can provide analysis about the impact of the operational environment on adversary capabilities and possible courses of actions.
- Evaluating adversary capabilities: Creating and analyzing adversary models, situations, capabilities, etc.
- COA development: Identify adversary possible courses of actions (COAs), evaluate and prioritize those actions.

An operation execution involves stages such as deployment, redeployment, and mobilization. Security intelligence can provide different types of support for execution activities. Examples of such support include:

- Provide situational awareness on the adversary, operation environment, etc.

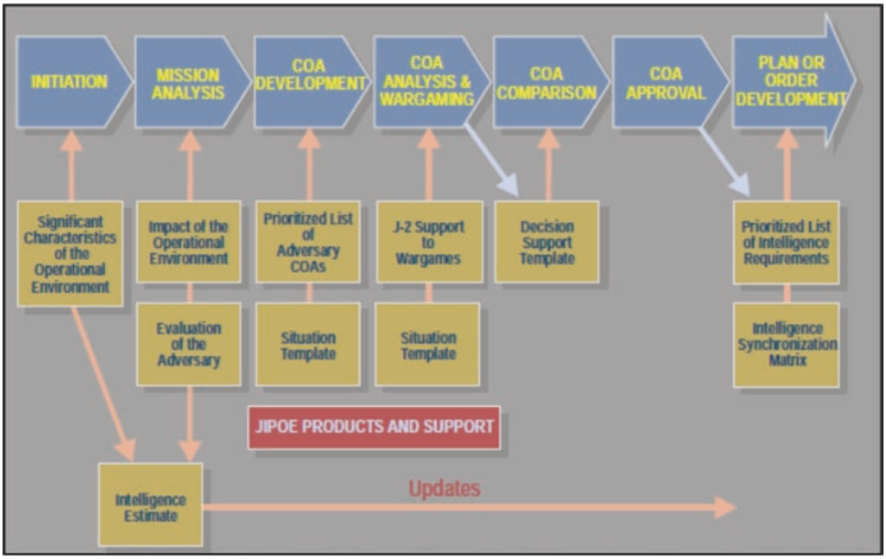

INITIATION
MISSION ANALYSIS
COA DEVELOPMENT
COA ANALYSIS & WARGAMING
COA COMPARISON
COA APPROVAL
PLAN OR ORDER DEVELOPMENT
Significant Characteristics of the Operational Environment
Impact of the Operational Environment
Prioritized List of Adversary COAs
J-2 Support to Wargames
Decision Support Template
Prioritized List of Intelligence Requirements
Evaluation of the Adversary
Situation Template
Situation Template
Intelligence Synchronization Matrix
JIPOE PRODUCTS AND SUPPORT
Intelligence Estimate
Updates

Fig. 6.15 An example of intelligence support to planning (MCC guidebook 2014)

Table 6.1 A sample model for intelligence support for execution phases (DoD Joint publication 2-0, 2013)

Execution phase	Intelligence action
Shape	Prepare and prevent
Deter	Crisis defined
Seize the initiative	Assure friendly freedom of action Access theater infrastructure
Dominate	Establish dominant force capabilities Achieve enemy culmination or joint force commander's favorable conditions for transition
Stabilize	Establish security restore services
Enable civil authority	Transfer to civil authorities, redeploy

- Current status of adversary or foreign transportation and communication infrastructure.
- Protection measures to combat operation-related incidents, injuries, etc.

Table 6.1 shows a model for execution phases along with intelligence support for each phase (DoD Joint publication 2-0, 2013). One difference in terms of intelligence support to planning and execution phases is that in execution phases, typically time to support intelligence is shorter and sensitive (e.g., in hours, rather than days, weeks). Additionally, the amount of information and target are more focused (e.g., more intelligence requirements and more details).

K0484: Knowledge of Midpoint Collection (Process, Objectives, Organization, Targets, etc.)

Midpoint collection is one of the desired collection capabilities for intelligence collection systems. Midpoint collection processes try to intercept and eavesdrop on the different types of communication links. Midpoint collection is a covert form of SIGINT which enables passive/continuous listening on communication channels using virtual or physical access techniques. Collected data is sent directly to midpoint collection points. In comparison with endpoint collection activities that try to collect intelligence from endpoints (e.g., computers, servers, databases, etc. data at rest), midpoint collection focuses on the communication channels (i.e., data in transit).

As part of a large acquisition system (ValiantEagle), GENIE project is adopted by NSA Computer Network Operations (CNO) program to conduct endpoint operations to implement midpoint programs.

Intelligence organizations may also use Internet Service Providers (ISPs) as backbone midpoints for large data collections. Encryption and routing algorithms may create challenges for such large-scale collection or interception schemes.

K0492: Knowledge of Non-traditional Collection Methodologies

Non-traditional collection methodologies may use means or sources different from those described earlier for intelligence collection. For example, personnel from outside the intelligence field or the traditional intelligence organizations can provide sensitive or valuable information. Given that such individuals are not from the intelligence-related fields and are not trained or professional in collecting intelligence information, they (1) may not understand or realize the value of the information, (2) may not be willing to share such information, or (3) lack the proper channel to do so. Espionage can be seen as another example of this type of non-traditional collection methods. In espionage, companies or countries use experts in some fields to spy on other companies or countries for the use and transfer of intelligence and technologies (e.g., see Brown 2009).

Non-traditional collection may refer also to the nature of the collection information as being non-traditional intelligence information. Such information may not have direct intelligence implications or values. Data aggregated and processed from different sources may show unprecedented values when compared with isolated pieces of information.

In another form of non-traditional collection, traditional collection methods or tools may be utilized or used in a different way.

Between traditional and non-traditional collection methodologies, different intelligence experts may have different perspectives. For example, while intelligence collection methods such as: IMINT, SIGINT, HUMINT are traditional, to many MASINT is less traditional and may include non-traditional components such as real-time situation awareness.

K0514: Knowledge of Organizational Structures and Associated Intelligence Capabilities

Organizations who collect and utilize intelligence capabilities may have different organizational structures. For intelligence organizations, the ultimate goal of intelligence collection is to match target threats, to be able to deal with them.

As cyber threats continuously evolve and as attackers continuously change their tactics, intelligence organizational structure should be flexible to support such agility. There are some factors in the organization structure that can significantly impact its intelligence capabilities such as:

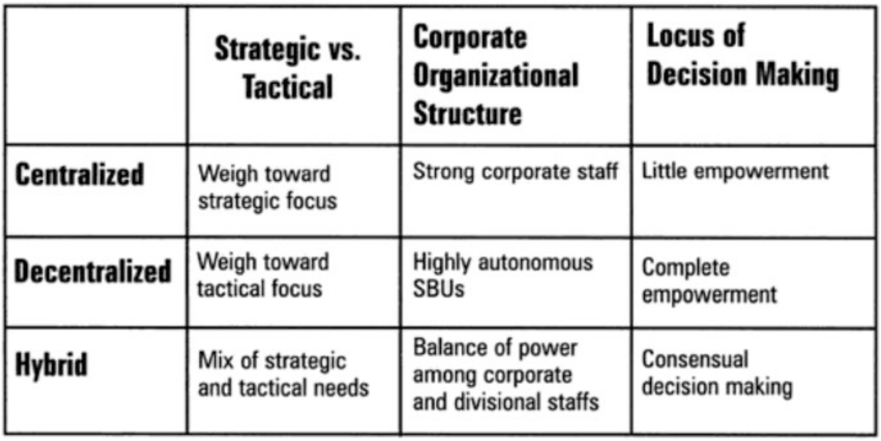
- Strategic vs tactical intelligence capabilities. For example, tactical intelligence should highly consider timeliness of information collection and hence be supported by decentralized organizational structure in comparison with strategic intelligence and centralized architectures.
- Locus of decision-making: In connection with centralized and decentralized architectures, effective operational intelligence requires organizations with distributed powers among the different hierarchical levels. Available/acceptable communication channels can also impact the timeliness of intelligence collection and dissemination.
- Integration of intelligence and operation: Short decision cycles require closer integration between intelligence collection and dissemination or operations taken based on the intelligence (Barger 2005).
- Skills' coordination between the different organization members in order to integrate and utilize existing technologies with intelligence. The goal is to produce timely intelligence products that are mission or goal focused.
- The ability to adopt new tools, or technologies to optimize intelligence collection and usage.

Figure 6.16 shows a chart of balance between organizational structure types and support for intelligence capabilities (Miller 1999):

K0544: Knowledge of Target Intelligence Gathering and Operational Preparation Techniques and Lifecycles

Intelligence gathering activities identify key targets, their infrastructure, personnel, assets, etc. to locate information in them that can be useful and relevant. Intelligence gathering can utilize the different traditional all-source intelligence and non-traditional intelligence collection areas that we described earlier.

Operational preparation of the environment (OPE) is the range of activities that can facilitate future combat operations (Kenny 2006). Such activities can help military "know the target area" before conducting military operations. Those are usually traditional intelligence military activities that are not part of intelligence functions



	Strategic vs. Tactical	Corporate Organizational Structure	Locus of Decision Making
Centralized	Weigh toward strategic focus	Strong corporate staff	Little empowerment
Decentralized	Weigh toward tactical focus	Highly autonomous SBUs	Complete empowerment
Hybrid	Mix of strategic and tactical needs	Balance of power among corporate and divisional staffs	Consensual decision making

Fig. 6.16 Organizational structure vs intelligence capabilities (Miller 1999)

Table 6.2 Examples of operational preparation activities (Keys 2005)

Reconnaissance and surveillance
Weather operations
Airfield surveys and assessments
Navigation and positioning
Command and control (C2) battle management
Air traffic control and assault zone marking
Terminal attack control
Time-sensitive weaponizing and targeting
Combat search and rescue
Field trauma care
Information operations

or activities from intelligence agencies (e.g., CIA, NSA), Table 6.2 (Keys 2005). The term "OPE" itself is evolved from the term "Operational Preparation of the Battlespace" (OPB). OPE includes three major components (Kenny 2006, Kuyers 2013):

1. Orientation activities such as: situational awareness, surveys and assessments, and knowledge of the quickest routes
2. Target development activities such as: persistent surveillance, overt and covert engagement with host state counterparts and cultivating relationships with members of host state society
3. Preliminary engagement activities such as: terminal guidance and small-scale direct action

Joint Publication 3-13 (Information operation, DoD-JP 2012) defines OPE as "non-intelligence activities conducted to plan and prepare for potential follow-on military operations" under Title 10 authority.

K0577: Knowledge of the Intelligence Frameworks, Processes, and Related Systems

Table 6.3 below shows a list of popular cyber threat intelligence frameworks or standards to describe, aggregate, and exchange cyber threats. A sample of those will be covered below with few details.

Open Indicators of Compromise (OpenIOC) Framework

Indicators of compromise (IOCs), introduced first in 2011 (OpenIOC, 2011), indicate possible evidence (that exist in the network traffic, files, hashes, registry keys, Dynamic link libraries (DLLs), Mutual exclusion (mutex), etc.) that can identify potentially malicious activity on a system or a network. They can help detecting data breaches, malware infections, or other security threat activities. IOCs are examples of actional types of cyber threat intelligence (CTI). In comparison with anti-malware systems, using IOC methods can help us look at the symptoms or indicators of malicious activities rather than on their outputs or payloads. IOCs can help answering details about how attacks and malwares occurred. Table 6.4 shows

Table 6.3 A sample of cyber threat frameworks and standards

OpenIOC—Open Indicators of Compromise framework
VERIS—Vocabulary for Event Recording and Incident Sharing
CybOX—Cyber Observable eXpression
IODEF—Incident Object Description and Exchange Format
TAXII—Trusted Automated eXchange of Indicator Information
MITRE Common Vulnerabilities and Exposures (CVE)
STIX—Structured threat Information Expression
MILE—Managed Incident Lightweight Exchange
TLP—Traffic Light Protocol
OTX—Open Threat Exchange
CIF—Collective Intelligence Framework

Table 6.4 Examples of IOCs (Chickowski 2013)

Unusual outbound network traffic	Mismatched port-application traffic
Anomalies in privileged user account activity	Suspicious registry or system file changes
Geographical irregularities	Unusual DNS requests
Log-in red flags	Unexpected patching of systems
Increases in database read volume	Mobile device profile changes
HTML response sizes	Bundles of data in the wrong place
Large numbers of requests for the same file	Web traffic with unhuman behavior
Signs of DDoS activity	

examples of IOCs (Chickowski 2013). Similar to IOCs, indicators of attack focus on identifying attacker activity while an attack is in process.

Public repositories such as: MISP and Virustotal can be used to extract historical network and file-based IOCs. Many open source tools such as Loki (https://github.com/Neo23x0/Loki) can be used to extract IOCs from public repositories and test systems where they are victims of such IOCs or not. The knowledge of IOCs can help security experts understand malwares and design mechanisms to defense system from future similar threats. They can also be used for threats' triage and remediation. IOC supports different formats related to OpenIOC, TAXII, STIX, CybOX, Yara, IETF, Tardis, etc (Fig. 6.17).

Collective Intelligence Framework (CIF)

Collective Intelligence Framework (CIF) is developed by REN-ISAC (https://csirt-gadgets.com/collective-intelligence-framework). It allows to combine known malicious information from many sources and use such information for incident response, IDS\IPS, or mitigation. One of the main goals of CIF and similar frameworks is to create a unified structure that can allow security analysts to aggregate, integrate, or exchange information about the different malicious threats. CIF can

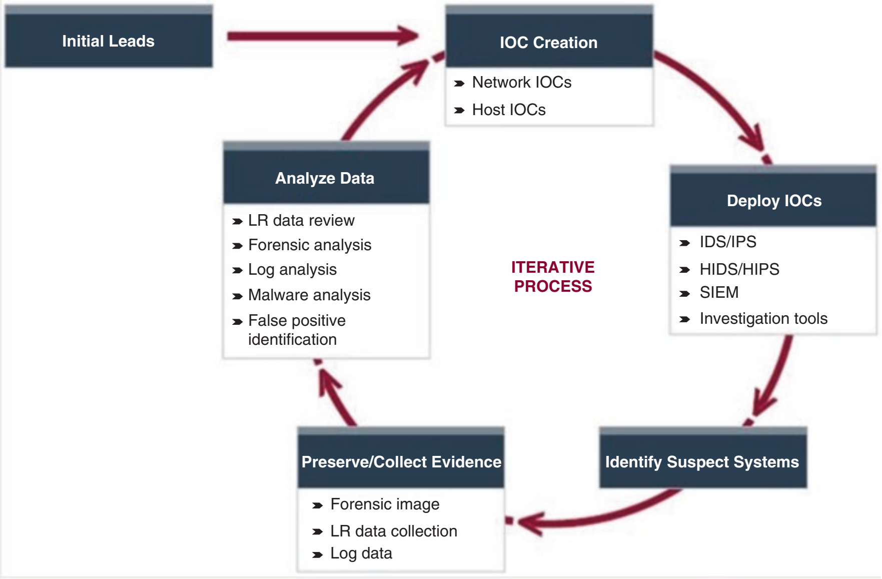


Fig. 6.17 OpenIOC process flow (OpenIOC 2011)

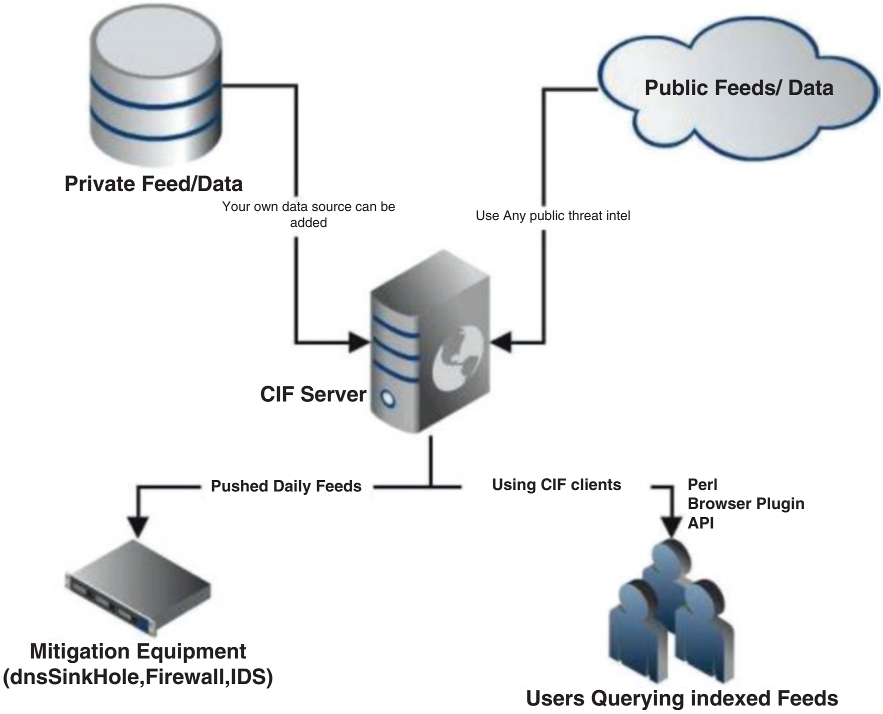

Private Feed/Data
Public Feeds/ Data
Your own data source can be added
Use Any public threat intel
CIF Server
Pushed Daily Feeds
Using CIF clients
Perl
Browser Plugin
API
Mitigation Equipment (dnsSinkHole,Firewall,IDS)
Users Querying indexed Feeds

Fig. 6.18 CIF architecture, (Bambenek 2013)

integrate with many other tools such as: Kibana, Snort, Bro, Bind, Tipping Point, PassiveDNS, and FireEye (https://github.com/csirtgadgets/massive-octo-spice/wiki/The-CIF-Book). Data types in CIF include URLs, Domains, IPs, or MD5s (Fig. 6.18).

Open Threat Exchange (OTX)

Open Threat Exchange (OTX) from AlienVault provides an open access mechanism to a global community of threat researchers and security professionals to aggregate and exchange security threats. In addition to creating a unified communication mechanism and language, OTX tries to provide actionable advices for security community to follow in order to learn from historical threats or attacks. OTX tries also to enable preventative response through an **automated**, real-time, threat exchange framework.

Table 6.5 A sample of open malware scanners

Malwr—Cuckoo	https://malwr.com
Hybrid analysis	https://www.hybrid-analysis.com
PE dump	https://github.com/zed-0xff/pedump
Yararules	https://analysis.yararules.com/
Virscan	http://www.virscan.org/
Virusade	http://virusade.com/
VirusTotal	http://www.virustotal.com/
AndroTotal	https://andrototal.org/
Comodo	https://cit.valkyrie.comodo.com/
VirScan	http://r.virscan.org/
ID Ransomware	https://id-ransomware.malwarehunterteam.com/
Document Analyzer	http://www.document-analyzer.net/
Malware tracker	http://www.cryptam.com/
Jotti	http://virusscan.jotti.org/it
ViCheck	https://www.vicheck.ca/
PDF examiner	http://www.pdfexaminer.com/
Malware tracker	https://www.malwaretracker.com

Security analysts who want to collect data from those different frameworks can build their own crawlers or use APIs provided by some malware analysis providers such as MISP and Virustotal, malwr.com, etc., Table 6.5.

Bibliography

Bambenek J (2013) Hacker hotshots, 11/27/2013

Barger DG (2005) Toward a revolution in intelligence affairs, RAND corporations

Bianco D (2017) The pyramid of pain: threat hunting edition, Huntpedia: your threat hunting knowledge compendium

Brown AE (Georgetown University, 2009) Directed or diffuse? Chinese human intelligence targeting of US defense technology

Chickowski E (2013) Top 15 Indicators of Compromise, darkreading.com, 10/9/2013

Chismon D, Ruks M (2015) Threat intelligence: collecting, analyzing, evaluating. MWR InfoSecurity Ltd. https://www.gpo.gov/fdsys/pkg/GPO-IC21

DoD Joint Publication 2-01, Joint and National Intelligence Support to Military Operations, 22 October 2013. https://fas.org/irp/doddir/dod/jp2_0.pdf

Fischer EA (2014) Federal laws relating to cybersecurity: overview of major issues, current laws, and proposed legislation. https://fas.org/sgp/crs/natsec/R42114.pdf

Gellman B, Poitras L (2013) U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. Washington post, June 7, 2013

Grant J (2010) Will there be cybersecurity legislation? 4 J. NAT'L SECURITY L. & POL'Y 103, 111

Information Collection, FM 3-55, Department of the Army, No. 3-55 Washington, DC, 23, April 2012. https://fas.org/irp/doddir/army/fm3-55.pdf

Information technology industry council: the IT Industry's Cybersecurity Principles for Industry and Government (2011) https://www.itic.org/dotAsset/31bcabf8-514e-498e-a0af-7ed37e-3a92ef.pdf, www.itic.org, version 3

Intelligence analysis, Department of the army, FM 34-3 https://www.globalsecurity.org/intell/library/policy/army/fm/34-3/fm34-3.pdf

Interagency Threat Assessment and Coordination Group (2009) Homeland security digital library. https://www.hsdl.org/?view&did=33087

IRTPA (2004) The Intelligence Reform and Terrorism Prevention Act, DNI.gov, https://www.dni.gov/index.php/ic-legalreference-book/intelligence-reform-and-terrorism-prevention-act-of-2004

ITACG intelligence guide for first responders, 2nd edn (2011) National Counterterrorism Center (NCTC). http://www.ise.gov/sites/default/files/ITACG_Guide_2ed.pdf

Joint Publication 2-01, Joint and National Intelligence Support to Military Operations, 5 July 2017. https://fas.org/irp/doddir/dod/jp2_01.pdf

Joint Publication 3-13 "Information Operations"—27 Nov. 2012. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf

Kenny MT (2006) Leveraging operational preparation of the environment in the GWOT, School of advanced military studies, AY 05-06

Keys RE (4 February 2005) Air Force Policy Directive 10-35: Battlefield Airmen

Kuyers J (2013) 'Operational preparation of the environment': 'intelligence activity' or 'covert action' by any other name? 4 Am. U. Nat'l Security Law Brief 21 (Winter 2013). Available at SSRN: https://ssrn.com/abstract=2398500

Lingel S, Rhodes C, Cordova A, Hagen J, Kvitky J, Menthe L (2008) Methodology for improving the planning, execution, and assessment of intelligence, surveillance, and reconnaissance operations, RAND project airforce. www.rand.org

Lowenthal MM (2008) Towards a reasonable standard for analysis: how right, how often on which issues? Intell Natl Secur 23(3):303–315

Lowenthal MM (2012) Intelligence: from secrets to policy, 5th edn. SAGE/CQ Press, Los Angeles, p 252

Lowenthal MM (2009) Intelligence: from secrets to policy. CQ Press, Washington, D.C. JK 468. I6 L69.

Lowenthal MM, Clark RM (2016) The five disciplines of intelligence collection. CQ Press, Washington DC

Military Decision-making Process (2014) https://usacac.army.mil/sites/default/files/publications/15-06_0.pdf

Miller JP (1999) Millennium intelligence: understanding and conducting competitive intelligence in the digital age, 1st edn. Information Today, Inc.

Naval war college, Maritime component commander guidebook, July 2014

NSA slides explain the PRISM data-collection program (2013) Washington post, June 7, 2013

OpenIOC (2011, October) An introduction to openioc. Retrieved from http://openioc.org/resources/An_Introduction_to_OpenIOC.pdf

SANS Digital Forensics and Incident Response Blog (2009) https://digital-forensics.sans.org, https://digital-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain/

Senkowski RM, Dawson MW (2009) Cybersecurity: a briefing—part II. Wiley Rein LLP, August 5, 2009. http://ccbjournal.com/articles/11615/cybersecurity-briefing-part-ii

Stech F, Heckman K, Strom BE (2016) Integrating cyber-D&D into adversary modeling for active cyber defense. In: Cyber deception, July 2016

Strategic Intelligence, JP 1-02, 509, John G. Heidenrich, "The intelligence community's neglect of strategic intelligence", Studies in intelligence, cia.gov. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol51no2/the-state-of-strategic-intelligence.html#2-strategic-intelligence-jp

Suspicious Activity Reporting, Process Implementation Checklist, Nationwide SAR initiative, NSI. https://nsi.ncirc.gov/documents/sar_implementation_checklist.pdf

Tanner (2014) Examining the need for a cyber intelligence discipline. J Homeland Natl Secur Perspect 1:1

U.S. Department of Homeland Security, Target Capabilities List, A companion to the National Preparedness Guidelines (2007)

Vez J-L (2017) Guidance on Public Private Information Sharing against Cybercrime, World economic forum

White paper: "Sophisticated indicators for the modern threat landscape: an introduction to OpenIOC" (2013) www.openioc.org

Chapter 7
Cyber Operational Planning

K0028 Knowledge of Organization's Evaluation and Validation Requirements

The process of collecting business, software, or information systems' requirements in general and security requirements in particular can take different approaches, structured or unstructured. At the end of the requirements collection process or stage, we may have one or more examples of the following problems that trigger the need for a thorough evaluation or validation process:

- Requirements, comprehensives, or completion issues: How can we judge that we collected **all** necessary requirements? What is the possible and best reference that we should choose to judge such completion? Organization goals, missions, or regulations? General national standards and regulations? Time and budget limitation? Model-based evaluation? Or something else? It is possible in many cases that the answer is actually a mixture of all those references.
  For security requirements, the lack of properly accommodating some security requirements is translated to possibly creating some system vulnerabilities. On the other hand, realistically, completion without a specific and limited reference is very expensive and time-consuming to achieve. Risk management should always consider the trade-off between asset values and the amount of time and budget investment we can allocate for such assets.
- Requirements consistency and conflict issues: When we talk about security requirements, in most cases such requirements cover categories or sections from different business functions. Situations may happen in which some security requirements from a business function contradict with other or over business functions or overall security goals. For example, assume that an organization-wide security policy prevent access for remote users. On the other hand, one or more business functions require employees or customers to be able to access certain information systems or databases remotely. In such case, should

I. Alsmadi, *The NICE Cyber Security Framework*,
https://doi.org/10.1007/978-3-030-02360-7_7

exceptions be made or not? Should we allow such exception only on that business function or eventually make a structured exception that everyone else can use?

Consistency is also related to writing security requirements in the same level of abstraction and details. If unstructured methods are used to collect or document those requirements, chances are that requirements will not be consistent. On the other hand, using a formal modeling tool to write and document such requirements may improve consistency and facilitate validation, but with overhead related to time to learn such formal methods and also time to build such models.

We should differentiate between high-level user visible policies that are usually wide and large in meanings as well as platform, or system independent, and low-level policies, or rules that are concrete and more specific to some security controls or information systems. The need to have such different levels of abstractions (at least those two levels) does not contradict with the need to have consistent security requirements, in the same abstraction level.

How do we validate requirements? We can classify the general validation process based on when we are validating the requirements or based on what reference? For example, in early stages of the process, we will start security requirements elicitation process based on business goals, information systems, environment, compliance with regulations, etc. The output of such process will be the security requirement which can be validated against those different inputs to make sure that nothing in those requirements contradicts with any of those inputs that were used to create such requirements. The validation process in this stage can be a mixture of structured and unstructured methods including, but not limited to: formal documents' reviews, users and customers' interviews or meetings, etc.

In later stages of security controls' design and implementations, we can test security controls, policies, and low-level rules as outputs or deliverables implemented based on early security requirements. Vulnerability testing and penetration testing methods can also be used to test and validate our security requirements.

K0234: Knowledge of Full Spectrum Cyber Capabilities

Full spectrum refers to the overall understanding (e.g., intelligence collection capabilities) and countering of threats across the Cyber Electronic Warfare (EW) domain or spectrum with the goal of providing full cyber control of allies and denying those to adversaries (i.e., both defensive and offensive cyber activities). It refers to including research, knowledge, and development of sensors, concepts, techniques, and technologies encompassing collection, exploitation, and engagement of all data and signals across the Cyber EW spectrum. Full spectrum cyber is a term coined by the DoD to include both defensive and offensive cyber operations. Full spectrum cyber refers also to the full cyber support life cycle: from providing network and systems designed to operational support, security intelligence, and cyber training and exercise support.

In the USA, one military unit, U.S. Army Cyber Command (ARCYBER) provides cyber soldiers to support military missions. These soldiers are tasked with defending army networks and providing full spectrum cyber capabilities.

CNA/D/E/O

Full spectrum capabilities try to integrate elements from: computer network defense (CND) with offense: attack and exploitation (CNA/E) into one platform.

- Computer network attack (CNA) indicates actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves (DoD 2010).
- Computer network defense (CND). Actions that are taken to protect, monitor, analyze, detect, and respond to unauthorized activities within information systems and computer networks, (DoD 2010).
- Computer network exploitation (CNE). Enabling operations and intelligence collection capabilities that are conducted through the use of computer networks to gather data from target or adversary information systems or networks, (DoD 2010).

  Full spectrum analysis requires multi-INT analysis approach. Multi-INT (i.e., multiple-intelligence) is the fusion, integration, and correlation of different types of data collected from different sources to provide a full operating view. The main two intelligence components to integrate are SIGINT, GEOINT, and MASINT. Open source and social media data are also important recent components. More recent components evolved such as: Activity-based intelligence (ABI).
- Computer network operations (CNO).

In addition to multi-INT in terms of the different sources or methods of collecting intelligence data, multi-INT should employ sharing and operations:

- Cross-agency multi-INT sharing: Between the different intelligence agencies, public and private sectors. One example of such efforts a project called MISP—Open source threat intelligence platform and open standards for threat information sharing, www.misp-project.org
- Cross-domain multi-INT operations: Ideally, this should be in the form of autonomous or self-adaptive security controls that learn threats in the domain and adapt itself to counter such threats.

K0316: Knowledge of Business or Military Operation Plans, Concept Operation Plans, Orders, Policies, and Standing Rules of Engagement

Operational plans are the means by which organizations use their resources to achieve strategic objectives. Unlike strategic plans that plan for long-term goals, operational plans orchestrate activities over a short period of time (e.g., tactical, day-to-day activities). On the other hand, an operational plan is part of an organization's strategic plan. Operational plan covers (1) the work to be carried out and (2) the workflow of activities, personnel, roles, schedules, including all the resources that are required. Operational plan should also (3) cover risks that will be dealt with and how the progress of the plan will be sustained.

Main components of an operational plan include:

- Goals and objectives
- Activities or tasks to be delivered
- Quality standards and control
- Key performance and progress indicators (KPIs): Quantitative, qualitative, leading, lagging, input, process, and output indicators
- Risk management plan
- Staffing and scheduling
- Time and budget estimation

Users can utilize many online, open source and commercial tools to support operational plan functions such as: Work Breakdown Structure (WBS), GANTT charts, Project Evaluation, and Review Technique (PERT). When selecting objectives, make sure they are SMART: specific, measurable, achievable, realistic, and time-bound objectives.

For military operations, deliberate plans are prepared under joint procedures and in prescribed formats as either an Operation Plan (OPLAN), Operation Plan in Concept.

Format (CONPLAN). OPLAN is an operation plan for the conduct of joint operations that can be used as a basis to develop the detailed operation order OPORD (i.e., the OPORD is the realization of the OPLAN). An Operation Plan in Concept Format (CONPLAN) is an abbreviated operation plan that would require considerable expansion or alteration to be converted into an OPLAN or OPORD (globalsecurity.org). OPLAN includes more details about Courses of Actions (COAs) development and selection in comparison with CONPLAN. Figure 7.1 shows an example joint plan summary indicating the relations between OPLAN, CONPLAN, COA, and OPORD (acq.osd.mil 2007).

The standing rules of engagement (SROE) establish fundamental policies and procedures governing the actions to be taken during all military operations and contingencies and routine military department functions occurring outside US territory. The standing rules for the use of force (SRUF) establish fundamental policies and procedures governing the actions during all DOD civil support (e.g. military assistance to civil authorities) and routine military department functions occurring within US territory or US territorial waters, (US Naval War College 2014). SROE

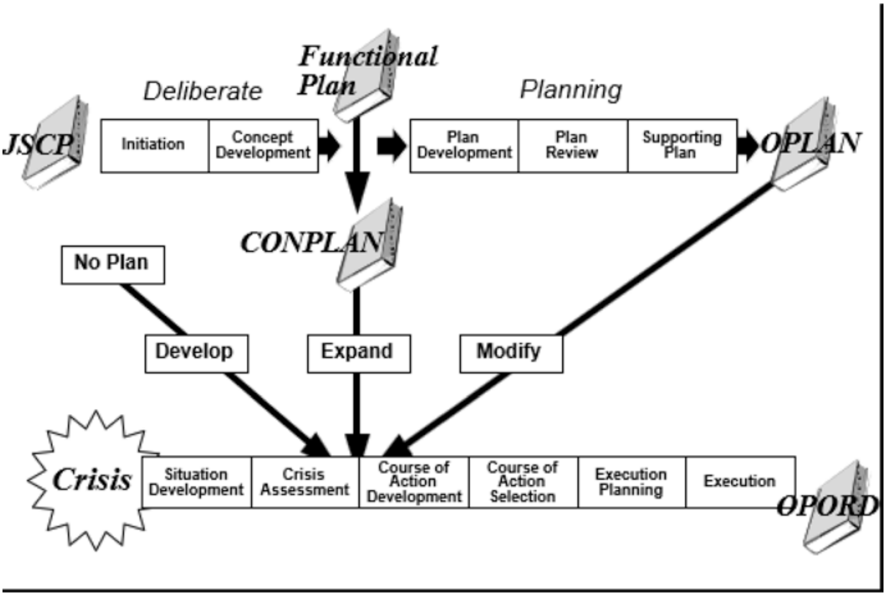


Fig. 7.1 An example of military joint planning summary (acq.osd.mil 2007)

that is specified for an operation provides implementation guidance on self-defense and the application of force for mission accomplishment. SROE provides lists of numbered supplemental measures that may be provided by, or requested from, higher authority to tailor ROE for a particular situation (Joint Pub 1999).

K0367: Knowledge of Basic Cyber Operations Activity Concepts (e.g., Foot-Printing, Scanning and Enumeration, Penetration Testing, White/Black Listing)

For attacking, hacking, or offensive operations, there are different stages in which such operations are conducted. Foot-printing, scanning, and enumerations are usually initial or early steps any offensive operation will start with. This early stage is usually called "information gathering" stage.

Penetration, or usually abbreviated as Pen, testing, typically conducted by security teams to ensure that systems, networks, assets, servers, etc. are immune against the different types of attacks. They follow somewhat the similar stages typically occur in attacks: information gathering, vulnerability assessment and analysis, and third exploitation phase. The term "ethical hacking" is used sometimes to indicate penetration testing or defense team testing activities. It implies also learning the same hacking methods, but usually for defensive goals.

Penetration testing usually starts with a clear agreement between parties clarifying: (1) the Dos and Don'ts, (2) the systems or assets to be tested, (3) any exceptions to be excluded from the testing process in those assets, (4) details about the testing team, the workflow process, data privacy issues, exploiting and reporting mechanisms, etc. The main output of the penetration testing process, a detailed report indicates the different types of discovered vulnerabilities that can be related to the network, the systems, the software, the personnel, or the workflow. Further, recommendations are important from the testing or auditing team to show how such vulnerabilities can be fixed.

Penetration testing can be black-box or blind where testers will not be provided with details about the systems and assets they are going to test and the employees and users of those assets will not be informed about the ongoing penetration testing. In white-box approach, both teams will have knowledge about each other (i.e., full disclosure). Partial disclosure or gray-box is also a third variation. As a service, penetration testing can also be by external parties with variations from simple information gathering activities to full organization audit.

Foot-printing: Foot-printing is an early phase of information gathering (to give you a foot-print) that involves interactions with the target in order to gain information to know details about that target such as: web server version, IP addresses, phone numbers, emails, namespaces, subnet info, OS info, and subdomain information for the given URL.

Examples of some tools that can be used at foot-printing stage: Netcraft (helps obtain web server version, IP address, subnet info, OS info, and subdomain information), Link Extractor (a utility to extract links or URLs), Google Maps for address details, Echosec and Maltego for online social media search, EDGAR for public company and financial information extraction, and LexisNexis for people search. In most cases, foot-printing tools are considered passive; receiving traffic and information without actively sending the target any signal. This helps attacker to keep interaction with the target to the minimum to avoid detection.

Next to foot-printing scanning activities try to get more details about the target. Ping sweeps, traceroutes, port scans are examples of scanning tools and methods. Nmap, with its different flavors is one of the very popular scanning tools to scan TCP/UDP ports looking for open ports that can be used to access target systems.

In the next phase, enumeration, much more detailed information is extracted the target systems. The information gathered during phase 3 typically includes, but is not limited to, the following: login or usernames, passwords, hidden shares, device information, network topology, protocol information, servers, services, etc.

White/black listing methods, especially for URLs and IP addresses are popular and simple to eliminate known attacking addresses. For threat detection systems, it is important to monitor URLs that are known for previous malicious attempts.

Many websites and links exist that report on periodic bases malicious IP addresses or URLs. Those malicious activities can be related to hacking, spam, Denial of Service (DoS), or being part of any type of attack or malware dissemination. Some threat detection systems create black lists of such URLs (e.g., to be blocked in the network access controls). However, using such black lists can cause several problems or challenges:

- The number of URLs or links in this black list database can be huge, millions of links. This will cause significant overhead or performance issues on security access controls. For a network with many users or internet connections, to require that each traffic request will be tested first against the malicious list can be a serious overhead problem.

- Many of those URLs or IP addresses may change with time due to different reasons. Attackers may do that intentionally to avoid detection. They may use spoofing methods to change or fake their IP addresses. Additionally, those URLs and IP addresses can be sold from time to time to different users or owners.

As an alternative to dictionary-based malicious URLs' detection, rule-based detections methods can be used to study patterns of attacks. While the previous method can be more accurate in known malicious URLs' territories, methods of detection based on attack common features can work more effectively in unknown territories.

K0400: Knowledge of Crisis Action Planning for Cyber Operations

A Crisis Action Plan (CAP) is an operational plan driven by current events (e.g., a malware breakout). A CAP is typically developed in reaction to an actual threat or incident. Crisis action plans should be flexible and adaptive to the environment changing factors. Unlike contingency plans that do not have a defined start date, time is a key to crisis action plans and their validity is limited to a certain period of time. Both contingency plans and crisis action plans contain execution objectives that can guide the delivery of capabilities across mission areas.

For cyber operations, crisis action plans can be developed in case of malware breaches, hacking attacks, etc. with the main goals of (1) mitigating impacts, (2) remove intruders from our systems, and (3) ensure business continuity.

In USAF, AFI 10–403, Deployment Planning and Execution, Deliberate and Crisis Action Planning and Execution Segments (DCAPES) are designed to communicate OPLAN requirements to minimize unnecessary movement of personnel and equipment into operations during execution stages.

CAP can be developed by external consultants or internal organization members. For example, company can assign chief information, security, or operations officer to lead the project to create CAP. It is more recommended to have an internal team that has more knowledge of the company, assets, stake holders, etc. Previous cases such as the case of Morgan Stanley in 2001 (Klann 2003) show that CAP can save resources and also lives. In order for CAP to be effective, it should be supported by organization leaders and allow CAP personnel to have the right authority for the proper design and implementation or deployment of CAP whenever needed.

CAP designers can search for available templates online. They will have then to customize it based on the nature of their organization and the candidate events. Figure 7.2 shows a sample of crisis action plan checklist to be covered in the plan (Klann 2003).

- Define what constitutes a crisis for your organization and what does not.
- Develop and implement risk identification and assessment procedures.
- Define events and indicators that show a crisis is imminent.
- Define the immediate actions to be taken when a crisis occurs.
- Select who activates the CAP and how it occurs.
- Develop a detailed internal and external communication plan with specific reporting and notification responsibilities.

Fig. 7.2 A sample of crisis action plan checklist (Klann 2003)

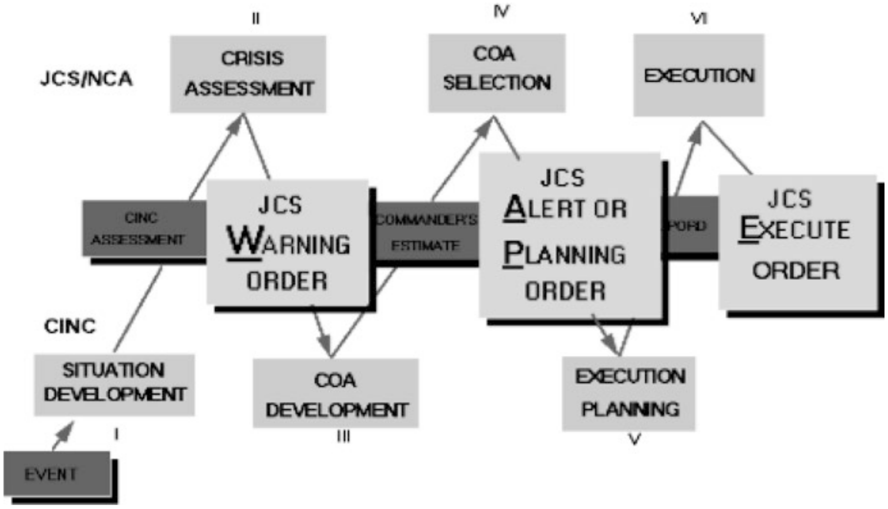


Fig. 7.3 CAP phases (Buchanan 2018)

Define a Crisis

It's very important to decide when to trigger the CAP process or not. A balance should be made not to trigger CAP too often, which consume resources and is not justified if the problem is not severe or does impact one or few numbers of users. The definition and category of crisis to a business can vary based on the business nature, company size, etc. A crisis assessment process can be used to judge whether to trigger CAP or not.

CAP typically includes six phases (Buchanan 2018, Fig. 7.3):

- Situation development
- Crisis assessment
- Course of action development
- COA selection
- Execution planning
- Execution

Due to the time sensitivity of the situation, steps may be accomplished out of sequence or simultaneously.

K0413: Knowledge of Cyber Operation Objectives, Policies, and Legalities

Cyber operations' interdisciplinary major covers the entire scope of cyberspace and related operations, both technical and non-technical aspects. In addition to computer science and information technology technical knowledge and skills, this major cover knowledge from other disciplines related to: policy, law, ethics, and social engineering.

Cyber operation functions are classified into offensive and defensive. In offensive/exploitation operations, cyber operation specialists target adversary systems, activities, and capabilities. In defensive operations, that are usually reactive, cyber operation specialists are trying to defend friendly systems, assets, networks, etc. and respond to adversary attacks. Examples of defensive cyber operations:

- Detect malicious/unauthorized network traffic.
- Identify the source of the malicious traffic.
- Mitigate the threat traffic while maintaining essential business continuity services.

In terms of workforce categories, cyber operation is divided into:

- Defensive operations.
- Operations and maintenance.
- Information assurance.

Within the US military different branches, more than 70 job titles are currently available in cyber operations' major (DoD 2011).

With the expansion of defensive and offensive cyber operations at the national and international levels, legal issues start to bring some concerns. While not every action in cyber operations is illegal, many of especially offensive cyber operations are clearly in breach of international laws (Wrange 2014). Two main reasons: violation of sovereignty of other countries or as a violation of individual's privacy and human rights. However, debates exist whether cyber operations can fall within the international definition of sovereignty violation (e.g., see UN Resolution 3314, in 1974 that states that aggression "is the use of armed force by a State against the sovereignty of other states").

Different states tend to view cyber operations the same way as more traditional methods of intimidation (Steiner 2017). Whether cyber operations can be considered as cases of cyber wars or not is debatable (e.g., see Rid 2013, D'Aspremont 2016). This is especially the case when those are covert operations; not part of conventional wars. Given the facts those operations are not on physical battlefields, whether they actual occurred or not is also debatable.

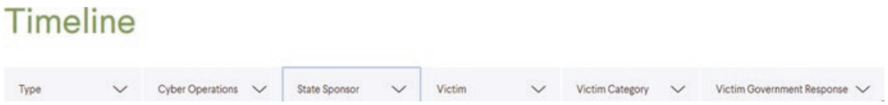


Fig. 7.4 Reports on cyber operations from www.cfr.org

Several websites track and report cyber operation incidents. For example, the website https://www.cfr.org/interactive/cyber-operations reports cyber operation incidents and classifies them according to: type, cyber operations, state sponsor, victim, victim category, and victim government response (Fig. 7.4).

One more issue that can complicate legal issues related to cyber operations is that cyber operation members can be either (1) country or state employees (e.g., from the cyber intelligence-related departments), (2) they can also be state-sponsored individuals, or (3) they can be individuals or teams of individuals working on their own. Further, within international conflicts, the ability to distinguish to which group of those three previously mentioned the cyber team belongs is not a trivial task. Two major reasons seem to dominate offensive cyber operations:

- Political reasons: which typically involve state or state-sponsored members.
- Financial or monetary reasons: which typically involve individuals or teams working on their own.

Industrial or technology espionage is also popular in cyber operations where states or companies conduct cyber operations to acquire certain knowledge or technologies.

From a legal perspective, the ability to trace the impact of a cyber operation offensive is very complex as it usually includes many users and assets in different areas. Non-state individuals can cause impacts similar to or even more than state-sponsored teams or efforts especially as cost to conduct large-scale cyber offensive can be sometimes next to nothing.

K0415: Knowledge of Cyber Operations Terminology/Lexicon

K0436: Knowledge of Fundamental Cyber Operations Concepts, Terminology/Lexicon (i.e., Environment Preparation, Cyber-Attack, Cyber Defense), Principles, Capabilities, Limitations, and Effects

In this section, several terms related to cyber operation will be briefly introduced.

CyberSpace

Cyberspace is defined by US DoD as the global domain that consists of the interdependent networks of information technology infrastructures and resident data. This includes the Internet, telecommunications networks, computer systems, in addition to embedded processors and controllers (CRS 2015).

With electromagnetic signals from the different applications in the spectrum sending and receiving those invisible data elements around us, everything around us is part of this cyberspace. The Internet, or the web, online social networks (OSNs), smart phones, cloud computing, and Internet of things (IoT) are some other main milestones or contributes to the continuous growth of the cyberspace. All elements in those technologies are contributing nodes to this invisible, large, and complex virtual cyberspace around us.

Full Spectrum Cyber

We described in earlier sections the different implications for full spectrum cyber operations, analysis, etc. This is one of the "buzz" words in cyber operations and intelligence largely used by companies for marketing purposes. Originally, the term spectrum is related to the EW frequency spectrum from telecommunication products, applications, bands, etc. This also integrated IT, software, hardware, and network environments and does not focus cyber applications on the software side only.

Cyber Ranges and Information Technology Ranges

Cyber ranges are large virtual labs that exist to provide and support safe and legal training on cyber security, intelligence, and operations. One of the main drivers for such labs is the need to equip cyber personnel with skills and hands-on trainings in addition to the theoretical learning or knowledge.

Typically, those are emulation rather than simulation. It means that many of those labs represent actual physical networks and labs, but users can access them virtually from anywhere in the world, once they are given the right credentials. Virtualization is also common in those labs where users can use images with virtual operating systems. This can typically facilitate minimizing the effort for users to mimic the actual lab or exercise environment. It can also help users perform their training on virtual operating systems isolated from their host operating systems. For cyber security experiments, this can shield host operating systems from risks related to conducting experiments that can harm those operating systems.

Early cyber ranges were DoD private for internal employees only. There are many large-scale cyber ranges such as US national cyber range, NCR: (https://www.acq.osd.mil/dte-trmc/ncr.html) developed by Defense Advanced Research

Projects Agency (DARPA). There are some other projects such as Geni (www.geni.net), Deterlab (https://www.isi.deterlab.net), Emulab (https://www.emulab.net), etc. that provide public access to computing and system resources for students, researchers, etc.

Cyber Espionage

In classical espionage, a company may hire an undercover employee to work with another company and spy on some products, technologies, etc. This may be similar in cyber espionage or may be completely virtual where individuals performing the espionage may not be physically in contact with target states, companies, or systems. Espionage can be for spying on government or military personnel, systems, or assets. It can also be to transfer new technologies, inventions, copyrighted products, etc. In one recent cyber espionage case, the USA charged five Chinese hackers for cyber espionage against U.S. Corporations for commercial advantages (Department of Justice 2014).

Cyber Deterrence

Cyber deterrence is an active defense approach to respond and attack back adversary attackers. Cyber deterrence can serve two main goals: (1) To harden our systems and the job of hacking them. Many hackers start by searching the cyberspace looking for victims. By making our systems harder that the typical or the majority of other systems, we can avoid untargeted attacks. Those are the attacks that are not focusing on one target, but rather any victim target that is vulnerable. The second goal of deterrence or active defense is to make the attacker or hacker think of consequences, whether those consequences are legal, monetary, etc. Deterrence may not be always possible or simple. For example, when amateur international individuals target state or country large-scale systems, countering back such individuals may not cause significant cost or consequences on the attackers' side.

Cyberwar and Cyber Warfare

Those are wars performed in and from computers and the networks/systems connecting them, waged by states or their proxies against other states or countries.

With the continuous expansion of Internet of Things (IoT) in particular, many things in our real life are monitored and controlled through the Internet (e.g., transportation systems, telecommunication, power, GPS, and water systems). This indicates that future cyber warfare can seriously touch and impact human lives and safety similar to classical wars and weapons.

Cyber Persona

Cyber persona refers to an identity that is used in cyberspace to obtain information or influence others, while hiding or dissociating the actor's true identity or affiliation (CI glossary 2011). The cyber world does not correlate clearly with the real world where many, in the cyber world may play more than one identity or fake their real identity. Additionally, it is very common for security defense personnel to masquerade as hackers in some hacking websites to gain information about tools and users in those websites, etc. Drawing the line between ethical and unethical hacking can be in some cases very challenging especially as both teams may try to masquerade each other. Additionally, security defense personnel work in different organizations and may not synchronize with each other or communicate with details on their defensive and offensive cyber operations. Another challenge is related to insider threats when they exist, intentionally or unintentionally as in both cases consequences can be very serious.

Cyber Weapons

The term cyber weapons can refer to the tools and mechanisms attackers or cyber operation offensive teams can use to attack adversary targets. This includes main categories such as malwares, botnets, denial of services (DoS), worms, etc. Cyber weapons and tools continuously evolve and the competition between both cyber operations defense and offense teams is very high to keep up with tools and mechanisms of the other side. Typically, offensive job is easier than defensive where from an attack or offense perspective, all what it takes, is one vulnerability or exploit to successfully attack a system. This vulnerability can come from a wide range of targets such as: software, hardware, network, operation system, servers, websites, or users. Typically, a major attack starts from one exploit that can be escalated later on.

Cyber Warriors

Individuals or teams who launch cyber offense operations are typically called cyber warriors. Whether true or not, many cyber warriors in different countries work on their own without being members of government agencies or state-sponsored members. One reason, states adopt such models is to avoid legal consequences or international relational problems.

Cyber Deception

Cyber deception enables a proactive security approach by seeking to deceive attackers, detect them and then defeat them, allowing systems to return to normal operations.

Cyber-Hacktivists

Cyber-hacktivists are individuals who perform cyber-attacks for political, environmental, or other nonmonetary reasons. One of the most popular examples of cyber-hacktivists is anonymous group. Anonymous is a large decentralized international hacktivist group that is widely known for performing various DDOS cyber-attacks or web defacements against several governments. In some other cases, those can be in the form of cyber-riots with large individuals against their own country protesting their own government, policies, etc.

Cyber Operations Limitations

One of the significant efforts that talked about limitations on cyber wars and operations is Tallinn Manual (NATO 2013, Schmitt 2013, 2017). The manual represents 3 years effort to assess how current international laws react to cyber operations, warfare, etc. One important limitation in cyber operations focused in the manual is related to the protection of civilians and the need to take all possible measures to protect humans from the impacts of cyber operations. From practical perspective and due to the nature of the Internet and cyber world where everything is interconnected, achieving such goal in all cyber operations is almost impossible. States are responsible and liable for cyber operations committed by their members or proxies (Schmitt 2013). The ability to limit or trace back all types of impacts that a cyber operation caused can take effort much more the effort required to plan and deploy those cyber operations. This can be seen as similar to the "collateral damage" in conventional wars (i.e., unintended damage).

The detection of activities by adversaries in the cyberspace is a difficult and long process (Joint Publication 3-12, 2013). Further the assessment of the impact of a cyber operation is also tedious and time-consuming. It is possible that friendly cyber operation may cause direct or indirect impacts on friendly assets that were unaccounted for as planning for the impact of a cyber operation is tedious and may not be always accurate.

K0416: Knowledge of Cyber Operations

Cyber operations evolve as an interdisciplinary major that covers the whole cyberspace activities and that requires skills from different disciplines such as cyber and network security, data analytics, software engineering, computing architectures, and operating systems. There are also knowledge required to understand humans (e.g., users, attackers, hackers) behaviors, mindsets, and related human and social aspects.

In the USA, this major is witnessing a staggering job demands in both public and private sectors. Courses and training in cyber operations start to grow from government and military sectors to Universities and private sectors. Many of the jobs offered in this area require certain levels of clearance even at the private sector.

The knowledge and skills in cyber operations span the life cycle of three major entities:

1. Malwares: Including the stages of creating analyzing and reverse engineering malwares.
2. Attacks: How attacks are created, initiated, launched, and analyzed. Cyber operations student should be able to switch between the defense and offense roles. When the student is learning the roles of the defense team, they need to learn how to prevent against attacks, how to stop attacks in real time, and how to analyze launched attacks and learn to protect systems in future. When they masquerade the offense roles, they need to learn and practice how to start attacks and find weaknesses in systems, software, networks, etc., how to maintain those attacks and protect or hide their attacks and identities.
3. Systems and assets: Cyber operations' students should learn about the different systems and assets that they need to protect. They need to understand them thoroughly from a defender perspective. They will learn for example penetration testing methods and how to screen the different systems for possible vulnerabilities. They need also to learn about the different types of security controls (e.g., firewalls, IDS/IPS.). They need to learn how to program those security controls, update them, etc.

Different programs in cyber operations have different focuses. Below are some of the most popular sub-areas that fall within this major:

- Offensive cyber operations.
- Defensive cyber operations.
- Cyber threat intelligence.
- Software security analysis and exploitation.
- Malware analysis.
- Networking and digital forensics.
- Cryptography.
- Cyber laws: Legal and ethical issues.

Cyber operations can be divided into: (1) exploitation and (2) attack.

- Cyber exploitation which includes activities such as to identify theft or theft of information and denial of service attacks.
- Cyber-attacks which include serious cyber offensive operations that can cause serious destructions or impacts (Hilfiker 2013). Cyber operations can also be divided into three categories: Access operations, disrupting operations, and attack operations, Fig. 7.5, (Hilfiker 2013).

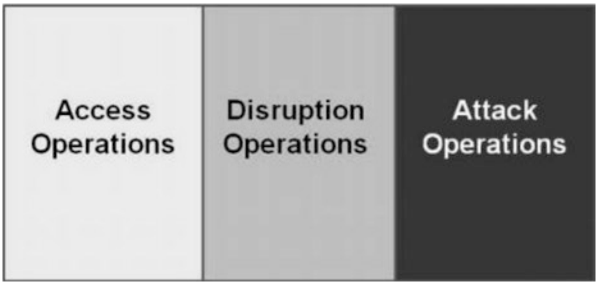


Fig. 7.5 Classification of cyber operations (Hilfiker 2013)

K0424: Knowledge of Denial and Deception Techniques

Information superiority is one of the key elements in winning current and future wars in general and cyber wars in particular. However, one of the challenges to achieve full information superiority is adversary ability to conduct denial and deception (D&D) techniques.

Denial is the ability to deny the adversary from having access to accurate information, about assets, events, personnel, equipment, etc. Deception is the ability to provide or present adversaries with incorrect or inaccurate information as if it is correct or accurate.

For example, some of the techniques military adversaries are using are related to presenting fake targets. Once targeted, those fake targets can cause embarrassment (e.g., targeting civilians, religious sites), incorrect focuses, etc. Table 7.1. shows D&D matrix showing the methods needed in cyber defense to achieve D&D superiority (Heckman et al. 2015).

The deception chain, whether from friends or adversary side, can be modeled similarly. This deception chain can take eight phases or steps (Heckman et al. 2015):

- Define deception purpose and success criteria
- Collect intelligence
- Design cover story
- Plan for deception activities
- Prepare
- Execute
- Monitor
- Reinforce

K0442: Knowledge of How Converged Technologies Impact Cyber Operations (e.g., Digital, Telephony, Wireless)

Several recent technologies impacted and continue to impact cyber operations. We will cover some of the main ones and examples of how they can impact cyber operations.

Table 7.1 D&D methods matrix (Heckman et al. 2015)

Facts/ fiction	Deception revealing on our side	Denial concealing on adversary side
Facts	Methods to show facts and truth after adversary deceptions	Methods to conceal our facts from adversaries
Fiction	Methods to reveal false information spread by adversary	Method to spread false information to adversaries

Internet of Things (IoT)

In the IoT world, not only our computers, laptops, and smart phones are going to be connected to the Internet, have their own IP addresses, and be data receiving and sending nodes, but this can be extended to almost all entities or objects around us. This will include, for example, our cars, houses, refrigerators, beds, toys, camera systems, garage doors, monitoring gadgets, utilities, and many others. How is that going to impact cyber operations?

From a cyber defense perspective, this can seriously complicate the cyber defense task and effort as adversaries can now have not only control on our laptops, desktops, or phones, but they can control things that can have more serious and direct impact on our life, safety, etc. This is particularly true as with the expansion of IoT applications and domains, IoT is deployed in hardware and physical components/objects with very lightweight computing resources. This means that such objects are typically (1) slow in terms of how frequent updates they will go through. In other words, the cycle to discover and patch vulnerabilities in those objects is very long if compared with the cycle to do that with computing machines, servers, etc. This means also that (2) such objects typically have limited computing resources that limit defender options of security controls and mechanisms that can be deployed on those objects. For example, encryption methods are the most popular mechanism in security to protect confidentiality, privacy, etc. However, employing reliable and robust encryption schemes in many IoT environments can cause serious performance and efficiency issues. Typically, IoT networks contain IoT agents on the field for monitoring and collecting data and communicating such data with centralized servers or cloud services. Targeting the telecommunication channel between IoT agents and servers in any form of Man in the Middle (MiM) attacks will expose private or sensitive data and cause serious data breaches, privacy, or integrity issues.

On the cyber operation offense side, cyber warriors can deploy attacks that impact physical systems. One early example of malwares that impacted physical rather than software components was the virus: CIH, also known as Chernobyl or Spacefiller that targeted computers BIOSes. Stuxnet is another example of a malware or specifically a worm that targeted SCADA systems, specifically Programmable Logic Controllers (PLC) in Iran nuclear program starting from the year 2010. Some of the recent action movies show cyber operations to control traffic lights, utility systems, etc. and those may not be far from reality.

Clearly, legal, confidentiality and privacy concerns are already serious issues in cyber operations. With the IoT and the fact that those objects can be part of all human life aspects and activities such concerns are getting even more serious.

Safety is a key driver to security concerns in industrial control systems as they expand in terms of their network and Internet connectivity.

Availability of services in IoT environment is also important. Most of those IoTs or SCADAs can be deployed to monitor critical human life or infrastructure-related networks (e.g., water or power utilities). A denial of service attack that can bring such infrastructures down for several hours or days can impact directly human lives. Timeliness and information availability when requested especially in critical systems (e.g., health and aviation systems) is very critical. Denying the access to such information when requested will impact those critical system and result in serious life-threatening consequences.

Cloud Computing

Cloud computing offers users with infrastructure, computing, network, and data services online as an alternative to local assets. Cloud computing brings opportunities to cyber operations as well as challenges. Cloud computing offers access to data from the cloud, from anywhere, lowering the risk of data loss or corruption, and the costs associated with hosting and maintaining locally the data and infrastructure. For cyber operations training, students can have access to training portals and labs from anywhere and can attend and participate in all courses and trainings virtually, from home, or while they are deployed in the field. Brining all resources and facilities to the soldier in the battlefield is possible on their lightweight portable equipment. This same advantage can be a disadvantage if such information is also available (e.g., through hacking or illegal methods) to adversaries to either acquire and take advantage of or destroy and deprive us from utilizing.

From a defense perspective, as more and more public and private infrastructures and assets are moving to the cloud, the concerns are that hackers and adversaries can now have more targets to attack and impact our systems and infrastructure. Security is the biggest concern in cloud computing. In the USA, most government contracts for cloud services have restrictions on who, how, and where cloud services can be provided and data can be hosted. In 2012, US DoD issues a cloud strategy to take advantage of cloud computing services while ensure only certified public or private providers are allowed to offer such services. In 2016, DOD finalized the defense federal acquisition regulation supplement rule on network penetration reporting that standardizes infrastructure requirements (GAO 2017).

Smart Phones

Currently, mobile phones provide services beyond the classical phone calls. Those services are gradually converging to the same services can be offered by computing desktops or laptops. On the other hand, as smart phones accompany users almost everywhere, they can provide valuable location-based information.

Wireless transmissions are not always encrypted. Information such as emails sent by a mobile device is usually not encrypted while in transit. In addition, many applications do not encrypt the data they transmit and receive over the network, making it easy for the data to be intercepted. For example, if an application is transmitting data over an unencrypted WIFI network using http (rather than secure http), the data can be easily intercepted. When a wireless transmission is not encrypted, data can be easily intercepted by eavesdroppers, who may gain unauthorized access to sensitive information (e.g., host computers) without the need to be host administrators, power users, or even users in those local hosts. Their root level role implies having an administrator privilege in all network or system resources.

You could connect to an unsecured network, and the data you send, including sensitive information such as passwords and account numbers, could potentially be intercepted. Many attackers can possibly create "free WIFI" networks to be used as honeypots. They can provide users with free Internet access while intercepting and spying on their sensitive data. In mobile operating systems, it is unconventional to allow users to have "root" access to the operating system. This "privilege elevation to root" is called jail-breaking. Users are not recommended to try to perform jail-breaking, using certain methods or tools. This may open the operating system for several possible vulnerabilities and break the pre-designed operating system security architecture (Alsmadi et al. 2018).

A user of an Apple mobile phone can have the ability to wipe their phone remotely using a mobile device management (MDM) server and iCloud or ActiveSync. All files will be then inaccessible and new user may need to create a new encryption with their new OS installation. System can also be automatically wiped after several unsuccessful PIN attempts. They can also lock their phones. In recent investigations, there were some cases that FBI requested access to credentials of iPhone that were locked (e.g., see CBS 2016). On the other hand, black market provides all types of support and mechanisms to jail-break phones and counter activation or service provider locks.

Using smart phones is convenient and no one can afford abandoning them these days. On the other hand, they can be a weak point through which hackers or adversaries can target or track humans and their data. Their weakness does not only arise from the fact that they can be always used to track human targets, but also because they tend to have weaker overall security controls when compared with desktops or laptops (Underwood 2018).

Smart phones most popular attack types include: scams, phishing, data stealing and spying apps, malware and ransomware.

Online Social Networks

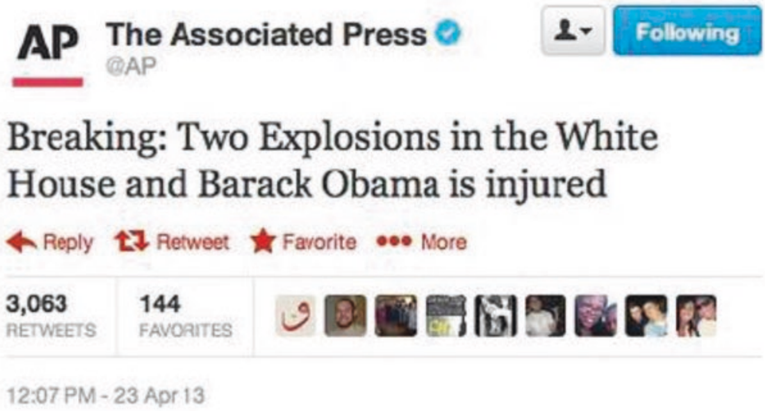
Online social networks (OSNs) provide a wealth source of information for cyber operations. They allow each individual in the world to be an information source. Users share different types of information, activities, articles, and also contribute to others' activities. Users can be source of news and not only news receivers. From a security intelligence perspective, the ability to communicate with any individual around the world became very easy. Given that it is impossible to hire a large number of security intelligence personnel to be able to track all types of information from OSNs, outsourcing this to a large open network of volunteers is possible. We described earlier, different attempts to build open channels of security intelligence and operations around the world to exchange cyber threats' information.

Smart phones are now available all over the world and the use of OSNs is also popular even in regions where income levels are low, so there are few barriers to using this technology to share information. The speed to transfer the intelligence or the information is also very short (NATO 2016).

With the continuous increase of using different OSNs by humans all over the world, tasks to collect human intelligence and aggregating such intelligence with location, activities, interests, etc. became easier and handier to acquire.

The wealth of information provided by OSNs is available for friends as well as foes or adversaries. Several studies showed serious concerns of private or sensitive information leakage through OSNs. Those may not be as a direct exposure from government or military personnel, but through their families and spouses (Cho et al. 2016).

In cyber offensive operations, accounts in OSNs can be targets to expose and steal private information. In some other cases, cyber attackers may try to intrude those accounts and post activities on behalf of account owner. Other offensive goals in OSNs can be simply preventing legitimate users from the ability to access and use their accounts in those OSNs, typically temporarily, Fig. 7.6: (NATO 2016).



The Associated Press
@AP

Breaking: Two Explosions in the White House and Barack Obama is injured

3,063 RETWEETS
144 FAVORITES

12:07 PM - 23 Apr 13

Fig. 7.6 A sample of OSN cyber-attack (NATO 2016)

K0465: Knowledge of Internal and External Partner Cyber Operations Capabilities and Tools

K0494: Knowledge of Objectives, Situation, Operational Environment, and the Status and Disposition of Internal and External Partner Collection Capabilities Available to Support Planning

Cyber operations capabilities can be divided under different categories. We described two classifications earlier:

- Cyber defensive operations: All operations that help friends' teams to defend and protect their systems and assets. This includes:
  - Cyber operations support
  - Securing access to key allies' network systems or nodes
  - Situation awareness
  - Cyber reconnaissance
  - Electronic support or exploitation operations
  - Vulnerability assessment and penetration testing: Examples of existing support capabilities include: network and system vulnerability assessments, industrial, SCADA and physical vulnerability assessment, vulnerability assessment of public utilities. Some organizations provide also vulnerability assessments for public and private organizations per their requests
- Cyber offensive operations: All operations that target adversaries and their assets. Examples of cyber offensive operations include:
  - Electronic attacks: Jamming, decoys, etc
  - Securing access to key adversary network systems or nodes
  - Zero-day exploit (ZDE) cyber capabilities
  - Cyber-attacks: DOS attacks, phishing, malwares, deception, etc
  - Deterrence attacks where the goal is to distract adversary forces (e.g., using honeypots)
  - Implanting cyber access tools or malwares
  - Cyber exploitations: Cyber-attacks to steal information

Some references divided cyber offensive operations into other categories such as: Selected attack options (SAO), Major attack options (MAO), and Limited Cyber Option (LCO) (Long 2017). Targets can also be divided into countervalue (i.e., targets that have no significant military value) and counterforce (targets that have military significant value) (Long 2017).

