HACK LIKE A PRO IN 7 DAYS

LEARN THE MINDSET, REAL WORLD TOOLS & THE TECHNIQUES TO BE A PROFESSIONAL HACKER

Content is for Education Purposes. Don't use the material for any unlawful activity.

Helps in preparing for CEH & OSCP certification exams

HACK LIKE A PRO IN 7 DAYS

LEARN THE MINDSET, REAL WORLD TOOLS & THE TECHNIQUES TO BE A PROFESSIONAL HACKER

Content is for Education Purposes. Don't use the material for any unlawful activity.

Helps in preparing for CEH & OSCP certification exams

HACK LIKE A PRO IN 7 DAYS

Learn the mindset, tools and the techniques to be a professional hacker.

www.ipspecialist.net Document Control

Proposal Name : Hack Like a Pro in 7 Days
Document Version : 1.0
Document Release Date : 03-Nov-2020
Reference : IPS-HACK-TECH

Feedback:
If you have any comments regarding the quality of this book, or otherwise alter it to suit your needs better, you can contact us by email at info@ipspecialist.net
Please make sure to include the book title and ISBN in your message.

Read this First!

Thank you for reading this book. Your decision to purchase this book may turn out to be the smartest decision you've ever made. As you are about to learn, this book totally delivers on the promise that I have made on the cover page – Hack like a Professional in 7 Days.

Due to the rapid rise in cybercrime, Cyber Security has been evolving. More companies are starting to realize that if you want to prevent a hacker you must think like a hacker. This mindset has created a new way of protecting networks, by approaching cyber security from a different perspective. Offensive security measures are focused on seeking out the perpetrators and in some cases attempting to disable or at least disrupt their operations.

This book will teach you the latest commercial-grade hacking tools, techniques, and methodologies used by hackers and information security professionals to lawfully hack an organization. This is a complete hands-on material to make you a professional ethical hacker. The one thing that apart an elite ethical hacker from script kiddies is 'persistence'. It is important to remember that failure is part of the process. Sometimes a particular vector just seems like it should be more effective. The first step in developing persistence, it seems, is looking for why or how a particular approach is failing. Often this will lead to new approaches and new ideas.

Our goal is to provide the best, most complete book that leave our students with both the techniques and disposition necessary to be effective and successful beyond theory. We have carefully designed this book and labs to teach the mindset and the techniques to be a successful ethical hacker.

What you will learn?
■ The basics of ethical hacking.
■ Gathering information about your target.
■ Identify services running on and around your target. ■ Establish an active connection with the target.
■ Finding the weakness for exploitation.
■ Sniffing, Social Engineering and Denial of Service (DoS) attacks. ■ Evading the security appliances.

■ Hacking web servers.
■ Hacking wireless networks.
■ Hacking mobile applications.
■ Internet of Things (IoT) hacking.
■ Cloud computing attacks.

Before you begin this book, there's something you need to understand first: It will not be easy. It will take hard work and dedication from YOU. It will require you to believe 100% in yourself, and it will require you to back that belief with persistence.

No matter where you are on your career journey, I hope this book dramatically helps to become a professional ethical hacker.
I want to thank you again for reading this book.

Ready? Let's get started!

Disclaimer:
Do not attempt to violate the law with anything contained here. If you planned to use the content for illegal purpose, we will not be responsible for your any illegal actions. The misuse of the information in this book can result in criminal charges brought against the persons in question. The authors will not be held responsible in the event any criminal charges be brought against any individuals misusing the information in this book to break the law.

About IPSpecialist

IPSPECIALIST LTD. IS COMMITTED TO EXCELLENCE AND DEDICATED TO YOUR SUCCESS.

Our philosophy is to treat our customers like family. We want you to succeed, and we are willing to do anything possible to help you make it happen. We have the proof to back up our claims. We strive to accelerate billions of careers with great courses, accessibility, and affordability. We believe that continuous learning and knowledge evolution are most important things to keep re-skilling and up-skilling the world. Planning and creating a specific goal is where IPSpecialist helps.

We can create a career track that suits your visions as well as develop the competencies you need to become a professional Network Engineer. We can also assist you with the execution and evaluation of proficiency level based on the career track you choose, as they are customized to fit your specific goals.

We help you STAND OUT from the crowd through our detailed IP training content packages.

Course Features:

· *Self-Paced Learning*

O Learn at your own pace and in your own time

· *Covers Complete Exam Blueprint*

O Prep-up for the exam with confidence

· *Case Study Based Learning*

O Relate the content to real-life scenarios

· *Subscriptions that Suits You*

O Get more pay less with IPS Subscriptions

· *Career Advisory Services*

O Let industry experts plan your career journey

· *Virtual Labs to Test Your Skills*

O With IPS vRacks, you can testify your exam preparations

· *Practice Questions*

O Practice Questions to measure your preparation standards

· *On Request Digital Certification*

O On request, digital certification from IPSpecialist LTD.

About the Authors:

We compiled this workbook under the supervision of multiple professional engineers. These engineers specialize in different fields, i.e., Networking, Security, Cloud, Big Data, IoT, and so forth. Each engineer develops content in his/her specialized field that is compiled to form a comprehensive certification guide.

About the Technical Reviewers:

Nouman Ahmed Khan

AWS-Architect, CCDE, CCIEX 5 (R&S, SP, Security, DC, Wireless), CISSP, CISA, CISM is a Solution Architect working with a major telecommunication provider in Qatar. He works with enterprises, mega-projects, and service providers to help them select the best-fit technology solutions. He also works as a consultant to understand customer business processes and helps select an appropriate technology strategy to support business goals. He has more than fourteen years of experience working in Pakistan/Middle-East & UK. He holds a Bachelor of Engineering Degree from NED University, Pakistan, and M.Sc. in Computer Networks from the UK.

Abubakar Saeed

Abubakar Saeed has more than twenty-five years of experience, Managing, Consulting, Designing, and implementing large-scale technology projects, extensive experience heading ISP operations, solutions integration, heading Product Development, Pre-sales, and Solution Design. Emphasizing on adhering to Project timelines and delivering as per customer expectations, he always leads the project in the right direction with his innovative ideas and excellent management.

Muhammad Yousuf

Muhammad Yousuf is a professional technical content writer. He is a Certified Ethical Hacker (v 10) and Cisco Certified Network Associate in Routing and Switching, holding a Bachelor's Degree in Telecommunication Engineering from Sir Syed University of Engineering and Technology. He has both technical knowledge and industry sounding information, which he uses perfectly in his career.

Free Resources:

With each workbook you buy from Amazon, IPSpecialist offers free resources to our valuable customers. Once you buy this book you will have to contact us at support@ipspecialist.net or tweet @ipspecialistnet to get this limited time offer without any extra charges.

Free Resources Include:

Exam Practice Questions in Quiz Simulation: IP Specialists' Practice Questions have been developed keeping in mind the certification exam perspective. The collection of these questions from our technology workbooks is prepared to keep the exam blueprint in mind covering not only important but necessary topics as well. It is an ideal document to practice and revise your certification.

Career Report: This report is a step by step guide for a novice who wants to develop his/her career in the field of computer networks. It answers the following queries: ■ Current scenarios and future prospects.

■ Is this industry moving towards saturation or are new opportunities knocking at the door?
■ What will the monetary benefits be?
■ Why to get certified?
■ How to plan and when will I complete the certifications if I start today?
■ Is there any career track that I can follow to accomplish specialization level?

Furthermore, this guide provides a comprehensive career path towards being a specialist in the field of networking and also highlights the tracks needed to obtain certification.

IPS Personalized Technical Support for Customers: Good customer service means helping customers efficiently, in a friendly manner. It is essential to be able to handle issues for customers and do your best to ensure they are satisfied. Providing good service is one of the most important things that can set our business apart from the others of its kind.

Great customer service will result in attracting more customers and attain maximum customer retention.

IPS is offering personalized TECH support to its customers to provide better value for money. If you have any queries related to technology and labs you can simply ask our technical team for assistance via Live Chat or Email.

Contents at a Glance

Table of Contents

About this Workbook

This workbook covers all the information you need to pass the EC-Council's Certified Ethical Hacking 3 12-50 exam. The workbook is designed to take a practical approach to learning with real-life examples and case studies.

- ➢ Covers complete CEH blueprint
- ➢ Summarized content
- ➢ Case Study based approach
- ➢ Ready to practice labs on VM
- ➢ Pass guarantee
- ➢ Exam tips
- ➢ Mind maps

CEHv 10 3 rd Edition Update

CEH v 10 covers new modules for the security of IoT devices, vulnerability analysis, focus on emerging attack vectors on the cloud, artificial intelligence, and machine learning including a complete malware analysis process. Our CEH workbook delivers a deep understanding of applications of the vulnerability analysis in a real-world environment.

EC-Council Certifications

The International Council of E-Commerce Consultants (EC-Council) is a member-based organization that certifies individuals in various e-business and information security skills. It is the owner and creator of the world famous Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (CHFI) and EC-Council Certified Security Analyst (ECSA)/License Penetration Tester (LPT) certification, and as well as many others certification schemes, that are offered in over 87 countries globally.

EC-Council mission is to validate information security professionals having necessary skills and knowledge required in a specialized information security domain that helps them avert a cyber-war, "should the need ever arise". EC-Council is committed to withholding the highest level of impartiality and objectivity in its practices, decision making, and authority in all matters related to certification.

EC-Council Certification Tracks

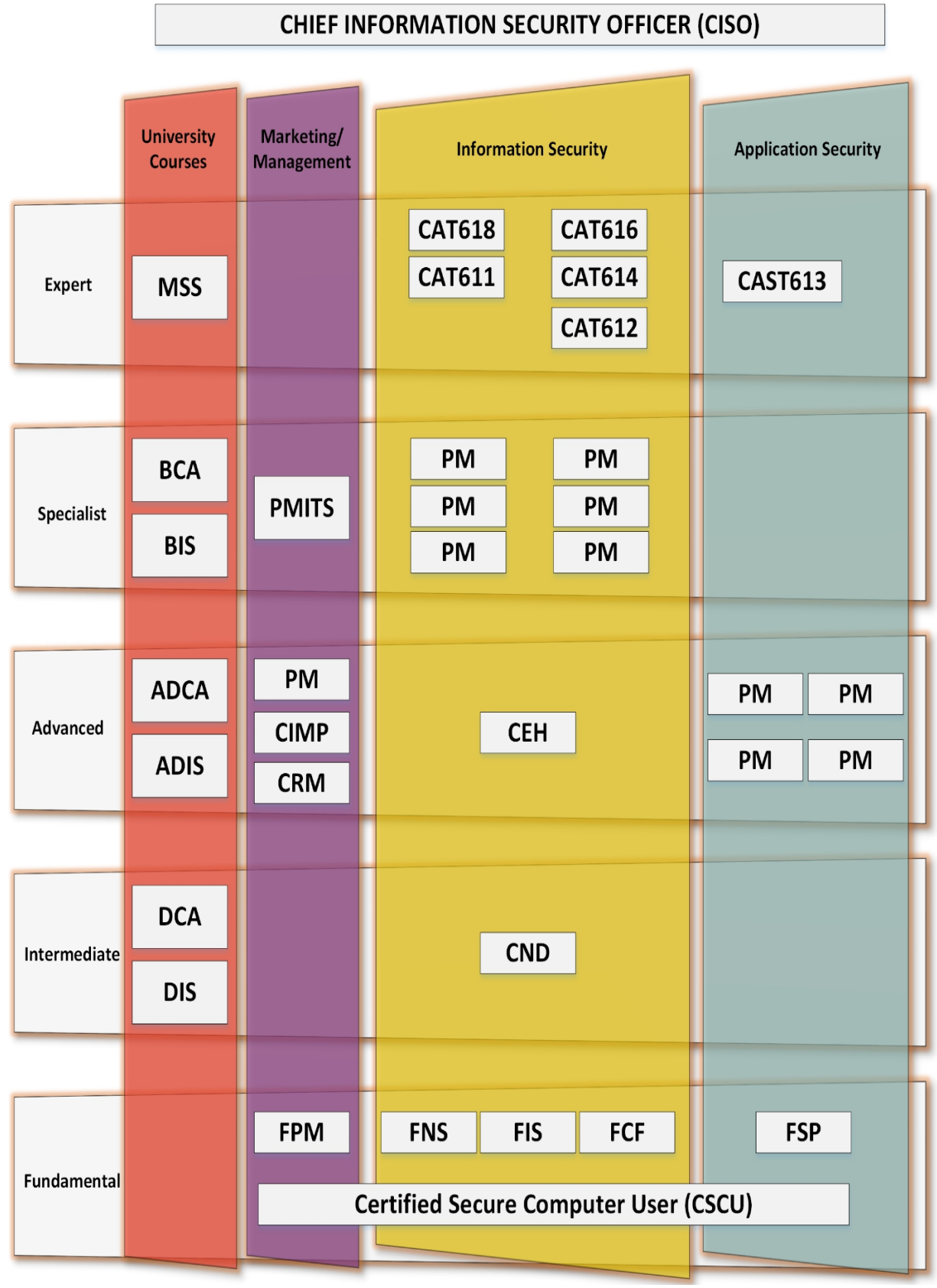


Figure 1: EC-Council Certifications Track

How does CEH Certification Help?

The purpose of the CEH credential is to:

➢ Establish and govern minimum standards for credentialing professional information security specialists in ethical hacking measures.

➢ Inform the public that credentialed individuals meet or exceed the minimum standards.

➢ Reinforce ethical hacking as a unique and self-regulating profession.

