Department of CSE

- Course Name:-Ethical Hacking
- Course Code: UCSPE601
- Course Evaluation:
  - ESE Passing Marks – 20
  - Course Passing Marks – 40
- Faculty In charge: Ranjeeta Pandhare
- Course Prerequisite Knowledge:

- Basics of Computer System : Better
- Computer Network and OS : Better
- Network Security Fundamentals : Best

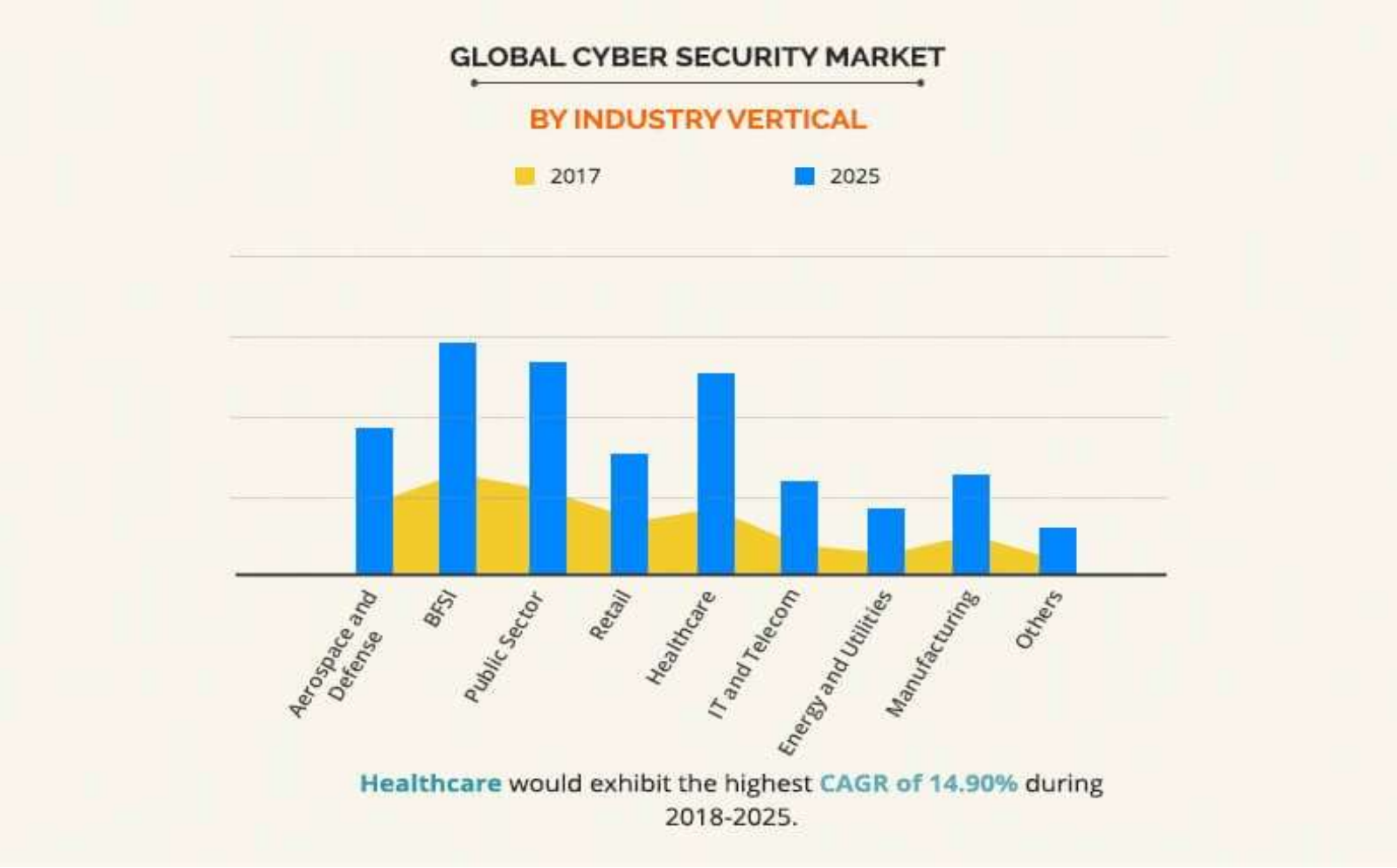
Component	Marks
ISE-I	10
ISE –II	10
MSE	30
ESE	50

