Chapter 1: Introduction to Ethical Hacking

Technology Brief

Information Security Overview

The methods and processes to protect information and information systems from unauthorized access, the disclosure of information, usage or modification. Information security ensures the confidentiality, integrity, and availability. An organization without security policies and appropriate security rules are at great risk, and the confidential information and data related to that organization are not secure in the absence of these security policies. An organization along with well-defined security policies and procedures helps in protecting the assets of that organization from unauthorized access and disclosures. In the modern world, with the latest technologies and platforms, millions of users interacting with each other every minute. These sixty seconds can be vulnerable and costly to the private and public organizations due to the presence of various types of old and modern threats all over the world. Public internet is the most common and rapid option for spreading threats all over the world. Malicious Codes and Scripts, Viruses, Spams, and Malware are always waiting for you. That is why the Security risk to a network or a system can never eliminate. It is always a great challenge to implement a security policy that is effective and beneficial to the organization instead of the application of an unnecessary security implementation which can waste the resources and create a loophole for threats. Our Security objectives are surrounding these three basic concepts:

Data Breach

eBay Data Breach

One of the real-life examples describing the need for information and network security within the corporate network is eBay data breach. eBay is well-known online auction platform that is widely used all over the world.

eBay announced its massive data breach in 2014 which contained sensitive data. 145 million customers were estimated having data loss in this attack. According to eBay, the data breach compromised the following information including:

- Customers' names
- Encrypted passwords
- Email address
- Postal Address
- Contact Numbers
- Date of birth

These sensitive information must be stored in an encrypted form that uses strong encryption. Information must be encrypted, instead of being stored in plain text. eBay claims that no information relating to Security numbers like credit cards information was compromised, although identity and password theft can also cause severe risk. eBay database containing financial information such as credit cards information and other financial related information are claimed to be kept in a separate and encrypted format.

The Origin of eBay data breach for hackers is by compromising a small number of employees credentials via phishing in between February & March 2014. Specific employees may be targeted to get access to eBay's network or may eBay network was entirely being monitored and then compromised. They claimed detection of this cyberattack within two weeks.

Google Play Hack

A Turkish Hacker, "**Ibrahim Balic**" hacked Google Play twice. He conceded the responsibility of the Google Play attack. It was not his first attempt; he acclaimed that he was behind the Apple's Developer site attack. He tested vulnerabilities in Google's Developer Console and found a flaw in the Android Operating System, which he tested twice to make sure about it causing crash again and again.

Using the result of his vulnerability testing, he developed an android application to exploit the vulnerability. 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

Theft of information from payment cards, like credit cards is common nowadays. In 2014, Home Depot's Point of Sale Systems were compromised. A released statement from Home Depot on the 8th of September 2014 claimed breach of their systems.

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

Home Depot has taken several remediation actions against the attack, using EMV Chip-&-Pin payment cards. These Chip-& Pin payment cards has a security chip embedded into it to ensure duplicity with magstripe.

Essential Terminology

Hack Value

The term Hack Value refers to a value that denotes attractiveness, interest or something that is worthy. Value describes the targets' level of attraction to the hacker.

Zero-Day Attack

Zero-Day Attacks referrs to threats and vulnerabilities that can exploit the victim before the developer identify or address and release any patch for that vulnerability.

Vulnerability

The vulnerability refers to a weak point, loophole or a cause in any system or network which can be helpful and utilized by the attackers to go through it. Any vulnerability can be an entry point for them to reach the target.

Daisy Chaining

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

Exploit

Exploit is a breach of security of a system through Vulnerabilities, Zero-Day Attacks or any other hacking techniques.

Doxing

The term Doxing referrs to Publishing information or a set of information associated with an individual. This information is collected publicly, mostly from social media or other sources.

Payload

The payload referrs 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 the potentially harmful activity and actions such as exploit, opening backdoors, and hijacking.

Bot

The bots are software that is used to control the target remotely and to execute predefined tasks. It is capable to run automated scripts over the internet. The bots are also known as for Internet Bot or Web Robot. These Bots can be used for Social purposes such as Chatterbots, Commercial purpose or intended Malicious Purpose such as Spambots, Viruses, and Worms spreading, Botnets, DDoS attacks.

Elements of Information Security

Confidentiality

We want to make sure that our secret and sensitive data is secure. Confidentiality means that only authorized persons 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: data in motion as it moves across the network and data at rest, when data is in any media storage (such as servers, local hard drives, cloud). For data in motion, we need to make sure data encryption before sending it over the network. Another option we can use along with encryption is to use a separate network for sensitive data. For data at rest, we can apply encryption at storage media drive so that no one can read it in case of theft.

Integrity

We do not want our data to be accessible or manipulated by unauthorized persons. Data integrity ensures that only authorized parties can modify data.

Availability

Availability applies to systems and data. If authorized persons cannot get the data due to general network failure or denial-of-service(DOS) attack, then that is the problem as long as the business is concerned. It may also result in loss of revenues or recording some important results.

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

CIA	Risk	Control
Confidentiality	Loss of privacy. Unauthorized access to information. Identity theft.	Encryption. Authentication. Access Control
Integrity	Information is no longer reliable or accurate. Fraud.	Maker/Checker. Quality Assurance. Audit Logs
Availability	Business disruption. Loss of customer's confidence. Loss of revenue.	Business continuity. Plans and test. Backup storage. Sufficient capacity.

Table 1-01: Risk and Its Protection by Implementing CIA

Authenticity

Authentication is the process which identifies the user, or device to grant privileges, access and certain rules and policies. Similarly, Authenticity ensures the authentication of certain information initiates from a valid user claiming to be the source of that information & message transactions. The process of authentication through the combined function of identities and passwords can achieve Authenticity.

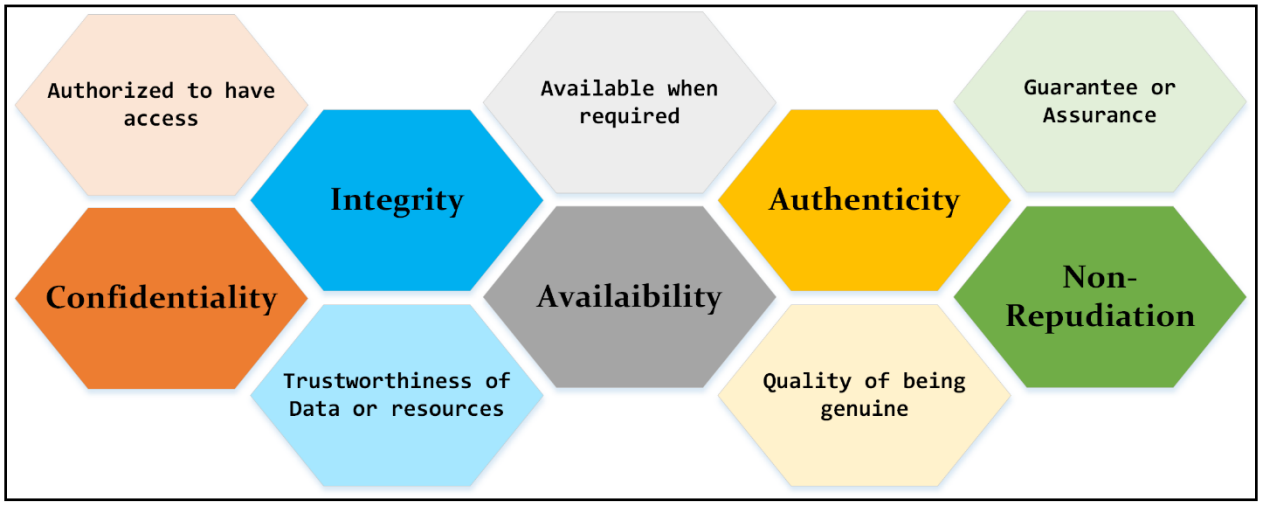


Figure 1-1 Elements of Information Security

Non-Repudiation

Nonrepudiation is one of the Information Assurance (IA) pillar which guarantees the information transmission & receiving between the sender and receiver via different techniques such as digital signatures and encryption. Non-repudiation is the assurance the communication and its authenticity, so the sender cannot deny from what he sent. Similarly, the receiver cannot deny from receiving. Digital contracts, signatures and email messages use Nonrepudiation techniques.

The Security, Functionality, and Usability Triangle

In a System, Level of Security is a measure of the strength of the Security in the system, Functionality, and Usability. These three components are known as the Security, Functionality and Usability triangle. Consider a ball in this triangle, if the ball is centered, 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 feature and function of the system and Usability requires attention. A secure system must provide strong protection along with offering all services and features and usability to the user.

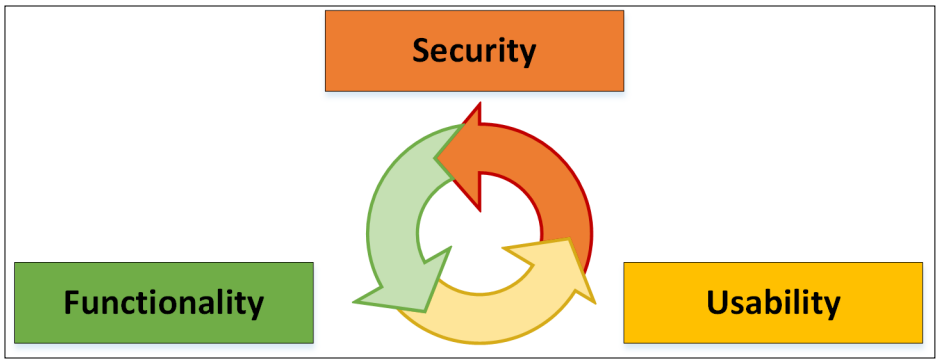


Figure 1-2 Security, Functionality & Usability Triangle

Implementation of High level of Security typically impacts the level of functionality and usability with ease. The system becomes nonuser-friendly with a decrease in performance. While developing an application, deployment of security in a system, Security experts must keep in mind to make sure about functionality & ease of usability. These three components of a triangle must be balanced.

Information Security Threats and Attack Vectors

Motives, Goals, and Objectives of Information Security Attacks

In the information security world, an attacker attacks the target system with the three main components behind it. "Motive or Objective" of an attack makes an attacker focus on attacking a particular system. Another major component is "Method" that is used by an attacker to gain access to a target system. Vulnerability also helps the attacker to fulfill his intentions. These three components are the major blocks on which an attack depends.

Motive and Objective of an attacker to attack a system may depend upon something valuable stored in that specific system. The reason might be ethical or non-ethical. However, there must be a goal to achieve for the hacker, which leads to the threat to the system. Some typical motives of behind attacks are information theft, Manipulation of data, Disruption, propagation of political or religious beliefs, attack on target's reputation or taking revenge. Method of attack & Vulnerability runs side by side. Intruder applies various tools and number of advanced & older techniques to exploit a vulnerability within a system, or security policy to breach & achieve their motives.