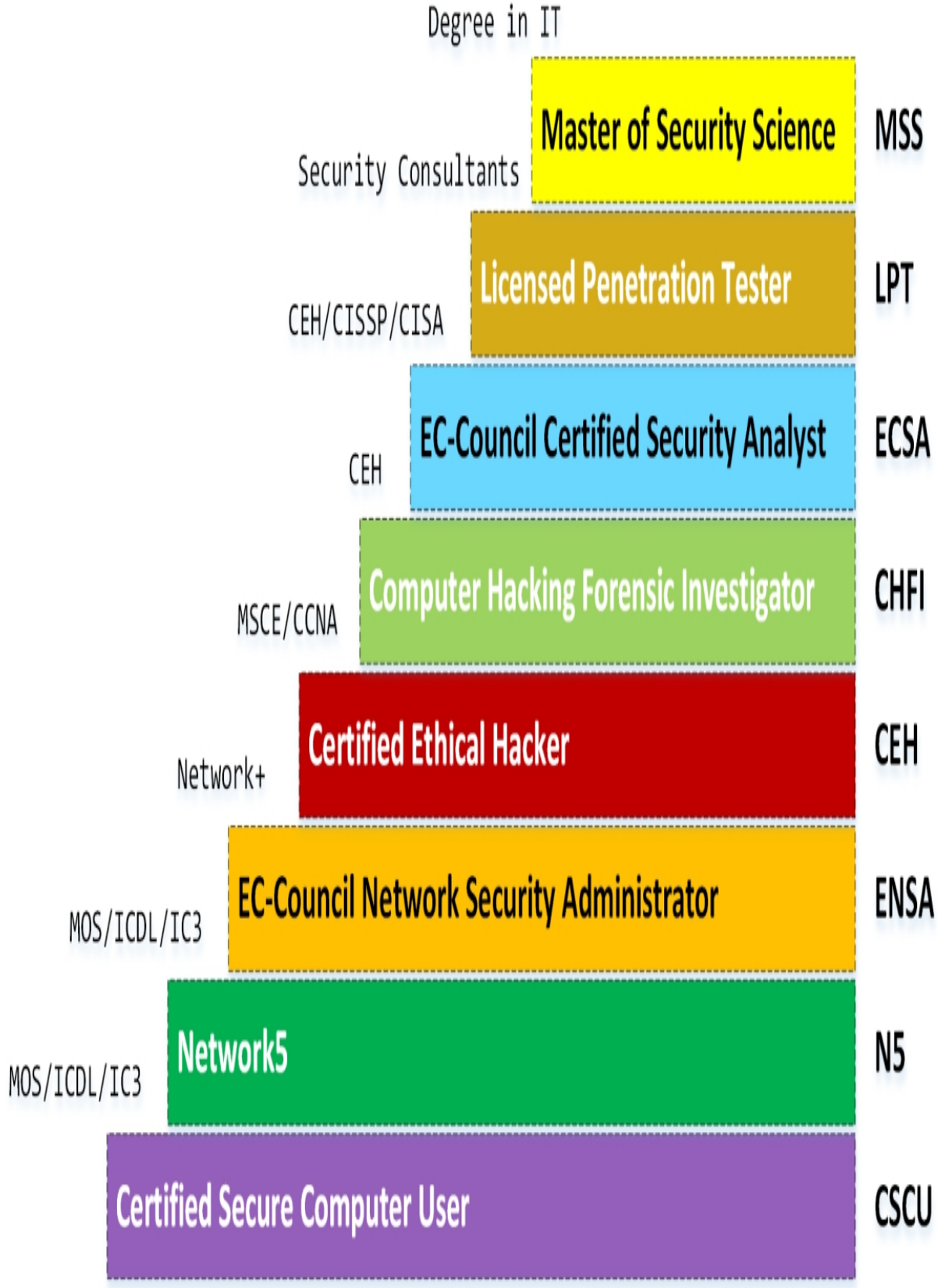


Figure 2: EC-Council Certifications Skill Matrix

Figure 2: EC-Council Certifications Skill Matrix

About the CEH Exam

➢ Number of Questions:
➢ Test Duration:
➢ Test Format:
➢ Test Delivery:
➢ Exam Prefix:

125
4 Hours
Multiple Choice
ECC EXAM, VUE
3 12-50 (ECC EXAM), 3 12-50 (VUE)

A Certified Ethical Hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but lawfully and legitimately to assess the security posture of a target system(s). The CEH credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.

Domain Objective Weightage Questions
Background
Analysis / Assessment
Security
Tools / System / Program
Procedure and Methodologies
Network and Communication Technology
Information Security Threats and Attack Vectors 2 1.79% 27 Information Security Technologies
Information Security Assessment and Analysis 12.73% 16Information Security Assessment Process

Information Security Controls
Information Security Attack Detections 23.73% 30 Information Security Attack Prevention

Information Security Systems
Information Security Programs 28.9 1% 36 Information Security Tools

Information Security Procedures 8.77% 1 1 Information Security Assessment Methodology

Regulation / Policies

Information Security Policies / Laws / Acts 1.90% 2

Ethics Ethics of Information Security 2. 17% 3

Pre-Requisites

All the three programs, CEH, CHFI, and ECSA, require the candidate to have two years of work experience in the Information Security domain and should be able to provide proof of the same as validated through the application process unless the candidate attends official training.

Chapter 1: Introduction to Ethical Hacking

Technology Brief

System security consists of methods and processes used for protecting information and information systems from unauthorized access, disclosure, usage or modification. Information security ensures the confidentiality, integrity, and availability of information. If an organization lacks security policies and appropriate security rules, its confidential information and data will not be secure, putting the organization at great risk. Well-defined security policies and procedures help in protecting the assets of an organization from unauthorized access and disclosures.

In the modern world, with the help of the latest technologies and platforms, millions of users interact with each other every minute. These sixty seconds can be very vulnerable and costly to private and public organizations due to the presence of various types of threats, both old and modern, that are present worldwide. The most common and rapid option for spreading threats all over the world is the public internet. Malicious Codes and Scripts, Viruses, Spams, and Malware are constantly waiting to be accessed. Which is why security risks to a network or a system can never be entirely eliminated. Implementing a security policy that is effective and efficient, rather than consisting of unnecessary security implementations that can result in a waste of resources and create loopholes for threats, is a continual challenge.

Data Breach

eBay Data Breach

One famous example demonstrating the need for corporate information and network security is the data breach that occurred at eBay. eBay is a well-known online auction platform that is widely used all over the world.

In 2004, eBay reported a massive data breach. According to eBay, the sensitive data of 145 million customers was compromised in this attack. The data included the following:

- Customers' names
- Encrypted passwords
- Email addresses
- Postal addresses
- Contact numbers
- Dates of birth

Information such as that listed above must always be stored in an encrypted form rather than in plain text, and it must use strong encryption. eBay claims that no information related to security numbers such as credit cards was compromised because its database containing financial information is kept in a separate and encrypted format. However, identity and password thefts can also result in severe risks.

Hackers carried out the eBay data breach by compromising a small number of employees' credentials through phishing between February and March 20 14. Specific employees may have been targeted in order to gain access to eBay's network, or it is possible that eBay's entire network was being monitored prior to the attack. eBay claim to have detected this cyber-attack within two weeks.

Google Play Hack

A Turkish hacker, "Ibrahim Balic ", hacked Google Play twice. He admitted responsibility for the Google Play attack and claimed that he had been behind the Apple's Developer site attack. He tested

vulnerabilities in Google's Developer Console and found a flaw in the Android Operating System. He tested the flaw twice, to make sure that a vulnerability really existed, and used the results of his vulnerability testing to develop an Android application to exploit the flaw. When the developer's console crashed, users were unable to download applications and developers were unable to upload their applications.

The Home Depot Data Breach

The theft of information from payment cards, for example credit cards, is very common nowadays. On the September 8, 20 14, Home Depot released a statement claiming that hackers had breached their Point of Sale system.

The attacker accessed the POS network and gained access to third-party vendors' login credentials. Zero-Day vulnerability exploited Windows, which created a loophole to enter Home Depot's corporate network via a path from the third-party environment. After accessing the corporate network, Memory Scrapping Malware was released and then the Point of Sale terminals were attacked. Memory Scraping Malware is highly effective, and it successfully grabbed the information on millions of payment card.

Home Depot took remedial action against the attack. They started using EMV Chip and Pin payment cards. These Chip and Pin payment cards have a security chip embedded into them to avoid duplicity of the magnetic-stripe. EMV cards prevent fraudulent transactions. Several countries today use EMV cards as a standard payment card because of the chip card technology. It is capable of declining certain types of credit card frauds.

Essential Terminology

Hack Value

The term Hack Value refers to the attractiveness, interest, or thing of worth to the hacker. The value describes the targets' level of attractiveness to the hacker.

Zero-Day Attack

Zero-Day Attack refers to threats and vulnerabilities that can be used to exploit the victim before the developer identifies or addresses them and releases a patch for them. *Vulnerability*

Vulnerability refers to a weak point or loophole in any system or network that can be helpful and utilized by attackers to hack into the system. Any vulnerability can be an entry point from which they can reach their target.

Daisy Chaining

Daisy Chaining is a sequence of hacking or attacking attempts to gain access to a network or system, one after another, using the same information and the information obtained from the previous attempt.

Exploit

Exploit is a breach of a system's security through vulnerabilities, Zero-Day Attacks or any other hacking technique.

Doxing

The term Doxing means publishing information, or a set of information, associated with an individual. This information is collected from publicly available databases, mostly social media and similar sources.

Payload

Payload refers to the actual section of information or data in a frame as opposed to automatically generated metadata. In information security, payload is a section or part of a malicious and exploited code that causes potentially harmful activities and actions such as exploiting, opening backdoors, and hijacking.

Bot

Bot is a software used to control the target remotely and to execute predefined tasks. It is capable of running automated scripts over the internet. Bots are also known as Internet Bots or Web Robots. These Bots can be used for social purposes, for example, chatterbots and live chats. Furthermore, they can also be used for malicious purposes

in the form of malware. Malware bots are used by hackers to gain complete authority over a computer.

Elements of Information Security

Confidentiality

The National Institute of Standards and Technology (NIST) defines confidentiality as "*Preserving authorized restrictions on information access and disclosure, while including means for protecting personal privacy and proprietary information".*

We always want to make sure that our secret and sensitive data is secure. Confidentiality means that only authorized personnel can work with and see our infrastructure's digital resources. It also implies that unauthorized persons should not have any access to the data. There are two types of data in general. First is data in motion, as it moves across the network, and data at rest, when the data is in any media storage (such as servers, local hard drives, the cloud). For data in motion, we need to ensure data encryption before sending it over the network. Another option, which we can use along with encryption, is to use a separate network for sensitive data. For data at rest, we can apply encryption on storage media drives so that it can't read in the event of theft.

Integrity

The NIST defines integrity as " *Guarding against improper information modification or destruction, this includes ensuring information non-repudiation and authenticity"* .
We never want our sensitive and personal data to be modified or manipulated by unauthorized persons. Data integrity ensures that only authorized parties can modify data. NIST SP 800-56B defines data integrity as a property whereby data has not been altered in an unauthorized manner since it was created, transmitted or stored. In this Recommendation, the statement that a cryptographic algorithm "provides data integrity" means that the algorithm is used to detect unauthorized alterations.

Availability

Ensuring timely and reliable access to and use of information applying to systems and data is termed as Availability. If authorized personnel cannot access data due to general network failure or a Denial-of-Service (DOS) attack, then it is considered a critical problem from the point of view of business, as it may result in loss of revenue or of records of some important results.

We can use the term "CIA" to remember these basic yet most important security concepts.

CIA
Confidentiality
Integrity
Availability

Risk
Loss of privacy,
Unauthorized access to information & Identity theft

Information is no longer reliable or accurate, Fraud

Business disruption, Loss of customer's confidence, Loss of revenue

Control
Encryption, Authentication, Access Control
Maker/Checker, Quality Assurance, Audit Logs
Business continuity, Plans and tests Backup storage, Sufficient capacity
Table 1-01: Risk and Its Protection by Implementing CIA

Authenticity

Authentication is the process of identifying credentials of authorized users or devices before granting privileges or access to a system or network, and enforcing certain rules

and policies. Similarly, authenticity ensures the appropriateness of certain information and whether it has been initiated by a valid user who

claims to be the source of that information. Authenticity can be verified through the process of authentication.