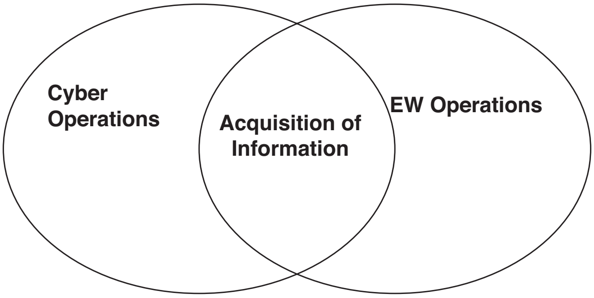


Fig. 7.7 Cyber and EW operations (Arnold 2012)

Most of current cyber operations strategies call for integration of electronic warfare (EW) strategies. For both cyber and EW operations, intelligence and information acquisition are common goals, Fig. 7.7 (Arnold 2012).

In 2009, US started Cyber Command ("CYBERCOM"), with NSA to help secure US systems from cyber-attacks. Cyber offensive operations indicate another major function for CYBERCOM. Some examples of cyber offensive attacks claimed to be associated with CYBERCOM include Stuxnet, Olympic games, and Flame virus targeting Iran nuclear facilities.

K0495: Knowledge of Ongoing and Future Operations

In this section, few examples of recent cyber operations will be summarized.

Stuxnet, Olympic Games, Nitro Zeus, and Flame

As briefly mentioned earlier, those three names indicate different effort in different time periods, believed largely by US and Israel to target Iran nuclear facilities. Officially, this was never confirmed by intelligence organizations in the two countries. The different cyber offensive operations or attacks have different goals related to tampering with different components or modules in Iran nuclear facilities (e.g. programmable logical Units, PLUs). Quick facts about the cyber operations:

- Stuxnet operation starts with a worm in 2010 that targets Iran nuclear SCADA system.
- In particular, Stuxnet targets the PLCs that allow the automation of electromechanical processes.
- Stuxnet has three modules: a worm that triggers the main payload of the attack; a link file that propagates copies of the worm; and a rootkit that hides all malicious files and processes, avoiding Stuxnet detection.

- Flame, also known as Flamer, sKyWIper, or Skywiper is a malware launched in 2012 that targets computers running Microsoft Windows operating systems where most of the targeted machines were in Iran.
- Flame was largely a spyware or espionage tool. It can record audio, screenshots, keyboard activity, network traffic, and skype conversations.

Russia's Hack or Ukraine's Power Grid

This attack occurs mainly toward the end of 2015 and is considered one of the major successful cyber-attacks on power grids. Three major energy distribution companies in Ukraine were impacted by the attack, and their services were interrupted for several hours. Attacks were traced back to IP addresses located in Russia. Quick facts about the cyber operations:

- In initial stages, IT and system administration staff were targeted by spear-phishing emails.
- Once users accept/enable macros in phishing emails, BlackEnergy3 backdoor will be installed.
- Attackers were able eventually to reach power grid SCADA system and force systems' shutdown.
- They also reconfigured uninterruptible power supply (UPS) to tamper backup plans.
- KillDisk malware was used to wipe call center files.
- Attackers also launched a telephone DoS attacks against customer call centers to prevent customers from reporting the outage.

Russia Cyber Operations in Georgia

Another example of Russia heavily employing cyber operations in their recent warfare is the cyber operations conducted in Georgia conflict in 2008. Here are examples of different instances, operations, and tactics:

- In the town of Gori, Georgia, Russians disabled government and news websites with DDoS attacks prior to an air attack to infiltrate news coverage.
- Cyber operations mainly focused on DDoS, but they also included website defacements. There were also significant levels of email spamming.
- To fake or hide their identity, Russian attackers routed their assault through foreign servers IP addresses and created false/spoofed IP addresses.
- Some websites from Russia such as www.stopgeorgia.ru provided instructions and downloads for hackers on how to join the attack.

Cyber Operations in Estonia

Cyber operations in Estonia in 2007 are believed to be connected with Russia hackers or Russia local supporters in Estonia. No physical damages were reported, however, there was economical loss by business activities relying on the Internet. Most of the attacks were DDoS and Spam attacks. The direct result of the cyber-attacks was the creation of NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) in Tallinn, Estonia.

Sony Hack in 2014

An important amount of private data was stolen from Sony and released publicly in November 2014. The data included personal information about employees and their families, emails, etc.

The hackers (called themselves: Guardians of Peace (GOP)) demanded the cancellation of the release of the film "The Interview." As such it is believed that North Korea sponsored the attack. The US-CERT stated that attackers used a Server Message Block (SMB) Worm to conduct attacks against Sony.

Democratic National Committee Hack in 2016

WikiLeaks website leaked thousands of emails and attachments from the Democratic National Committee (DNC) during the campaign for the 2016 Democratic Party presidential primaries. In June 2016, Crowdstrike cyber security company published its conclusions that the hacking was the work of two different groups: Cozy Bear and Fancy Bear. On October 2016, US DHS and DNI affirmed that the Russian government was responsible for various hacks on DNC.

K0496: Knowledge of Operational Asset Constraints

There are different types and categories of constraints that can limit the usage of cyber operational assets. Here are few examples:

- Mission goals and needs: All activities in a cyber operation should serve initially defined operation goals. Capabilities of the assist may go beyond the goals but should be limited to serve those goals.
- Asset supporting resources required by the asset should be available to implement and maintain the asset.
- Develop the right procedures, standards, and workflows.

- The existence of the proper organizational structure, roles, and responsibilities which support implementation of the cyber operation.
- Statutory, regulatory, contractual, and supply chain collaboration requirements.
- Availability of suitable expertise and trusted partners.
- Operating environments and stakeholders.

K0497: Knowledge of Operational Effectiveness Assessment

Operational effectiveness shows the extent to which a system is capable of accomplishing its intended missions when it is used in the environment planned or expected. It can be defined as the ability "to safely and sustainably do what it is meant to do, when and where it is needed, with qualified and competent people and enabling support systems," (Mead and Kersha 2016). In security controls and operations, the implication of the need to continuously perform operational effectiveness assessment is that the existence of the right tools and assets by itself is not enough to ensure proper security control and management. Proper processes should be planned to ensure the optimization of security resources to fit mission goals and needs.

One of the important meanings of "effectiveness" is related to relevance or fitness of the cyber operation to its initial goals. Without properly and initially defining operation goals, it will be hard to assess the operation effectiveness. Transparency is also important to be able to describe in details what went wrong "weaknesses" and what went right "strengths" in each operation in order to learn and improve in future. This includes capability assessments and gap analysis in the current operations to help plan for future ones.

Operational effectiveness assessment provides the roadmap to focus efforts on those problems that hinder growth and performance. Many organizational management theories consider operational effectiveness to be a source of competitive advantage, particularly where operational effectiveness includes capabilities that enable an organization to rapidly adapt to changes in requirements or environmental factors. Organizations often approach operational effectiveness through following governance frameworks such as COBIT or quality management approaches such as Six Sigma, Total Quality Management (TQM), ISO 9004, or ISO 15504.

K0498: Knowledge of Operational Planning Processes

Operational planning refers to the yearly cycle of planning for routine operations and contingency readiness guidance which does not specifically report strategic, budget, and crisis action planning.

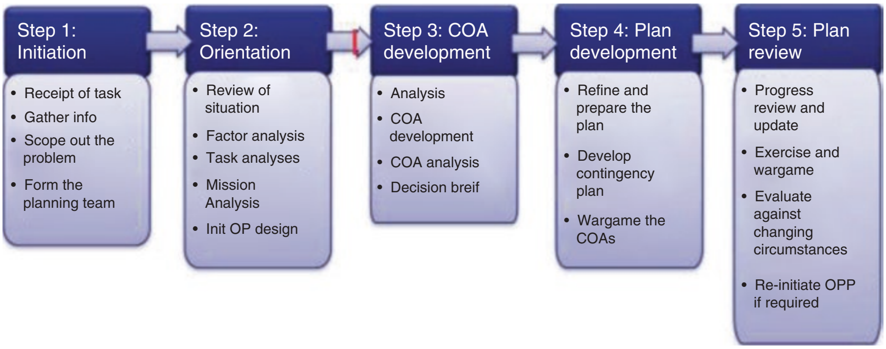


Fig. 7.8 Operational plan process (Lizotte and Derbentseva 2016)

Different cyber security management processes should be integrated and incorporated with IT strategic planning, budget planning and distribution, and different strategic and operational activities.

Cyber operation planning process as described in NATO Comprehensive Operational Planning Directive (COPD v2.4) includes (Kuusisto et al. 2015):

- Analysis of the situation.
- Assessment of the military options.
- Selection of the commander course of actions (COAs) in order to realize strategic objectives.

An operational plan process model described in (Lizotte and Derbentseva 2016) includes the following five steps (Fig. 7.8):

1. Initiation
2. Orientation
3. COA development
4. Plan development
5. Plan review

Another model of seven steps is described in (JOPP 2013).

K0499: Knowledge of Operations Security

Operations security, OpSec, OPSEC, or operational security refers to operations to deny adversaries information that could be used to do harm to an organization or individual. Some of the major goals behind OPSEC are to protect privacy and ensure anonymity.

OPSEC is a process to identify critical information and subsequently analyze friendly actions attendant to military operations and other activities to:

(a) Identify those actions that can be observed by adversary intelligence systems,

(b) Determine indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information that can be useful to adversaries,
(c) Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation (DOD JP 1994; JCS 1997).

OPSEC as a methodology originated during the Vietnam War. A group of individuals was assigned to find out how the enemy was obtaining advance information on certain combat operations (AGLearn 2018). One difference between cyber and operations security is that cyber security focuses on protecting our systems and networks while OPSEC focuses on protecting our unclassified critical information and indicators (Magdalenski 2016).

Defenders as well as attackers utilize OPSEC (Holland 2016). Attackers use OPSEC to: (1) avoid detection, (2) maintain availability of compromised assets and environments. Two examples of cases that indicate attackers' failures to protect their anonymity and avoid detection: Moldovan hacker Andrey Ghinkul (2016–2017) for the "Bugat" malware. His mistake was through associating his real name with nick name (Holland 2016). The second case is for hacktivist Sabu (Leyden 2012) who has been cautious in most of his activities. "But then just once he slipped. He logged into an Internet relay chatroom from his own IP address without masking it," (Leyden 2012).

OPSEC can be assessed through a thorough evaluation of the effectiveness of an organization implementation of OPSEC methodologies, resources, and tools. Assessments (a) are used to evaluate the effectiveness of the organization OPSEC program and (b) can be used at the program level to determine whether or not a program is a viable candidate for an OPSEC survey (OPSA 2018).

According to NIST SP 800–53 (Security and Privacy Controls for Information Systems and Organizations), the following security controls can deal with OPSEC:

1. PM-14: An Operations Security (OPSEC) Program.

The process involves five steps (Fig. 7.9, AGLearn 2018): identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

2. SC-40: OPSEC Safeguards to Protect Key Organizational Information

OPSEC safeguards are applied to both organizational information systems and the environments in which those systems operate. They help protect the confidentiality of key information.

3. AC-22 Publicly Accessible Content

The organization should:

(a) Designate individuals authorized to post information onto a publicly accessible information system.

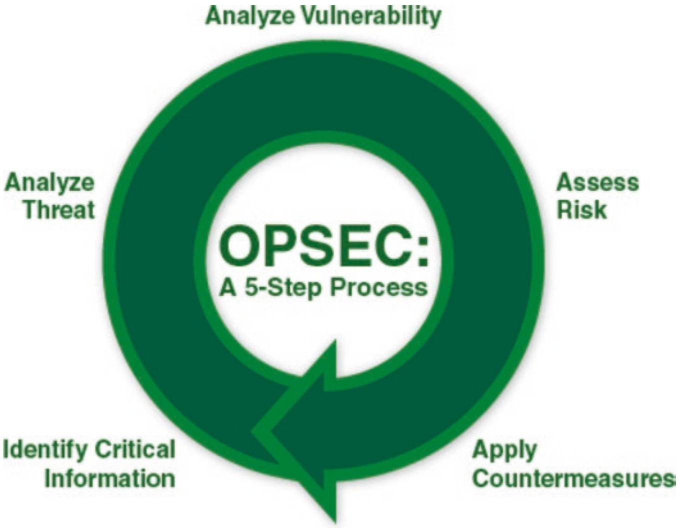


Fig. 7.9 OPSEC steps (AGLearn 2018)

(b) Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information.
(c) Review the proposed content of information prior to posting onto the publicly accessible information system to ensure nonpublic information is not included.
(d) Review the content on the publicly accessible information system for nonpublic information [Assignment: organization-defined frequency] and removes such information, if discovered.

NIST manual NIST SP 800–53 lists critical information to be protected under OPSEC: AC-21, CA-2, CA-3, CA-5, CM-2, CM-3, CM-4, CM-8, CP-2, CP-2(8), CP-9, CP-9(3), PE-18, PL-2, RA-3, RA-5, SA-5, SA-14, SA-15, SA-15(3), SA-15(4), SA-15(5), SI-2 (Refer to NIST manual for names and details on those information).

NIST manual NIST SP 800–53 also lists OPSEC Indicators of compromise: AC-22, AU-6, AU-6, AU-13, CA-7, PE-19, SI-4, SI-4(8), SI-4(13), SI-4(17), SI-4(18), SI-4(19), SI-4(20), (Refer to NIST manual for names and details on those information).

NIST manual NIST SP 800–53 also lists OPSEC countermeasures: AC-3, AC-4, AT-2, AT-2(2), AT-3, CM-5, CM-5(1), CM-5(4), CP-12, CP-13, IR-4, IR-4(6), IR-4(7), IR-9, MA-6, PE-3, SA-12, SA-12(1), SA-12(9), SA-12(14), SA-18, SA-19, SC-4, SC-5, SC-5(1), SC-7, SC-7,(9) SC-7(10), SC-7(16), SC-8, SC-9, SC-11, SC-12, SC-13, SC-14, SC-26, SC-28, SC-29, SC-30, SC-30(2), SC-30(3), SC-30(4), SC-30(5), SC-31, SC-32, SC-35, SC-36, SC-38, SC-39, SC-39(1), SC-41, SC-42, SI-6 (Refer to NIST manual for names and details on those information).

K0503: Knowledge of Organization Formats of Resource and Asset Readiness Reporting, Its Operational Relevance and Intelligence Collection Impact

The goal of readiness reporting or assessment system is to reveal whether personnel/systems are prepared to perform their assigned missions. The Defense Readiness Reporting System, describes a process beyond the standard resource accounting approach of traditional readiness reporting by providing assessments of organization's ability to conduct assigned tasks either in the context of their core mission or assigned operations (DoD 2011). One of the methods that is used to evaluate and track progress is a Language Readiness Index (LRI) that is used to measure DoD's ability to meet prescribed language missions. DoD DRRS encompasses automated, near real-time readiness reporting systems that provide current readiness status for operational forces and defense support organizations in terms of their ability to perform their METLs (DoD 2018a, b). Under title 10, DoD DRRS should be able to measure personnel readiness in an objective, accurate, and timely manner. DODD7730.65 establishes a capabilities-based, adaptive, near real-time readiness reporting system.

Mission Essential Task Lists METL is an operational readiness construct that describes capabilities for assessment and reporting of readiness to conduct the missions prescribed. A METL consists of METs (Tasks based on mission analysis) with associated conditions and standards and appropriate supporting tasks. METLs can guide the key collective tasks that training can be selected from. METL can also help to assess mission readiness whether an organization can accomplish some specific tasks under some specific conditions to meet some specific standards.

CJCS Instruction (CJCSI) 3401.02B, force readiness reporting establishes the following P-level readiness assessment metrics: total available strength, critical personnel, and critical grade fill cyberspace workforce readiness (Usrey 2014).

K0519: Knowledge of Planning Timelines Adaptive, Crisis Action, and Time-Sensitive Planning

Operations developed during time-sensitive mission planning are usually follow-on targets. Time-sensitive target types include emerging and increasing value targets.

Time-sensitive planning refers to planning for the deployment of allocated forces and resources that occurs in response to an actual situation. Contingency targeting and mission planning can be deliberate or time sensitive:

1. Deliberate: In peacetime, deliberate planning procedures are used to evaluate anticipated future situations to which militarily response is expected. While deliberate planning is conducted in anticipation of future events, there are always situations arising/changing.

2. Time-sensitive planning: Events may occur that are weighed as significant to national security and require national response. These time-sensitive situations may generate crisis action planning (CAP). Crisis and combat mission planning are normally time sensitive (Joint Publication 3-05.5 1993).

We described in an earlier KSA (K0400) CAP phases. Deliberate planning has three main phases: (1) Initiation, (2) Concept Development, and (3) Plan Development. Deliberate planning phases 1 and 2 correspond roughly to CAP phases 1 through 4. Deliberate planning phase 3 corresponds roughly to CAP phase 5. The key differences between deliberate and CAP are:

- Time sensitivity and
- Probability of implementation

Similar to CAP incident planning is also time sensitive that occurs to direct or coordinate the response to imminent or ongoing incidents and events.

Time sensitivity can be associated with the target or the mission (Joint Publication 3-05.5, 1993). A target is time sensitive when it requires an immediate response because it poses a real danger. Those targets are possible mobile and time is key to eliminate them. A mission is time sensitive when there is an operationally a small-time window during which the objective of the mission must be accomplished.

K0572: Knowledge of the Functions and Capabilities of Internal Teams that Emulate Threat Activities to Benefit the Organization

Cyber security teams play both defense and offense roles. In most cases, their defense roles are more visible and important. Software defense team may not only spend their time testing for assets vulnerabilities and make sure to eliminate them, but they also act as their adversary offensive teams to see if they can exploit friends' systems and assets.

From knowledge and skills' perspectives, most of the tools used in ethical hacking, white hacking, and penetration testing are also candidate tools for hacking and offense. The major different between black and white hacking is the intention from using the different tools to test for vulnerabilities and exploit them or patch them. To use their abilities for good, ethical, and legal purposes rather than for bad, unethical, and criminal purposes.

Defense teams may exploit vulnerabilities and bring some services down, part of partially or fully disclosed exercises; however, the intention again is not to expose and utilize those exploits but rather to bring more attention to security risks.

White hackers can be internal company employees or they can be sub-contracted to do this occasionally. There are several levels of penetrating testing, vulnerability, and exploit activities. The two teams (i.e., organization and security testing team) should agree on all details before the initiation of the process.

Bug Bounty Programs

In the large national-level scale, large teams of cyber warriors and white or ethical hackers can test for or emulate threat activities. In a contest in 2017 that is called "Hack the Air Force," US military invited hackers through a contest to hack some of its websites. Hackers are requested first to create an account and be vetted through the website (hackerone.com). This is the third in a series of similar contests: "Hack the Pentagon" and "Hack the Army contests," (Greene 2017).

White-hat hackers sometimes work as freelancers. One of the popular examples is the case of Sandeep Singh known as "Geekboy." He finds vulnerabilities in companies and reports them, and companies on return paid him for such services (CBS News 2017).

In a project to crowd source vulnerability discovery, US IRS awarded Synack (https://www.synack.com/government/) a $two million contract to provide penetration testing through ethical hackers or researchers who have no knowledge of IRS systems.

In the private sector, Bug bounty programs have been implemented by several large organizations, including Mozilla, Facebook, Yahoo!, Google, Reddit, Square, [8] and Microsoft.

Open Bug Bounty is another popular website or platform for non-profit white-hat hackers: https://www.openbugbounty.org/. For black-hat hackers, they share and exchange exploit information through the dark web and other cyber-arms industry outlets.

K0585: Knowledge of the Organizational Structure as It Pertains to Full Spectrum Cyber Operations, Including the Functions, Responsibilities, and Interrelationships Among Distinct Internal Elements

Teams Employment Category

In the USA and most other countries, a debate exists in terms of hiring in the cyber and intelligence fields whether hired members should be part of the military, government sectors, private sectors or citizens, contractors, etc. Each category can have its strengths and weaknesses in terms of, for example, cost, security clearance, sensitivity of information and mission, etc.

US cyber command team is divided across five different functional types of teams: National Mission (NMT), National Support (NST), Combat Mission (CMT), Combat Support (CST), and Cyber Protection (CPT) (Barth et al. 2015). Each team members can come from different employment category: military, civilian, contractor, or NSA. Figure 7.10 shows distribution in numbers for NMT team (Barth et al. 2015).

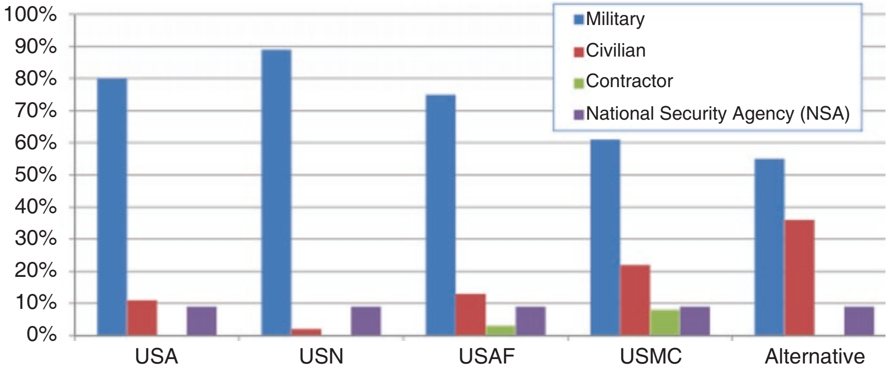


Fig. 7.10 NMT team employment distribution (Barth et al. 2015)

In terms of employment category, several factors impact the selection such as mission criticality, availability of personnel/skills, and cost. For example, civilians tend to generally have the least in percentage in the teams while they cost the least in terms of salary, etc. (Barth et al. 2015).

Organizational Structure

Another dimension to consider is related to the organizational structure and its impact on cyber operations and missions.

US cyber command five teams described earlier represent one organizational structure on how to distribute cyber operations' workforce. Those five teams are evenly distributed across US three major armed forces: Army, Air force, and Navy. Each of the services had different approaches to organizing and has different views on how to build the cyber structure. This is influenced by each service's organizational culture and bureaucratic tendencies (Riddle 2016).

The five teams have different functionalities and hence their skills, tools, and capabilities are expected to be different.

There are several challenges related to allocating the "best" team to the mission. One major issue is the availability of proper skills. Clearly, this area is of high demand in the public and private sectors. Additionally, for high and mastery levels, long time of training and experience are expected. The type and nature of skills vary rapidly in the cyber world and each mission can have or expect different or unique type of skills. The ability to benchmark performance of the different teams and evaluate the success of their missions is not always trivial or each to assess.

The decisions whether to centralize or decentralize cyber operation teams can have strengths and weaknesses in both models and architectures. The main disadvantage of a centralized architecture is related to response time especially in cases of time-sensitive operations.

Many models can be hybrid where some tasks can be centralized. For example, recruitment, HR, and training can be centralized for the different teams.

K0588: Knowledge of the Priority Information Requirements from Subordinate, Lateral, and Higher Levels of the Organization

Priority information requirements (PIRs) refer to information that intelligent team must be aware of as soon as it is known (Shakarian et al. 2013). PIR directs intelligent gathering operation as it indicates what information is more important to the mission.

Good selection of PIRs should have the following criteria (Bautista 2018):

- Focused, ask only one question on specific event, fact, or activity.
- Provide an intelligence to support a single decision.

Master information requirements includes priority, active and inactive information requirements, Fig. 7.11 (Bautista 2018).

During operations, collection manager manages hundreds of individual information requirements. This number would also include the intelligence requirements to support targeting, lower priority information requirements, requests for information from subordinate units, or taskings from higher commanders (Spinuzzi 2007).

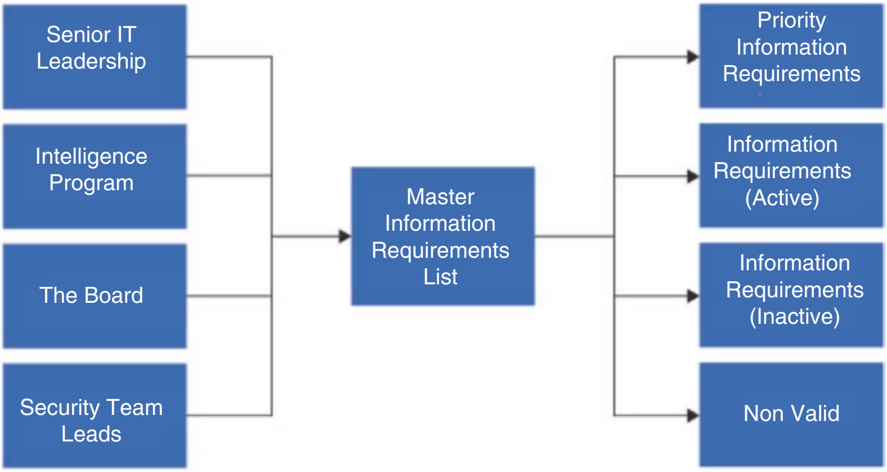

Senior IT Leadership
Intelligence Program
The Board
Security Team Leads
Master Information Requirements List
Priority Information Requirements
Information Requirements (Active)
Information Requirements (Inactive)
Non Valid

Fig. 7.11 Master information requirements list (Bautista 2018)

K0589: Knowledge of the Process Used to Assess the Performance and Impact of Operations

Cyber operations' performance or impact analysis varies based on the nature of the cyber-attacks or missions or operations (e.g., defensive or offensive). For example, the following cyber analysis activities can be used in cyber operations assessment (Kott et al. 2015):

- Detect attacks in a mission-supporting manner.
- Assess damages relevant to the mission: Forensic tools are important to understand the attack, attackers, and assess damages.
- Investigate impacts on mission elements.
- Recover from attacks.
- Decide on how to respond to cyber-attacks to maximize mission success.
- Evaluate different possible mitigation alternatives.

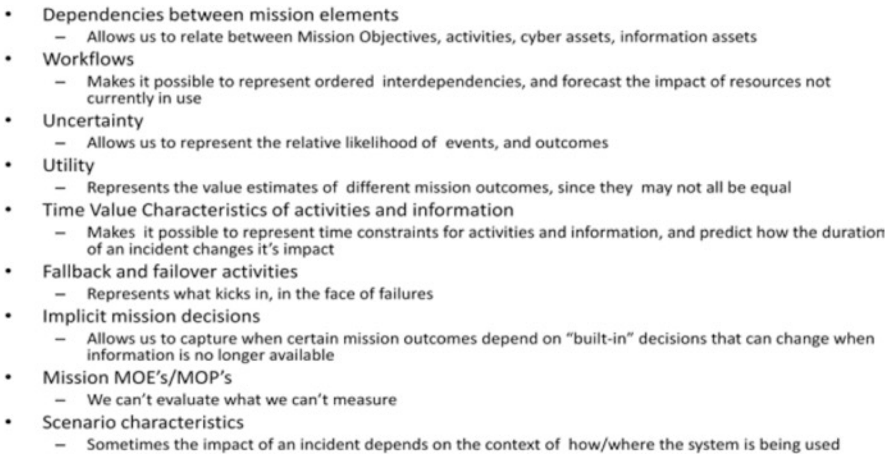
Kott et al. (2015) discussed different models to cyber operations' impact analysis (COIA) such as: risk analysis problem, control theoretic style, game theoretic, reverse engineering, malware analysis, and adversary modeling. In studying cyber operations' impact analysis, we should not also ignore the dimensions related to understand humans' behavior; whether those are the defenders or the attackers. Cognitive modeling and tools such as Adaptive Control of Thought—Rational (ACT-R) can be used to model attackers' behaviors. Kott et al. (2015) mentioned two particular models that can be utilized in COIA, namely: Canadian Automated Computer Network Defense (ARMOUR) demonstrator and European Union PANOPTESEC.

In a COIA model by MITRE (www.mitre.org), the model described several model requirements through which assessment can be thorough and accurate, Fig. 7.12, (Musman et al. 2009). This model is an example of a data-flow representation.

Extending MITRE Cyber Mission Impact Assessment (CMIA) Tool, AMICA model combines process modeling, discrete-event simulation, graph-based dependency modeling, and dynamic visualizations (Noel et al. 2015). Jakobson (2011) proposes an impact dependency graph, Fig. 7.13.

K0593: Knowledge of the Range of Cyber Operations and Their Underlying Intelligence Support Needs, Topics, and Focus Areas

A cyber threat intelligence process must be able to accommodate both, supporting not only tactical security operations but also informing the organization's strategic goals.



- Dependencies between mission elements
  - Allows us to relate between Mission Objectives, activities, cyber assets, information assets
- Workflows
  - Makes it possible to represent ordered interdependencies, and forecast the impact of resources not currently in use
- Uncertainty
  - Allows us to represent the relative likelihood of events, and outcomes
- Utility
  - Represents the value estimates of different mission outcomes, since they may not all be equal
- Time Value Characteristics of activities and information
  - Makes it possible to represent time constraints for activities and information, and predict how the duration of an incident changes it's impact
- Fallback and failover activities
  - Represents what kicks in, in the face of failures
- Implicit mission decisions
  - Allows us to capture when certain mission outcomes depend on "built-in" decisions that can change when information is no longer available
- Mission MOE's/MOP's
  - We can't evaluate what we can't measure
- Scenario characteristics
  - Sometimes the impact of an incident depends on the context of how/where the system is being used

Fig. 7.12 COIA model requirements (Musman et al. 2009)

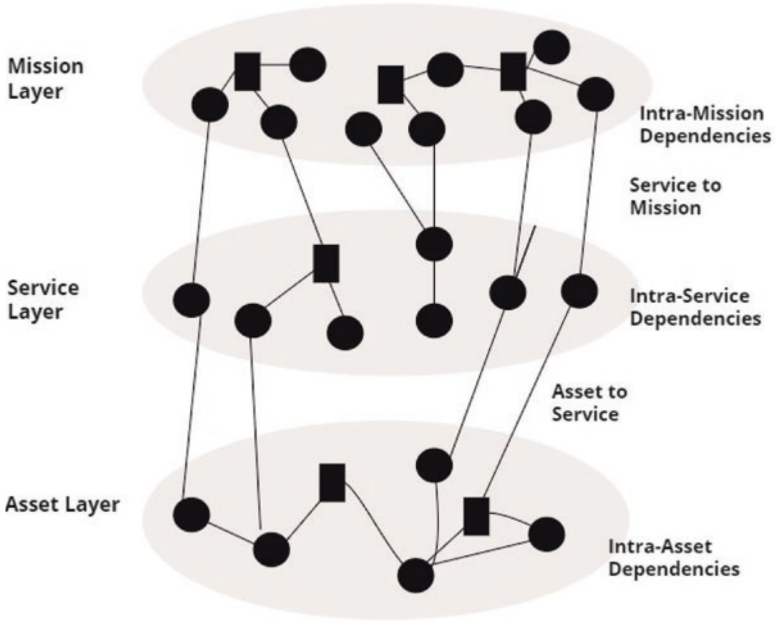


Fig. 7.13 Impact dependency graph, Jakobson 2011

DoD Joint doctrine in 2009 described four steps in intelligence preparation of operational environment (IPOE), (Lemay et al. 2014):

- Define the operational environment.
- Describe environment impact.

- Study adversaries.
- Study adversaries COAs.

Intelligence Preparation of the Cyber Environment (IPCE) is proposed in (Lemay et al. 2014) in comparison to intelligence Preparation of the Battlefield to focus on how intelligence can support cyber operations. IPCE can be considered as a form of IPOE.

"IPCE is a systematic and continuous process of analyzing: the means and motives of threat actors; your digital environment and the digital environment in which you operate; in order to understand the likely scenarios in which you will face threats, enhancing your operational resiliency," (Dartnall 2017). Dartnall described four stages in IPCE to determine: (Fig. 7.14, Dartnall 2017):

- The operational environment: This environment is generally divided into two main categories: inside organization network and outside it.
- Threat scenarios: MLCoA vs. MDCoA (Most likely and Most dangerous course of actions).
- Threat actors: who, what, where, when, how, and why.
- Influences on the environment: different types of influences (e.g., legal, social, technological).

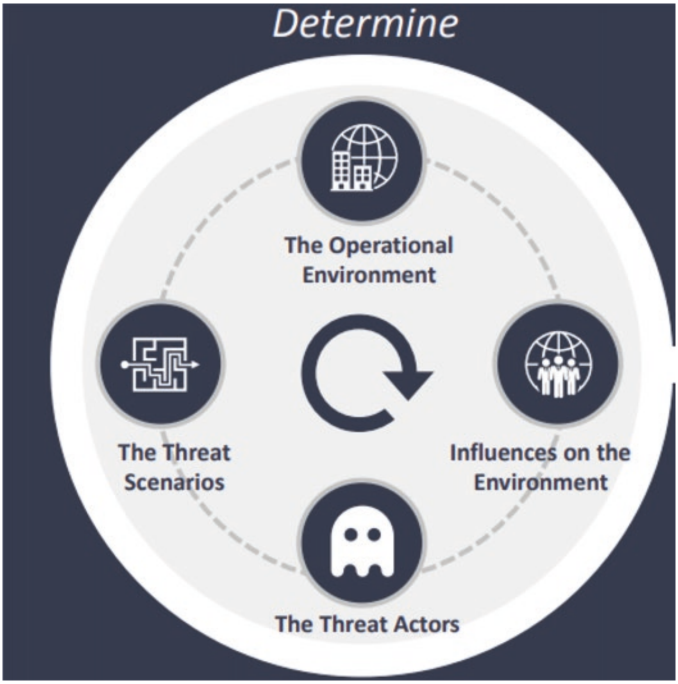


Fig. 7.14 IPCE activities (Dartnall 2017)

During cyber operation analysis, staff identifies information gaps about the adversary and other.

relevant aspects of the operational environment. After gap analysis, the staff formulates intelligence requirements (IRs), which are general or specific subjects upon which there is a need for the collection of information or the production of intelligence (Joint Publication 3-12 2018).

Intelligence support to cyberspace operations planning process includes, (Joint Publication 3-12 2018):

1. Planning and direction to include identification of target vulnerabilities to enable continuous planning and direction of cyber intelligence activities
2. Collection sensors to information about cyberspace
3. Processing and exploitation of collected data, including identification of useful information from collected data
4. Analysis of information and production of intelligence products
5. Dissemination and integration of intelligence related to cyber operations
6. Evaluation and feedback regarding intelligence effectiveness and quality

K0594: Knowledge of the Relationships Between End States, Objectives, Effects, Lines of Operation, etc

As part of cyber operations' assessment, their progress is continuously evaluated toward meeting their defined goals. Forecasted effects of the operation are compared with actual outcomes. This progress evaluation can help also decide when the operation can be terminated reaching its end state and achieving original goals or objectives.

If cyber operators can't understand cyberspace as an integral part of the OE, they cannot be expected to accurately describe end states or objectives of the cyber operation that should be aligned with mission objectives.

K0613: Knowledge of Who the Organization's Operational Planners Are, How and Where They Can be Contacted, and What Are Their Expectations

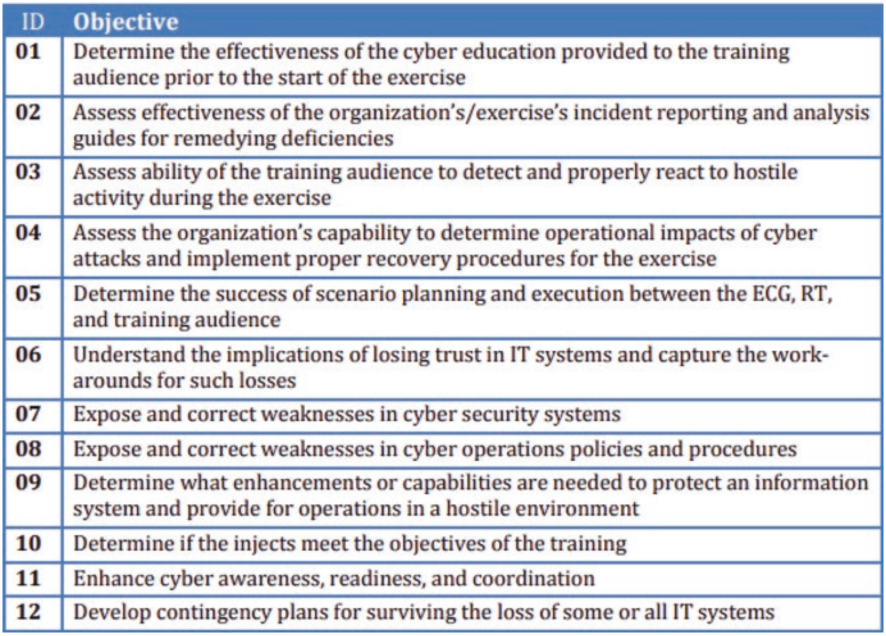
In order to conduct cyber operations planning, operational planners study the cyber threats across the three layers of cyberspace (physical, logical, and persona) to identify target system components, and possibly specific hacker sub-networks, to counter (Joint Publication 3-12 2013). Intelligence support should focus on helping operational planners to identify the requirements and vulnerabilities in the hacker's cyber-attack processes.

The tasks of operational planners are different from those of technical level planners. For example, while technical level planners need to know detail technical data about target systems, operational planners care more about the sum of impacts of adversaries and their functions (Barber et al. 2015).

S0030: Skill in Developing Operations-Based Testing Scenarios

Different cyber operations' exercises can serve different objectives. Figure 7.15 (Kick 2014) below shows a sample of cyber operation objectives that can be used to guide selected exercises.

Table 7.2 shows three styles of exercises that can be performed: table top, hybrid, and full live (Kick 2014). Those three types or styles show a balance between time to complete, knowledge and skills, complexity, required resources, etc. In reference (Kick 2014), Table 10. Sample cyber injects show different exercises that can be implemented along with each exercise objectives and outcomes. Readers are recommended to try at least one exercise from the list.



ID	Objective
01	Determine the effectiveness of the cyber education provided to the training audience prior to the start of the exercise
02	Assess effectiveness of the organization's/exercise's incident reporting and analysis guides for remedying deficiencies
03	Assess ability of the training audience to detect and properly react to hostile activity during the exercise
04	Assess the organization's capability to determine operational impacts of cyber attacks and implement proper recovery procedures for the exercise
05	Determine the success of scenario planning and execution between the ECG, RT, and training audience
06	Understand the implications of losing trust in IT systems and capture the work-arounds for such losses
07	Expose and correct weaknesses in cyber security systems
08	Expose and correct weaknesses in cyber operations policies and procedures
09	Determine what enhancements or capabilities are needed to protect an information system and provide for operations in a hostile environment
10	Determine if the injects meet the objectives of the training
11	Enhance cyber awareness, readiness, and coordination
12	Develop contingency plans for surviving the loss of some or all IT systems

Fig. 7.15 A sample of objectives for cyber operations' exercises (Kick 2014)

Table 7.2 Different possible styles of exercises (Kick 2014)

Style	Description	Complexity	Timing	Resources	Matches
Table Top	Paper-driven exercise with injects scripted by exercise planners and delivered via paper (cards/discussion)	This type of exercise can be planned and executed quickly, depending on the number of organizations involved	Planning: 1–2 months	Limited resources needed, depending on number of organizations	• Organizations new to exercises and to assessing organizational IA objectives
			Execution: 1–3 days		• Organizations that need to validate processes/train personnel in-between other exercises
Hybrid	Paper injects with some live scenarios facilitated by a RT for realism (probes, scans, e-mail spoofing, etc.)	This type of exercise requires more planning and longer execution times.	Planning: 3–6 months Execution: 3–5 days	Requires more people and time, real targets for scenarios, deconfliction contacts	Organizations familiar with inter- organization exercises and a strong knowledge of their own objectives
Full Live	Exercise plan incorporates real scenarios and injects into the exercise. Paper injects only used to stimulate if necessary	This type of exercise requires detailed coordination and planning.	Planning: 6–12 months Buildup: 2–3 months Execution: 7–14 days	Large number of organizational participants, IT resources, travel budget for meetings, deconfliction contacts	Organizations familiar with exercises, RTs, and their own organizational objectives

- There are several websites (e.g., https://www.cybercompex.org/, hackerone.com, http://www.nationalccdc.org/, www.hackthebox.eu) that post frequent national competitions on cyber operations. Reader can register and participate in one of those exercises to fulfill this skill.

S0055: Skill in Using Knowledge Management Technologies

Knowledge management is a structured and systematic process to extract learning from past activities to make better future decisions. Knowledge management processes deliver measurable benefits. We will focus in this section on examples of using machine learning (ML) techniques in cyber operations especially for cyber analysts.

A ML approach usually consists of two phases: training and testing. Often, the following steps are performed (Buczak and Guven 2016):

- Identify class attributes (features) and classes (class labels) from training data.
- Identify a subset of the attributes necessary for classification (i.e., dimensionality reduction, feature selection, etc.).
- Divide data into training and testing; learn the model using the training data.
- Use the trained model to classify the unknown data.

Some of the popular algorithms: ANN, SVM, GA, KNN, Random forest, HMM, etc.

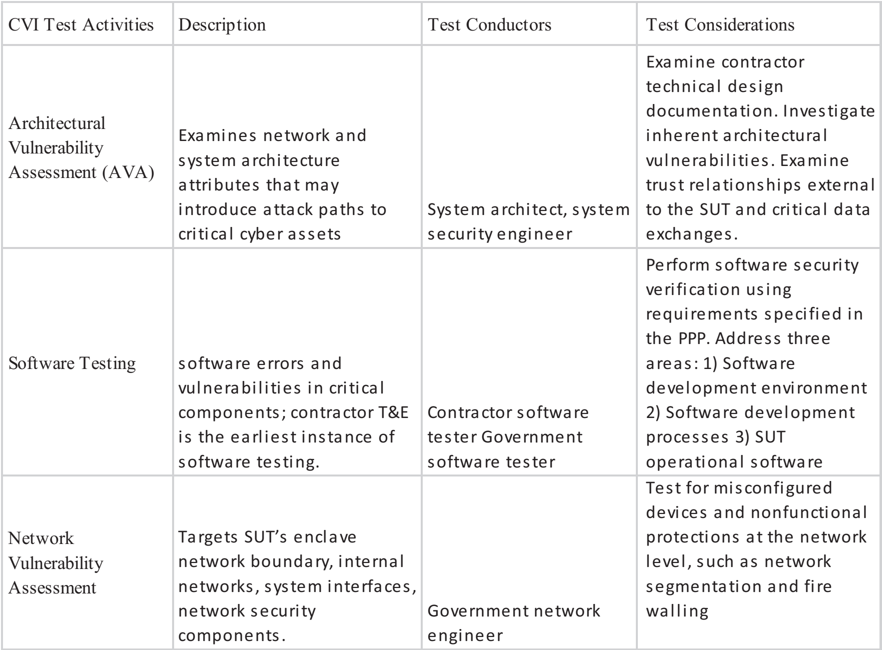
Readers are expected to learn some of the popular data mining tools such as:

- Python: One of the most popular programming/scripting languages for cyber security and data analytics. Several open source IDEs can be used to write and execute Python code such as PyCharm and Anaconda. Some of the popular Python libraries to learn in this scope: Scikit learn and TensorFlow.
- R: Of the popular GUI IDEs based on R is R-studio. Users can write scripts which utilize rich libraries built and available in R.
- Weka: A simple but popular open source GUI-based data mining tool. Libraries also exist to export Weka to Java.
- Knime (knime.com), written in Java, Knime is a free and open source data analytics' reporting and integration platform.
- RapidMiner.
- H2O.
- MATLAB/Octave.
- Julia.
- Several tools and libraries in Java (e.g., see deep learning for Java: https://deeplearning4j.org).

S0061: Skill in Writing Test Plans

Cyber Security T&E Policy in DoDI 5000.02

- The reference (DoD: dote.osd.mil 2015) includes several categories of cyber testing metrics. Readers are advised to pick different categories and use them to evaluate a system or asset from cyber defense perspectives.
- The reference (DoD: dote.osd.mil 2015) includes a table, Table 1 that shows the operational tests involving cyber security, and the DOT&E-funded cyber security assessments conducted during FY16 2016. Readers are advised to read the table and get familiar with the different operational tests listed.
- Table below from (DoD: T&E, dote.osd.mil 2018a, b) shows examples of testing activities that can be developed in security testing (Fig. 7.16).



CVI Test Activities	Description	Test Conductors	Test Considerations
Architectural Vulnerability Assessment (AVA)	Examines network and system architecture attributes that may introduce attack paths to critical cyber assets	System architect, system security engineer	Examine contractor technical design documentation. Investigate inherent architectural vulnerabilities. Examine trust relationships external to the SUT and critical data exchanges.
Software Testing	software errors and vulnerabilities in critical components; contractor T&E is the earliest instance of software testing.	Contractor software tester Government software tester	Perform software security verification using requirements specified in the PPP. Address three areas: 1) Software development environment 2) Software development processes 3) SUT operational software
Network Vulnerability Assessment	Targets SUT's enclave network boundary, internal networks, system interfaces, network security components.	Government network engineer	Test for misconfigured devices and nonfunctional protections at the network level, such as network segmentation and fire walling

Fig. 7.16 Examples of security testing activities, (DoD T&E guidebook 2018)

The main test and evaluation T&E activities conducted during the life cycle of a system are (Acqnotes 2018):

- Test and Evaluation Strategy.
- Developmental Test and Evaluation.
- Initial Operational Test and Evaluation.
- Operational Test and Evaluation.
- Follow-on Operational Test and Evaluation.
- Test and Evaluation Master Plan.
- Operational Assessment.
- Live-Fire Test and Evaluation.

S0082: Skill in Evaluating Test Plans for Applicability and Completeness

In security and vulnerability assessment in particular, testing coverage is very important to ensure that all possible weaknesses are accounted for. At the end, all what it takes for a hacker to get in is to find and exploit on vulnerability.

Applicability refers to the unique nature of every test plan and its applicable environment. Test designers should understand first the systems and domains they are testing and create test plans for those systems and domains as an alternative of using or reusing generic test plans from other systems or environments. Other terms that can be used in quality assessment related to applicability is "fitness" to refer to whether requirements and implementation fit and target initial operation goals or objectives. In terms of cyber intelligence, applicability can track the focus of intelligence activities on tasks that fit the mission and avoid losing focus by spending time and effort on collecting data that, while it can be important, is irrelevant to the specific operation mission. Detailed operational test plans should be evaluated to determine that the test-imposed conditions on the crew do not invalidate the applicability of the collected data (T&E Guide 1993).

Completeness refer to check that test plans cover all security aspects in the systems and assets under test and that no aspect is incomplete or missing.

Some of the general questions to be used as part of a checklist to answer to verify completeness (Schulmeyer 2008):

- Do the requirements specified carry out the mission in a consistent fashion?
- Do the requirements include the essential needs of the mission, users, operational, and maintenance communities?
- Does each requirement stand alone or have clearly stated dependencies?
- Is the requirements document complete with all TBDs eliminated?
- Are any requirements missing?
- Are necessary requirements distinguished from those "add-on" requirements?

S0104: Skill in Conducting Test Readiness Reviews

A Test Readiness Review (TRR) is conducted to determine if the system under review is ready to proceed into formal testing by deciding whether the test procedures are complete and verify their compliance with test plans and descriptions, ((TRR), AcqNotes 2017).

- The checklist excel file in (DoD Test Readiness Review (TRR) Risk Assessment) from the reference (test readiness review (TRR), AcqNotes 2017) includes several questions to be answered as part of TRR. Review and answer those questions while selecting a particular context.
- In an experiment or system of your choice, answer the question in the section (the TRR should answer the following questions) in the reference: ((TRR), AcqNotes 2017).

Bibliography

AcqNotes (2018) Test & evaluation overview. acqnotes.com

AGLearn (2018) Operations Security. https://aglearn.usda.gov/customcontent/APHIS/APHIS-OPSEC/OPSsummary.htm

Alsmadi I, Burdwell R, Aleroud A, Wahbeh A, Al-Qudah MA, Al-Omari A (2018) Practical information security. Springer, Berlin

Arnold JT (2012) The shoreline: where cyber and electronic warfare operations coexist. BiblioScholar

Balaish T (2017) Cyber soldiers: White-hat hackers, *CBS News*, 21 Aug 2017

Barber DE, Alan Bobo T, Sturm KP (2015) Cyberspace operations planning: operating a technical military force beyond the kinetic domains. J Military Cyber Professionals Assoc 1(1)

Barth TH, Horowitz SA, Kaye MF, Wu L (2015) Staffing Cyber Operations (Presentation). Institute For Defense Analyses, Alexandria, VA

Bautista W (2018) Practical cyber intelligence: how action-based intelligence can be an effective response to incidents. Packt, Birmingham

Buchanan B (2018) CWPC contingency wartime planning course, global security

Buczak AL, Guven E (2016) A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun Surveys Tutorials 18(2):1153–1176

CBS News (2016) http://www.cbsnews.com/news/fbi-paid-more-than-1-million-for-san-bernardino-iphone-hack-james-comey/

Cho J-H, Alsmadi I, Xu D (2016) Privacy and social capital in Online Social Networks, Global Communications Conference (GLOBECOM), IEEE. pp 1–7. Accessed 12 Apr 2016

CI Glossary – Terms & Definitions of Interest for DoD CI Professionals (2 May 2011), Deffense intelligence agency, https://www.dni.gov/files/NCSC/documents/ci/CI_Glossary.pdf

CRS (2015) Cyber Operations in DOD Policy and Plans: Issues for Congress, Congressional Research Service, 7–5700, www.crs.gov, R43848

Cyber Operations Personnel Report (2011) Department of Defense, Report to the Congressional Defense Committees

D’Aspremont J (2016) Cyber operations and international law: an interventionist legal thought. J Conflict Security Law 21(3):367–368

Dartnall R (2017) Intelligence preparation of the cyber environment. sans.org

Defense Information Systems Agency (2016) DOD Cloud Computing Strategy Security Requirements Guide, Version 1, Release 2, Mar 18

Deliberate and Crisis Action Planning (2007) A presentation. www.acq.osd.mil

Department of Justice (2014) U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage, May 19. http://www.justice.gov/opa/pr/2014/May/14-ag-528.html

DoD (1994) Joint tactics, techniques and procedures for noncombat evacuation operations (Joint Report 3-07.51, Second Draft). Washington, DC: Department of Defense

DoD (2010) Joint publication 1-02, Department of Defense Dictionary of military and associated terms

DoD (2011) DRRS Primer for Senior Leaders. http://www.highgroundconsulting.net

DoD (2015) Cybersecurity test and evaluation guidebook, Version 1, dote.osd.mil

DoD (2018a) Department of Defense Readiness Reporting System (DRRS)

DoD (2018b) Cybersecurity test and evaluation guidebook, Version 2. dote.osd.mil

FY16 Cybersecurity (2016) dote.osd.mil

GAO (2017) Defense cyber security, DOD’s monitoring of progress in implementing cyber strategies can be strengthened, GAO-17-512

Goldsmith J (2010) Can we stop the cyber arms race? *WASH POST*, Feb 1, 2010, at A17

Greene T (2017) U.S. military wants white-hat hackers to target its cyber security systems ‘Hack the Air Force’ invites vetted attackers to test its public web sites, network world. Accessed 27 Apr 2017

Heckman KE, Stech FJ, Schmocker BS, Thomas RK (2015) Denial and deception in cyber defense. Computer 48:36–44. https://doi.org/10.1109/mc.2015.104

Hilfiker JL (2013) Responding to cyber attacks and the applicability of existing international law, United States Army War College. http://www.dtic.mil/dtic/tr/fulltext/u2/a589333.pdf

Holland R (2016) The OPSEC Opportunity. https://www.digitalshadows.com/blog-and-research/the-opsec-opportunity/. Accessed 31 May 2016

Jakobson G (2011) Mission cyber security situation assessment using impact dependency graphs. In: Proceedings of the 14th International Conference on Information Fusion (FUSION), pp 1–8

Joint Pub (1999) Joint task force planning guidance and procedures. https://www.hsdl.org/?abstract&did=771543

Joint Publication 3-05.5 (1993) Joint special operations targeting and mission planning procedures. Accessed 10 Aug 1993

Joint Publication 3-12 (2013) Cyberspace Operations, Joint Publication 3-12 (R). Accessed 5 Feb 2013. fas.org

Joint Publication 3-12 (2018) Cyberspace operations Accessed 8 Jun 2018

JOPP (2013) Joint operational planning process workbook, NWC 4111J, JMO Department, Naval War College, 1 July 2013 (With Chg1)

Kick J (2014) Cyber exercise playbook. The MITRE Corporation, McLean, VA

Klann G (2003) Crisis leadership: using military lessons, organizational experiences, and the power of influence to lessen the impact of chaos on the people you lead. Center for Creative Leadership, Greensboro, NC

Kott A, Stoianov N, Baykal N, Moller A, Sawilla R, Jain P, Lange M, Vidu C (2015) Assessing Mission impact of cyberattacks: report of the NATO IST-128 Workshop, ARL-TR-7566, Dec 2015

Kott A, Ludwig J, Lange M (2017) Assessing Mission impact of cyberattacks: toward a model-driven paradigm. IEEE Security Privacy 15(5):65–74. https://doi.org/10.1109/MSP.2017.3681068

Kuusisto T, Kuusisto R, Roehrig W (2015) Situation understanding for operational art in cyber operations. 14th European conference on cyber warfare and security, ECCWS

Lemay A, Knight S, Fernandez J (2014) Intelligence preparation of the cyber environment, finding the high ground in cyberspace. J Inform Warfare 13(3)

Leyden J (2012) The 'one tiny slip' that put LulzSec chief Sabu in the FBI's pocket Well, at least this'll make a half decent movie, https://www.theregister.co.uk/2012/03/07/lulzsec_takedown_analysis/. Accesssed 7 Mar 2012

Lizotte M, Derbentseva N (2016) Collaborative understanding of complex situations A Toolbox for Multidisciplinary Collaboration (TMC), Defense Research and Development Canada Scientific Report DRDC-RDDC-2016-R057, April 2015

Long A (2017) A cyber SIOP? Operational considerations for strategic offensive cyber planning. J Cybersecurity 3(1):19–28

Magdalenski J (2016) Operations Security or Cybersecurity? http://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=7377

Mahvi AJ (2018) Strategic offensive cyber operations: capabilities, limitations, and role of the intelligence community. In: Kosal M (ed) Technology and the intelligence community. Advanced sciences and technologies for security applications. Springer, Cham

Mead J, Kersha D (2016) Shaping defense science and technology in the maritime domain 2016–2026. www.dst.defence.gov.au

Musman S, Temin A, Tanner M, Fox D, Pridemore B (2009) Evaluating the impact of cyber attacks on missions. MITRE, McLean, VA

Musman S, Temin A, Tanner M, Fox D, Pridemore B (2010) Evaluating the impact of cyber attacks on missions. 5th international conference on information warfare and security

NATO (2013) Cooperative Cyber Defense Centre of Excellence (CCDCOE), 'The Tallinn Manual'. http://www.ccdcoe.org/249.html. Accessed 12 Sep 2013

NATO (2016) Social media as a tool of hybrid warfare. NATO StratCOM COE

Noel S, Ludwig J, Jain P, Johnson D, Thomas R, McFarland J, King B, Webster S, Tello B (2015) Analyzing mission impacts of cyber actions. In: Proceedings of the NATO IST-128 workshop on cyber attack detection. Forensics and Attribution for Assessment of Mission Impact, Istanbul

OPSA (2018) Operational security professional's association, https://www.opsecprofessionals.org/terms.html

Rid T (2013) Cyber war will not take place. Oxford University Press, New York, p 32

Riddle BJ (2016) Army cyber structure alignment. Air University, Maxwell, AFB, AL

Schmitt MN (2013) Tallinn manual on the international law applicable to cyber warfare. Cambridge University Press, New York, NY, pp 6–19

Schmitt MN (2017) Peacetime cyber responses and wartime cyber operations under international law: an analytical Vade Mecum. Har Nat Sec J 8:239–282

Schulmeyer G (2008) Handbook of software quality assurance, 4th edn. Artech House, Norwood, MA

Shakarian P, Shakarian J, Ruef A (2013) Introduction to cyber warfare. Elsevier, Amsterdam

Spinuzzi MA (2007) CCIR for complex and uncertain environments. School of Advanced Military Studies, Leavenworth, KS

Steiner H (2017) Cyber operations legal rules and state practice. Authority and control in International Humanitarian Law. Stockholm University

T&E Guide (1993) Test and evaluation management guide, defense systems management college

Test Readiness Review (TRR), AcqNotes (2017) http://acqnotes.com/acqnote/acquisitions/test-readiness-review

Theohary CA, Harrington AI (2015) Cyber Operations in DOD Policy and Plans: Issues for Congress. Congressional Research Service, Washington, DC. https://pdfs.semanticscholar.org/73f1/5e0fb26f8ad007_d1f8257651fd04f45691e8.pdf. Accessed 25 Oct 2016

U.S. Joint Chiefs of Staff (2015) "Cyberspace Operations" Joint Publication 3-12(R). US Joint Chiefs of Staff, Washington, DC. Accessed 3 Feb 2015

Underwood K (2018) DHS builds mobile defenses. The cyber edge, July 1, 2018

United States, Joint Chiefs of Staff (1997) DOD Dictionary of Military Terms and Associated Terms. Joint Publication 1-02. Washington, DC: JCS

US Naval War College (2014) Maritime component commander guidebook

Usrey J (2014), Changing personnel readiness reporting to measure capability, Army sustainment

Wrange P (2014) Intervention in National and Private Cyber Space and International Law. In: Ebbesson J, Jacobsson M, Klamberg MA (eds) International law and changing perceptions of security. Brill Academic, Leiden

Chapter 8
Cyber Policy and Strategy Management

Strategy management is defined as a procedure to determine the relationship between the organization and its environment through the use of selected objectives and resources allocation, which allow the development of efficient and effective action programs (Schendel and Hatten 1972).

Cyber policies for states, public and private organizations represent an important step toward safe and trusted networks.

K0065: Knowledge of Policy-Based and Risk-Adaptive Access Controls

Policy-based access control (PBAC) is a digital security method or architecture that uses digital policies, comprised of rules, to guide authorization or access control decisions.

PBACs exist in different forms in most of information systems. For example, operating systems that have active directories of users and their privileges represent one form of PBACs. Similar models can be found in DBMSs, web servers, etc. Most of distributed and client server applications include PBACs to define and specify rules and permissions for the different users.

At the network level, routers, firewalls, switches, etc. have also their own models of PBACs. Some of the major advantages to have PBACs (Cox 2011):

- Define dynamically defined privileges.
- Provide risk-adaptive capabilities.
- Fine-grained authorization.
- Balance the need to know and the need to share.

Access controls (also called authorization) represent one of the main security controls in systems and assets. In comparison with authentication and identity

I. Alsmadi, *The NICE Cyber Security Framework*,
https://doi.org/10.1007/978-3-030-02360-7_8

management, which usually represents the first layer of defense, access control typically exists as the second layer of defense. In access controls, different users are given different levels of access and control on resources based on their roles. Generally, there are four main architectures of access controls that can be used to control access on resources (more details on those architectures will be covered in other sections of the book):

- Object or attribute-based access control (OBAC or ABAC). The most recent access control architecture. Both show fine-grained details and abilities to control access on resources in comparison with the rest of access control architectures. XACML represents the most popular ABAC implementation utilizing the popular XML standard (Fig. 8.1).
- Role-based Access Control (RBAC) is determined by system policies and user-role assignments.
- Mandatory Access Control (MAC) is a rule-based system for restricting access.
- Discretionary Access Control (DAC) allows users to manipulate access settings of objects under their control.

Adaptive access controls refer to access control architectures that have the capability to support policies that can change. The system should be flexible to be able to dynamically grant and provoke privileges based on certain real-time context attribute values. For example, an IT or network administrator can have administrator privileges that give them granted access to most system resources. An adaptive access control system should be able to revoke that privilege, one time in a certain context, if that administrator violated one system policy. Risks are defined based on many factors. An adaptive access control should be able to make different access

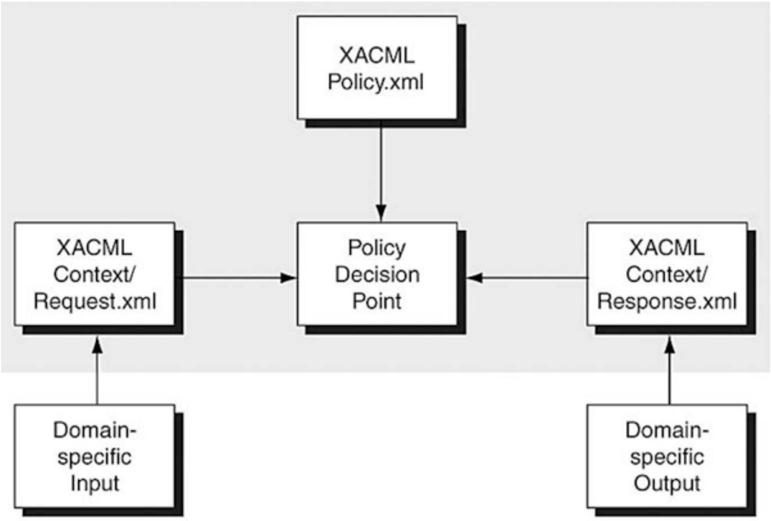


Fig. 8.1 XACML general architecture (Steel et al. 2009)

control decisions based on the overall situation risk assessment. For example, the same user on the same resource can be granted in one context and denied in another based on the different risk assessments in the two cases.

In one example of an adaptive access control, Critically Aware Access Control (CAAC) is introduced as an adaptive access control mechanism for emergency management in smart environments based on RBAC (Venkata Subramanian et al. 2014).

K0191: Knowledge of Signature Implementation Impact

There are several methods which antivirus scanners can use to identify malwares:

- Signature-based detection: To identify malwares, AV compares the contents of a file to its database of known malware signatures.
- Heuristic-based detection: Detects malware based on characteristics typically used in known malwares.
- Behavioral-based detection: This is based on the behavioral aspects of the malware at run time. This technique can detect (known or unknown) malware based on their behaviors.
- Data mining techniques: Data mining and machine learning algorithms are used to try to classify the behavior of a file or an http link (as either malicious or benign) given a series of extracted features.

Scanners of antiviruses or anti-malwares search files or packets using a set of predefined signatures to determine if those files or packets are malicious. Those signatures are the known, from previous knowledge, patterns of malicious files. Some signatures can represent simple pattern-matching techniques (e.g., finding a specific string, CRCs (checksums), or MD5 hashes). Those simple signatures may work in some cases. Other fuzzy logic-based signatures, such as applying the CRC algorithm on specific chunks of data (as opposed to hashing the whole file), can also identify various files (Koret and Bachaalany 2015).

Most notable AV signatures include (Koret and Bachaalany 2015):

- Byte-streams: The simplest form of an antivirus signature is a byte-stream that is specific to a malware file.
- Checksums: The most typical signature-matching algorithm is used by almost all existing AV engines and is based on calculating CRCs.
- Cryptographic hashes: A cryptographic hash function generates a "signature" that univocally identifies one buffer and just one buffer, which thus reduces producing a false-positive result.
- Fuzzy hashing: A fuzzy hashing signature is the result of a hash function that aims to detect groups of files instead of just a single file, such as the cryptographic hash functions' counterparts do.

K0248: Knowledge of Strategic Theory and Practice

Strategic theory is a method of analysis that can be used to assist in the comprehension of decision-making. It is used to refer to anything from governments' policies to personal choices. Some of the public researchers in strategic theories include: Thomas Schelling, John Boyd and Colin Gray. Gray argues that cyberwar can benefit from strategic theories tailored for the realisms of behaviors (Gray 2007, 2013).

Strategic theory not only describes, organizes, and explains a body of knowledge, but also it guides actions.

Strategic theory prompts us to consider the costs and risks of our decisions and weigh the consequences of those of our adversaries and friends (Yarger 2006).

High-quality strategic theory about cyber security was a challenge especially due to the technical nature of such strategies, if exist. A related term in cyber is: "Cyber power." Cyber power is "the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power," (Kuehl 2009). However, this definition has offensive-minded focus on cyber-related activities. This is expected as cyber power theories are still in their infant stages. Cyber power theories should evolve to consider full spectrum (defensive and offensive) capabilities, (Nguyen 2017). Cyber power can be an effective act of war even though physical or military forces cannot be generated directly from networked computers. Cyber warfare is the fifth domain of warfare joining land, sea, air, and space.

K0288: Knowledge of Industry Standard Security Models

A standard security model is the one that is widely accepted and is used in many tools and implementations.

In this section, we will cover a selection of standard security models from different security environments.

Access Control Models

We described earlier four popular access control models: ABAC/OBAC, RBAC, MAC, and MAC, each one of those have different implementations in the industry. For example:

- ABAC/OBAC: We described XACML as the most popular implementation of ABAC/OBAC.
- RBAC: Widely popular and has implementations in the different access control architectures such as access control lists (ACLs) that can be found in firewalls, switches, routers, etc.

- Discretionary access control (DAC): Different file systems use DAC to control users' access to the different files.
- Mandatory access control (MAC): Early implementations of MAC focused on multilevel security to protect military-oriented security classification levels with robust enforcement. Most of today's operating systems use DAC as their primary access control.

No access control model of those previously mentioned can be claimed as the best in all types of implementations. Certain quality attributes based on the usage of the model justify selecting one of the models in particular. For example, in many military applications two main criteria come first: confidentiality of certain information and greatly limit access to that information. For those two reasons hard-coded security in MAC is preferred. In many private companies, other quality attributes are more or as important: productivity, interorganizational data sharing, and information workflow between different. In such cases, DAC model can be a good choice. ABAC/OBAC recently evolves to take more market share especially due to its ability to limit or specific access based on more details on attributes related to (1) users who request the access, (2) accessed resources, (3) the environment, (4) the access context, etc.

ISO 27001

ISO 27001 replaced ISO 1799. Provides practical advice for how to implement security controls. Uses 10 domains to address information security management system, ISMS.

NIST SP 800–53

NIST SP 800–53: Guide for Assessing the Security Controls in Federal Information Systems and Organizations. It also describes building Effective Security Assessment Plans; NIST SP 800-53 is the functional successor to SP 800-26.

Authentication Protocols or Standards (OWASP 2017)

- OAuth: Open authorization (OAuth) is a protocol that allows an application to authenticate against a server as a user, without requiring passwords or any third-party server that acts as an identity provider.
- OpenID: OpenID is an HTTP-based protocol that uses identity providers to validate users. It allows a service provider-initiated way for single sign-on (SSO).
- SAML: Like OpenID, security assertion Markup language (SAML) uses identity providers, but unlike OpenID, it is XML based and provides more flexibility.

- FIDO: The fast identity online (FIDO) Alliance has created two protocols to facilitate online authentication: The universal authentication framework (UAF) protocol and the universal second factor (U2F) protocol. Both protocols are based on a public key cryptography challenge-response model.

Another classification of authentication standard divides it into: single, two, and multi-factor authentications.

Encryption Standards

Key-based encryption techniques can be broadly classified into: symmetric and asymmetric algorithms.

Symmetric Encryption Algorithms

The term symmetric indicates that the same keys are used for encryption and decryption. Those can be further classified into: block and stream ciphers. Examples of block cipher known encryption algorithms are: DES, AES, Blowfish, etc.

In comparison with block cipher, stream cipher encrypts messages one bit or byte at a time rather than working on a block of data in block cipher. In one difference, stream cipher can suffer less from data noise as the size of data sent each time is much less. Examples of stream cipher encryption algorithms include: RCA, RC4, SEAL, FISH, BMGI, etc.