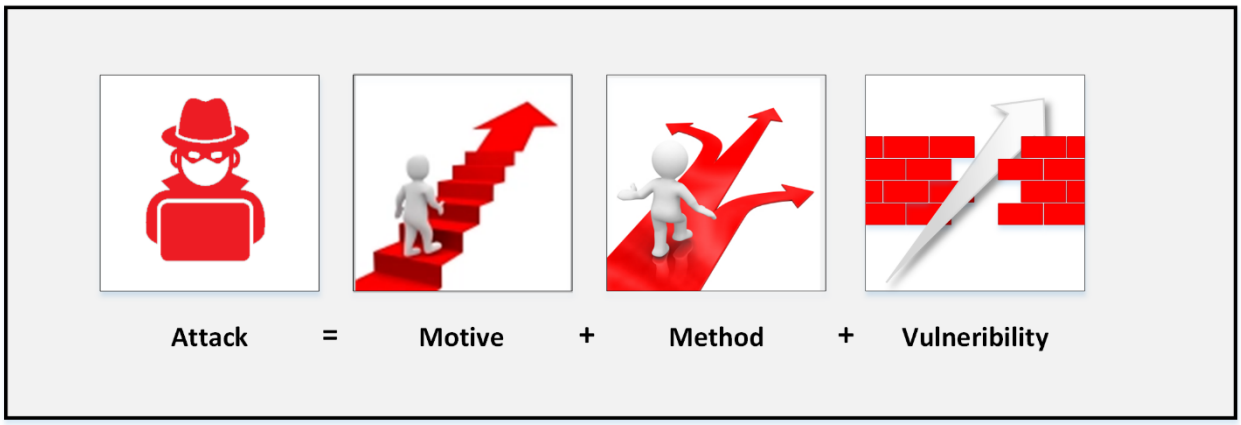


Figure 1-3 Information Security Attack

Top Information Security Attack Vectors

Cloud Computing Threats

Cloud Computing is the most common trend & popularly in use nowadays. It does not mean that threats to cloud computing or cloud security are fewer. Mostly, the same issues

as in traditionally hosted environments also exist in the cloud computing. It is very important to secure Cloud computing to protect services and important data.

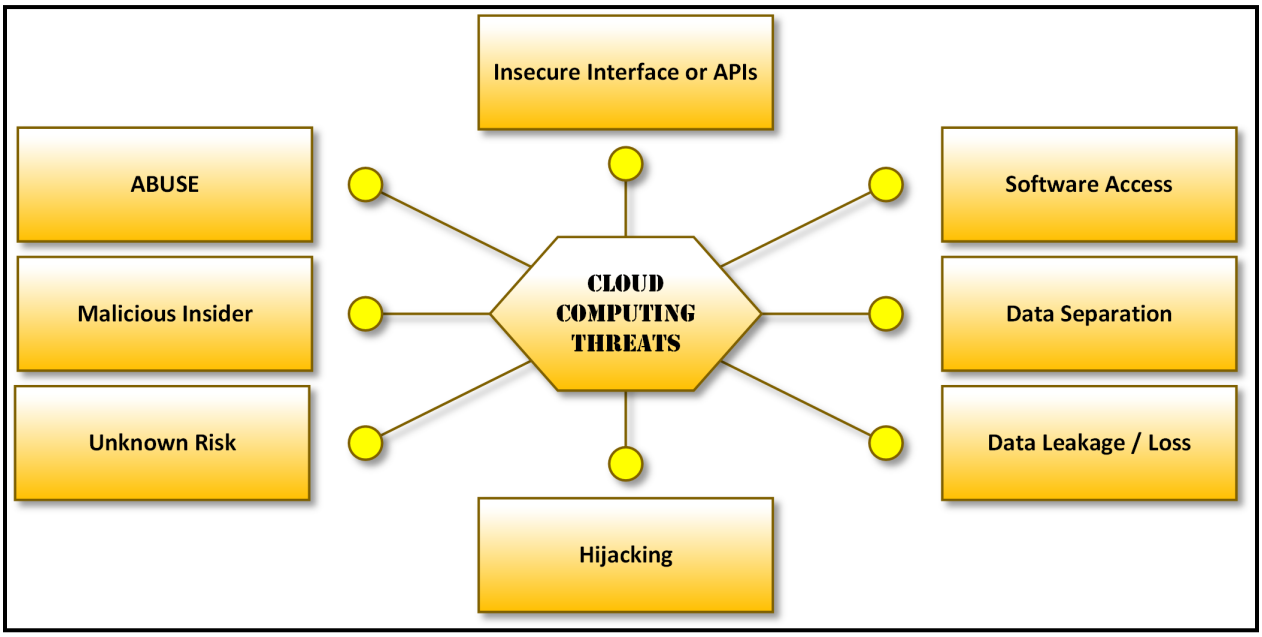


Figure 1-4 Cloud Computing Threats

The following are some threats that exist in the Cloud Security:

- In the Cloud Computing Environment, a major threat to cloud security is a single data breach that can to result loss. Additionally, it allows the hacker to further have access to the records which allows the hacker to have access to multiple records over the cloud. It is the extremely worst situation where compromising of single entity leads to compromise multiple records.
- Data Loss is one of the most common potential threats that is vulnerable to Cloud security as well. Data loss may be due to intended or accidental means. It may be large scales or small scale; however massive data loss is catastrophic & costly.
- Another Major threat to Cloud computing is the hijacking of Account over cloud and Services. Applications running on a cloud having software flaws, weak encryption, loopholes, and vulnerabilities allows the intruder to control.

Furthermore, there are several more threats to Cloud computing which are:

- Insecure APIs
- Denial of Services
- Malicious Insiders
- Poor Security
- Multi-Tenancy

Advanced Persistent Threats

An advanced persistent threat (APT) is the process of stealing information by a continuous process. An Advanced Persistent Threat usually focuses on private organizations or for political motives. The APT process relies upon advanced, sophisticated techniques to exploit vulnerabilities within a system. The "persistent" term defines the process of an external command and controlling system that is continuously monitoring and fetching data from a target. The "threat" process indicates the involvement attacker with potentially harmful intentions.

Characteristics of APT Criteria are:

Characteristics	Description
Objectives	Motive or Goal of threat
Timeliness	Time spend 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 System involved
Knowledge Source	Discern information regarding threats

Table 1-2 Advanced Persistent Threat Criteria

Viruses and Worms

Term "Virus" in Network and Information security describes malicious software. This malicious software is developed to spread, replicate themselves, and attach themselves to other files. Attaching with other files helps to transfer onto other systems. These viruses require user interaction to trigger and initiate malicious activities on the resident system.

Unlike Viruses, Worms are capable of replicating themselves. This capability of worms makes them spread on a resident system very quickly. Worms are propagating in different forms since the 1980s. Some types of emerging worms are very destructive, responsible for devastating DoS attacks.

Mobile Threats

Emerging mobile phone technology, especially Smartphones has raised the focus of attacker over mobile devices. As Smartphones are popularly used all over the world, it has shifted the focus of attackers to steal business and personal information through mobile devices. The most common threat to mobile devices are:

- Data leakage
- Unsecured 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 Insider has privileges and it is authorized to access the network resources.

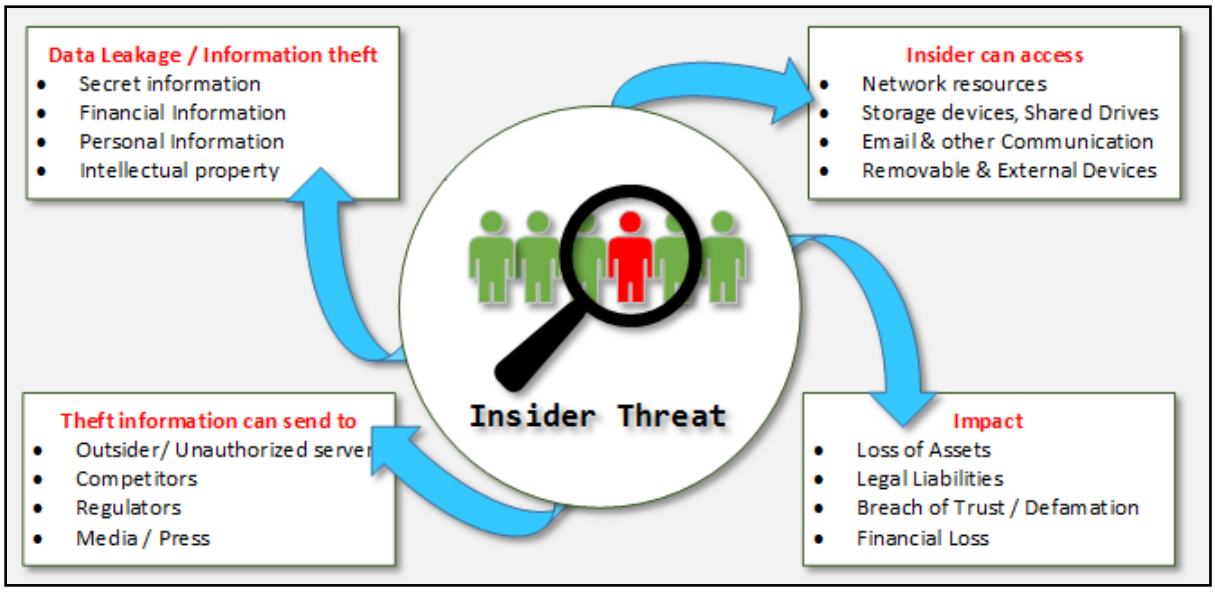


Figure 1-5 Insider Threats

Botnets

Combination of the functionality of Robot and Network develop a continuously working Botnet on a repetitive task. It is the basic fundamental of a bot. They are known as the workhorses of the Internet. These botnets perform repetitive tasks. The most often of botnets are in connection with Internet Relay Chat. These types of botnets are legal and beneficial.

A botnet may use for positive intentions but there also some botnets which are illegal and intended for malicious activities. These malicious botnets can gain access to the systems using malicious scripts and codes either by directly hacking the system or through "Spider." Spider program crawls over the internet and searches for holes in security. Bots introduce the system on the hacker's web by contacting the master computer. It alerts the master computer when the system is under control. Attacker remotely controls all bots from Master computer.

Information Security Threat Categories

Information Security Threats 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. The poorly configured device offers intruder to exploit. Common vulnerabilities on the network include using default installation settings, open access controls, Weak encryption & Passwords, and devices lacking the latest security patches. Top network level threats include:

- Information gathering
- Sniffing & Eavesdropping
- Spoofing
- Session hijacking
- Man-in-the-Middle Attack
- DNS & ARP Poisoning
- Password-based Attacks
- Denial-of-Services Attacks
- Compromised Key Attacks
- Firewall & IDS Attacks

Host Threats

Host threats are focused on system software; Applications are built or running over this software such as Windows 2000, .NET Framework, SQL Server, and others. The Host Level Threats includes:

- 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 category. Main threats to the application are:

- Improper Data / Input Validation

- Authentication & Authorization Attack
- Security Misconfiguration
- Information Disclosure
- Broken Session Management
- Buffer Overflow Issues
- Cryptography Attacks
- SQL Injection
- Improper Error handling & 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 found any vulnerability in an Operating System, they exploit to attack against the operating system. Some most common vulnerabilities of an operating system are:

- ***Buffer overflow vulnerabilities***

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

- ***Bugs in the operating system***

  In software exploitation attack & bugs in software, the attacker tries to exploit the vulnerabilities in software. This vulnerability might be a mistake by the developer while developing the program code. Attackers can discover these mistakes, use them to gain access to the system.