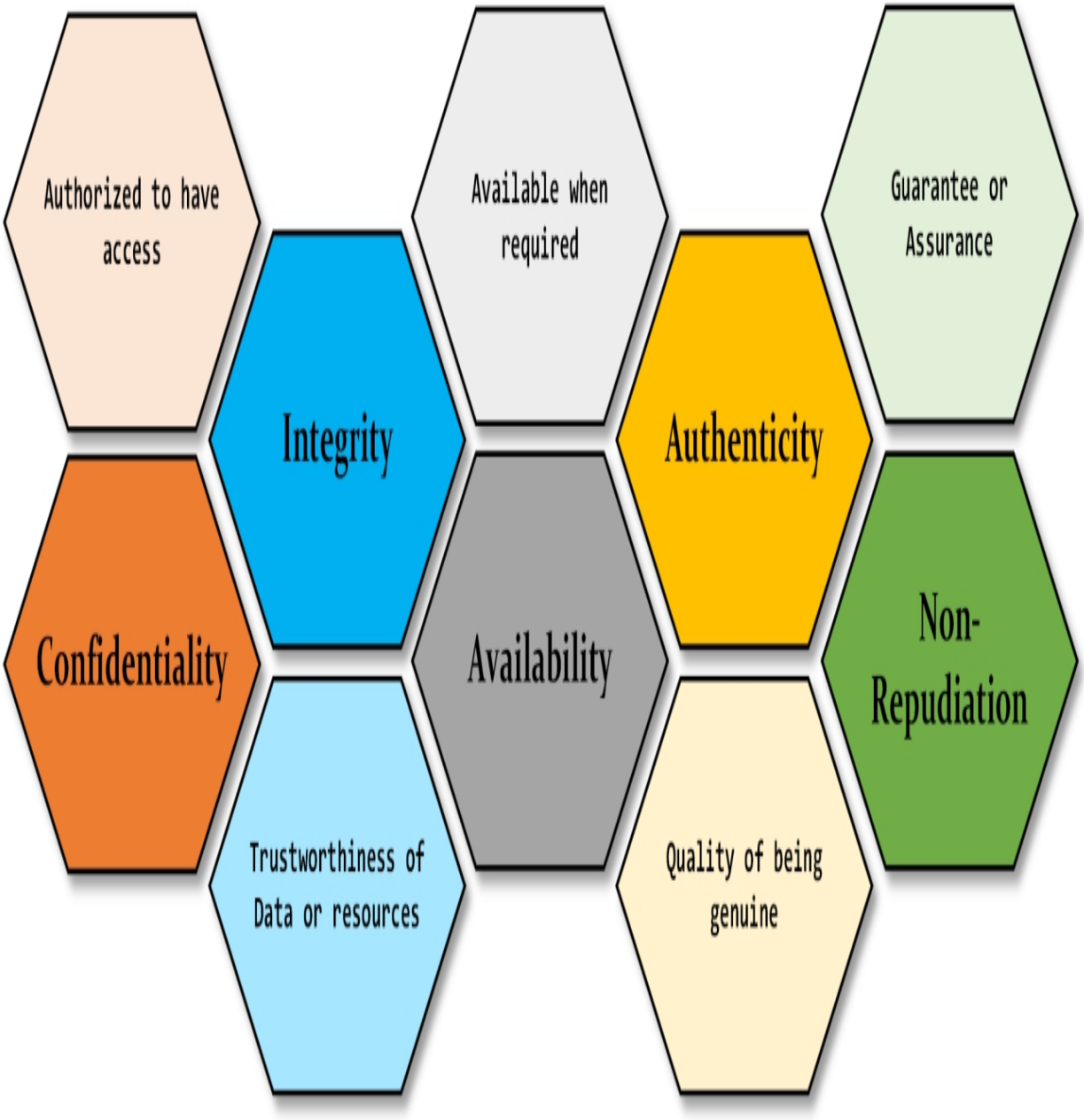


Figure 1-01: Elements of Information Security

Non-Repudiation

Non-repudiation is one of the Information Assurance (IA) pillars. It guarantees the transmission and receiving of information between the

sender and receiver via different techniques, such as digital signatures and encryption. Non-repudiation is the assurance

of communication and its authenticity so that the sender is unable to deny the sent message. Similarly, the receiver cannot deny what she/he has received. Signatures, digital contracts, and email messages use non-repudiation techniques.

The Security, Functionality, and Usability Triangle

In a system, the level of security is a measure of the strength of a system's Security, Functionality, and Usability. These three components form the Security, Functionality and Usability triangle. Consider a ball in this triangle—if the ball is sits in the center, it means all three components are stronger. On the other hand, if the ball is closer to Security, it means the system is consuming more resources for Security, and the system's Function and Usability require attention. A secure system must provide strong protection along with offering complete services, features, and usability to the user.

Figure 1-02: Security, Functionality & Usability Triangle

Implementation of high level security typically impacts the level of functionality and ease of usability. High level security will quite often make the system nonuser-friendly and cause a decrease in performance. While deploying security in a system, security experts must ensure a reliable level of functionality and ease of usability. These three components of the triangle must always be balanced.

Information Security Threats and Attack Vectors
Motives, Methods, and Vulnerabilities of Information Security Attacks

To penetrate information security, an attacker attacks the target system with three attack vectors in mind: Motive or objective, method, and vulnerability. These three components are the major blocks on which an attack depends.

- Motive or Objective: The reason an attacker focuses on a particular system

- Method: The technique or process used by an attacker to gain access to a target system
- Vulnerability: These help the attacker in fulfilling his intentions

An attacker's notive or objective for attacking a system may be a thing of value stored in that specific system. It may be ethical or it may be non-ethical. However, there is always a goal for the hacker to achieve that leads to the threat to the system. Some typical motives behind attacks are information theft, manipulation of data, disruption, propagation of political or religious beliefs, attacks on the target's reputation, or revenge. The method of attack and vulnerability run side by side. To achieve their motives, hackers use various tools and techniques to exploit a system once a vulnerability has been detected.

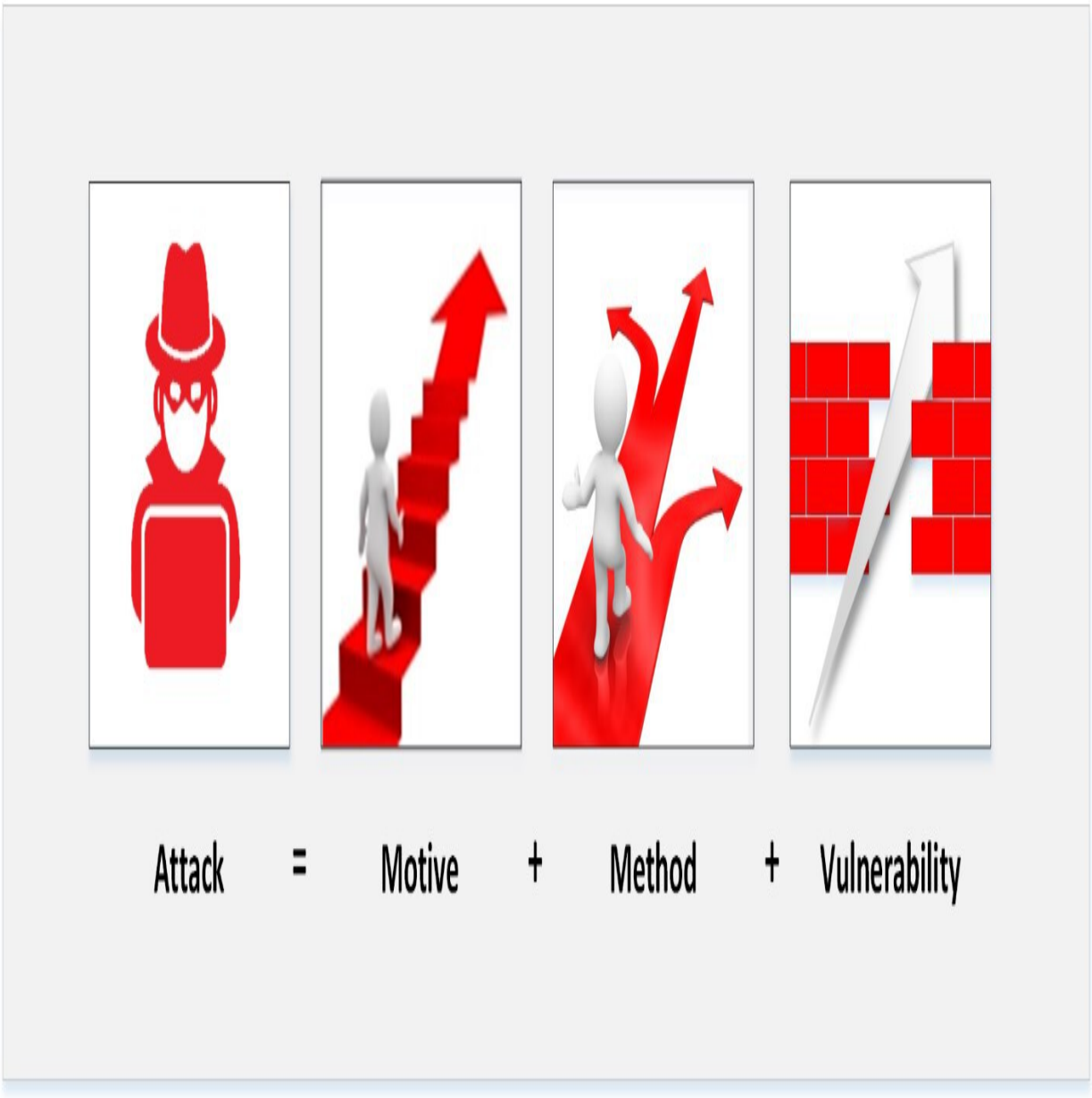


Figure 1-03: Information Security Attack

Top Information Security Attack Vectors

Cloud Computing Threats

Cloud computing has become a popular trend today. Its widespread implementation has exposed it to several security threats. Most of the threats are similar to those faced by traditionally hosted environments. It is essential to secure cloud computing for the purpose of protecting important and confidential data.

Following are some threats that exist in cloud security:

• In the environment of cloud computing, a major threat to cloud security is a single data breach that results in significant loss. It allows the hacker to have access to records; hence, a single breach may compromise all the information available on the cloud. It is an extremely serious situation as the compromise of a single record can lead multiple records being compromised

• Data loss is one of the most common potential threats that make cloud security vulnerable. Data loss may be due to intended or accidental means. It may be large scale or small scale; though massive data loss is catastrophic and costly

• Another major threat to cloud computing is the hijacking of an account or a service over the cloud. Applications running on a cloud with flaws, weak encryption, loopholes, and vulnerabilities allow the intruder to gain control, manipulate data, and alter the functionality of the service

Figure 1-04: Cloud Computing Threats

Furthermore, there are several other threats faced by cloud computing, which are as follows:

• Insecure APIs
• Denial of Services
• Malicious Insiders
• Poor SecurityMulti-Tenancy

Advanced Persistent Threats

An Advanced Persistent Threat (APT) is the process of stealing information through a

continuous procedure. An advanced persistent threat or political motives. The APT process organizations

sophisticated usually focuses on private relies upon advanced and

techniques to exploit vulnerabilities within a system. The term "persistent" defines the process of an external command and controlling

system, which continuously monitors and fetches data from a target. The term "threat" indicates the involvement of an attacker with potentially harmful intentions.

The characteristics of APT criteria are:
Characteristics Description Objectives Motive or goal of threat Timeliness Time spent in probing & accessing the target Resources Level of knowledge & tools Risk Tolerance Tolerance to remain undetected Skills & Methods Tools & techniques used throughout the event Actions Precise action of threat Attack Origination Points Number of origination points Numbers Involved in Attack Number of internal & external systems involved Knowledge Source Discern information regarding threats *Table 1-02: Advanced Persistent Threat Criteria*

Viruses and Worms

The term virus in network and information security describes malicious software. This malicious software is designed to spread by attaching itself to other files. Attaching to other files helps it to transfer onto other systems. These viruses require user interaction to trigger, infect, and initiate malicious activities on the resident system.

Unlike viruses, worms are capable of replicating themselves. This ability of worms enables them to spread on a resident system very quickly. Worms have been propagated in different forms since the 1980's. A few types of worms have emerged that are very destructive and are responsible for devastating DoS attacks.

Mobile Threats

Emerging mobile phone technology, especially smartphones, has raised the focus of attacks over mobile devices. As smartphones became popularly used all over the world, attackers' focus shifted to stealing business and personal information through mobile devices. The most common threats to mobile devices are:

- Data Leakage
- Unsecure Wi-Fi
- Network Spoofing
- Phishing Attacks
- Spyware

- Broken Cryptography
- Improper Session Handling

Insider Attack

An insider attack is the type of attack that is performed on a system, within a corporate network, by a trusted person. Trusted User is termed as “Insider” because an Insider has privileges and is authorized to access the network resources.

Figure 1-05: Insider Threats

Botnets

Botnets are the group of bots connected through the internet to perform a distributed task continuously. They are known as the workhorses of the internet. These botnets perform repetitive tasks (Robot) over the internet (Network). Botnets are mostly used in Internet Relay Chats. These types of botnets are legal and useful.

A botnet may be used for positive intentions but there also some botnets that are illegal and intended for malicious activities. These malicious botnets can gain access to a system by using malicious scripts and codes, either through directly hacking the system or through a "Spider”. A Spider program crawls over the internet and searches for holes in security. Bots introduce the system to the hacker’s web by contacting the master computer. It alerts the master computer when the system is under control. Attackers remotely control all bots from the master computer.

Threat Categories

Information Security Threat categories are as follows:

Network Threats

The primary components of network infrastructure are routers, switches, and firewalls. These devices not only perform routing and other network operations but they also control and protect the running applications, servers, and devices from attacks and intrusions. A poorly configured device allows an intruder to exploit targets. Common

vulnerabilities that are present on a network include using default installation settings, open access controls, weak encryption and passwords, and devices lacking the latest security patches. Top network level threats include:
• Information Gathering • Sniffing and Eavesdropping • Spoofing
• Session Hijacking
• Man-in-the-Middle Attack • DNS and ARP Poisoning • Password-based Attacks • Denial-of-Services Attacks • Compromised Key Attacks • Firewall and IDS Attacks

Host Threats
Host threats are focused on system software. Applications such as Windows 2000, .NET Framework, SQL Server are built or run over this software. Host level Threats include:

- Malware Attacks
- Footprinting
- Password Attacks
- Denial-of-Services Attacks
- Arbitrary Code Execution
- Unauthorized Access
- Privilege Escalation
- Backdoor Attacks
- Physical Security Threats

Application Threats
Best practice to analyze application threats is by organizing them into application vulnerability categories. Main threats to the application are:

- Improper Data / Input Validation
- Authentication and Authorization Attack
- Security Misconfiguration
- Information Disclosure
- Broken Session Management
- Buffer Overflow Issues
- Cryptography Attacks
- SQL Injection

Improper Error Handling and Exception Management

Types of Attacks on a System

Operating System Attacks

In Operating System Attacks, attackers always search for an Operating System's vulnerabilities. If they find a vulnerability in the Operating System, they exploit it to attack the system. Some of the most common vulnerabilities of an Operating System are:

- Buffer Overflow Vulnerabilities

Buffer Overflow is one of the major types of Operating System Attack. It is related to software exploitation attacks. When a program or application does not have welldefined boundaries, such as restrictions or pre-defined functional areas regarding the capacity of data it can handle or the type of data that can be inputted, buffer overflow causes problems such as Denial of Service (DoS), rebooting, attaining unrestricted access, and freezing.