Curriculum Emphasises on

Unit Wise:-

1. Introduction to Ethical Hacking and Cyber attacks
2. Methodology used for attacking computer systems and computer network
3. Demonstration of Sniffing and Social engineering attacks
4. Session Hijacking ,Firewall and Web server security configuration
5. Hacking different web application and SQL injection
6. Hacking different wireless and mobile networks

At Glance


GLOBAL CYBER SECURITY MARKET
BY INDUSTRY VERTICAL
2017
2025
Aerospace and Defense
BFSI
Public Sector
Retail
Healthcare
IT and Telecom
Energy and Utilities
Manufacturing
Others
Healthcare would exhibit the highest CAGR of 14.90% during 2018-2025.

Ethical Hacking

- Security and our Daily Life
- Possible Threats to Data on Computer
- Information Security Overview
- Data Breach Examples : eBay Data Breach in 2014

- ***Google Play Hack***
- A Turkish Hacker, "**Ibrahim Balic"** hacked Google Play twice.
- 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.
- 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.

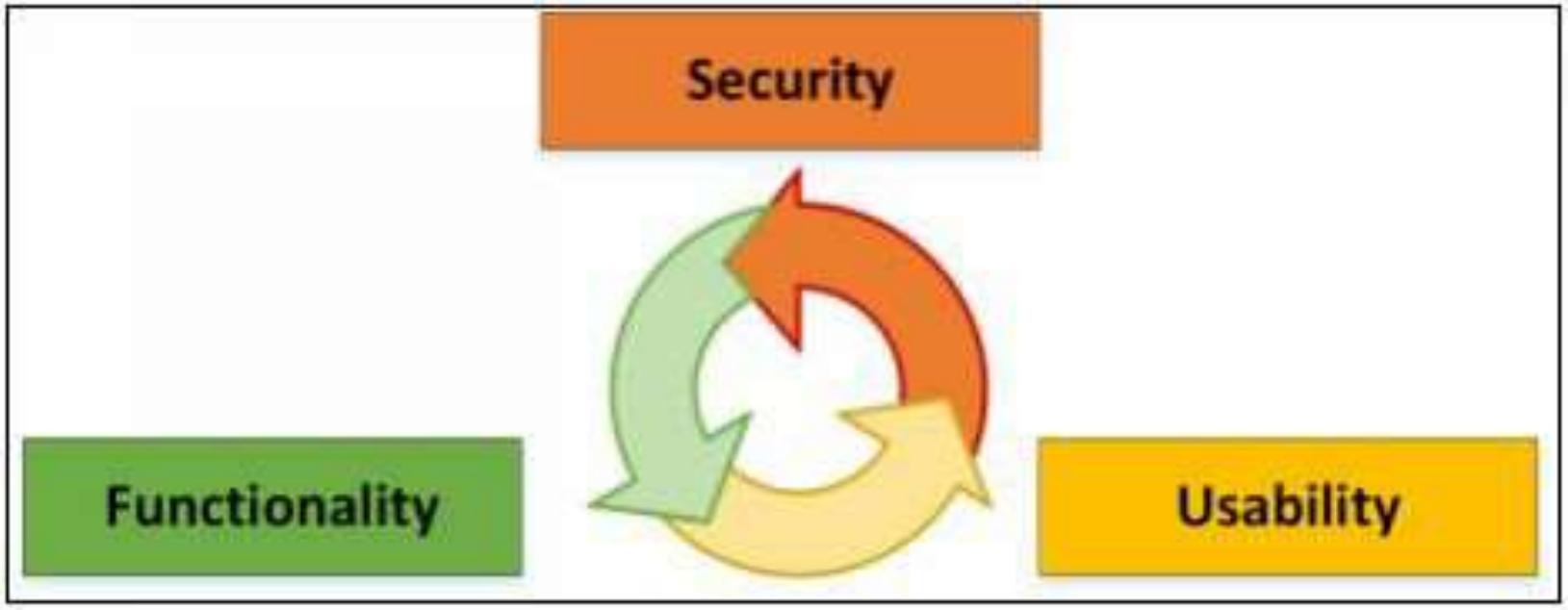
Essential Terminology

- **Hack Value-**Value describes the targets' level of attraction to the hacker.
- **Zero Day attack**-Zero-Day Attacks refers to threats and vulnerabilities that can exploit the victim before the developer identify or address and release any patch for that vulnerability.
- **Vulnerability**-weak point, loophole or a cause in any system or network which can be helpful and utilized by the attackers to go through it
- **Daisy Chaining**-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**-breach of security of a system through Vulnerabilities, Zero-Day Attacks or any other hacking techniques
- **Doxing**-Publishing information or a set of information associated with an individual.
- **Payload-**The payload refers to the actual section of information or data in a frame as opposed to automatically generated metadata
- **Bot**-The bots are software that is used to control the target remotely and to execute predefined tasks.

Elements of Information Security

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
three components of a triangle must be balanced.