- ***Unpatched operating system***

  Unpatched Operating System allows malicious activities, or could not completely block malicious traffic into a system. Successful intrusion can impact severely in the form of compromising sensitive information, data loss and disruption of regular operation.

Misconfiguration Attacks

In a corporate network while installation of new devices, the administrator must have to change the default configurations. If devices are left upon default configuration, using default credentials, any user who does not have the privileges to access the device but has

connectivity can access the device. It is not a big deal for an intruder to access such type of device because default configuration has common, weak passwords and there are no security policies are enabled on devices by default.

Similarly, permitting an unauthorized person or giving resources and permission to a person more than his privileges might also lead to an attack. Additionally, Using the organization in Username & password attributes make it easier for hackers to gain access.

Application-Level Attacks

Before releasing an application, the developer must make sure, test & verify from its end, manufactures or from developer's 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

Shrink Wrap code attack is the type of attack in which hacker uses the shrink wrap code method for gaining access to a system. In this type of attack, hacker exploits holes in unpatched Operating systems, poorly configured software and application. To understand shrink wrap vulnerabilities, consider an operating system has a bug in its original software version. The vendor may have released the update, but it is the most critical time between the release of a patch by vendor till client's systems updates. During this critical time, unpatched systems are vulnerable to the Shrinkwrap attack. Shrinkwrap attack also includes vulnerable to the system installed with software that is bundled with insecure test pages and debugging scripts. The developer must have to remove these scripts before release.

Information Warfare

Information warfare is a concept of warfare, to get involved in the warfare of information to gain the most of information. The term, "**Information Warfare**" or "**Info War**" describes the use of information and communication technology (ICT). The major reason or focus of this information war is to get a competitive advantage over the opponent or enemy. The following is the classification of Information warfare into two classes: -

1. **Defensive Information Warfare**

Defensive Information warfare term is used to refer to all defensive actions that are taken to defend from attacks to steal information and information-based processes. Defensive Information ware fare areas are: -

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

2. **Offensive Information Warfare**
   The offensive term is associated with the military. Offensive warfare is an aggressive operation that is taken against the enemies dynamically instead of waiting for the attackers to launch an attack. Accessing their territory to gain instead of losing territory is the fundamental concept of offensive warfare. The major advantage of offensive warfare is to identify the opponent, strategies of the opponent, and other information. Offensive Information warfare prevents or modifies the information from being in use by considering integrity, availability, and confidentiality.

Hacking Concepts, Types, and Phases

Hacker

Hacker is the one who is smart enough to steal the information such as Business data, personal data, financial information, credit card information, username & Password from the system he is unauthorized to get this information by taking unauthorized control over that system using different techniques and tools. Hackers have great skill, ability to develop software and explore software and hardware. Their intention can be either doing illegal things for fun or sometimes they are paid to hack.

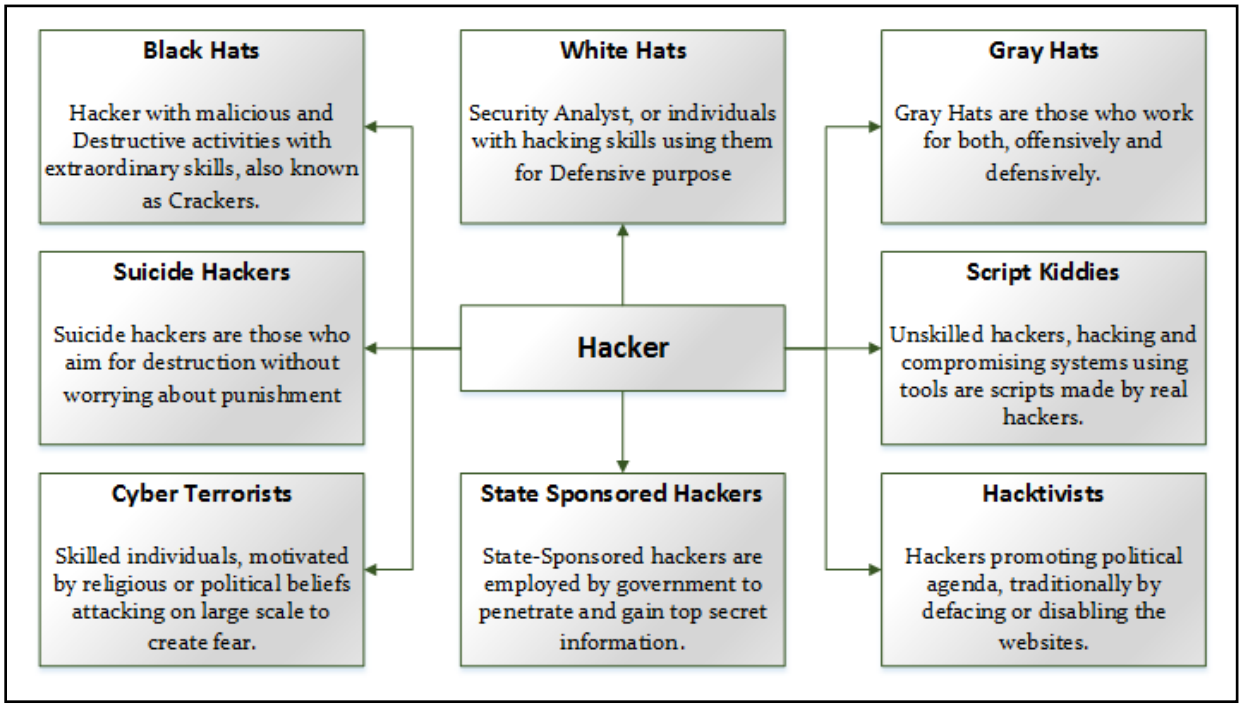


Figure 1-6 Types of Hacker

Hacking

The Term "Hacking" in information security refers to exploiting the vulnerabilities in a system, compromising the security to gain unauthorized command and control over the system resources. Purpose of hacking may include modification of system resources, disruption of features and services to achieve goals. It can also be used to steal information for any use like sending it to competitors, regulatory bodies or publicizing the sensitive information.

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 preparing phase for the attacker to get ready for an attack by gathering the information about the target before launching an attack using different tools and techniques. Gathering of information about the target makes it easier for an attacker, even on a large scale. Similarly, in large scale, it helps to identify the target range.

In ***Passive Reconnaissance***, the hacker is acquiring the information about target without interacting the target directly. An example of passive reconnaissance is public or social media searching for gaining information about the target.

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

Scanning

Scanning phase is a pre-attack phase. In this phase, attacker scans the network by information acquired during the initial phase of reconnaissance. Scanning tools include Dialler, Scanners such as Port scanners, Network mappers, client tools such as ping, as well as vulnerabilities scanner. During the scanning phase, attacker finally fetches the information of ports including port status, operating system information, device type, live machines, and other information depending upon scanning.

Gaining Access

Gaining access phase of hacking is the point where the hacker gets the control over an operating system, application or computer network. Control gained by the attacker defines the access level such as operating system level, application level or network level access. Techniques include password cracking, denial of service, session hijacking or buffer overflow and others are used to gain unauthorized access. After accessing the system; the attacker escalates the privileges to obtain complete control over services and process and compromise the connected intermediate systems.

Maintaining Access / Escalation of Privileges

Maintaining access phase is the point when an attacker is trying to maintain the access, ownership & control over the compromised systems. Similarly, attacker prevents the owner from being owned by any other hacker. They use ***Backdoors***, ***Rootkits*** or ***Trojans*** to retain their ownership. In this phase, an attacker may steal information by uploading the information to the remote server, download any file on the resident system, and manipulate the data and configuration. To compromise other systems, the attacker uses this compromised system to launch attacks.

Clearing Tracks

An attacker must hide his identity by covering the tracks. Covering tracks are those activities which are carried out to hide the malicious activities. Covering track is most required for an attacker to fulfill their intentions by continuing the access to the compromised system, remain undetected & gain what they want, remain unnoticed and wipe all evidence that indicates his identity. To manipulate the identity and evidence, the attacker overwrites the system, application, and other related logs to avoid suspicion.

Ethical Hacking Concepts and Scope

Ethical Hacking

Ethical hacking and penetration testing are common terms, popular in information security environment for a long time. Increase in cybercrimes and hacking create a great challenge for security experts and analyst and regulations over the last decade. It is a popular war between hackers and security professionals.

Fundamental Challenges to these security experts are of finding weaknesses and deficiencies in running and upcoming systems, applications, software and addressing them proactively. It is less costly to investigate proactively before an attack instead of investigating after falling into an attack, or while dealing with an attack. For security aspect, prevention and protection, organizations have their penetration testing teams internally as well as contracted outside professional experts when and if they are needed depending on the severity and scope of the attack.

Why Ethical Hacking is Necessary

The rise in malicious activates, cybercrimes and appearance of different forms of advanced attacks require to need of penetration tester who penetrate the security of system and networks to be determined, prepare and take precaution and remediation action against these 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

Increase in these type of attacks, hacking cases, and cyber attacks, because of increase of use of online transaction and online services in the last decade. It becomes more attractive for hackers and attackers to tempt to steal financial information. Computer or Cybercrime law has slowed down prank activities only, whereas real attacks and cybercrimes rise. It focuses on the requirement of Pentester, a shortened form of Penetration tester for the search for vulnerabilities and flaw within a system before waiting for an attack.

If you want to beat the attacker and hacker, you have to be smart enough to think like them and act like them. As we know, hackers are skilled, with great knowledge of hardware, software, and exploration capabilities. It ensures the need and importance of ethical hacking which allows the ethical hacker to counter the attack from malicious hackers by anticipating methods. Another major advantage and need for ethical hacking are to uncover the vulnerabilities in systems and security deployments to take action to secure them before they are used by a hacker to breach security.

Scope and Limitations of Ethical Hacking

Ethical Hacking is an important and crucial component of risk assessment, auditing, counter frauds. Ethical hacking is widely used as penetration testing to identify the vulnerabilities, risk, and highlight the holes to take remedial actions against attacks. However, there is also some limitations where ethical hacking is not enough, or just through ethical hacking, the issue could not resolve. An organization must first know what it is looking for before hiring an external pentester. It helps focus the goals to achieve and save time. The testing team dedicated in troubleshooting the actual problem in resolving the issues. The ethical hacker also helps to understand the security system of an organization better. It is up to the organization to take recommended actions 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 & Reconnaissance
2. Scanning
3. Enumeration
4. System Hacking
5. Escalation of Privileges
6. Covering Tracks

Skills of an Ethical Hacker

A skilled, ethical hacker has a set of technical and non-technical skills.