Asymmetric Encryption Algorithms

Unlike symmetric encryptions, in asymmetric encryptions, two different keys are used for encryption/decryption. In other words, message is encrypted with one key and decrypted with another key. In comparison with symmetric encryption, we described at the beginning of this chapter three methods to break encryption messages. While symmetric encryptions are subjected to all three types, asymmetric encryption can only be subjected to the last one (i.e., brute force). Examples of asymmetric encryption algorithms include: RSA, ECDH, ECC, Diffic-Hellman, etc.

Cloud Security Models (Kaur and Sharma 2014)

- Cloud multiple-tenancy model of NIST.
- Cloud risk accumulation model of CSA.
- Jerico Formu’s cloud cube model.

K0311: Knowledge of Industry Indicators Useful for Identifying Technology Trends

Gartner 'Top 10 Strategic Technology Trends'

Every year, Garner (https://www.gartner.com) creates reports on top 10 technology trends. Here is the list for the most recent year, 2018 (Gartner 2017):

AI Foundation

Artificial intelligence continues to be an important research trend in many applications. Creating systems that learn, adapt, and potentially act **autonomously** will be a major battleground for technology vendors through at least 2020.

Security intelligence plays a key role in building security controls with effective defense mechanisms. Unfortunately, the process to extract (1) **useful** and (2) **relevant knowledge** from monitoring agents or systems is not trivial. If we add two more criteria (3) (**real time**) and (4) **autonomous or self-adaptive**, the number of applications for such systems, *when they exist*, are enormous. For example, an elite team from US Army Labs, ARL (Kott et al. 2018) published a recent positioning paper on (An Intelligent Autonomous Agent for Cyber Defense) and the need for such agents ("performing active, largely autonomous cyber defense actions") for the army and defense systems.

Intelligent Apps and Analytics

This second trend is related to the first one on trends for intelligence applications integrating AI, machine learning, and some other technologies.

AI is also driving advances for several new intelligence things (IoTs, autonomous vehicles, robots, and drones).

Digital Twin

Digital representations of real-world entities or systems (e.g., in the context of IoTs).

Cloud to the Edge

In edge computing information processing, and content collection and delivery are placed closer to the sources of information.

Conversational Platforms

Humans interaction with the digital world show different recent technology trends (e.g., virtual realities). In a similar trend, conversational platforms refer to a platform in which humans interactively interact with the digital worlds and applications (i.e., in a form of conversation).

Immersive Experience

Immersive experience refers to the illusory environment that completely surrounds users where they feel they are inside it and part of it. The term is associated with technology environments that command the senses such as virtual reality (VR), augmented reality (AR), and mixed reality.

Blockchain

Blockchain is evolving from a digital currency infrastructure into a platform for digital transformation. Blockchains have many potential applications, related to government, healthcare, manufacturing, media distribution, identity verification, etc.

Event Driven

Business events could be anything that is noted digitally, reflecting the discovery of notable states or state changes that require triggering certain tasks or activities.

Continuous Adaptive Risk and Trust

Security and risk management leaders must adopt a continuous adaptive risk and trust assessment (CARTA) approach to allow real-time, risk and trust-based decision-making with adaptive responses.

Deloitte Technical Trends

Figure 8.2 shows Deloitte technical trends on different domains: digital, analytics, and cyber over the last 9 years (Deloitte 2018). In cyber security, key terms in the trend are: cyber security, cyber intelligence, digital identifiers, no such thing as hacker-proof, blockchain democratized trust and trust economy.

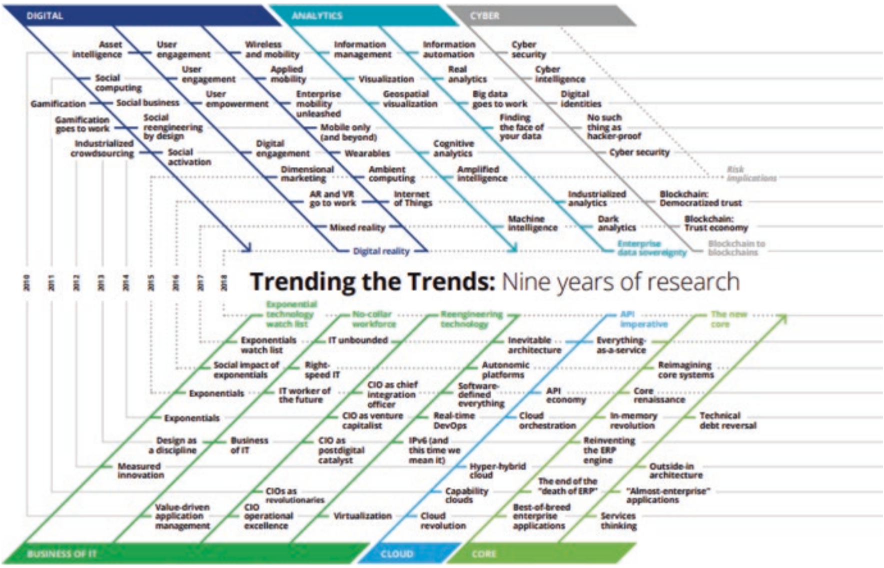


Fig. 8.2 Deloitte technical trends (Deloitte Technical Trends 2018)

Few examples of other websites that also reported in 2018, top 10 technology trends:

- Accenture, (Accenture 2018).
- Huffington post, (Machaiah 2017).
- Forbes, (Singh 2018).
- Fortune, (Samit 2017).
- Medium, (Bobriakov 2018).

K0335: Knowledge of Current and Emerging Cyber Technologies

10 Top Cyber Security Companies

In the article (10 Top Cyber Security Companies) Yogesh (2018) listed the top 10 cyber security companies in 2018 (ranked per their cyber share) with their cyber focus:

1. CyberArk software: The company offers numerous services including credential protection and management, session isolation and monitoring.
2. Cisco: Current share price: The most popular computer networking company known for their routers and firewalls.

3. IBM: A large and popular computing company in almost all software, data, and computing products. For this list in particular, the company is classified for its enterprise IT security solutions, which range across mobile, data, network, and endpoint solutions. IBM uses AI and cloud platforms to protect and detect threats.
4. Microsoft: Another large and popular computing company in almost all software, data, and computing products. Microsoft is classified in this list for its datacenter to endpoint protection sector. The company provides numerous offerings to counter cybercrime starting from its prime windows defender product to its cloud-based azure and office 365 security compliance centers.
5. Amazon: The giant e-business company is included in this list for its cloud powered security solutions with abilities to mitigate a large inventory of attacks. They are also known for their Amazon web Services (AWS).
6. FireEye: Offers advanced threat protection services and several solutions for enterprise security, threat intelligence solutions, etc.
7. Lockheed Martin: A large aviation company that is involved in different cyber and EW defense and offense products. The company claims to build a cyber center of excellence through its skilled analysts and superior technology.
8. Check point software: Offers a unified threat management software solution.
9. Symantec: With their Norton, a long time popular anti-malwares' solutions' company. The company expanded their services from protecting regular laptops/desktops to other environments (e.g., the cloud, mobile platforms).
10. BAE systems: BAE systems is a British multinational defense, security and aerospace company. The company provides cyber security risk management services.

In addition to BAE and Lockheed, the other popular defense contractors are: Raytheon, Boeing, General Dynamics, Northrop Grumman, United Technologies, and L-3.

To cover different perspectives, we expand the list to other players in cyber security described in (Morgan 2017):

- Accenture: The company provides business process outsourcing, IT services, cloud services, managed operations, security, and infrastructure services.
- Apple: The popular computing and smart phones company continuously improves their operating system security features. Apple includes face ID and recognition in their new phones to improve their access and identity management platform.
- Dell: The company known for their laptops and servers provides security solutions for servers and data centers.
- Facebook: The popular online social networks' company went into several recent issues that impact their privacy and security platform. Given that the company is a major hacking target, they continue improvements on cyber threat detection/protection mechanisms.
- Google: The popular search engine company continues to expand their services to users. Their email application, Gmail employs smart techniques to protect against phishing, spam, ransomwares, etc.

K0412: Knowledge of Cyber Lexicon/Terminology

K0435 Knowledge of Fundamental Cyber Concepts, Principles, Limitations, and Effects

Please refer to websites such as the followings for cyber security terms:

- https://csrc.nist.gov/glossary
- https://niccs.us-cert.gov/glossary
- https://www.globalsecurity.org
- https://www.cybrary.it/glossary/
- https://www.threatconnect.com/cyber-security-glossary/
- https://thecyberwire.com/glossary.html
- https://cybersecurityventures.com/cybersecurity-glossary/
- https://www.sans.org/security-resources/glossary-of-terms/
- https://www.bsigroup.com/en-GB/Cyber-Security/Cyber-security-for-SMEs/Glossary-of-cyber-security-terms/

K0454: Knowledge of Information Needs

Information is needed to make decisions. The higher the quality of the collected information and the more comprehensive the information, the more sound the decision.

Information needs refer to any general or specific subject for which a state or local agency has a continuing need for intelligence (GAO 2010). They are also defined as: insights needed to manage objectives, goals, risks, and problems [ISO/IEC 2007].

It is important to make sure that information needs are articulated, clarified, assigned, and fulfilled, using intelligence processes in a timely manner. In cyber security, information needs are primarily focused on threat, vulnerability, consequences, warning, and countermeasures.

To adequately assess cyber threats, information is needed for a comprehensive analysis. In some cases, during the course of the analytic process, critical information may be missing that prevents a complete and accurate assessment of the issue. Such gap or unanswered question related to the threat triggers an intelligence requirement process/information need.

In order to ensure the efficiency of the intelligence collection process, the information collection process needs to be focused so that specific information needs are fulfilled. Some procedures that can enhance the process of information needs collection and processing (FBI 2003):

- Identify, prioritize, and address state and local information needs.
- Share intelligence, analytical techniques, and tools.
- Timely distribution of appropriate intelligence.
- Seek feedback concerning the effectiveness of the support.

Typically, based on time information needs can be divided into three categories (ISAO 2016):

- Immediate—Information needs that concern actions to defend against or respond to new threats, vulnerabilities, or incidents as soon as possible.
- Tactical—Information needs that concern decisions on how to best deploy an organization's existing resources against the change in situational awareness.
- Strategic—Information needs that concern making plans and decisions on the efforts and resources needed to address emerging or future threat environments.

K0504: Knowledge of Organization Issues, Objectives, and Operations in Cyber as Well as Regulations and Policy Directives Governing Cyber Operations

Presidential Policy Directive (PPD) 20

PPD 20 provides a framework for US cyber security by establishing principles and processes. Started in 2012, this directive supersedes National Security Presidential Directive NSPD-38. The directive complements NSPD-54/Homeland Security Presidential Directive HSPD-23.

This directive pertains to cyber operations, including those that support or enable kinetic, information, or other types of operations. Most of this directive is directed exclusively to defensive and offensive cyber effects operations: DCEO and OCEO.

National Security Presidential Directive 54 (NSPD 54)

Started in 2008, NSPD 54 was issued concurrently as Homeland Security Presidential Directive 23. The NSPD 54/HSPD 23 authorized the DHS (together with OMB) to set minimum operational standards for Federal Executive Branch civilian networks. It empowers DHS to lead and coordinate the national cyber security effort to protect cyberspace and the computers connected to it. The directive contains the Comprehensive National Cybersecurity Initiative (CNCI), (EPIC 2018).

Comprehensive National Cybersecurity Initiative (CNCI)

Started in 2008, CNCI now works nationally to support full spectrum cyber operations. The main actions of the CNCI are, (Pernik and Wojtkowiak 2016):

- Create or enhance shared situational awareness within federal government, and with other government agencies and the private sector.

- Create or enhance the ability to respond quickly to prevent intrusions.
- Enhance counterintelligence capabilities.
- Increase the security of the supply chain for key information technologies.
- Expand cyber education.
- Coordinate and redirect research and development efforts.
- Develop deterrence strategies.

K0521: Knowledge of Priority Information, How It Is Derived, Where It Is Published, How to Access, etc

Based on the important of information, information can be classified under different categories (Kamila 2017):

- Priority information: Sensitive information with high timely value (e.g., emergency, accidents, terrorist activities).
- Nominally priority information: High valuable but routinely information (no sensitive time value).
- Non-priority information: Regular information (i.e., no high value and no sensitive time).

Examples of intelligence reports with priority information classification:

- Suspicious incident reports (SIRs).
- Suspicious activity reports (SARs).
- Situational awareness reporting.

When it comes to priority information, given its high value and critical time factor, it is important first to ensure the credibility and accuracy of the collected information and second, it's also important to ensure that such priority information is received, on time, by the right or intended audience (e.g., to those law enforcement authorities and national entities to support its inclusion into national patterns and trends analysis).

K0526: Knowledge of Research Strategies and Knowledge Management

The rapid and continuous evolution of cyber security triggers a large volume of research in this area focusing on both challenges and opportunities. Cyber security integrates knowledge areas from different domains and fields, not only computing, networking, or technical areas.

In National Cyber Leap Year Summit 2009 (NCL 2009), three ideas were proposed to promote "Cyber security proactive design strategies":

- Enable tailored trustworthy spaces within the generally untrusted cyberspace. Different applications and environments require different levels of security.

Additionally, they require different levels of security attributes (e.g., confidentiality, privacy, availability, access control). Proposing one trust-model that can fit all environments is impractical. Trust formula should be dynamically created based on the current context. Dynamic access controls that can provide fine level details (e.g., ABAC) can be used.

- Thwart attackers with moving target defenses: Moving target defense mechanisms are used by both defenders and attackers. The idea is to make targets look different (e.g., polymorphism viruses) in different environments, times, or locations. This can be combined with randomization to make target changes unpredictable.
- Reward responsible behavior with economic and other incentives: Ultimate security protection in the open uncontrolled cyber security world cannot be handled by one entity. Methods and incentives should be put in place to encourage the public to participate. Table 8.1 shows different deception techniques that can be employed by attackers (Guri 2016).

The World Cyber Security Technology Research Summit (Belfast 2011) identified four research themes that are critical to the cyber security defenses:

- **Adaptive cyber security technologies**, or (adaptive cyber defense): The development of autonomous, self-adaptive, self-learning, and self-awareness cyber security technologies.
- The concept of "adaptive cyber defense" is also introduced in other research venues ().
- **Protection of smart utility grids:** Protection methods and technologies for smart grids components; secure technologies for smart grid communications; etc.
- **Security of the Mobile platform and applications**: Focus on malwares and attacks on mobile platforms and defense mechanisms.
- **Multi-faceted approach to cyber security research:** Research must consider the different domain knowledge that are required and interact in cyber security from technical to social and behavioral.

Table 8.1 Malware deception techniques

Technique	Deception method
Polymorphism	Change malware signature
Metamorphism/ self-modification	Change malware code on the fly
Obfuscation	Conceal code and logic
Self-encryption	Change malware signature and hide malicious code and data
Anti-VM/sandboxes	Evade forensic analysis by changing behavior in forensic environments
Anti-debugging	Evade automated/manual investigation by changing behavior in forensic environments
Encrypted exploits	Evade automated/manual investigation by changing parameters and signatures

K0535: Knowledge of Strategies and Tools for Target Research

The main objective of moving target defensive (MTD) is to provide a new layer of protection that depends on changing occasionally systems' attributes to complicate adversaries' attempt to analyze and attack those systems. MTD creates an abstract, dynamic view of the network to conceal the network's topology and vulnerabilities (Skamser 2017).

There are three main categories of MTD:

- Network level MTD.
- Host level MTD.
- Application level MTD.

A significant portion of MT research involves developing techniques that modify system characteristics in one or more of the following dimensions or characteristics, (NITRD 2014):

- Policies: Risk-adaptive policies, movement scheduling.
- Data: Secure distributed data chunking and decentralization, data encryption.
- Networks: Dynamic networking, dynamic domain name system (DNS), internet protocol (IP) address randomization.
- Software: Source code diversity, just-in-time compiling, disposable applications.
- System: Diversity in operating systems, instruction set randomization.
- Systems of systems: Non-persistent virtual machines, system self-cleansing, machine rotations.
- Hardware: Multicore processing, cache randomization.

Major goals in MT research include, (NITRD 2014):

- Design resilient systems that can operate reliably in compromised environments.
- Increase the cost of staging and executing attacks (as a defense mechanism).
- Shift from reactive security postures to active and preemptive ones.
- Develop MT mechanisms that can create disruptions particularly for the adversaries.
- Develop the ability to optimize moving target mechanisms against various attacks.

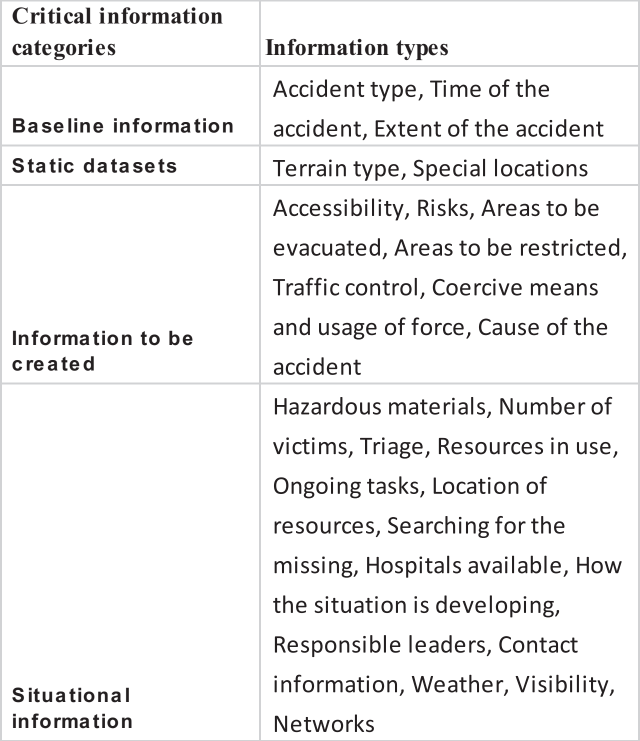
Table 8.2 shows examples of defense deception methods (Guri 2016).

K0566: Knowledge of the Critical Information Requirements and How They're Used in Planning

Intelligence requirements can fall into different categories: critical information requirements CIR, priority information requirements, non-priority information requirements, etc. Figure 8.3 **shows different categories of CIRs** (Seppänen 2015).

Table 8.2 Examples of defense deception methods (Guri 2016)

Information system part	Deception method
Network	Route change; random addresses, names and ports
Firewall/IDS	Policy change
Host	Change host address, replace host image
OS	Change version and release; change host ID; change memory addresses, structures, resource names



Critical information categories	Information types
Baseline information	Accident type, Time of the accident, Extent of the accident
Static datasets	Terrain type, Special locations
Information to be created	Accessibility, Risks, Areas to be evacuated, Areas to be restricted, Traffic control, Coercive means and usage of force, Cause of the accident
Situational information	Hazardous materials, Number of victims, Triage, Resources in use, Ongoing tasks, Location of resources, Searching for the missing, Hospitals available, How the situation is developing, Responsible leaders, Contact information, Weather, Visibility, Networks

Fig. 8.3 Critical information categories and elements (Seppänen 2015)

Differentiate between CIRs and other important information requirements is that most of other requirements are often of a tactical nature, not essential for key operational level decisions. CIRs support commanders' situational understanding and decision-making at every level. CIRs are developed during design and planning, not during execution. CIRs include information required in assessments that better drive the far-reaching planning decisions at the operational level.

S0018: Skill in Creating Policies that Reflect System Security Objectives

S0145 Skill in Integrating and Applying Policies that Meet System Security Objectives

Policies that regulate system or network traffic and information exist in different areas. We will cover quickly creating policies in the following areas:

Creating Policies in Operating Systems

Operating systems in servers and clients' machines host other application and also control access to those applications. Users can be granted administrator privileges in an operating system active directory which can then be transferred to most applications that are hosted within that operating system. The basis of OS protection is separation. The separation can be of four different kinds: physical, temporal, logical, and cryptographic.

Different operating systems provide different policy mechanisms and procedures. However, the following general categories are common to be included within OS security policies:

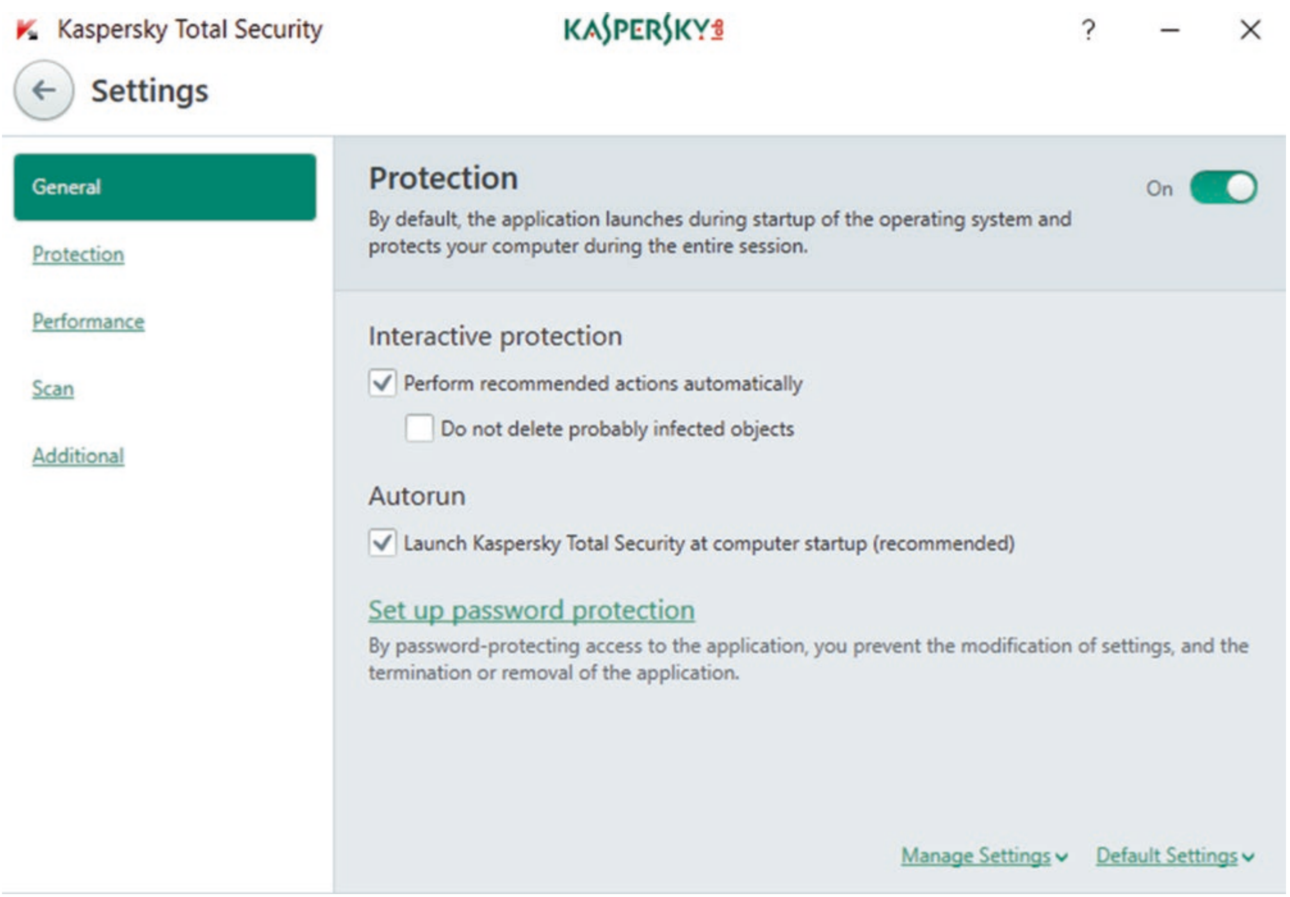
- Users accounts, roles, and permissions.
- Accounts policies.
- Files and file system policies.
- Network services policies.
- System patches and updates policies.
- Logging and monitoring policies.
- Integration or communication with other applications' policies.

As one example to exercise this KSA, refer to Windows 2016 server group policies and how to deploy such policies. You can also practice using basic access control in open source Linux operating systems.

Creating Policies in Firewalls

Firewalls exist largely in L2-L3 of the OSI layers. New generation firewalls exist also in layer 7 or application layer, Fig. 8.4. In such cases, they are integrated within multi-purpose anti-malware or threat protection systems.

As a demonstration in this part, you can try working with the simple open source firewall (UFW) that can be deployed in Kali, Fig. 8.5.



Protection

On

By default, the application launches during startup of the operating system and protects your computer during the entire session.

Interactive protection

☑ Perform recommended actions automatically

□ Do not delete probably infected objects

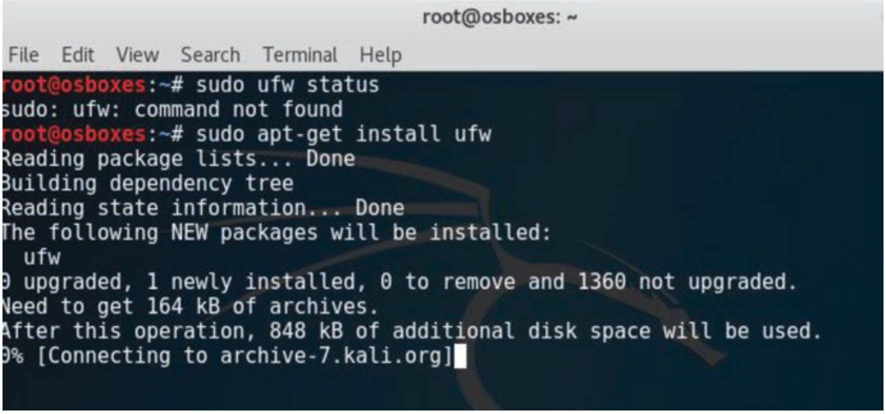
Autorun

☑ Launch Kaspersky Total Security at computer startup (recommended)

Set up password protection

By password-protecting access to the application, you prevent the modification of settings, and the termination or removal of the application.

Fig. 8.4 An example of application layer firewalls



```
root@osboxes:~# sudo ufw status
sudo: ufw: command not found
root@osboxes:~# sudo apt-get install ufw
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  ufw
0 upgraded, 1 newly installed, 0 to remove and 1360 not upgraded.
Need to get 164 kB of archives.
After this operation, 848 kB of additional disk space will be used.
0% [Connecting to archive-7.kali.org]
```

Fig. 8.5 UFW firewall in Kali

Creating Policies in Switches and Routers

Similar to firewalls, switches and routers include Access Control Lists (ACLs) through which policies to control traffic can be created. Use the open source GNS3 (https://www.gns3.com/) to install and experiment with any router to show how to create and test ACLs.

Creating Policies in DBMS

Similar to operating systems, there are several areas to go through when considering security issues in DBMSs: User identification, access control, auditing, encryption, and inference control, Fig. 8.6, (Zaman et al. 2017).

Search for a reference that describes security policies walkthrough in a DBMS of your choice. Make sure you cover the different perspectives described in Fig. 8.6.

Creating Policies in Web Servers

One method to prevent several web attacks (content injection attacks) such as cross site scripting XSS is to use content security policies. Find some references about CSP (e.g., https://content-security-policy.com/) and see how to implement that on a web server such as Apache.

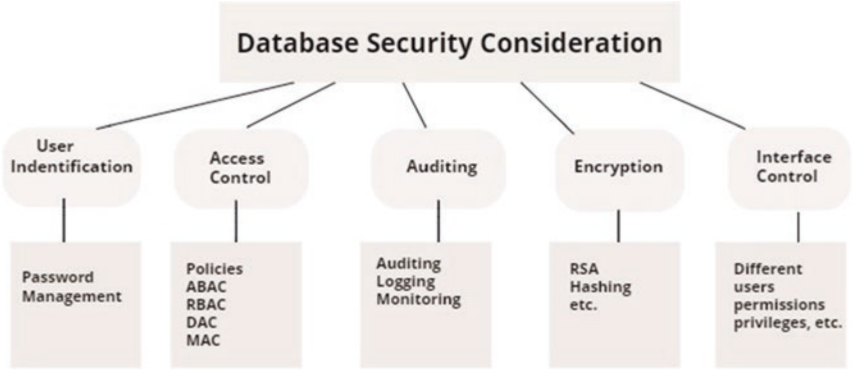


Fig. 8.6 Security considerations in DBMS (Zaman et al. 2017)

S0146: Skill in Creating Policies that Enable Systems to Meet Performance Objectives (e.g., Traffic Routing, SLA's, CPU Specifications)

Routing algorithms represent the key intelligence in routers. Those routing algorithms decide in real time the **best** route to take in each traffic quest or context. Early routing protocols were either static, manually configured or dynamic but based on basic and fixed attributes (e.g., Routing Information Protocol, RIP) that makes routing decisions based on simple attribute values (e.g., select the route that has the lowest number of routers or hubs to destination). More recent dynamic routing protocols (Fig. 8.7, Cisco Networking Academy 2014) are more complex and consider several attributes related to the network topology, health, etc.

Routing policies can be imported to the routing tables in routers or they can be exported or advertised to neighbors, Fig. 8.8, (Juniper 2017).

Amazon Route 53

AWS offers four routing policies in Amazon Route 53 Traffic Flow (Weighted routing, Latency-based routing, Failover routing, and Geolocation routing). Each option has its usage and balances heavy traffic loads.

Amazon route 53 (https://aws.amazon.com/route53, https://docs.aws.amazon.com/Route53) "is a highly available and scalable cloud Domain Name System (DNS) web service. It is designed to give developers and businesses an extremely reliable and cost-effective way to route end users to Internet applications by trans-

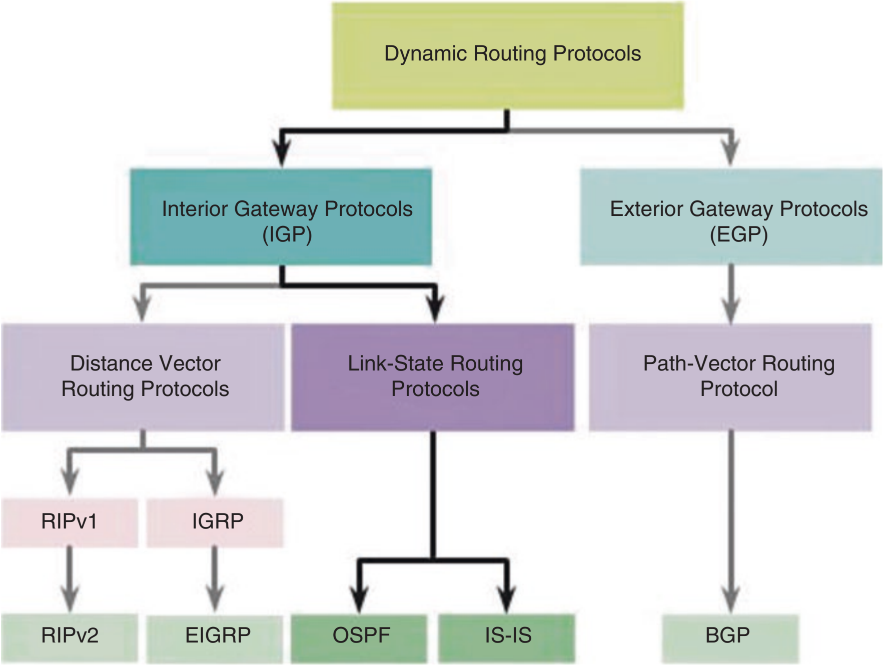

Dynamic Routing Protocols
Interior Gateway Protocols (IGP)
Exterior Gateway Protocols (EGP)
Distance Vector Routing Protocols
Link-State Routing Protocols
Path-Vector Routing Protocol
RIPv1
IGRP
RIPv2
EIGRP
OSPF
IS-IS
BGP

Fig. 8.7 Dynamic routing protocols (Cisco Networking Academy 2014)

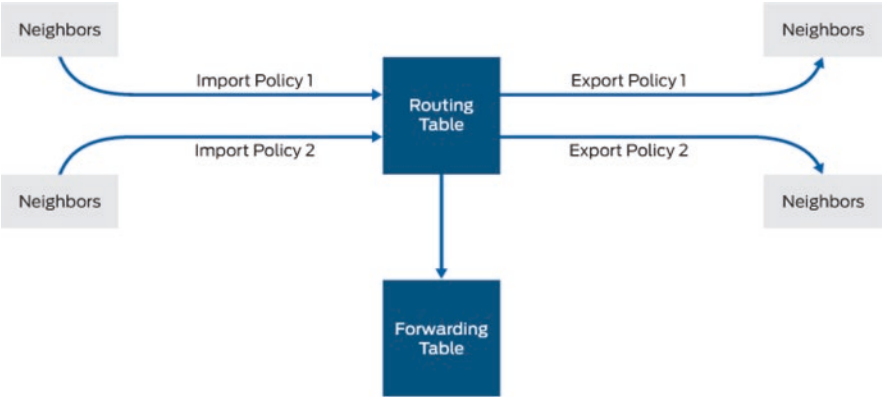


Fig. 8.8 Importing and exporting routing policies (Juniper 2017)

lating names like www.example.com into the numeric IP addresses like 192.0.2.1 that computers use to connect to each other" (https://aws.amazon.com/route53).

Follow instructions in: (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/traffic-policies.html) on how to create traffic policies using route 53.

A0034: Ability to Develop, Update, and/or Maintain Standard Operating Procedures (SOPs)

A standard operating procedure, SOP, is a set of prescribed and structured instructions created to help workers carry out complex routine operations. SOPs main goal is to achieve efficiency, quality, and uniformity of performance, while reducing miscommunication and failures to comply with regulations.

Reader is recommended to search for examples of SOPs in cyber security (e.g., procedures to protect systems, assets).

Bibliography

Accenture (2018) Technology Vision 2018, Intelligent Enterprise Unleashed. https://www.accenture.com/us-en/insight-technology-trends-2018?c=us_us_technologyvisio_10220142&n=psgs_generic_exact_top_-technology_trends_0218&gclid=CjwKCAjwy_XaBRAWEiwApfjKHoOcQFRBiK6gAEVOSYApnkrAoNNoymVYBljgoqIPubdZRbdl5xT6BoCpWEQAvD_BwE

Belfast (2011) http://www.csit.qub.ac.uk/News/Events/Belfast2011/, http://www.csit.qub.ac.uk/News/Events/Belfast2011/

Bobriakov I (2018) The top 10 technology trends of 2018. https://medium.com/activewizards-machine-learning-company/the-top-10-technology-trends-of-2018-5fce940c7ce6. Accessed 19 Feb 2018

Cisco Networking Academy (2014) Cisco networking academy's introduction to routing dynamically. Cisco Press, Indianapolis, IN

Cox BJ (2011) Policy-based access control (PBAC) for diverse DoD domains. Technica Corporation, Sterling, VA

Deloitte (2018) Tech trends 2018, the symphonic enterprise. Deloitte, London

EPIC (2018) Electronic Privacy Information Center, epic.org, Presidential Directives and Cybersecurity Concerning the use of Presidential Directives in Cybersecurity Policy, 2018. https://epic.org/privacy/cybersecurity/presidential-directives/cybersecurity.html

FBI Office of Intelligence (2003) FBI intelligence production and use. Concept of operations report. FBI Headquarters Divisions and the Office of Intelligence, Washington, DC, p 18

GAO (2010) GAO Report, GAO-11-223. https://www.gao.gov/assets/320/314120.html

Gartner (2017) Identifies the Top 10 Strategic Technology Trends for 2018. https://www.gartner.com/newsroom/id/3812063. Accessed 4 Oct 2017

Gray CS (2007) The airpower advantage in future warfare (Maxwell Air Force Base), Ala: Air University. Airpower Research Institute, Maxwell AFB, AL

Gray CS (2013) Making strategic sense of cyber power: why the sky is not falling. http://www.dtic.mil/dtic/tr/fulltext/u2/a584060.pdf

Guri M (2016) Moving target defense vs. moving target attacks: the two faces of deception. *Network World*. Accessed 4 Jan 2016

ISAO (2016) 100-1, guidelines for establishing an ISAO, ISAO standards organization, July 22

Juniper (2017) Understanding Routing Policies. https://www.juniper.net/documentation/en_US/junos/topics/concept/policy-routing-policies-overview.html

Kamila NK (2017) Advancing cloud database systems and capacity planning with dynamic applications. IGI, Hershey, PA

Kaur B, Sharma S (2014) Parametric analysis of various cloud computing security models. Int J Inform Comput Technol 4(15)

Koret J, Bachaalany E (2015) The antivirus Hacker's handbook, 1st edn. Wiley, New York. Accessed 28 Sept 2015

Kott A, Mancini LV, Théron P, Drašar M, Dushku E, Günther H, Kont M, LeBlanc B, Panico A, Pihelgas M, Rzadca K (2018) Initial reference architecture of an intelligent autonomous agent for cyber defense, ARL-TR-8337, Mar 2018

Kuehl D (2009) From cyberspace to cyberpower, defining the problem. In: Cyberpower and national security. National Defense University Press, Washington, DC

Machaiah P (2017) Top 10 transformative technology trends. *Huffington Post*. Accessed 27 Dec 2017

Morgan S (2017) Cyber security business report. www.csoonline.com. Accessed 20 Dec 2017

National Cyber Leap Year Summit (2009) Co-Chairs' Report, Sept r6 2009 (2009, September r6) (Online]. http://www.cyber.st.dhs.gov/docs/National_Cyber_Leap_Year_Summit_2009_Co-Chairs_Report.pdf

Nguyen K (2017) Learning to mow grass: IDF adaptations to hybrid. School of Advanced Military Studies, Leavenworth, KS

NITRD (2014) Report on Implementing the Federal Cybersecurity Research and Development Strategy. https://www.nitrd.gov/PUBS/ImplFedCybersecurityRDStrategy-June2014.pdf

Authentication Cheat Sheet, OWASP.org (2017), https://www.owasp.org/index.php/Authentication_Cheat_Sheet

Pernik P, Wojtkowiak J (2016) Alexander Verschoor-Kirss, NATO cooperative cyber defense center of excellence. CCDCOE, Tallinn

Samit J (2017) 4 technology trends that will transform our world in 2018. Fortune.com. http://fortune.com/2017/12/26/4-technology-trends-2018/. Accessed 26 Dec 2017

Schendel DE, Hatten KJ (1972) Business policy or strategic management: a broader view for an emerging discipline. Acad Manag Natl Meet

Seppänen H (2015) Doctoral dissertation, Aalto University Publication Series

Singh S (2018) Top 10 Tech Trends for 2018. Forbes.com. https://www.forbes.com/sites/sarwantsingh/2018/02/01/top-10-trends-for-2018/#46cd56517cb3. Accessed 1 Feb 2018

Skamser C (2017) Moving Target Defense (MTD) and Attack Surface Segmentation Cyber Security, CRI advantage, June 2nd

Steel C, Lai R, Nagappan R (2009) Core security patterns: identity management standards and technologies, introduction to XACML

Venkata Subramanian KK, Mukherjee T, Gupta SK (2014) CAAC: an adaptive and proactive access control approach for emergencies in smart infrastructures. ACM Trans Autonom Adapt Syst 8(4):20

Yarger HR (2006) Strategic theory of for the 21st century: the little book on big strategy. Strategic Studies Institute, Carlisle, PA, p 2

Yogesh B (2018) 10 Top Cybersecurity Companies. https://investingnews.com/daily/tech-investing/cybersecurity-investing/top-cyber-security-companies/. Accessed 16 May 2018

Zaman F, Raza B, Malik AK, Anjum A (2017) Self-protection against insider threats in DBMS through policies implementation. Int J Adv Comput Sci Appl 8(3)

Chapter 9
Cyber Threat Analysis

In cyber threat analysis, knowledge of internal and external vulnerabilities related to a particular system or organization is analyzed and matched against real-world cyber-attacks relevant to that system or organization. Figure 9.1 shows a model that describes threat analysis components:

- Scope of system to analyze relevant threats
- Gather relevant cyber threat information from different sources
- Analyze and integrate gathered information from those different sources
- Make actions and intelligence-driven decisions based on learned information

K0426: Knowledge of Dynamic and Deliberate Targeting

There are two targeting categories—deliberate targeting and dynamic targeting: (ATP 3-60-2015)

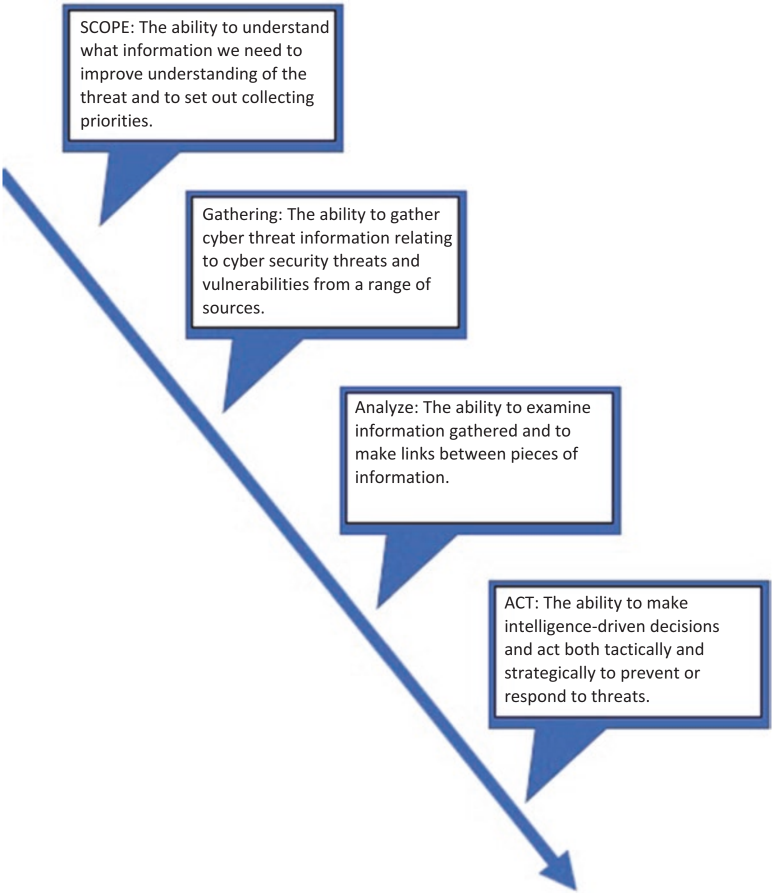
1. Deliberate targets

   Deliberate targets are targets that exist in an operational area with actions scheduled. Examples range from targets on Joint Target Lists (JTLs) in the applicable campaign plan, in the applicable plan or order, targets detected in sufficient time to be placed in the joint air tasking cycle, mission-type orders, or fire support plans, to mission-type orders, etc. Deliberate targeting prosecutes planned targets.

   Deliberate targets have two subcategories: (1) scheduled and (2) on-call (Fig. 9.2):

   - Scheduled targets exist in the area of operations and are located in sufficient time to take actions at a specific, planned time.
   - On-call targets have actions planned, but not for a specific delivery time.

I. Alsmadi, *The NICE Cyber Security Framework*,
https://doi.org/10.1007/978-3-030-02360-7_9



SCOPE: The ability to understand what information we need to improve understanding of the threat and to set out collecting priorities.

Gathering: The ability to gather cyber threat information relating to cyber security threats and vulnerabilities from a range of sources.

Analyze: The ability to examine information gathered and to make links between pieces of information.

ACT: The ability to make intelligence-driven decisions and act both tactically and strategically to prevent or respond to threats.

Fig. 9.1 Components of threat analysis (General security 2014)

2. Dynamic targets

Dynamic targets are unscheduled, unplanned, or unanticipated targets: identified too late, or not selected for action in time to be included in the normal targeting cycle.

Dynamic targets are planned to deal with time-sensitive targets. “Target acquisition must be rapid and accurate, and procedures must be developed to minimize the latency or delay between identification and engagement of potentially fleeting critical targets,” (JOAC 2012).

Targets of opportunity are targets identified too late, or not selected for action in time, to be included in deliberate targeting. Targets engaged as part of dynamic targeting are: unanticipated, unplanned, or newly detected.

There are two types of targets of opportunity: unplanned and unanticipated (Fig. 9.2):

- Unplanned targets are known to exist in the area of operations while no actions have been planned against them.

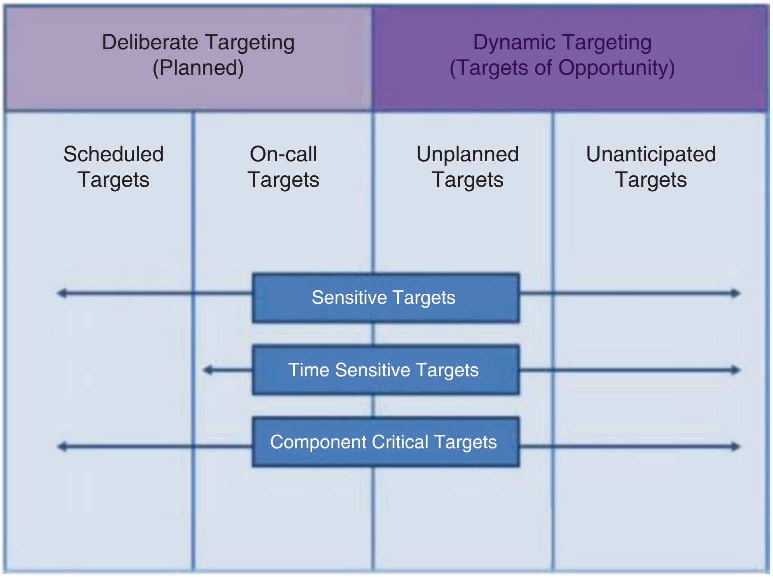


Fig. 9.2 Categories of targets/targeting (Julian Assange 2014)

- Unanticipated targets are unknown or not expected to exist in the area of operations.

The process developed to facilitate dynamic targeting at the joint level is find, fix, track, target, engage, and assess (F2T2EA) (FM-3-60 2010).

K0430: Knowledge of Evasion Strategies and Techniques

Evasion is a technique that malware developers and hackers use to avoid analysis and detection of the malware by security or forensic analysts and eventually eradication. In a larger scope, evasion is a strategy used by cyber defenders and attackers to avoid attack, infiltration, liability, or being labeled and identified.

Evasions operating at the lower OSI layers result in a bigger impact on security than those operating at the upper layers (e.g., HTTP, FTP) because lower level evasions impact a broader range of exploits. Anti-evasion techniques exist in the different OSI layers. The list in Fig. 9.3 includes only a subset provided by (NSS labs 2012).

IDS/IPS Evasion

Attackers and malwares try to develop or use techniques to avoid detection and eradication by IDS/IPSs so that they can reach their goals or destinations.

- IP Packet Fragmentation
- TCP Stream Segmentation
- RPC Fragmentation
- SMB & NetBIOS Evasions
- FTP Evasion
- IP Fragmentation + TCP Segmentation
- IP Fragmentation + MSRPC Fragmentation
- IP Fragmentation + SMB Evasions
- TCP Segmentation + SMB/NETBIOS Evasions

- URL Obfuscation
- HTTP Encoding
- HTTP Compression
- HTML Obfuscation
- Payload Encoding
- Payload Compression & Encoding

Fig. 9.3 Anti-evasion techniques (NSS lab 2012)

Network IDS/IPS can detect attacks through one of two methods:

- Signature matching: This is the typical approach for known malwares. Their signature is recorded from previous analysis. This signature can be a certain port the malware uses for penetration, or a header/file signature. For files and some other artifacts, hash values are recorded and can be used for quick signature comparison.
- Abnormality detection: For unknown malwares, signature method will not work. As an alternative, abnormal behaviors are defined and any traffic that behaves abnormally based on such roles is flagged as a malware. Apparently, false alarms (i.e., normal traffic to be detected as malware) may frequently occur in this abnormal detection technique and hence the process can go through several cycles of tuning to improve accuracy of detection.

The following methods are used to avoid detection by IDS/IPS (SANS 2003, 2016):

- Obfuscation: In software programs, obfuscation is a process used to protect program ownership through preventing it from being reverse engineered to extract original source code. Closed source programs are provided to users as executables (not the source code). Hackers and malware designers use similar methods to avoid malware analysis. Encryption is the most popular technique in which obfuscation in this case is accomplished. Obfuscation is also used in URL links to avoid blacklisting.

  In network traffic, obfuscation refers to changing partially traffic or malware signature so that it will not match original signature recorded by IDS/IPS.
- Fragmentation: Several abnormal behavior detection techniques count the existence of several attributes in the subject traffic to be flagged as malicious. Fragmenting the malicious attack across several packets may help in avoiding such “stateful” inspection techniques.

- Encryption: Probably the most popular widely used technique in evasion. Strong encryption is very hard to break or may take very long time, for both attacker and defender, the time is a key. In network-evasion, encryption can be used in several dimensions. Bottom line, encrypted traffic cannot be analyzed.
- Flooding traffic: Denial of Service (DoS): Many hackers use flooding (from a single source DoS or distributed from a botnet, DDoS) as part of the attack campaign. Evasion in this case occur in making IDS/IPS or network analysis tools busy or idle from working to monitor normal traffic or the actual attack traffic.

Evasion attacks against anomaly-based IDS/IPS have demonstrated two main evasion strategies: poisoning, i.e., erosion of a model of normality (Kymie et al. 2002), and mimicry, i.e., insertion of a normal content into the target data (Wagner and Soto 2002).

Sandbox Evasion

Sandbox refers to creating a computing environment that is isolated so that programs or files run in it without having any effect on the application it executes.

If a malware is in a sandbox environment, then that's an indication that somebody is trying to analyze and investigate that malware. Hence, many professional malware designers want their malwares in this case not to act, normally, if it was in an "operational" environment.

Sandbox evasion techniques can fall largely into one of three categories (Fireeye 2014):

- Human interaction: Within the sandbox environment, malware expects no human interaction. As such, malwares can use such lack of humans' interactions as a sign that they are in a sandbox environment.

  To fool sandbox-detecting malware, some vendors now simulate mouse movements and clicks in their virtual-machine environments to mimic human activities. On the other hand, malware authors are working on methods to counter such human-interaction simulation.
- Configuration specific. Malware in this category takes advantage of the inherent constraints of file-based sandboxes. For example, knowing that a sandbox can spend, say, 5 min running suspicious code for analysis, malware authors can create code that automatically "sleep" for a longer period. If the code is still running after that, it's probably not in a sandbox.
- Environment specific. In this category, malware checks for significant or specific signs that its code is running in widely used VM environments. It checks for obscure files unique to virtual environments.
- Delayed onset: In this configuration, malware designers delay execution when detecting sandbox environment.

Domain Generation Algorithms; DGAs

The main goal of DGAs is to avoid blacklisting domains and allow creating domains that can be used for cyber-attacks. Many of the recent malwares such as botnets, ransomwares, and spams are shown to be using such technique. Top-5 countries hosting DGA-based crimeware, Ukraine, Romania, Russia, Hungary, and Turkey. Most known malwares to use DGA: Conficker, Murofet, BankPatch, Bonnana, and Bobax (Core security 2017).

Stevanovic and Pedersen (2013) classified evasion techniques into eight categories:

1. ET1: Evasion of host-based detection
2. ET2: Evasion by traffic encryption
3. ET3: Time-based evasion
4. ET4: Evasion by flow perturbation
5. ET5: Evasion by performing only a subset of available attacks
6. ET6: Evasion by restricting the number of attack targets
7. ET7: Evasion of cross-host clustering
8. ET8: Evasion by coordination of bots out-of-band

Bano (2010) classified botnets evasion techniques into four categories, those of the: Bot, Bot-master, C&C server, and C&C (Fig. 9.4)

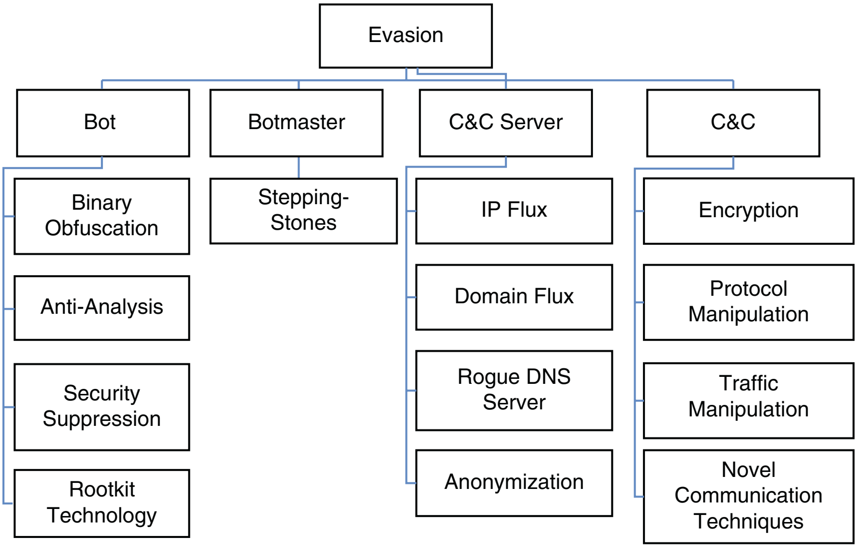


Fig. 9.4 Botnet evasion techniques (Bano 2010)

Resilient Intelligent Networks in 2015 listed their top eight sandbox evasion techniques as:

- Logic Bombs
- Rootkit and Bootkit
- Sandbox Detection Techniques
- Botnet Command and Control Window
- Network Fast Flux, DGAs
- Encrypted Archives
- Binary Packers
- Polymorphic Malwares

K0453: Knowledge of Indications and Warning

In the cyber world, there is generally very little warning before threat exploits (DoD EWS 2006). With the Internet connecting all computing machines, smart phones, IoTs, etc. throughout the world, the fast spread of malwares is common.

In a previous KSA, we elaborated on Indicators of Compromise (IOC) as one large area in cyber security to extract different types of IOCs (e.g., malicious links, files, hashes, registries).

Cyber Threats Indications and Warning

The knowledge about possible future attacks and attackers is largely used for reactive or defensive purposes. This knowledge can help defenders prepare and fortify their systems and assets based on the candidate attack details. On the other hand, such knowledge can be used for offensive operations (e.g., counter attacks or anti-attacks). Anti-cyber-attack is often associated with active and passive defensive measures to protect systems from attacks. Counter-cyber-attack assumes more preemptive offensive strategies to analyze signatures or behaviors and deny the adversary through preventing, deterring, preempting, and neutralizing hostile acts and intrusions (Robinson et al. 2012).

Opened in May 1998 and operating out of the FBI, National Infrastructure Protection Center (NIPC) is primarily a joint DoJ-DoD organization whose charter includes indications and warning, crisis management and coordination, computer security, and education and awareness.

The collection of intelligence about possible future attacks is a key step in knowledge acquisition as well as in the type and nature of response. Some of the key success factors:

- Accuracy and correctness: Attackers employ different techniques to ensure anonymity, avoid attribution, or detection. It is important to know the attackers and the nature of the attack to properly respond. False positives and false negatives are possible while aggregating information from different tools or intelligence sources will help improve accuracy.

With the huge amount of activities in the cyber world, the ability to distinguish attacks from normal activities is a continuous challenge. Additionally, attacker and defender tasks are asymmetric, defenders need to monitor and catch all possible warnings while attackers need only one chance to succeed.

Threat analysts must also determine whether collected intelligence is relevant or irrelevant to the malicious activity.

- Time sensitivity: Cyber-attacks leverage the Internet, social networks, smart phones, and all recent technologies to spread fast to reach the maximum possible number of victims. Even in very focused targets, time is very sensitive to detect and respond to attacks.
- Collaboration: It is important to collaboration at the national level or with friends and allies to create a network of communication to spread early attack warning. The amount of possible attack and attackers are continuously growing and any source of intelligence or information can help. For example, the Cyber Warning and Information Network CWIN intends to provide an “out-of-band” private and secure communications network for government and industry, with the purpose of sharing cyber alert and warning information (Vaida 2003).
- Integration with forensic analysis capabilities: Integrating forensic analysis is important to cyber-attack indications and warning capabilities as part of cyber command and control.
- DNS monitoring: Security was not in mind when originally DNS was designed. Many attacks utilize weaknesses in DNS architecture and hence monitoring violations in DNS can be used for attacks’ warning. DNS is one of the top three most frequently used attack vectors to date this year, according to Akamai (2017).

Robinson et al. (2012) proposed a framework of 12 steps:

1. Problem Identification: Determine the Issue
2. Identifying Potential Actors
3. Actor Courses of Action: Viability and Probability
4. Determine Scenario Enablement
5. Manifested Scenario Focal Events
6. Create Focal Event Indicators: An adversary prepares for hostilities
7. Collect and Monitor through Indicators: Assess Emerging Trends
8. Discern the Probable Scenario that is Trending
9. Readjust for New Manifestations of the Scenario
10. Deception in Indicators
11. Mental Model Avoidance: Is it expectation or actuality; theory or current developments?
12. Strategic Options Analyzed Against Viable Scenarios

K0469: Knowledge of Internal Tactics to Anticipate and/or Emulate Threat Capabilities and Actions

Threat Emulation and Sandboxing

Emulating threats represent one of the defense layers in which defenders evaluate their system readiness for different types of threats. Figure 9.5 shows a pyramid of threat intelligence in which threat emulation is part of its third and top layer.

Threat emulation is a proactive defensive operation. It can be conducted by internal or external red teams (Fig. 9.6). It can also be used as part of testing in cyber offensive operations.

MITRE Adversary Emulation Plans

MITRE (a not-for-profit organization that operates research and development centers sponsored by the federal government) created adversary emulation plans as part of show cases for the practical use of Adversarial Tactics, Techniques, and Common Knowledge: ATT&CK (https://attack.mitre.org/wiki/Main_Page). Known APT behaviors are documented in ATT&CK-based cyber games. MITRE provides also simulation/emulation environments to deploy the threat scenarios.

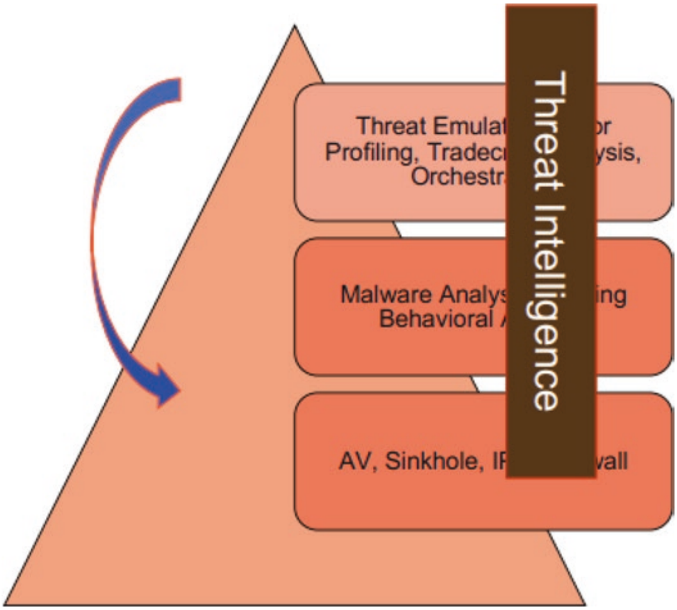


Fig. 9.5 Threat intelligence pyramid (Splunk 2017)

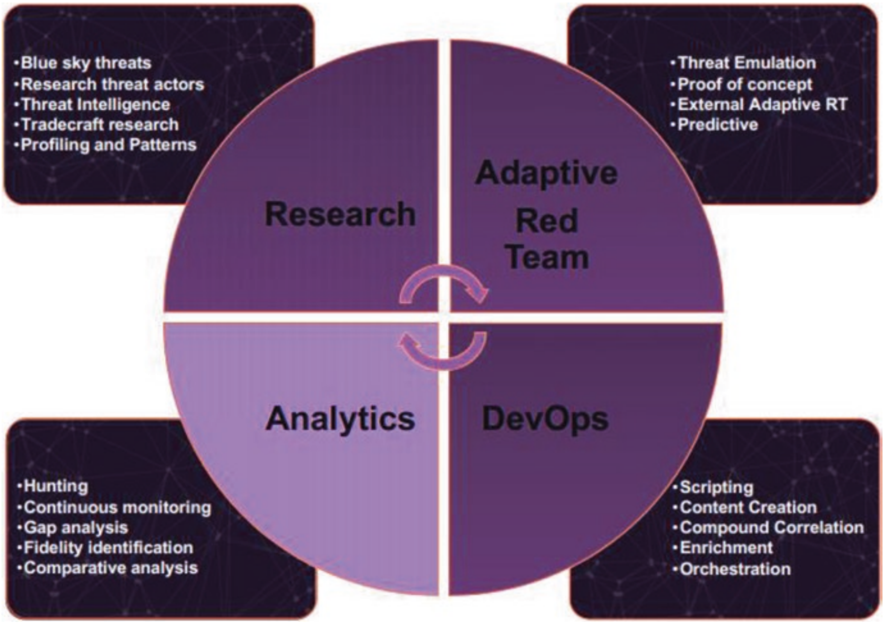


Fig. 9.6 Cyber threat team (Splunk 2017)

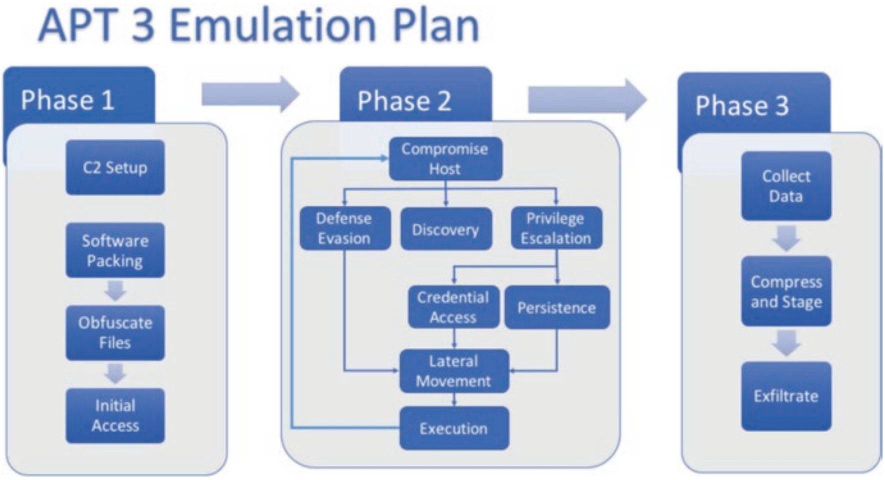


Fig. 9.7 A sample threat emulation plan (MITRE 2018)

Figure 9.7 shows a sample threat emulation plan. Those plans can be used by adversary emulation teams to test organizations' network security and security products against specific threats. Those threat plans or scenarios are typically built from known tactics, techniques, and procedures (TTPs) used by adversary groups to target a particular network.

Some companies provide threat emulation environments for commercial use such as:

- SandBlast Threat Emulation from Check Point SandBlast Zero-Day Protection solution or Threat Emulation Software Blade.

When selecting a sandboxing environment for threat emulation, below are some attributes to look for (Checkpoint 2016):

1. The ability to analyze a broad range of suspicious objects
2. Static analysis and other pre-filtering techniques
3. Comprehensive operating system and application stack
4. Anti-evasion support
5. The rate at which objects can be analyzed in the sandbox
6. A combination of virtualization and emulation-based sandboxing analysis
7. Contextual information about the malware or targeted attack
8. Integration with forensics tools

K0474: Knowledge of Key Cyber Threat Actors and Their Equities

Cyber Criminals

A large category of cyber threat actors are independent hackers looking for financial gains. They use different types of malwares such as worms, phishing, and ransomwares to steal sensitive personal and financial information (e.g., banking or credit card details, SSN, accounts to e-businesses). They may commit large-scale attacks on national infrastructures. In some cases, they may act as states' proxies, hired by states or companies to commit other types of attacks such as DDoS, worms, stealing copyright materials, and patents.

Cyber Activists

Many cyber activists exist and work for different political, environmental, or social causes. In some cases, they can be very radical and commit large-scale attacks that impact large citizens. This is particularly important to them where one of their main goals is to be more visible where their message can reach a large spectrum of audience. Denial of service and web defacements are very popular examples of attacks typically committed by those groups.

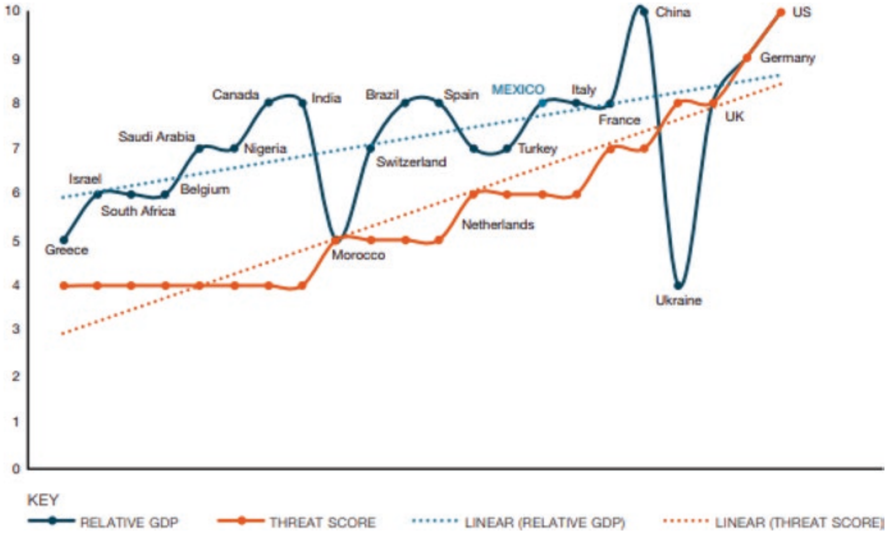


Fig. 9.8 Top countries with highest threat levels (Control risks 2015)

Nation States

Cyber wars between countries continue to exist at different levels and scales. The USA is one of the major targets for such attacks coming from states such as Russia, China, North and Korea (Fig. 9.8). Many of the APTs that are persistent and evolve through several cycles or versions of malwares are known to be created or sponsored by nations. We described examples of those in an earlier KSA.

There are many instances of attacks where affiliation between nation states and independent cyber attackers occur. States may consider such proxy options to avoid possible consequences or liabilities given the rise of international cyber laws and regulations.

K0533: Knowledge of Specific Target Identifiers and Their Usage

Target identification and analysis is part of most cyber offensive and hacking operations. Those can be divided into:

- Target identification and selection: In most of the cases, this is a passive task that does not need interactions with the target. Subset tasks include: area and point target identifications. Basic information to collect include: target name, place, organization name, website, account, application, file name, etc.
- Target profiling (e.g., system, social)

- Target enumeration
- Target refinement
- Target validation
- Target analysis

K0536: Knowledge of Structure, Approach, and Strategy of Exploitation Tools (e.g., Sniffers, Keyloggers) and Techniques (e.g., Gaining Backdoor Access, Collecting/Exfiltrating Data, Conducting Vulnerability Analysis of Other Systems in the Network)

Exploitation Tools

There are different methods to classify exploitation tools. In one classification, exploitation tools can be classified into remote and local exploitation tools:

- A remote exploit works over a network without any prior access to the vulnerable system.
- A local exploit requires prior access to the vulnerable system.