How does it occur?

■ Due to an excess of data in the buffer memory

■ When a program or process attempts to write more data to a fixed length block of memory (a buffer)
■ Coding errors

How to prevent it?

Open Web Application Security Project (OWASP) defines a number of general techniques to prevent buffer overflows include:
o Code auditing (automated or manual)
o Developer training – bounds checking, use of unsafe functions, and group standards

o Non-executable stacks – many operating systems have at least some support for this
o Compiler tools – StackShield, StackGuard, and Libsafe, among others
o Safe functions – use strncat instead of strcat, strncpy instead of strcpy, etc

o Patches – Be sure to keep your web and application servers fully patched, and be aware of bug reports relating to applications upon which your code is dependent.
o Periodically scan your application with one or more of the commonly available scanners that look for buffer overflow flaws in your server products and your custom web applications.

- Bugs in the Operating System

In a Software Exploitation Attack, attackers find a bug in the software and exploit it. This vulnerability might be a mistake by the developer while developing the program code. Attackers can discover these mistakes and use them to gain access to the system.

- Unpatched Operating System

Unpatched Operating Systems allow malicious activities or fail to completely block malicious traffic from entering into a system. Successful intrusions can impact severely in the form of compromising sensitive information, data loss and disruption of regular operation.

Misconfiguration Attacks

In a corporate network, while installing new devices, the administrator must change the default configurations. If devices are left on default configuration, any user who does not have the privilege to access the device but has connectivity, can access it using default credentials. It is not a big deal for an intruder to access such devices because the default configuration has common and weak passwords and there are no security policies enabled on devices by default.

Similarly, permitting an unauthorized person or giving resources and permission to a person beyond the privileges, might also lead to an attack. Additionally, using the organization's name as a username or password makes it easier for hackers to guess the credentials.

Application Level Attacks

Before releasing an application, developers must make sure to test and

verify it from their end. In an Application Level Attack, a hacker can use:

- Buffer Overflow
- Active Content
- Cross-Site Script
- Denial of Service
- SQL Injection
- Session Hijacking
- Phishing

Shrink Wrap Code Attacks

A Shrink Wrap Code Attack is the type of attack in which hackers use the shrink wrap code method for gaining access to a system. In this type of attack, hackers exploit holes in unpatched Operating Systems and poorly configured software and applications. To understand shrink wrap vulnerabilities, consider an Operating System that has a bug in its original software version. The vendor may have released the update, but the time between the release of a patch by the vendor and the client's system updates is very critical. During this critical time, unpatched systems are vulnerable to the Shrinkwrap attack. Shrinkwrap attacks also exploit vulnerable software in an Operating System, bundled with insecure test pages and debugging scripts. The developer must remove these scripts before releasing the software.

Information Warfare

Information warfare is a concept of warfare over control of information. The term, "Information Warfare" or "Info War" describes the use of Information and Communication Technology (ICT) to get a competitive advantage over an opponent or rival. Information warfare is classified into two types:

1. Defensive Information Warfare

The term "Defensive Information Warfare" is used to refer to all defensive actions that are taken to protect oneself from attacks

executed to steal information and information-based processes. Defensive Information warfare areas are:

- Prevention
- Deterrence
- Indication and Warning
- Detection
- Emergency Preparedness
- Response

2. Offensive Information Warfare

Offensive warfare is an aggressive operation that is taken against a rival proactively rather than waiting for the attackers to launch an attack. Accessing their territory to occupy it rather than lose it is the fundamental concept of offensive warfare. During offensive warfare, the opponent and his strategies are identified, and the attacker makes the decision to attack based on the available information. Offensive Information warfare prevents information from being used by considering integrity, availability, and confidentiality.

Hacking Concepts, Types, and Phases

Hacker

A Hacker is a person capable of stealing information such as business data, personal data, financial information, credit card information, username and password from a system she or he has no authorized access to. An attacker gains access by taking unauthorized control over that system using different techniques and tools. They have great skills and abilities for developing software and exploring both software and hardware. There can be several reasons for hacking, the most common ones being fun, money, thrills or a personal vendetta.

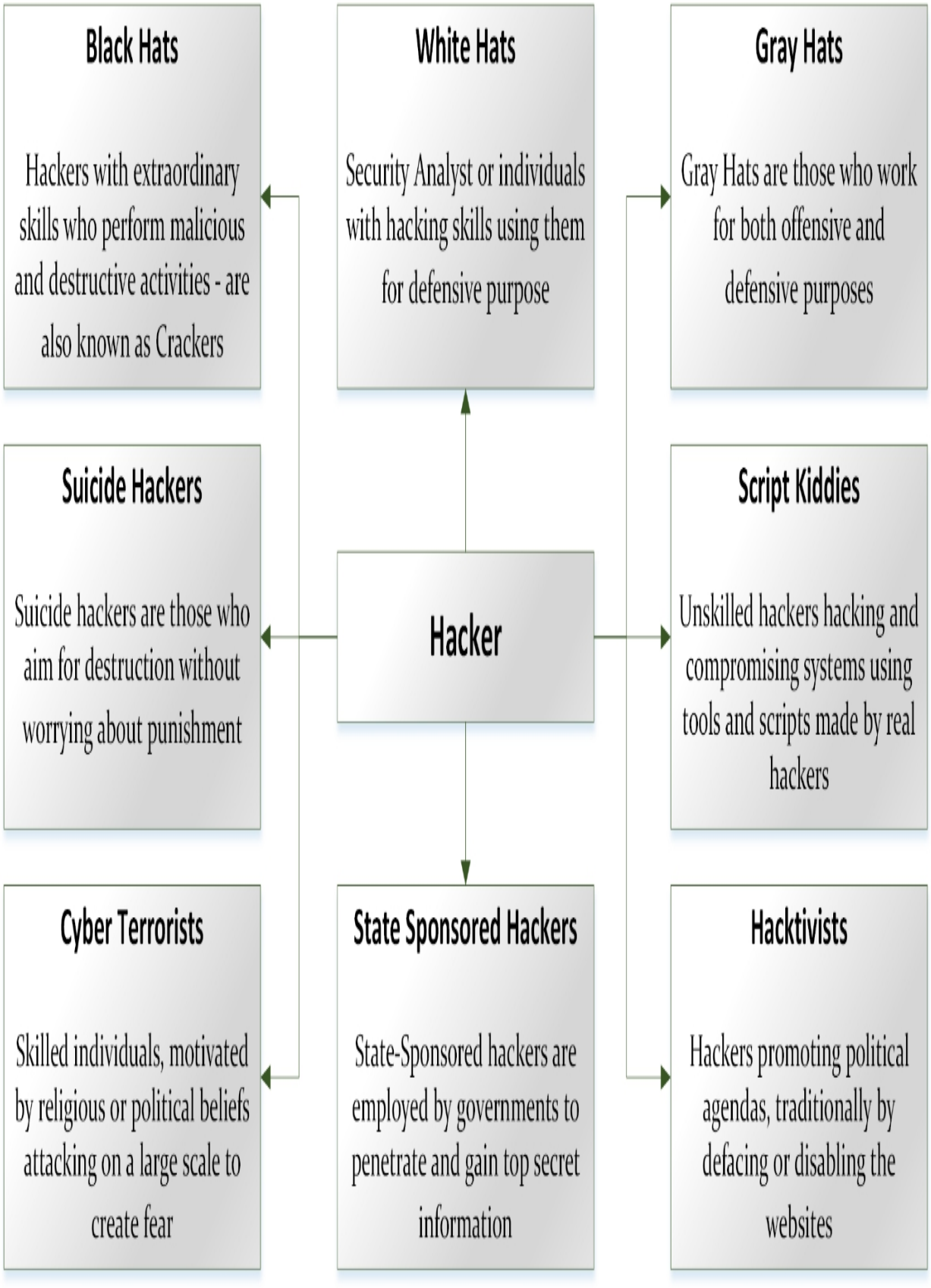


Figure 1. 06: Types of Hacker

Figure 1-06: Types of Hacker

Hacking

The term hacking in information security refers to exploiting vulnerabilities in a system and compromising the security to gain unauthorized command and control of the system. The purpose for hacking may include alteration of a system's resources or disruption of features and services to achieve other goals. Hacking can also be used to steal confidential information for any use such as sending it to competitors, regulatory bodies, or publicizing it.

Hacking Phases

The following are the five phases of hacking:

1. Reconnaissance
2. Scanning
3. Gaining Access
4. Maintaining Access
5. Clearing Tracks

Reconnaissance

Reconnaissance is an initial preparation phase for the attacker to prepare for an attack by gathering information about the target prior to launching an attack using different tools and techniques. Gathering information about the target makes it easier for an attacker. It helps to identify the target range for large scale attacks.

In Passive Reconnaissance , a hacker acquires information about the target without directly interacting with the target. An example of passive reconnaissance is searching social media to obtain the target's information.

Active Reconnaissance is gaining information by directly interacting with the target. Examples of active reconnaissance include interacting with the target via calls, emails, help desk, or technical departments.

Scanning

Scanning is a pre-attack phase. In this phase, an attacker scans the network through information acquired during the initial phase of reconnaissance. Scanning tools include diallers, scanners such as port scanners, network mappers, and client tools such as ping, as well as vulnerability scanners. During the scanning phase, attackers finally fetch the ports' information including port status, Operating System information, device type, live machines, and other information depending on scanning.

Gaining Access

This phase of hacking is the point where the hacker gains control over an Operating System (OS), application, or computer network. The control gained by the attacker defines the access level, whether the Operating System level, application level, or network level. Techniques include password cracking, denial of service, session hijacking, buffer overflow, or other techniques used for gaining unauthorized access. After accessing the system, the attacker escalates the privileges to a point to obtain complete control over services and processes and compromise the connected intermediate system.

Maintaining Access / Escalation of Privileges

The maintaining access phase is the point where an attacker tries to maintain access, ownership, and control over the compromised systems. The hacker usually strengthens the system in order to secure it from being accessed by security personnel or some other hacker. They use *Backdoors* , *Rootkits* or *Trojans* to retain their ownership. In this phase, an attacker may either steal information by uploading it to the remote server, download any file on the resident system, or manipulate the data and configuration settings. To compromise other systems, the attacker uses this compromised system to launch attacks.

Clearing Tracks

An attacker must hide his identity by clearing or covering tracks. Clearing tracks is an activity that is carried out to hide malicious activities. If

attackers want to fulfil their intentions and gain whatever they want without being noticed, it is necessary for them to wipe all tracks and evidence that can possibly lead to their identity. In order to do so, attackers usually overwrite the system, applications, and other related logs.

Ethical Hacking Concepts and Scope

Ethical Hacking

Ethical hacking and penetration testing are common terms and have been popular in information security environment for a long time. The increase in cybercrimes and hacking has created a great challenge for security experts, analysts, and regulations over the last decade. The virtual war between hackers and security professionals has become very common.

Fundamental challenges faced by security experts include finding weaknesses and deficiencies in running upcoming systems, applications, or software and addressing them proactively. It is less costly to investigate before an attack occurs than investigating after facing an attack, or while dealing with an attack. For the purpose of security and protection, organizations appoint internal teams as well as external experts for penetration testing. This usually depends on the severity and scope of the attack.

Why Ethical Hacking is Necessary

The rising number of malicious activities and cybercrimes and appearance of different forms of advanced attacks has created the need for ethical hacking. An ethical hacker penetrates security of systems and networks in order to determine their security level and advise organizations to take precautions and remediation actions against aggressive attacks. These aggressive and advanced attacks include:

- Denial-of-Services Attacks
- Manipulation of Data
- Identity Theft
- Vandalism

- Credit Card Theft
- Piracy
- Theft of Services

The increase in these types of attacks, hacking cases, and cyber attacks is mainly due to the increase in the use of online transactions and online services over the last decade. It has become much easier for hackers to steal financial information. Cybercrime law has only managed to slow down prank activities, whereas real attacks and cybercrimes have risen. Ethical hacking focuses on the requirement of a pen-tester, penetration tester in short, who searches for vulnerabilities and flaws in a system before it is compromised.

If you want to win in the war against attackers or hackers, you have to be smart enough to think and act like them. Hackers are extremely skilled and they possess great knowledge of hardware, software, and exploration capabilities. Therefore, ethical hacking has become essential. An ethical hacker is able to counter malicious hackers' attacks by anticipating their methods. Ethical hacking is also needed to uncover the vulnerabilities in systems and security controls to secure them before they are compromised.

Scope and Limitations of Ethical Hacking

Ethical Hacking is an important and crucial component of risk assessment, auditing, and of countering fraud. Ethical hacking is widely used as penetration testing to identify vulnerabilities and risks and highlight loopholes in order to take preventive action against attacks. However, there are some limitations to ethical hacking. In some cases, ethical hacking is insufficient for resolving the issue. For example, before hiring an external pentester, an organization must first figure out what it is looking for. This helps in achieving goals and saving time, as then the testing team can focus on troubleshooting the actual problem and resolve the issues. The ethical hacker also helps to understand the security system of an organization better. It is up to the organization to take the action recommended by the pentester and enforce security policies over the system and network.