Technical Skills

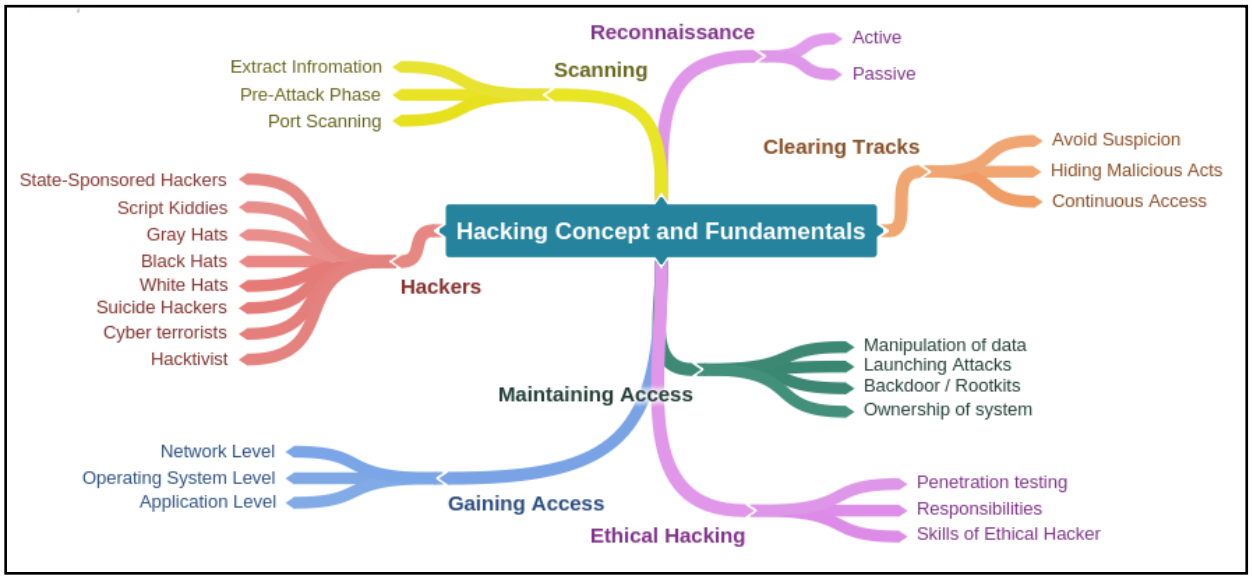
1. Ethical Hacker has in-depth knowledge of almost all operating systems, including all popular, widely- used operating systems such as Windows, Linux, Unix, and Macintosh.
2. These ethical hackers are skilled at networking, basic and detailed concepts, technologies, and exploring capabilities of hardware and software.
3. Ethical hackers must have a strong command over security areas, related issues, and technical domains.

4. They must have detailed knowledge of older, advanced, 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, known as IA, depends upon the components that are ***Integrity, Availability, Confidentiality,*** and ***Authenticity***. With the combination of these components, assurance of information and information systems are ensured and protected during the processes, usage, storage, and communication. These components are defined earlier in this chapter.

Apart from these components, some methods and processes also help in the achievement of information assurance such as: -

- Policies and Processes.
- Network Authentication.
- User Authentication.
- Network Vulnerabilities.

- Identifying problems and resources.
- Implementation of a plan for identified requirements.
- Application of information assurance control.

Information Security Management Program

Information Security Management programs are the programs that are specially designed to focus on reducing the risk and vulnerabilities towards information security environment to train the organization and users to work in the less vulnerable state. The Information Security Management is a combined management solution to achieve the required level of information security using well-defined security policies, processes of classification, reporting, and management and standards. The diagram on the next page shows the EC-Council defined Information Security Management Framework: -

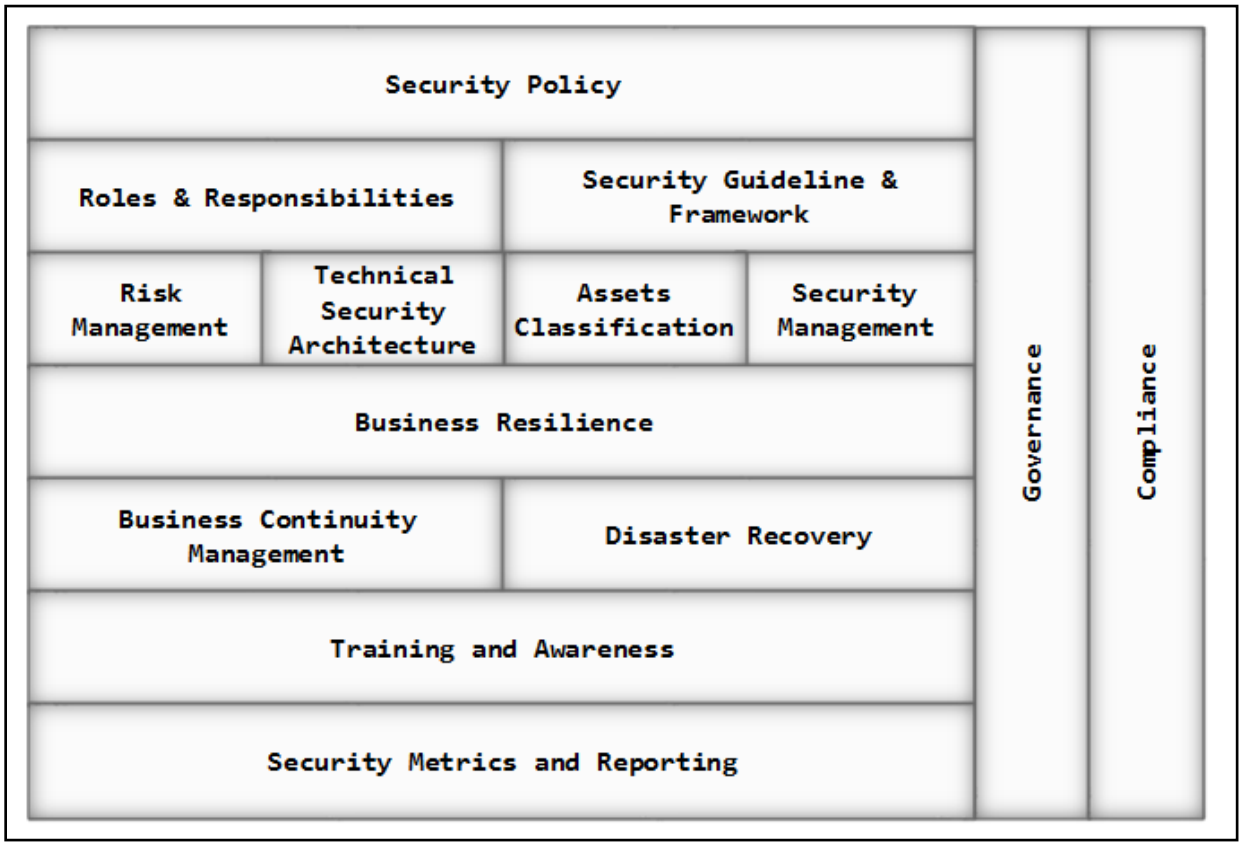


Figure 1-7 Information Security Management Framework

Threat Modeling

Threat Modeling is the process or approach to identify, diagnose, and assist the threats and vulnerabilities of the system. It is an approach to risk management which dedicatedly focuses on analyzing the system security and application security against security objectives. This identification of threats and risks helps to focus and take action on an

event to achieve the goals. Capturing data of an organization, implementing identification and assessment processes over the captured information to analyze the information that can impact the security of an application. Application overview includes the identification process of an application to determine the trust boundaries and data flow. Decomposition of an application and identification of a threat helped to a detailed review of threats, identification of threat that is breaching the security control. This identification and detailed review of every aspect expose the vulnerabilities and weaknesses of the information security environment.

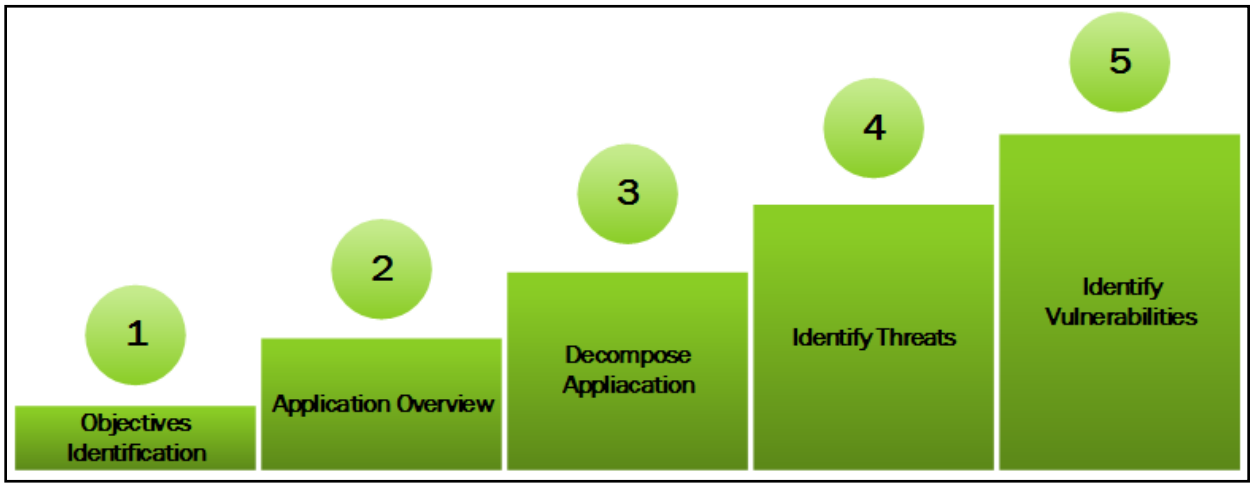


Figure 1-8 Threat Modelling

Enterprise Information Security Architecture (EISA)

Enterprise Information Security Architecture is the combination of requirements and processes that help in determination, investigation, monitoring the structure of behavior of information system. The following are the goals of EISA: -