Motive ,Goals and Objective of Security Attack

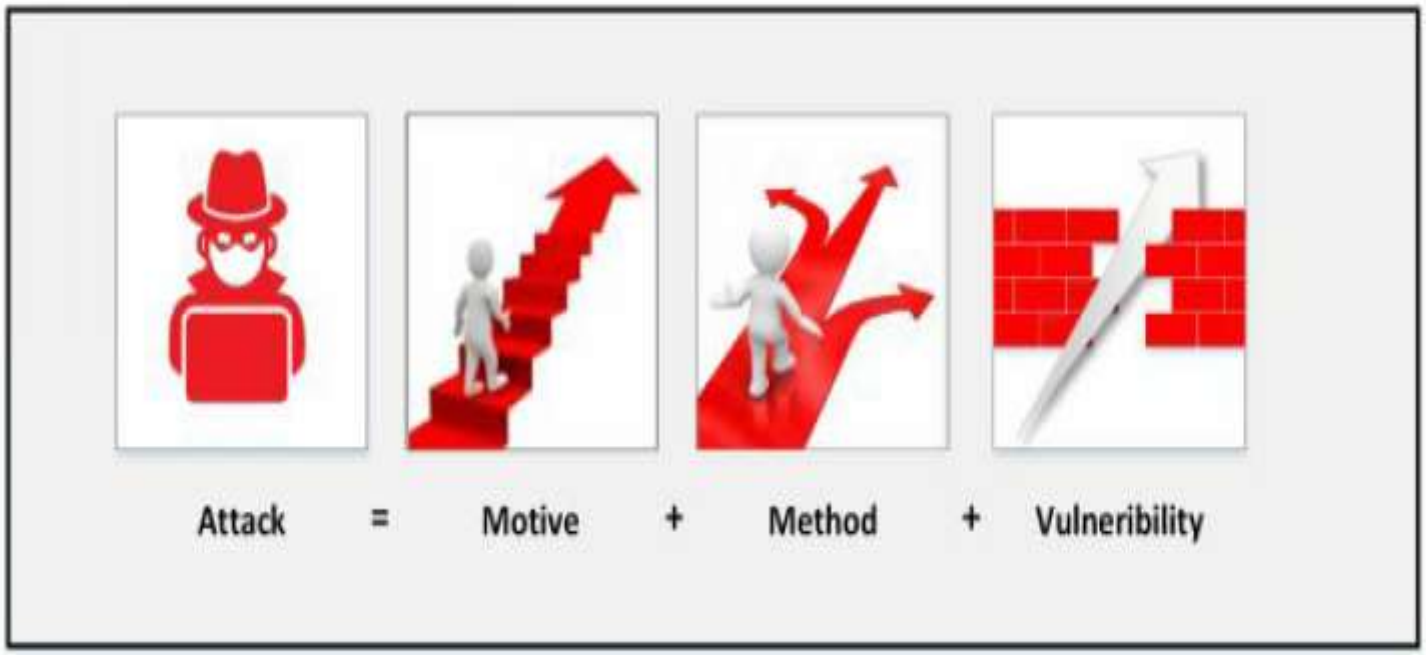


Figure 1-3 Information Security Attack

Top Information Security Attack Vectors

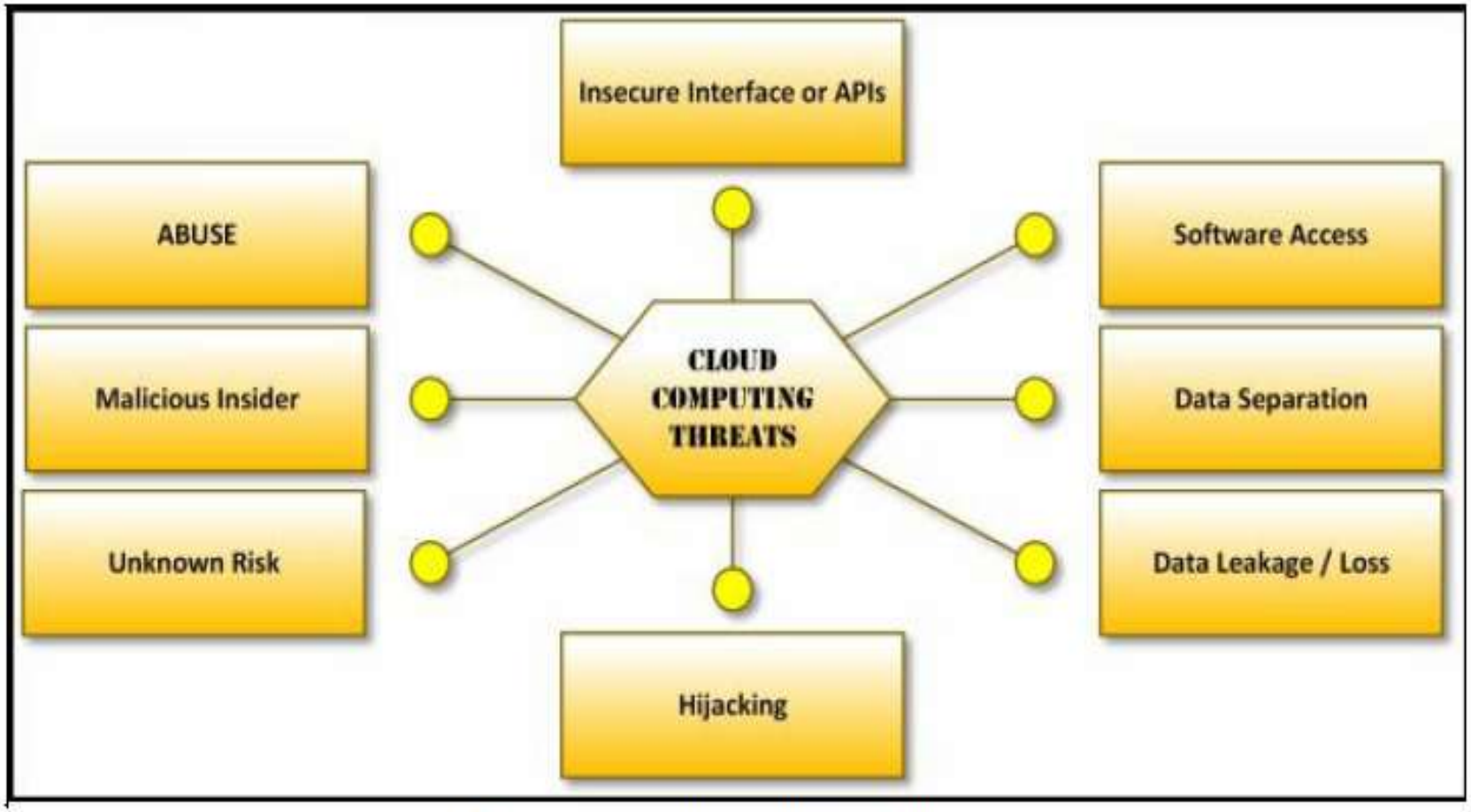


Figure 1-4 Cloud Computing Threats

Top Information Security Attack Vectors

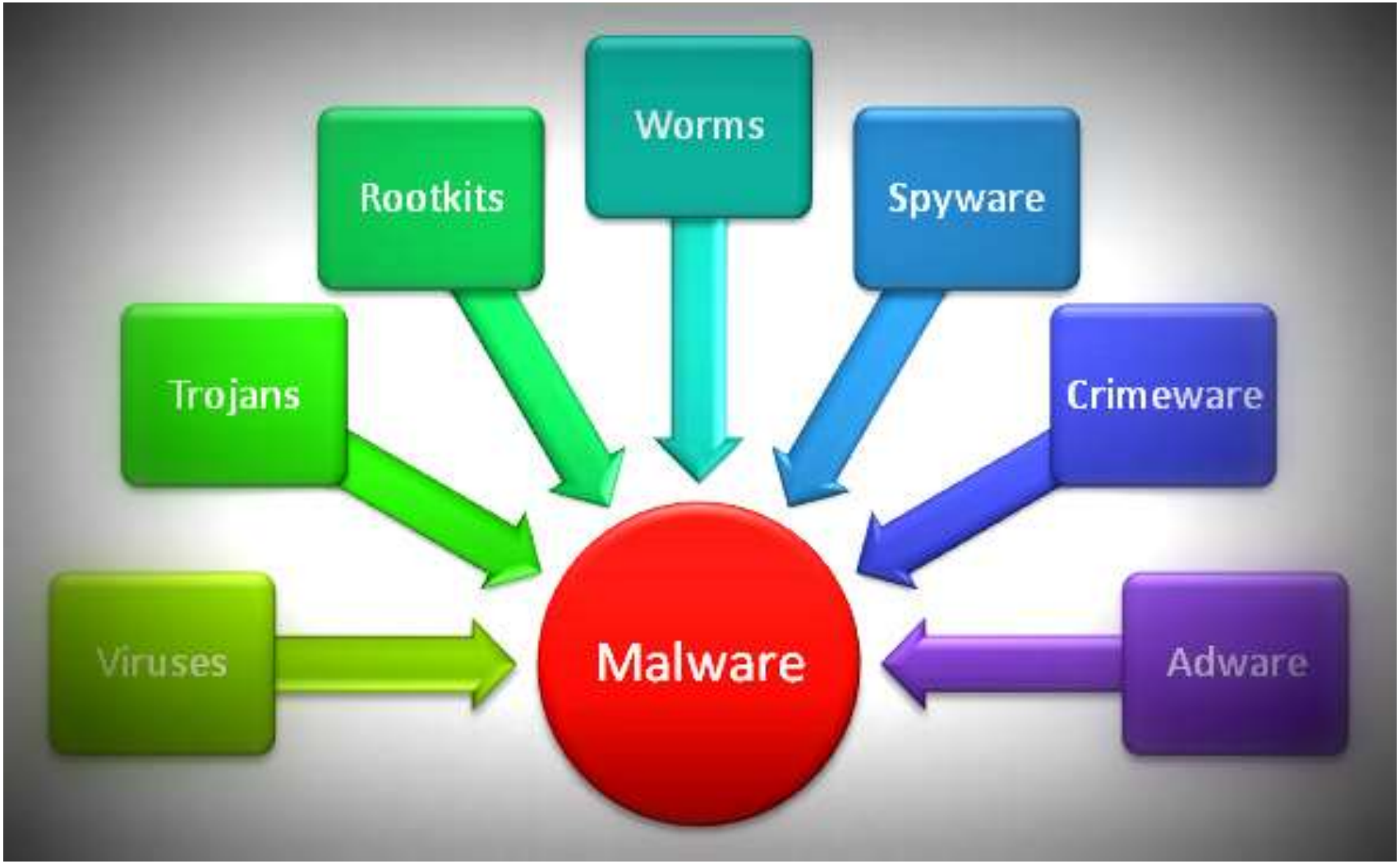
- *Advanced Persistent Threats*
- *Viruses and Worms*
- *Mobile Threats*

Advanced Persistent Threat

- An advanced persistent threat (APT) is the process of stealing information by a continuous process.
- APT 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 syst**em**
- **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

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.