Phases of Ethical Hacking

Ethical Hacking is the combination of the following phases:

1. Footprinting and Reconnaissance
2. Scanning
3. Enumeration
4. System Hacking
5. Escalation of Privileges
6. Covering Tracks

Skills of an Ethical Hacker

An expert ethical hacker has a set of technical and non-technical skills, as outlined below:

Technical Skills

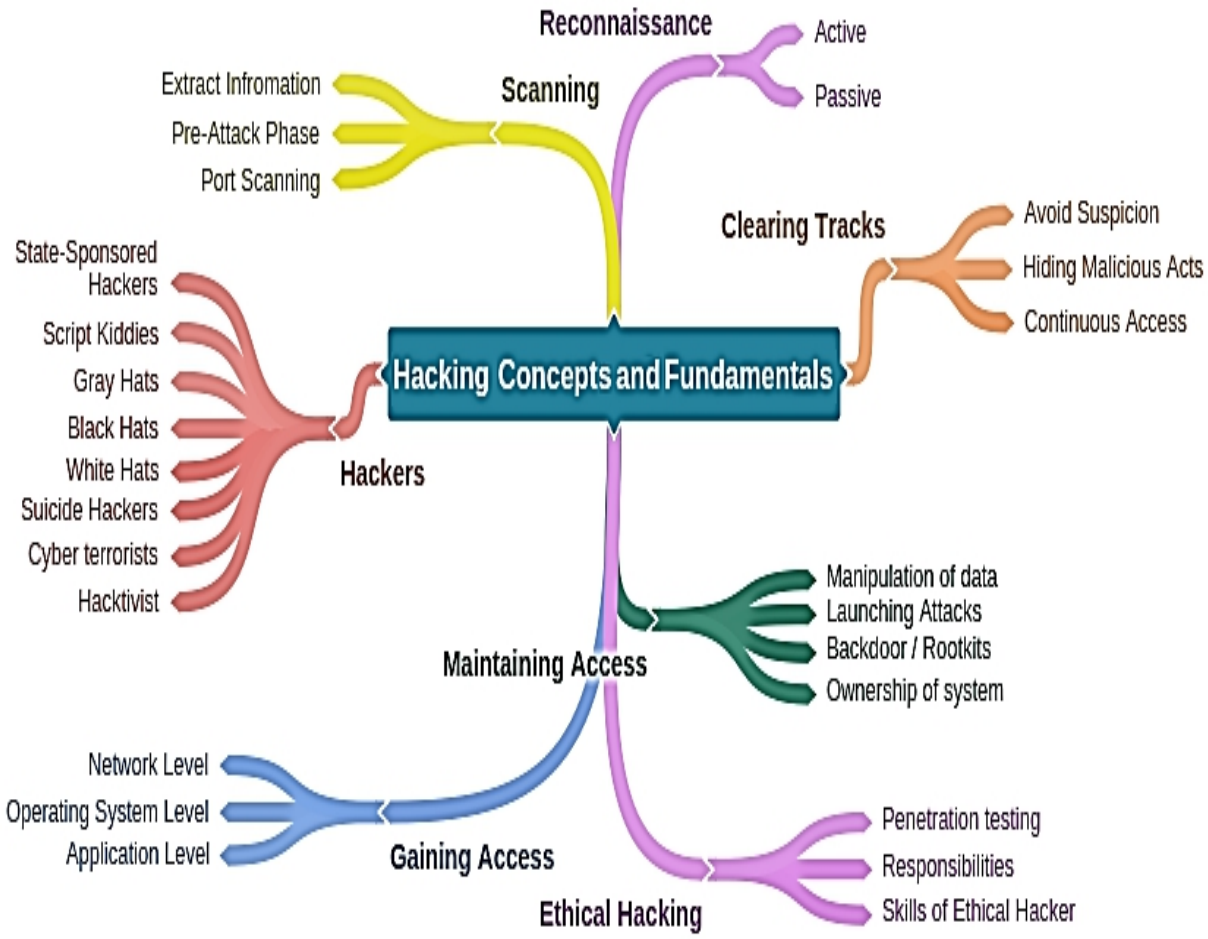
1. Ethical Hackers have in-depth knowledge of almost all Operating Systems, including all popular, widely-used OSes such as Windows, Linux, Unix, and Macintosh.

2. Ethical hackers are skilled at networking, basic and detailed concepts, technologies, and exploring capabilities of hardware and software.
3. Ethical hackers have a strong command over security areas, information security related issues, and technical domains.
4. They must have detailed knowledge of all older, advanced and sophisticated attacks.

Non-Technical Skills

1. Learning ability
2. Problem-solving skills
3. Communication skills
4. Committed to security policies
5. Awareness of laws, standards, and regulations

Mind Map



Information Security Controls
Information Assurance (IA)

Information Assurance, in short IA, depends upon Integrity, Availability, Confidentiality, and Authenticity. Combining these components guarantees the assurance of information and information systems and their protection during usage, storage, and communication. These components have already been defined earlier in this chapter.

Apart from these components, some methods and processes also help in the achievement of information assurance, for example:

- Policies and Processes
- Network Authentication
- User Authentication

- Network Vulnerabilities
- Identifying Problems
- Implementation of a Plan for Identified Requirements
- Enforcement of IA Contro

Information Security Management Program

Information Security Management programs are specially designed to focus on reducing the risks and vulnerabilities concerning the information security environment. This is done in order to train organizations and users to work in less vulnerable states. Information Security Management is a combined management solution to achieve the required level of information security using well-defined security policies as well as processes of classification, reporting, and management standards. The diagram below shows the EC-Council defined Information Security Management Framework:

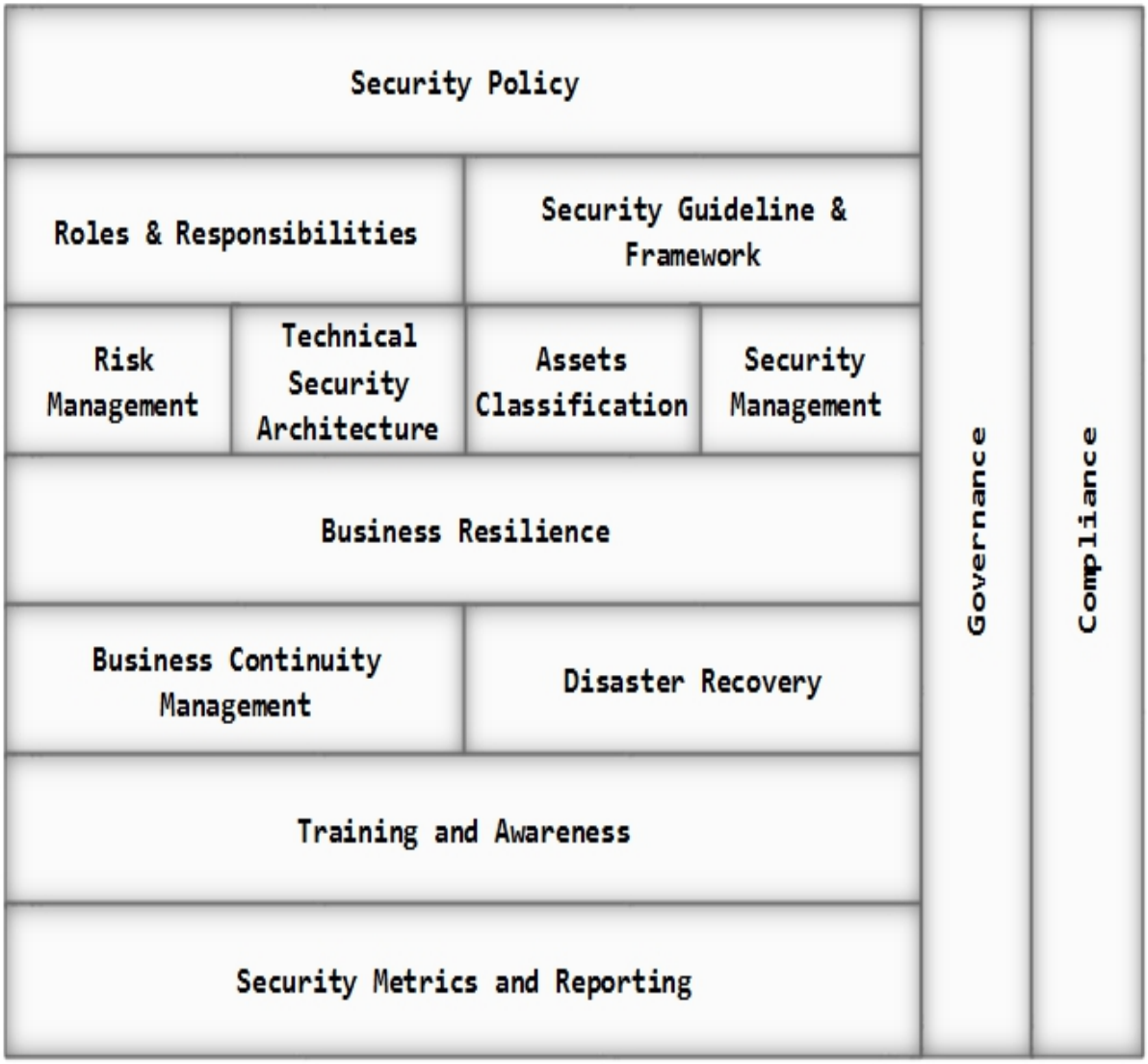


Figure 1-07: Information Security Management Framework

Threat Modeling

Threat Modeling is the process or approach to identifying, diagnosing, and assessing the threats and vulnerabilities of a system or application. It is an approach of threat assessment dedicated to focussing on analyzing the systems and applications while considering the security objectives. This identification of threats and risks helps to validate security and enables an organization to take remedial action to achieve the specified objectives of the application. The process of Threat Modeling includes capturing data, and implementing the controls for identification and assessment of the captured packets to analyze the

impact in case of compromise. Application overview includes the identification process of an application to determine the trust boundaries and data flow. Decomposition of an application and identification of threats helps to create a detailed review of threats that are breaching the security control. This identification and detailed review of every aspect exposes the vulnerabilities and weaknesses of the information security environment.

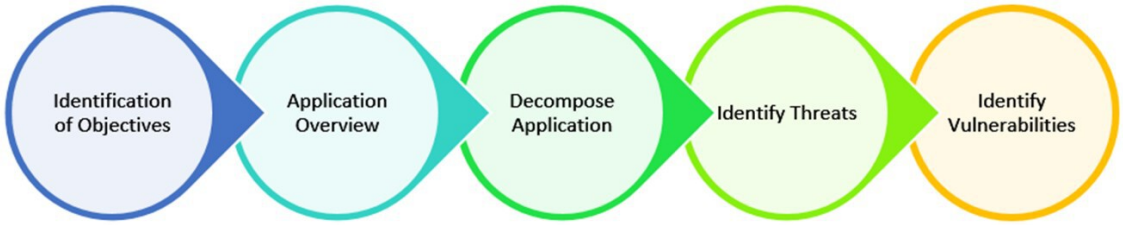


Figure 1-08: Threat Modeling

Enterprise Information Security Architecture (EISA)

Enterprise Information Security Architecture is the combination of requirements and processes that helps in determining, investigating, and monitoring the structure of the behavior of an information system. The following are the goals of EISA:

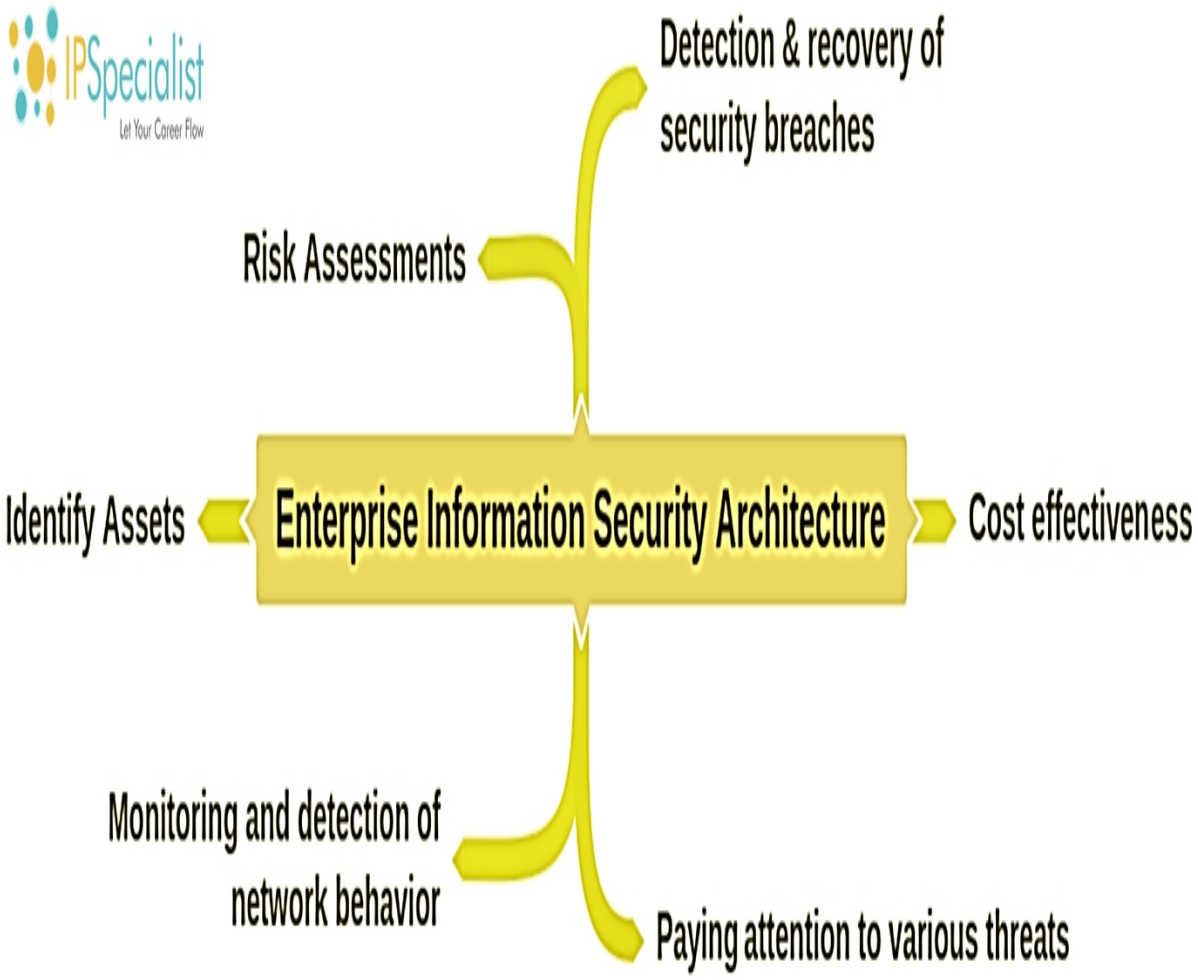


Figure 1-09: Enterprise Information Security Architecture (EISA)

Network Security Zoning

Managing and deploying an organization's architecture in different security zones is called Network Security Zoning. These security zones are a set of network devices with a specific security level. Different security zones may have a similar or different security level. Defining different security zones with their security levels helps in monitoring and controlling inbound and outbound traffic across the network.