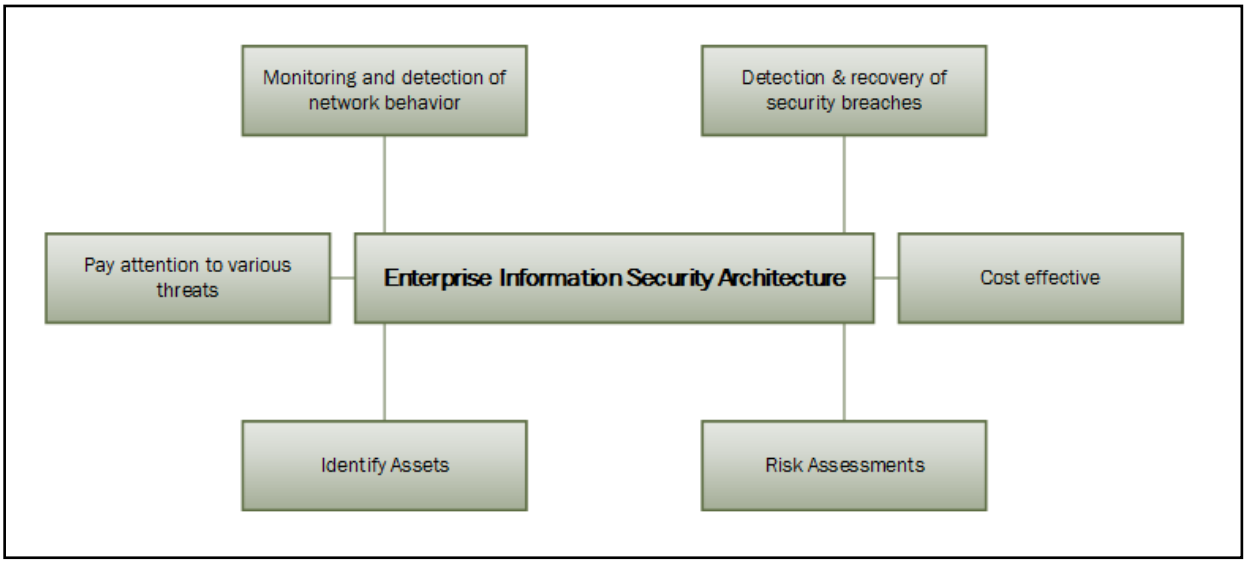


Figure 1-9 EISA

Network Security Zoning

Managing, deploying an architecture of an organization in different security zones is called Network Security Zoning. These security zones are the set of network devices having 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 of inbound and outbound traffic across the network.

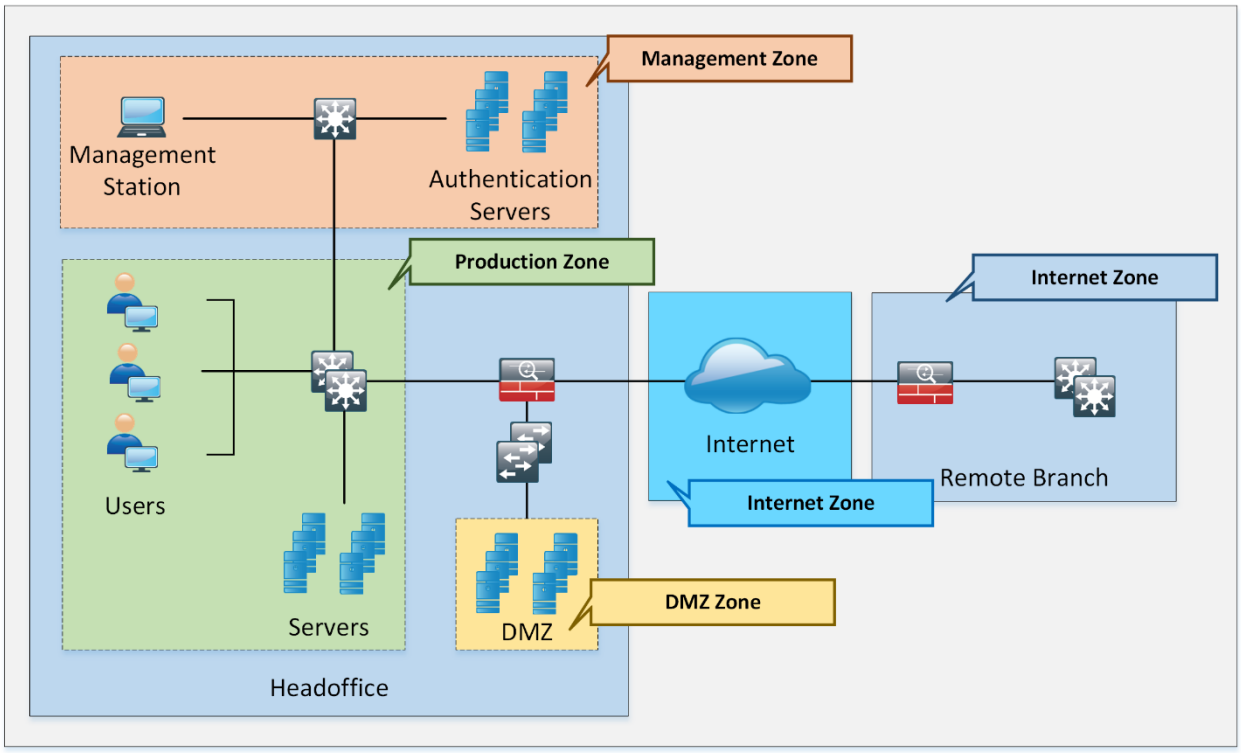


Figure 1-10 Network Security Zoning

Information Security Policies

Information Security Policies are the fundamental and the most dependent component of the information security infrastructure. Fundamental security requirements, conditions, 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.

Figure 1-11 Steps to enforce Information Security

The basic goals and objectives of the Information Security Policies are: -

- Cover Security requirements and conditions of the organization
- Protect organizations resources
- Eliminate legal liabilities
- Minimize the wastage of resources
- Prevent against unauthorized access / modification etc.
- Minimize the risk
- 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 has no restriction on usage of system resources.

Permissive policy

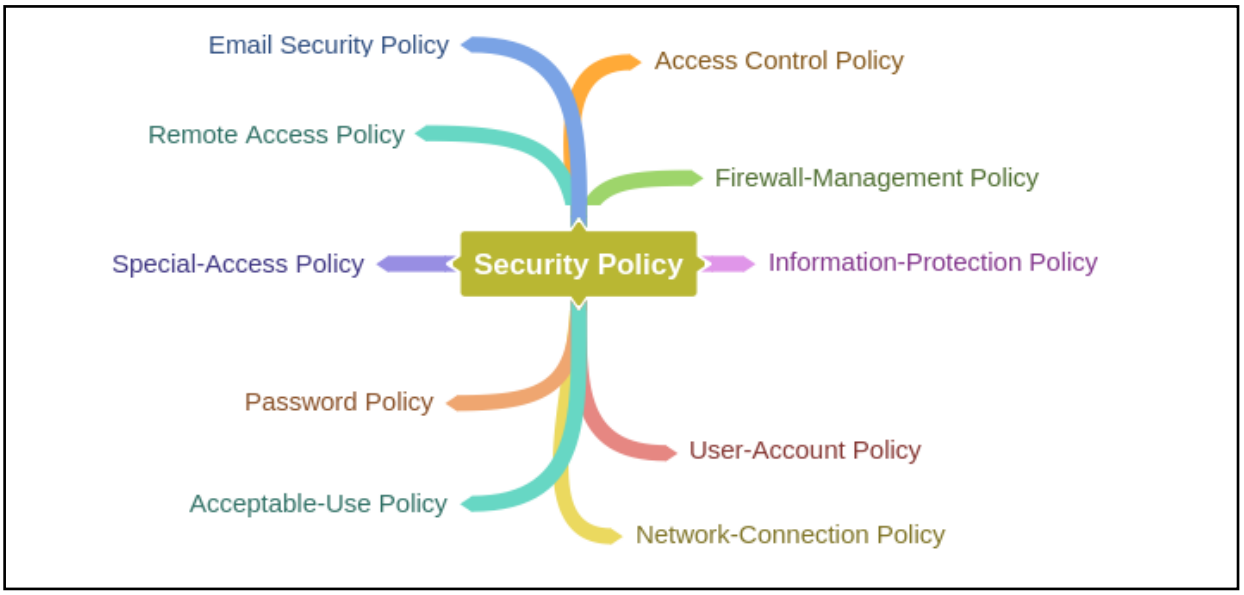
The permissive policy restricts only widely known, dangerous attacks or behavior.

Prudent Policy

The prudent policy ensures maximum and strongest security among them. However, it allows known, necessary risks, blocking all other service but individually enabled services. Every event is log in prudent policy.

Paranoid Policy

Paranoid Policy denied everything, limiting internet usage.



Implications for Security Policy Enforcement

HR & Legal Implication of Security Policies

HR department has the responsibility of making sure the organization is aware regarding security policies as well as providing sufficient training. With the cooperation of the management or administration within an organization, the HR department monitors the enforcement of security policies & deals with any violation, issues arise in the deployment.

Legal implication of security policies enforces under the supervision of the professionals. These professionals are legal experts, consultant which comply with laws, especially local laws and regulations. Any violation of legal implication leads to lawsuits against the 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, unauthorized physical access as well as environmental impacts such as rain, dust, power failure and fire.