Worms
Rootkits
Spyware
Trojans
Crimeware
Viruses
Malware
Adware

Insider Attack

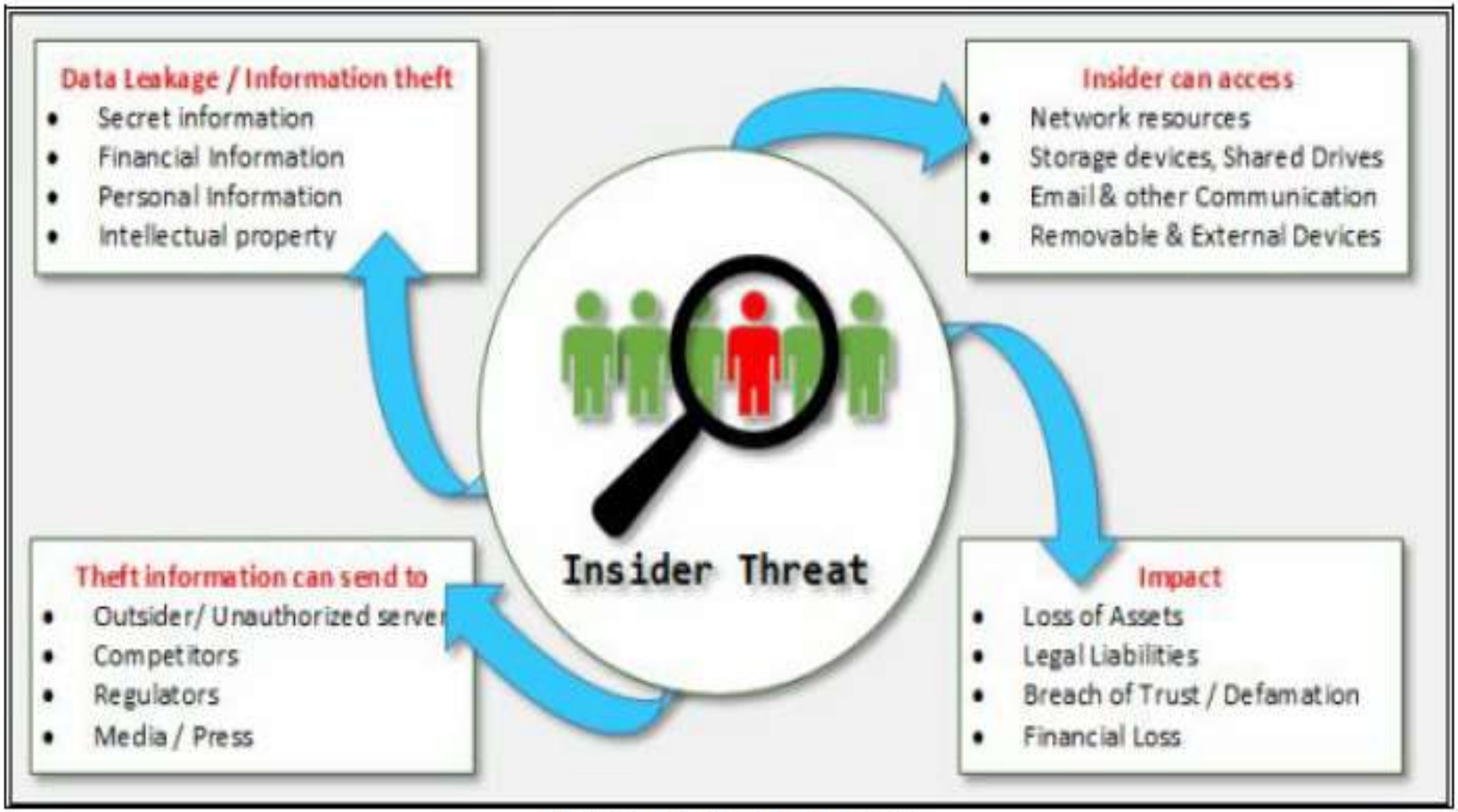


Figure 1-5 Insider Threats

Mobile threats

- Data leakage
- Unsecured Wi-Fi
- Network Spoofing
- Phishing Attacks
- Spyware
- Broken Cryptography
- Improper Session Handling

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.