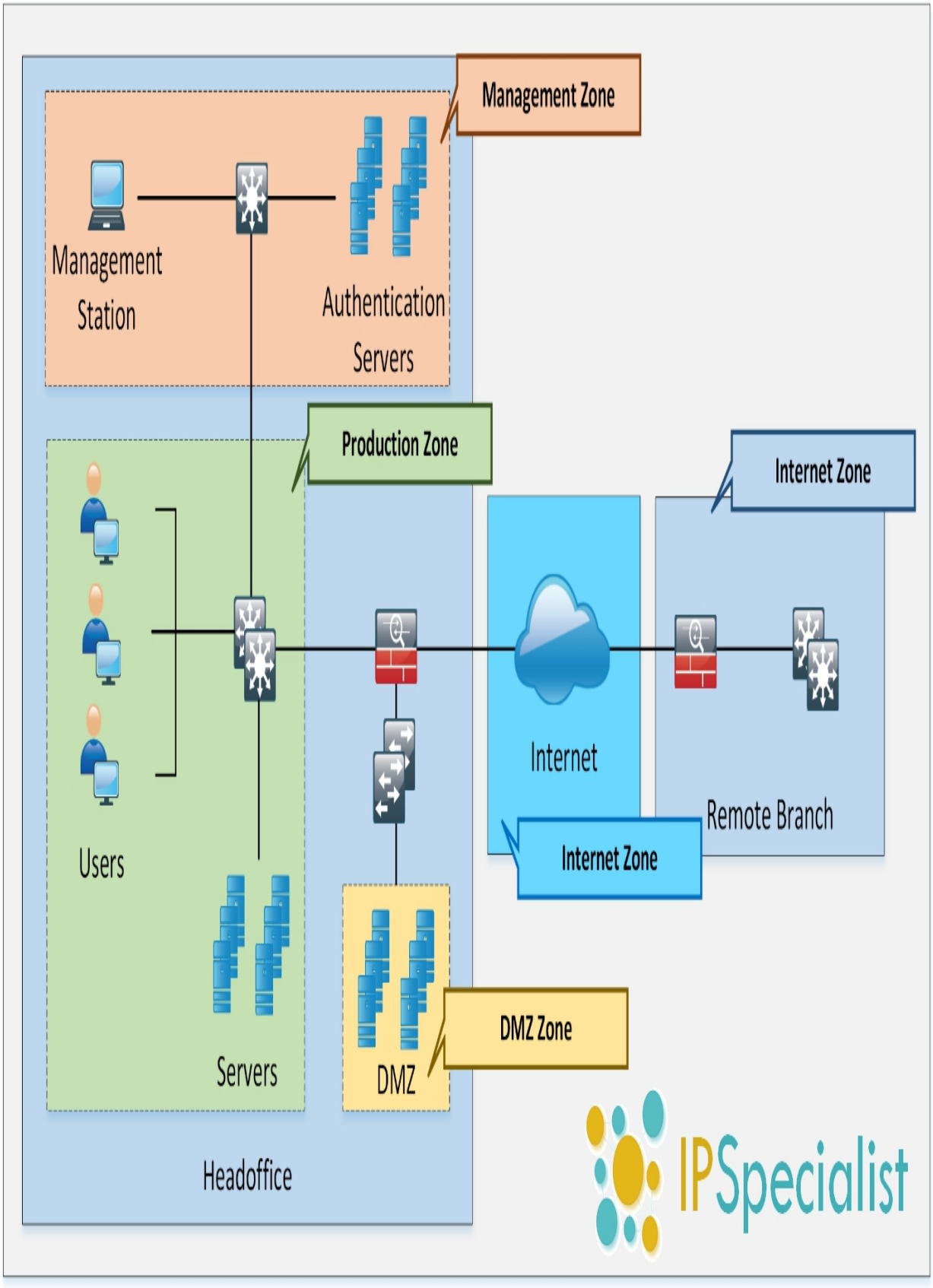


Figure 1-10: Network Security Zoning

Figure 1-10: Network Security Zoning

Information Security Policies

Information Security Policies are the fundamental and most dependent component of any information security infrastructure. Fundamental security requirements, conditions, and rules are configured to be enforced in an information security policy to secure the organization's resources. These policies cover the outlines of management, administration and security requirements within an information security architecture.

Note: Information Security Policy (ISP) is the set of rules and policies for users or employees to comply with issued by an organization.

1- Risk Assessment	2- Guidelines	3- Management
Identify risk	Learn standards	Include senior management / related staff
4- Penalties	**5- Finalization**	**6- Agreement**
Set penalties	Ready final version	Ensure everyone has agreed & understood
7- Enforcement	**8- Training**	**9- Review / Update**
Deploy the policy	Train the employees	Regular review, Update

Figure 1-11: Steps to Enforce Information Security

The basic goals and objectives of Information Security Policies are: • Cover security requirements and conditions of the organization • Protect the organization's resources
- Eliminate legal liabilities
- Minimize the wastage of resources
- Prevent unauthorized access/modification etc.
- Minimize risks
- Information Assurance

Types of Security Policies

The different types of security policies are as follows:
1. Promiscuous Policy
2. Permissive Policy
3. Prudent Policy
4. Paranoid Policy

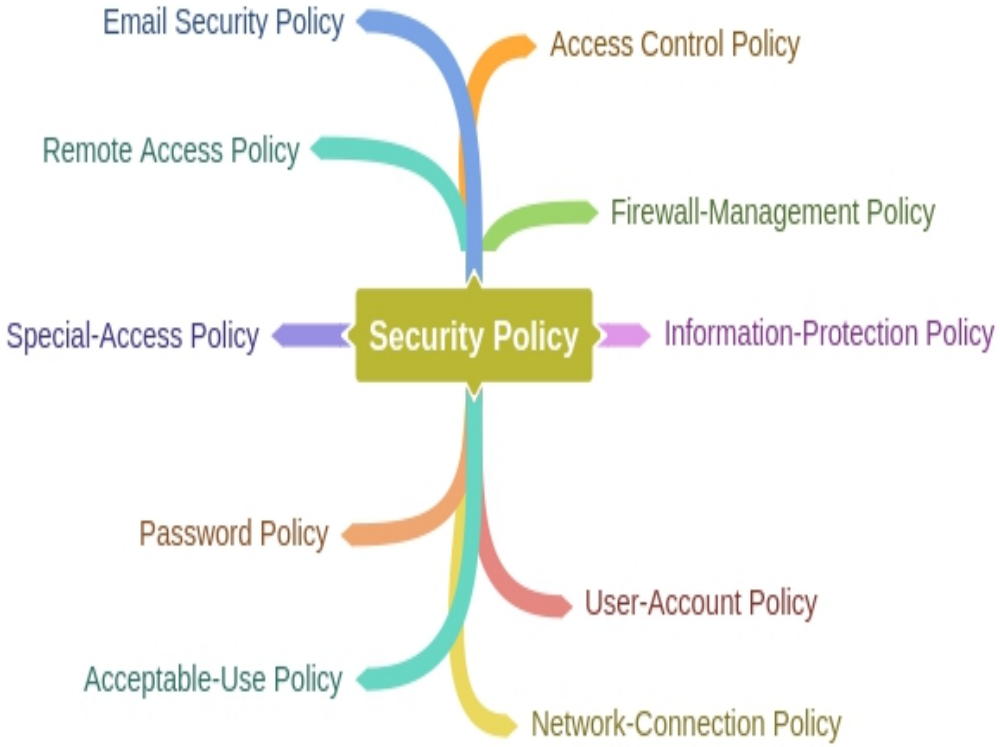
Promiscuous Policy
The Promiscuous Policy provides for no restriction on the usage of system resources.

Permissive Policy
The Permissive Policy restricts only widely known dangerous attacks or behaviors.

Prudent Policy

The Prudent Policy ensures the maximum and strongest security of all the policies. However, it allows known and necessary risks while blocking all other services except individually enabled services. Every event is logged in a prudent policy.

Paranoid Policy
Paranoid Policy denies everything and limits internet usage.



Implications for Security Policy Enforcement

HR & Legal Implication of Security Policies

The Human Resources department has the responsibility of making sure that the organization is aware of security policies and is providing sufficient training. With the cooperation of management or the administration within an organization, the HR department monitors the enforcement of security policies and deals with any violation issues that arise during deployment.

Legal implication of security policies is enforced under the supervision of professionals. These professionals are legal experts and consultants who comply with laws, especially local laws and regulations. Any violation of legal implication leads to lawsuits against those responsible.

Physical Security

Physical Security is always the top priority in securing anything. In Information Security, it is also considered important and regarded as the

first layer of protection. Physical security includes protection against human-made attacks such as theft, damage, and unauthorized physical access as well as environmental impacts such as rain, dust, power failure, and fire.

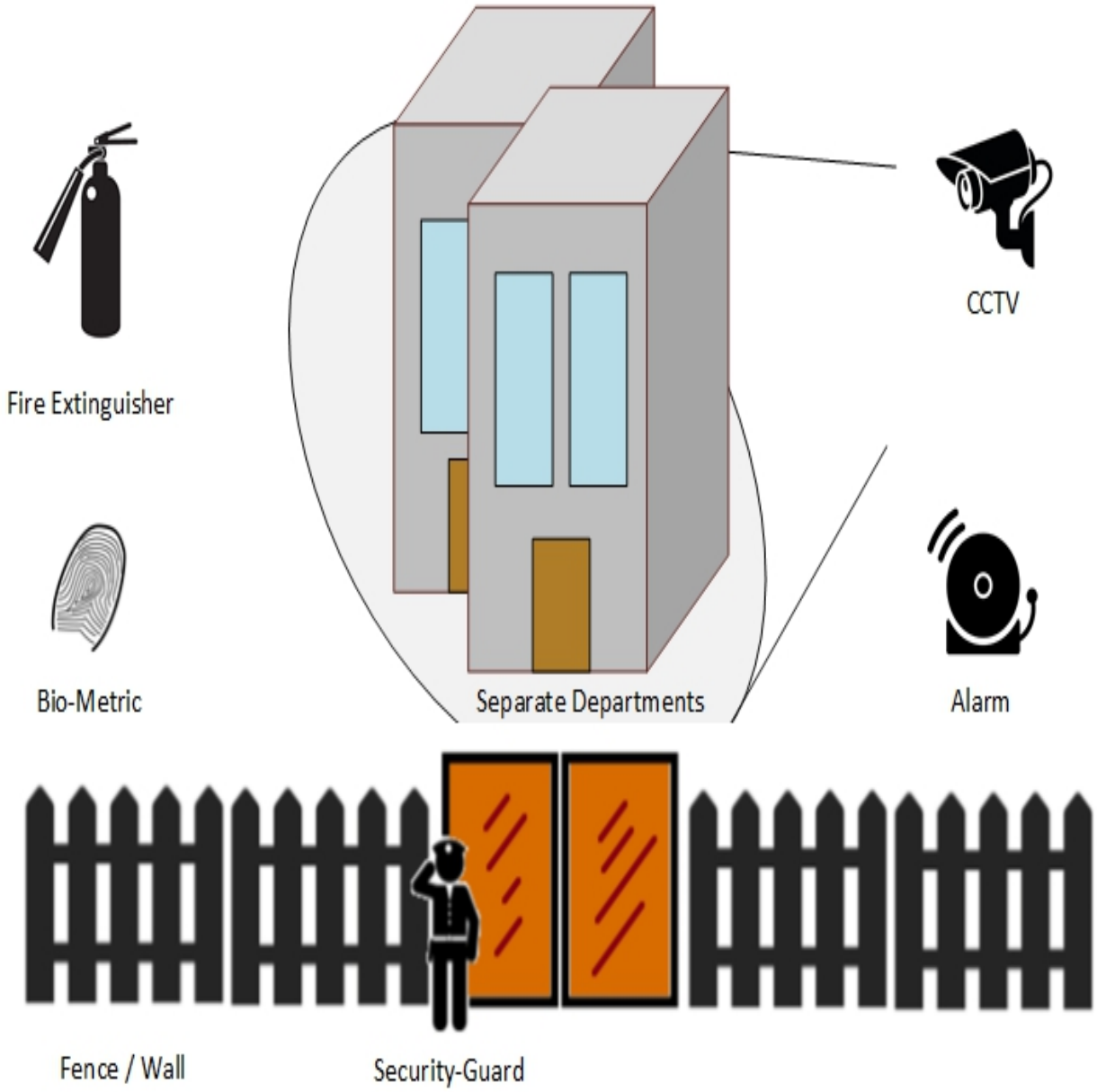


Figure 1-12: Physical Security

Physical security is required to prevent stealing, tampering, damage, theft, and many more physical attacks. To secure the premises and assets, fences, guards, CCTV cameras, intruder monitoring system, burglar alarms, and deadlocks are setup. Only authorized persons

should be allowed to access important files and documents. These files should not be left at any unsecured location, even within an organization. Functional areas must be separated and biometrically protected. Continuous or frequent monitoring such as monitoring of wiretapping, computer equipment, HVAC, and firefighting system should also be done.