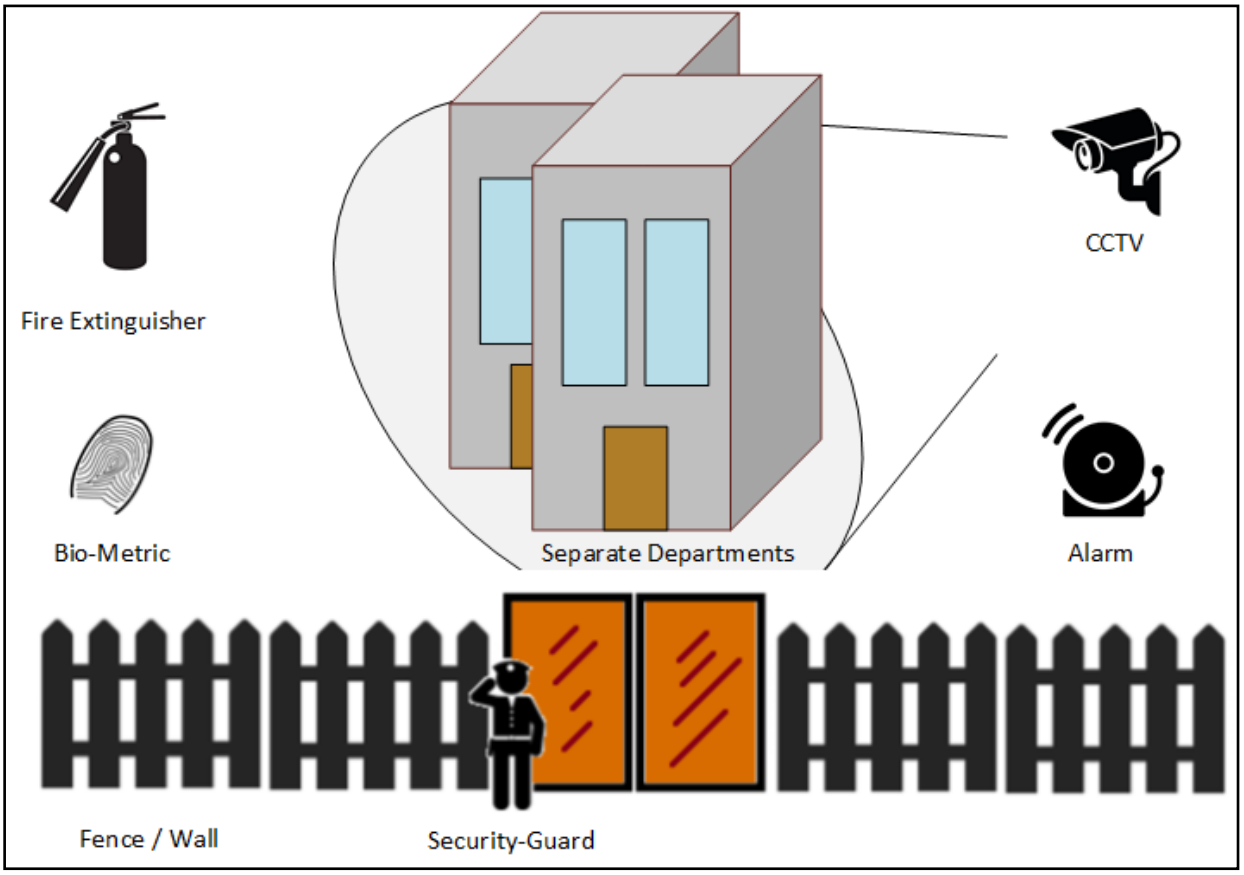


Figure 1-12 Physical Security

Physical security is required to prevent stealing, tampering, damage, theft and many more physical attacks. To secure the premises and assets, setup of fences, guards, CCTV cameras, intruder monitoring system, burglar alarms, deadlocks to secures the premises. Important files and documents should be available on any unsecured location even within an organization or keep locked, available to authorized persons only. Function area must be separated, 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 an incident that occurs. This incident may be any specific violation of any condition, policies, or else. Similarly, in information security, incident responses are the remediation actions or steps taken as the response of an incident depending upon identification of an event, threat or attack to the removal or elimination (when system become 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 actions required when a system is facing a threat to its

confidentiality, integrity, authenticity, availability depending upon the threat level. Initially, the important thing to remember is when a system is dealing with an attack, it requires sophisticated, dedicated troubleshooting by an expert. While responding to the incident, the professional collects the evidence, information, and clues that are helpful for prevention in future, tracing the attacker and finding the holes and vulnerabilities in the system.

Incident Management Process

Incident Response Management processes include: -

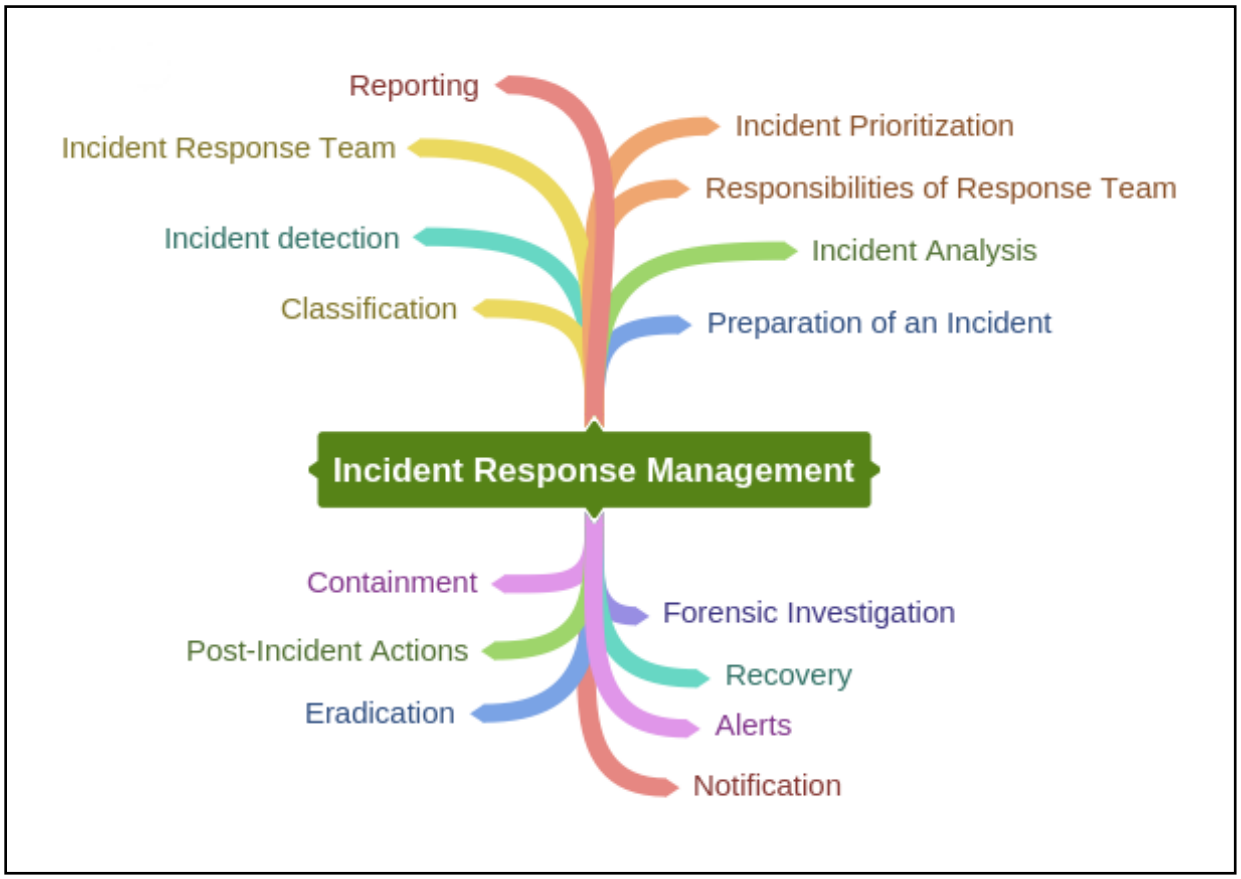
1. Preparation for Incident Response
2. Detection and Analysis of Incident Response
3. Classification of an incident and its prioritization
4. Notification and Announcements
5. Containment
6. Forensic Investigation of an incident
7. Eradication and Recovery
8. Post-Incident Activities

Responsibilities of Incident Response Team

The Incident Response team is consists of the members who are well-aware of dealing with incidents. This Response team is consists of trained officials who are expert in collecting the information and secure all evidence of an attack from the incident system. As far as the member of Incident response team is concerned, this team includes IT personnel, HR, Public Relation officers, Local Law enforcement, and Chief Security officer.

- The major responsibility of this team is to take action according to Incident Response Plan (IRP). If IRP is not defined, not applicable on that case, the team has to follow the leading examiner to perform a coordinated operation.
- Examination and evaluation of event, determination of damage or scope of an attack.
- Document the event, processes.
- If required, take the support of external security professional or consultant.
- If required, take the support of local law enforcement.
- Facts Collection.
- Reporting.

Mind Map



Vulnerability Assessment

Vulnerability assessment is the procedure of examination, identification, and analysis of system or application abilities including security processes running on a system to withstand any threat. Through vulnerability assessment, you can identify weaknesses and threat to a system, scope a vulnerability, estimate the requirement and effectiveness of any additional security layer.

Types of Vulnerability Assessment

The 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
8. Application Assessment

Network Vulnerability Assessment Methodology

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

1. Acquisition
2. Identification
3. Analyzing
4. Evaluation
5. Generating Reports

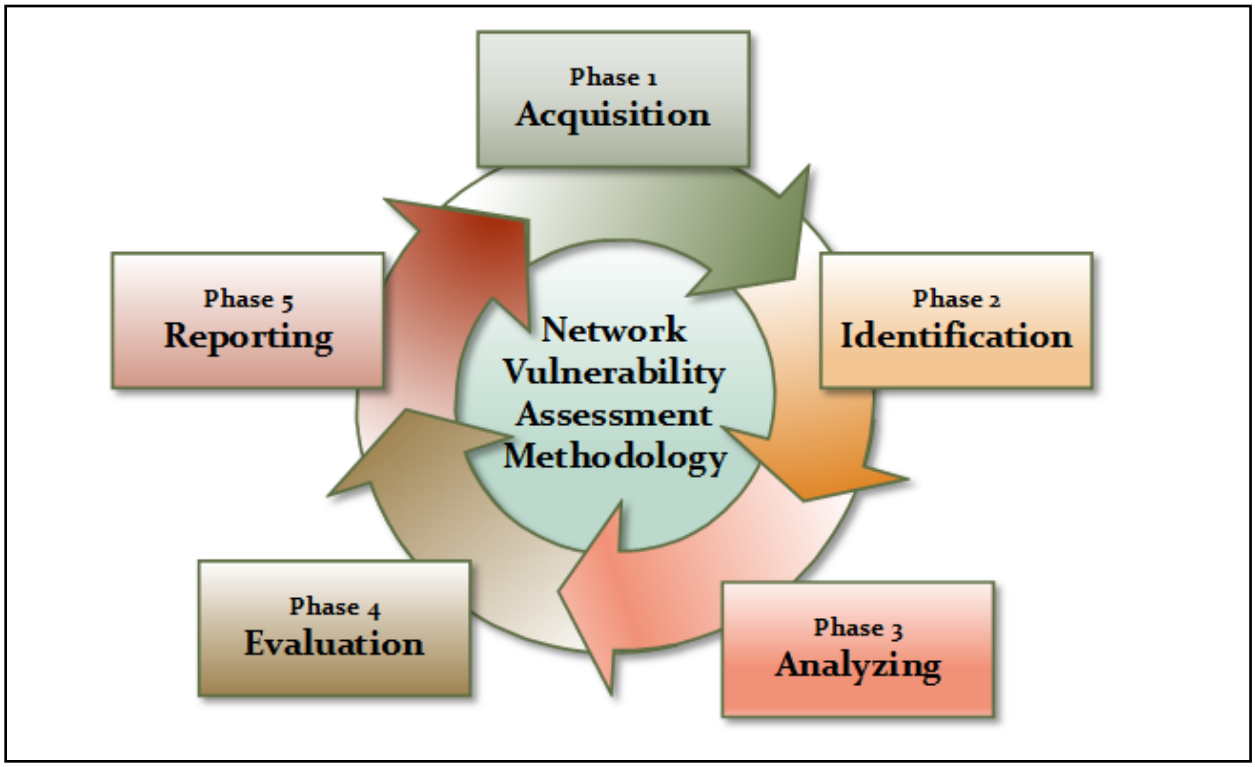


Figure 1-13 Network Vulnerability Assessment Methodology

Acquisition

The acquisition phase compares and review 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 that are involved in designing the network architecture to gather the technical information.

Analyzing

Analyzing phase reviews, the gathered, collected information in the form of a collection of documentation or one-to-one interaction. Analyzing phase is basically: -

- Review information.
- Analyzing previously identified vulnerabilities results.
- Risk Assessment.
- Vulnerability and Risk Analysis.
- Evaluation of the effectiveness of existing security policies.