Here is a brief description of exploitation tools listed in Kali Linux (https://tools.kali.org/tools-listing):

- Armitage: A GUI-based tool that is built on top of Metasploit framework. It supports scripts' execution, visualization, etc.
- Backdoor Factory: BDF can patch executable binaries with user desired shellcode and continue normal execution of the prebatched state.
- BeEF: Web browsers exploitation framework. It can be used in penetration testing to test targets against client-side attack vectors.
- cisco-auditing-tool: Perl scripts to scan Cisco routers for vulnerabilities.
- cisco-global-exploiter: Another Perl Cisco exploitation tool.
- cisco-ocs: Cisco scanning tool.
- cisco-torch: Scanning tool with multiple functionalities.
- Commix: Written in Python for testing web applications for possible vulnerabilities.
- Crackle: To crack and decrypt network packets.
- Exploitdb: Search through the exploit database (https://www.exploit-db.com/).
- jboss-autopwn: Java script JSP shell to target JBoss AS server.
- Linux Exploit Suggester: Scripts to track Linux vulnerabilities.
- Maltego Teeth: A multi-purpose application that can be used to collect information about people, machines, domains, IP addresses, etc.

- Metasploit Framework: Probably the most popular exploitation tool/framework. It represents a complete penetration platform to find, exploit, and validate vulnerabilities. Rapid7 owns the commercial version of Metasploit.
- MSFPC: A payload wrapper that generates multiple types of payloads.
- RouterSploit: An open source exploitation framework dedicated to embedded devices.
- SET: A Social-Engineer Toolkit for penetration testing.
- ShellNoob: Writing Python Shell codes.
- Sqlmap: A tool to search for and exploit SQL injection vulnerabilities.
- THC-IPV6: Attack weakness in network protocols such as IPv6.
- Yersinia: A framework for performing layer 2 (i.e., MAC or data link layer) attacks.

Traffic Sniffers

Many tools exist to list to and analyze incoming and outgoing network traffic. Network traffic analysis can be utilized in almost all cyber operation and forensic activities. Some of the popular open source sniffing tools are:

- TShark and Wireshark: Non-GUI and GUI tools for traffic sniffing and analysis. The tools are open source, widely popular, and can be used in most platforms. Wireshark (previously named Ethereal) is popular for using a large set of filters that can help network analysts find what they are searching for based on a large set of traffic related attributes in all OSI layers. Wireshark has also modules to sniff different interfaces (e.g., wireless, USB).
- Tcpdump: Similar to TShark, tcpdump is a lightweight console-based sniffing tool
- Kismet and KisMac: Wireless network sniffers
- Ettercap
- Ntop
- P0f

Keyloggers

Keyloggers are spying tools usually used part of hacking schemes. Once installed in a machine, it can record all keys logged by the user (i.e., while typing) and also mouse activities. The tools then typically email reports of those activities to the server installed by the hacker.

Keyloggers are typically blocked by most anti-malware systems. Users may not be able to download/install them unless if they disable their anti-malware system. Following is a list of some of the popular Keyloggers: Free keylogger, REFOG, DanuSoft, Revealer, Kidlogger, BlackBox Express, Spyrix, and G3 iSam.

Exploitation Techniques

Exploitation techniques can fall under different categories. We will divide them based on the different platforms or environments.

Software Exploitation Techniques

Software exploits can be categorized according to different types.

1. Vulnerability type

   Some of the popular software vulnerabilities:

   - Memory overflows, memory leaks, memory corruptions

     Those are seen in literature related to buffers, stacks, and heaps. Buffers just a block or portion of memory allocated for data storage of programs such as variables. Stack is another dynamic memory Buffer portion that is used to store data implicitly normally during the run time. Another one is the heap, also a buffer that can be used to store the program data explicitly.

     https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=%22Memory+corruption%22

     - Buffer overflow: Overflow exploits are old and classical. The term "Buffer" used is general because there are several types of Buffers that normally can be over flown such as stack and heap. A large list of Buffer overflows can be viewed at:
     - https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=%22buffer+overflow%22
     - Stack overflow
     - Heap overflow: A heap overflow condition is a Buffer overflow, where the Buffer that can be overwritten is allocated in the heap portion of memory.
   - Integer overflow or underflow: If a value is larger than the maximum value is used, it will trigger a segmentation fault (that can be further exploit).
   - (e.g., MS DirectX MIDI Lib), https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=%22integer+overflow%22
   - Heap spray: Code that sprays the heap will try to inject a certain sequence of bytes at a predetermined location in the memory of a target process by having it allocate (large) blocks on the process's heap and fill the bytes in these blocks with the right values.
   - https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=%22Heap+spray%22
   - Memory corruption
   - https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=%22Memory+corruption%22
   - Arbitrary write: This exploit is based on the ability to write user-controlled data to user-controlled locations. The attacker goal is to directly alter control-flow sensitive data.

- Arbitrary call: A very simple vulnerability to expose by attackers. It occurs whenever data that is control-flow sensitive, such as a function pointer or return address, gets corrupted. It requires knowing at least the address of user-controlled data.
- Format strings: Intentionally manipulated input strings from attackers can trigger such exploits especially when software developers provide no string validation techniques (e.g., using regular expressions).

In C programming language, disabling the "%n" specifier prevents using format string vulnerability to directly cause an arbitrary write primitive. However, format strings manipulation can still be used to exploit other vulnerabilities such as buffer overflow.

2. Local or remote software exploits

   Software exploits can also be divided based on whether they need to run on the same machine as the program that has the vulnerability (local) or run on one machine to attack a program running on another machine (remote).

   - Local code execution vulnerabilities:
   - https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=%22local+code+execution+vulnerability%22
   - Remote code execution vulnerabilities:
   - https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=%22remote+code+execution+vulnerability%22

Windows Exploitation Techniques

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=%22windows+exploit%22

- Windows stack overflows
- Windows heap overflows
- Kernel-based Windows overflows
- Windows Kernel Memory Corruption
- DCOM: (Distributed Common Object Model) and DCOM/Remote Procedure Calls
- Recon, fuzz, and exploit with Dave Aitel's SPIKE and other tools
- Structured Exception Handler (SEH): When an illegal operation occurs, such as divide by zero, the processor sends an exception. SHE can be exploited through: (1) Overwriting the pointer to the SEH chain, (2) overwriting the function pointer for the handler on the stack, or (3) overwriting the default exception handler.
- Internet Explorer (IE) exploits
- Windows user mode components (UMC) exploits

Table 9.1 shows a list of recorded Windows vulnerabilities and patches in 2014 (ESET 2015).

Table 9.1 Windows vulnerabilities in patches, 2014 (ESET 2015)

Component	Bulletin	Type	Vulnerability
Windows UMC	MS14-011	Remote Code	CVE-2014-0271, CVE-2014-0263, CVE-2014-0266,
VBScript	MS14-007	Execution(11)	CVE-2014-0301, CVE-2014-0317, CVE-2014-0315,
Direct2D, MSXML,	MS14-005,	Information	CVE-2014-1807, CVE-2014-1816, CVE-2014-0296,
DirectShow, SAMR,	MS14-016,	Disclosure(3),	CVE-2014-1824, CVE-2014-2781, CVE-2014-2780,
File Handling/	MS14-016	Security	CVE-2014-4060, CVE-2014-1814, CVE-2014-4074,
kernel32.dll, Shell	MS14-027,	Feature	CVE-2014-4114, CVE-2014-4917, CVE-2014-6332,
handier/shell32.dll,	MS14-030,	Bypass(4),	CVE-2014-6352, CVE-2014-6321, CVE-2014-4118,
Remote Desktop,	MS14-033,	Elevation of Privilege (9)	CVE-2014-6324, CVE-2014-6322, CVE-2014-6318,
Keyboard, Media	MS14-039,	Tampering(1)	CVE-2014-0316, CVE-2014-6363, CVE-2014-6355,
center/mcplayer.	MS14-041,		
dll, Installer,	MS14-043,		
Task Scheduler,	MS14-049,		
OLE, Message	MS14-054,		
Queuing Schannel,	MS14-060,		
Kerberos. Audio	MS14-062,		
Service, IIS, IME	MS14-064,		
(Japanese), GDI+/	MS14-066,		
gdi32.dll, RPC/	MS14-067,		
rpcrt4.dll. Graphics/	MS14-068,		
windowscodecs.dll	MS14-071,		
	MS14-074,		
	MS14-076,		
	MS14-078,		
	MS14-036,		
	MS14-047,		
	MS14-084,		
	MS14-085,		

(continued)

Table 9.1 (continued)

Component	Bulletin	Type	Vulnerability
Win32k	MS14-003,	Elevation of Privilege (4)	CVE-2014-0262, CVE-2014-0300, CVE-2014-0323,
	MS14-045,	Denial of Service (1)	CVE-2014-4148, CVE-2014-6317
	MS14-079		
KM drivers (ndproxy. sys, tcpip. sys, afd.sys, fastfat. sys)	MS14-002,	Elevation of Privilege (5)	CVE-2013-5065, CVE-2014-0254, CVE-2014-1811,
	MS14-031,	Denial of Service (2)	CVE-2014-4076
	MS14-045,		
	MS14-063,		
	MS14-070,		
.NET Framework	MS14-009,	Elevation of Privilege (3)	CVE-2014-0253, CVE-2014-0257, CVE-2014-0295
	MS14-046,	Security	(ASLR Bypass), CVE-2014-4072, CVE-2014-4073,
	MS14-053,	Feature	CVE-2014-4121, CVE-2014-4122 (ASLR Bypass),
	MS14-057,	Bypass(1),	CVE-2014-4149
	MS14-072	Denial of Service(1), Remote Code Execution(1)	

Figure 9.9 shows Windows exploitations per application. Windows user model components, Internet Explorer, and Office recorded highest number of reported exploits. In comparison with a similar chart, 2 years after in 2016, a new application, Edge shows rising volume of exploits (Fig. 9.10).

Linux Exploitation Techniques

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=%22linux+kernel%22

- Uninitialized/non-validated/corrupted pointer dereference: The main example on this category is null pointer dereference: In C/C++, a pointer is a variable that holds the address to another variable in memory. Each time the pointer is dereferenced, the value that is contained at the memory address it holds is retrieved.
- Memory corruption exploits, Kernel (stack and heap): As a result of code improperly implemented, kernel memory is corrupted and may overwrite memory content.
- Integer overflow and signedness exploits

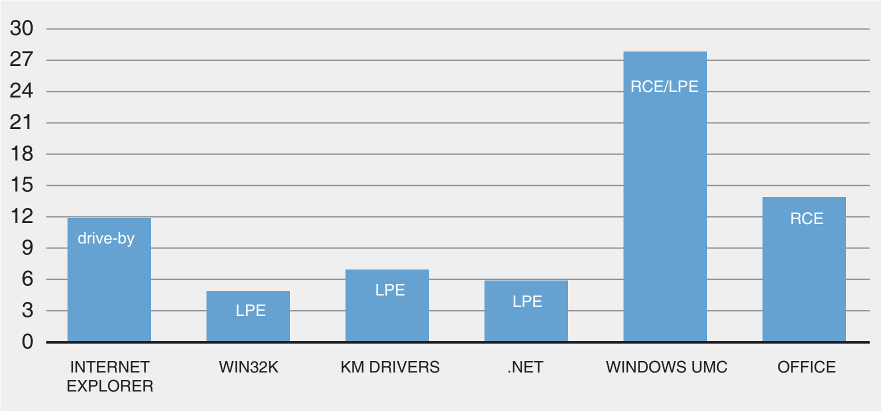


Fig. 9.9 Windows exploitation/application, in 2014 (ESET 2015)

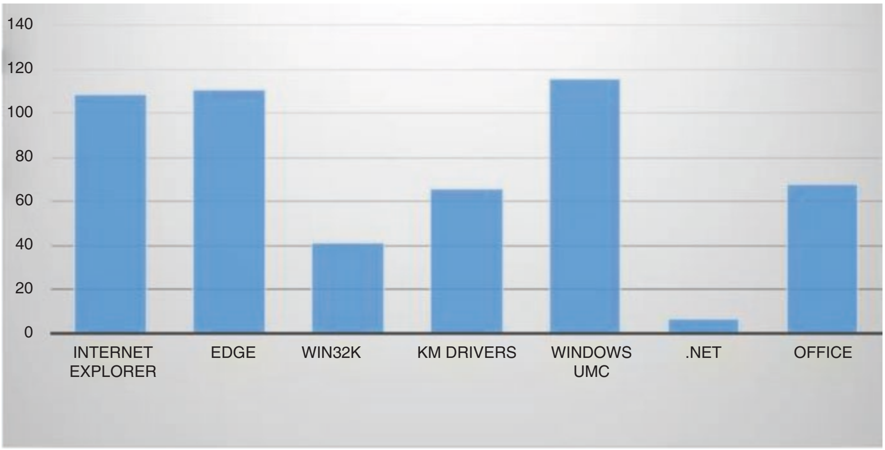


Fig. 9.10 Windows exploitation/application, in 2016 (ESET 2015)

- Race conditions: Different processes/threads (concurrent and interleaved) are competing for scarce resources.
- Logic bugs and exploits (e.g., CVE-2017-14398).
- Reference counter overflow exploits.
- Out of bounds (OOB) memory access exploits (e.g., CVE-2016-3710).
- Use-after-free (UAF) exploits: An object gets created and is associated with a v-table then (2) later on the object gets called by a v-table pointer. If we free the object before it gets called, the program will crash when it later tries to call the object (e.g., it tries to Use the object After it was Freed—UAF) (Fuzzy security 2018).
- Return-oriented programming.

Cisco OS Exploitation Techniques

https://www.cvedetails.com/vulnerability-list/vendor_id-16/product_id-19/Cisco-IOS.html

- +Priv CSRF (e.g., CVE-2018-0255, CVE-2018-0152).
- DoS Exec Code Overflow (e.g., CVE-2018-0151, CVE-2017-6744, CVE-2017-6743, CVE-2017-6740, CVE-2017-6739, CVE-2017-6738, CVE-2017-6737, CVE-2017-6736)
- Exec Code (e.g., CVE-2017-3881)
- DoS (e.g., CVE-2018-0180, CVE-2018-0179, CVE-2018-0174)
- DoS Exec Code (e.g., CVE-2018-0175)
- DoS Overflow (e.g., CVE-2018-0172)
- DoS Bypass (e.g., CVE-2015-0635)
- Bypass (e.g., CVE-2018-0163)

Another classification is provided by Exploit Database (https://www.exploit-db.com) (Fig. 9.11):

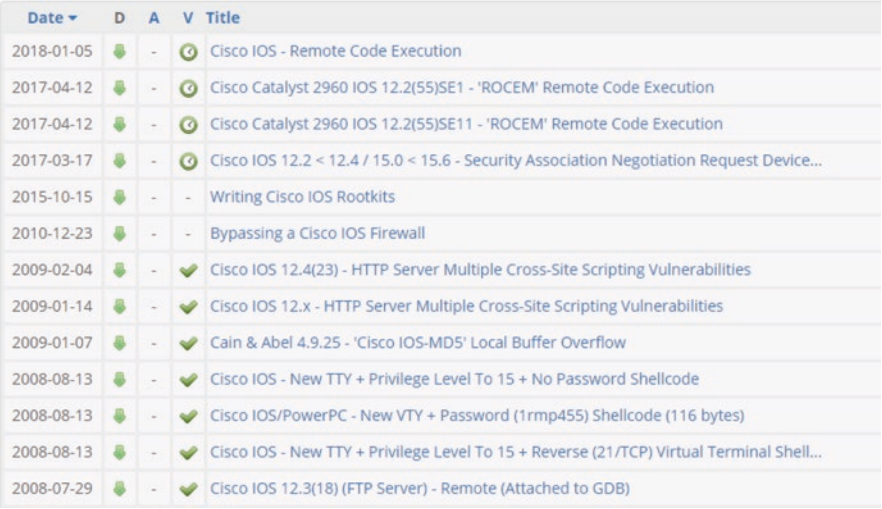
Recently, Cisco released the following exploits (http://techgenix.com/cisco-vulnerabilities/):

CVE-2018-0151, CVE-2018-0171, CVE-2018-0150

Apple iOS Exploitation Techniques

https://www.exploit-db.com/platform/?p=iOS

Apple iOS in the desktop, laptop, and mobile environment is a target for different types of attacks. Some of the OS vulnerabilities are used by national organizations



Date ▾	D	A	V	Title
2018-01-05	⬇	-	◷	Cisco IOS - Remote Code Execution
2017-04-12	⬇	-	◷	Cisco Catalyst 2960 IOS 12.2(55)SE1 - 'ROCEM' Remote Code Execution
2017-04-12	⬇	-	◷	Cisco Catalyst 2960 IOS 12.2(55)SE11 - 'ROCEM' Remote Code Execution
2017-03-17	⬇	-	◷	Cisco IOS 12.2 < 12.4 / 15.0 < 15.6 - Security Association Negotiation Request Device...
2015-10-15	⬇	-	-	Writing Cisco IOS Rootkits
2010-12-23	⬇	-	-	Bypassing a Cisco IOS Firewall
2009-02-04	⬇	-	✓	Cisco IOS 12.4(23) - HTTP Server Multiple Cross-Site Scripting Vulnerabilities
2009-01-14	⬇	-	✓	Cisco IOS 12.x - HTTP Server Multiple Cross-Site Scripting Vulnerabilities
2009-01-07	⬇	-	✓	Cain & Abel 4.9.25 - 'Cisco IOS-MD5' Local Buffer Overflow
2008-08-13	⬇	-	✓	Cisco IOS - New TTY + Privilege Level To 15 + No Password Shellcode
2008-08-13	⬇	-	✓	Cisco IOS/PowerPC - New VTY + Password (1rmp455) Shellcode (116 bytes)
2008-08-13	⬇	-	✓	Cisco IOS - New TTY + Privilege Level To 15 + Reverse (21/TCP) Virtual Terminal Shell...
2008-07-29	⬇	-	✓	Cisco IOS 12.3(18) (FTP Server) - Remote (Attached to GDB)

Fig. 9.11 Cisco OS vulnerabilities provided by: exploit-db.com

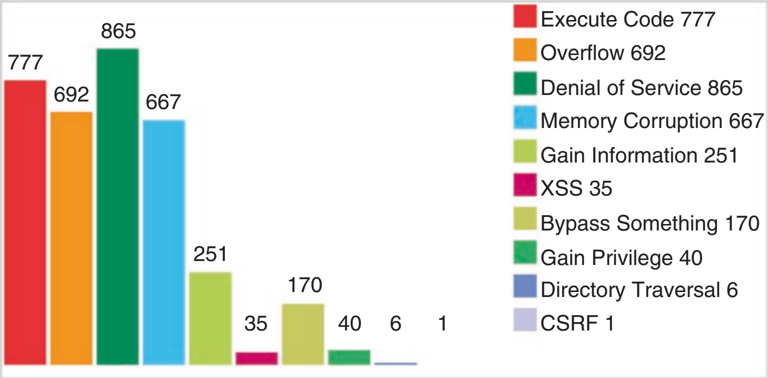


Fig. 9.12 iOS volumes and types of attacks (CVE Details 2018)

(https://wikileaks.org/ciav7p1/cms/page_13205587.html). Figure 9.12 shows recent volumes and categories of attacks on Apple iOS, CVE Details 2018. The following are the top five listed categories.

- Denial of Service, DoS, is a popular attack in most environments. It is usually used as part of major attacks, in early stages.
- Execute code or code execution: An attacker can exploit iOS to execute arbitrary code within the context of the affected application.
- Overflow exploits: Similar to the software and Windows Overflow exploits that were described earlier.
- Memory corruption.
- Gain information.

Figure 9.13 shows volume increase in attacks over the years with nearly continuous and steady increase of the different attacks over the years.

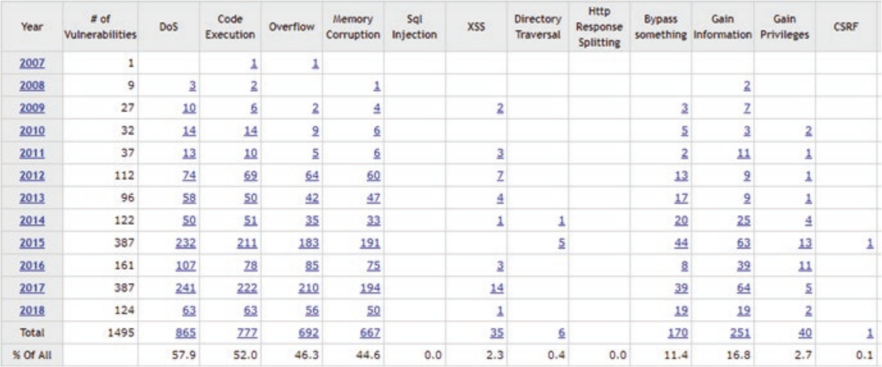
Android Exploitation Techniques

https://www.exploit-db.com/platform/?p=Android

https://www.cvedetails.com/vulnerability-list/vendor_id-1224/product_id-19997/Google-Android.html

Some of the serious or significant recent exploits on Android:

- Overflow attacks (e.g., CVE-2018-5850, CVE-2018-3580, CVE-2018-3578)
- +Priv (e.g., CVE-2011-2344, CVE-2013-7457, CVE-2014-7920 264, CVE-2014-7921)
- Exec Code Overflow (e.g., CVE-2014-9902)



Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF
2007	1		1	1									
2008	9	3	2		1						2		
2009	27	10	6	2	4		2			3	7		
2010	32	14	14	9	6					5	3	2	
2011	37	13	10	5	6		3			2	11	1	
2012	112	74	69	64	60		7			13	9	1	
2013	96	58	50	42	47		4			17	9	1	
2014	122	50	51	35	33		1	1		20	25	4	
2015	387	232	211	183	191			5		44	63	13	1
2016	161	107	78	85	75		3			8	39	11	
2017	387	241	222	210	194		14			39	64	5	
2018	124	63	63	56	50		1			19	19	2	
Total	1495	865	777	692	667		35	6		170	251	40	1
% Of All		57.9	52.0	46.3	44.6	0.0	2.3	0.4	0.0	11.4	16.8	2.7	0.1

Fig. 9.13 Vulnerability trends over time (CVE Details 2018)

K0540: Knowledge of Target Communication Tools and Techniques

Cyber security operations, offensive or defensive use different communication tools and techniques that are relevant to the mission goals and also the target. We will cover a subset of those most popular communication techniques.

Centralized Communication

The majority of Internet and network applications seen around us use a centralized network architecture in which two main entities exist:

- A server that provides the services. All websites that exist through the Internet are hosted by a form of a server. Server-side applications such as web servers (e.g., Microsoft IIS, Apache), email servers, information server, and many others provide services to their intended users.
- Clients that call and use services provided by the server. The architecture is centralized around the servers that represent the center of the architecture. If the server is down, then the whole network is down.

For legal and legitimate use, centralized servers are more controlled and secure. Examples of some of the limitations are related to creating a single point of control and failure. Performance and efficiency issues may exist especially when the server is incapable of handling the large number of concurrent clients or users.

P2P Communication

Peer-to-peer networks refer to networks in which communication channels occur dynamically between typically two users who are willing to communicate and share some information. Those two communication partners are peers, none of them is a server or a client.

From a security perspective, most of the gray area communication platforms (e.g., websites that exchange movies, files, songs) prefer this model. Additionally, such platforms are rich environments to spread malwares.

Covert or Anonymous Communication

Covert communication, a powerful anonymizing mechanism, is the transmission of information using system resources that were not intended for that purpose. The goal of covert communication is to hide the fact that the communication is being occurred.

Using proxies and Virtual Private Networks (VPNs) are covert communication mechanisms used by many users to ensure anonymity and privacy.

One popular example of covert communications is steganography, in which messages are hidden in other messages or (more typically) in pictures. Steganography has been used in human history for a long time and is still in use in many security-related operations.

One difference between encryption and steganography is that in encryption the goal is to completely hide a particular content or message, where in steganography the goal is to confuse users and hide "the existence" of a hidden message. In the scope of steganography, watermarking is very similar to steganography except that the goal in watermarking is largely "copyright-related" where the watermark in the message may not be hidden but cannot be removed.

Some common anonymous networks include TOR browser (https://www.torproject.org) Freenet (https://freenetproject.org), Tarzan (https://gnunet.org/tarzan), Gap GNU net (https://gnunet.org/gap), and I2P (https://geti2p.net).

K0546: Knowledge of Target List Development (i.e., RTL, JTL, CTL)

Each cyber operation has one or more systems or assets to target. The selection of the target takes into consideration the operation mission and what it is trying to achieve. In cyber targeting process, mission can also decide target granularity or fidelity (Cyber defense review 2016).

Target system analysis is a structured process to determine adversary vulnerabilities and exploits. It can show what effects will likely impact target systems and their associated activities. Analysts should review the functions and interactions between components and elements of a target to determine how they work.

By reviewing probabilities of damage and arrival for a weapon system, analysts can evaluate the effects of attacks to plan the interruption or neutralization of the target.

Cyber Target Template

A cyber target template is the information about the target for the attack. The goal of the target template is to decide several questions such as:

Who is in charge? Who runs the System administrator position?

There are several ways to access such information using specialized techniques that can enable an individual to bypass security.

Cyber Target Development

The process of providing timely and accurate locations of adversary targets that may impact on current or future operations.

Cyber target development includes different activities:

- Identification of cyber-enabled crime networks
- Identification of cyber-enabled actors
- Identification of cyber-enabled techniques that may represent a cyber threat to systemically important associated infrastructures, and exploitation of emerging technologies

Cyber targeting cycle includes four major steps (ATP-3-60, 2015):

- Observe: (e.g., target intelligence gathering)
- Orient: (focus on the target, weaknesses, TTPs)
- Decide: (e.g., weigh options and consequences)
- Act: execute and assess (Fig. 9.14)

Target development generally results in four products: target development nominations, target folders, collection and exploitation requirements, and target briefs (Global security, FM-3-60, 2010).

K0548: Knowledge of Target or Threat Cyber Actors and Procedures. K0549

Cyber actors try to obscure their actions through the rest of the Internet's traffic, where about five billion users are using this public network continuously. We described in an earlier KSA the major cyber actors: cyber criminals, cyber activists,

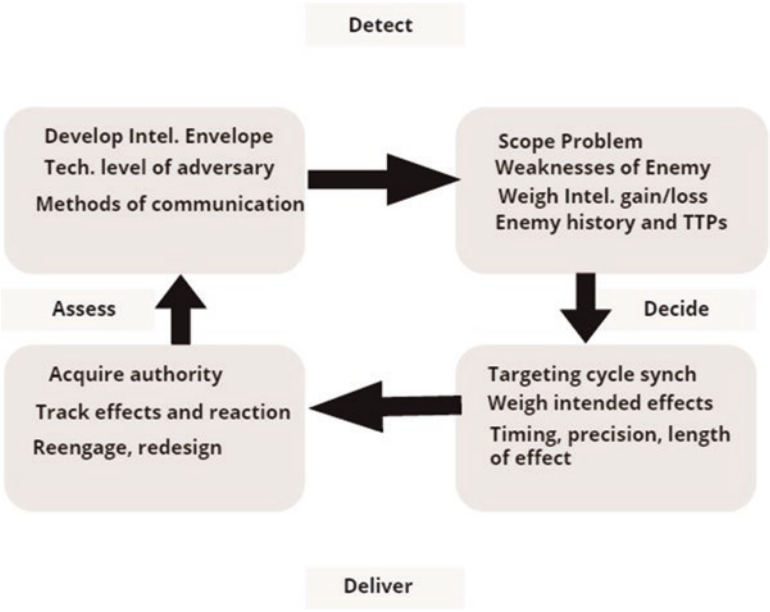


Fig. 9.14 An example of cyber targeting cycle (ATP-3-60, 2015)

and nation states. For nation states against the USA, top cyber actors include: Russia, China, North Korea, and Iran. According to a report by FireEye in 2013, new cyber nation states such as Taiwan, Brazil, and Poland are rising.

Although US organizations dominate and control a significant portion of the Internet, they also heavily rely on it for most of their business functions. From cyber security perspectives, this can create a large pool of candidate actors of all categories who are interested to target US infrastructure.

Legal laws try to distinguish cyber actors who are working as part of state wars from cyber actors who work independently (e.g., for financial, social, or political reasons). For example, the Tallinn Manual agrees that civilians who take a direct part in hostilities via cyber activity are “unprivileged belligerents” (NATO 2013, Schmitt 2013, Schmitt 2017).

The differences between some independent cyber actors are becoming less different from those state-actors or state-sponsored actors. Activity by some cyber criminals can be more sophisticated than those conducted by some nation states. States started expanding their cyber operations and power to offensive operations not only defensive operations as they realized that, sometimes, even for pure defensive and deterrence purposes, some cyber operations are necessary (Sliwinski 2014).

Cyber Attribution

Cyber attribution refers to the ability to identify cyber actors in a particular cyber operation. When an attack occurs, an organization often conducts investigations to attribute the incident to specific threat actors to gain a complete picture of the attack.

One of the main challenges in cyber attribution is related to having the right resources to conduct security and forensic analysis. For many organizations, such resources are not internally available and they may need to hire external security experts for such purpose.

Hackers employ different evasion techniques to avoid detection such as IP spoofing and anonymization.

K0549: Knowledge of Target Vetting and Validation Procedures

Target vetting is an intelligence function that assesses the accuracy and ensures the fidelity of the supporting intelligence in order to establish confidence in a candidate target's functional characterization (Joint targeting school 2014). Target vetting and validation must be revisited as new intelligence becomes available or as the situation changes.

At a minimum, the vetting considers the following factors:

- Target identification
- Target significance
- Collateral damage estimates and location issues
- Actions' impact on the enemy
- Intelligence gain/loss concerns

Target validation ensures that system targeting complies with the law of armed conflicts and the rules of engagement. Once targets are developed, vetted, and validated, planners nominate them for approval for military action in a given time period (M&S Journal 2013).

K0551: Knowledge of Targeting Cycles

The targeting cycle starts with finding the target and fixing its location. Traditionally, it is within the responsibility of signals intelligence (SIGINT) organizations.

D3A Targeting Framework

Target planning framework with four steps:

- Decide
- Detect
- Deliver
- Assess

F3EAD Targeting Cycle

F3EAD, Figure 9.15, is a version of the targeting methodology utilized by the special operations forces (SOF) that is responsible for some of the most highly publicized missions (Havok Journal 2017).

F3EAD involves the following six stages:

- Find: Establishing a start point for intelligence collection.
- Fix: It indicates that intelligence operation has enough information about the target to execute the operation or the mission.

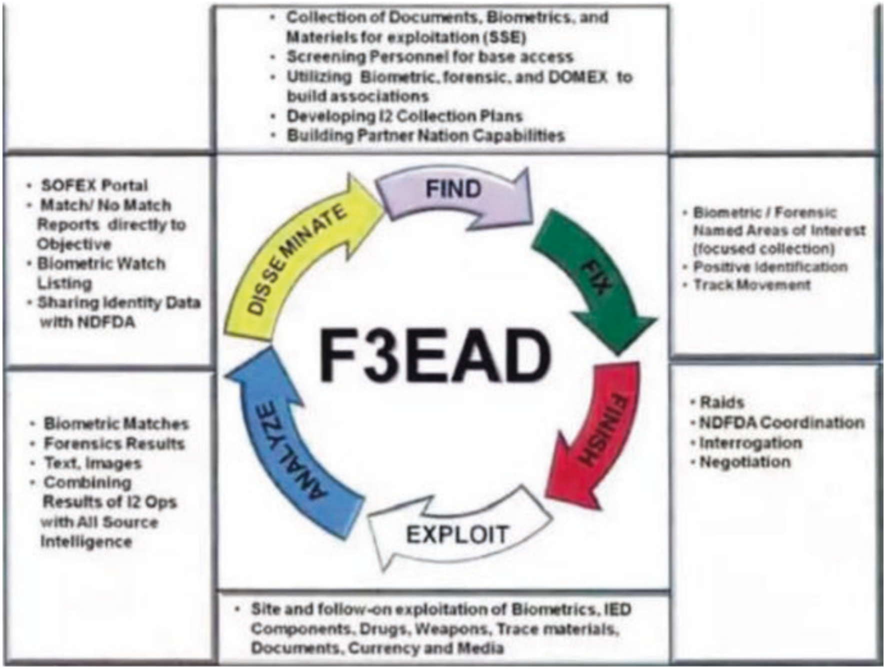

• Collection of Documents, Biometrics, and Materiels for exploitation (SSE)
• Screening Personnel for base access
• Utilizing Biometric, forensic, and DOMEX to build associations
• Developing I2 Collection Plans
• Building Partner Nation Capabilities
• SOFEX Portal
• Match/ No Match Reports directly to Objective
• Biometric Watch Listing
• Sharing Identity Data with NDFDA
FIND
FIX
FINISH
EXPLOIT
ANALYZE
DISSEMINATE
F3EAD
• Biometric / Forensic Named Areas of Interest (focused collection)
• Positive Identification
• Track Movement
• Raids
• NDFDA Coordination
• Interrogation
• Negotiation
• Biometric Matches
• Forensics Results
• Text, Images
• Combining Results of I2 Ops with All Source Intelligence
• Site and follow-on exploitation of Biometrics, IED Components, Drugs, Weapons, Trace materials, Documents, Currency and Media

Fig. 9.15 F3EAD targeting cycle (Trevithick 2017)

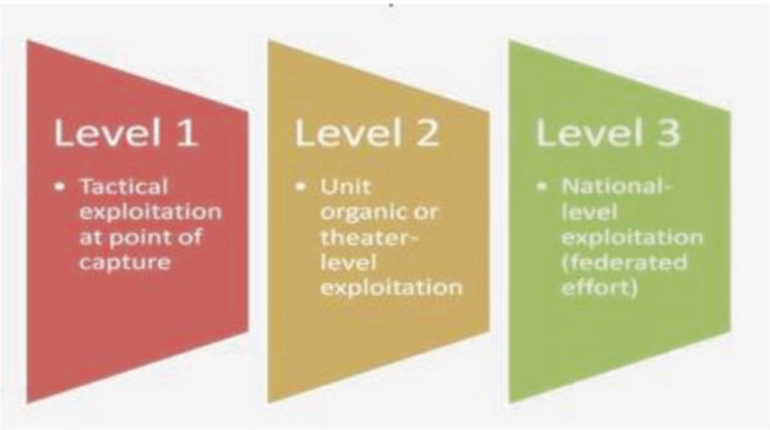

Level 1
• Tactical exploitation at point of capture
Level 2
• Unit organic or theater-level exploitation
Level 3
• National-level exploitation (federated effort)

Fig. 9.16 Exploitation levels (Faint and Harris 2011)

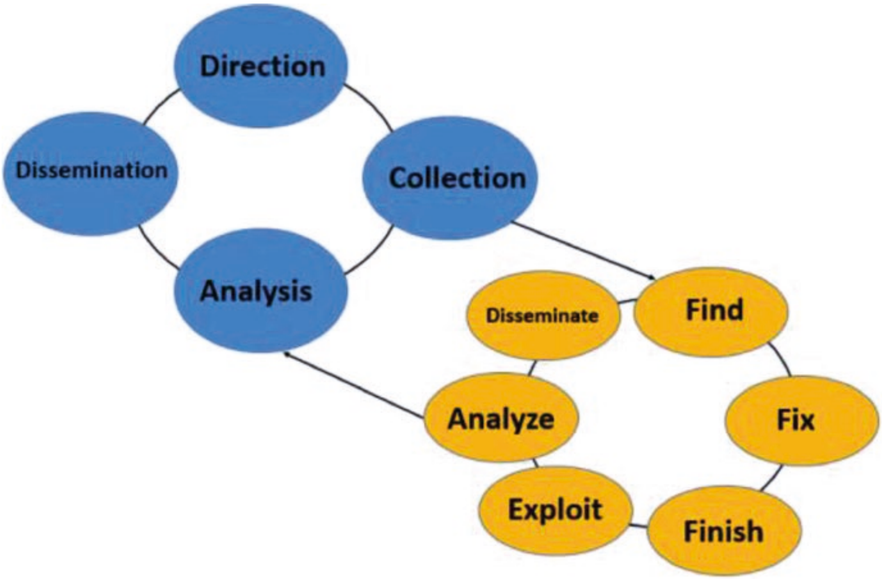


Fig. 9.17 Relation between intelligence and targeting cycles (Bertram 2017)

- Finish: Execute and finish specific mission or task on target.
- Exploit: Turn intelligence into evidence and action to prosecute adversary target. Exploitation can have three levels, Fig. 9.16 (Faint and Harris 2011).
- Analyze: Turn information collected in previous activities into intelligence to drive future operations (Fig. 9.17).
- Disseminate

Joint Targeting Cycles

Joint targeting cycle includes six steps (M&S Journal 2013):

1. End State and Commander's Objectives
2. Target Development and Prioritization
3. Capabilities Analysis
4. Commander's Decision and Force Assignment
5. Mission Planning and Force Execution
6. Assessment

K0603: Knowledge of the Ways in Which Targets or Threats Use the Internet

The Internet is a very large and convenient communication channel used by normal users, cyber actors, attacks, etc. to communicate with all types of media: emails, messages, files, videos, etc. We will focus on three main goals in which cyber attackers use the Internet: Communication, malware deployment, and information gathering or intelligence.

Communication

Hackers use the Internet to communicate about hacking tools, methods, etc. We described in an earlier KSA the large number of hacking websites and the type of information and services they provide. In fact, some, under cover, cyber security and intelligence agents visit those websites searching for intelligence information about hacking tools, mechanisms, zero-day exploits, etc.

Zero-day (i.e., never discovered or exploited before) exploits represent a big market in hackers' websites. Hackers learn from each other. Depending on their nature and personality, some hackers like to brag about their hacking skills and operations.

Malware Deployment

The Internet itself contributes to the significant increase of volumes and types of malwares. Some of the significant malware categories that took advantage of the Internet include:

- Worms: Before the Internet, majority of computer malwares were viruses. Viruses have the ability to spread through CDs, flash drives, etc. In comparison with worms, viruses propagate or spread from one victim machine to another slowly. Worms, using the Internet can spread through a large number of victim machines or users in a short amount of time. Due to this nature, worms because one of the most popular malware types in large-scale cyber-attacks.

- Spam emails and messages: Unsolicited messages can be used for marketing, financial and identity theft as well as in cyber-attacks. Similar to worms, spammers main goal is to be able to reach a large number of candidate audience where typically it is expected that a small percentage of those receivers will respond to and interact with the spam message.
- Flooding and denial of service: Attackers who want to target a server or a system to bring it down, accomplish this usually within two stages. In the first stage, they target transitional victims and control them. Those initial victims can then be used to perform a Distributed Denial of Service (DDoS) on the actual target. One of the key factors to succeed in such attacks is to push a large volume of traffic in a short amount of time.
- Ransomwares: Hackers attack users' machines to encrypt their files. Users will not be able to access those files except if they communicate with attackers and pay them to decrypt their files. The Internet made such attacks easy where victim users are typically reached through the Internet.

Information Gathering or Intelligence

Cyber attackers have their own information intelligence and collection processes. Every cyber offensive operation requires initial target identification, collection, and analysis stages. Table 9.2 shows Kali tools that can be used in information gathering stages.

Table 9.2 Kali information gathering tools (tools.kali.org)

acccheck	Dnsmap	goofile	SET
ace-voip	DNSRecon	hping3	smtp-user-enum
Amap	Dnstracer	InTrace	snmpcheck
Automater	Dnswalk	iSMTP	Sslcaudit
bing-ip2hosts	DotDotPwn	lbd	SSLsplit
braa	enum4linux	Maltego Teeth	Sslstrip
CaseFile	enumIAX	masscan	SSLyze
CDPSnarf	Exploitdb	Metagoofil	THC-IPV6
cisco-torch	Fierce	Miranda	theHarvester
Cookie Cadger	Firewalk	Nmap	TLSSLed
copy-router-config	Fragroute	ntop	Twofi
Dmitry	Fragrouter	p0f	URLCrazy
Dnmap	Ghost Phisher	Parsero	Wireshark
Dnsenum	GoLismero	Recon-ng	WOL-E
			Xplico

K0612: Knowledge of What Constitutes a "Threat" to a Network

We will introduce the following issues when considering "what constitutes a threat":

Subjectivity

Security is inherently political; not all actors share the same perspectives in terms of what is, or should be, the object of security, and/or what constitutes a "threat" (Deibert 2012).

Priority or Importance

Not all threats can pose the same level of risks. It is impossible, infeasible, or impractical to accommodate all system or organization risks. This will require very large amount of resources and time. Hence, every organization frequently monitors and prioritizes their risks. Based on the available resources, they will have to decide to deal with the most serious risks, currently.

Evolution and Dynamics

A risk or a threat that was very serious today or this year may not be as serious tomorrow or next year, or vice versa. Risks and threats should be continuously monitored as things continuously change. The priority or seriousness of a certain threat may go down as since it will be taken from the monitoring radar (i.e., to take actions against). Alternatively, this threat seriousness may stay the same while other threats advanced to become more important and serious to handle and deal with.

The Environment

The environment in which organizations operate is also very dynamic. For example, company overall security procedures, policies, etc. can be working very well for several years. However, due to changes in the environment, such security state is not anymore enough or effective. Some systems or applications are possibly vulnerable but never exploited before. However, that does not make them immune.

Those four factors that we described are only a subset of why defining what constitutes a threat in general is not an easy task. The answer to such question will have to be context-driven, given a certain: time, organization, environment, etc.

S0022: Skill in Designing Countermeasures to Identified Security Risks

A major category to security threats and risks includes all types of security controls such as:

- Anti-malware systems, antiviruses, anti-spams, etc.
- Firewalls (L2–L3, or L7 firewalls), port controls, etc.
- IDS/IPS
- Access controls (e.g., in operating systems, VPN, DBMS, switches, routers)
- Traffic monitoring tools, SIEM, SMTP, etc.
- Policy management tools and frameworks (e.g., ABAC, XACML)
- Privacy and information protection controls (e.g., encryption methods)
- Threat detection tools
- Security analytics

Security controls can also be classified based on how they filter permitted from denied users, applications, traffic, etc. Such classification can include:

- Simple dictionary-based mechanisms (e.g., Black vs. White lists).
- Signature-based mechanisms
- Role-based or anomaly-based mechanisms

Security controls or countermeasures can also be divided into:

- Physical controls or countermeasures (e.g., doors, gates, locks).
- Logical controls (e.g., passwords, fingerprints)
- Network controls (e.g., firewalls)

Countermeasures should take the following important factors into consideration:

- The importance/value of the asset. Not all organization or system assets have the same value (e.g., monetary, information sensitivity, liability). With hundreds of assets for a typical organization, protecting all assets with the same level of security control or protection may not be practical or feasible.
- The possible threats, risks, or vulnerabilities an asset may be exposed to. As we mentioned earlier, threats are very subjective, dynamic, and environment dependent. Additionally, the value an asset can have to possible attackers can be different. Bottom line, avoid making your assets an easy target for attackers to exploit.

- Countermeasures' cost and overhead. If a threat is inevitable, actions are necessary to either:
  - Stop the threat or lower the possibility of its occurrence (e.g., detection, prevention, or protection mechanisms).
  - Lower the impact of the threat once it occurs (e.g., tolerance, mitigation).

  Cyber countermeasures can be classified into:

- Cyber offense
- Cyber defense
- Cyber deterrence

S0044: Skill in Mimicking Threat Behaviors.

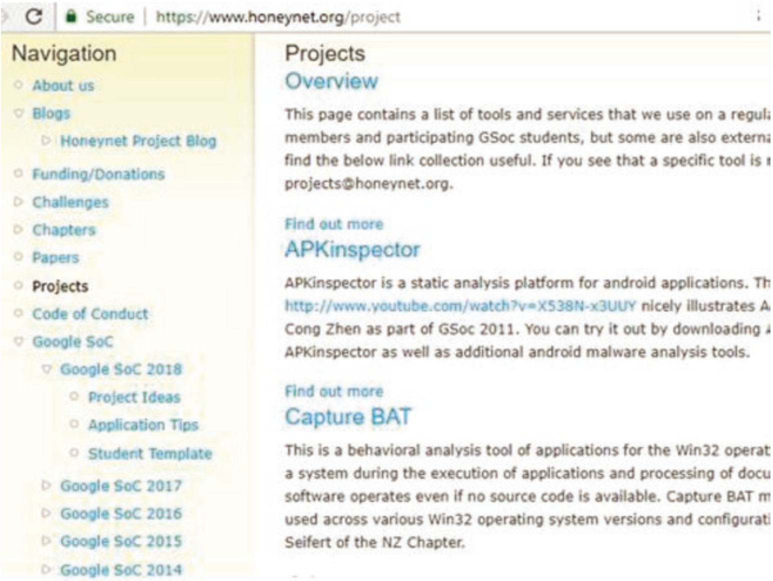
Threat analysis techniques are used to understand how threats behave in attack modes. One of the most common techniques to study attacker and malware behavior are target simulation tools honeypots or honeynets. They can be used to detect different types of malicious attackers including spammers and possible insiders. Honeypots simulate some vulnerable system aspects in order to trap in attackers to study what actions they take and their attacking steps or behaviors (Edgar and Manz 2017).

Examples of free or open source honeypot projects that can be used for threat behavior analysis:

- Tools described in Honeynet.org project: The Honeynet.org project, https://www.honeynet.org, includes a large list of tools that can be used in threats' analysis (Fig. 9.18).
- Another last categorized list of honeypots is included in https://github.com/paralax/awesome-honeypots (Fig. 9.19)

There are several categories of threat simulation tools that are useful in understanding the different tasks and behaviors of attackers. This includes (Edgar and Manz 2017):

- Failure simulators: The main goal in those tools is to test systems' behaviors in failure scenarios. While security controls and defense mechanisms focus on protecting systems from failures to begin with, however, they should not leave those systems reach unaccounted-for behaviors if they fail (e.g., under exceptional attacks, natural disasters).
- Vulnerability scanners: Many open source and commercial vulnerability scanners exist to test systems, applications, or components for different categories of vulnerabilities. OWASP listed a good selection of those commercial, free, and open source vulnerability scanners that users can evaluate (OWASP 2018) (Fig. 9.20).



Secure | https://www.honeynet.org/project

Navigation

- About us
- Blogs
  - Honeynet Project Blog
- Funding/Donations
- Challenges
- Chapters
- Papers
- Projects
- Code of Conduct
- Google SoC
  - Google SoC 2018
    - Project Ideas
    - Application Tips
    - Student Template
  - Google SoC 2017
  - Google SoC 2016
  - Google SoC 2015
  - Google SoC 2014

Projects

Overview

This page contains a list of tools and services that we use on a regul members and participating GSoc students, but some are also extern find the below link collection useful. If you see that a specific tool is projects@honeynet.org.

Find out more

APKinspector

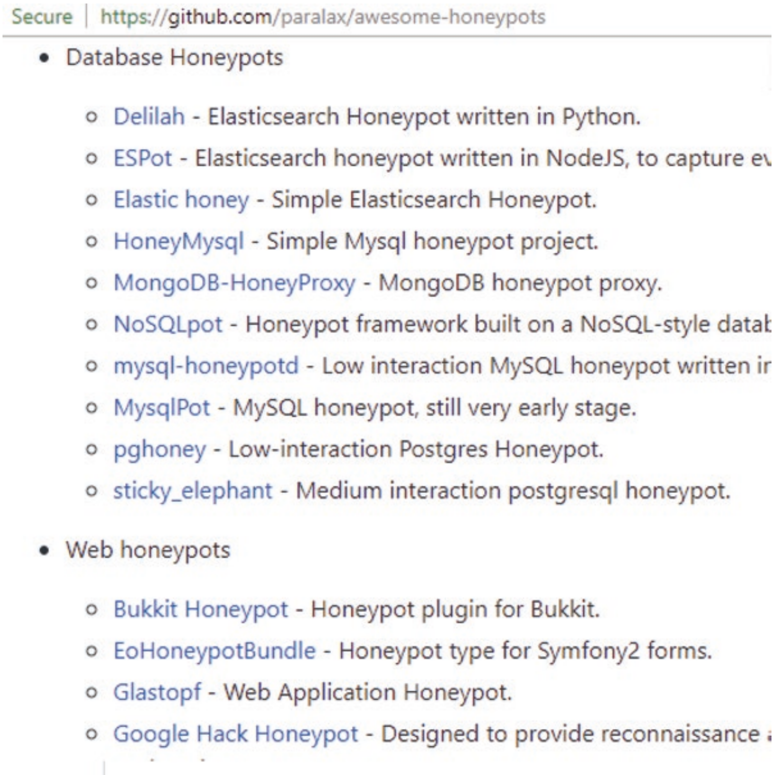
APKinspector is a static analysis platform for android applications. Th http://www.youtube.com/watch?v=X538N-x3UUY nicely illustrates A Cong Zhen as part of GSoc 2011. You can try it out by downloading APKinspector as well as additional android malware analysis tools.

Find out more

Capture BAT

This is a behavioral analysis tool of applications for the Win32 operat a system during the execution of applications and processing of docu software operates even if no source code is available. Capture BAT m used across various Win32 operating system versions and configurat Seifert of the NZ Chapter.

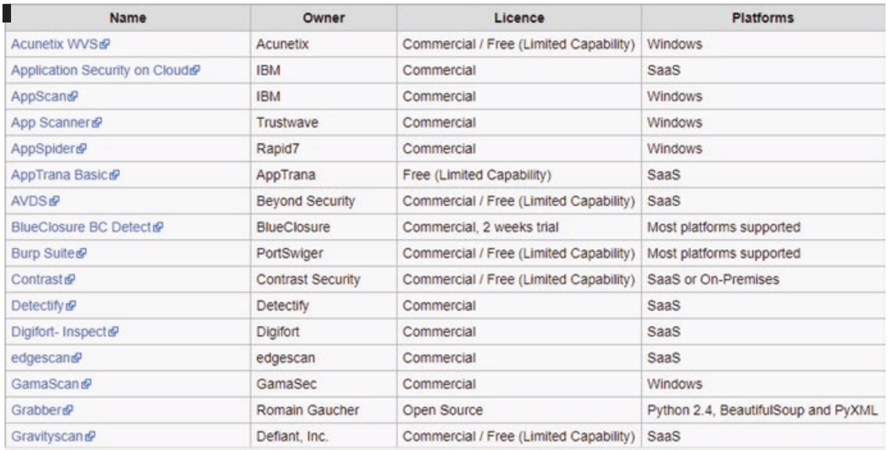
Fig. 9.18 Honeynet project tools (https://www.honeynet.org)



Secure | https://github.com/paralax/awesome-honeypots

- Database Honeypots
  - Delilah - Elasticsearch Honeypot written in Python.
  - ESPot - Elasticsearch honeypot written in NodeJS, to capture e
  - Elastic honey - Simple Elasticsearch Honeypot.
  - HoneyMysql - Simple Mysql honeypot project.
  - MongoDB-HoneyProxy - MongoDB honeypot proxy.
  - NoSQLpot - Honeypot framework built on a NoSQL-style data
  - mysql-honeypotd - Low interaction MySQL honeypot written i
  - MysqlPot - MySQL honeypot, still very early stage.
  - pghoney - Low-interaction Postgres Honeypot.
  - sticky_elephant - Medium interaction postgresql honeypot.
- Web honeypots
  - Bukkit Honeypot - Honeypot plugin for Bukkit.
  - EoHoneypotBundle - Honeypot type for Symfony2 forms.
  - Glastopf - Web Application Honeypot.
  - Google Hack Honeypot - Designed to provide reconnaissance

Fig. 9.19 Examples of Honeypot tools (https://github.com/paralax/awesome-honeypots)



Name	Owner	Licence	Platforms
Acunetix WVS	Acunetix	Commercial / Free (Limited Capability)	Windows
Application Security on Cloud	IBM	Commercial	SaaS
AppScan	IBM	Commercial	Windows
App Scanner	Trustwave	Commercial	Windows
AppSpider	Rapid7	Commercial	Windows
AppTrana Basic	AppTrana	Free (Limited Capability)	SaaS
AVDS	Beyond Security	Commercial / Free (Limited Capability)	SaaS
BlueClosure BC Detect	BlueClosure	Commercial, 2 weeks trial	Most platforms supported
Burp Suite	PortSwiger	Commercial / Free (Limited Capability)	Most platforms supported
Contrast	Contrast Security	Commercial / Free (Limited Capability)	SaaS or On-Premises
Detectify	Detectify	Commercial	SaaS
Digifort- Inspect	Digifort	Commercial	SaaS
edgescan	edgescan	Commercial	SaaS
GamaScan	GamaSec	Commercial	Windows
Grabber	Romain Gaucher	Open Source	Python 2.4, BeautifulSoup and PyXML
Gravityscan	Defiant, Inc.	Commercial / Free (Limited Capability)	SaaS

Fig. 9.20 Examples of vulnerability scanners (OWASP 2018)

- Exploit testing platforms: One of the most popular open source exploit platforms that users can evaluate is in Metasploit (https://www.metasploit.com). Canvas (Immunity 2017) and Core Impact (CoreSecurity 2017) are examples of commercial exploit frameworks.
- Social engineering: Many organizations start conducting frequent social engineering trainings and exercises to increase employees' security awareness and be careful when dealing with messages from strangers.

S0052: Skill in the Use of Social Engineering Techniques

Social Engineering Techniques for Cyber Operations and Vulnerability Assessment

- Baiting: In this technique, an attacker offers an incentive (i.e., a bait) to target victims and trick them.
- Pretexting: In pretexting, attackers use misrepresentations to gain access to privileged information.
- Phishing emails and messages: Phishing is a technique in which attackers attempt to obtain users' private information.
- Whaling or Spear-phishing: This is a targeted phishing type where a selection of high profile victims is targeted by the attack. Search engines and online social networks (OSNs) are used to collect information about those whales before targeting them.
- Spoofing, identity theft, or impersonation: Attackers can fake their identities as legitimate users or websites. They may hack legitimate users accounts (e.g., email accounts, Facebook, Twitter) and then use those hacked accounts for social

engineering attacks to the victim friends. In another example, attackers may fake identities for known company personnel (e.g., CEO, CTO). When employees receive emails from such persons, they will have little doubt that those emails are illegitimate.

- Piggybacking, jargon, and dropping: Techniques in which attackers gain insider information and use it to gain victims' trust.
- Influence and persuasion: Interacting with victims through emails, phone calls, messages, etc. and create trust to trick them into any type of risky actions that can cause information exposure, assets' destruction, etc.

S0109: Skill in Identifying Hidden Patterns or Relationships

Hidden patterns include knowledge that cannot be extracted directly from an event. Those are typically discovered by data mining techniques such as: sequential pattern, time-series mining, predictive mining, clustering analysis, and association rules. Some of the more recent techniques include deep learning and big data.

When an incident occurs, the ability to perform effective root-cause analysis within short and critical time windows can be of extreme importance and can distinguish a success from failure cyber team. As such, cyber team should have the right tools and skills to accomplish discovery of such knowledge within an acceptable time window.

Examples of hidden patterns in cyber security and analytics that can be discovered using those previous techniques include:

- Trends and behaviors for users (e.g., normal users or attackers)
- Accounts abuse or misuse
- Hackers classifications, clusters, or segments
- Associations roles (e.g., two types of behaviors that are usually associated with each other)

Information leaks or different types of abnormal behaviors.

Bibliography

Akamai's [state of the internet]/security, Q1 2017 report (2017) www.akamai.com

ATP 3-60 (FM 3-60) (2015) https://fas.org/irp/doddir/army/atp3-60.pdf

Bano R (2010) "Muslim women 'Radicalised' in UK." http://news.bbc.co.uk/2/hi/uk_news/8496821.stm (Last Accessed 4 February 2010)

Bertram SK (2017) F3EAD: find, fix, finish, exploit, analyze and disseminate – the alternative intelligence cycle. Digital shadows

Checkpoint (2016) How to choose your next sandboxing solution

Control Risks Group Limited (2015) Cyber threats to the Mexican financial sector

Core Security (2016) Core impact. https://www.coresecurity.com/core-impact. Retrieved 23 Feb 2017

Core Security (2017) DGAs in the hands of cyber-criminals, examining the state of the art in malware evasion techniques

CVE Details 2018 The ultimate security vulnerability data source. https://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49

Rock DM, Wright DR (2006) Cyber Attack: The Department of Defense's Inability to Provide Cyber Indications and Warning, dtic.mil. http://www.dtic.mil/dtic/tr/fulltext/u2/a499025.pdf

Cyber Threat Analysis, general security, July 17th 2014. https://resources.infosecinstitute.com/cyber-threat-analysis/#gref

Cyber warfare is no computer game. M&S Journal, Summer 2013

Deibert R (2012) Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace. Journal of military and strategic studies. 14

Department of the Army. Army Techniques Publication (ATP) 3-60, 1 May 2015, 2-1. http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/atp3_60.pdf

Edgar TW, Manz DO (2017) Research methods for cyber security. Elsevier Syngress, Waltham

ESET (2015) Windows exploitation in 2014. https://www.welivesecurity.com/wp-content/uploads/2015/01/Windows-Exploitation-in-2014.pdf

ESET (2017) Windows exploitation in 2016. https://www.welivesecurity.com/2017/01/05/windows-exploitation-2016/

F3EAD: Ops/Intel Fusion "Feeds" The SOF Targeting Process, by Charles Faint and Michael Harris. Small Wars Journal, January 31, 2012

FireEye (2013) World War C: understanding nation-state motives behind today's advanced cyber attacks. FireEye white paper, pp 1–21

FM 3-60 (2010) The targeting process. Department of the Army. https://www.globalsecurity.org/military/library/policy/army/fm/3-60/fm3-60.pdf

Frei S, Artes F (2012) Cybercrime kill chain vs. defense effectiveness. NSS labs, Austin

Fuzzy security (2018) https://www.fuzzysecurity.com/tutorials.html

Hulnick AS (2005) Indications and warning for homeland security: seeking a new paradigm. Int J Intell Counter Intell 18(4):599–600

Immunity (2017) Canvas. Retrieved February 23, 2017, from https://www.immunityinc.com/products/canvas/

Joint Fires and Targeting Student Guide (2014) http://www.jcs.mil/Portals/36/Documents/Doctrine/-training/jts/jts_studentguide.pdf?ver=2017-12-29-171316-067

Julian Assange (2014) OR Books announces a major new book with Julian Assange, Available: http://cryptome.org/2014/04/google-wikileaks.htm last accessed 2nd April 2014

Keragala D (2016) Detecting malware and sandbox evasion techniques. SANS

MITRE (2018) https://attack.mitre.org/

Montgomery J (2016) Division cyber operations. Cyber defense review, May 16th 2016

NATO (2013) The Tallinn Manual on International Law Applicable to Cyber Warfare. Cambridge: Cambridge University Press, 215p

OWASP (2018) Category: vulnerability scanning tools, https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools

Resilient Intelligent Networks (2015) 8 most common sandbox evasion techniques & the best cyber security solutions. http://www.resilientiq.com/blog/common-sandbox-evasion-techniques

Robinson M, Astrich C, Swanson S (2012) Cyber threat indications & warning: predict, identify, counter. Small Wars J, http://smallwarsjournal.com/jrnl/art/cyber-threat-indications-warning-predict-identify-and-counter

SANS (2003) Intrusion detection evasion: how attackers get past the burglar alarm

Schmitt M (2013) Cyberspace and international law: the penumbral mist of uncertainty. Harvard, 126(176), 176–80

Schmitt M (Ed.) (2017) "Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare, Cambridge University Press

Sliwinski KF (2014) Moving beyond the European Union's weakness as a cyber-security agent. Contemp Security Policy 35(3):468–486

Stevanovic M, Pedersen JM (2013). Machine learning for identifying botnet network traffic

Talamantes A, Kight T (2017) Building a threat-based cyber team. Splunk

Tan KMC, Killourhy KS, Maxion RA (2002) Undermining an anomaly-based intrusion detection system using common exploits. In: Wespi A, Vigna G, Deri L (eds) Recent advances in intrusion detection (RAID). Springer, Berlin, pp 54–73

Tier one targeting: special operations and the F3EAD process. The Havok Journal, 12 Jun 2017

Trevithick J (2017) "Identity Intel Ops" Turn US Special Operators into Combat Detectives. thedrive.com

U.S. Department of Defense (2012) Joint Operational Access Concept (JOAC) Version 1.0. United States Department of Defense, Washington, DC, Foreword. http://www.defense.gov/pubs/pdfs/JOAC_Jan%2012_Signed.pdf

Vaida B (2003) Warning center for cyber-attacks is online, official says, daily briefing. GovExec.com

Vashisht SO, Singh A (2014) Turing test in reverse: new sandbox-evasion techniques seek human interaction. FireEye

Wagner D, Soto P (2002) Mimicry attacks on host-based intrusion detection systems. In: ACM conference on computer and communications security (CCS), pp 255–264

Wirtz JJ (2013) Indications and warning in an age of uncertainty. Int J Intell Counter Intell 26(3):550

Chapter 10
Cyber Security Management

Cyber security management integrates different processes to achieve the overall goal of corporate systems' and assets' protection, Fig. 10.1 (SANS, Dexter 2002).

Figure 10.1 shows the four major components of cyber security managements:

- Corporates' different assets to protect.
- Policies: Organizations should have security policies to control users' interactions with assets: risk managements, passwords, incident handling, etc.
- Technologies to implement and enforce security controls and processes.
- Planning, training, etc.

K0147: Knowledge of Emerging Security Issues, Risks, and Vulnerabilities

IoT Security Issues

Internet of Things (IoTs) continue to grow to cover different types of applications to connect us, our appliances, our gadgets, etc. with the Internet. Information uploaded from those devices or exchanged with them is very vital and can affect us significantly. As a result, security threats and attacks that can come through those devices impact us seriously.

Unlike powerful computing devices (e.g., HPCs, computing servers), or even normal computing devices (e.g., desktops, laptops, tablets, smart devices), most of IoT devices are much simpler than those previously mentioned in terms of computing power (e.g., processing, memory, storage, network).

OWASP (www.owasp.org) IoT project described the following as the top ten security issues/vulnerability categories in IoT devices/environments: Insecure Web Interfaces, Insufficient Authentication/Authorization, Insecure Network Services,

I. Alsmadi, *The NICE Cyber Security Framework*,
https://doi.org/10.1007/978-3-030-02360-7_10

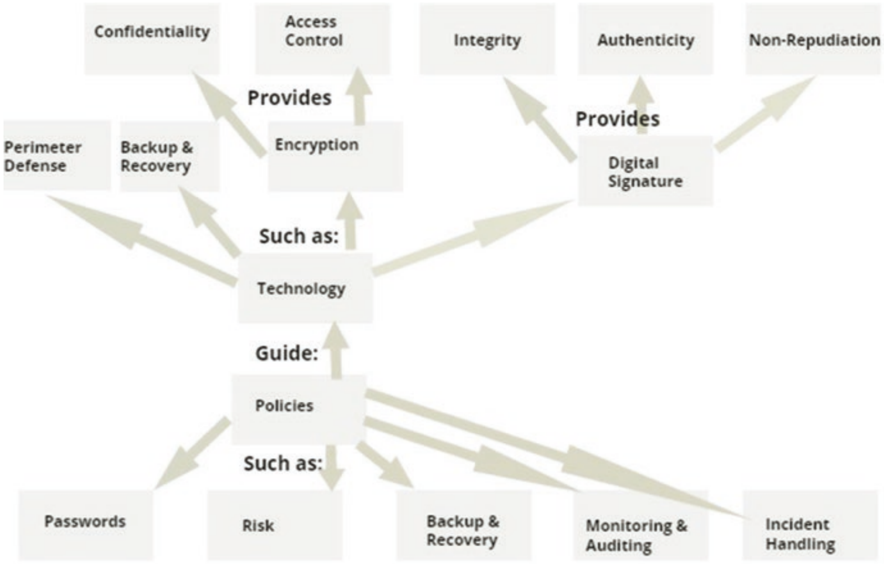


Fig. 10.1 Cyber security management (SANS, Dexter 2002)

Lack of Transport Encryption, Privacy Concerns, Insecure Cloud Interfaces, Insecure Mobile Interfaces, Insufficient Security Configurability, Insecure Software/Firmware, and Poor Physical Security.

Cryptocurrency, Bitcoin, Blockchain, and Security

Bitcoin is an emerging cryptocurrency method that records all transactions in a distributed public register called blockchain.

Blockchain main goal is to enable secure exchange of files and data between parties that have no formal or persistent communication. Blockchain relies on a ledger to keep track of all financial transactions. In blockchain, there are many distinct nodes. Each node has a complete copy of the digital ledger. These nodes can independently work to verify the transaction. If all the nodes don't agree, then the transaction is canceled. For blockchain to work properly, the number of nodes should be at least in terms of hundreds. The owners of these nodes are called miners. Miners who successfully add new blocks to the chain will earn Bitcoins as a reward.

Typically, this kind of central ledger would be an obvious point of vulnerability where if this centralized repository is targeted, the whole system will be compromised. Examples of attack goals will be to steal private/sensitive information (information exposure), change money values, changing or manipulating the chain (tampering), or simply bringing this system or service down (DoS).

Two main procedures in the system to ensure security:

- A cryptographic fingerprint, called hash, that is unique to each block.
- A consensus protocol which is the process by which the nodes in the network agree on a shared history.

One example of a recent Bitcoin attack is on NiceHash, a third-party Bitcoin mining company that was recently hacked, losing more than $60 million of cryptocurrency.

In summary, Bitcoin as a system is not inherently insecure. Similar to many other systems, vast majority of Bitcoin security breaches are related to human errors.

Security in the Cloud

Cloud computing is a new emerging concept in computing technology that utilizes Internet and remote servers to maintain data and applications. Security and privacy issues present a strong barrier for users to adapt into cloud computing. Issues related to information location by users pose a challenge to cloud computing security. Another issue is related to information segregation since information on the cloud is stored on devices that are shared with other cloud users. Finally, recovery is another important issue and the biggest challenge is the need for a contingency plan that cloud users can trust when information is threatened by security risks.

Security in Online Social Networks

The usage of online social networks, such as Facebook, YouTube, Twitter, and Instagram, is continuously and rapidly growing. Figure 10.2 shows Top OSNs in terms of No. of active users, in millions (Statista.com 2018).

OSNs start to be one of the main markets for hackers to distribute malwares for different reasons including:

- The large number of active users in OSNs. Many of those users are very active on daily bases, sending and receiving different types of media files. This makes them more vulnerable in terms of their readiness to accept and view files, links coming from friends or maybe even strangers.
- OSNs regular users may lack the basics of security training and awareness.
- Most users in OSNs are willing to expand their reach and networks. Once they accept new friends and if they have default security settings, such “friends” can expose them to different types of vulnerabilities.
- While most of those OSN architectures are centralized, yet security/privacy settings are left to users.