Spider

- 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

NETWORK THREATS

- 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

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

APPLICATION THREATS

- Improper Data / Input Validation
- Authentication & AuthorizationAttack
- Security Misconfiguration
- Information Disclosure
- Broken Session Management
- Buffer Overflow Issues
- Cryptography Attacks
- SQL Injection
- Improper Error handling & Exception Management

SYSTEM ATTACKS

- Operating System Attacks
  - Buffer overflow vulnerabilities
  - Bugs in the operating system
  - Unpatched operating system
- Misconfiguration Attacks
- Application-Level Attacks
- Shrink Wrap Code Attacks

BUFFER OVERFLOW

- is one of the major types of Operating System Attacks.
- related to software exploitation attacks.
- 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

- Vulnerability 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

- allows malicious activities, or could not completely block malicious traffic into a system
- compromising sensitive information, data loss and disruption of regular operation

APPLICATION LEVEL ATTACKS

- Buffer overflow
- Active content
- Cross-site script
- Denial of service
- SQL injection
- Session hijacking
- Phishing

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

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

Information Warfare

- **Defensive Information Warfare**
  - Prevention
  - Deterrence
  - Indication & Warning
  - Detection
  - Emergency Preparedness
  - Response
- **Offensive Information Warfare**
  - an aggressive operation that is taken against the enemies dynamically instead of waiting for the attackers to launch an attack