Evaluation

Evaluation phase includes: -

- Inspection of Identified Vulnerabilities.
- Identification of flaws, gaps in existing & required Security.
- Determination of Security Control required resolving issues & Vulnerabilities.
- Identify modification and Upgrades.

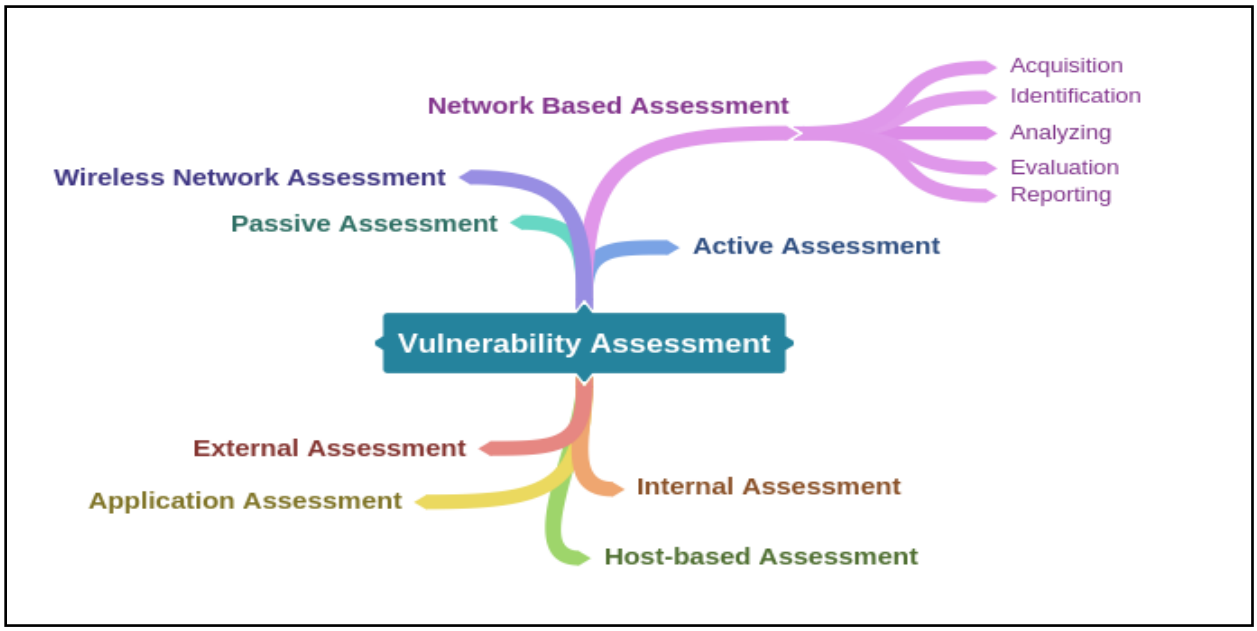
Generating Reports

Reporting phase is documentation of draft report required for future inspection. This report helps identify vulnerabilities in the acquisition phase. Audit and Penetration also require these previously collected reports. When any modification in security mechanism is required, these reports help to design security infrastructure. Central Databases usually holds these reports.

Reports contain: -

- Task did by each member of the team.
- Methods & tools used.
- Findings.
- Recommendations.
- Collected information from different phases.

Mind Map



Penetration Testing

Technology Overview

In the Ethical Hacking environment, the most common term that often uses is "***pentester***." Pentesters are the penetration tester that has permission to hack a system by owner. Penetration testing is the process of hacking a system with the permission from the owner of that system, to evaluate security, Hack Value, Target of Evaluation (TOE), attacks, exploits, zero-day vulnerability & other components such as threats, vulnerabilities, and daisy chaining.

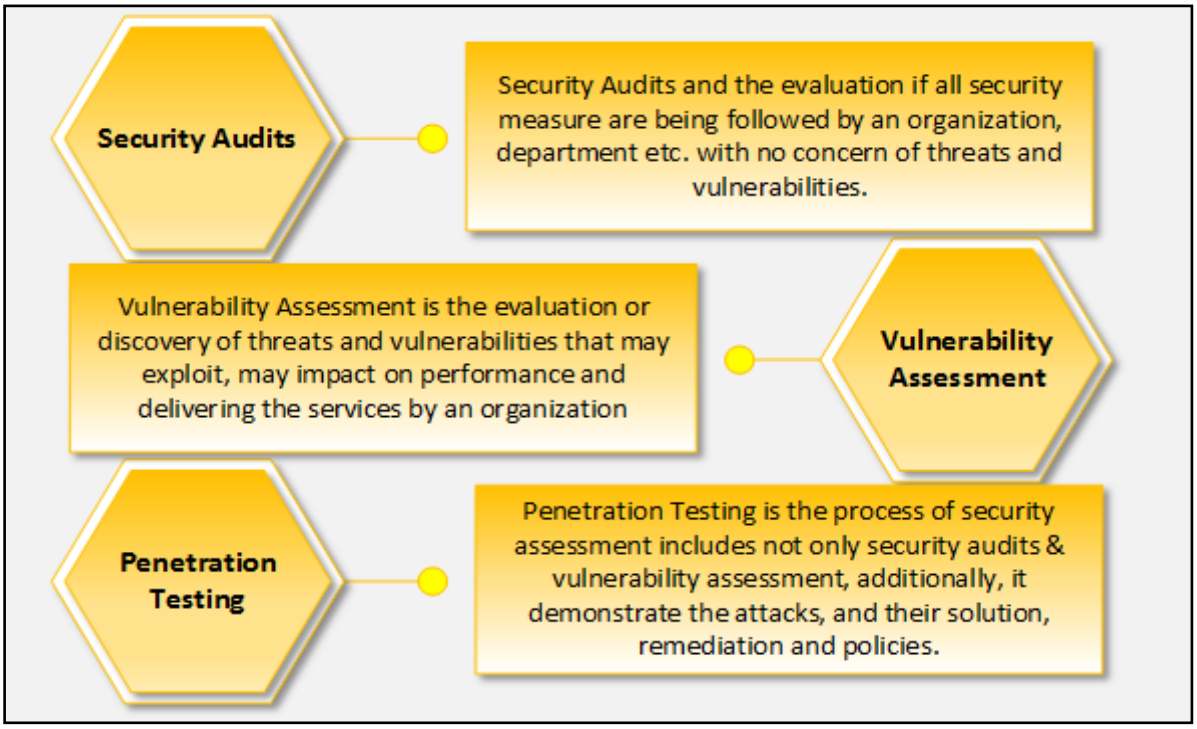


Figure 1-13 Comparing Pentesting

Important for Penetration testing

If you want to be ready for an attack, you must be smart, to think like them, act like them. Hackers are skilled, having detailed information of hardware's, software, networking and other related information. The need and importance of penetration testing, in the modern world where variously advanced threat such as Denial-of-service, Identity theft, theft of services, stealing information is common, system penetration ensure to counter the attack from malicious threat by anticipating methods. Some other major advantages and need for penetration testing is to uncover the vulnerabilities in systems and security deployments in the same way an attacker gains access: -

- To identify the threats and vulnerabilities to organizations assets.
- To provide a comprehensive assessment of policies, procedures, design, and architecture.
- To set remediation actions to secure them before they are used by a hacker to breach security.
- To identify what an attacker can access to steal.
- To identify what information can be theft and its use.
- To test and validate the security protection & identify the need for any additional protection layer.
- Modification and up-gradation of currently deployment security architecture.

- To reduce the expense of IT Security by enhancing Return on Security Investment (ROSI).

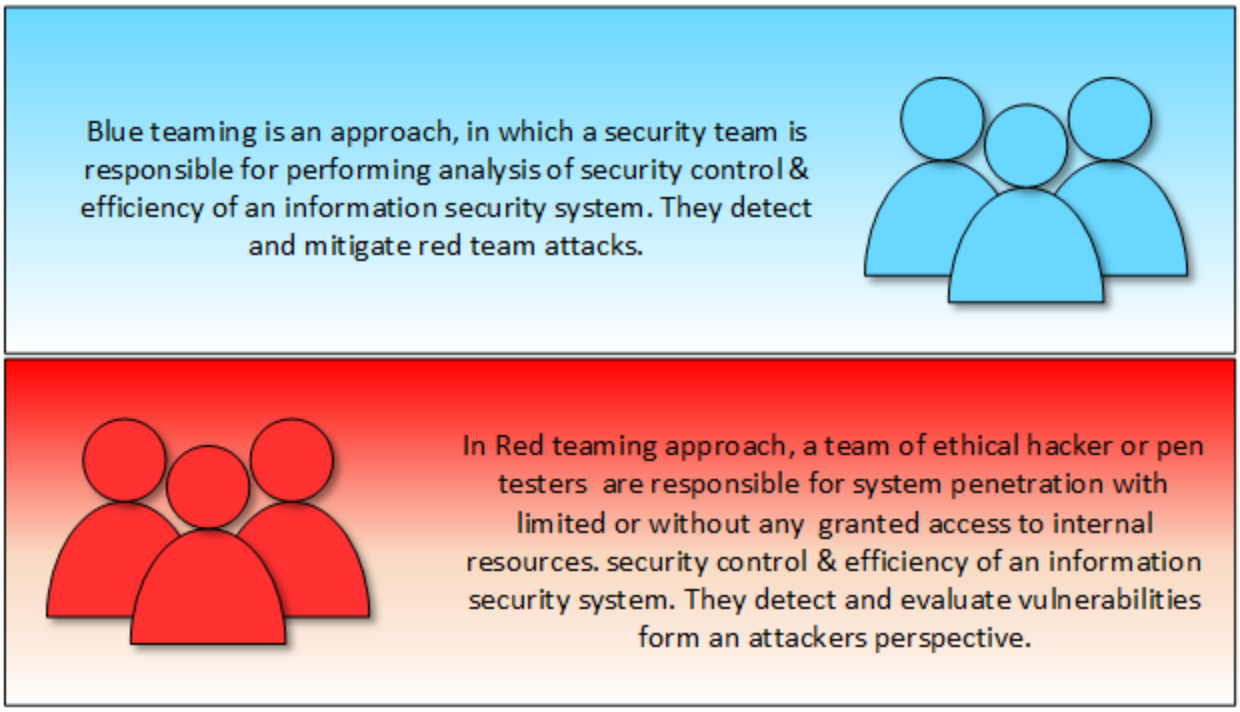


Figure 1-14 Comparing Blue & Red Teaming

Types of Penetration Testing

Three types of Penetration testing are important to be differentiated because a penetration tester may have asked to perform any of them.

Black Box

The black box is a type of penetration testing in which the pentester is blind testing or double-blind testing, i.e. provided with no prior knowledge of the system or any information of the target. Black boxing is designed to demonstrate an emulated situation as an attacker in countering an attack.