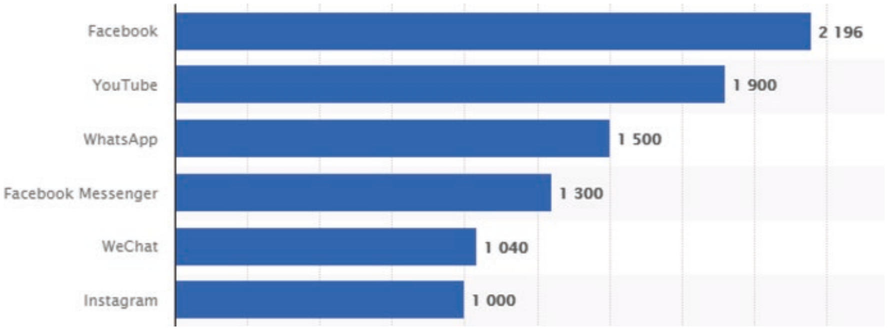


Fig. 10.2 Top OSNs in terms of number of active users, in millions (Statista.com 2018)

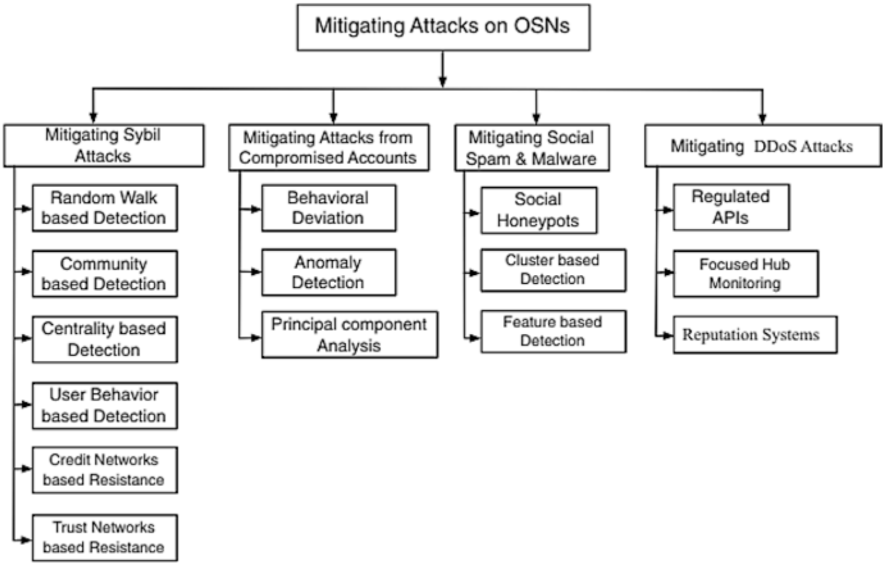

Mitigating Attacks on OSNs
Mitigating Sybil Attacks
Random Walk based Detection
Community based Detection
Centrality based Detection
User Behavior based Detection
Credit Networks based Resistance
Trust Networks based Resistance
Mitigating Attacks from Compromised Accounts
Behavioral Deviation
Anomaly Detection
Principal component Analysis
Mitigating Social Spam & Malware
Social Honeypots
Cluster based Detection
Feature based Detection
Mitigating DDoS Attacks
Regulated APIs
Focused Hub Monitoring
Reputation Systems

Fig. 10.3 Attacks and mitigations on OSNs (Kayes and Iamnitchi 2015)

In one approach, authors in, (Kayes and Iamnitchi 2015) described mitigations in OSN attacks based on four categories of attacks, Fig. 10.3:

- Sybil attacks: Users assuming multiple identities to manipulate the outcome of an action
- Comprising accounts
- Spams and malwares
- Flooding and DoS attacks

Smart Phones and Security

Mobile operating systems are the ground applications on mobile devices. They orchestrate control and management activities between (1): users, (2): their applications, (3): Internet and data service providers, (4): app-stores, as well as (5): others users and (6): their mobile devices. As a result, security in mobile devices can inherit strengths and weaknesses from any category of those five categories previously mentioned. Users like to associate weaknesses the operating system of their mobile or the applications they are using. However, most attacks start by tricking users to make the first stage in the malware attack.

In comparison with other mobile operating systems, Android platform is more popular and open source. From a security perspective and based on several statistics and malwares, Android is still more vulnerable than iOS or other mobile operating systems. Developers use popular programming languages such as C++ and Java to develop Android applications. Nonetheless, such statistics can always have different interpretations. For example, the popularity and openness of Android have many advantages while from a security perspective, it is expected to be more targeted. Such exposure can bring more vulnerabilities and simultaneously more fixes to those vulnerabilities. Android allows installing applications from third-party sources. While this has several advantages related to Android openness and flexibility, this seems to be one of the most serious sources of security vulnerabilities for Androids. While users should be aware of such issues and be careful of making decisions to install such applications from third parties, Android should find methods to make sure that malwares from those untrusted websites can be quarantined. Mobile platforms may need to enforce security policies to third-party application providers. Users will then only be allowed to install applications from those providers once those applications pass security policies.

In addition to vulnerabilities that may come from mobile operating system or installed applications, the mobile hardware and the network (i.e., data and voice providers) can also be sources of vulnerabilities that can be exposed by hackers. In this section, we will describe examples of security issues in the hardware and the networks of mobile phones.

Apple iPhone listed the followings as device/hardware security mechanisms or tools:

- Passcode protection
- iOS pairing model
- Configuration enforcement
- Mobile device management (MDM)
- Device restrictions
- Remote wipe
- “Find My iPhone” and “Activation Lock”

K0173: Knowledge of Operations Security

Operations Security (OPSEC) is the process in which critical information is protected through executing selected measures that eliminate or reduce adversary exploitation of those critical information. The focus is on preventing adversaries' access to information and actions that may compromise security or business operations. The term starts from military to refer particularly to protecting unclassified information.

Examples of potential critical information (aglearn.usda.gov 2018):

- Operations planning information
- Travel itineraries
- Passwords
- Inspection results
- Budget information
- Entry/exit security procedures

OPSEC indicates that information that is considered unclassified and no problem to be publicly exposed will not be so if aggregated with several other instances of "unclassified information" about the same subject. Currently, details about any person can be found online. Users can do their own search or can use websites that "sell" people information. While information in such websites seem to be private, those websites claim that such information is unclassified, aggregated from different public sources and records. You can check the link (http://www.willyancey.com/finding.htm#Public_Records) which includes a large list of "public records" websites that can be used to extract information about people, cases, businesses, etc.

Here is a list of websites that can be used to search for people:

- https://pipl.com/
- https://www.intelius.com/email-search-name
- https://linkedin.com
- http://www.yasni.com/
- https://www.lexisnexis.com/en-us/products/public-records.page
- https://search.fb.com/
- https://www.peoplesmart.com/
- https://connect.data.com/

OPSEC process includes five steps (Fig. 10.4):

K0242: Knowledge of Organizational Security Policies

Organizational security policies represent a set of rules or procedures that is imposed by an organization on its operations to protect its sensitive data and regulate its users and activities.

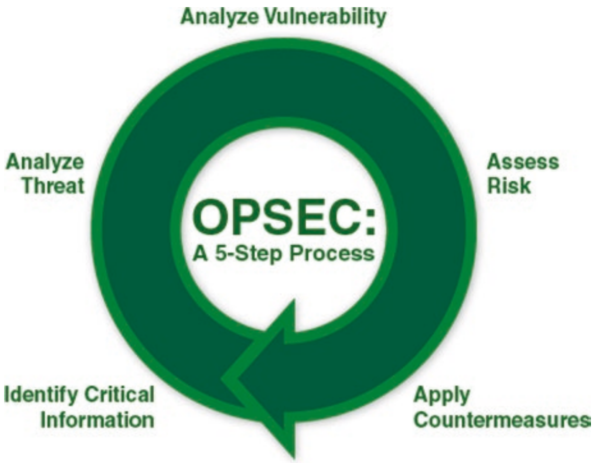


Fig. 10.4 OPSEC steps (aglearn.usda.gov 2018)

The development of organization security policies serves several policies such as:

- Set the rules for users' expected behaviors
- Authorize security personnel to monitor and investigate incidents
- Define and authorize the consequences of violations
- Define the organization consensus stance on security
- Help minimize risk as a result of threats or security incidents
- Help track compliance with regulations and standards

In one classification, security policies can be divided into two categories (NIST 2014):

- Technical policies implemented using hardware and software: We described different models used to model and describe such policies including: DAC, RBAC, and ABAC.
- Administrative policies performed by the people using the system and the people running it.

Security policies can also be divided into two categories:

- Security policies for users' behavioral management.
- Security policies for systems' and assets' management and control.

From security goals, security policies can be divided into security that protect each one of the major security goals (CIAAA: Confidentiality, Integrity, Availability, Access control, and Accountability).

US NIST categorizes information systems' security policies into three categories (Krutz and Vines 2004):

- Program policies that are used to create an organization's computer security program
- Issue-specific policies: to address specific organization issues or concerns
- System-specific policies: Managers' technical directives to protect information systems and assets

K0502: Knowledge of Organization Decision Support Tools and/or Methods

A Decision Support System (DSS) is a computer-based information system that supports business or organizational decision-making activities. When a business environment is dynamic and factors that impact decision-making frequently change, a DSS is an effective management tool to help in making the most suitable actions.

DSS supports human decision-making processes and/or act on their behalf in several decision-making-related actions. In most cases, such systems are not fully automated in which a problem is presented to the system and DSS will make decisions and enforce actions. Alternatively, DSS will make an advice, one action out of several possible alternatives and guide the problem-solving process, Fig. 10.5, (Stair and Reynolds 2016).

DSS can also present different possible actions or solutions and "costs" for each one of them. As data analytic activities, such decisions are also accompanied with accuracy or performance metrics to show the confidence levels in such decisions.

DSS in cyber security can serve different functions in addition to the main function (i.e., making decisions on how to respond to attacks, threats). For example, a DSS in cyber security can be used to help making decisions on how to best spend budgets on cyber security defense (Panaousis et al. 2014).

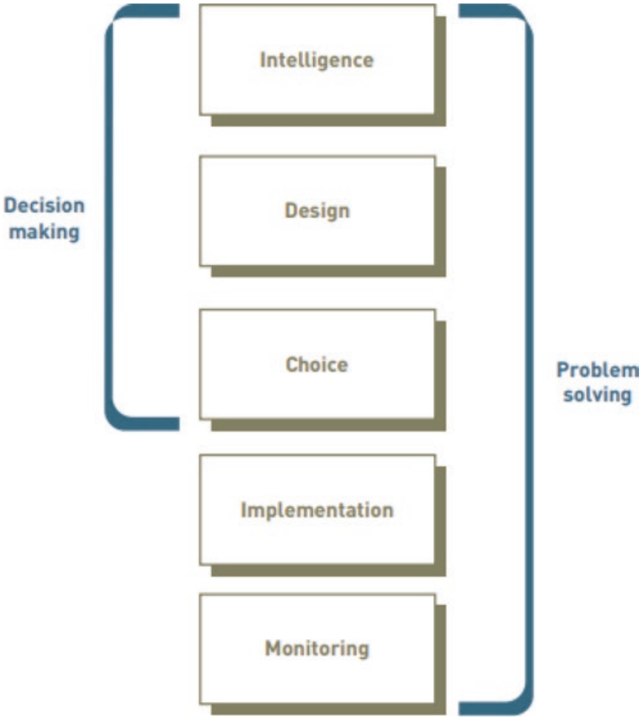


Fig. 10.5 Decision-making as a component of problem solving (Stair and Reynolds 2016)

Bibliography

aglearn.usda.gov (2018) Operations security. https://aglearn.usda.gov/customcontent/APHIS/APHIS-OPSEC/OPSsummary.htm

Dexter JH (2002) The Cyber Security Management System: a conceptual mapping. SANS Institute. www.SANS.org

Kayes I, Iamnitchi A (2015) A survey on privacy and security in online social networks. arXiv preprint arXiv 1504.03342

Krutz R, Vines R (2004) The CISSP prep guide, 2nd edn. Wiley, Chichester

NIST Security self-assessment guide for information technology systems. http://www.itl.nist.gov/lab/bulletns/bltnsep01.htm. Accessed 9 January 2014

Panaousis E, Fielder A, Malacaria P, Hankin C, Smeraldi F (2014) Cybersecurity games and investments: a decision support approach decision and game theory for security. Springer, New York, pp 266–286

Stair RM, Reynolds G (2016) Principles of information systems, 11 edn. ISBN-10:1133629660/ISBN-13:9781133629665

Statista (2018) The statistics portal, www.statista.com

Chapter 11
Forensics Analysis

K0017: Knowledge of Concepts and Practices of Processing Digital Forensics Data

In digital investigations, many software and hardware components include possible forensic artifacts that can be searched for. The process however is not trivial and such search should be focused in the context of the forensic case.

Digital forensic investigators should not only have knowledge on the subject case, but also on technical skills related to how to search for and acquire relevant information. Skills in disk and computer forensics continuously evolve with the evolution of computer hardware, software, operating systems, and environments.

Digital Forensic Process

The basic digital forensic process includes four major or generic activities, Fig. 11.1, (NIST 2006):

- Collection
- Examination
- Analysis
- Reporting

Searching for possible evidences related to an incident in a disk, a file, or operating system can be a very time-consuming and process. This can be as a result of three factors:

- The number of possible files and applications to search within is typically very large. This can take a significant amount of time and resources. Further, this volume of data is continuously growing where a typical current operating system can have thousands of files (Fig. 11.2) (Alsmadi et al. 2018).

I. Alsmadi, *The NICE Cyber Security Framework*,
https://doi.org/10.1007/978-3-030-02360-7_11

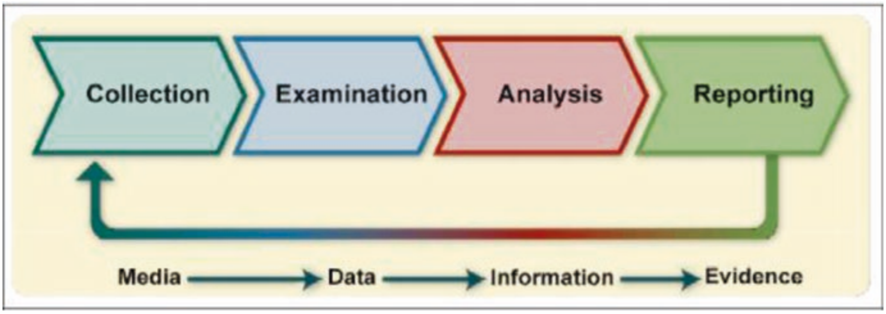
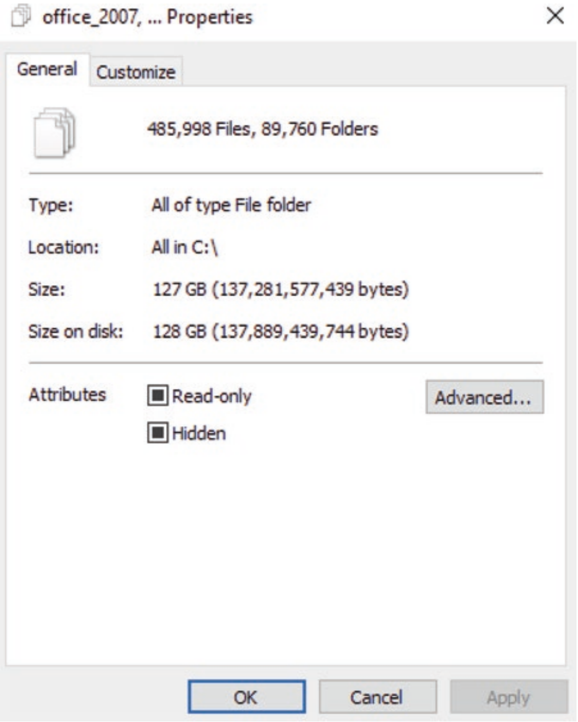


Fig. 11.1 Digital forensic process (Kent et al. 2006)

Fig. 11.2 An example of files/folders volumes in an operating system (Alsmadi et al. 2018)



485,998 Files, 89,760 Folders

Type: All of type File folder

Location: All in C:\

Size: 127 GB (137,281,577,439 bytes)

Size on disk: 128 GB (137,889,439,744 bytes)

Attributes ■ Read-only

■ Hidden

- So many variables in forensic cases: Forensic investigators are expected to study the subject case so that they can search for what is relevant to the case or within the case context. Making such connection may require looking at every single detail without ignoring any piece of information. In some cases, significant evidences may exist in places where many analysts will ignore.

- Disk and operating system investigation tools exist as: commercial, free, or open source. Those tools also continuously change to accommodate disk and operating system changes. Digital investigators may need to try a large number of tools in every case. They may see different and sometimes conflicting types of information.

Image Acquisition

Digital evidences exist in different types of disks (e.g., desktop or laptop disk drives, USB drives, mobile storage). The first step in forensic cases that include one or more of those disks is to acquire data from those disks and store them to a secondary, evidence-secure storage. In most cases, investigators must not conduct their analysis on live disks. The main reason is to preserve the evidence integrity and verify that none of the information that exists in the disk evidence exists as a result of the investigation process.

Copying files from evidence disk can take one of two major techniques:

- True image or Bit stream acquisition: Identical logical and physical imaging or copying which makes destination disk an exact copy/image of source one.
- Logical or sparse acquisition: Customized acquisition: It may include copying the whole data from original disk, but without guaranteeing the same location in the destination disk.

K0118: Knowledge of Processes for Seizing and Preserving Digital Evidence (e.g., Chain of Custody)

The basic digital forensic process described in Fig. 11.1 involves four main stages: collection, examination, analysis, and reporting. Any digital evidence that is collected as part of an investigation process should be properly handled from the moment the evidence is acquired or seized to the moment the evidence is presented in court. This whole chain from the start to the end is called chain of custody to include who handled the evidence throughout the process and how. The main reason behind such formal process is to ensure and be able to verify the integrity of the evidence and the process to collect and present that evidence. Any mishandling of such evidence may result in removing such evidence from the case. In other words, the integrity of the original disk or source of evidence media must be maintained throughout the entire investigation process. Only those individuals specifically trained for that purpose should be permitted to examine probable digital evidences.

Another goal for the formal evidence handling process is to ensure confidentiality and information protection. Special anti-static bags should be used to contain the digital evidence to prevent unintentional device damage from electromagnetic sources.

Probable Cause

In the USA, Fourth Amendment states that: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” So, is there is any difference between collecting digital evidences in comparison with physical or classical evidences? To apply the Fourth Amendment, investigators are required to get a warrant supported by probable cause.

The Fourth Amendment permits investigators or agents to seize a desktop, laptop, etc. temporarily if they have probable cause to believe that it contains evidence of a crime. The affidavit is a sworn statement of support of facts about the evidence, which can be enough to support a probable cause.

Documentation and Labeling

The forensic process should be very formal and structured, a curious or an enthusiastic investigator may risk losing evidence credibility. Documentation is also necessary where investigators should document all actions they took within the whole investigation process. Each acquired evidence should be labeled. Record each evidence information such as:

- The current date and time
- Evidence manufacture make and model, (e.g. Dell laptop Latitude...)
- Evidence unique features (e.g., serial numbers, IDs)
- Investigator name
- For digital evidences such as disks, hashing is used to create unique values to be tagged or labeled on the evidence. For verification, in court such values will be retrieved for match verification. This verifies that evidence was not tampered with since its seizure.

Seizure of Memory or Any Volatile Data

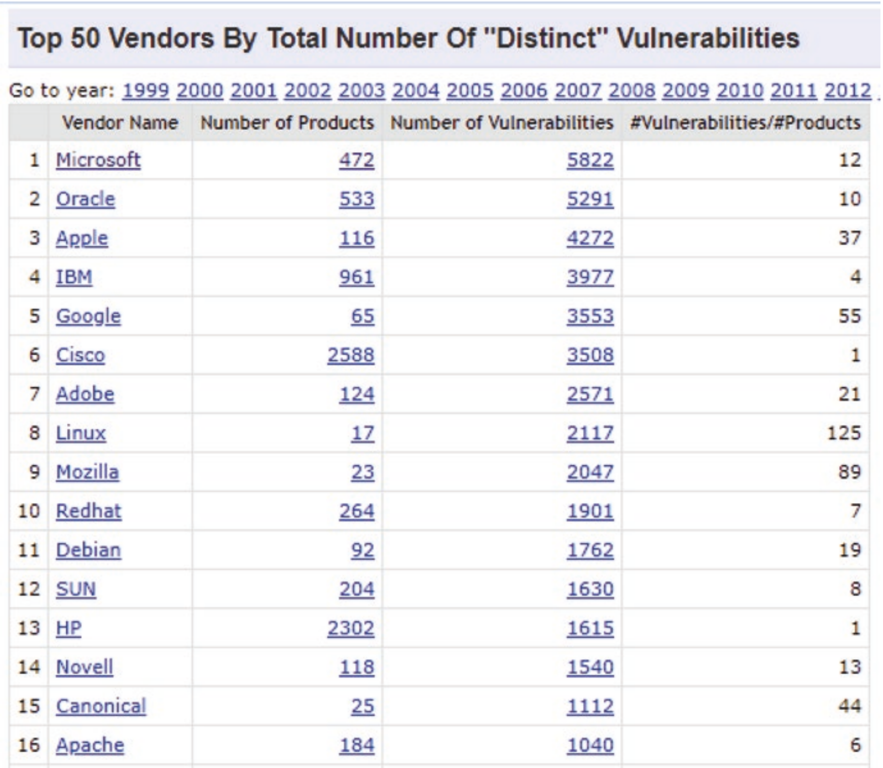
Data in disks is static; switching or restarting the computing machine will not result in losing such static data. However, data in memory (physical and virtual memories) is volatile and will be lost once the computing machine is switched off or restarted. In such cases, investigators should take the decision to capture such data while evidence system is still on or live (i.e., live acquisition). Certain forensic tools can be used to capture memory or volatile data (e.g., see the popular open source memory forensic tool; Volatility (https://www.volatilityfoundation.org/, https://github.com/volatilityfoundation/volatility)).

K0119: Knowledge of Hacking Methodologies in Windows or Unix/Linux Environment

Windows Hacking

In comparison with the different software vendors, Microsoft Windows operating system and other related products score the highest in terms of total number of vulnerabilities, Fig. 11.3. We should not ignore however, that Microsoft has a large market share in the software industry across the different software domains (e.g., operating systems, DBMS, programming IDEs, Internet browsers).

In this section, a selection of areas of interests for hacking and related hacking methods will be presented.



Top 50 Vendors By Total Number Of "Distinct" Vulnerabilities

Go to year: 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012

	Vendor Name	Number of Products	Number of Vulnerabilities	#Vulnerabilities/#Products
1	Microsoft	472	5822	12
2	Oracle	533	5291	10
3	Apple	116	4272	37
4	IBM	961	3977	4
5	Google	65	3553	55
6	Cisco	2588	3508	1
7	Adobe	124	2571	21
8	Linux	17	2117	125
9	Mozilla	23	2047	89
10	Redhat	264	1901	7
11	Debian	92	1762	19
12	SUN	204	1630	8
13	HP	2302	1615	1
14	Novell	118	1540	13
15	Canonical	25	1112	44
16	Apache	184	1040	6

Fig. 11.3 Top vendors by vulnerabilities (https://www.cvedetails.com)

Hacking Windows Registry and SAM

Windows registry is a hierarchical database or structure that contains information, settings, options, and other values for software programs and hardware installed on the different versions of Microsoft Windows operating systems (Fig. 11.4).

The Windows registry is targeted by hackers for different reasons:

- The Windows registry includes a wealth of information that can be used to learn about the target machine. Hackers can export the whole registry as a single file. Several tools exist that can help extract quick knowledge from the registry. Those who investigate Windows utilize Windows registry also to extract many forensic artifacts.
- Hackers can also inject keys in the registry which can manipulate victim machine to do certain actions. For example, some malwares keep hidden registry keys that allow them to reinstall themselves whenever they are removed.
- Windows SAM database includes information about users and their accounts that can be used to hack into the Windows system.

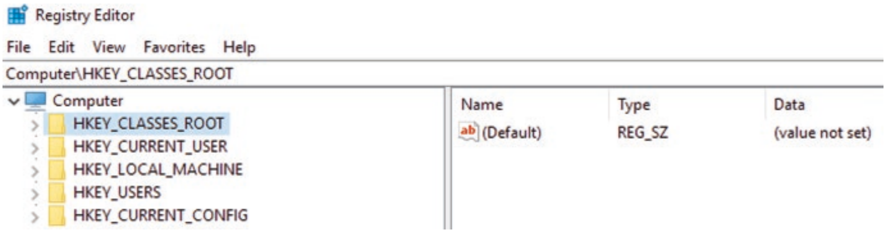
The Windows Security Accounts Manager (SAM) stores hashed versions of local Windows account passwords and also manages the password validation process during logins. Windows SAM database includes important accounts information and hence is targeted in hacking (Fig. 11.5).

Typically, SAM database exists in (Windows/system32/config/SAM). Of course, that file (SAM) will not allow you to open it or even copy it (when OS is live or online), using normal Windows tasks, and hence you have to look for alternative tools to do that.

Internet Explorer

Microsoft Internet explorer has been a target for many hacking schemes and malwares given its several discovered vulnerabilities, Fig. 11.6.

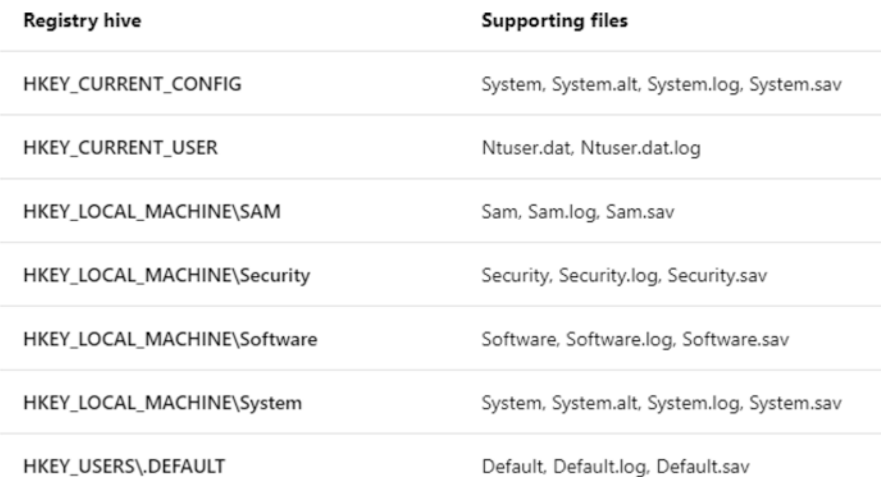
Figure 11.7 shows that Internet Explorer vulnerabilities have their peak in the years 2014–2015. Nonetheless, a significant number of vulnerabilities in the Internet browser still exists.



Computer\HKEY_CLASSES_ROOT

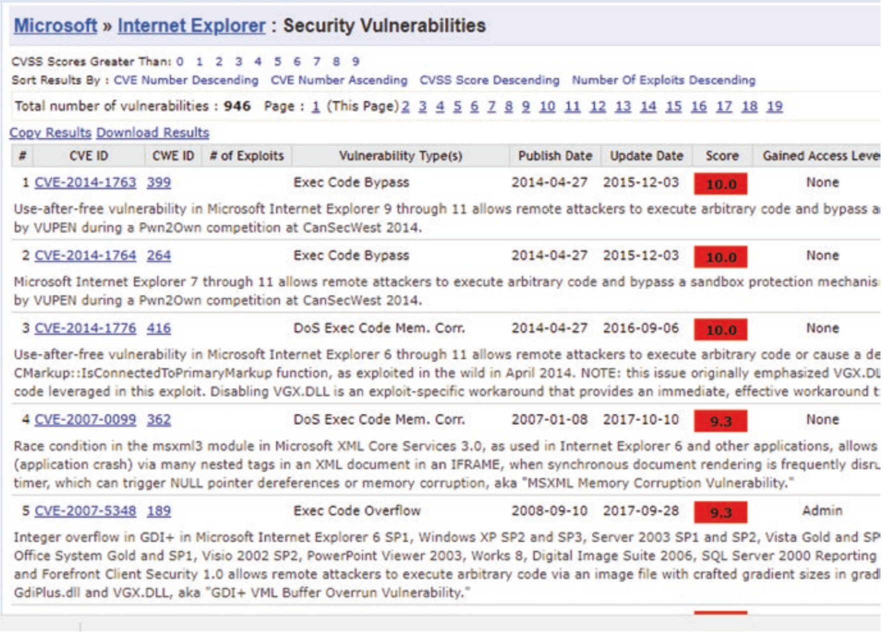
Name	Type	Data
(Default)	REG_SZ	(value not set)

Fig. 11.4 Windows registry



Registry hive	Supporting files
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav
HKEY_CURRENT_USER	Ntuser.dat, Ntuser.dat.log
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\System	System, System.alt, System.log, System.sav
HKEY_USERS\.DEFAULT	Default, Default.log, Default.sav

Fig. 11.5 Windows registry hives and their supporting files



Microsoft » Internet Explorer : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : **946** Page : 1 (This Page) 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Leve
1	CVE-2014-1763	399		Exec Code Bypass	2014-04-27	2015-12-03	10.0	None
Use-after-free vulnerability in Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code and bypass a by VUPEN during a Pwn2Own competition at CanSecWest 2014.								
2	CVE-2014-1764	264		Exec Code Bypass	2014-04-27	2015-12-03	10.0	None
Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code and bypass a sandbox protection mechanis by VUPEN during a Pwn2Own competition at CanSecWest 2014.								
3	CVE-2014-1776	416		DoS Exec Code Mem. Corr.	2014-04-27	2016-09-06	10.0	None
Use-after-free vulnerability in Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a de CMarkup::IsConnectedToPrimaryMarkup function, as exploited in the wild in April 2014. NOTE: this issue originally emphasized VGX.DL code leveraged in this exploit. Disabling VGX.DLL is an exploit-specific workaround that provides an immediate, effective workaround t								
4	CVE-2007-0099	362		DoS Exec Code Mem. Corr.	2007-01-08	2017-10-10	9.3	None
Race condition in the msxml3 module in Microsoft XML Core Services 3.0, as used in Internet Explorer 6 and other applications, allows (application crash) via many nested tags in an XML document in an IFRAME, when synchronous document rendering is frequently disru timer, which can trigger NULL pointer dereferences or memory corruption, aka "MSXML Memory Corruption Vulnerability."								
5	CVE-2007-5348	189		Exec Code Overflow	2008-09-10	2017-09-28	9.3	Admin
Integer overflow in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP Office System Gold and SP1, Visio 2002 SP2, PowerPoint Viewer 2003, Works 8, Digital Image Suite 2006, SQL Server 2000 Reporting and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via an image file with crafted gradient sizes in grad GdiPlus.dll and VGX.DLL, aka "GDI+ VML Buffer Overrun Vulnerability."								

Fig. 11.6 CVE list of Internet explorer vulnerabilities

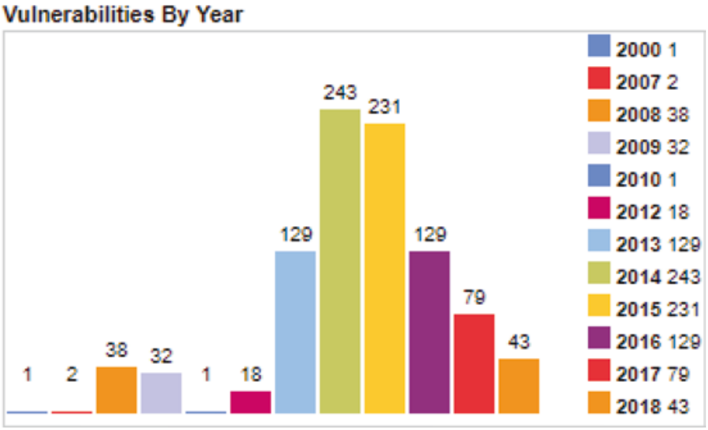


Fig. 11.7 IE vulnerabilities by year (https://www.cvedetails.com)

Such vulnerabilities are typically used by hackers as entry point to access the operating system for further hacking activities.

Windows Operating Systems

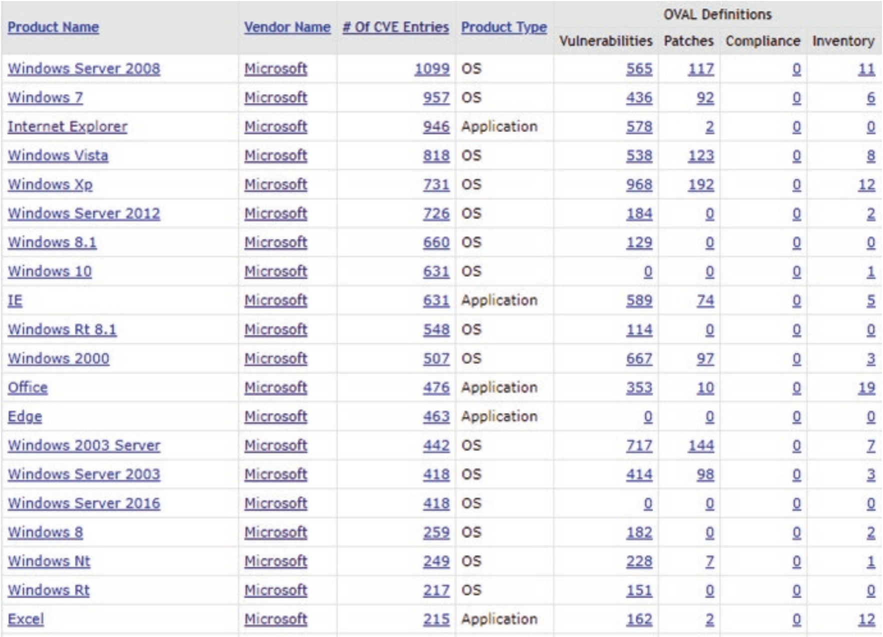
Windows have different operating systems starting from Windows for work group up to Windows 10. Starting Windows NT, Windows also branched server versions (e.g., 2008, 2012, 2016). Figure 11.8 shows top Microsoft vulnerable products. In terms of the different operating systems, Windows XP has the highest number of vulnerabilities. This is why its favorite hackers pick and also why many hacking training labs use it for simple exercises and demos.

Microsoft keep improving their security controls and mechanisms and Windows 10 has less reporting vulnerabilities or exploits.

.NET Framework

Another major Microsoft application that records a relatively large number of vulnerabilities is the .NET framework. The framework is required not only to program in C# or VB.NET but also to run most of software applications written in Windows environment. With .NET framework, ASP.NET reported also different types of vulnerabilities related to web attacks (e.g., XSS, Injections).

Other Microsoft applications reported significant volume of vulnerabilities that include Access and Chakracore (Microsoft Edge JavaScript engine).



Product Name	Vendor Name	# Of CVE Entries	Product Type	OVAL Definitions			
				Vulnerabilities	Patches	Compliance	Inventory
Windows Server 2008	Microsoft	1099	OS	565	117	0	11
Windows 7	Microsoft	957	OS	436	92	0	6
Internet Explorer	Microsoft	946	Application	578	2	0	0
Windows Vista	Microsoft	818	OS	538	123	0	8
Windows Xp	Microsoft	731	OS	968	192	0	12
Windows Server 2012	Microsoft	726	OS	184	0	0	2
Windows 8.1	Microsoft	660	OS	129	0	0	0
Windows 10	Microsoft	631	OS	0	0	0	1
IE	Microsoft	631	Application	589	74	0	5
Windows Rt 8.1	Microsoft	548	OS	114	0	0	0
Windows 2000	Microsoft	507	OS	667	97	0	3
Office	Microsoft	476	Application	353	10	0	19
Edge	Microsoft	463	Application	0	0	0	0
Windows 2003 Server	Microsoft	442	OS	717	144	0	7
Windows Server 2003	Microsoft	418	OS	414	98	0	3
Windows Server 2016	Microsoft	418	OS	0	0	0	0
Windows 8	Microsoft	259	OS	182	0	0	2
Windows Nt	Microsoft	249	OS	228	7	0	1
Windows Rt	Microsoft	217	OS	151	0	0	0
Excel	Microsoft	215	Application	162	2	0	12

Fig. 11.8 Microsoft vulnerabilities by products (https://www.cvedetails.com)

Pandemic and Grasshopper

WikiLeaks reported two tools developed by CIA to hack Windows systems Grasshopper (Kaser 2017) and Pandemic (Kumar 2017).

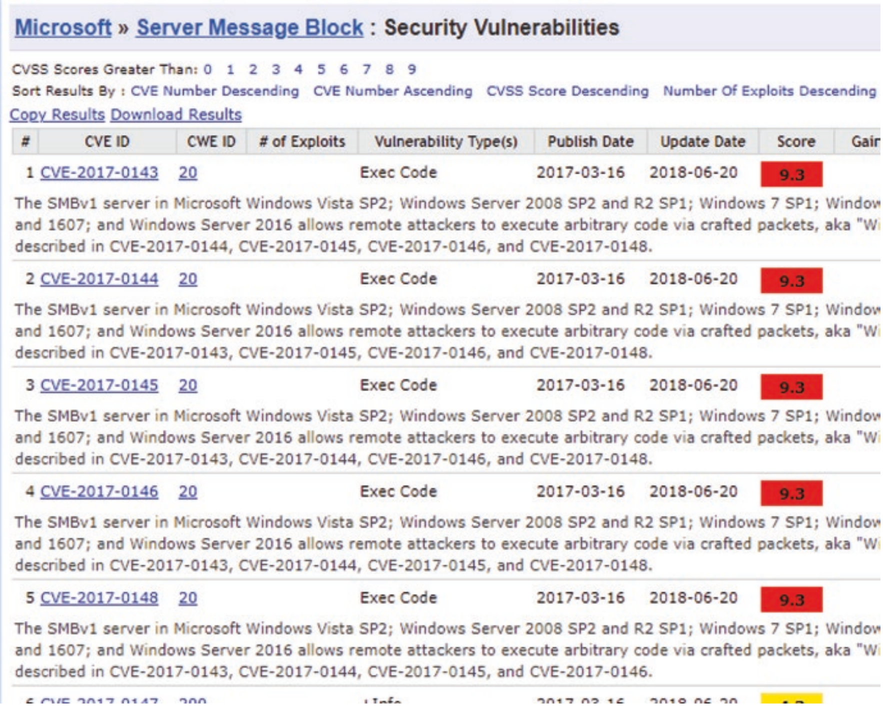
Pandemic (published by WikiLeaks under “Vault 7 series”) manipulate Windows file servers (Server Message Block, SMB) to allow sharing files with remote users on a local network. SMB reported several vulnerabilities over the years and is known to be used by hackers to access Windows machines (Fig. 11.9).

Grasshopper can make custom malware payloads and is developed to avoid anti-malware detection. The tool can install itself in Windows systems through manipulating Windows update feature.

Linux Hacking

Linux operating systems are popular and preferred environments for hackers and hacking tools for two main reasons.

- The first reason is that the OS is open source which enables hackers to know more details about the OS and how it works. Linux has many open source and commercialized distributions such as: Ubuntu, Debian, CentOS, Gentoo, Red Hat, and Fedora, Fig. 11.10 (w3techs.com 2018).



Microsoft » Server Message Block : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

<table>
<tr><th>#</th><th>CVE ID</th><th>CWE ID</th><th># of Exploits</th><th>Vulnerability Type(s)</th><th>Publish Date</th><th>Update Date</th><th>Score</th><th>Gair</th></tr>
<tr><td>1</td><td>CVE-2017-0143</td><td>20</td><td></td><td>Exec Code</td><td>2017-03-16</td><td>2018-06-20</td><td>9.3</td><td></td></tr>
<tr><td colspan="9">The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Window and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Wi described in CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.</td></tr>
<tr><td>2</td><td>CVE-2017-0144</td><td>20</td><td></td><td>Exec Code</td><td>2017-03-16</td><td>2018-06-20</td><td>9.3</td><td></td></tr>
<tr><td colspan="9">The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Window and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Wi described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.</td></tr>
<tr><td>3</td><td>CVE-2017-0145</td><td>20</td><td></td><td>Exec Code</td><td>2017-03-16</td><td>2018-06-20</td><td>9.3</td><td></td></tr>
<tr><td colspan="9">The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Window and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Wi described in CVE-2017-0143, CVE-2017-0144, CVE-2017-0146, and CVE-2017-0148.</td></tr>
<tr><td>4</td><td>CVE-2017-0146</td><td>20</td><td></td><td>Exec Code</td><td>2017-03-16</td><td>2018-06-20</td><td>9.3</td><td></td></tr>
<tr><td colspan="9">The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Window and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Wi described in CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, and CVE-2017-0148.</td></tr>
<tr><td>5</td><td>CVE-2017-0148</td><td>20</td><td></td><td>Exec Code</td><td>2017-03-16</td><td>2018-06-20</td><td>9.3</td><td></td></tr>
<tr><td colspan="9">The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Window and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Wi described in CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, and CVE-2017-0146.</td></tr>
<tr><td>6</td><td>CVE-2017-0147</td><td>200</td><td></td><td>+Info</td><td>2017-03-16</td><td>2018-06-20</td><td>[illegible]</td><td></td></tr>
</table>

Fig. 11.9 SMB vulnerabilities (https://www.cvedetails.com)

- Many Linux distributions and tools are openly available to try the different hacking staging and activities.

The following popular hacking environments or operating systems are developed under Linux OS distributions:

1. Kali: (https://www.kali.org/)
2. Parrot: (https://www.parrotsec.org/)
3. BackBox: (https://backbox.org/)
4. Samurai: (http://sourceforge.net/projects/samurai/)
5. Pentoo: (http://www.pentoo.ch/)
6. DEFT: (http://www.deftlinux.net/)
7. CAINE: (http://www.caine-live.net/)
8. BlackArch: (http://blackarch.org/)
9. Network Security Toolkit: (http://sourceforge.net/projects/nst/)
10. WifiSlax: (http://linux.softpedia.com/get/System/Operating-Systems/Linux-Distributions/Wifislax-21622.shtml)
11. Santoku: (https://santoku-linux.com/)
12. Bugtraq: (http://bugtraq-team.com)
13. Cyborg Hawk:(https://sourceforge.net/projects/cyborghawk1)

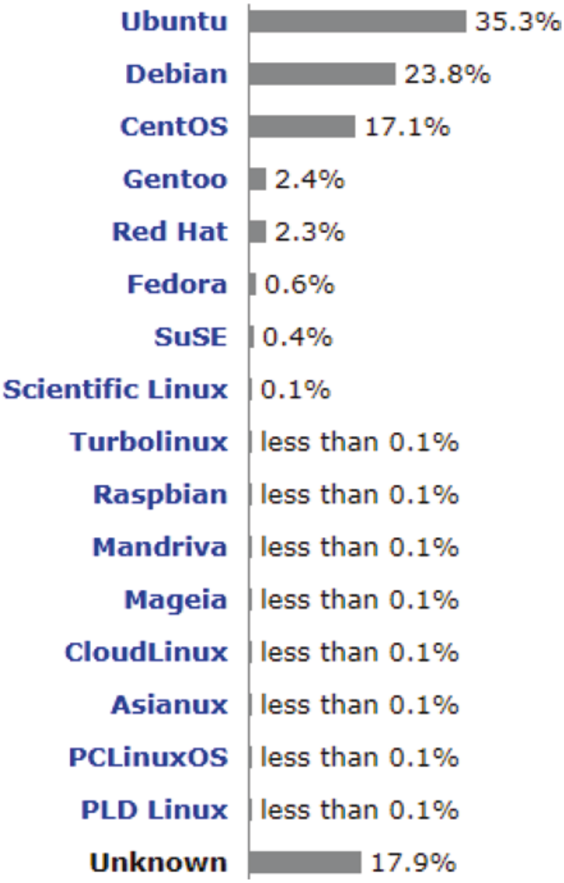


Fig. 11.10 Linux distributions on surveyed websites (w3techs.com 2018)

14. WeakNet: (www.weaknetlabs.com/)
15. NodeZero: (https://sourceforge.net/projects/nodezero/)
16. Fedora Security Spin (https://labs.fedoraproject.org/en/security/)
17. Knoppix STD: (https://s-t-d.org/)
18. Matriux: (www.matriux.com)

As an open source operating system with many distributions, it is expected to see steady volume of vulnerabilities over the years, Fig. 11.11, (https://www.cvedetails.com). The year 2017 reported the highest number of vulnerabilities so far.

Most of the vulnerabilities are reported on Linux Kernel. Major types of attacks on Linux are:

- Denial of Service
- Gain Information
- Memory Overflows
- Gain Privilege
- Code Execution

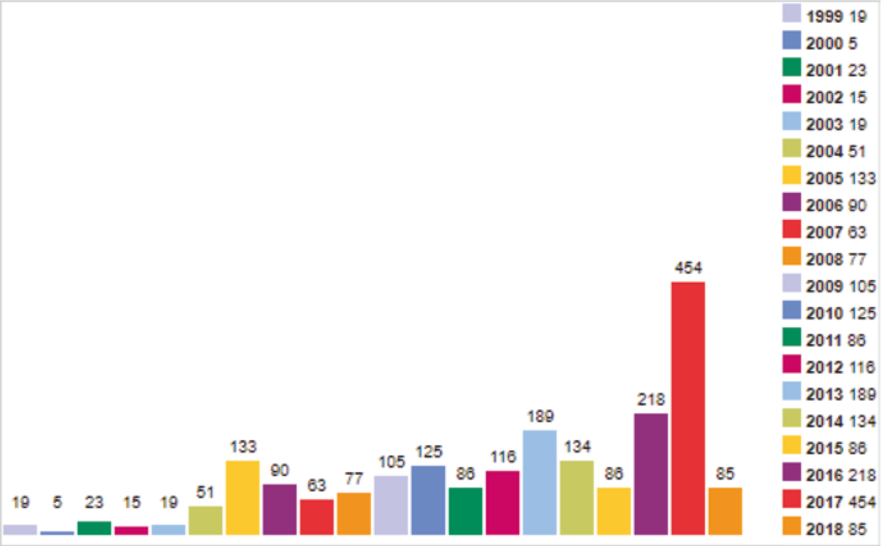


Fig. 11.11 Linux vulnerabilities over the years (https://www.cvedetails.com)

Users can also find open source Linux vulnerable distributions developed to try the different vulnerabilities and tools. Examples of those intentionally vulnerable or hackable images include:

- Damn Vulnerable: http://www.damnvulnerablelinux.org/
- Metasploitable: http://information.rapid7.com/metasploitable-download.html
- http://vulnhub.com/
- http://exploit-exercises.com/
- https://github.com/flyingcircusio/vulnix
- https://sourceforge.net/projects/holynix/
- http://www.pwnos.com/
- http://www.kioptrix.com/blog/dlvm

K0133: Knowledge of Types of Digital Forensics Data and How to Recognize Them

Forensic data or artifacts extracted from any digital evidence source depend on the source environment (e.g., desktop/laptop, smart phone, server), operating system, or file system. Tables 11.1 and 11.2 show examples of "areas of interests" for generic forensic artifacts that can be found in Windows and Linux systems.

We will cover different "areas of interests" that include forensic data and artifacts:

Table 11.1 An example of important forensic artifacts in Windows (Alsmadi et al. 2018)

Artifact	Typical Location
Registry and User-assist keys: This includes information about users, current users, sessions, installed applications, etc.	HKEY_LOCAL_MACHINE \SYSTEM: \system32\config\systemHKEY_LOCAL_MACHINE \SAM: \system32\config\samHKEY_LOCAL_MACHINE \SECURITY: \system32\config\securityHKEY_LOCAL_MACHINE \SOFTWARE: \system32\config\softwareHKEY_USERS \UserProfile: \winnt\profiles\usernameHKEY_USERS.DEFAULT: \system32\config\default HKEY_CURRENT_CONFIG
Event Logs	C:\Windows\System32\config
Internet Browser artifacts	Browser directory
Volume shadows	Settings-Computer and disk management
File systems	Settings-Computer and disk management
Link and recent files	AppData\Roaming\Microsoft\Windows\Recent
Cookies	Several different locations

Table 11.2 A sample of Linux forensic relevant system files (Alsmadi et al. 2018)

File	Details
/dev/had	First IDE hard drive on the system
/etc/aliases	Contains aliases used by sendmail and other mail transport agents.
/etc/bashrc	Contains global defaults used by the bash shell.
$HOME/.bash_history	Command history.
/etc/exports	Contains file systems available to other systems on the network via NFS.
/etc/fstab	The file system table contains the description of what disk devices are available at what mount points.
/etc/shadow	Hashed (e.g., MD5) versions of passwords.
/etc/group	Holds information regarding security group definitions.
/etc/grub.conf	Grub boot loader configuration file.
/etc/hosts	Contains host names/IP addresses used for name resolution in case a DNS server is unavailable.
/etc/mtab	Information about currently mounted devices and partitions.
/etc/sudoers	Usually, shows users with admin privileges.
/etc/passwd	Contains information about registered system users.
/etc/resolv.conf	Domain name servers (DNS) used by the local machine.
/proc/cpuinfo	Contains CPU-related information.
/proc/filesystems	Contains information about file systems that are currently in use.
/proc/ioports	A list of I/O addresses used by devices connected to the server.
/proc/meminfo	Contains memory usage information for both physical memory and swap.
/proc/modules	Lists currently loaded kernels.
/proc/mounts	Displays currently mounted file systems.
/proc/stat	Contains various statistics about the system.
/proc/swaps	Contains swap file utilization information.
/proc/version	Contains Linux version information.
/var/log/lastlog	Stores information about the last boot process.
/var/log/messages	Contains messages produced by the syslog during the boot process.
/var/log/wtmp	A binary data file holding login time and duration for current users.

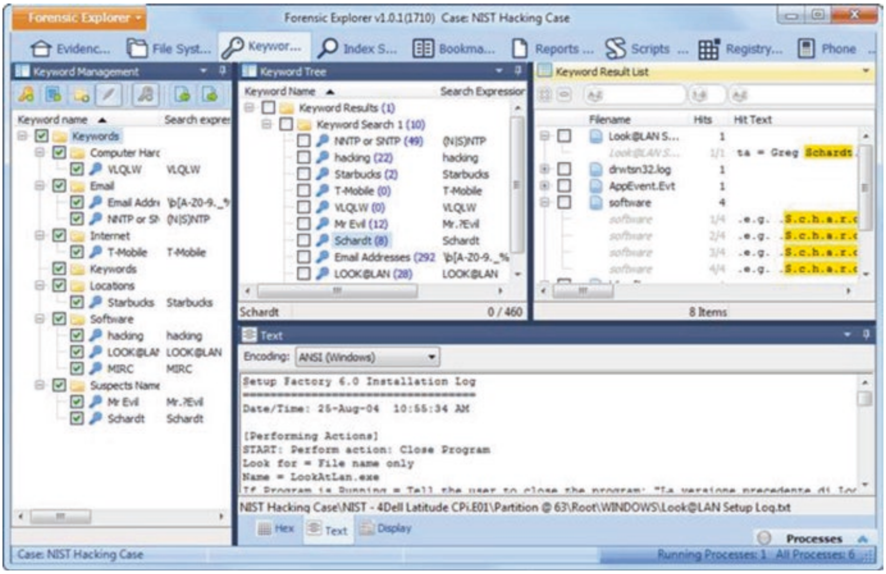
Disks Forensics

Data from disks are imaged in forensic processes so that they can be analyzed for possible evidences. The analysis activities vary based on the nature of the case and the disks or the images (e.g., operating system or file system type). Here are some generic activities that occur in most disk forensic cases:

- Hashing: In addition to creating and comparing hashes for disk files and folders, forensic tools can flag known files (e.g., system files) to be ignored from further search and analysis.
- Keyword search: In addition to generic search within the disk volumes, files, and folders, most disk forensic tools provide structured or predefined searches for keywords, Fig. 11.12.
- Timeline analysis: Forensic investigators try to focus their analysis in a window of time. Forensic tools can then help them aggregate all related files and activities within that border window. The following artifacts can be extracted: emails, IP addresses, web links, phone numbers, etc. Such information can be extracted from all files and folders in the disk.

Deleted Data

Deleted files should be checked by forensic analysts as suspects may try to delete certain files that they feel can be used as evidences against them. When files are deleted, their records in the file system are deleted. However, the actual file



```
Setup Factory 6.0 Installation Log
==================================
Date/Time: 25-Aug-04  10:55:34 AM

[Performing Actions]
START: Perform action: Close Program
Look for = File name only
Name = LookAtLan.exe
If Program is Running = Tell the user to close the program: "La versione precedente di Loo
```

NIST Hacking Case\NIST - 4Dell Latitude CPi.E01\Partition @ 63\Root\WINDOWS\Look@LAN Setup Log.txt

Fig. 11.12 An example of keyword search (Alsmadi et al. 2018)

information is not erased, in most operating systems, unless if a new content is added to the same ex-file location. Once files are deleted and their file system addresses are claimed by new files, they will not be recovered.

Hidden Data

A hidden data or area in a disk is that data/area that is not visible to the file system. Here are different examples of possible hidden areas in a disk:

- Unused disk sectors (e.g., unpartitioned areas)
- Slack spaces

Slack Spaces

There are different types of slack spaces that can be used to hide data including: file, RAM, drive, etc. A file slack is the empty data between the last bit of the file data and the end of the last cluster used by the file. Each file in the file system can have this "left over" and the total disk space can be the total slack spaces from all files. The RAM slack occurs in memory as data is written in memory in sectors (i.e., blocks of 512 bytes). As such, the last block in a retrieved file to the memory will be filled with random data to complete the last sector.

Slack spaces can be used, from a forensic perspective in two aspects:

- A professional hacker or a suspect can craft a malicious file, or application to be hidden in some or all the different partitions or disk slacks. While this may seem to be complicated, however, it is not impossible. On the other hand, such acts will be very hard for forensic investigators to detect.
- Slack spaces may keep data from earlier files. As a result, analysts may use tools to scan slack spaces looking for valuable information to steal. Users may assume that such data is deleted.

Memory Forensic Artifacts

Most commercial memory analysis tools prepare a list of predefined categories of information that can be relevant in general. Here is a list of such categories of information (Alsmadi et al. 2018):

- User credentials and account details: When users login to their accounts in emails, social networks, websites, etc., their credentials can be stored and extracted from the memory.

- Most recent opened software applications: In many computer crime cases, it is important to know the most recent software applications the victim or the suspect where recently using.
- Most recent opened or accessed data or files. This includes: created, modified, or accessed files.
- Content of email messages, posts, or comments in social networks, pictures, videos, etc. that were recently created, modified, or accessed.
- Most recent network connections, visited websites, etc.
- Many malwares reside in memory and may not write themselves in disks. Special information about those malwares can be extracted by forensic analysts when they are in memory.

Operating System Logs

Each operating system keeps records of different activities that within the operating system and installed applications. They can show details about system users, installation and used applications, and the different types of activities accomplished on those systems.

Regardless of the nature of the forensic case under-study, it is always important to investigate all system logs. It is also important to verify the integrity of those logs as some suspects or hackers can tamper those logs to intentionally mislead investigations.

For the integrity of the forensic case, it is important to retrieve all the users who had access to the subject system. In some cases, suspects can be themselves victims in which their systems were used to commit crimes without their explicit knowledge.

Logs exist also in DMBSs, websites or servers, switches, routers, and anti-malwares. Whenever logs in those different systems should be searched by forensic investigators.

If inspected machine or image has a running web server or site (e.g., Microsoft Internet Information Server IIS, or Apache (https://www.apache.org/)), web logs can be extracted from the machine. Such web logs may include many forensic artifacts related to the users or visitors of this website and their using activities.

Internet Forensic Data

With the heavy usage of Internet by users in all types of applications, the list of forensic data and artifacts extracted from Internet-related data will continue to grow. Literally, every application that uses the Internet will have possible forensic relevant data. Here, we will focus on major categories of applications.

The first important types of applications related to Internet usage that should be investigated are web browsers. Web browsers are software applications that enable users to access the different websites and applications. History of those browsers can help us see visited websites and pages and other user activities. The value and important of such information can vary from one forensic case to another.

The location on where such artifacts exist in the OS or the disk depends on the OS itself and also the Internet browser: (e.g., MS Internet explorer, Google Chrome, and Firefox).

Email Clients and Servers

Emails convey contents of high interests for forensic analysts. Despite the expanded usage of smart phones and online social networks, emails stay as one of the major human communication channels. In one major forensic example case, Enron case result in the exposure of millions of emails from Enron employees. Early published versions included many examples of private information in which users exchange very sensitive and private data through the emails.

K0134: Knowledge of Deployable Forensics

Cyber forensic exploitation teams should be able to work remotely or to deploy with forensic exploitation laboratories. Their services should be scalable, modular, and agile.

Deployable forensic laboratories try to provide mobile forensic capabilities in emergency or combat situations. Alternatively, they can work temporary as a replacement of forensic analysis capabilities after some natural disasters or other types of crisis.

NFSTC Deployable Forensics

US National Forensic Science Technology Center (NFSTC) is developing, in partnership with in partnership with the Department of Defense and the Defense Threat Reduction Agency (DTRA), deployable forensic labs to serve needs of different agents. The deployable lab can enable the collection of forensic evidence and data in real time, with capabilities to rival those of the typical stationary labs, (Tech 2009).

Deployable Configurations

For a forensic lab to be deployable, two main quality attributes should exist: modularity and mobility.

- Modularity
- A modular forensic lab enables easy configuration for adding/removing software, hardware, and network modules or components. This does not only support flexibility and extensibility to add any new components when needed, but it also helps the forensic lab to survive for several years. Forensic labs are typically expensive. Additionally, technology in this area moves fast. As such, it is important that such labs be able to support modularity to survive and operate for several years.
- Mobility
- Forensic analysts may need to work on some cases in their stationary labs. But they may also work on the field to collect and process evidences. It is unrealistic to expect that all forensic analysis activities can be moved to mobile options. This should be relative to the forensic stage or function. For example, most of activities in the forensic stage (collection), from Fig. 11.1 are expected to be mobile and enabled to function in the field. On the other hand, most of the activities in the forensic stage (analysis), from Fig. 11.1 are expected to be stationary and enabled to function in the field.

K0184: Knowledge of Anti-Forensics Tactics, Techniques, and Procedures

Anti-forensics term refers to techniques hackers, criminals, or users try to avoid or complicate their exposure or detection process.

Anti-Forensics' Goals

The followings summarize anti-forensics' goals (Liu and Brown 2006; Garfinkel 2007):

- Avoiding detection that some kind of event has taken place
- Disrupting the collection of information\evidence process
- Increasing forensic analyst effort and time on the case
- Casting doubt and integrity problems on the forensic report or findings (e.g., tampering with the evidence)
- Forcing the forensic tool to reveal its presence

- Subverting the functions of the forensic tools
- Countering back and attacking the forensic tools
- Hiding the existence of the anti-forensic tool

Anti-Forensics' Methods

Different references classify anti-forensics under different categories. Here is one of the popular classifications (Originated by Rogers 2006 and extended by Conlan et al. 2016):

- Data hiding: This method is further divided into the following sub-methods:
  - Steganography
  - Encryption
  - Data contraception
  - File system manipulation
  - Disk manipulation
  - Memory hiding
  - Network-based data hiding
- Artifact wiping:
  - Disk degaussing
  - Disk, file, log, etc. wiping
  - Metadata wiping
  - Registry wiping
- Trail obfuscation:
  - Backbone hopping
  - Data fabrication and obscurity
  - Data misdirection
  - Spoofing (e.g., IP and MAC addresses)
  - Log manipulation
  - Trojan commands
  - Zombie accounts
- AF techniques that exploit forensic process bugs, such as (Garfinkel 2007):
  - Failure to validate data
  - Denial of service attacks
  - Fragile heuristics
- Counter-forensics or attacks against the forensics' processes and tools
  - Detect forensic tools
  - Anti-reverse engineering
  - Forensic tools/process integrity attacks

- Forensic process integrity attacks (Fig. 11.13)

Countering forensics focus on targeting forensic tools and their integrity in one of the major forensic stages:

1. Identification: Anti-forensic tools (AF) will try to hide evidence or forensic artifact from detection (e.g., through encryption, steganography).
2. Preservation: AF tools target the evidence integrity (e.g., using log tampering).
3. Collection: AF tools try to obstruct the evidence collection process or their integrity.
4. Examination.
5. Analysis: For example, if a user disables hibernation, they can prevent memory snapshot or analysis.
6. Reporting.

K0185: Knowledge of Common Forensics Tool Configuration and Support Applications (e.g., VMware, WIRESHARK)

Virtual or sandboxing environments allow investigators to run analysis machines in isolated environment. This can serve several goals including:

- Ready-setups: Forensic setups can be very complex and require installations of several large products to work on the same machine. Having such setups ready in virtual images help carry such setups and install them in different locations.

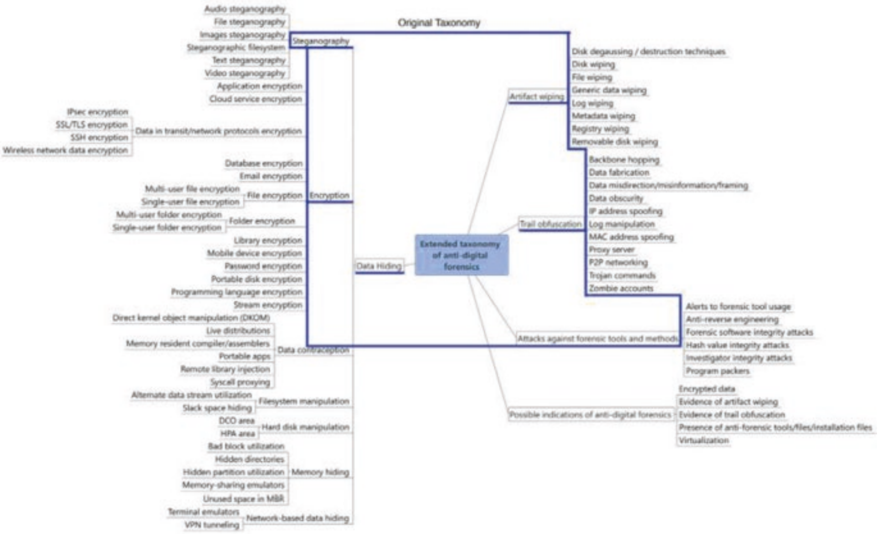


Fig. 11.13 Anti-forensics taxonomy (Conlan et al. 2016)

- Integrity issues: Investigators should isolate analysis environments from their own computing environments to eliminate their own possible tampering and hence risk evidence integrity.
- Security issues: Analyzing malwares is typically conducting in sandboxed isolated environments. This ensures that executing or deploying those malwares will not cause them to infect testing environment or propagate further.

Some of the popular virtual environments include:

- VMware products (e.g., vSphere: https://www.vmware.com/products/vsphere.html, ESXi: https://www.vmware.com/products/esxi-and-esx.html, and VMware Workstation: https://www.vmware.com/products/workstation-pro.html)
- Microsoft Hyper-V (https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows)
- Amazon Elastic Compute Cloud (EC2): aws.amazon.com/ec2
- Oracle VirtualBox (https://www.virtualbox.org/).
- CITRIX XenServer: https://xenserver.org

In addition to the virtual environments, several open source forensic distributions are available in which users can try free or open source available tools. Most of the listed Linux hacking distributions in (K0119) include sections for forensic tools. Some of the popular ones are: Kali, SIFT, (https://digital-forensics.sans.org/community/downloads), CAINE, DEFT, Martiux, and Santoku.

Network Forensics

In Network forensics traffic is analyzed, static or in real time searching for relevant information or evidences related to the subject case. The following link (https://www.forensicswiki.org/wiki/Tools:Network_Forensics) includes a list of several network forensic tools that users can use to analyze traffic or related artifacts:

- E-Detective: http://www.edecision4u.com/
- http://www.digi-forensics.com/home.html
- Burst: http://www.burstmedia.com/release/advertisers/geo_faq.htm
- CapAnalysis: http://www.capanalysis.net
- chkrootkit: http://www.chkrootkit.org
- cryptcat: http://farm9.org/Cryptcat/
- Enterasys Dragon: http://www.enterasys.com/products/advanced-security-apps/index.aspx
- ipfix/netflow v5/9: http://www.mantaro.com/products/MNIS/collector.htm
- Mantaro Network Intelligence Solutions (MNIS): http://www.mantaro.com/products/MNIS/index.htm
- MaxMind: http://www.maxmind.com
- netcat: http://netcat.sourceforge.net/

- netflow/flowtools: http://www.cisco.com/warp/public/732/Tech/nmp/netflow/index.shtml
- http://www.splintered.net/sw/flow-tools/, http://silktools.sourceforge.net/, http://www.vmware.com/vmtn/appliances/directory/293 Netflow Appliance (VMWare)
- NetDetector: http://www.niksun.com/product.php?id=4
- NetIntercept: http://www.sandstorm.net/products/netintercept
- NetVCR: http://www.niksun.com/product.php?id=3
- NIKSUN Full Function Appliance: http://www.niksun.com/product.php?id=11
- NetOmni: http://www.niksun.com/product.php?id=1
- NISUN Puma Portable: http://www.niksun.com/product.php?id=15
- ipfix/netflow v5/9: http://www.mantaro.com/products/MNIS/collector.htm
- NetSleuth: http://www.netgrab.co.uk/
- NetworkMiner: http://sourceforge.net/projects/networkminer/, http://www.netresec.com/?page=NetworkMiner
- pcap2wav: http://pcap2wav.xplico.org/
- rkhunter: http://rkhunter.sourceforge.net/
- ngrep: http://ngrep.sourceforge.net/
- nslookup: http://en.wikipedia.org/wiki/Nslookup
- Sguil: http://sguil.sourceforge.net/
- Snort: http://www.snort.org/
- ssldump: http://ssldump.sourceforge.net/
- tcpdump: http://www.tcpdump.org
- tcpxtract: http://tcpxtract.sourceforge.net/
- tcpflow: http://www.circlemud.org/~jelson/software/tcpflow/
- truewitness: http://www.nature-soft.com/forensic.html
- OmniPeek by WildPackets: http://www.wildpackets.com/solutions/network_forensics, http://www.wildpackets.com/products/network_analysis/omnipeek_network_analyzer/forensics_search
- Whois: http://www.arin.net/registration/agreements/bulkwhois.pdf Bulk WHOIS data request from ARIN
- Wireshark/Ethereal: http://www.wireshark.org/
- Kismet: http://www.kismetwireless.net/
- kisMAC: http://www.http://kismac-ng.org/
- Xplico: http://www.xplico.org/
- Expert Team - 3i System: http://www.expert-team.net
- fmadio 10G Packet Capture: http://fmad.io

K0268: Knowledge of Forensics Foot-Print Identification

The foot-prints are the small “left-over” traces or evidences behind the investigated user to help forensic analysts identify that person. Forensic examiners should have extensive understanding of the different computing environments and operating systems and how and where to look for possible evidences.

In the course of using computing machines and applications, users will leave artifacts or foot-prints scattered throughout the machine. Professional users can clean most of those traces but can also miss some of these buried forensic treasures.

From an attacker perspective foot-printing or fingerprinting activities focus on knowing the victim target in initial stages to focus attack activities. From a forensic perspective, it means the identification of the attacker, the malwares they deployed, the tools they have used, what exploits they targeted, and how they accomplished their attack.

Malware Foot-Printing

The process can start from a malware trace or foot-print that can be related to one of the following malware three related characteristics. Eventually, the goal is to know the details about those three main characteristics.

- Payload: The actual "piece of badness" that the malware aims to achieve. In other words, this is what will happen when the malware is executed. Malwares got their name from being software applications that have malicious intents. Few known malwares have benevolent intent.
- Propagation method: How the malware spreads from one file or machine to another.
- Intrusion or access methods: Each malware tries to find an entry point to its victim targets. This is typically through exploiting vulnerabilities in the target system.