Types of Hacker

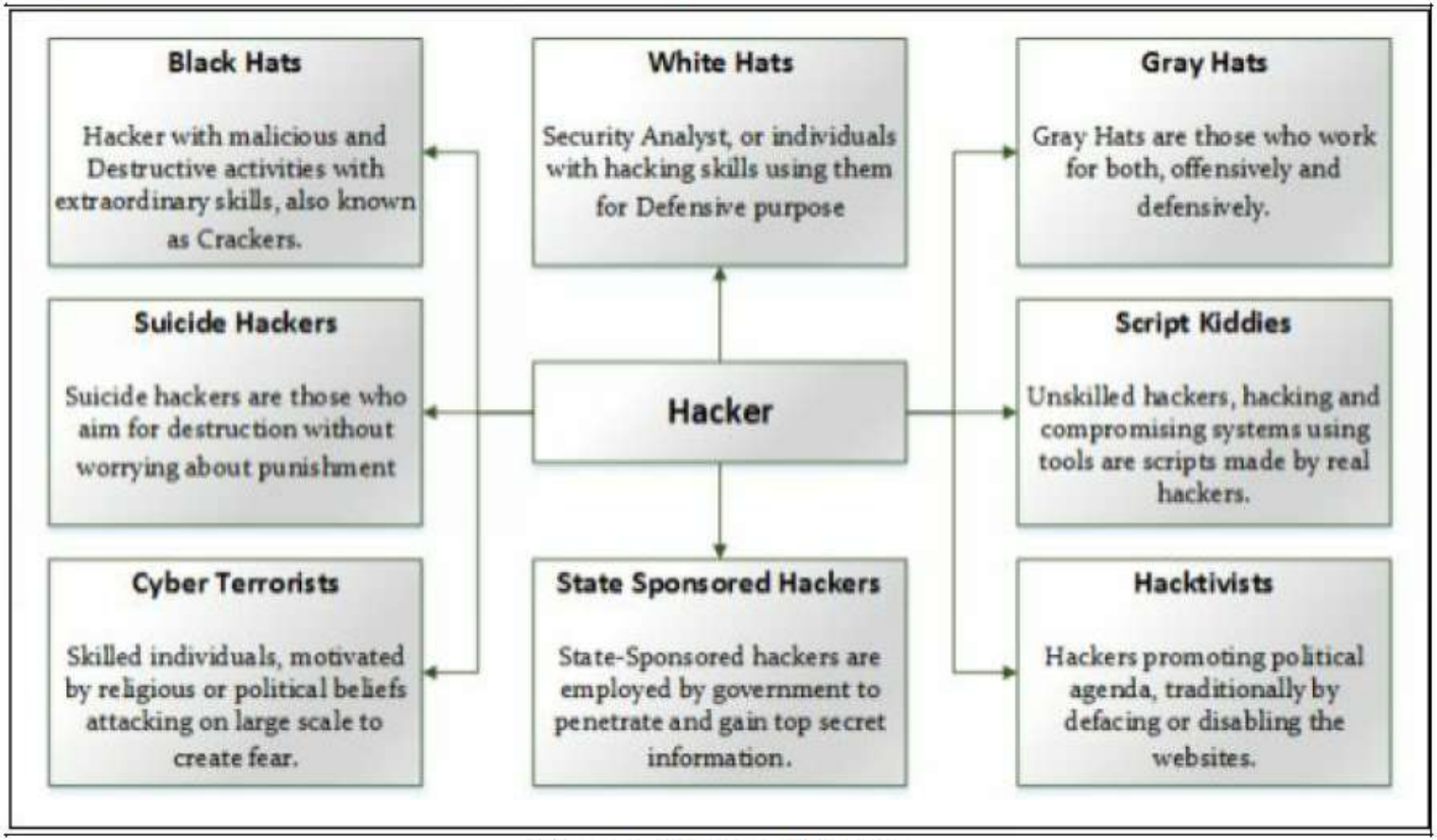


Figure 1-6 Types of Hacker

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.

Hacking Phases

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Clearing Tracks

Reconnaissance

- 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.
- 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 phase

- pre-attack phase.
- attacker scans the network by information acquired during the initial phase of reconnaissance.
- Scanning tools -Dialler, Scanners such as Port scanners, Network mappers, client tools such as ping, as well as vulnerabilities scanner.
- 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 phase

- 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

- 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 and penetration testing are common terms, popular in information security environment for a long time
- Fundamental Challenges to these security experts are of finding weaknesses and deficiencies in running and upcoming systems, applications, software and addressing them proactively

Why Ethical Hacking is Necessary

- The rise in malicious activities, cybercrimes and appearance of different forms of advanced attacks
- increase of use of online transaction and online services in the last decade.
- more attractive for hackers and attackers to tempt to steal financial Information
- 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.

Aggressive and advanced attacks

- Denial-of-Services Attacks
- Manipulation of data
- Identity Theft
- Vandalism
- Credit Card theft
- Piracy
- Theft of Services

Phases of Ethical Hacking

- Footprinting & Reconnaissance
- Scanning
- Enumeration
- System Hacking
- Escalation of Privileges
- Covering Tracks

Footprinting

- **Know Security Posture** – The data gathered will help us to get an overview of the security posture of the company such as details about the presence of a firewall, security configurations of applications etc.
- **Reduce Attack Area** – Can identify a specific range of systems and concentrate on particular targets only. This will greatly reduce the number of systems we are focussing on.
- **Identify vulnerabilities** – we can build an information database containing the vulnerabilities, threats, loopholes available in the system of the target organization.