Gray box

Gray box, is a type of penetration testing in which the pentester has very limited prior knowledge of the system or any information of targets such as IP addresses, Operating system or network information in very limited. Gary boxing is designed to demonstrate an emulated situation as an insider might have this information and to counter an attack as the pentester has basic, limited information regarding target.

White box

The white box is a type of penetration testing in which the pentester has complete knowledge of system and information of the target. This type of penetration is done by internal security teams or security audits teams to perform auditing.

Phases of Penetration Testing

Penetration testing is a three-phase process.

1- Pre-Attack Phase
2- Attack Phase
3- Post-Attack Phase

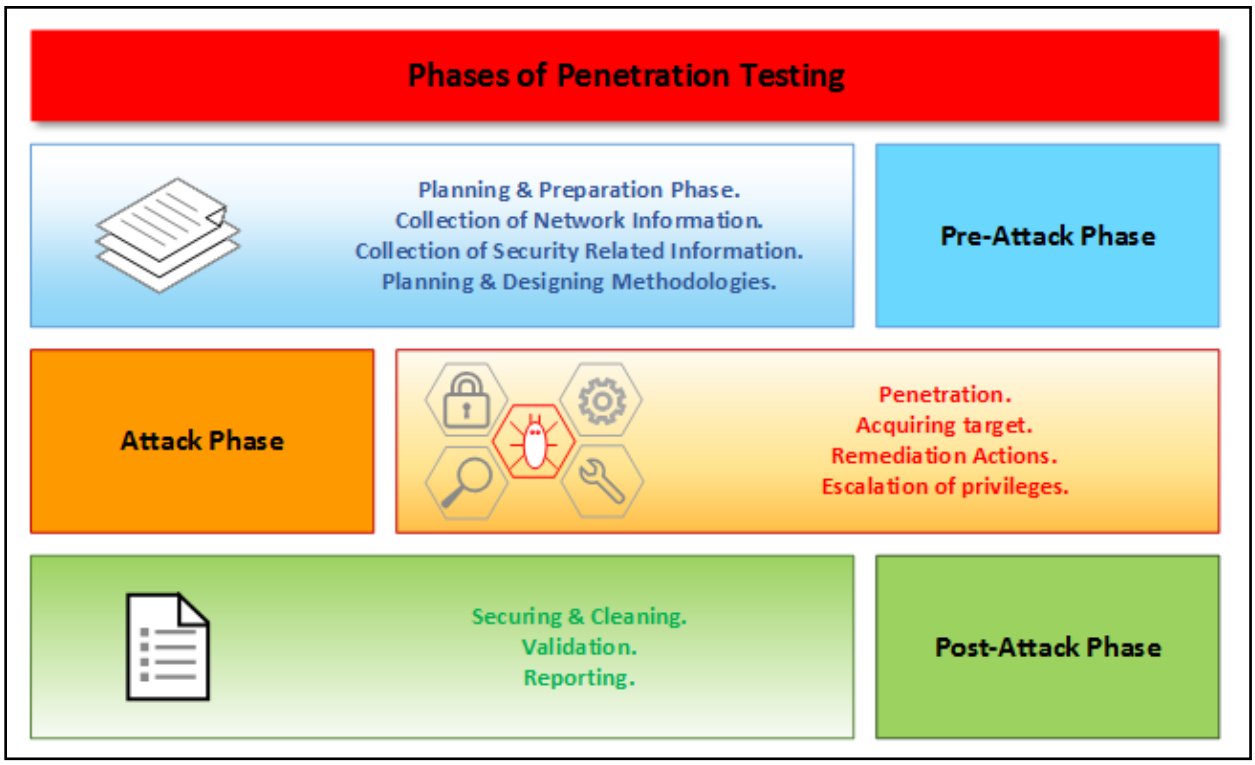


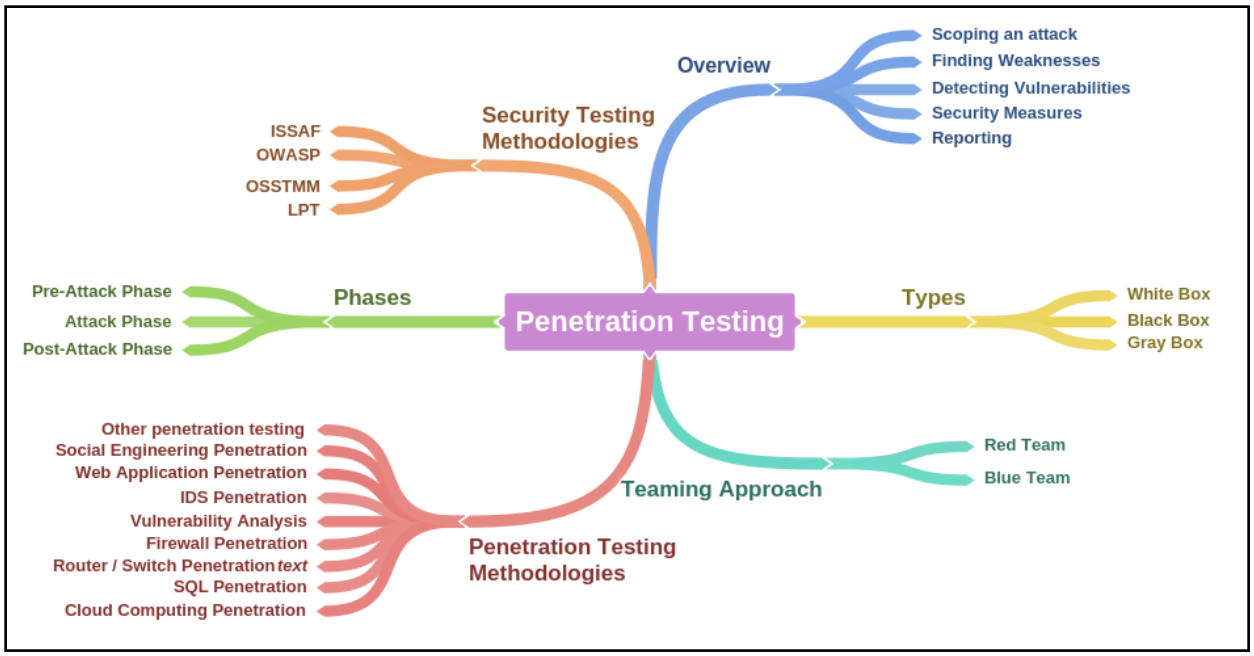
Figure 1-15 Penetration Testing Phases

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

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 by "***PCI Security Standards Council,***" available for organizations to develop, enhance and assess security standards for handling cardholder information and security standard for payment account security. PCI Security Standards Council develops security standards for payment card industry and provides tools required for enforcement of these standards like training, certification, assessment, and scanning.
Founding members of this council are: -

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

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

- Secure Network
- Strong Access Control
- Cardholder data security

- Regular Monitoring and Evaluation of Network
- Maintaining Vulnerability program
- Information security policy

ISO/IEC 27001:2013

International Organization for Standardization (ISO) and International Electro-Technical Commission (IEC) are organizations that globally develop and maintain their standards. ISO/IEC 27001:2013 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 27001:2005. ISO/IEC 27001:2013 cover the following key point in information security: -

- Implementation and maintaining Security requirements.
- Information security management processes.
- Assurance of Cost effective risk management.
- Status of Information Security Management Activities.
- Compliant with laws.

Health Insurance Portability and Accountability Act (HIPAA)

Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996 by Congress. HIPAA runs with Department of Health and Human Services (HHS) to develop and maintain regulation that associates with privacy and security of health information. HIPAA Security rules ensure what information is protected, additionally, the safeguards that must apply to secure electronic protected health information. HIPAA defines Electronic protected information, general rules, risk analysis, and management. Administrative safeguards including physical safeguards, technical safeguards ensure the confidentiality, integrity, and availability of electronic protected health information (e-PHI).

The major domains in information security where HIPAA is developing and maintain standards and regulations are: -

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

Sarbanes Oxley Act (SOX)

Sarbanes Oxley Act (SOX) key requirements or provisions organizes in the form of 11 titles which are as follows: -

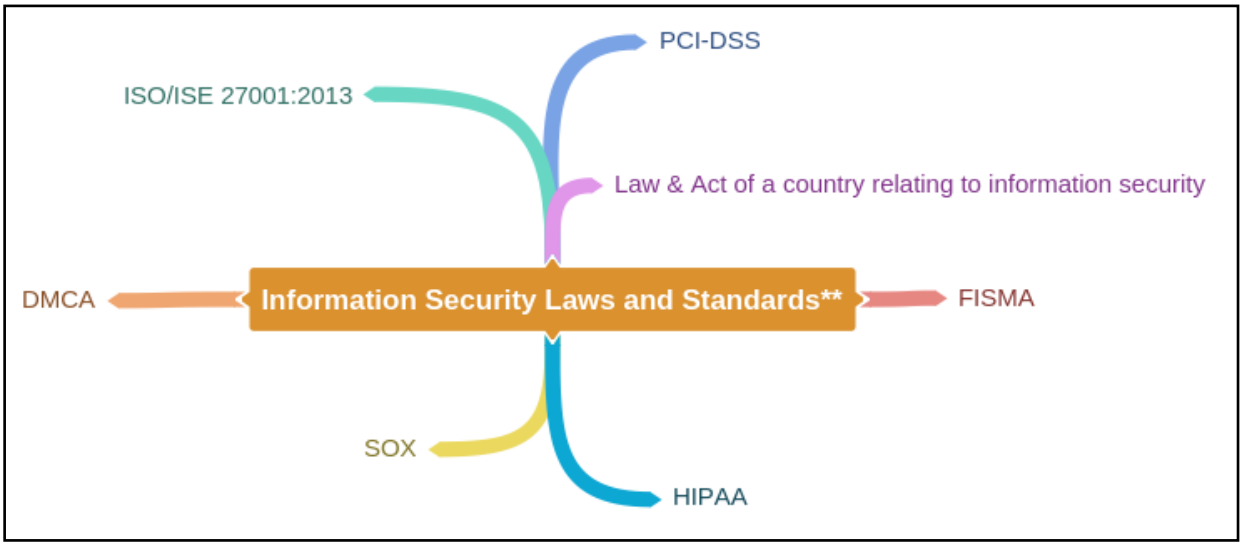
Title	Majors

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 the standards that are being deployed worldwide including Digital Millennium Copyright Act (DMCA) and Federal Information Security Management Act (FISMA). DMCA is United States copyright law whereas FISMA a framework for ensuring information security control effectiveness. According to Homeland Security, FISMA 2014 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 authority to develop and oversee the implementation of binding operational directives to other agencies, in coordination and consistent with OMB policies and practices. The Federal Information Security Modernization Act of 2014 amends the Federal Information Security Management Act of 2002 (FISMA).

Mind Map


PCI-DSS
ISO/ISE 27001:2013
Law & Act of a country relating to information security
DMCA
Information Security Laws and Standards**
FISMA
SOX
HIPAA