K0433: Knowledge of Forensics Implications of Operating System Structure and Operations

Regardless of the operating or file system under investigation, there are some major generic activities that should be conducted in any operating system:

- **Review all system logs**
- **Perform keyword searches**
- **Review relevant files**
- **Identify unauthorized user accounts or groups**
- **Check for Backdoors or Rootkits**
- **Identify malicious processes**

When analyzing a disk of interest, it is important to quickly know the operating and file system types on the disk. Hexadecimal editors can be used to analyze the disk and certain OS/FS indicators can be quickly observed. Table 11.3 shows different indicators for different operating and file systems.

Once the operating system and file systems are known on the disk, investigators should focus on where to find forensic artifacts on the subject OS/FS. Additionally,

Table 11.3 Examples of indicators for different operating and file systems

OS/FS indicator	FS/OS
0x00	Empty partition-table entry
0x01	DOS FAT12
0x02	XENIX /root file system
0x03	XENIX /usr file system
0x04	DOS FAT16 (up to 32 MB)
0x05	DOS 3.3+ extended partition
0x06	DOS 3.31+ FAT16 (over 32 MB)
0x07	OS/2 HPFS, Windows NT NTFS, Advanced Unix
0x08	OS/2 v1.0-1.3, AIX bootable partition, Split Drive
0x09	AIX data partition
0x0A	OS/2 Boot Manager
0x0B	Windows 95+ FAT32
0x0C	Windows 95+ FAT32 (using LBA-mode INT 13 extensions)
0x0E	DOS FAT16 (over 32 MB, using INT 13 extensions)
0x400h	HFS+

from a forensic perspective, some OS/FS have certain features that are of special implication to the forensic investigation process. We will use Alternate Data Stream (ADS) in NTFS as one example.

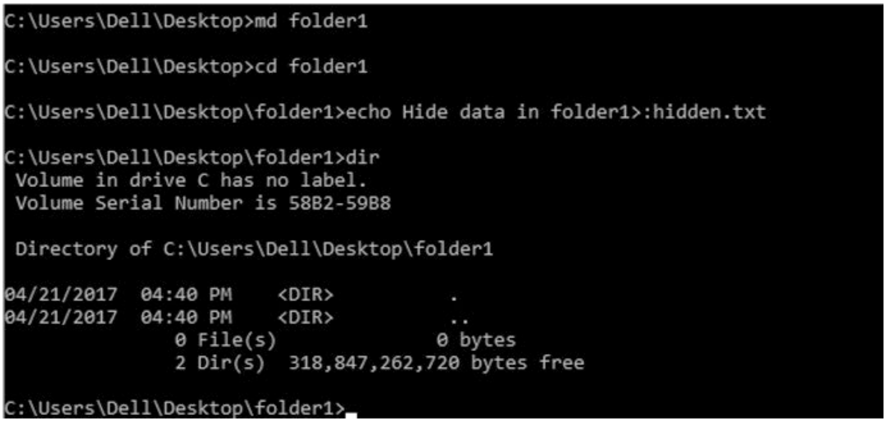
Alternate Data Stream: ADS

ADS feature in NTFS has a significant impact in forensics. Users can hide files and data in files using ADS. If an MFT file record has more than one $DATA attribute, those additional $DATA attributes are called ADS. ADS can be used to hide data as it does not show up in directory listing and the file size of original file. ADS data hiding is relatively easy to accomplish and the size of the data that can be hidden in ADS is unlimited.

Example: Fig. 11.14 below shows simple steps to hide a file (hidden.txt) in a folder.

Forensic Investigations in MAC Operating Systems

Apple MAC operating system is evolved from UNIX. Apple MAC artifacts and locations can be different based on the OS platform (i.e., desktops, laptops, tablets, or smart phones). Newer MAC operating systems are distinguished by the letter (X) from older versions. The mobile OS is distinguished by the letter (i; iOS).



```
C:\Users\Dell\Desktop>md folder1

C:\Users\Dell\Desktop>cd folder1

C:\Users\Dell\Desktop\folder1>echo Hide data in folder1>:hidden.txt

C:\Users\Dell\Desktop\folder1>dir
 Volume in drive C has no label.
 Volume Serial Number is 58B2-59B8

 Directory of C:\Users\Dell\Desktop\folder1

04/21/2017  04:40 PM    <DIR>          .
04/21/2017  04:40 PM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)  318,847,262,720 bytes free

C:\Users\Dell\Desktop\folder1>
```

Fig. 11.14 An example of hiding data using ADS

Apple continuously evolves their operating systems especially in terms of security architecture and updates. The followings are examples of forensic artifacts on MAC mobile devices.

- **System version:** /System/Library/CoreServices/SystemVersion.plist
- **User preferences:** %%users.homedir%%/Library/Preferences/*
- **Call History**: %%users.homedir%%//Library/CallHistory
- **Text messages**: %%users.homedir%%//Library/SMS
- **Address Book**: The location of this file is %%users.homedir%%//Library/AddressBook.
- **Recent Items**: Recent items in MAC can be typically found in preferences directory: – %%users.homedir%%/Library/Preferences/com.apple.recentitems.plist
- **Device backup locations**: Typically, the default location is: %%users.homedir%%/Library/ApplicationSupport/MobileSync/Backup/*
- **System Logs**: There are four main locations for logs: System log files (/var/log/*), Apple system logs (/var/log/asl/*), installation logs (/var/log/install.log), and audit logs (/var/audit/*).
- **Memory SWAP files:** Those are location of virtual memory used to support main physical memory: Those SWAP files can exist in: (/var/vm/sleepimage), (/var/vm/swapfile#).
- **Browser cookies/histories:** Google chrome: %%users.homedir%%/Library/ApplicationSupport/Google\Chrome\Default/*
- **Safari:** %%users.homedir%%/Library/Safari/History.plist/ and LastSession.plist
- **Cookies:** Cookies can be found in: %%users.homedir%%/Library/Cookies/Cookies.plist
- **Cache**: Cache can be found in: %%users.homedir%%/Library/Caches/com.apple.Safari/Cache.db

Visited site at: %%users.homedir%%/Library*/Safari/TopSites.plist*

K0449: Knowledge of How to Extract, Analyze, and Use Metadata

Metadata, often described as "data about data," is used to provide information about a specific, user, activity, program, file, or document. Forensic analysts use metadata to understand their case, correlate the different activities, reconstruct crime scene, or search for possible evidences.

Metadata can also be target for anti-forensic tools as we described earlier where suspects may try to destroy or manipulate such metadata and jeopardize case integrity.

Common Sources of Metadata

- Operating systems
- Web servers
- DBMS
- Switches, routers, firewalls
- Software applications
- Documents, videos, pictures
- File systems
- Emails, email clients and servers
- User-added metadata
- Vendor-added metadata

Examples of Metadata

- User, application, file, etc. name
- File extension (e.g., a document, video, picture)
- File size
- Hash value
- Date created
- Date last accessed
- Date last modified
- User/account who created/accessed or modified the file

File extensions help analysts know the right software to use to open or analyze subject file. Users can hide or change file extensions to complicate the analysis process. Digital evidences are stored in different types of disks (e.g., desktop or laptop disk drives, USB drives, mobile drives). The first step in forensic cases is to be able to acquire data from those disks and store them on a secondary storage. Investigators must not conduct their analysis on live disks. The main reason is to preserve the evidence integrity and verify that none of the information that exists in the disk evidence is added by the forensic investigators themselves.

Disk Acquisition Formats and Metadata

- Raw formats: Raw image file formats have the advantage of being open source, simple, and can be analyzed and used by many tools. However, little metadata can be extracted about the image using the raw formats.
- Commercial or proprietary formats and independent formats. Commercial disk analysis tools have their own proprietary formats. For example, EnCase (E01, E02, etc.), ILook (compressed (IDIF), non-compressed (IRBF), and encrypted (IEIF)), etc. Unlike raw image formats, proprietary formats extract metadata information, but can only be used within their specific tools.
- As a compromise between the two previous options, independent file formats (such as AFF, AFD, and AFM) can be used across different tools while they can also collect disk and imaging process metadata.

Investigators should be aware of those different data acquisition formats and tools. They need to take the proper choice of which acquisition format and tool to use for the current case they are investigating.

Examples of commercial forensic metadata analysis tools:

- FTK: Forensic toolkit
- Encase
- Metadata assistant
- Maltego
- Helix
- Paraben
- exiftool
- BlackLight
- MacQuisition

K0573: Knowledge of the Fundamentals of Digital Forensics in Order to Extract Actionable Intelligence.

Actionable Forensic Intelligence

The term actional intelligence is used to refer to using knowledge extracted from security intelligence into actions to guide and control security applications (e.g., firewalls, anti-malware systems, switches, routers, access controls). Here are some goals to be served producing actionable intelligence:

- Make informed decisions: In data science in general, it is important to focus analysis activities toward a specific goal. Users or decision-makers may not understand or need to know most of the information extracted from the forensic analysis. Rather, they only need to know what such extracted information means to them and their assets and systems.

- Guide security policies and roles: Security policies guide organization security controls. Policies and their concrete actions or roles should be extracted or designed based on several dimensions including:
  - The protected assets, their nature, their data, users, etc.
  - Security goals and their sensitivity (e.g., privacy, confidentiality, and availability issues).
  - The environment in which the organization or the systems exist, the types of threats or attacks they can be possibly exposed to, etc.
- Help decision-makers address and mitigate risk: Knowledge about threats in the organization environment can better help decision-makers plan for risk management, mitigation, etc.
- Help in protecting assets: Protecting organization assets is the ultimate goal of most security procedures and controls. Actionable forensic intelligence help security team better know how to best protect their assets given the environments they operate on and the resources they have.
- Help in security compliance.

One challenge when making actionable intelligence, especially if such actions are enforced programmatically is the accuracy of such intelligence. In an automated model, security agents are deployed to learn and make actionable intelligence.

Those agents should be:

- Active: They themselves or entities receiving data from other monitoring systems, continuously screen the subject network collecting, interesting, and relevant data.
- Intelligence: They are equipped with AI algorithms to extract knowledge relevant to the defense context.
- Autonomous: They can orchestrate this whole process and integrate activities from different systems (e.g., monitoring agents, AI intelligence agents, security controls) without or with the least human intervention.

Although this may seem straightforward, there are several challenges hindering this process such as:

- Environment complexity: First, typically the world that those agents work on is complex and the factors that can impact the process are very large. Additionally, those environments continuously evolve and intelligence agents should be able to accommodate such continuous evolution.
- Timeliness: The value of security intelligence information degrades significantly with time. But how can we conduct four large activities in a relatively small amount of time? (1) aggregate a large amount of data, (2) coming from different, sometimes heterogeneous sources, (3) to be processed and intelligently analyzed to extract relevant knowledge, and (4) finally pass it to systems or users who can take proper defense actions.
- Accuracy and performance issues: With many variables in the security intelligence process, false-positive and false-negative errors of detection are possible.

The ability to achieve high accuracy usually requires more time, which contradicts with another important factor, timeliness, or performance. Additionally, they (i.e., accuracy and timeliness) both contradict with overall system efficiency where security intelligence activities may hinder normal business functions or activities.

- Privacy and legal challenges: Activities related to data collection and intelligence face different types of barriers; privacy, and legal constraints as well as copyright, or data ownership.

Those are few examples of challenges toward the development, implementation, and deployment of cyber defense intelligence, self-adaptive, and autonomous agents.

Autonomous or self-adaptive systems are capable of handling run-time challenges with requirements in their known and unknown territories. They include activities that complete the cycle: (1) collect, (2) analyze, (3) decide, (4) act, (5) collect, and so on (Fig. 11.15). Building such systems poses several challenges. For example, such systems should be designed without knowing all requirements changes for security system and its environment and potential attacks that could take place.

Forensic knowledge can be extracted over a relatively long period of time, in collaboration from different teams, nationally and internationally. Many attempts

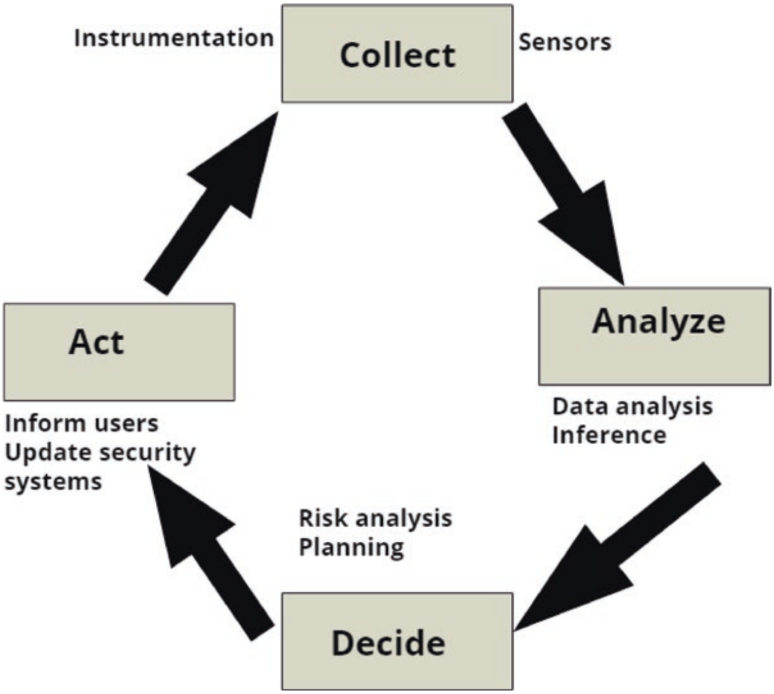


Fig. 11.15 Loop activities in autonomous, self-adaptive systems (Cheng et al. 2009)

exist to build public knowledge repositories to spread cyber intelligence. Examples of such websites include:

- MISP: http://www.misp-project.org/
- AlienVault: https://otx.alienvault.com/
- VirusTotal: https://www.virustotal.com/
- Pulsedive: https://pulsedive.com/
- Combine: https://github.com/mlsecproject/combine
- FireEye: https://github.com/fireeye/iocs

S0047: Skill in Preserving Evidence Integrity According to Standard Operating Procedures or National Standards

Digital evidence is defined as a set of reliable objects that uphold or refute a hypothesis, (Hargreaves 2009). When cataloging a digital evidence, one of the prime goals of the process is to preserve the evidence integrity. The intent is to ensure that no tampering with the process occur through the investigation process whether intentionally or unintentionally.

In order to preserve the evidence integrity, the integrity of both the people who conduct the investigation process as well as the process itself should be preserved. For example, we described in another KSA, the importance of structuring the evidence chain of custody to preserve evidence integrity. Another important procedure for analysts to follow is to never conduct their analysis on the original evidence, but on an identical image of that evidence.

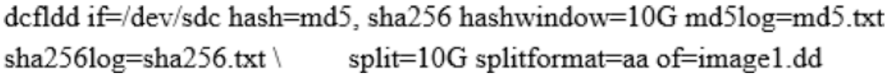
We will describe different mechanisms to do that:

Follow Current Standards, Guidelines, and Laws

Forensic investigators should stay current on relevant legislations. The goal of any forensic investigation process is not only the evidence discovery but also the ability to present that evidence in court. To do this, investigators should ensure that all aspects of the investigation are legal and that the integrity of the data presented cannot be questioned.

Hashing

Hashing is one of the most popular techniques used to preserve integrity. Most of the image acquisition tools include steps to hash the images through the initial acquisition. The same hashing value will be compared with the image in course to verify that integrity was preserved. Figure 11.16 shows a simple command for



```
dcfldd if=/dev/sdc hash=md5, sha256 hashwindow=10G md5log=md5.txt
sha256log=sha256.txt \       split=10G splitformat=aa of=image1.dd
```

Fig. 11.16 An example of generating a hashing value using dcfldd tool

image acquisition using dcfldd tool. The command uses MD5 hashing algorithm to generate the image hash value.

Some research references conducted experiments on different hashing algorithms and their resistance to collision. Many sorted the following in ascending order: MD5, SHA1, SHA224, SHA256, SHA384, and SHA512.

There are different types of attacks on hashing algorithms. Examples of those attacks include: Guessing attack, Birthday attack, precomputation of hash values, long-message attack for second preimage, etc. Select one type of those attacks and research on how to implement and evaluate such attack.

US NIST conducted a hash competition to evaluate hashing algorithms over the years from 2004 to 2007 (http://csrc.nist.gov/groups/ST/hash/sha-3/pre-sha-3-comp.html).

There are some tools that claim that they can crack hashing algorithms (e.g., https://crackstation.net/, https://hashkiller.co.uk/md5-decrypter.aspx, http://www.md5online.org/). Use the website (http://www.fileformat.info/tool/hash.htm) to hash some texts. Then use hash crackers to evaluate the percentage of your text that can be successfully cracked**.**

Write Blockers

Write blockers are hardware devices or software applications that enable the disk acquisition process without creating the possibility of accidentally corrupting or tampering with the disk and risking its integrity.

There are two types of write blockers:

- A native device uses the same interface on for both in and out, for example, an IDE to IDE write block. New solid-state drives post some challenges to the blockers process. There is a significant difference between SSDs and HDDs. Bus-level write blockers which work with HDDs are not effective when used to write block SSDs. The write blocker will obviously block writes from the host PC, while the data may still change.
- A Tailgate device uses different interfaces for data inputs and outputs, for example, a USB to SATA write block.

Some examples of software blockers include:

- https://github.com/msuhanov/Linux-write-blocker
- https://www.forensicsoft.com/safeblock.php
- http://macforensicslab.com/product/write-controller/

Based on NIST’s Software Write Block specifications, a software write block tool must operate by monitoring and filtering drive I/O commands sent from an application or OS through a given access interface.

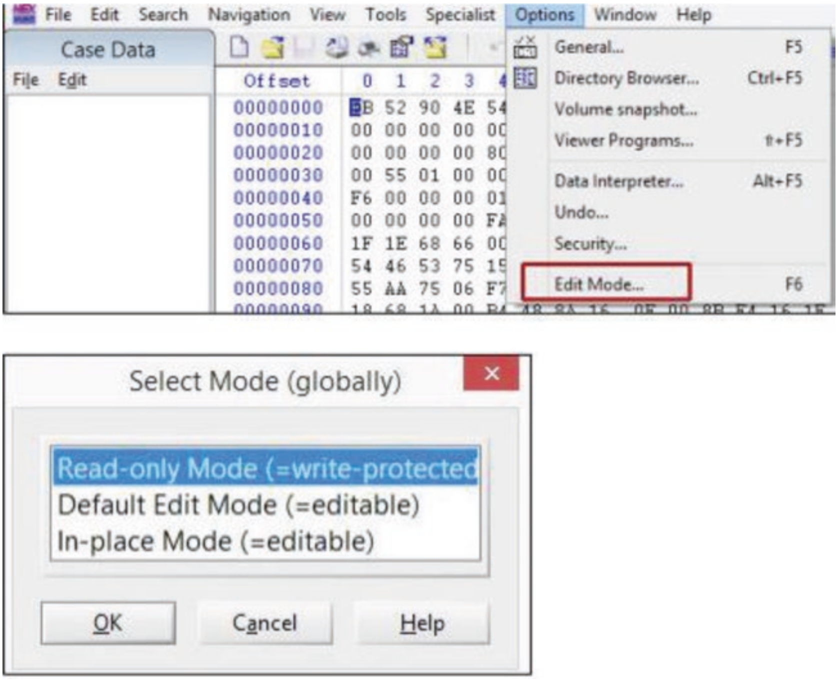
Even when using different types of forensic software tools, users should always look for read-only modes when conducting forensic analysis activities (Fig. 11.17).

Anti-Static Bags

Investigators should ensure proper handling and storage procedures of digital evidences or seized items. Anti-static bags prevent the evidence devices getting damaged due to electromagnetic interference and the data stored in them getting corrupted.

Memory Dumps

Memory information will be lost if the machine is started. As such investigators are expected to conduct the analysis activities while the subject machine is running or dump the memory using proper tools before shutting down or restarting the subject



```
Offset     0  1  2  3  4
00000000  EB 52 90 4E 54
00000010  00 00 00 00 0C
00000020  00 00 00 00 80
00000030  00 55 01 00 0C
00000040  F6 00 00 00 01
00000050  00 00 00 00 FA
00000060  1F 1E 68 66 0C
00000070  54 46 53 75 15
00000080  55 AA 75 06 F7
```

Read-only Mode (=write-protected
Default Edit Mode (=editable)
In-place Mode (=editable)

Fig. 11.17 An example of using read-only mode in Hex-editors

machine. The process to power off or not the subject machine should also be structured according to the standards. Every situation requires careful considerations of the nature of the case and the computing devices in question. What may be a workable set of actions for maintaining the integrity of one machine may lead to loss of evidence on another.

S0065: Skill in Identifying and Extracting Data of Forensic Interest in Diverse Media (i.e., Media Forensics)

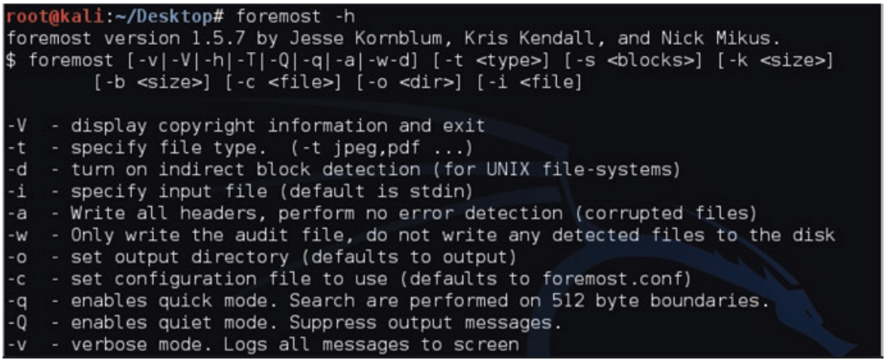
Disk Forensic Tools

Several forensic activities can be taken when dealing with data in a drive that is inaccessible to the file system. For example, "File carving" is a process in which files are reconstructed from raw data.

Many forensic tools such as: FTK forensic toolkit from access-data (accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk), EnCase (https://www.guidancesoftware.com/encase-forensic), Foremost (foremost.sourceforge.net), etc. can retrieve raw data based on file carving process. The process accomplishes this file retrieval based on the actual content rather than metadata extracted from file system.

Foremost is an open source file carving tool developed by US Air force agents in 1999, Fig. 11.18. It is also included within Kali forensic tools: http://tools.kali.org/forensics/foremost. It was also used for the first time to demo file carving in the 2006 forensic challenge: http://www.dfrws.org/2006.

Foremost can also be used to analyze network packets pcap files and extract files directly from this analysis.



```
root@kali:~/Desktop# foremost -h
foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus.
$ foremost [-v|-V|-h|-T|-Q|-q|-a|-w-d] [-t <type>] [-s <blocks>] [-k <size>]
        [-b <size>] [-c <file>] [-o <dir>] [-i <file]

-V  - display copyright information and exit
-t  - specify file type.  (-t jpeg,pdf ...)
-d  - turn on indirect block detection (for UNIX file-systems)
-i  - specify input file (default is stdin)
-a  - Write all headers, perform no error detection (corrupted files)
-w  - Only write the audit file, do not write any detected files to the disk
-o  - set output directory (defaults to output)
-c  - set configuration file to use (defaults to foremost.conf)
-q  - enables quick mode. Search are performed on 512 byte boundaries.
-Q  - enables quiet mode. Suppress output messages.
-v  - verbose mode. Logs all messages to screen
```

Fig. 11.18 Foremost forensic tool

Binwalk (http://tools.kali.org/forensics/binwalk, http://binwalk.org/) is another simple open source disk forensic tool. The disk can also extract information from raw images (e.g., bin routers, switches, and system firmwares) (Fig. 11.19).

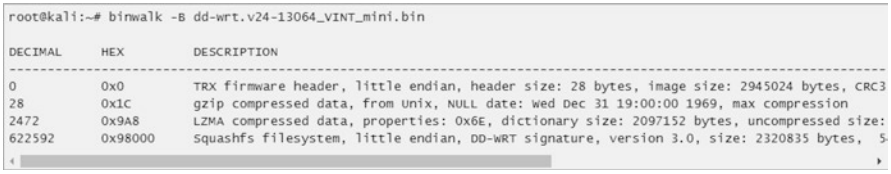
Disk Forensics

- Conduct a small experiment to show the difference between the two tools for image acquisition: dd and dcfldd.

Foremost and File Carving

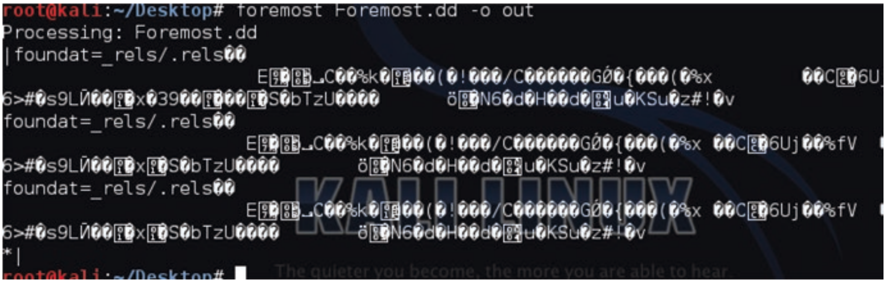
In this lab, you are expected to search for an image available through the Internet that includes "file carving" issues. Follow the steps similar to the images below to extract raw data files from the image.

- The command below, Fig. 11.20 will extract the image to an (out) folder
- We can check content of extracted folder. Foremost has predefined folders based on either files extension (jpg, gif, png, bmp, avi, exe, mpg, wav, riff, wmv, mov, pdf, ole, doc, zip, rar, htm, and cpp) or forensic-related information (zip codes, IP addresses, etc.), Fig. 11.21.
- The audit file, Fig. 11.22 shows extracted or recovered files from the image.
- Find a public pcap file and show how Foremost tool can be used to extract information from this file.



```
root@kali:~# binwalk -B dd-wrt.v24-13064_VINT_mini.bin

DECIMAL       HEX           DESCRIPTION
--------------------------------------------------------------------------------------------------------------
0             0x0           TRX firmware header, little endian, header size: 28 bytes, image size: 2945024 bytes, CRC3
28            0x1C          gzip compressed data, from Unix, NULL date: Wed Dec 31 19:00:00 1969, max compression
2472          0x9A8         LZMA compressed data, properties: 0x6E, dictionary size: 2097152 bytes, uncompressed size:
622592        0x98000       Squashfs filesystem, little endian, DD-WRT signature, version 3.0, size: 2320835 bytes,  5
```

Fig. 11.19 Binwalk disk forensic tool



```
root@kali:~/Desktop# foremost Foremost.dd -o out
Processing: Foremost.dd
|foundat=_rels/.rels��
                                   E□�□_C��%k�□��(�!���/C������GØ�{���(�%x         ��C□�6U
6>#�s9LЍ��□�x�39��□���□�S�bTzU����       ö□�N6�d�H��d�□u�KSu�z#!�v
foundat=_rels/.rels��
                                  E□�□_C��%k�□��(�!���/C������GØ�{���(�%x ��C□�6Uj��%fV
6>#�s9LЍ��□�x□�S�bTzU����        ö□�N6�d�H��d�□u�KSu�z#!�v
foundat=_rels/.rels��
                                  E□�□_C��%k�□��(�!���/C������GØ�{���(�%x ��C□�6Uj��%fV
6>#�s9LЍ��□�x□�S�bTzU����        ö□�N6�d�H��d�□u�KSu�z#!�v
*|
root@kali:~/Desktop#
```

Fig. 11.20 Foremost image extraction

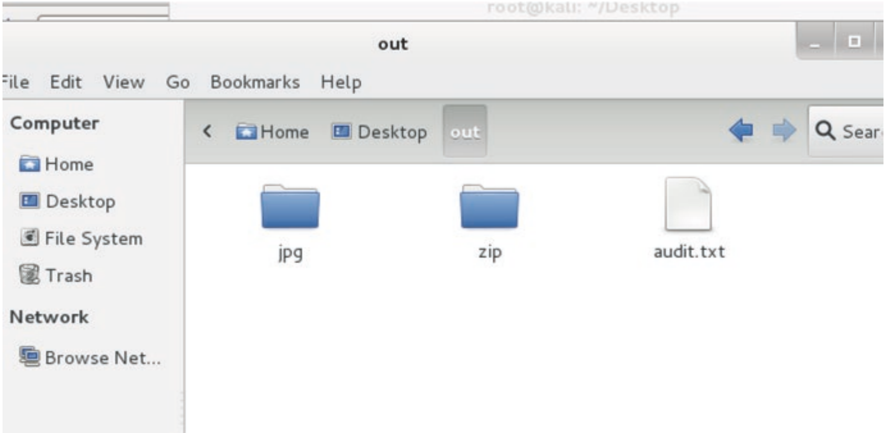
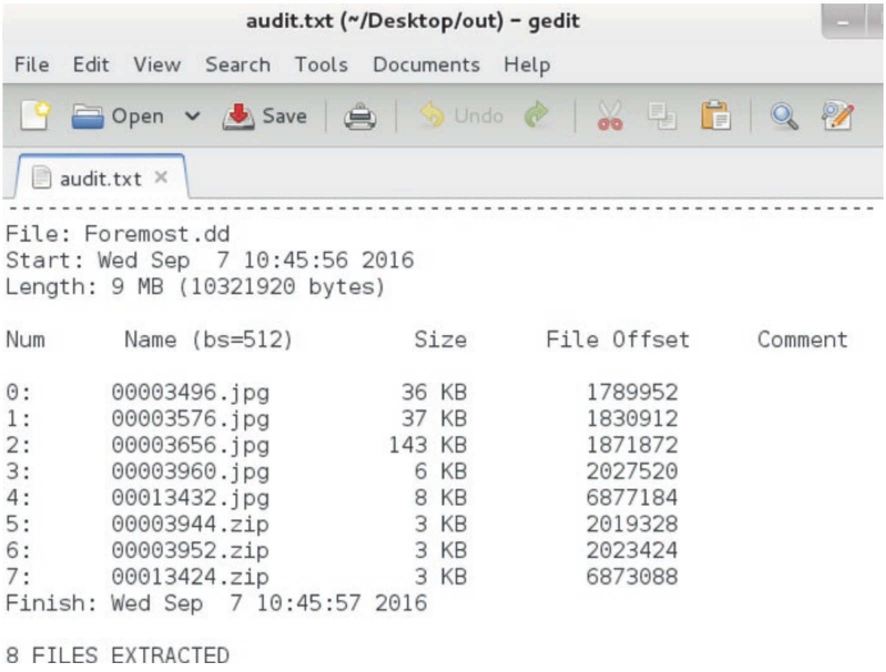


Fig. 11.21 Foremost tool output folder


audit.txt (~/Desktop/out) – gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
audit.txt

```
------------------------------------------------------------------
File: Foremost.dd
Start: Wed Sep  7 10:45:56 2016
Length: 9 MB (10321920 bytes)

Num      Name (bs=512)        Size      File Offset     Comment

0:      00003496.jpg         36 KB       1789952
1:      00003576.jpg         37 KB       1830912
2:      00003656.jpg        143 KB       1871872
3:      00003960.jpg          6 KB       2027520
4:      00013432.jpg          8 KB       6877184
5:      00003944.zip          3 KB       2019328
6:      00003952.zip          3 KB       2023424
7:      00013424.zip          3 KB       6873088
Finish: Wed Sep  7 10:45:57 2016

8 FILES EXTRACTED
```

Fig. 11.22 Foremost tool audit file content

S0069: Skill in Setting Up a Forensic Workstation

Forensic analysis activities and incident response procedures can be divided into 11 steps, (Mandia and Prosise 2001): (1) Planning and preparation, (2) Incident Detection, (3) Initial response, (4) Response strategy formulation, (5) Forensic backups, (6) Investigation, (7) Security measure implementation, (8) Network monitoring, (9) Recovery, (10) Reporting. A complete forensic workstation is expected to include tools for all those stages. We described in an earlier KSA different setups of forensic workstations: (e.g., mobile or stationary workstations).

Some of the popular commercial forensic workstations:

- Accessdata Forensic Toolkit (FTK)

- https://accessdata.com/products-services/forensic-toolkit-ftk
- Autopsy and others in Sleuthkit
- www.sleuthkit.org/autopsy/
- www.sleuthkit.org/sleuthkit/
- Blackbag Blacklight
- www.blackbagtech.com/blacklight.html
- Sumuri Recon
- sumuri.com/software/recon/
- Truxton Forensics
- www.truxtonforensics.com
- Vound Intella
- www.vound-software.com/individual-solutions
- X-Ways Forensics
- www.x-ways.net
- ProDiscover Forensic
- www.arcgroupny.com/products/prodiscover-forensic-edition/
- Perlustro iLookIX
- www.perlustro.com
- Paraben Forensics E3
- www.paraben.com/products/e3-universal
- OSForensics

- www.osforensics.com/osforensics.html

Workstations can have different combinations of hardware and software tools. They can be commercial, high end and expensive, or can also be built out of free or open source software tools (i.e., the software part of the workstation).

As forensic cases vary widely in several different perspectives, when building a forensic station, consider the following issues:

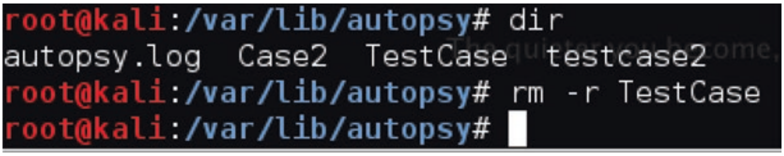
- Statistics of crimes in your local or national area: Several websites publish statistics about digital forensics-related crimes such as: crimes by different categories including computing environments (e.g., smart phones, laptops, desktops) or by malware category. As building a workstation that can deal with all types and domains of crimes can be very expensive, at least focus your resources on the popular crimes in your area.

- The disk and media types to use: Disk storage types change rapidly in the last decades where, for example, some technologies such as tapes, firewires, CDs, and DVDs became obsolete or rarely used. The USB storage media or communication now dominates the market not only on the desktop or laptop environments but almost all other environments.
- The operating systems to use. A forensic station may have to work with different operating system vendors: Microsoft, Apple, Linux, Unix, etc. Additionally, forensic analysts should have skills even in disconnected or rarely used operating systems (e.g., Windows 95, 98, XP) as they may need to deal with a machine still working on such operating systems.
- The different environments to support (e.g., mobile platform, desktops/laptops, embedded systems). They may need to extract information using unconventional methods or environments.
- The use of different sandboxing environments. A major skill required for forensic analysts is to be able to inspect evidence or suspect disks on isolated environments such as VMWare and VirtualBox.

S0071: Skill in Using Forensic Tool Suites (e.g., EnCase, Sleuthkit, FTK)

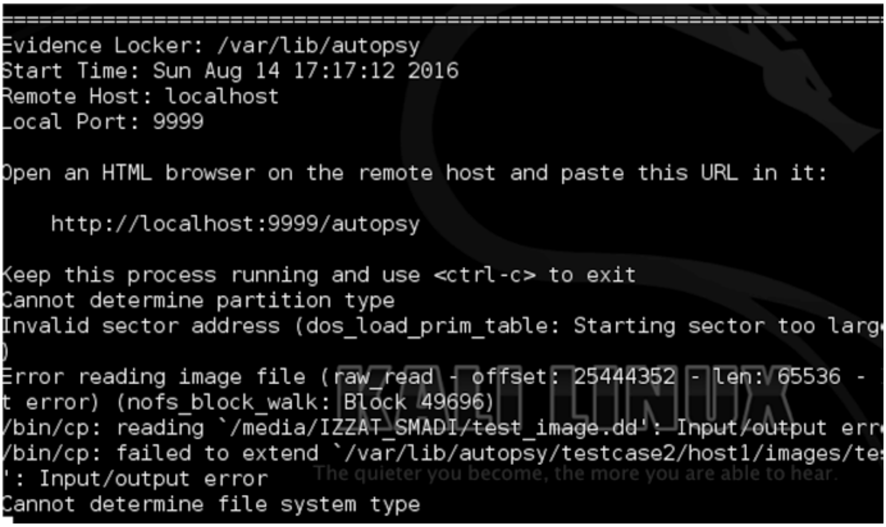
A Sample Usage of Sleuthkit Autopsy Tool

- Links for the tool:
- http://www.sleuthkit.org/autopsy
- http://www.autopsy.com/
- Autopsy is one of the computer forensic tools that can be used to manage a case investigation which may include one or more disks to look for possible evidences through.
- The tool allows investigators to document different types of information about the analysis process, analyzed disks, possible evidences or forensic artifacts, etc.
- The tool also allows users to hash (using different hashing algorithms such as MD5) disks before and after their process to ensure that such disks are not edited by the investigation process.
- The tool is free to install under different operating systems.
- I will demo the version that is already installed under Kali Linux.
- In Kali, the tool and all related files and folders are installed under the folder (/var/lib/autopsy) (Fig. 11.23).



```
root@kali:/var/lib/autopsy# dir
autopsy.log  Case2  TestCase  testcase2
root@kali:/var/lib/autopsy# rm -r TestCase
root@kali:/var/lib/autopsy# 
```

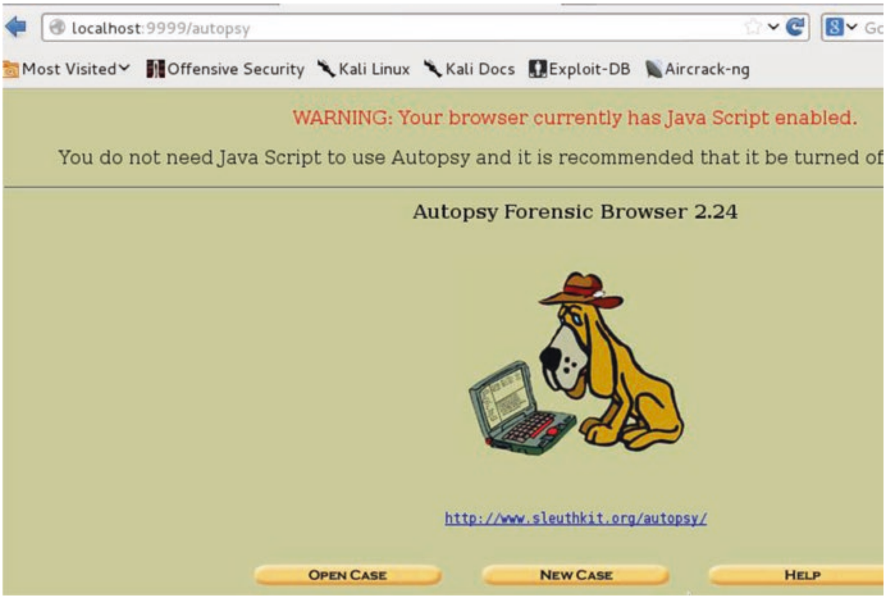
Fig. 11.23 Autopsy folder in Kali



```
================================================================================
Evidence Locker: /var/lib/autopsy
Start Time: Sun Aug 14 17:17:12 2016
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

    http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
Cannot determine partition type
Invalid sector address (dos_load_prim_table: Starting sector too larg
)
Error reading image file (raw_read - offset: 25444352 - len: 65536 - 
t error) (nofs_block_walk: Block 49696)
/bin/cp: reading `/media/IZZAT_SMADI/test_image.dd': Input/output err
/bin/cp: failed to extend `/var/lib/autopsy/testcase2/host1/images/te
': Input/output error
Cannot determine file system type
```

Fig. 11.24 Starting autopsy

- Once autopsy is typed in the console, the tool will start as a web-based application, its main GUI can be hence accessed through a browser surfing to the link: http://localhost:9999/autopsy (Fig. 11.24).
- If you don't have previous cases, you can start by creating a new case (Fig. 11.25).
- I then have to type basic information about the name and description, creator of the case (Fig. 11.26).
- My case is created and screen shows me what files are created for my case (Fig. 11.27).
- Mainly there is a file in the case folder with (.aut) extension.
- I will then be asked to add the host that I want to investigate with many optional features, for example, if there are locations where hashing will be ignored (e.g., temp files) (Fig. 11.28).
- If that information is not included, they will be set to default values (as described in the tool GUI).
- After creating the host, I will be asked to add the image (for the disk I am investigating) (Fig. 11.29).



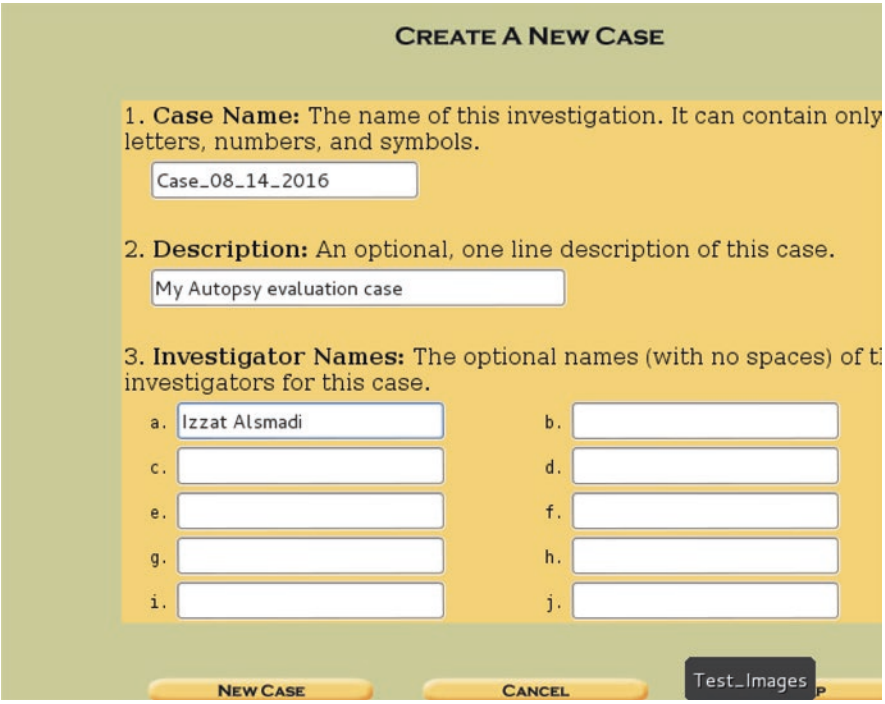
WARNING: Your browser currently has Java Script enabled.

You do not need Java Script to use Autopsy and it is recommended that it be turned of

Autopsy Forensic Browser 2.24

http://www.sleuthkit.org/autopsy/

Fig. 11.25 Autopsy web interface



CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

Case_08_14_2016

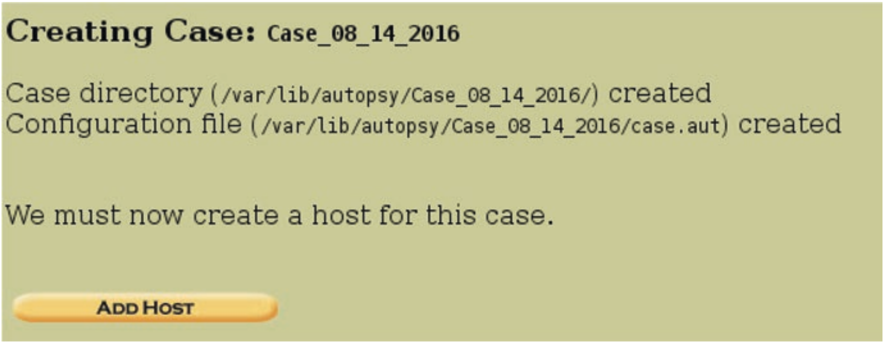
2. **Description:** An optional, one line description of this case.

My Autopsy evaluation case

3. **Investigator Names:** The optional names (with no spaces) of t investigators for this case.

a. Izzat Alsmadi

Fig. 11.26 Autopsy: create a new case, 1

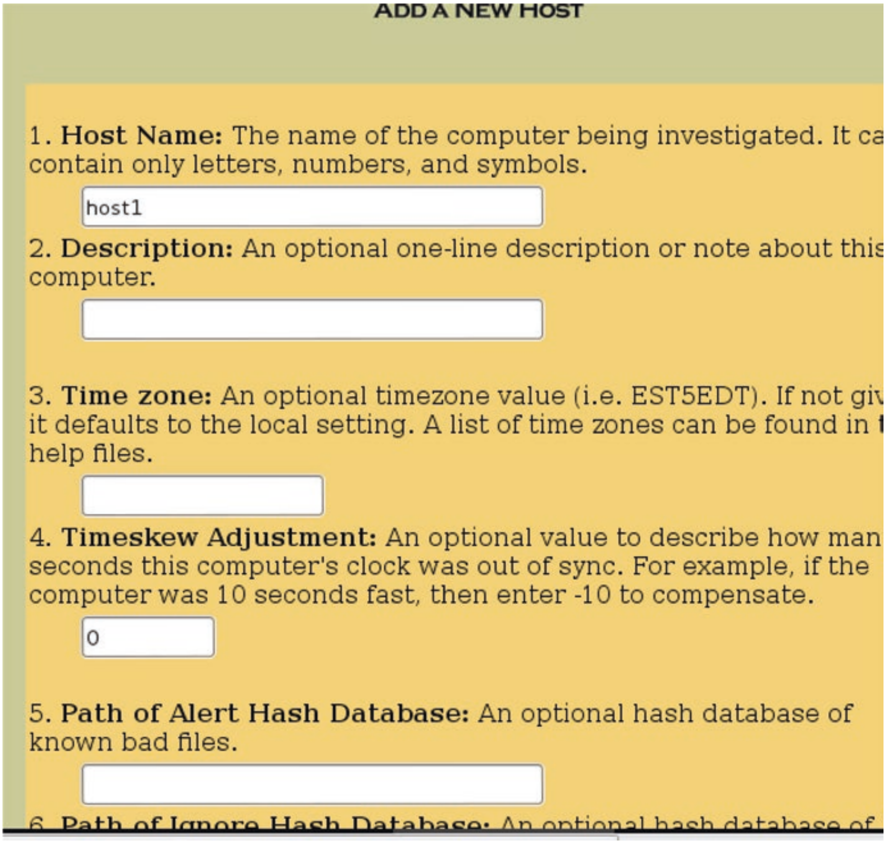


Creating Case: Case_08_14_2016

Case directory (/var/lib/autopsy/Case_08_14_2016/) created
Configuration file (/var/lib/autopsy/Case_08_14_2016/case.aut) created

We must now create a host for this case.

Fig. 11.27 Autopsy: create a new case, 2



ADD A NEW HOST

1. **Host Name:** The name of the computer being investigated. It ca contain only letters, numbers, and symbols.

host1

2. **Description:** An optional one-line description or note about this computer.

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not giv it defaults to the local setting. A list of time zones can be found in t help files.

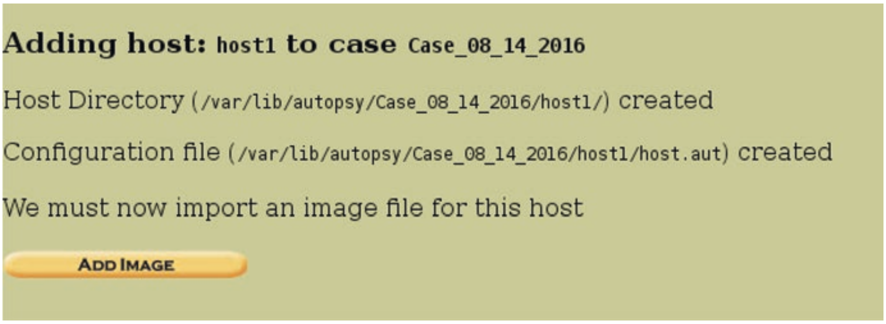
4. **Timeskew Adjustment:** An optional value to describe how man seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

0

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

6. **Path of Ignore Hash Database:** An optional hash database of

Fig. 11.28 Autopsy: create a new case, 3



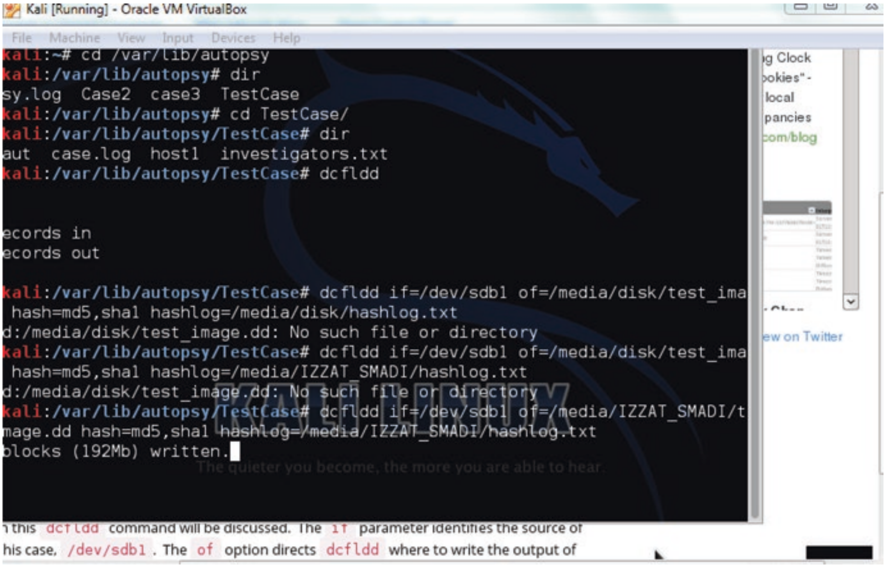
Adding host: host1 to case Case_08_14_2016

Host Directory (/var/lib/autopsy/Case_08_14_2016/host1/) created

Configuration file (/var/lib/autopsy/Case_08_14_2016/host1/host.aut) created

We must now import an image file for this host

Fig. 11.29 Autopsy: adding a host to the case



Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
ıg Clock
ɔokies" -
local
pancies
com/blog
ew on Twitter
The quieter you become, the more you are able to hear.
KALI LINUX

```
kali:~# cd /var/lib/autopsy
kali:/var/lib/autopsy# dir
sy.log  Case2  case3  TestCase
kali:/var/lib/autopsy# cd TestCase/
kali:/var/lib/autopsy/TestCase# dir
aut  case.log  host1  investigators.txt
kali:/var/lib/autopsy/TestCase# dcfldd


ecords in
ecords out

kali:/var/lib/autopsy/TestCase# dcfldd if=/dev/sdb1 of=/media/disk/test_ima
 hash=md5,sha1 hashlog=/media/disk/hashlog.txt
d:/media/disk/test_image.dd: No such file or directory
kali:/var/lib/autopsy/TestCase# dcfldd if=/dev/sdb1 of=/media/disk/test_ima
 hash=md5,sha1 hashlog=/media/IZZAT_SMADI/hashlog.txt
d:/media/disk/test_image.dd: No such file or directory
kali:/var/lib/autopsy/TestCase# dcfldd if=/dev/sdb1 of=/media/IZZAT_SMADI/t
mage.dd hash=md5,sha1 hashlog=/media/IZZAT_SMADI/hashlog.txt
blocks (192Mb) written.
```

n this dcfldd command will be discussed. The if parameter identifies the source of
his case, /dev/sdb1 . The of option directs dcfldd where to write the output of

Fig. 11.30 Using dcfldd to image a disk

- Either create your own forensic image, for experimentation, or use some of the public forensic images from some websites such as:
  - https://digitalcorpora.org/corpora/disk-images
  - https://www.forensicfocus.com/images-and-challenges
  - https://www.cfreds.nist.gov/
- In my case, I want to create a small sample image. I used a tool called (dcfldd) which exists in Kali to create an image from my flash drive. I inserted my flash drive (named IZZAT_SMADI) and using the command shown below, I created an image called test_image.dd (Fig. 11.30).
- I then copied this image file to Kali desktop so that I can import it (Fig. 11.31).
- In the next step, we can add the image we just created (Fig. 11.32).

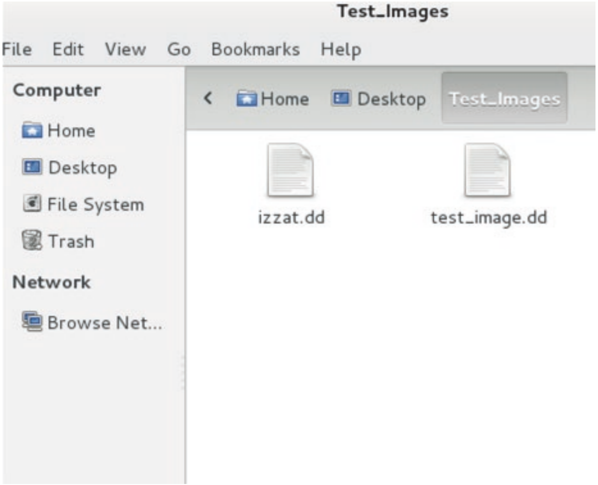
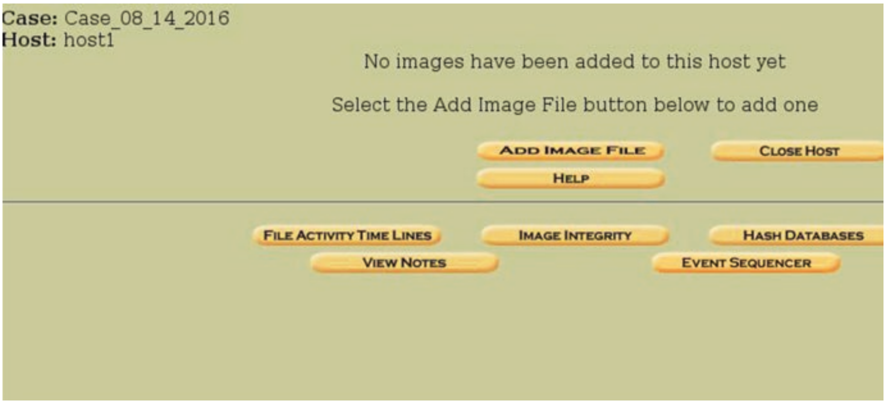


Fig. 11.31 A sample of raw images

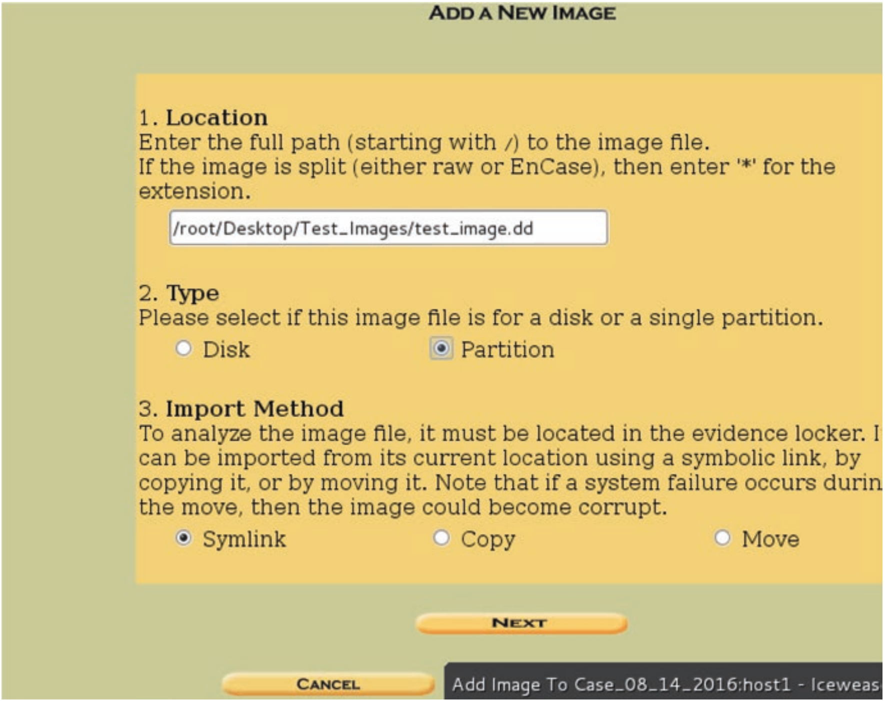

Case: Case_08_14_2016
Host: host1

No images have been added to this host yet

Select the Add Image File button below to add one

Fig. 11.32 Autopsy: adding a disk image to the case, 1

- There are different options that I can pick from to decide the nature of the image I am copying or what I want to do with that image (Fig. 11.33).
- My image will be detected by Autopsy based on its type and I will be asked to select more options related to the Hashing process (Fig. 11.34).
- The next GUI shows that I added successfully my image and will be asked if I want to add more images to the case or not (Fig. 11.35).
- The last GUI in the creation of the case process shows my case and image with what I can do next (i.e., the analysis process) (Fig. 11.36).
- I will start a sample of the analysis process (which is usually context dependent, what you have and what you are searching for) (Fig. 11.37).



ADD A NEW IMAGE

1. **Location**
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

/root/Desktop/Test_Images/test_image.dd

2. **Type**
Please select if this image file is for a disk or a single partition.

○ Disk ● Partition

3. **Import Method**
To analyze the image file, it must be located in the evidence locker. I can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs durin the move, then the image could become corrupt.

● Symlink ○ Copy ○ Move

Fig. 11.33 Autopsy: adding a disk image to the case, 2

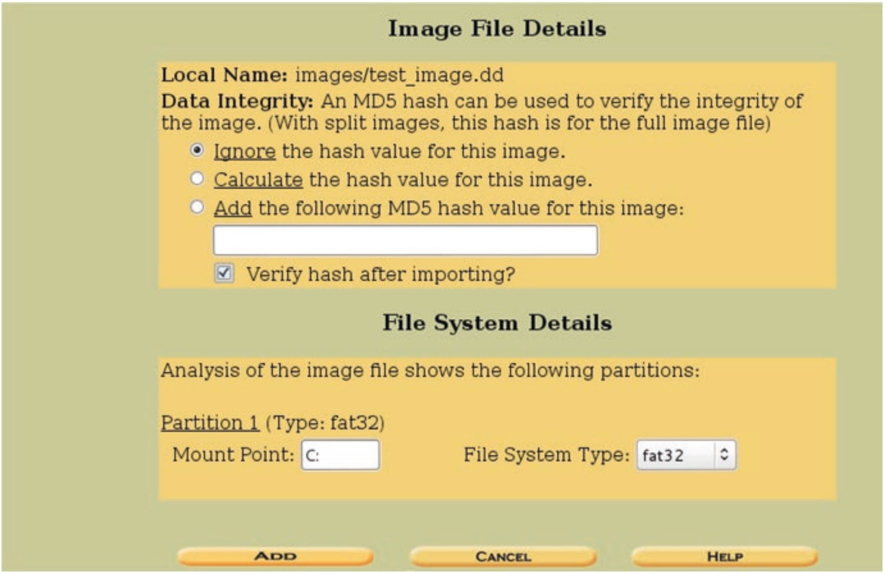


Image File Details

Local Name: images/test_image.dd
Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

● Ignore the hash value for this image.
○ Calculate the hash value for this image.
○ Add the following MD5 hash value for this image:

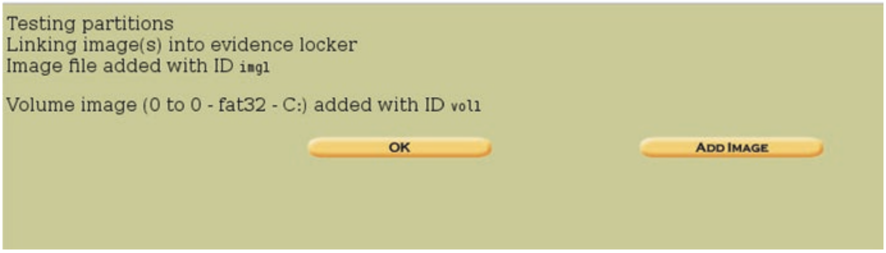
☑ Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: fat32)
Mount Point: C: File System Type: fat32

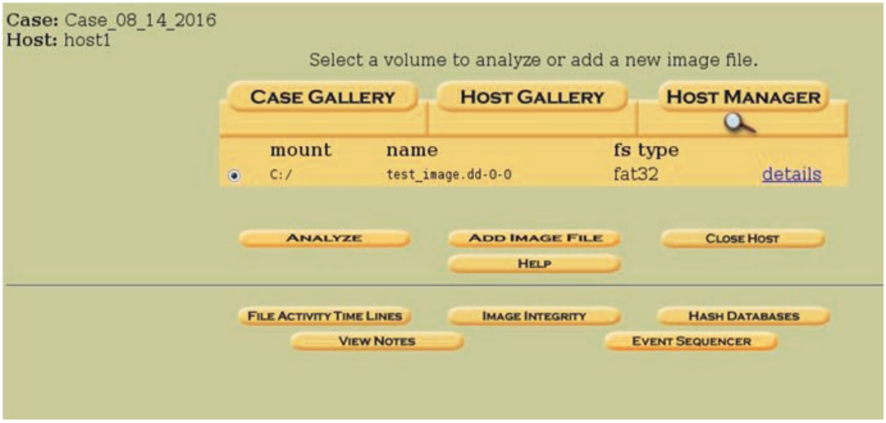
Fig. 11.34 Autopsy: adding a disk image to the case, 3



Testing partitions
Linking image(s) into evidence locker
Image file added with ID img1

Volume image (0 to 0 - fat32 - C:) added with ID vol1

Fig. 11.35 Autopsy: adding a disk image to the case, 4

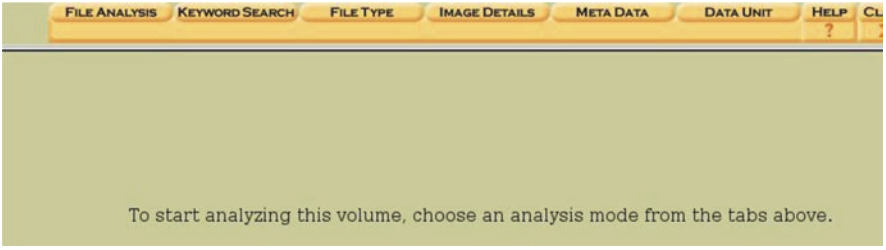


Case: Case_08_14_2016
Host: host1

Select a volume to analyze or add a new image file.

	mount	name	fs type	
●	C:/	test_image.dd-0-0	fat32	details

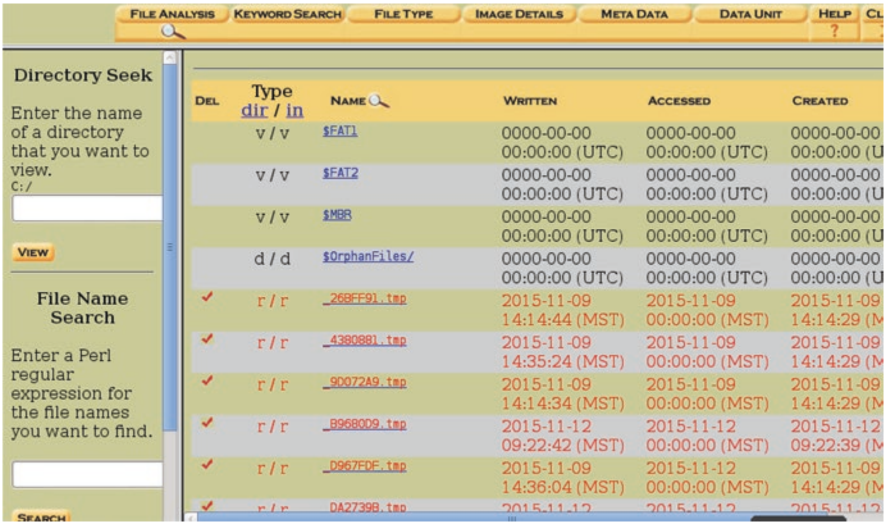
Fig. 11.36 Autopsy: adding a disk image to the case, 5



To start analyzing this volume, choose an analysis mode from the tabs above.

Fig. 11.37 Autopsy: start the analysis process, 1

- I can do: File analysis, keyword search, file type, image details, metadata, data unit (Fig. 11.38).
- The file analysis shows me a screen somewhat similar to what we see in Windows explorer about files (i.e., names, locations, MAC). I can also do regular file search.
- I can do keyword search looking for clues. There are some built-in keyword searches to pick from as well, Fig. 11.39.



Directory Seek

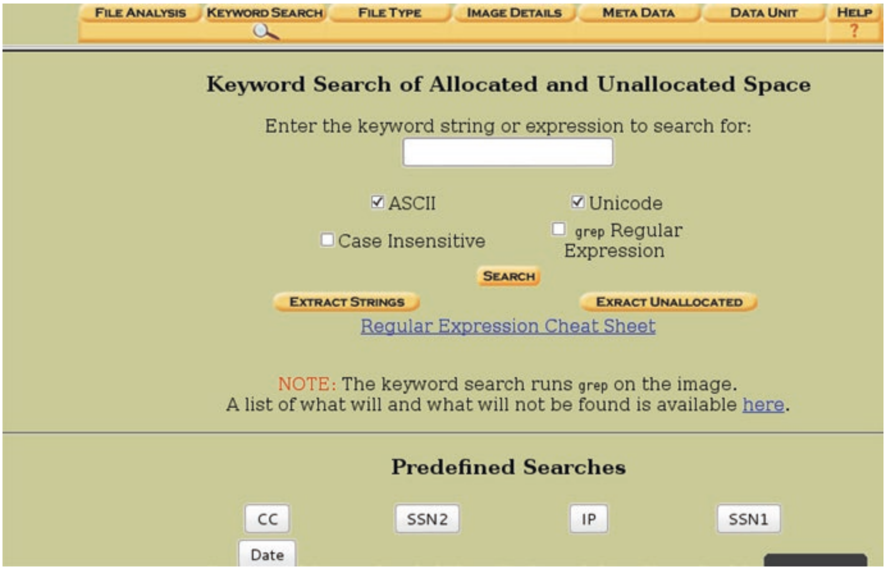
Enter the name of a directory that you want to view.
C:/

File Name Search

Enter a Perl regular expression for the file names you want to find.

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CREATED
	v / v	$FAT1	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (U
	v / v	$FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (U
	v / v	$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (U
	d / d	$OrphanFiles/	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (U
✓	r / r	_26BFF91.tmp	2015-11-09 14:14:44 (MST)	2015-11-09 00:00:00 (MST)	2015-11-09 14:14:29 (M
✓	r / r	_4380881.tmp	2015-11-09 14:35:24 (MST)	2015-11-09 00:00:00 (MST)	2015-11-09 14:14:29 (M
✓	r / r	_9D072A9.tmp	2015-11-09 14:14:34 (MST)	2015-11-09 00:00:00 (MST)	2015-11-09 14:14:29 (M
✓	r / r	_B9680D9.tmp	2015-11-12 09:22:42 (MST)	2015-11-12 00:00:00 (MST)	2015-11-12 09:22:39 (M
✓	r / r	_D967FDF.tmp	2015-11-09 14:36:04 (MST)	2015-11-12 00:00:00 (MST)	2015-11-09 14:14:29 (M
✓	r / r	DA2739B.tmp	2015-11-12	2015-11-12	2015-11-12

Fig. 11.38 Autopsy: start the analysis process, 2



Keyword Search of Allocated and Unallocated Space

Enter the keyword string or expression to search for:

☑ ASCII ☑ Unicode

☐ Case Insensitive ☐ grep Regular Expression

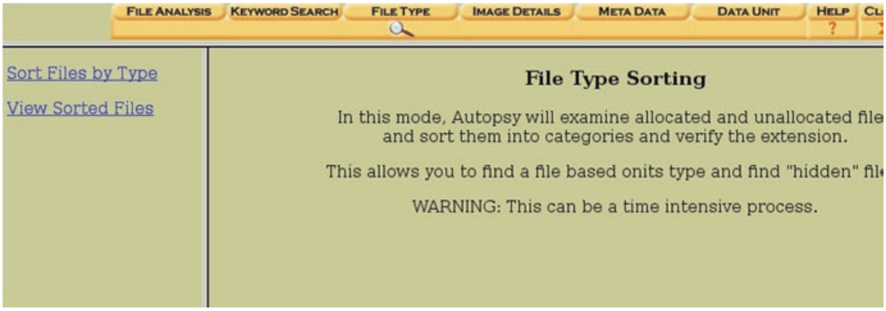
Regular Expression Cheat Sheet

NOTE: The keyword search runs grep on the image.
A list of what will and what will not be found is available here.