Incident Management

Incident Response Management is the procedure and method of handling any incident that occurs. This incident may be a violation of any condition, policy, etc. Similarly, in information security, incident responses are the remediation actions or steps taken as the response of an incident to make the system stable, secure, and functional again. Incident response management defines the roles and responsibilities of penetration testers, users or employees of an organization. Additionally, incident response management defines the action required to be taken when a system is facing a threat to its confidentiality, integrity, authenticity, and availability depending upon the threat level. Initially, the important thing to remember is when a system is dealing with an attack, it requires sophisticated and dedicated troubleshooting by an expert. While responding to an incident, the expert collects evidence, information, and clues that are helpful for prevention in future, tracing the attacker and finding loopholes and vulnerabilities in the system.

Incident Management Process

Incident Response Management processes include:

1. Preparation for Incident Response
2. Detection and Analysis of Incident Response
3. Classification of an incident and its prioritization
4. Notification and Announcements
5. Containment
6. Forensic Investigation of an Incident
7. Eradication and Recovery
8. Post-Incident Activities

Incident Response Team

An Incident Response team consists of members who are well-aware of how to deal with incidents. This response team consists of trained officials who are expert in gathering information and securing all evidence of an attack collected from the incident system. An Incident Response team is made up of IT personnel, HR, Public Relations officers, local law enforcement, and a chief security officer.

Responsibilities of an Incident Response Team

• The major responsibility of this team is to take action according to the Incident Response Plan (IRP). If an IRP is not defined or not applicable to that case, the team has to follow the leading examiner to perform a coordinated operation

• Examine and evaluate an event, determine the damage or scope of an attack • Document the event and processes
• If required, get the support of an external security professional or consultant • If required, get the support of local law enforcement
• Collection of facts
• Report

Mind Map

Vulnerability Assessment

Vulnerability assessment is the procedure of examining, identifying, and analyzing the ability of a system or application, including security processes running on a system, to withstand any threat. Through vulnerability assessment, you can identify weaknesses in a system, prioritize vulnerabilities, and estimate the requirement and effectiveness of any additional security layer.

Types of Vulnerability Assessment

Following are the types of vulnerability assessment:

1. Active Assessment
2. Passive Assessment
3. Host-based Assessment
4. Internal Assessment

5. External Assessment
6. Network Assessment
7. Wireless Network Assessment

Application Assessment Network Vulnerability Assessment Methodology

Network Vulnerability Assessment is an examination of possibilities of an attack and vulnerabilities in a network. The following are the phases of a Network Vulnerability Assessment:

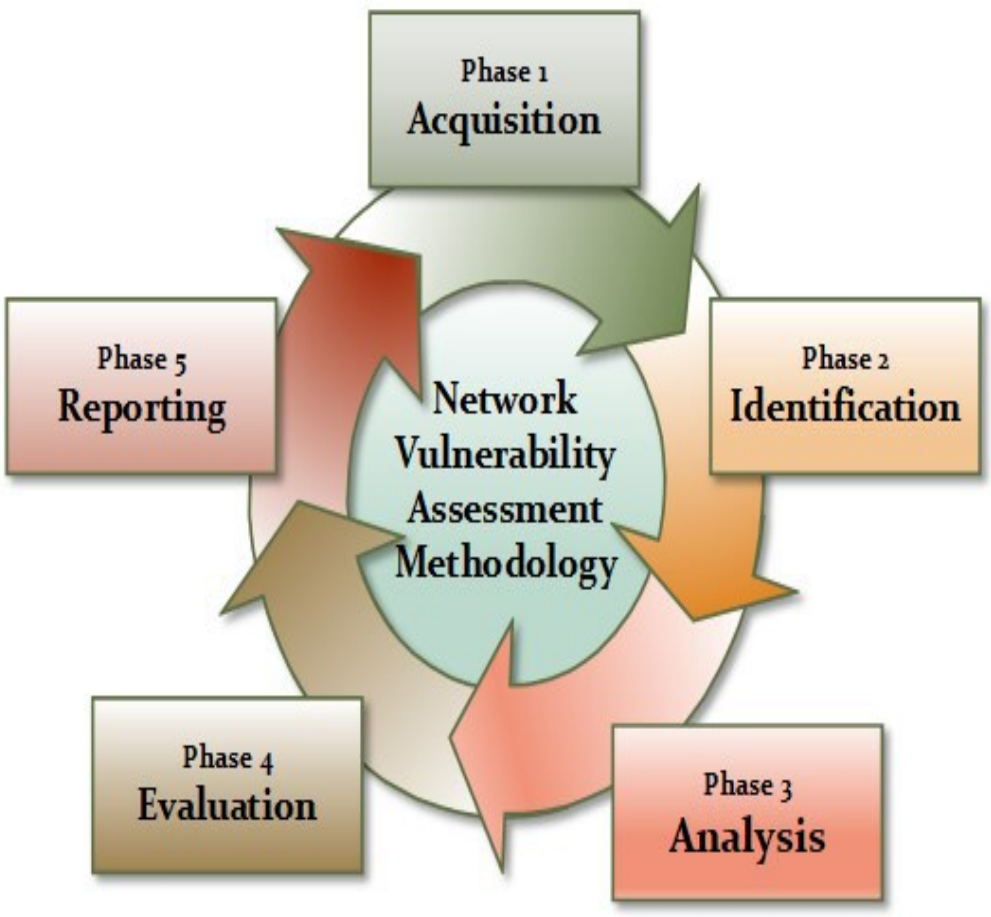


Figure 1-13: Network Vulnerability Assessment Methodology

Acquisition

The Acquisition phase compares and reviews previously-identified vulnerabilities, laws, and procedures that are related to network

vulnerability assessment.

Identification

In the Identification phase, interaction with customers, employees, administration, or other people involved in designing the network architecture to gather the technical information.

Analysis

The Analysis phase reviews the gathered information. It basically consists of:

- Reviewing information
- Analyzing the results of previously identified vulnerabilities
- Risk assessment
- Vulnerability and risk analysis
- Evaluating the effectiveness of existing security policies

Evaluation

The Evaluation phase includes:

- Inspection of identified vulnerabilities

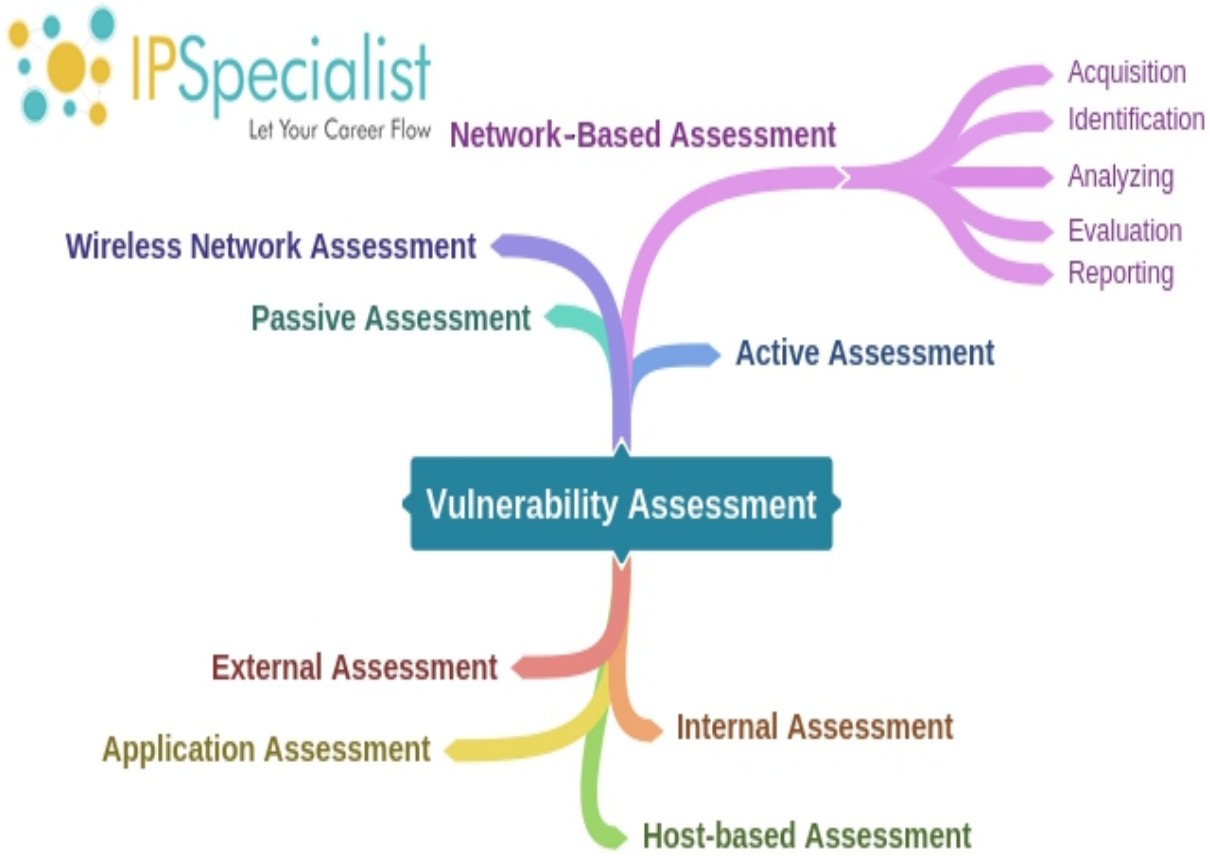
- Identification of flaws, gaps in an existing network, and required security considerations in a network design
- Determination of security controls required to resolve issues and vulnerabilities • Identifion of the required modification and upgrades

Generating Reports

In the Reporting phase, reports are drafted for documenting the security event, and for presenting them to higher authorities such as a security manager, board of directors, or others. This documentation is also helpful for future inspection. This report helps to identify vulnerabilities in the acquisition phase. Audit and Penetration also require these previously collected reports. When any modification in the security mechanism is required, these reports help to design the security infrastructure. Central databases usually hold these reports. Reports contain:

- Tasks completed by each member of the team
- Methods and tools used
- Findings
- Recommendations
- Gathered information

Mind Map



Penetration Testing Technology Overview

Penetration Testing is the process of hacking a system, with permission from the owner of that system, to evaluate security, Hack Value, Target of Evaluation (TOE), attacks, exploits, zero-day vulnerability, and other components such as threats, vulnerabilities, and daisy chaining. In the environment of Ethical Hacking, a pentester is an individual authorized by an owner to hack into a system to perform penetration testing.

The Importance of Penetration testing

In today's dynamic technological environment, denial-of-service, identity theft, theft of services, and theft of information have become the most common cybercrimes. System penetration is used to protect the system from such malicious threats by identifying vulnerabilities in it. Some other major advantages of penetration testing are:

- Identifying vulnerabilities in systems and security controls in the same way an attacker searches for and exploits vulnerabilities to bypass security
- Identifying the threats and vulnerabilities of an organization's assets
- Providing a comprehensive assessment of policies, procedures, design, and architecture
- Setting remedial actions before a hacker identifies and breaches security
- Identifying what an attacker can access to steal
- Identifying the value of information
- Testing and validating the security controls and identifying the need for any additional protection layer
- Modifying and up-grading currently deployed security architecture
- Reducing the expense of IT Security by enhancing Return on Security Investment (ROSI)

Vulnerability Assessment and Penetration Testing (VAPT) is needed because it protects us from harm, secures us from intrusion, keeps our confidential data confidential, and conceals our information from prying eyes. Every corporate manager or network administrator needs to know their weak points so they can address them. We all know that networks are vulnerable, but we do not all know where and how; this is where vulnerable assessment comes in.

It is a comprehensive check of physical weaknesses in computers and networks. It identifies potential risks and threats at any exposure and develops strategies for dealing with them.