Predefined Searches

Fig. 11.39 Autopsy: start the analysis process, 3

- I can do extensive search based on file types (Fig. 11.40).
- In the image details part, I can extract metadata about the image itself (Fig. 11.41).
- I can use metadata for more details about folders or directories (mine does not show many as my flash includes only several files without folders or directories) (Fig. 11.42).
- I can do sector-by-sector analysis in the data unit section (Fig. 11.43).



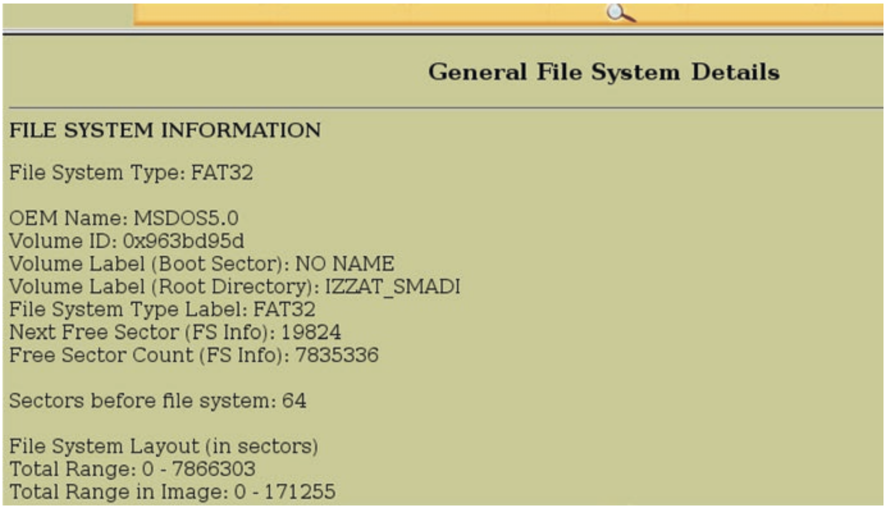
File Type Sorting

In this mode, Autopsy will examine allocated and unallocated file
and sort them into categories and verify the extension.

This allows you to find a file based onits type and find "hidden" fil

WARNING: This can be a time intensive process.

Fig. 11.40 Autopsy: start the analysis process, 4



General File System Details

FILE SYSTEM INFORMATION

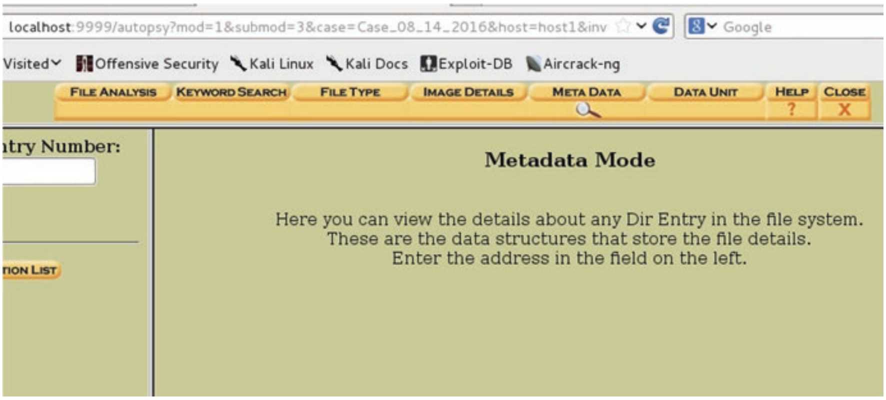
File System Type: FAT32

OEM Name: MSDOS5.0
Volume ID: 0x963bd95d
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory): IZZAT_SMADI
File System Type Label: FAT32
Next Free Sector (FS Info): 19824
Free Sector Count (FS Info): 7835336

Sectors before file system: 64

File System Layout (in sectors)
Total Range: 0 - 7866303
Total Range in Image: 0 - 171255

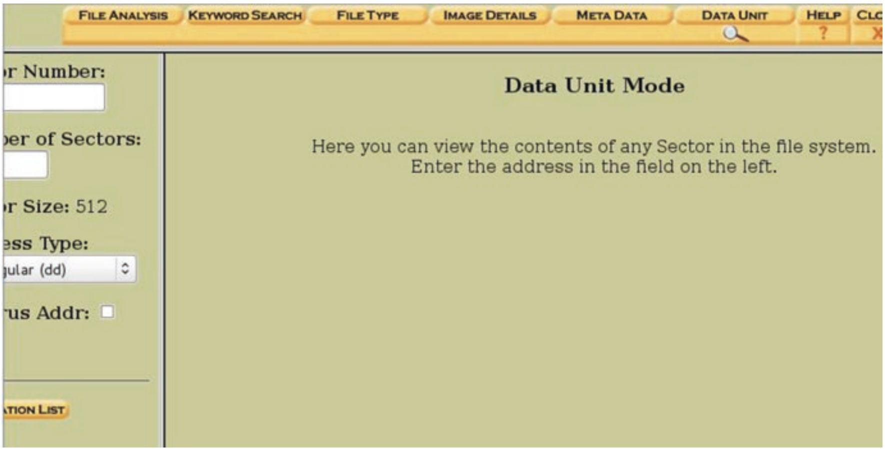
Fig. 11.41 Autopsy: start the analysis process, 5



Metadata Mode

Here you can view the details about any Dir Entry in the file system.
These are the data structures that store the file details.
Enter the address in the field on the left.

Fig. 11.42 Autopsy: start the analysis process, 6



r Number:

er of Sectors:

r Size: 512

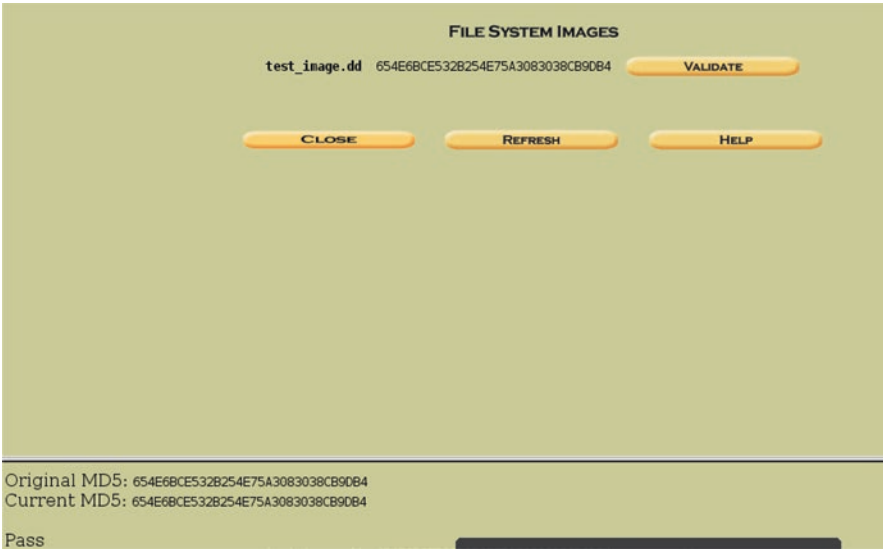
ess Type: ular (dd)

us Addr: □

Data Unit Mode

Here you can view the contents of any Sector in the file system.
Enter the address in the field on the left.

Fig. 11.43 Autopsy: start the analysis process, 7



FILE SYSTEM IMAGES

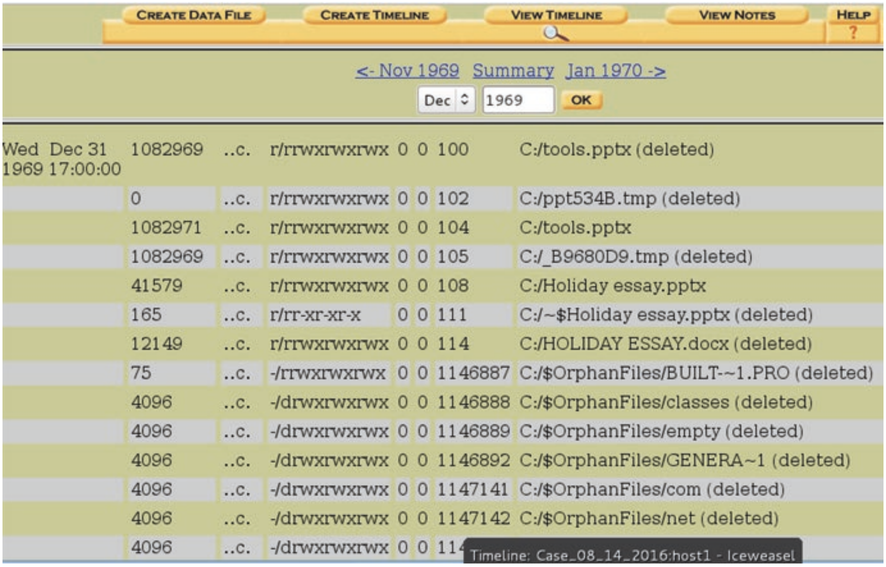
test_image.dd 654E6BCE532B254E75A3083038CB9DB4

Original MD5: 654E6BCE532B254E75A3083038CB9DB4
Current MD5: 654E6BCE532B254E75A3083038CB9DB4

Pass

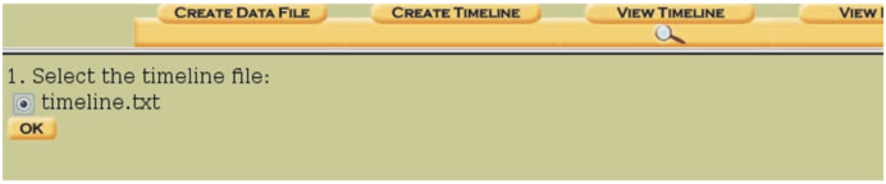
Fig. 11.44 Autopsy: image integrity verification

- Validating the image integrity showed that original and current MD5 hashing are the same which shows that I did not edit the image, Fig. 11.44.
- I then created a timeline to show different activities on file system (useful to know if some files are deleted and when) (I didn't show here how to create the timeline) (Fig. 11.45).
- I saved the timeline to a separate file (Fig. 11.46).



```
Wed  Dec 31     1082969  ..c.  r/rrwxrwxrwx  0 0 100      C:/tools.pptx (deleted)
1969 17:00:00
                0        ..c.  r/rrwxrwxrwx  0 0 102      C:/ppt534B.tmp (deleted)
                1082971  ..c.  r/rrwxrwxrwx  0 0 104      C:/tools.pptx
                1082969  ..c.  r/rrwxrwxrwx  0 0 105      C:/_B9680D9.tmp (deleted)
                41579    ..c.  r/rrwxrwxrwx  0 0 108      C:/Holiday essay.pptx
                165      ..c.  r/rr-xr-xr-x  0 0 111      C:/~$Holiday essay.pptx (deleted)
                12149    ..c.  r/rrwxrwxrwx  0 0 114      C:/HOLIDAY ESSAY.docx (deleted)
                75       ..c.  -/rrwxrwxrwx  0 0 1146887  C:/$OrphanFiles/BUILT-~1.PRO (deleted)
                4096     ..c.  -/drwxrwxrwx  0 0 1146888  C:/$OrphanFiles/classes (deleted)
                4096     ..c.  -/drwxrwxrwx  0 0 1146889  C:/$OrphanFiles/empty (deleted)
                4096     ..c.  -/drwxrwxrwx  0 0 1146892  C:/$OrphanFiles/GENERA~1 (deleted)
                4096     ..c.  -/drwxrwxrwx  0 0 1147141  C:/$OrphanFiles/com (deleted)
                4096     ..c.  -/drwxrwxrwx  0 0 1147142  C:/$OrphanFiles/net (deleted)
                4096     ..c.  -/drwxrwxrwx  0 0 114
```

Fig. 11.45 Autopsy: start the analysis process, 8



1. Select the timeline file:
● timeline.txt

Fig. 11.46 Autopsy: start the analysis process, 9

S0075: Skill in Conducting Forensic Analyses in Multiple Operating System Environments (e.g., Mobile Device Systems)

Using Santoku: https://santoku-linux.com

- Download Santoku image and follow instructions to install it in an image
- (https://santoku-linux.com/howtos/). Then follow instructions to complete one of the five mobile forensic exercises described in the previous link, under (Mobile Forensics):
- HOWTO use AFLogical OSE for Logical Forensics of an Android Device
- HOWTO use iPhone Backup Analyzer on Santoku Linux
- HOWTO brute force Android Encryption on Santoku Linux

- HOWTO forensically examine an Android device with AFLogical OSE on Santoku Linux
- HOWTO create a logical iOS device backup using libi mobile device on Santoku Linux

S0087: Skill in Deep Analysis of Captured Malicious Code (e.g., Malware Forensics)

Deep analysis in data science using different algorithms to look for deep or hidden knowledge, intelligence, or patterns in analyzed data. Some of the open source tools and mechanisms that can be used in forensics deep analysis:

- Java packages such as DL4j (https://deeplearning4j.org) and TensorFlow: (https://www.tensorflow.org/install/install_java)
- Python with Deep learning libraries such as:
  - Caffe: http://caffe.berkeleyvision.org/
  - Theano: http://deeplearning.net/software/theano/
  - TensorFlow https://www.tensorflow.org/
- R and R-Studio: Libraries such as TensorFlow and Keras (https://keras.io)
- MATLAB: https://www.mathworks.com/solutions/deep-learning.html

We also described in another skill (S0055) examples of IDEs and management technologies that learner should be exposed to.

In terms of the areas applicable in security intelligence in general or forensics in particular, we described examples of those application areas in the skill (S0109).

S0088: Skill in Using Binary Analysis Tools (e.g., Hexedit, Command Code xxd, hexdump)

- Several hackers use steganography to hide text in pictures. Search for a picture online that has steganography. Then use a hex-editor program (e.g., WinHex: http://www.x-ways.net/winhex/) to open and analyze this file. Your goal is to extract the hidden text or file, find out its type, size (modify its extension to reflect its actual type). Hint (as a jpeg file, check its start and EOF markers to know the end of the first file and copy the rest to a new file. Each file ends with certain hex-markers and then 00000).
- Search for a file online that has no file extension or an unknown file extension. Then use hexadecimal editors to know/correct the file extensions and then open the file and retrieve its content.

- Download Hex Workshop and follow the steps described in the link. (http://blog.hakzone.info/posts-and-articles/bios/analysing-the-master-boot-record-mbr-with-a-hex-editor-hex-workshop/) to describe the file structure in your disk). Be careful not to change any single bit or you may destroy your OS in your main disk.

S0120: Skill in Reviewing Logs to Identify Evidence of Past Intrusions

- In LinuxZoo website, (https://linuxzoo.net/page/tut_log.html) complete the practice exercises for Snort log analysis.
- Search through the Internet for "SNORT Log analysis tools," (e.g., SNORTALog http://www.securiteam.com/tools/5UP0G1FE0C.html) and find a proper tool to analyze a sample of SNORT log file that you can download from an image (or your own Kali image). Show several screenshots from your analysis and any interesting information or knowledge you can get from SNORT log.

S0175: Skill in Performing Root-Cause Analysis

In this chapter, root-cause analysis (RCA) focuses on trying to study and understand attacker or suspect behaviors, how they attacked the victim user or machine. This is accomplished through identifying and understanding the remnants they left on the victim system and the attack vector used to compromise the system.

In RCA, the examination follows a scientific method that consists of formulating hypotheses for all the probable causes of the incident and predicting and testing evidence for each hypothesis. The root cause is the hypothesis that accounts for most of the evidence (Noon, 2001). Searching for evidences includes looking for incident artifacts in one of the following categories, Fig. 11.47, (Harrell 2012):

- Source and delivery mechanisms such as: the Internet, emails, the network services, removable media, or physical access
- Exploit and delivery mechanisms such as: the Internet, the network services, or removable media
- Payload
- Indicators (e.g., IOC) or symptoms

Evidences or traces may start in one of those categories, but will eventually help analysts find out the other pieces of the puzzle. Figure 11.48 shows an example with instances of the attack artifacts based on the model described in Fig. 11.47.

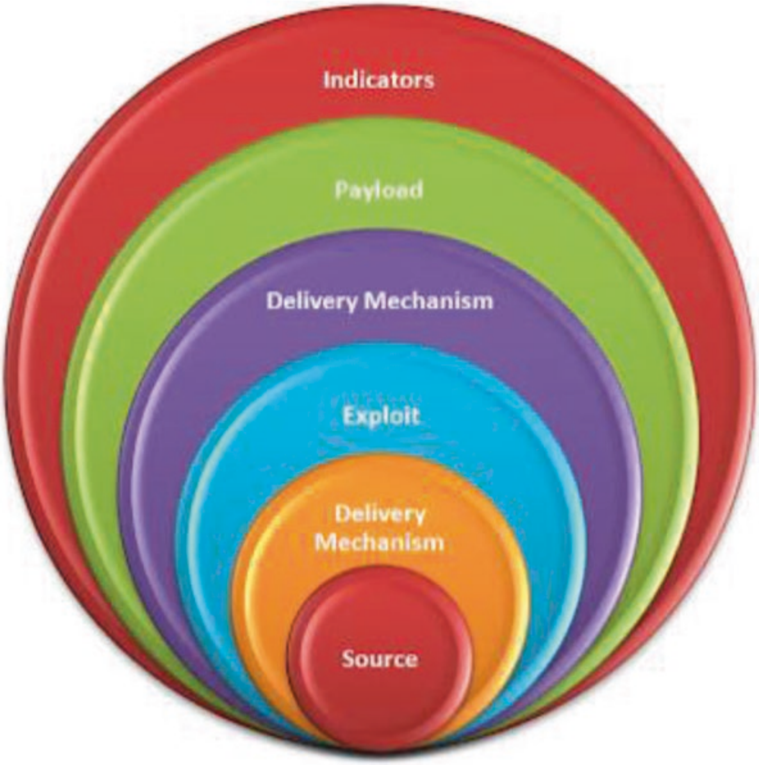
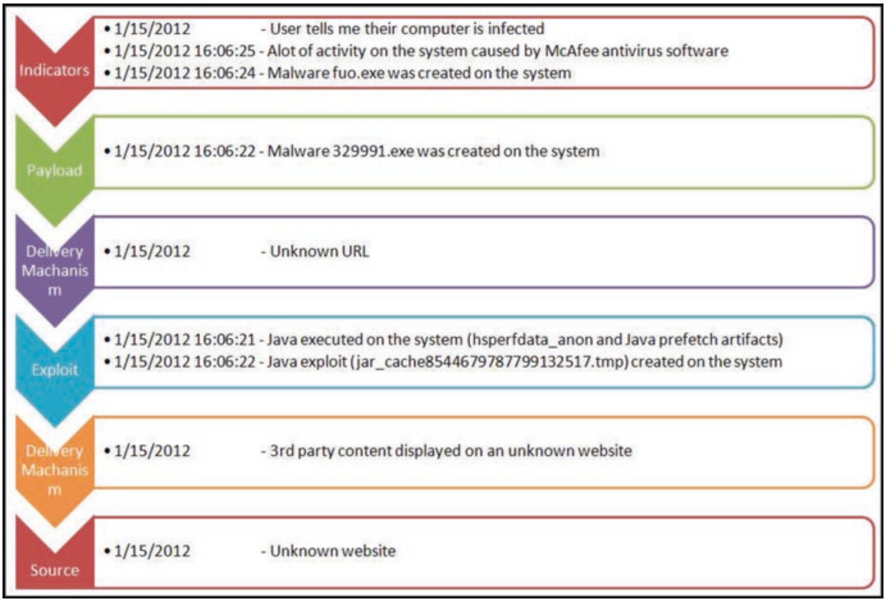


Fig. 11.47 Attack artifacts (Harrell 2012)

A0010: Ability to Analyze Malware

1. Start from the link (Malware analysis and incident response tools for the frugal and lazy, https://postmodernsecurity.com/tag/malware-analysis/) which includes a large number of online malware analysis tools. They can do either web links analysis or files analysis. You are expected to select either a website for links tests or files for the file test. Select those from your machine (files) and links from a website to test, of your choice. As an alternative, you can select from public known malicious links. (e.g., https://malwared.malwaremustdie.org/db/fulllist.php) and public known malicious files (e.g., https://zeltser.com/malware-sample-sources/). For the safety of your own machine, use a sandboxing environment (e.g., Kali in a virtual environment).
2. Sandboxie (https://www.sandboxie.com/) is an example of a free tool that can be used to analyze malwares in an isolated environment. Download and analyze malwares using Sandboxie from one of the following public malware resources:

   https://virusshare.com/
   https://zeltser.com/malware-sample-sources/



- 1/15/2012 - User tells me their computer is infected
- 1/15/2012 16:06:25 - Alot of activity on the system caused by McAfee antivirus software
- 1/15/2012 16:06:24 - Malware fuo.exe was created on the system

- 1/15/2012 16:06:22 - Malware 329991.exe was created on the system

- 1/15/2012 - Unknown URL

- 1/15/2012 16:06:21 - Java executed on the system (hsperfdata_anon and Java prefetch artifacts)
- 1/15/2012 16:06:22 - Java exploit (jar_cache8544679787799132517.tmp) created on the system

- 1/15/2012 - 3rd party content displayed on an unknown website

- 1/15/2012 - Unknown website

Fig. 11.48 Instances of attack artifacts (Harrell 2012)

https://github.com/ytisf/theZoo
https://www.megabeets.net/fantastic-malware-and-where-to-find-them/
https://support.clean-mx.com/clean-mx/viruses
https://zeustracker.abuse.ch/monitor.php?browse=binaries
http://contagiodump.blogspot.com/
http://www.kernelmode.info/forum/viewforum.php?f=16
http://labs.sucuri.net/?malware
https://www.scumware.org/index.scumware
http://www.malwaredomainlist.com/update.php
http://urlquery.net/
http://malwareurls.joxeankoret.com/normal.txt

3. Demo the usage of NSRL public hash database
   This lab demonstrates the use of publicly hashed datasets provided by the National Software Reference Library (https://www.nist.gov/software-quality-group/national-software-reference-library-nsrl). The goals of this lab are as follows:

Use a virtual machine as a server for the hash dataset

Use a different virtual machine as a client and compare the hashes of all the files in its system to the hash dataset. Hashes that do not appear in the server's dataset can be regarded as suspicious and deserving of further inspection.

I created a clone of my Kali machine in VirtualBox. One will be the server, the other the client. Both machines will be able to reach each other and the Internet by way of a NatNetwork.

Server (NSRLserver) Experiment

In order to install nsrlserver, the machine needs a gcc compiler, cmake, and boost (Fig. 11.49).

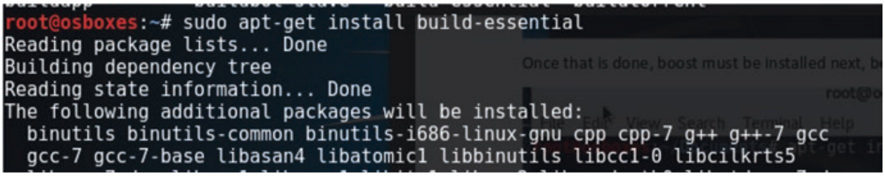
Once that is done, boost must be installed next, before cmake (Fig. 11.50):

Cmake is last. Here is the procedure to download it with wget (Fig. 11.51):

– wget https://cmake.org/files/v3.7/cmake-3.7.2.tar.gz
– tar xzvf cmake-3.7.2.tar.gz
– cd cmake-3.7.2
– ./bootstrap
– make
– make install

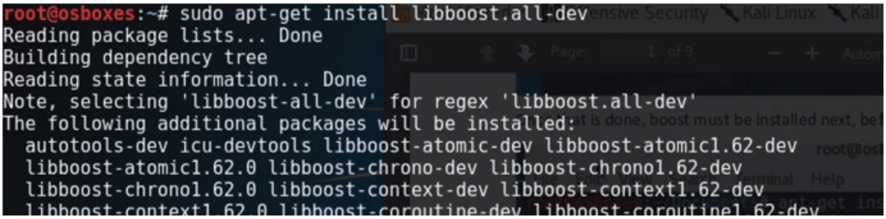
After all those prerequisites, I can install nsrlserver:

– Wget https://github.com/rjhansen/nsrlsvr/tarball/master
– tar xzvf master
– cd rjhansen-nsrlsvr-eaaf166



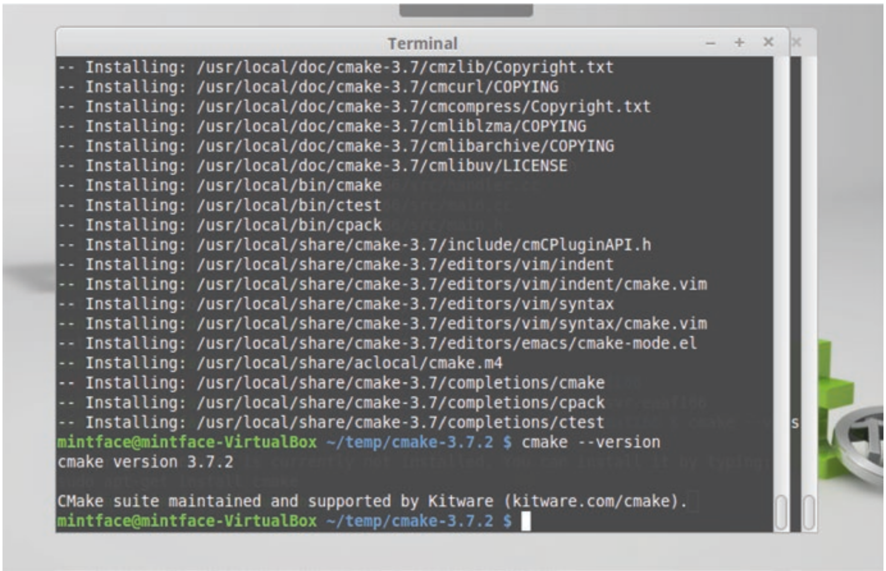
```
root@osboxes:~# sudo apt-get install build-essential
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  binutils binutils-common binutils-i686-linux-gnu cpp cpp-7 g++ g++-7 gcc
  gcc-7 gcc-7-base libasan4 libatomic1 libbinutils libcc1-0 libcilkrts5
```

Fig. 11.49 nsrlserver prerequisite installation, 1



```
root@osboxes:~# sudo apt-get install libboost.all-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'libboost-all-dev' for regex 'libboost.all-dev'
The following additional packages will be installed:
  autotools-dev icu-devtools libboost-atomic-dev libboost-atomic1.62-dev
  libboost-atomic1.62.0 libboost-chrono-dev libboost-chrono1.62-dev
  libboost-chrono1.62.0 libboost-context-dev libboost-context1.62-dev
  libboost-context1.62.0 libboost-coroutine-dev libboost-coroutine1.62-dev
```

Fig. 11.50 nsrlserver prerequisite installation, 2



```
-- Installing: /usr/local/doc/cmake-3.7/cmzlib/Copyright.txt
-- Installing: /usr/local/doc/cmake-3.7/cmcurl/COPYING
-- Installing: /usr/local/doc/cmake-3.7/cmcompress/Copyright.txt
-- Installing: /usr/local/doc/cmake-3.7/cmliblzma/COPYING
-- Installing: /usr/local/doc/cmake-3.7/cmlibarchive/COPYING
-- Installing: /usr/local/doc/cmake-3.7/cmlibuv/LICENSE
-- Installing: /usr/local/bin/cmake
-- Installing: /usr/local/bin/ctest
-- Installing: /usr/local/bin/cpack
-- Installing: /usr/local/share/cmake-3.7/include/cmCPluginAPI.h
-- Installing: /usr/local/share/cmake-3.7/editors/vim/indent
-- Installing: /usr/local/share/cmake-3.7/editors/vim/indent/cmake.vim
-- Installing: /usr/local/share/cmake-3.7/editors/vim/syntax
-- Installing: /usr/local/share/cmake-3.7/editors/vim/syntax/cmake.vim
-- Installing: /usr/local/share/cmake-3.7/editors/emacs/cmake-mode.el
-- Installing: /usr/local/share/aclocal/cmake.m4
-- Installing: /usr/local/share/cmake-3.7/completions/cmake
-- Installing: /usr/local/share/cmake-3.7/completions/cpack
-- Installing: /usr/local/share/cmake-3.7/completions/ctest
mintface@mintface-VirtualBox ~/temp/cmake-3.7.2 $ cmake --version
cmake version 3.7.2

CMake suite maintained and supported by Kitware (kitware.com/cmake).
mintface@mintface-VirtualBox ~/temp/cmake-3.7.2 $
```

Fig. 11.51 nsrlserver prerequisite installation, 3

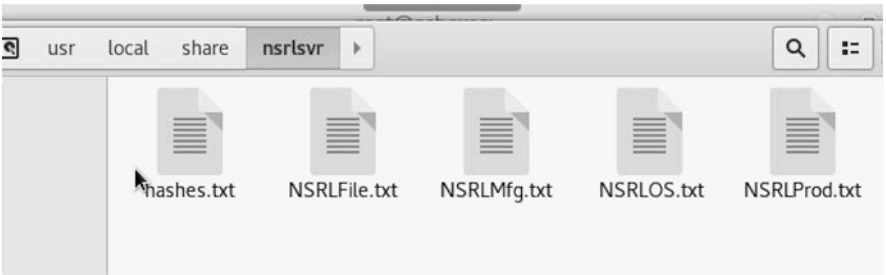


Fig. 11.52 Creating hashes.txt file

There is a ReadMe file that details the installation process. You need to find the location of Python3 on your computer and add it to the path of this command:

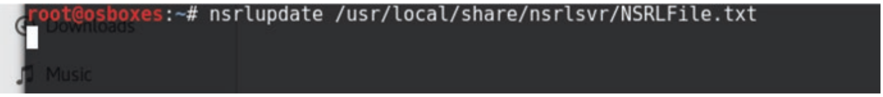
- cmake -DPYTHON_EXECUTABLE=usr/bin/python3 (The trailing zero is important.)
- make install

I then created an empty text file, hashes.txt and put it here (Fig. 11.52):

Then, we need to download a dataset of known, good files, from NSRL national repository. I used the minimal hashset (http://www.nsrl.nist.gov/Downloads.htm#isos). Download and unzip it to NSRLFile.txt in the same previous directory.

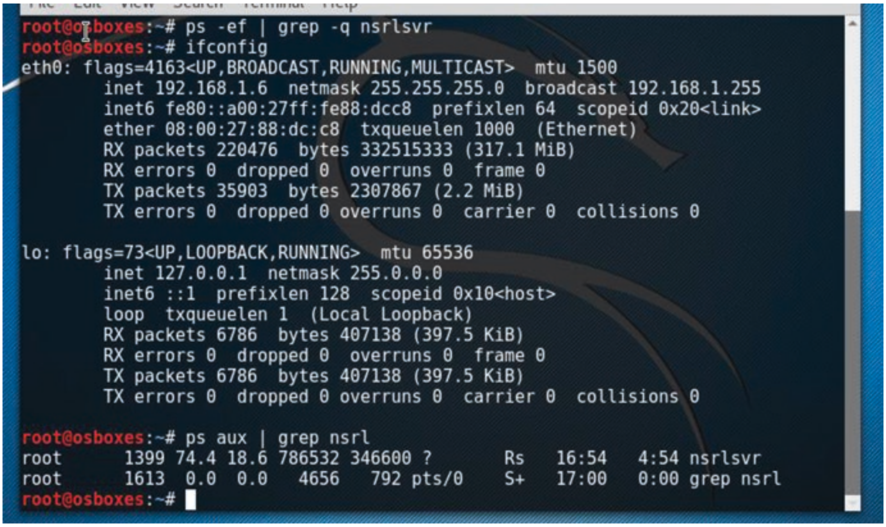
Using terminal, use the command nsrlupdate (Fig. 11.53):

hashes.txt will host more than 1 GB worth of hashes. Now our server is ready, and we can start it by typing “nsrlsvr” (Fig. 11.54).



```
root@osboxes:~# nsrlupdate /usr/local/share/nsrlsvr/NSRLFile.txt
```

Fig. 11.53 Use nsrlupdate to install on the server



```
root@osboxes:~# ps -ef | grep -q nsrlsvr
root@osboxes:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.6  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe88:dcc8  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:88:dc:c8  txqueuelen 1000  (Ethernet)
        RX packets 220476  bytes 332515333 (317.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 35903  bytes 2307867 (2.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 6786  bytes 407138 (397.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6786  bytes 407138 (397.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@osboxes:~# ps aux | grep nsrl
root      1399 74.4 18.6 786532 346600 ?       Rs   16:54   4:54 nsrlsvr
root      1613  0.0  0.0   4656   792 pts/0    S+   17:00   0:00 grep nsrl
root@osboxes:~# 
```

Fig. 11.54 Starting NSRL server

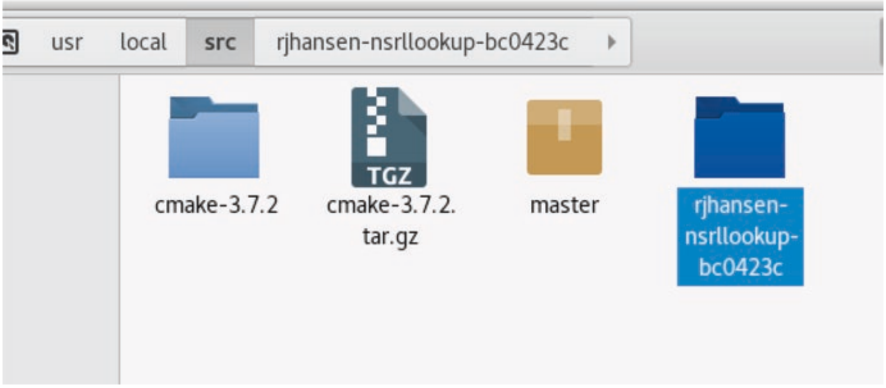


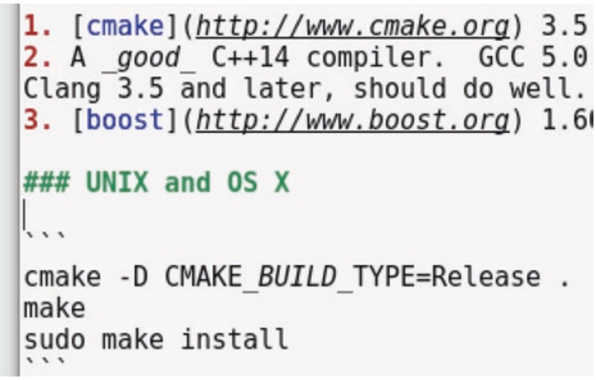
Fig. 11.55 Installing client nsrllookup, 1

Install the Client Side (nsrllookup)

The client needs the same prerequisites for nsrllookup, and they are installed exactly the same way (Fig. 11.55).

The steps are described in the ReadMe file (Figs. 11.56 and 11.57).

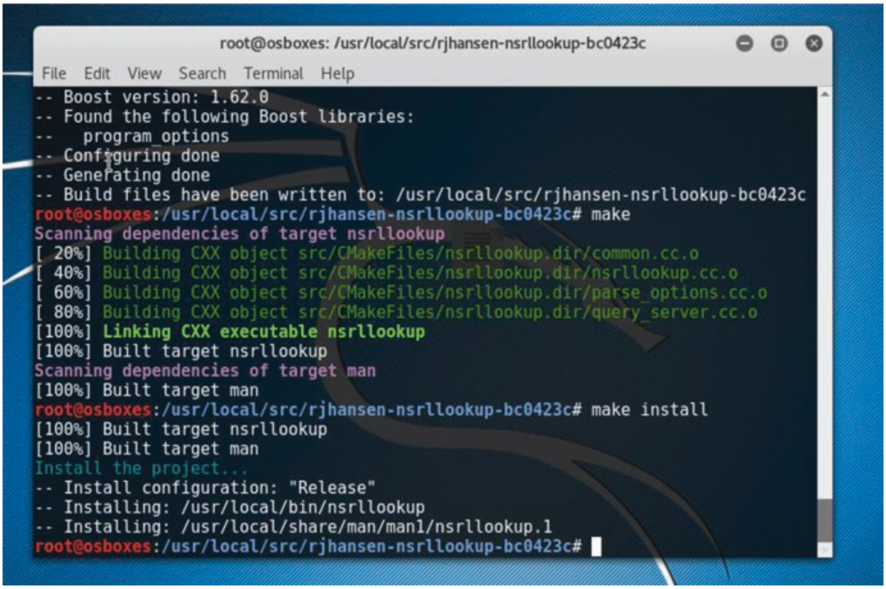
The next step is to install md5deep using apt-get (Fig. 11.58):



```
1. [cmake](http://www.cmake.org) 3.5
2. A _good_ C++14 compiler.  GCC 5.0
Clang 3.5 and later, should do well.
3. [boost](http://www.boost.org) 1.6

### UNIX and OS X

```

cmake -D CMAKE_BUILD_TYPE=Release .
make
sudo make install
```
```

Fig. 11.56 nsrllookup ReadMe file



root@osboxes: /usr/local/src/rjhansen-nsrllookup-bc0423c
File Edit View Search Terminal Help

```
-- Boost version: 1.62.0
-- Found the following Boost libraries:
--   program_options
-- Configuring done
-- Generating done
-- Build files have been written to: /usr/local/src/rjhansen-nsrllookup-bc0423c
root@osboxes:/usr/local/src/rjhansen-nsrllookup-bc0423c# make
Scanning dependencies of target nsrllookup
[ 20%] Building CXX object src/CMakeFiles/nsrllookup.dir/common.cc.o
[ 40%] Building CXX object src/CMakeFiles/nsrllookup.dir/nsrllookup.cc.o
[ 60%] Building CXX object src/CMakeFiles/nsrllookup.dir/parse_options.cc.o
[ 80%] Building CXX object src/CMakeFiles/nsrllookup.dir/query_server.cc.o
[100%] Linking CXX executable nsrllookup
[100%] Built target nsrllookup
Scanning dependencies of target man
[100%] Built target man
root@osboxes:/usr/local/src/rjhansen-nsrllookup-bc0423c# make install
[100%] Built target nsrllookup
[100%] Built target man
Install the project...
-- Install configuration: "Release"
-- Installing: /usr/local/bin/nsrllookup
-- Installing: /usr/local/share/man/man1/nsrllookup.1
root@osboxes:/usr/local/src/rjhansen-nsrllookup-bc0423c#
```

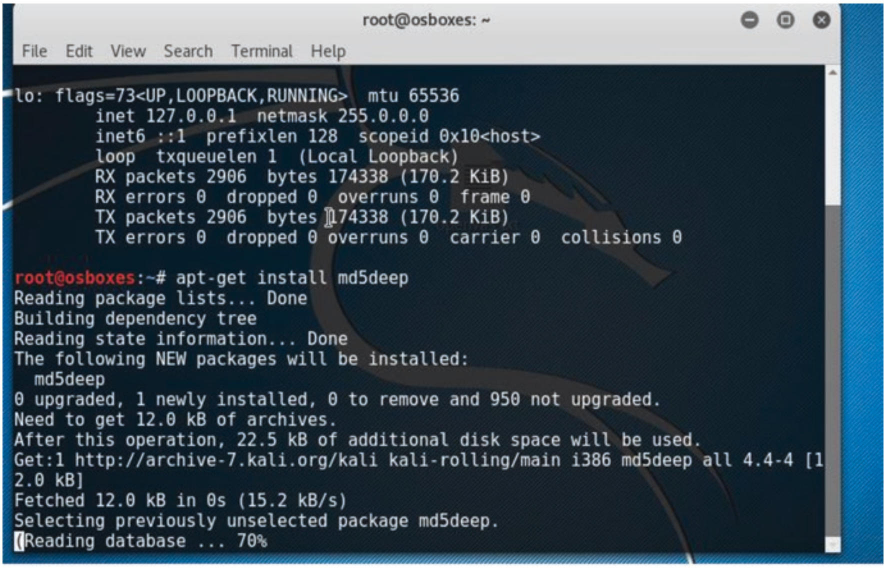
Fig. 11.57 Installing client nsrllookup, 2

Testing of the Malware Server

In the last stage, we will demo the usage of the developed malware analysis system. In this example, I hashed every location on the root drive that contains executables. First, I piped md5deep through nsrllookup to get a file of KNOWN hashes (Fig. 11.59):

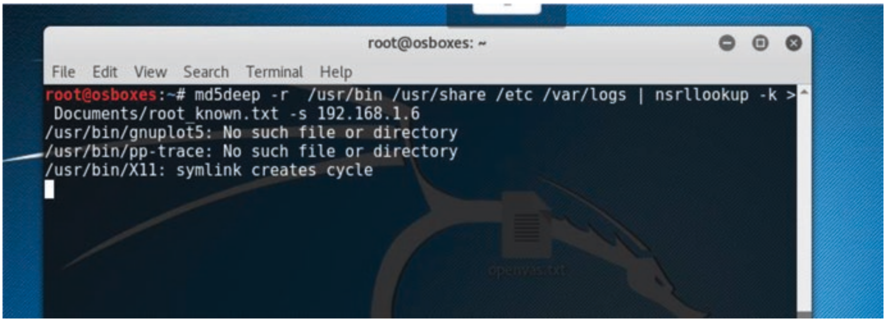
Then, the same thing is accomplished for the unknown hashes (Fig. 11.60):

Md5deep gives a list of hashes as well as the associated filename, but when it is run through nsrllookup the filenames are stripped off. You can make your own



```
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 2906  bytes 174338 (170.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2906  bytes 174338 (170.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@osboxes:~# apt-get install md5deep
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  md5deep
0 upgraded, 1 newly installed, 0 to remove and 950 not upgraded.
Need to get 12.0 kB of archives.
After this operation, 22.5 kB of additional disk space will be used.
Get:1 http://archive-7.kali.org/kali kali-rolling/main i386 md5deep all 4.4-4 [1
2.0 kB]
Fetched 12.0 kB in 0s (15.2 kB/s)
Selecting previously unselected package md5deep.
(Reading database ... 70%
```

Fig. 11.58 Installation of md5deep on the client



```
root@osboxes:~# md5deep -r  /usr/bin /usr/share /etc /var/logs | nsrllookup -k >
 Documents/root_known.txt -s 192.168.1.6
/usr/bin/gnuplot5: No such file or directory
/usr/bin/pp-trace: No such file or directory
/usr/bin/X11: symlink creates cycle
```

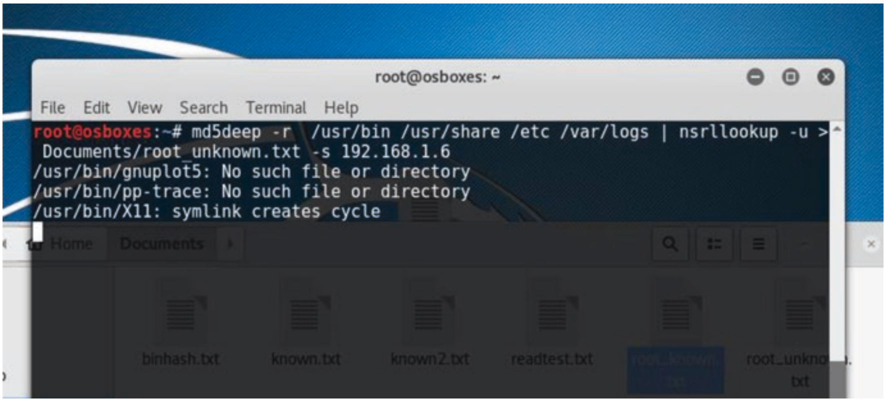
Fig. 11.59 Hashing of user known files

hashlist of the same directories without the need to run them through nsrllookup (Fig. 11.61):

Then, copy and use the script below (Fig. 11.62):

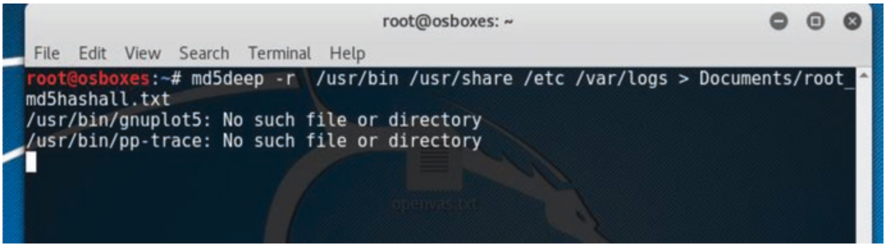
Then, it's just a matter of filtering the unknown, unnamed hashes through my hashlist (Fig. 11.63):

As you can see, the hashes match. There are several duplicate hashes as well, but after a quick inspection it turns out that those are hashes of the exact same file, just a different name (Fig. 11.64).



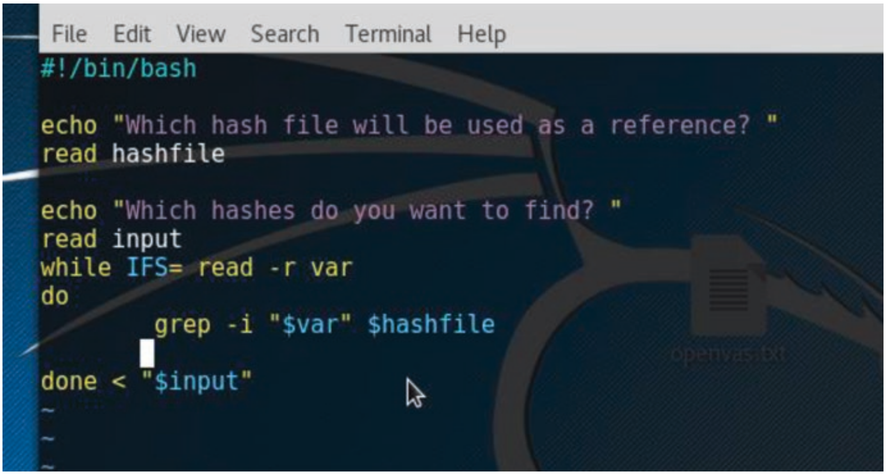
```
root@osboxes:~# md5deep -r  /usr/bin /usr/share /etc /var/logs | nsrllookup -u >
 Documents/root_unknown.txt -s 192.168.1.6
/usr/bin/gnuplot5: No such file or directory
/usr/bin/pp-trace: No such file or directory
/usr/bin/X11: symlink creates cycle
```

Fig. 11.60 Hashing of unknown files



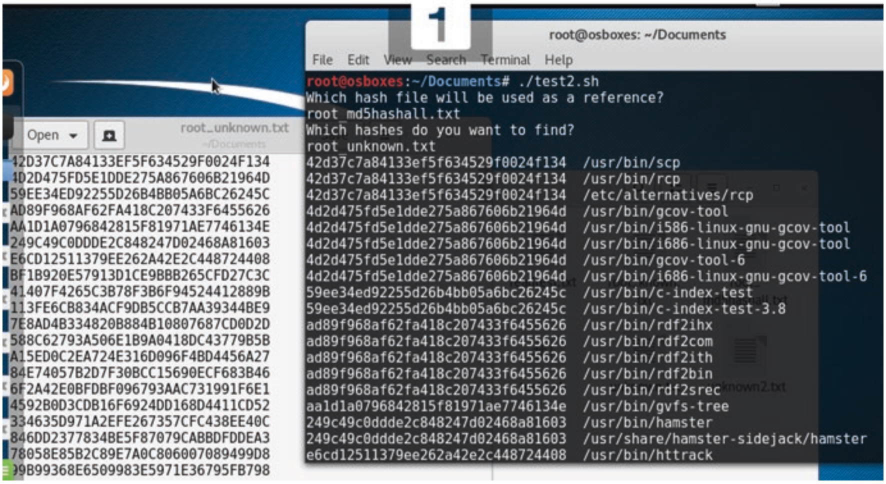
```
root@osboxes:~# md5deep -r  /usr/bin /usr/share /etc /var/logs > Documents/root_
md5hashall.txt
/usr/bin/gnuplot5: No such file or directory
/usr/bin/pp-trace: No such file or directory
```

Fig. 11.61 Creating hashes of known files using md5deep



```
#!/bin/bash

echo "Which hash file will be used as a reference? "
read hashfile

echo "Which hashes do you want to find? "
read input
while IFS= read -r var
do
        grep -i "$var" $hashfile

done < "$input"
~
~
~
```

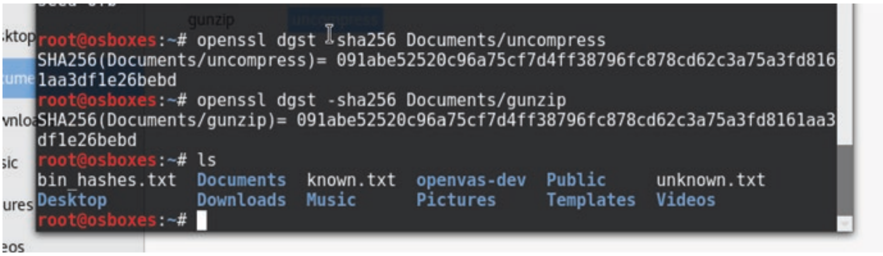
Fig. 11.62 A script to read hashes


Open
root_unknown.txt
~/Documents
root@osboxes: ~/Documents
File Edit View Search Terminal Help

```
42D37C7A84133EF5F634529F0024F134
4D2D475FD5E1DDE275A867606B21964D
59EE34ED92255D26B4BB05A6BC26245C
AD89F968AF62FA418C207433F6455626
AA1D1A0796842815F81971AE7746134E
249C49C0DDDE2C848247D02468A81603
E6CD12511379EE262A42E2C448724408
BF1B920E57913D1CE9BBB265CFD27C3C
41407F4265C3B78F3B6F94524412889B
113FE6CB834ACF9DB5CCB7AA39344BE9
7E8AD4B334820B884B10807687CD0D2D
588C62793A506E1B9A0418DC43779B5B
A15ED0C2EA724E316D096F4BD4456A27
84E74057B2D7F30BCC15690ECF683B46
6F2A42E0BFDBF096793AAC731991F6E1
4592B0D3CDB16F6924DD168D4411CD52
334635D971A2EFE267357CFC438EE40C
846DD2377834BE5F87079CABBDFDDEA3
78058E85B2C89E7A0C806007089499D8
99B99368E6509983E5971E36795FB798
```

```
root@osboxes:~/Documents# ./test2.sh
Which hash file will be used as a reference?
root_md5hashall.txt
Which hashes do you want to find?
root_unknown.txt
42d37c7a84133ef5f634529f0024f134  /usr/bin/scp
42d37c7a84133ef5f634529f0024f134  /usr/bin/rcp
42d37c7a84133ef5f634529f0024f134  /etc/alternatives/rcp
4d2d475fd5e1dde275a867606b21964d  /usr/bin/gcov-tool
4d2d475fd5e1dde275a867606b21964d  /usr/bin/i586-linux-gnu-gcov-tool
4d2d475fd5e1dde275a867606b21964d  /usr/bin/i686-linux-gnu-gcov-tool
4d2d475fd5e1dde275a867606b21964d  /usr/bin/gcov-tool-6
4d2d475fd5e1dde275a867606b21964d  /usr/bin/i686-linux-gnu-gcov-tool-6
59ee34ed92255d26b4bb05a6bc26245c  /usr/bin/c-index-test
59ee34ed92255d26b4bb05a6bc26245c  /usr/bin/c-index-test-3.8
ad89f968af62fa418c207433f6455626  /usr/bin/rdf2ihx
ad89f968af62fa418c207433f6455626  /usr/bin/rdf2com
ad89f968af62fa418c207433f6455626  /usr/bin/rdf2ith
ad89f968af62fa418c207433f6455626  /usr/bin/rdf2bin
ad89f968af62fa418c207433f6455626  /usr/bin/rdf2srec
aa1d1a0796842815f81971ae7746134e  /usr/bin/gvfs-tree
249c49c0ddde2c848247d02468a81603  /usr/bin/hamster
249c49c0ddde2c848247d02468a81603  /usr/share/hamster-sidejack/hamster
e6cd12511379ee262a42e2c448724408  /usr/bin/httrack
```

Fig. 11.63 Hash comparison, 1



```
root@osboxes:~# openssl dgst -sha256 Documents/uncompress
SHA256(Documents/uncompress)= 091abe52520c96a75cf7d4ff38796fc878cd62c3a75a3fd816
1aa3df1e26bebd
root@osboxes:~# openssl dgst -sha256 Documents/gunzip
SHA256(Documents/gunzip)= 091abe52520c96a75cf7d4ff38796fc878cd62c3a75a3fd8161aa3
df1e26bebd
root@osboxes:~# ls
bin_hashes.txt  Documents  known.txt  openvas-dev  Public     unknown.txt
Desktop         Downloads  Music      Pictures     Templates  Videos
root@osboxes:~# 
```

Fig. 11.64 Hash comparison, 2

A0043: Ability to Conduct Forensic Analyses in and for Both Windows and Unix/Linux Environments

1. Demo the usage of ADS (alternate data streams) to hide data/files in Windows NTFS following the steps described in this video: Alternate Data Streams—a hacking and forensics how-to (https://www.youtube.com/watch?v=rF4sIxDIhEk).
2. Use one of the following Windows tools (Syslog, IISLogger, Syslog-ng, Kiwi Syslog Daemon, Microsoft Log Parser Studio, Adaptive Security Analyzer (ASA) Pro, GFI EventsManager, EventReporter, Configuring the Windows Time Service). Pick one tool, install it, and show samples of forensic artifacts that the tool can extract.
3. The document: Law Enforcement and Forensic Examiner's Introduction to Linux, (Linux LEO, https://www.linuxleo.com/) includes an essential reference

for Linux users to understand how to extract forensic artifacts from Linux operating systems. Using your own version of Linux, or a forensic image from those public sources we described earlier, show the output of each command mentioned in the previously mentioned document.

Bibliography

Alsmadi I, Burdwell R, Aleroud A, Wahbeh A, Al-Qudah MA, Al-Omari A (2018) Introduction to information security. In: Practical information security. Springer, New York

Cheng BH et al (2009) Software engineering for self-adaptive systems: a research roadmap. In: Cheng BH, de Lemos R, Giese H, Inverardi P, Magee J (eds) Software engineering for self-adaptive systems. Springer, Berlin, pp 1–26. https://doi.org/10.1007/978-3-642-02161-9_1

Conlan K, Baggili I, Breitinger F (2016) Anti-forensics: furthering digital forensic science through a new extended, granular taxonomy. In: Proceedings of the 16th annual USA digital forensics research conference, DFRWS

Garfinkel S (2007) Anti-forensics: techniques, detection and countermeasure. Calhoun

Hargreaves CJ (2009) Assessing the reliability of digital evidence from live investigations involving encryption. PhD thesis, Cranfield University, Shrivenham

Harrell C (2012) Malware root cause analysis. Journey into Incident Response

Kaser R (2017) WikiLeaks reveals grasshopper, the CIA's Windows hacking tool. https://thenextweb.com/security/2017/04/07/wikileaks-reveals-grasshopper-cias-windows-hacking-tool/

Kent K, Chevalier S, Grance T, Dang H (2006) Guide to integrating forensic techniques into incident response, NIST SP800-86

Kumar M (2017) This CIA tool hacks windows computers silently over the network. https://thehackernews.com/2017/06/windows-hacking-implant.html

Liu, Brown (2006) Bleeding-edge anti-forensics. Infosec world conference & expo, MIS Training Institute

Mandia K, Prosise C (2001) Incident response: investigating computer crime. Osborne/McGraw-Hill, Berkeley, pp 16–17

Noon RK (2001) Forensic engineering investigation, 1st edn. CRC Press, Boca Raton, p 1

Rogers M (2006) Anti-forensics: the coming wave in digital forensics. Accessed 7 Sept 2006

Tech (2009) Forensic analysis on the go, Deployable Forensics Lab makes crime-related investigations mobile, Tech, the newsletter of the first responder technologies program, volume 2, issue 3, March 2009.

Chapter 12
Identity Management

Access controls are considered as important security mechanisms. They usually target (authenticated users: Those users who can legally access subject information system or resource). This indicates that they typically come after an initial stage called (authentication). In authentication, the main goal is to decide whether a subject user, traffic, or request can be authenticated to access the information resource or not. As such authentication security control decision or output is a binary of either, yes (authenticated; pass-in), or no (unauthenticated; block). Access control or authorization is then considered the second stage in this layered security control mechanism. For example, it is important to decide whether subject user has a view/read, modify, execute, etc. type of permission or privilege on subject information resource. In this chapter, we will cover issues related to access controls in operating systems, databases, websites, etc.

In the Internet or web environment, many of the personal/physical types of identification methods are unapplicable or impractical. On the other hand, as e-commerce and the use of the Internet as a business media is continuously growing; identity theft is a very serious issue. Yearly reports on monetary loses due to identity theft are showing that such problems will continue to be serious security problems in the near future.

Identity management systems are information systems in charge of the source of authenticating e-commerce parties to each other. Identity management systems work as authentication, rather than authorization systems. Access control systems represent a second stage security layer after identity management in a layered security system. An access control system that cannot first properly distinguish authenticated from unauthenticated entities will fail in all access control tasks.

I. Alsmadi, *The NICE Cyber Security Framework*,
https://doi.org/10.1007/978-3-030-02360-7_12

Single-Sign-On (SSO)

In addition, to caching users' access profiles on their laptops, smart phones, tablets, etc. websites offer SSO methods to allow users to access all website resources with only one-time access or login request. Even if the website includes different back-end databases and servers, user credentials will be passed on from the first page that requested the credentials to any other system that require those credentials.

Session Time-Out

Users create or start sessions when they login to a website. If the website detects that user has been inactive for some time, the session will be closed and the user has to login again when they come back. There is no specific time that all websites use where after the session will expire. Rather, the session time-out depends on the time the user has been "inactive" since they started the session. Such "inactivity" can be observed from the website when the user is not triggering any object in the websites. If the user is reading some documents in the website without any mouse, keyboard, touch-screen interactions, he/she can be seen as "inactive" by the system.

There are four types of session-based attacks: interception/hijacking, prediction, brute force, and fixation. Session time-out can be one of the effective methods to counter those types of attacks. Other methods include session encryption, long and randomly generating session IDs.

Sessions can be location, rather than time sensitive. For example, your account in anyone of those websites may stay open in your smart phone for a very long time. However, if you tried to access your account from a new machine or phone that you never used before, this will trigger a new session.

Most current websites try to combine more than one authentication method to counter username/password hackings. For example, websites such as: Gmail, Yahoo mail, and Facebook encourage users to include their phone numbers or secondary email accounts. If a user tries to login to an account from a new machine (a machine that was not associated with this user before), the website may send to the phone or the secondary email a verification code. The user is then asked to provide such code before accessing the account.

Kerberos

Kerberos is a ticket-based network authentication protocol that allows nodes communicating over a non-secure network in order to prove their identity to one another. Kerberos is proposed as an alternative to logical or password-based authentications that can be defeated by eavesdropping. In addition, this can be a convenient option where users do not need to remember their usernames and passwords. In Kerberos, information for authentication is sent encrypted between communication parties. Current Kerberos uses the data encryption standard (DES) for encryption.

Digital Certificates

Software companies lost a significant portion of their forecasted profit due to illegal copy, download, and transfer of software between users through the Internet. Digital certificates are proposed to authorize the users' downloaded copies of software applications. When users buy/download new commercial software, they are asked to activate their copies as soon as they are online. Typically, a digital certificate (in a file format) is created for the user machine and is transferred to software company license server. The certificate is embedded with information related to the hardware components of the user host (e.g., disk drivers, CPU, physical memory, network card). Users may need to reactivate their license if they change any of that equipment.

Certificates are also used in identity managements. They are typically used as alternatives to user credentials (i.e., login usernames and passwords). Files with information about communication partners are saved locally. Information in those files is exchanged once the user logs in to the target server.

K0007: Knowledge of Authentication, Authorization, and Access Control Methods

In this section, we will cover the role of access controls in operating systems, DBMSs, and web applications. Those three categories represent the most mature information systems. Access controls exists in other types of information system with similar concepts and different types of implementations based on the maturity and the complexity of the information system. We will also study the two most popular access control architectures or models used to develop access control systems, RBAC and OBAC. In addition to OBAC and RBAC some information systems utilize other models. For example, Mandatory Access Controls: MAC (such as Biba and Bell-LaPadula) where control is centralized and managed by system owners. In contrary with the centrality nature of MAC, Discretionary Access Control (DAC) is uncentralized and users can manage access controls on resources they own. One example of DAC model is NTFS permissions on Windows OS. On NTFS each file and folder has an owner. The owner can use Access Control Lists (ACL) and decide which users or group of users have access to the file or folder. Most today's operating systems use DAC as their main access control model.

Permissions: Permissions are the roles in an access control system to decide system constraints. The three main components in any permission include:

- **Entity**: The user/role or system that is granted/denied the permission.
- **Action**: This can typically include: view/read/write/create/insert/modify, etc.
- **Object**: This is the information system resource that will be the action object or where action is going to be implemented or executed.

- Those are the minimum three elements that access control permission should have. Based on the nature of the access control system, many other optional elements can be included.

Access Controls in Operating and File Systems

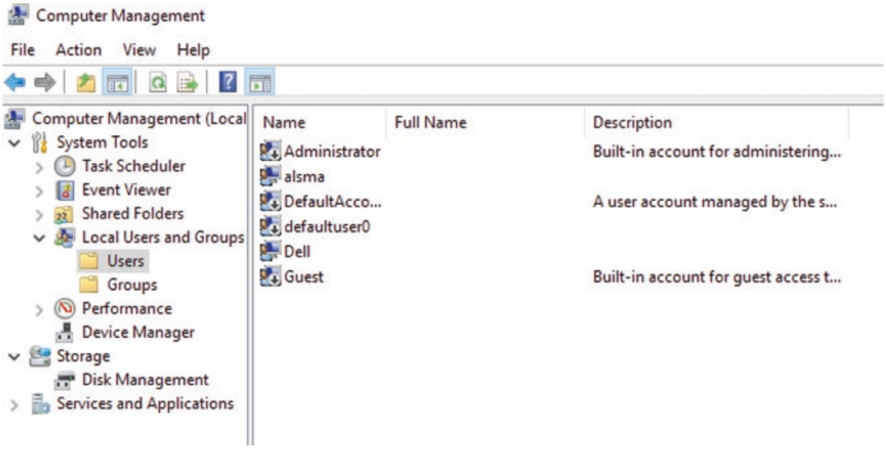
Operating systems evolve and continue to evolve with the continuous progress that we see in both the hardware and software industries. The operating system represents a complex software application that is used to manage all other software applications installed on that same personal computer, server, etc. It is also responsible to control and manage the communication between the three main entities in an information system: users, software applications, and hardware. The basic management modules that most mature operating systems include: memory, processes, file, disk, and network management. The tasks of access control in operating systems exist in different places and using different mechanisms. The basic structure depends on identifying users for the operating system and identifies their access levels on the different OS and system resources. In this sense, they combine access control with authentication. For example, users are prompted when they start an operating system to type a username and password. Such username and password should exist in the directory of authenticated users in the OS with the right password. Usernames and passwords fall in the category of authentication mechanism (something you know). Operating systems can also use other types of mechanisms such as: something you have (e.g., an access card) or something you are (e.g., a fingerprint). System administrators can also decide different levels of constraints on the passwords that users are choosing for their accounts, how often they need to change it, etc. While usernames and roles can be visible to other operating system users, passwords are encrypted. Rather than string the passwords themselves, hash values of those passwords are stored in the (shadow) passwords' folder.

You will learn in skills section how to check locations of accounts/passwords in Linux and Windows. We will also evaluate tools/methods to crack such passwords. Password crackers typically used either dictionary or brute force methods to crack those passwords. To counter dictionary-based password crackers, users should avoid using words from the dictionaries as passwords. To counter brute force methods, systems should block users after a certain number of password attempts.

Users can be distinguished by unique names or they can use (roles) or groups and categories of people. Figure 12.1 shows a snapshot of Windows 10 computer management with built-in and generated user/role accounts.

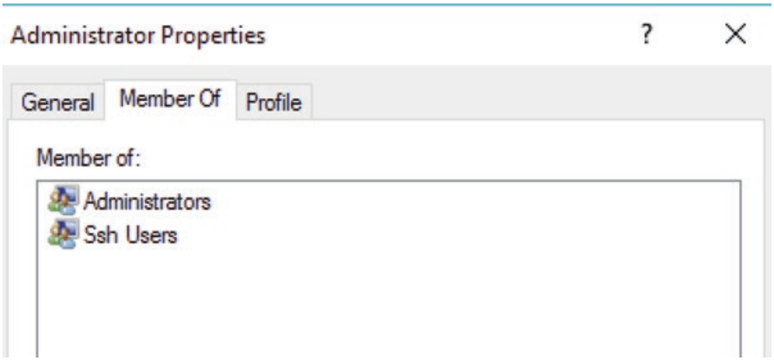
Administrators (local host administrators) have the highest possible permissions in OS resources. A user can be added as an administrator when they are included in the (administrators' group, Fig. 12.2).

In some operating systems, a special user (root) is defined as (a super user). Such uniquely identified user may have special privileges that cannot be granted to other created users or accounts.



Name	Full Name	Description
Administrator		Built-in account for administering...
alsma		
DefaultAcco...		A user account managed by the s...
defaultuser0		
Dell		
Guest		Built-in account for guest access t...

Fig. 12.1 Windows 10: users and groups



Member of:

Administrators
Ssh Users

Fig. 12.2 Adding a user to the administrators' group

There are basic system access control principles that designers/administrators should consider:

- **Principle of Least Privilege**: This means that the default access is nothing for a user. Users will then be granted access to the resources that they need. In this regard, users are encouraged not to use administrator accounts all the time. If their accounts are exposed, with such high privileges, an attacker can significantly hurt the system. Alternatively, they should use normal or power user accounts and only elevate to administrators when they need to.
- **Separation of Duties**: Users should not accumulate responsibilities. They should not have open accounts that can play different roles in different occasions. Such roles should be divided.
- **Principle of Least Knowledge**: Similar to the principle of least privilege, users do not need to see resources that they have no associated tasks with. Intentionally or unintentionally users can abuse their privileges. In some phishing or social engineering types of attacks, those users can be victims and their accounts can be used without their consent knowledge to commit attacks on systems or expose their resources.

Operating systems logically control access through Access Control Lists (ACLs). ACLs are mechanisms or concrete implementations of access control models.

ACLs represent permissions on system objects to decide who can have view/create/modify/execute a system resource or object. In operating system ACLs, an access control entry (ACE) is configured using four parameters:

- A security identifier (SID)
- An access mask
- A flag about operations that can be performed on the object
- A flag to determine inherited permissions of the object

Access Controls in File Systems

File systems represent the management modules of files/folders in operating systems. As such, they inherent most of their access control roles from underlying operating system. File systems differentiate between user generated file and operating system file. Access control decisions on operating system files are usually decided by the operating system access control. They may need special/administrative level permissions before users can change their attributes.

The concept of file/folder ownership evolves when operating systems start to allow more than one user to access/use the same operating system environment and applications. With this evolution also, operating systems now have the ability to audit files history to see who did what and when. Those are usually critical information components to know when conducting a computer or digital investigation.

In Microsoft and Windows operating systems, one of the main goals of moving from FAT to NTFS file systems was to enable features related to file/folder access control auditing. FAT system was initially proposed before the era of operating system multi-users. In comparison with access control in database management systems, access control in file systems focuses on the file level access control. For a database, this will include for example roles on tables in comparison with roles on database schema in database access control.

UNIX file access permissions decide access on files based on three classes of users: Files' owners, members of the group which owns the file and all other users. Each of these three categories of users has permissions for reading, writing, and/or executing.

Access Controls in Database Management Systems

Most of access control models and methods described in operating system section are applicable for database management systems. Access controls restrict which entity can add/delete, modify, or view an information resource. They can restrict access to specific attributes, specific tables, or the whole database.

Unlike primitive flat-files based types of databases (e.g., MS Access) where users have exclusive access control on file-based databases, relational, object-based, or object-oriented databases have more complex access controls that allow many users to have different levels of access controls on the same database. Shared types of databases may have access control-related problems from both authorized and unauthorized users. Security threats such as privilege escalation may cause some authorizations users to illegally have access resources privilege or permission they are not supposed to have.

- **User Views**: Each user in the database can have his/her own unique view of the database. In centralized databases, database administrators are expected to create and manage the different users' views and permissions. In the scope of "Big Data," a user view can be extracted from more than one database or data source and can include metadata customized based on the user preferences. User views can also be distinguished from authority levels. For example, in a University database, faculties, employees, and students may all have "view" access to the students-grades table. However, in addition to seeing or viewing, faculties can create/modify/delete records in their own students' records. Some employees can have view/read/print access on those records. Students have also view/read/print access only on their own records from this, possibly large students-grades table.
- Database Authorization Table: Similar to Access Control Lists (ACLs) in operating systems, database authorization tables contain users and their actions' limits. Table 12.1 shows an example of a database authorization table for one employee or role of employees and a database system.

Table 12.1 indicates that in a large database management system, we typically have a large number or instances of this authorization table.

Table 12.1 A sample database authorization table

Authority level	Orders	Items	Payments
Read	Y	Y	Y
Insert/create	Y	N	Y
Modify	N	N	N
Delete	Y	N	Y

- **SQL GRANT/REVOKE commands**: Database administrators and privileged users can also change access control roles using user-defined procedures. For example, SQL GRANT command can be used to allow user(s) to have certain access levels on certain objects or resources. The general syntax for the command is:

```
GRANT INSERT ON Students to Adam
GRANT SELECT ON Students to students
GRANT INSERT ON Students to Admin WITH GRANT OPTION
```

The addition (WITH GRANT OPTION) allows granted user/role to pass grants to other users/roles.

REVOKE statement is used to remove privileges from a specific user or role. The syntax is very similar to GRANT statement. The following are some examples:

```
REVOKE DELETE ON students FROM Admin
REVOKE ALL ON students FROM Adam
```

- **Data Encryption**: In addition to the different view/access level described earlier, encryption can be used to extend those levels. If an object or a resource is encrypted for a possible user, they may possibly be able to view it, but due to encryption viewed data will not be human readable. In particular, encryption is used to protect data in transit. This became more important recently with the cloud environment, where the whole database can be hosted remotely in the cloud and hence every single query will be transmitted over the Internet.
- **Inference controls**: Research in statistics with information about humans exists in many disciplines. The significant growth of online social networks (OSNs) in particular provides a wealth of information for statistical and social students. One problem associated with research or surveys in those areas is how to handle privacy issues on users' data. The goal of inference controls in data is to modify data to hide personal private information while not impacting data accuracy (Domingo-Ferrer 2009).

Access Controls in Websites and Web Applications

Access control mechanisms in web systems are very critical to the security of those systems. When we survey the types and nature of web systems' attacks, we can see that the majority of those attacks target vulnerabilities/weaknesses in access control mechanisms (OWASP 2018).

While most access control models and methods in websites and web applications are similar to those on operating and database systems, however, they have their own unique access control aspects. For example, real time, current logged-in users, cache, and cookies are all access control web-related aspects that are unique in comparison with operating and database systems. On your own laptop, tablet, or smart phone, you may not need to enter your credentials for your favorite websites (e.g., Facebook, Twitter, Gmail, Amazon), whenever you logged in. Those are cached for you from previous access times. It is important in the web environment to balance between security and user convenience. In real-time environments, user views are not only controlled by access control roles, but also by user history, profile, favorites, etc. For example, when a user logs in to Amazon or e-bay, many of the items they will see (e.g., future possible items to buy) are customized based on the user profile and their buying history.

Most web systems include two main classes of users: Administrators to create and maintain web pages and users or customers to use those pages. Users in most cases are not allowed to create/delete or modify pages. As users, most of the data they communicate will exist in the backend databases.

RBAC (Role-Based Access Control)

Role-based access control (RBAC) is a popular access control model for kernel security control enforcements. Many of the policy-based security systems adopt RBAC when writing and enforcing security roles (NIST 2010 report). The report showed that RBAC adaptation continuously increases between the years 1992 and 2010. The NIST RBAC model is defined in terms of four model components: core, hierarchical, static separation of duty relations, and dynamic separation of duty relations.

RBAC is a policy-based centralized access control system. In terms of centralization, it is similar to Mandatory Access Control (MAC) where access to system resources is controlled by the operating system and system administrators. Unlike centralized control in MAC, Discretionary Access Control (DAC) allows users to control access to their own resources (only). In DAC, resource objects have ACLs associated with them.

Figure 12.3 shows the basic RBAC model. Users should not be given access control permissions based on their own identities. They should be assigned to “logical” roles. Eventually, they will request to access resources based on their assigned roles. Permissions are assigned to roles. Permissions decide actions on objects or resources. This can facilitate security auditing for a large system. Roles in policies should not make references to users, their names, login names, etc. They should make references to the different types of roles employees play in the different information systems. Relations between users, roles, permissions, and objects or resources are not exclusive. Different users can be assigned to the same role. Different roles can be given same permissions (some similar permissions, as if all permissions are identical then maybe those different roles should be combined).

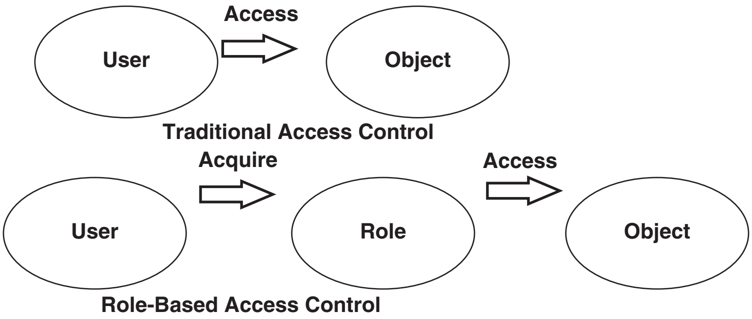


Fig. 12.3 Basic RBAC model

Operations or sessions include activities or requests performed by users. Policies or roles in the access control system can decide whether to authorize those operations or not. Objects refer to system resources. The granularity level of such objects can vary significantly. For example, the whole DMBS can be seen as an object in one role. In another role, a table, a field, a record, or even a cell of a database in that DBMS can be the object in the role request.

As the term implies (roles), RBAC consider the roles of users or entities as the basis to create policies. RBAC systems include a set of (policies). A policy can be a high-level (human nature) statement. For example, the following can represent a security policy (users of the company network should not be allowed to access websites with improper contents). The following can be stated about this policy:

- This policy can be easily understood by humans.
- This policy is very abstract in terms of network or security tools. In other words, no existing security tool (e.g., a firewall, a router, a Virtual Private Network (VPN), an Intrusion Detection or Protection System: IDS/IPS) can take this policy and enforce it (without extra tools/programs/humans to do the translation between this high-level policy and low-level security roles).
- Typically, such high-level policy can be enforced using a set of low-level roles that can be understood and enforced by security control systems.

In RBAC users/roles can't make changes on policies/roles that impact them. RBAC policies are usually created and managed by system administrators.

Users are different from roles in RBAC. Typically, roles are created and then each user can be assigned a role. For example, in a University system, we can define roles such as: Employee, Faculty, Student, System administrator, and Manager. Users can also play more than one role simultaneously or in different times, environments, functions, etc. For example, in a University system some employees can be students as well. This means that the RBAC system should be able to differentiate the current role they are playing while using or requesting a resource and hence assign them to the right role.

RBAC is popular in network-based information or distributed systems. This is largely as policies in network or security components are written as roles.

For example, policies in firewalls (software and hardware), routers, switches, IDS/IPS, etc. are all written as roles.

Roles in RBAC can also have hierarchies where children roles can inherit permissions from parent roles. For example, in a network domain controller, domain controller administrators have the highest, or root permission level. This means that they can access resources in lower levels (e.g., host computers) without the need to be host administrators, power users or even users in those local hosts. Their root level role implies having an administrator privilege in all network or system resources.

OBAC (Object-Based Access Control)

With the evolution of object-oriented paradigms in software design, programming and database management systems, OBAC evolves recently. In OBAC, objects rather than roles are the central entity in the access control systems. In OBAC, not only users, roles, or entities are objects, but also resources and decisions themselves can be objects (to have their own attributes and actions).

Attribute-based access control (ABAC) falls in the same category of OBAC in trying to design roles with finer details. In ABAC, roles include who (user-role) is going to do what (permission), on what (object or resources). However, each one of those entities (i.e., users, roles, permissions, and objects) can have attributes and values for those attributes. Hence, the final operation can be denied or permitted based on values of some attributes. For example, the policy role (Employees can use company Internet services within work-time or weekdays) has the same users, roles, permissions, and objects. However, while all those are identical, in one instance or operation, such employee will be permitted (if it's Monday) or will be denied (if it's Sunday). Similarly, one of the main drivers to use OBAC as a replacement to ABAC is that in OBAC we can make policy roles with much finer details in comparison with RBAC. Those roles can also be dynamic, rather than static. Attribute values for different entities can change with time, or some other environmental factors. Policy enforcement system is expected to be more complex to be able to evaluate the attribute values of all entities related to the operation or request.

Figure 12.4 shows OBAC/ABAC reference architecture. Major components are:

- Policy Enforcement Point (PEP): This module is in charge of enforcing the final (action decision) for an access control request. It will receive the request and context from the application. It will also receive final decision from Policy Decision Point (PDP).
- Policy Decision Point (PDP): This module represents the decision engine in the access control system. This is why it communicates with most components. Actual policies or instances of policies exist in policy store. Network administrators can have access to this store in order to create/delete/modify policies.
- Policy Information Points: In addition to policies, system should also know the different types of entities (i.e., users, roles, entities, objects, permissions). All those should exist in PIP. Each one of those can have its attributes. Attribute values can

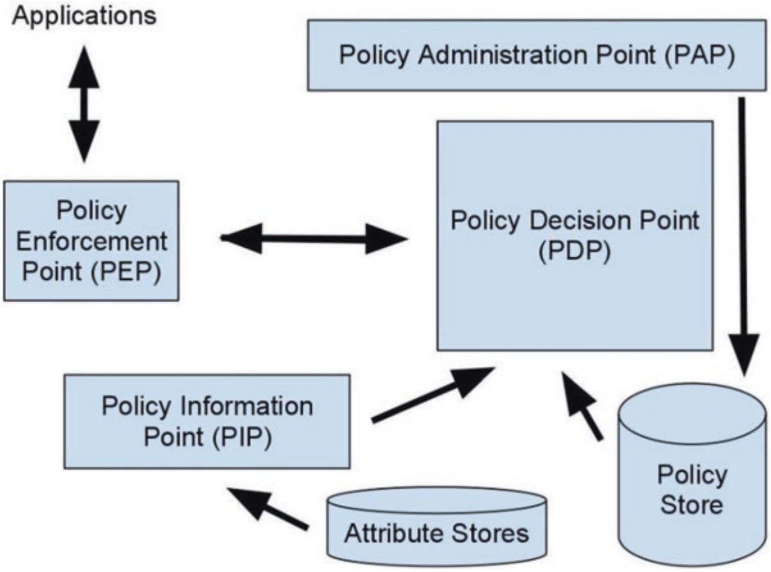

Applications
Policy Administration Point (PAP)
Policy Enforcement Point (PEP)
Policy Decision Point (PDP)
Policy Information Point (PIP)
Policy Store
Attribute Stores

Fig. 12.4 OBAC/ABAC reference architecture

be extracted in real time from the application, environment, etc. Each operation or request can make queries to read a different set of entities or entity attributes.

- Policy Administration Point (PAP): For general access control system control and management issues.

As the most recent models of access control, in skills' section, you will be asked to evaluate a concrete OBAC/ABAC access control implementation.

There are some challenges that exist in all access control systems such as the nature of relations between different roles. For example, in roles' conflicts' cases, different roles in an access control system may contradict with each other in terms of actions or decisions. Final decision made on a request may not what system administrators are expecting. Roles can also be contained within other roles where inner roles are hidden and can never be enforced in any permission request. In such case, those roles, while they exist, they are dead or useless.

K0033: Knowledge of Host/Network Access Control Mechanisms (e.g., Access Control List)

Access Control in Distributed and Operating Systems

Access Control Lists (ACL) in the most popular Network Operating Systems (NOS), NFS are inherited from UNIX-based operating systems. In some NOSs (e.g., Andrew file system, AFS), ACLs are based on directories rather than files.

As an alternative to ACLs, some NOSs (e.g., WebFS) use authorization certificates or a hybrid scheme of both access control implementations. Certificates are created and authorized by third parties; Certificate Authorities (CA).

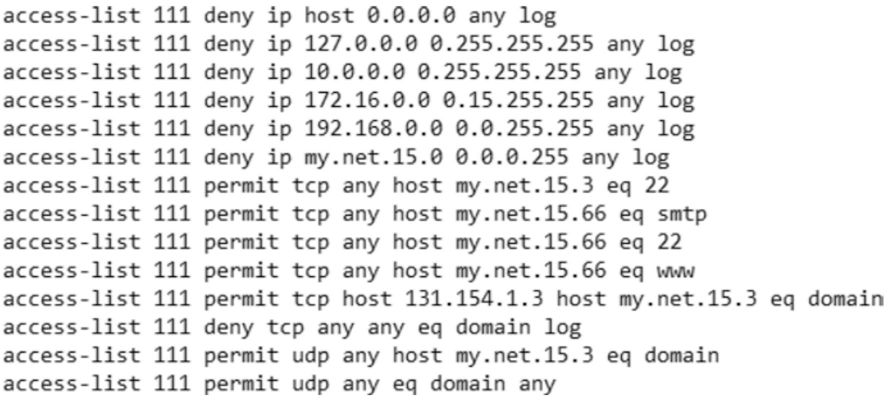
Network switches and routers include their own operating systems. Part of their operating systems, they also include access control systems or modules. In addition to access controls related to users, NOS may include access controls for other systems, applications, and even traffic. Host-based access control uses host IP, DNS, and possibly MAC addresses. Several network-based attacks related to those attributes are possible. Examples of those attacks include: IP/MAC/ARP spoofing, DNS pharming, etc. Figure 12.5 shows a sample ACL from a Cisco router.

More recent software-controlled NOSs such as Software Defined Networking (SDN) Controllers aim at giving users and their applications a fine-grained level of access control on traffic from and to the network (For more details, see OpenDayLight project or platform at: https://www.opendaylight.org).

One use case which is related to access control and mentioned in SDN projects is related to wireless AAA (Authentication, Access control, and Accountability). In our home wireless Internet, those three are typically combined in one. This is since current methods assume one user account and management systems for the three functions (Alsmadi and Xu 2015).

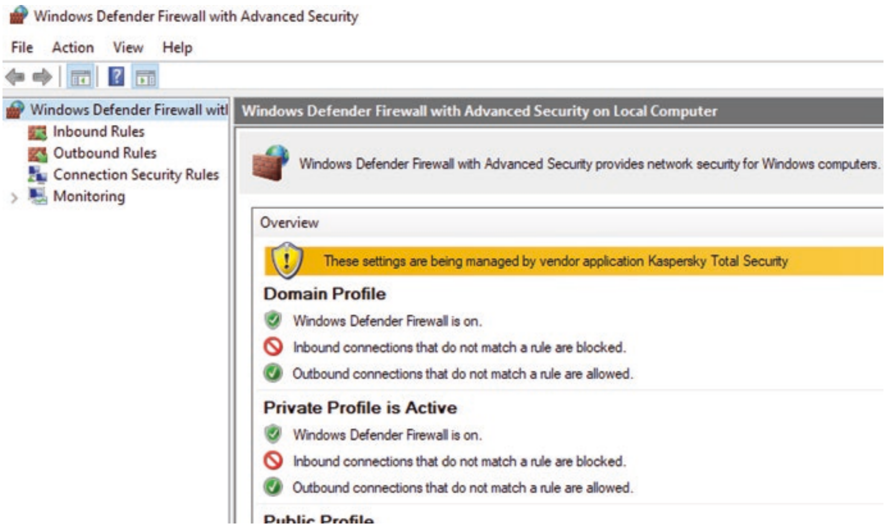
Access Controls in Firewalls

Firewalls are one of the most popular security controls in information systems. They are distinguished as lightweight actionable security controls that make decisions to block traffic based on a limited number of attributes in OSI Layers two and three (L2–L3 firewalls). However, this is the case in what can be referred to as “classical



```
access-list 111 deny ip host 0.0.0.0 any log
access-list 111 deny ip 127.0.0.0 0.255.255.255 any log
access-list 111 deny ip 10.0.0.0 0.255.255.255 any log
access-list 111 deny ip 172.16.0.0 0.15.255.255 any log
access-list 111 deny ip 192.168.0.0 0.0.255.255 any log
access-list 111 deny ip my.net.15.0 0.0.0.255 any log
access-list 111 permit tcp any host my.net.15.3 eq 22
access-list 111 permit tcp any host my.net.15.66 eq smtp
access-list 111 permit tcp any host my.net.15.66 eq 22
access-list 111 permit tcp any host my.net.15.66 eq www
access-list 111 permit tcp host 131.154.1.3 host my.net.15.3 eq domain
access-list 111 deny tcp any any eq domain log
access-list 111 permit udp any host my.net.15.3 eq domain
access-list 111 permit udp any eq domain any
```

Fig. 12.5 A sample router ACL


Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Defender Firewall with Advanced Security on Local Computer
Overview

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

These settings are being managed by vendor application Kaspersky Total Security

Domain Profile

Windows Defender Firewall is on.

Inbound connections that do not match a rule are blocked.

Outbound connections that do not match a rule are allowed.

Private Profile is Active

Windows Defender Firewall is on.

Inbound connections that do not match a rule are blocked.

Outbound connections that do not match a rule are allowed.

Public Profile

Fig. 12.6 Windows firewall settings

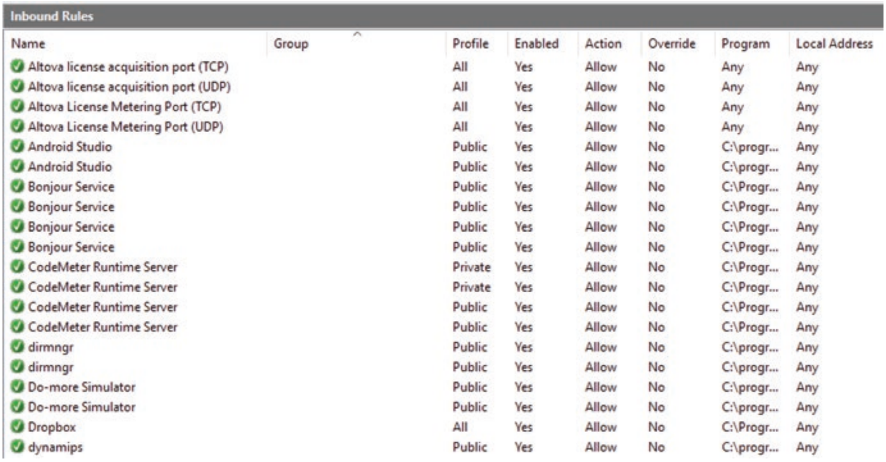
firewalls" as a new generation of firewalls operate on the application layer or layer 7 in OSI. Figure 12.6 shows a sample GUI from Windows firewall settings.

Rules in firewalls are generally classified under two main categories:

- Inbound rules: Rules that apply on incoming traffic. This is very important as our firewall main goal is to protect our system from harmful incoming traffic.
- Outbound rules: Rules that control traffic going out from our system or network. While this category is less important, in general, that the first category for our system security, however, from a liability perspective, it is important to make sure that our system or network is not harming other systems or is used, without our consensus knowledge to attack others.

Figure 12.7 shows a sample of Windows firewall inbound rules and the type of attributes included such as:

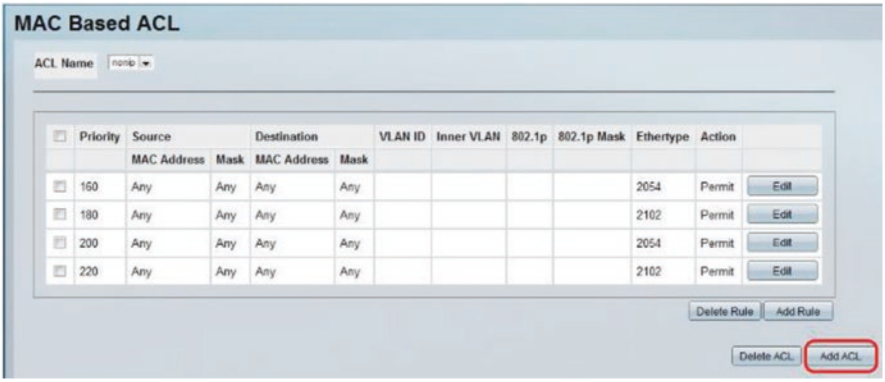
- Profile: All, public, domain, private
- Enabled: Yes or No (i.e., a rule may exist but may not be active)
- Action: Allow or deny
- Override: Yes or No
- Program (i.e., application using or requesting such rule)
- Local address



Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address
Altova license acquisition port (TCP)		All	Yes	Allow	No	Any	Any
Altova license acquisition port (UDP)		All	Yes	Allow	No	Any	Any
Altova License Metering Port (TCP)		All	Yes	Allow	No	Any	Any
Altova License Metering Port (UDP)		All	Yes	Allow	No	Any	Any
Android Studio		Public	Yes	Allow	No	C:\progr...	Any
Android Studio		Public	Yes	Allow	No	C:\progr...	Any
Bonjour Service		Public	Yes	Allow	No	C:\Progr...	Any
Bonjour Service		Public	Yes	Allow	No	C:\Progr...	Any
Bonjour Service		Public	Yes	Allow	No	C:\Progr...	Any
Bonjour Service		Public	Yes	Allow	No	C:\Progr...	Any
CodeMeter Runtime Server		Private	Yes	Allow	No	C:\Progr...	Any
CodeMeter Runtime Server		Private	Yes	Allow	No	C:\Progr...	Any
CodeMeter Runtime Server		Public	Yes	Allow	No	C:\Progr...	Any
CodeMeter Runtime Server		Public	Yes	Allow	No	C:\Progr...	Any
dirmngr		Public	Yes	Allow	No	C:\progr...	Any
dirmngr		Public	Yes	Allow	No	C:\progr...	Any
Do-more Simulator		Public	Yes	Allow	No	C:\progr...	Any
Do-more Simulator		Public	Yes	Allow	No	C:\progr...	Any
Dropbox		All	Yes	Allow	No	C:\Progr...	Any
dynamips		Public	Yes	Allow	No	C:\progr...	Any

Fig. 12.7 A sample of Windows firewall inbound rules



MAC Based ACL

ACL Name: nonb

☐	Priority	Source		Destination		VLAN ID	Inner VLAN	802.1p	802.1p Mask	Ethertype	Action	
		MAC Address	Mask	MAC Address	Mask							
☐	160	Any	Any	Any	Any					2054	Permit	Edit
☐	180	Any	Any	Any	Any					2102	Permit	Edit
☐	200	Any	Any	Any	Any					2054	Permit	Edit
☐	220	Any	Any	Any	Any					2102	Permit	Edit

Fig. 12.8 MAC-based ACL, Cisco Knowledge Base 2018

Access Controls in Switches

Switches are network hardware components that are used to connect local computers (i.e., Local Area Networks, LAN). Switches transfer or switch traffic from source to destination based on Layer 2 (i.e., MAC) information. As such, Access Control List (ACL) information in switches is accomplished based on MACs, Fig. 12.8, (Cisco Knowledge Base 2018).

VLAN ID attribute allows the creation of virtual LANs that redefine physical networks logically, rather than physically (i.e., based on the physical switches and topology). This concept is one of the key concept enablers in cloud computing and network virtualization.

Access Controls in Routers

Routers are very popular and key network components that connect different networks with each other. The whole Internet is about a large number of routers as intersections connecting the different computing machines, servers, networks, etc. with each other.

While routers' main function is to transfer or route traffic from one location to another, deciding on the best route to do that, however they can also perform firewalling or access control functions. As such, many routers are sold with built-in firewalls. Similar to firewalls they will have rules for inbound and outbound traffic. Similarly, they can filter traffic-based inbound or outbound port numbers, IP addresses (V4 and V6) and MAC addresses (Fig. 12.9).

Access Controls in IDS/IPS

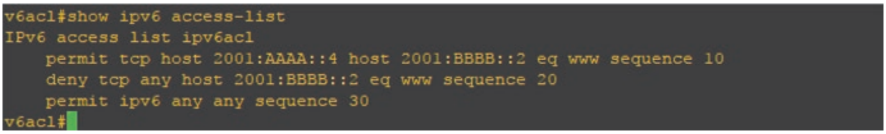
Intrusion Detection and Protection Systems (IDS/IPS) are intelligence security controls that include more details in their ACLs to permit or deny traffic. This is in comparison with the basic 6–10 attributes typically exist in classical firewalls and switches (i.e., inbound and outbound port numbers, IP and MAC addresses, protocol).

In terms of actions, IDS/IPS takes more actions than just permit or deny. For example, other actions such as:

- Log: Record the traffic (e.g., without dropping it)
- Alert: Send an alarm message if such traffic pattern occurs
- Drop: Make Iptables drop the packet and log the packet details
- Reject: In addition to drop actions, send a TCP reset if TCP protocol or ICMP unreachable if UDP

Figure 12.10 shows a simple example of an IDS/IPS rule with all attributes described.

Unlike classical firewalls, IDS/IPS can drop or deny traffic based on application layer information such as a certain content in that traffic, Fig. 12.11.



```
v6acl#show ipv6 access-list
IPv6 access list ipv6acl
    permit tcp host 2001:AAAA::4 host 2001:BBBB::2 eq www sequence 10
    deny tcp any host 2001:BBBB::2 eq www sequence 20
    permit ipv6 any any sequence 30
v6acl#
```

Fig. 12.9 An ACL example in routers

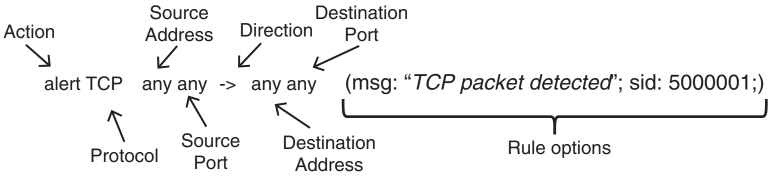
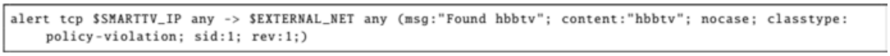


Fig. 12.10 A simple example of IDS/IPS rule



```
alert tcp $SMARTTV_IP any -> $EXTERNAL_NET any (msg:"Found hbbtv"; content:"hbbtv"; nocase; classtype:
    policy-violation; sid:1; rev:1;)
```

Fig. 12.11 IDS/IPS rule with content-based filtering (Ghiglieri 2017)

Bibliography

Alsmadi I, Xu D (2015) Security of software defined networks: a survey. Comput Secur 53:79–108

Cisco Knowledge Base (2018) Configuration of MAC based access control lists on ESW500 series switches. Article ID: 503. Cisco. https://sbkb.cisco.com/CiscoSB/GetArticle.aspx?docid=cbf8f6291d654ff1a840b0726680815c_MAC_Based_ACL_On_ESW_500_Series_Devices.xml&pid=2&converted=0

Domingo-Ferrer J (2009) Inference control in statistical databases. In: Encyclopedia of database systems. Springer, New York, pp 1472–1476

Ghiglieri M (2017) Smart TV privacy risks and protection measures. Ph.D. Thesis, Technische Universität, Darmstadt

NIST 2010. A report on: 2010 economic analysis of role-based access control. http://csrc.nist.gov/groups/SNS/rbac/documents/20101219_RBAC2_Final_Report.pdf

OWASP (2018) https://www.owasp.org/index.php/Access_Control_Cheat_Sheet#tab=Other_Cheatsheets

Chapter 13
Incident Response

A security incident is an insider or adversary event that can impact organization assets and compromise their security goals (e.g., confidentiality, integrity, availability, access control).

A security incident is an event that indicates that an organization's systems or data may have been compromised or that the security measures to protect them have failed. This definition shows two criteria in which one of them is enough to trigger the occurrence of a security incident:

- An indicator of a security breach or compromise.
- An indicator of a malfunction of a security control. Such malfunction detection can be a result of the first indicator or some other events (e.g., through testing or auditing).

As response in real-time security incident will be very traumatic, organizations form and train special incident response team to handle proper real-time response.

K0041: Knowledge of Incident Categories, Incident Responses, and Timelines for Responses

For a security incident, the following information includes the minimum to collect (Campbell 2003, NIST 2012):

- The attacker or attack origin
- The tool they have used
- The vulnerability exploited
- The exploitation actions performed
- The intended target(s)
- The attack consequences
- The attack objective

I. Alsmadi, *The NICE Cyber Security Framework*,
https://doi.org/10.1007/978-3-030-02360-7_13

- Incident Category Type (e.g., CAT 1, CAT 2)
- Incident date and time, including time zone
- Source IP, port, and protocol
- Destination IP, port, and protocol
- Operating system, including version, patches, etc.
- System function (e.g., DNS/web server, workstation)

Security incidents can be divided into different categories from different perspectives. The goal is to cluster the incidents into different groups based on common attributes. We will cover some of the popular references in security incident categories.

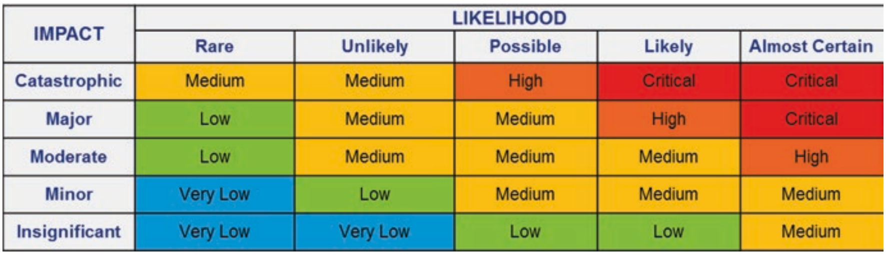
NIST Special publication 800-61 specifies the seven categories shown in Table 13.1 below.

Some references use the term "attack vectors" instead of incident categories. For example, OWASP lists the following attack vectors:

- Abuse of Functionality
- Automated Threat
- Data Structure Attacks
- Embedded Malicious Code
- Exploitation of Authentication
- Injection
- Path Traversal Attack

Table 13.1 NIST 7 security incident categories (NIST 2012)

CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises, and approved activity testing of internal/external network defenses or responses
CAT 1	Unauthorized Access	In this category, an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource
CAT 2	Denial of Service (DoS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim or participating in the DoS
CAT 3	Malicious Code	Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been successfully quarantined by antivirus (AV) software
CAT 4	Improper Usage	A person violates acceptable computing use policies
CAT 5	Scans/Probes/Attempted Access	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service
CAT 6	Investigation	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review



IMPACT	LIKELIHOOD				
	Rare	Unlikely	Possible	Likely	Almost Certain
Catastrophic	Medium	Medium	High	Critical	Critical
Major	Low	Medium	Medium	High	Critical
Moderate	Low	Medium	Medium	Medium	High
Minor	Very Low	Low	Medium	Medium	Medium
Insignificant	Very Low	Very Low	Low	Low	Medium

Fig. 13.1 Security Incidents' classification based on severity, InfoSec Nirvana 2015

- Probabilistic Techniques
- Protocol Manipulation
- Resource Depletion
- Resource Manipulation
- Sniffing Attacks
- Spoofing

NIST 2012 publication lists the following attack vectors based on the source of the attack: External/removable media, attrition, web, email, impersonation, improper usage, loss or theft of equipment, and others.

Incidents can also be categorized based on the severity of the incident (Fig. 13.1, (InfoSec Nirvana 2015)). This classification considers two factors: The probability or likelihood that the incident will occur (or occur again), and the impact on systems, assets, etc.

K0042: Knowledge of Incident Response and Handling Methodologies

Incident response is a structured approach that addresses and manages the outcome of a security incident. The goal is to handle the situation in a way that limits damage and reduces recovery expenses.

Typically organizations assign a special team: computer security incident response team (CSIRT) to plan and conduct incident responses that should comply with the organization's incident response plan (IRP).

Typically, incident response includes six stages (Fig. 13.2):

- Preparation stage
- Identification stage
- Classification stage
- Traceback
- Reaction
- Postmortem

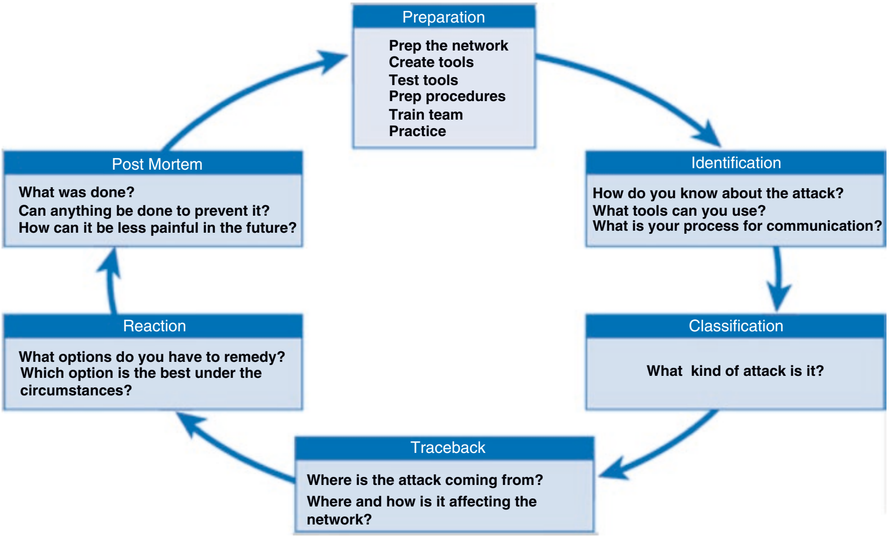

Preparation
Prep the network
Create tools
Test tools
Prep procedures
Train team
Practice
Identification
How do you know about the attack?
What tools can you use?
What is your process for communication?
Classification
What kind of attack is it?
Traceback
Where is the attack coming from?
Where and how is it affecting the network?
Reaction
What options do you have to remedy?
Which option is the best under the circumstances?
Post Mortem
What was done?
Can anything be done to prevent it?
How can it be less painful in the future?

Fig. 13.2 Incident response stages (Trivedi 2007)

In an incident lifecycle, Fig. 13.3, (Bejtlich 2010) incident response focuses on the following short-term activities:

- Incident Handlers: Security experts to establish incident knowledge-base. Once an incident is discovered, the organization incident handlers started their response to the intrusion.

Incident handling covers the logistics, communications, coordination, and planning functions needed in order to resolve an incident in a professional and efficient manner. Basic required in incident handling in addition to technical security-related skills: communication and project management skills.

The incident handling process includes six phases: preparation, identification, eradication, recovery and lessons learned (follow-up).

- Event Analysts: In incident response, event analysis is necessary in order to identify weaknesses and whether/what corrective actions are required. Event analysis includes recreating, analyzing, and evaluating events that have occurred during the incident.

Incident Analysis: Cyber incident analysis includes activities to find out what happened in the incident. The purpose of this analysis is to understand the technical details, root cause(s), and potential impact of the incident. The main objectives of this phase include (I-Assure 2018):

- Ensuring the accuracy of incident reports.
- Characterizing and communicating the potential impacts of the incident.

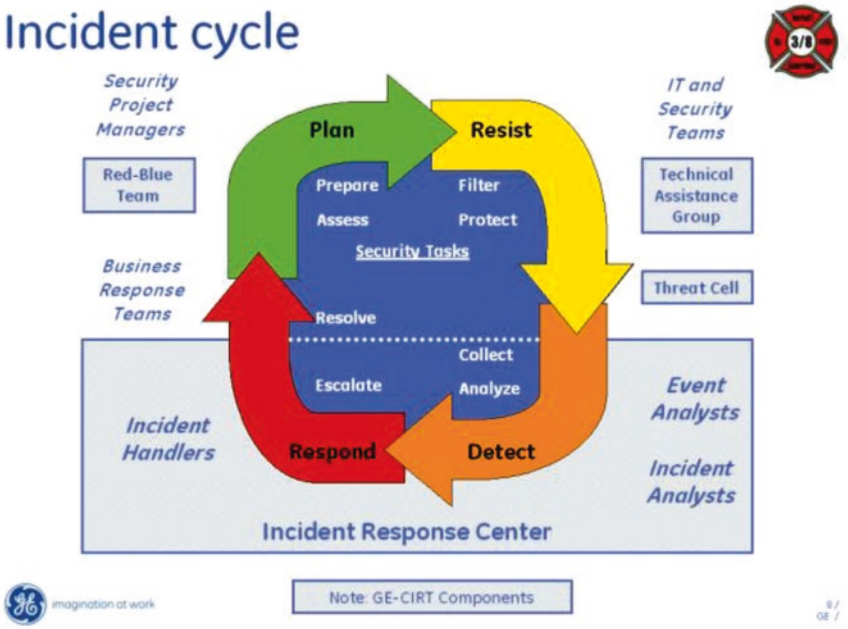


Fig. 13.3 Incident cycle and incident response, Bejtlich 2010

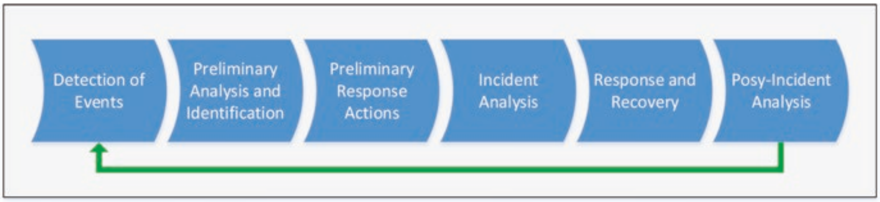


Fig. 13.4 DoD incident handling lifecycle (I-Assure 2018)

- Capturing the methods used in the attack and the security controls targeted.
- Researching actions that can be taken to respond to and eradicate the incident or similar ones.
- Understanding patterns of activity to characterize the threat and direct protective and defensive strategies.
- Identifying the root cause(s) of the incident.

To assist in incident analysis, handlers may want to duplicate an aspect of an incident that was not adequately recorded. For example, a user visited a malicious website, which then compromised the workstation.

DoD described cyber incident handling process of six steps shown in Fig. 13.4 (I-Assure 2018).

K0145: Knowledge of Security Event Correlation Tools

Security Information and Event Management (SIEM)

SIEM is an umbrella for security software tools including log management systems, security log, event management, security information management and security event correlation.

SIEM tools main functions include:

- Log collection and analysis
- Normalization: Collect logs and transfer them into a standard format
- Notifications and alerts—Security threats' notification
- Security incident detection
- Incident response workflow

Mehta 2014 described top six use cases for SIEM tools:

- Detection of Possible Brute Force Attack
- Detection of Insider Threat
- Application Defense Check
- Suspicious Behavior of Log Source
- Malware Check
- Detection of Anomalous Ports, Services and Unpatched Hosts/Network Devices

Examples of popular SIEM tools and vendors:

- LogRhythm: www.logrhythm.com
- McAfee (Nitro Security): https://www.mcafee.com/enterprise/en-us/products/siem-products.html
- IBM (QRadar): www.ibm.com/QRadar/Analytics
- Splunk: https://www.splunk.com
- Rapid7: www.rapid7.com
- AlienVault: www.alienvault.com/siem
- Micro Focus ArcSight: https://software.microfocus.com

Event correlation tools aggregates and analyzes log data from network applications, systems, and devices, making it possible to discover security threats and malicious patterns of behaviors. The most common data sources include network IDS/IPS, vulnerability assessment tool, and servers. Figure 13.5 shows typical security correlation tools' major tasks: Collection of logs, analysis and reporting.

Correlation and root-cause analysis support IT performance monitoring and can help IT departments to determine the underlying cause of a problem and resolve it quickly to minimize business impacts.

Some of the benefits in using event correlation tools include (Zhang 2017):

- Real-time threat visibility.
- Vigilance of network safety.

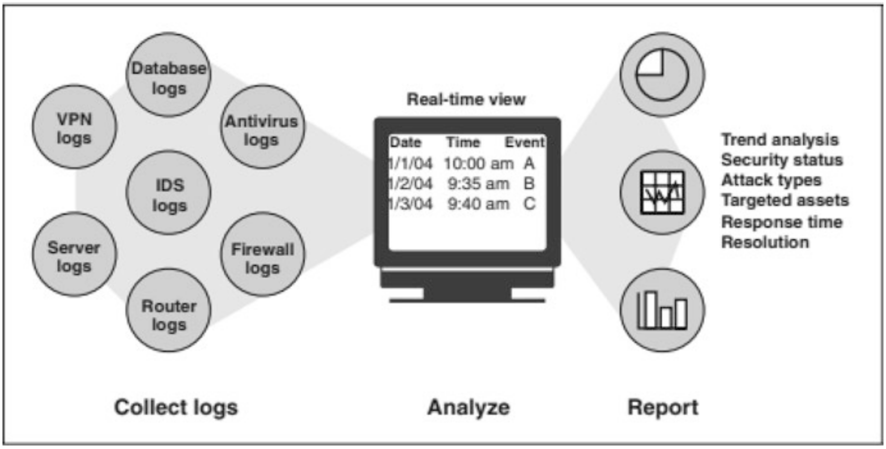


Fig. 13.5 Correlation tools' major tasks (GAO 2004)

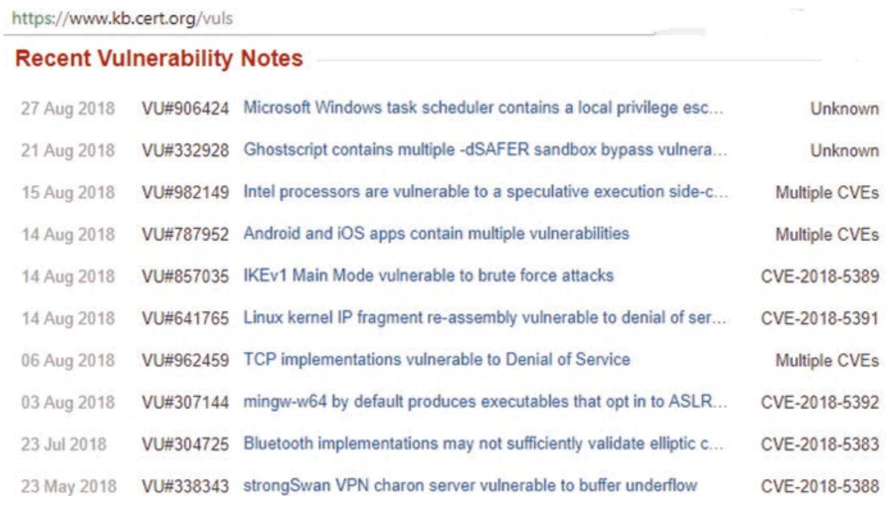
- Continuous compliance reports.
- Reduces operational costs.
- Improves time management.

K0150: Knowledge of Enterprise Incident Response Program, Roles, and Responsibilities

National Computer Security Incident Response Programs

In the US, there are several reporting organizations that enable users/vendors to keep track of reported vulnerabilities and available patches in vendor-supplied software. Following is a list of most popular ones:

- US-CERT, https://www.us-cert.gov
  Part of DHS National Protection and Programs Directorate (NPPD), United States Computer Emergency Readiness Team (US-CERT) main responsibilities include analyzing and mitigating cyber threats, vulnerabilities, disseminating cyber threat warning information, and synchronizing incident response activities. The US-CERT team members aid with incident handling aspects that are consistent with activities defined in the NIST 800-61 incident response lifecycle: Incident triage, coordination and resolution. Figure 13.6 shows an example of "recent vulnerability notes" from CERT vulnerability database.
  In addition to the information shown above, vulnerabilities include a Common Vulnerability Scoring System (CVSS) score (https://nvd.nist.gov/vuln-metrics/cvss) to scale the vulnerability into a scale of three levels in CVSS 2.0 and five levels in CVSS 3.0 is also included in CERT, Fig. 13.7.

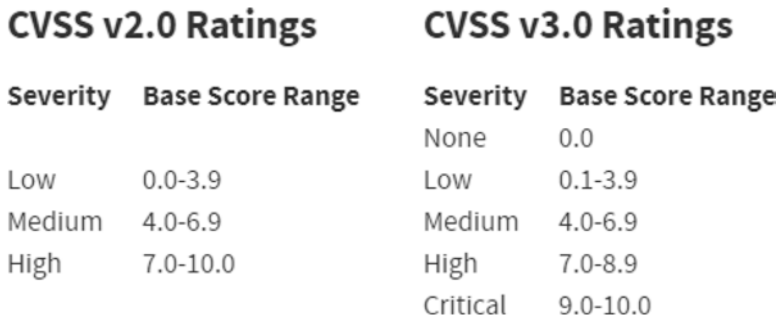


https://www.kb.cert.org/vuls

Recent Vulnerability Notes

27 Aug 2018	VU#906424	Microsoft Windows task scheduler contains a local privilege esc...	Unknown
21 Aug 2018	VU#332928	Ghostscript contains multiple -dSAFER sandbox bypass vulnera...	Unknown
15 Aug 2018	VU#982149	Intel processors are vulnerable to a speculative execution side-c...	Multiple CVEs
14 Aug 2018	VU#787952	Android and iOS apps contain multiple vulnerabilities	Multiple CVEs
14 Aug 2018	VU#857035	IKEv1 Main Mode vulnerable to brute force attacks	CVE-2018-5389
14 Aug 2018	VU#641765	Linux kernel IP fragment re-assembly vulnerable to denial of ser...	CVE-2018-5391
06 Aug 2018	VU#962459	TCP implementations vulnerable to Denial of Service	Multiple CVEs
03 Aug 2018	VU#307144	mingw-w64 by default produces executables that opt in to ASLR...	CVE-2018-5392
23 Jul 2018	VU#304725	Bluetooth implementations may not sufficiently validate elliptic c...	CVE-2018-5383
23 May 2018	VU#338343	strongSwan VPN charon server vulnerable to buffer underflow	CVE-2018-5388

Fig. 13.6 An example of "recent vulnerability notes" from CERT vulnerability database

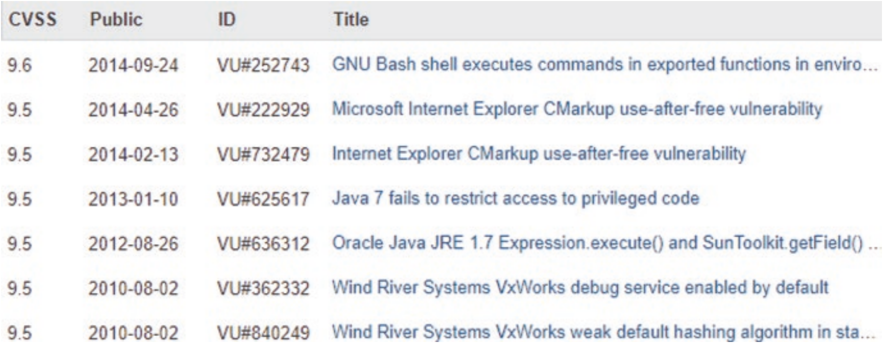


CVSS v2.0 Ratings		CVSS v3.0 Ratings	
Severity	Base Score Range	Severity	Base Score Range
		None	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

Fig. 13.7 CVSS 2 and three scoring levels (https://nvd.nist.gov/vuln-metrics/cvss)

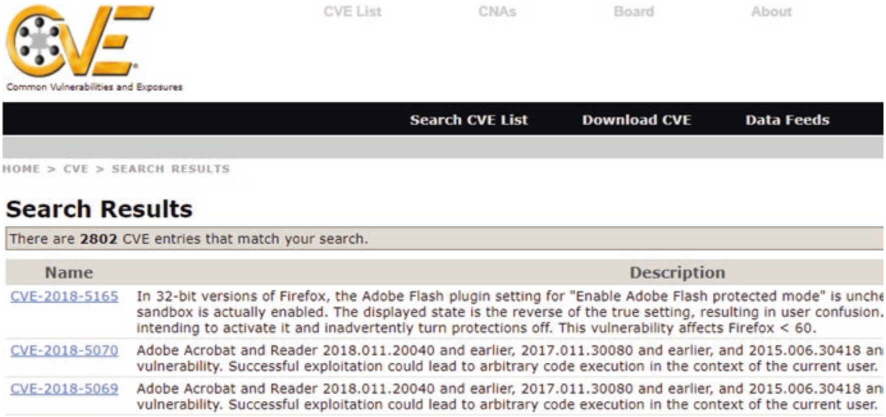
Figure 13.8 shows a sample of vulnerabilities with their CVSS score.

- MITRE CVE (https://cve.mitre.org), and (https://www.cvedetails.com/)
  Funded by US DHS, MITRE CVE is a formal initiative whose goal is to standardize the names for all publicly known vulnerabilities and security exploits (Fig. 13.9).
- FIRST (https://www.first.org)
  FIRST is an international confederation of trusted computer incident response teams who cooperatively handle computer security incidents and promote incident prevention programs.
  First was formed in 1990 in response to two significant malwares, Internet worm in 1998 and Wank worm in 1989.



CVSS	Public	ID	Title
9.6	2014-09-24	VU#252743	GNU Bash shell executes commands in exported functions in enviro...
9.5	2014-04-26	VU#222929	Microsoft Internet Explorer CMarkup use-after-free vulnerability
9.5	2014-02-13	VU#732479	Internet Explorer CMarkup use-after-free vulnerability
9.5	2013-01-10	VU#625617	Java 7 fails to restrict access to privileged code
9.5	2012-08-26	VU#636312	Oracle Java JRE 1.7 Expression.execute() and SunToolkit.getField() ...
9.5	2010-08-02	VU#362332	Wind River Systems VxWorks debug service enabled by default
9.5	2010-08-02	VU#840249	Wind River Systems VxWorks weak default hashing algorithm in sta...

Fig. 13.8 A sample of CERT vulnerabilities with CVSS score (https://www.kb.cert.org/vuls/byCVSS)



CVE
Common Vulnerabilities and Exposures
CVE List
CNAs
Board
About
Search CVE List
Download CVE
Data Feeds
HOME > CVE > SEARCH RESULTS

Search Results

There are **2802** CVE entries that match your search.

Name	Description
CVE-2018-5165	In 32-bit versions of Firefox, the Adobe Flash plugin setting for "Enable Adobe Flash protected mode" is unche sandbox is actually enabled. The displayed state is the reverse of the true setting, resulting in user confusion. intending to activate it and inadvertently turn protections off. This vulnerability affects Firefox < 60.
CVE-2018-5070	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 an vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.
CVE-2018-5069	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 an vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.

Fig. 13.9 CVE vulnerabilities database (https://cve.mitre.org)

K0193: Knowledge of Advanced Data Remediation Security Features in Databases

Data remediation or harmonization involves the ability to push the clean data back into the source data stores. The process is not always doable as restrictions in the source system may prevent remediating cleansed data.

With time and different processing and transactions data may have quality issues and may need to be checked for quality issues such as: completeness, conformity, consistency, duplicates, integrity, and accuracy. The following data remediation features are used in databases:

- Data encryption: Security team can leverage technologies such as encryption to identify sensitive information and encrypt it as a remediation tool for possible security incidents. Security team can then mitigate the potential of inappropriate data exposure.

- Shredding: File destruction or shredding, (according to some standards such as DoD 5220-22.M deletion standard) ensures that data cannot be recovered using software-based forensic tools.
- Redacting: Scrubbing sensitive data, replacing it with non-sensitive characters.
- Quarantining of files: Quarantine allows users to securely move files containing sensitive data to a local or remote location that has been considered secure.

K0230: Knowledge of Cloud Service Models and Possible Limitations for an Incident Response

Cloud environments present a unique set of risks, weaknesses, and threats in comparison with classical networks and architectures. Security teams should update their threat models to account for these challenges and differences.

Infrastructure distribution of the cloud can create confusion on who is responsible for what and where data is kept. Proper documentation, tracking and communicating everything ensures that IR processes are as clear as possible. Clear roles and responsibilities between service providers, technology vendors, and users should be continuously maintained and clarified.

Collaboration and efforts' integration are also a key in conducting successful incident responses in the cloud where open, continuous and unified channels of communication should exist between the different groups.

K0317: Knowledge of Procedures Used for Documenting and Querying Reported Incidents, Problems, and Events

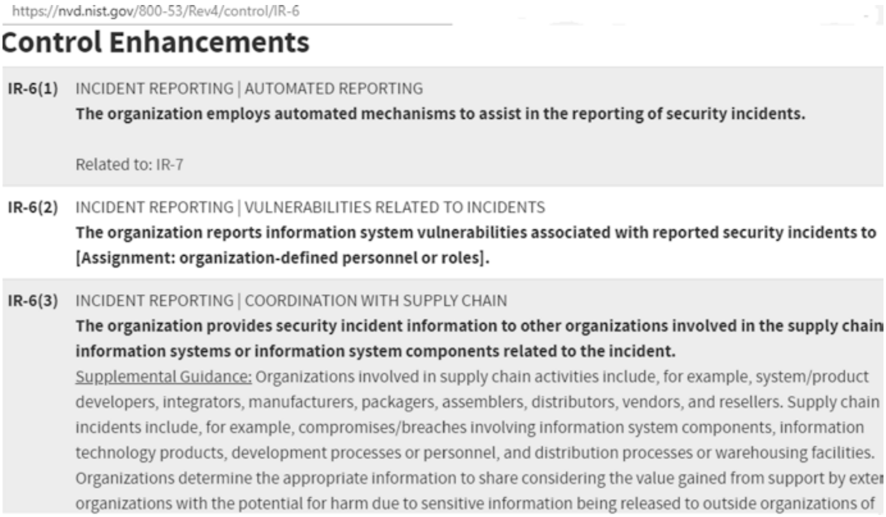
Security Incident Reporting Procedures

NIST Special Publication 800-53 (Rev. 4) IR6 includes details on incident reporting. The standard specifies reporting guidelines including what to report and who to report to.

Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to US-CERT (Fig. 13.10).

K0381: Knowledge of Collateral Damage and Estimating Impact(s)

Collateral damages are incidentals to the intended target. It is often used in military to refer to the incidental destruction of civilian properties and non-combatant casualties.



https://nvd.nist.gov/800-53/Rev4/control/IR-6

Control Enhancements

IR-6(1) INCIDENT REPORTING | AUTOMATED REPORTING
The organization employs automated mechanisms to assist in the reporting of security incidents.

Related to: IR-7

IR-6(2) INCIDENT REPORTING | VULNERABILITIES RELATED TO INCIDENTS
The organization reports information system vulnerabilities associated with reported security incidents to [Assignment: organization-defined personnel or roles].

IR-6(3) INCIDENT REPORTING | COORDINATION WITH SUPPLY CHAIN
The organization provides security incident information to other organizations involved in the supply chain information systems or information system components related to the incident.
Supplemental Guidance: Organizations involved in supply chain activities include, for example, system/product developers, integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents include, for example, compromises/breaches involving information system components, information technology products, development processes or personnel, and distribution processes or warehousing facilities. Organizations determine the appropriate information to share considering the value gained from support by exter organizations with the potential for harm due to sensitive information being released to outside organizations of

Fig. 13.10 IR6 Control enhancements (https://nvd.nist.gov/800-53/Rev4/control/IR-6)

In the cyber security world, cyber offensive operations may impact users, systems or resources unintentionally. The attacker may find it difficult to make good and reliable estimates of collateral damage as identifying target indirect dependencies can be difficult.

A common DoS attack directed against a customer involves generating a large volume of attack traffic destined for the target victim through their service provider. Other customers within the service provide network may suffer DoS collateral damage or negative effects to other customers or the network infrastructure as well (Kumari McPherson 2009).

Highly focused targets can help lower the occurrence of such cases of collateral damages. Security experts should always assess collateral damages due to ethical, legal and technical considerations.

Another reason why attackers should try to minimize collateral damages is that an attack that spreads wide is more likely to be discovered or noticed by the targets, which may lead the defenders to take countermeasures (Sang-Hun 2016, Libicki 2017).

Domain Name Servers (DNS) usually suffer from collateral damage attacks especially in indirect DDoS (Bellovin et al. 2017). DNSs require less bandwidth that most websites and hence are incapable of handling high transactions/requests.

Damaging but not destroying one computer system can have unforeseen effects on other connected systems (Bellovin et al. 2017). When target system is destroyed connected systems will abandon the target and its resources. On the other hand, if the target is damaged in such a way that communication and interaction with connected systems continue. This may cause more severe impact on those connected systems. One typical example of such case is when many attackers launch their attacks within two phases. In the first phase, they target intermediate systems and control them. Those victim machines become the source of the attack. Those systems were not destroyed but damaged in a form that make them the attacker zombie.

S0054: Skill in Using Incident Handling Methodologies

Some of the public organizations that have incident handling methodologies:

- NIST: The National Institute of Standards and Technology Special Publication 800-61 is the Computer Security Incident Handling Guide.
  NIST guideline includes steps and recommendations for incident handling teams such as proper planning and training. Additionally, IR team should be aware of their environment and also of using the right tools to learn about the incident, contain it and ensure business continuity.
  NIST advises that incident handling plans should include enough containment to sandbox the adversary to avoid potential liabilities. NIST described an incident response lifecycle of four steps: (1) Preparation, (2) detection and analysis, (3) containment, eradication and recovery, and (4) post-incident activities, Fig. 13.11.
- SANS: The SANS incident handling process consists of six phases: Preparation, identification, containment, eradication, recovery, and lessons learned, Fig. 13.12, (Gennuso 2012).
- CERT: US-CERT provides different types of services related to security, vulnerabilities, education, training and incident handling.

There are several ways for defining CERT constituency (groups that CERT handle their incidents). It can be defined by categories such:

- Ranges of IP addresses
- Domain names

US-CERT is continuously evolving and improving their incident handling methodology along with other services that they provide.

- ISO: ISO/IEC 27035:2016—Information technology—Security techniques—Information security incident management: The standard covers the processes for managing information security events, incidents and vulnerabilities.

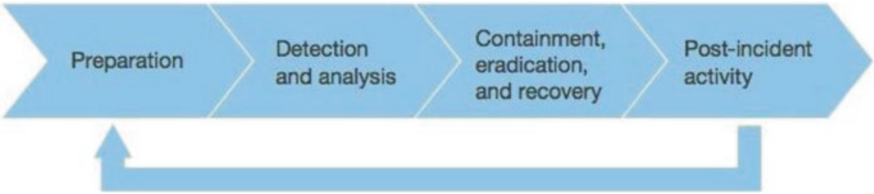


Fig. 13.11 Incident response lifecycle

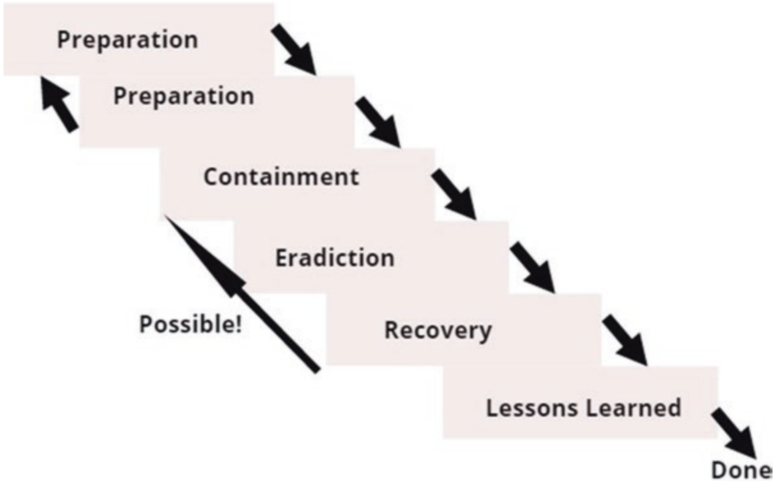


Fig. 13.12 SANS incident handling method

ISO/IEC 27035expands on the information security incident management section of ISO/IEC 27002. In this standard incident is handled through the following steps (ISO 2018):

1. Prepare to deal with incidents
2. Identify and report security incidents
3. Assess incidents and make decisions about how they are to be addressed
4. Respond to incidents, i.e., contain, mitigate them
5. Learn the lessons

ISO/IEC 27035 replaced ISO TR 18044. It was published in 2011 and revised and split into three parts.

- ISO/IEC 27035-1:2016 Principles of incident management
- ISO/IEC 27035-2:2016 Guidelines to plan and prepare for incident response
- ISO/IEC 27035-3: Guidelines for incident response operations
- Symantec DLP: For detecting, alerting, and preventing the exposure of confidential data.

S0080: Skill in Performing Damage Assessments

In general, damage assessment is a postmortem task that occurs late in the incident lifecycle (e.g., in the recovery stage). Some of the impacts of an incident may take some time to discover or assess.

Damage assessment to evaluate the level of impact an incident cause on systems or assets is used to serve different purposes such as:

- Liability issues: In principle, an attacker is liable on damages their actions caused on target systems, intentionally or unintentionally.
- Court and legal considerations: Whenever a case is in process as a result of a security incident, damage assessment is a key task for both plaintiffs and victims.
- Mitigation actions: The amount and level of damages an incident may cause can trigger different types of mitigation activities based on the severity of the impact.
- Future security actions (e.g., impacts on security policies, controls).

In information systems, damages can fall largely on the following categories:

- Users and services' interruption (e.g., on availability, DoS attacks).
- Physical, network, and hardware damage.
- Software and data corruption (e.g., ransomwares).
- Data breaches, identity theft, etc.
- Impact on credibility, reputation, etc. This is usually the hardest to assess or evaluate.

S0098: Skill in Detecting Host and Network-Based Intrusions via Intrusion Detection Technologies

We described similar examples in KSAs: S0096 and S0170

S0173: Skill in Using Security Event Correlation Tools

Examples of popular open source event correlation tools include:

- Simple Event Correlator (SEC): Perl-based lightweight, platform-independent event correlation tool, http://simple-evcorr.github.io/.
- RightITnow: Has open and commercial options.
- OpenNMS: OpenNMS contains an event correlation engine based upon the Drools engine, https://www.opennms.org/en
- Esper (and Nesper): Available in different programming languages, http://www.espertech.com/esper/
- LOGalyze: http://www.logalyze.com/

A0025: Ability to Accurately Define Incidents, Problems, and Events in the Trouble Ticketing System

Trouble ticketing systems are used in fault management. Using a trouble ticketing software, the network administrator can design (1) a trouble ticket that reflects the interests of the end users and (2) a ticket transition graph that enforces the proper escalation and routing of a ticket to closure, Olson and Blackwell 1990.

For time-critical services, the downtime that can elapse from the observation of a fault, the submission of a trouble ticket, to the closure of the trouble ticket can be expensive. This downtime can be reduced by providing a communication path between the fault detection system and a trouble ticketing system (Lewis 1993).

The following are examples of free and commercial trouble ticketing systems:

- Zoho: https://www.zoho.com/desk/lp/trouble-ticketing-software.html.
- ManageEngine: https://www.manageengine.com/products/service-desk/trouble-ticket-software.html.
- ZenDesk: https://www.zendesk.com/support.
- FreshService: https://freshservice.com/it-helpdesk-ticketing.
- TroubleTicketExpress: http://www.troubleticketexpress.com/open-source-software.html.
- HappyFox: https://www.happyfox.com/software/trouble-ticket-software/.
- OTRS: https://sourceforge.net/projects/otrs-persian/.
- OpenTT: https://sourceforge.net/projects/opentt/.

Bibliography

Bejtlich R (2010) CIRT-level response to advanced persistent threat. SANS Forensics Incident Response Summit

Bellovin SM, Landau S, Lin HS (2017) Limiting the undesired impact of cyber weapons: technical requirements and policy implications. J Cybersecur 3(1):59–68. https://doi.org/10.1093/cybsec/tyx001

Campbell T (2003) An introduction to the computer security incident response team (CSIRT) set-up and operational considerations. Global information assurance certification paper. giac.org

Cichonski P, Millar T, Grance T (NIST), Scarfone K (Scarfone Cybersecurity) (2012) NIST Special publication 800-61, SP 800-61 Rev. 2. Computer security incident handling guide, August 2012

Gennuso K (2012) Shedding light on security incidents using network flows. SANS. https://www.sans.org/reading-room/whitepapers/incident/shedding-light-security-incidents-network-flows-33935

Incident Response Plan (2018) Document version: 1.0.0. http://www.i-assure.com, www.i-assure.com/wp-content/uploads/dlm.../RMF_Incident-Response-plan.docx

Information security Technologies to Secure Federal Systems (2004) GAO report to congressional requesters. GAO-04-467. www.gao.gov.

InfoSec Nirvana (2015) Part 2, Incident classification, security investigation series. http://infosec-nirvana.com/part-2-incident-classification/

ISO/IEC 27035 (2018) http://www.iso27001security.com/html/27035.html

Kumari W, McPherson D (2009) Remote triggered black hole filtering with unicast reverse path forwarding (uRPF). Network working group, request for comments: 5635

Lewis L (1993) A case-based reasoning approach to the management of faults in communications networks. CAIA

Libicki M (2017) Second acts in cyberspace. J Cybersec 3:29–35

Mehta L (2014) Top 6 SIEM Use Cases—InfoSec Institute. http://resources.infosecinstitute.com/top-6-seim-usecases/. Accessed 6 Sept 2014

Olson L, Blackwell A (1990) Understanding network management with OOA. IEEE network magazine

Sang-Hun C (2016) Computer networks in South Korea are paralyzed in cyberattacks. New York Times. http://www.nytimes.com/2013/03/21/world/asia/southkorea-computer-network-crashes.html. Last Accessed 26 June 2016

Trivedi K (2007) A standards-based approach for offering a managed security service in a multi-vendor network environment. Internet Protocol J 10(3)

Zhang E (2017) What is event correlation, examples, benefits and more. Digi Guardian, https://digitalguardian.com/blog/what-event-correlation-examples-benefits-and-more

Index

I. Alsmadi, *The NICE Cyber Security Framework*,
https://doi.org/10.1007/978-3-030-02360-7