"Prevention is better than cure".
Another reason for VAPT is to prevent hacking incidents. We are very

much aware of hacks such as the loss of:

- Sensitive data
- Account numbers
- Email addresses
- Personal information

These security incidents happen every day in the world of computer networking. This is why you need to look at your network from the outside and see it as an attacker would see it. Learn its strengths, its weaknesses and then plug the gaps. Your infrastructure may be secure, your servers may lock down the firewall on strong policies, but what about the default configuration of peripheral devices, for example the printers, scanners, fax machines, , etc. Your network is adorned with them and their vulnerability is often neglected. A vulnerability assessment and penetration testing would highlight any problems in seconds. Any network with users is not as secure as you might think. Protecting your network should be your priority. In summary, the reasons for performing VAPT are:

- To protect the network from attacks
- To learn its strengths and weaknesses
- To safeguard information from theft
- To comply with data security standards
- To add reliability and value to services

Security Audits

- Security audits are the evaluation of security controls. It makes sure that controls are being enforced and

followed properly throughout the
organization,
without any concern about the threats and vulnerabilities

Vulnerability Assessments

- Vulnerability
Assessment process is to identify

vulnerabilities and threats, which may exploit and impact an organization financially or
reputationally

Penetration Testing

• Penetration is the process of security assessment, which includes security audits and

vulnerability
assessment.
Furthermore, it demonstrates the attack, its solution and required remedial actions

Figure 1-14: Comparing Pentesting
Types of Penetration Testing It is important to understand the difference between the three types of Penetration Testing because a penetration tester might be asked to perform any one of them. *Black Box*

Black Box is a type of penetration testing in which the pentester is blind testing or double-blind testing. This means that the pentester has no prior knowledge of the system or any information of the target.

Gray Box

Gray Box is a type of penetration testing in which the pentester has very limited prior knowledge of the organization's network. For example, information related to the operating system or network might be very limited.

White Box

White Box is a type of penetration testing in which the pentester has complete information of the system and the target. This type of penetration testing is performed by internal security teams or security audit teams in order to carry out an audit.

Blue

• Blue team is responsible for analyzing security controls and efficiency of an information

Team

security system
• They detect and mitigate red team's attacks

Red

• Red team consists of pentesters and ethical hackers who are responsible for system

Team

penetration
• They find vulnerabilities and exploit them from
an attacker's perspective

Figure 1-15: A Comparison of Blue & Red Teaming

Phases of Penetration Testing

Penetration Testing is a three-phase process:

Penetration Testing is a three-phase process: Pre-Attack Phase
Pre-Attack Phase
Attack Phase
Attack Phase
Post-Attack Phase

Figure 1- 16: Penetration Testing Phases

Figure 1-16: Penetration Testing Phases

Security Testing Methodology

There are some methodological approaches to be adopted for security or penetration testing. Industry-leading Penetration Testing Methodologies are:

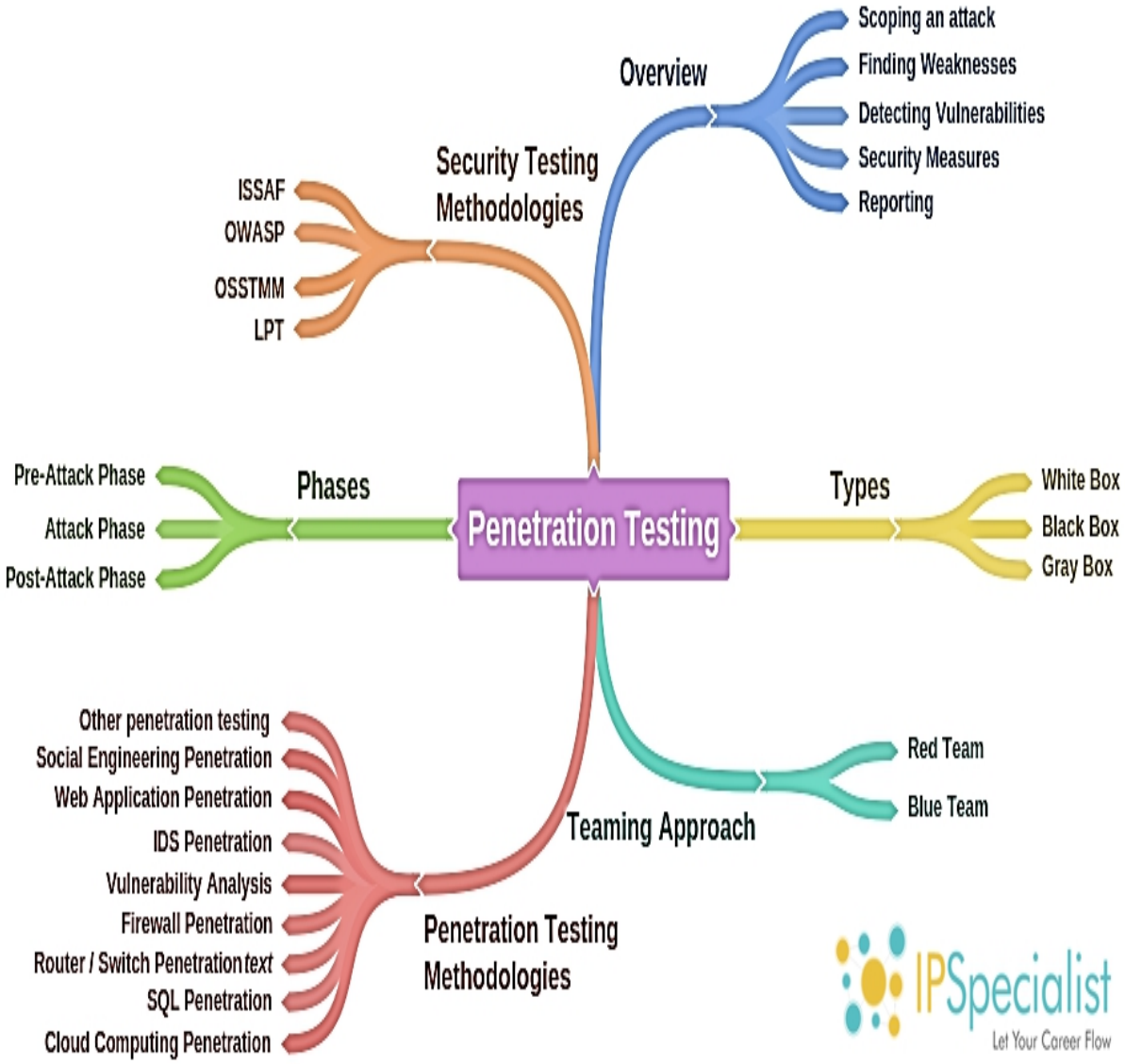
- Open Web Application Security Project (OWASP)
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISAF)
- EC-Council Licensed Penetration Tester (LPT) Methodology

Note: Python is popularly used but limited to penetration testing, information gathering, scripting tool, automating and forensics.

Open Source Security Testing Methodology Manual (OSSTMM) is a peer-reviewed manual of security testing and analysis whose results are verified facts. These facts provide actionable information that can measurably improve your operational security.

Common Criteria (CC) is an international set of guidelines and specification developed for evaluating information security products, specifically to ensure that they meet an agreed upon security standard for governmental deployment.

Mind Map



Information Security Laws and Standards
Payment Card Industry Data Security Standard (PCI-DSS)

Payment Card Industry Data Security Standard (PCI-DSS) is a global information security standard created by "*PCI Security Standards Council*". It was created for organizations to develop, enhance and assess security standards required for handling cardholder information and payment account security. The PCI Security Standards Council develops security standards for the payment card industry and provides

the tools required for enforcement of these standards such as training, certification, assessment, and scanning.

The founding members of this council are:

- American Express
- Discover Financial Services
- JCB International
- MasterCard
- Visa Inc.

PCI data security standard deals basically with cardholder data security for debit, credit, prepaid, e-purse, POS, and ATM cards. A high-level overview of PCI-DSS provides:

- Secure Network
- Strong Access Control
- Cardholder Data Security
- Regular Monitoring and Evaluation of Network • Maintaining Vulnerability Program
- Information Security Policy

ISO/IEC 2700 1:20 13

The International Organization for Standardization (ISO) and International ElectroTechnical Commission (IEC) are organizations that globally develop and maintain their standards. ISO/IEC 2700 1:20 13 standard ensures the requirement for implementation, maintenance, and improvement of an information security management system. This standard is a revised edition (second) of the first edition ISO/ISE 2700 1:2005. ISO/IEC 2700 1:20 13 covers the following key points of information security:

- Implementing and maintaining security requirements
- Information security management processes
- Assurance of cost effective risk management
- Status of information security management activities
- Compliance with laws

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996 by Congress. The HIPAA works with the Department of Health and Human Services (HHS) to develop and maintain a regulation that is associated with privacy and security of health information. It establishes the national standards and safeguards that must be implemented to secure electronic protected health information. The HIPAA also defines general rules for risk analysis and management of E-PHI. These rules include a series of administrative, physical, and technical security procedures to ensure the confidentiality, integrity, and availability of electronically protected health information (E-PHI).

The major domains in information security where the HIPAA is developing and maintaining standards and regulations are:

- Electronic Transaction and Code Sets Standards
- Privacy Rules
- Security Rules
- National Identifier Requirements
- Enforcement Rules

Sarbanes Oxley Act (SOX)

The key requirements or provisions of the Sarbanes Oxley Act (SOX) are organized in the form of 1 1 titles, and they are as follows:
Title Majors Title I Public company accounting oversight board Title II Auditor independence Title III Corporate responsibility Title IV Enhanced financial disclosures Title V Analyst conflicts of interest Title VI Commission resources and authority Title VII Studies and reports Title VIII Corporate and criminal fraud accountability Title IX White-collar crime penalty enhancements Title X Corporate tax returns Title XI Corporate fraud and accountability *Table 1-03: SOX Titles*

Some other regulatory bodies are offering standards that are being deployed worldwide, including the Digital Millennium Copyright Act (DMCA) and the Federal Information Security Management Act (FISMA). The DMCA is the United States' copyright law— whereas, The FISMA is a framework for ensuring the effectiveness of information security

control. According to Homeland Security, FISMA 20 14 codifies the Department of Homeland Security's role in administering the implementation of information security policies for Federal Executive Branch civilian agencies, overseeing agencies' compliance with those policies, and assisting OMB in developing those policies. The legislation provides the Department with the authority to develop and oversee the implementation of binding operational directives to other agencies, in coordination and consistence with OMB policies and practices. The Federal Information Security Modernization Act of 20 14 amends the Federal Information Security Management Act of 2002 (FISMA).

Industry Standard Framework and Reference Architecture

Industry standard framework and reference architecture can be referred to as a conceptual model that describes the operation and structure of the IT system in any organization.

Regulatory

The business processes and procedures that are compliance related are known as Regulatory bodies. There are some rules and regulations that are required to be followed for performing specific functions. For example, public companies deal with a lot of Sarbanes Oxley (SOX) regulation.

Non-Regulatory

Some processes in an organization are not compliance concerned, which means that there is no rule of law required to perform a particular function. NIOSH (National Institute for Occupational Safety and Health), for example, is a non-regulatory body.

National vs International There are a lot of national instructions and practices for and international frameworks

information security. FISMA that provide proper (Federal Information

Security Management Act) is the United States' law developed for the protection of government data and resources against dreadful threats.

Industry-Specific Framework

The Industry-Specific Framework has been formed by bodies within a specific industry for addressing regulatory requirements or because of industry-specific risks or concerns. Examples of Industry-Specific Framework are HITRUST Common Security Framework (CSF) and COBIT (Control Objectives for Information and Related Technologies).

Benchmarks/Secure Configuration Guides

When Operating Systems, database servers, web servers, or other technologies are installed, they are far away from the secured configuration. Systems with default configuration are not secure. Some guidelines are needed to keep everything safe and secure.

Platform-Specific Guide

The Platform-Specific Guide is the finest guide to come from the manufacturer of each device. This guide includes all the essential principles regarding installation, configuration, and sometimes operations as well.

Mind Map

Note:

Payment Card Industry Data Security Standards (PCI DSS): The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures intended to optimize the security of credit, debit, and cash card transactions and protect cardholders against misuse of their personal information.

Sarbanes-Oxley Act: The Sarbanes-Oxley Act is designed to oversee the financial reporting landscape for finance professionals. Its purpose is to review legislative audit requirements and to protect investors by improving the accuracy and reliability of corporate disclosures.

Practice Questions:

1. Which of the following does an Ethical Hacker require to penetrate a system? A. Training
B. Permission
C. Planning
D. Nothing

2. What is Gray Box Pentesting?
A. Pentesting with no knowledge B. Pentesting with partial knowledge
C. Pentesting with complete knowledge D. Pentesting with permission

3. If you have been hired to perform an attack against a target system to find and exploit vulnerabilities, what type of hacker are you?
A. Gray Hat
B. Black Hat
C. White Hat
D. Red Hat

4. Which of the following describes an attacker who goes after a target to draw attention to a cause?
A. Terrorist
B. Criminal
C. Hacktivist

D. Script Kiddie
5. What is the level of knowledge does a Script Kiddie have?
A. Low
B. Average
C. High
D. Advanced

6. A White Box test requires: A. No knowledge
B. Some knowledge C. Complete knowledge D. Permission

7. Which of the following describes a hacker who attacks without regard for being caught or punished?
A. Hacktivist
B. Terrorist
C. Criminal
D. Suicide Hacker

8. A penetration test is required for which of the following reasons? (Choose 2) A. Troubleshooting network issues
B. Finding vulnerabilities
C. To perform an audit
D. To monitor performance

9. Hacker using their skills for both benign and malicious goals at different times are:
A. White Hat
B. Gray Hat
C. Black Hat
D. Suicide Hacker

10. Vulnerability analysis is basically:
A. Monitoring for threats
B. Disclosure, scope & prioritization of vulnerabilities C. Defending techniques from vulnerabilities D. Security application

11. What is Black Box testing?
A. Pentesting with no knowledge B. Pentesting with complete