- **Draw Network map** – helps to draw a network map of the networks in the target organization covering topology, trusted routers, presence of server and other information.

Footprinting

- Domain name
- IP Addresses
- Namespaces
- Employee information
- Phone numbers
- E-mails
- Job Information

- Domain Name Information
- You can use http://www.whois.com/whois
- ip2location.com website
- You can obtain a range of IP addresses assigned to a particular company using American Registry for Internet Numbers (ARIN).
- complete history of any website using www.archive.org

Passive footprinting

- DNS expiry info can be used illegally
- Eg : google pays 8 lakhs to Sanmay Ved who bought google.com
- NEW YORK: Search engine giant Google has paid Sanmay Ved, the man who owned Google.com for a minute, $6,006.13 (about Rs 4.07 lakh) and later doubled the amount when he donated his reward to charity.

  In September last year, the ex-Googler, while searching Google Domains, found that Google.com (domain name) was available for purchase. He bought the domain for $12 and gained access to its webmaster tools before Google cancelled the sale.

  However, the Mandvi resident (in country's Kutch region) had said it was never about money and wanted the amount to be donated to the Art of Living India Foundation.

- Inurl index.shtml
- footprinting hacking filetype .ppt site:edu
- https://www.iplocation.net/
- http://www.ipvoid.com/
- https://iplogger.org/
- https://www.greycampus.com/opencampus/ethical-hacking/what-is-ethical-hacking

Scanning

- Scanning is a set of procedures for identifying live hosts, ports, and services, discovering Operating system and architecture of target system, Identifying vulnerabilities and threats in the network.
- Network scanning is used to create a profile of the target organization.
- Scanning refers to collecting more information using complex and aggressive reconnaissance techniques.

Scanning Methodology

- **Check for Live Systems:** Ping scan checks for the live system by sending ICMP echo request packets. If a system is alive, the system responds with ICMP echo reply packet containing details of TTL, packet size etc.
- **Check for Open Ports:** Port scanning helps us to find out open ports, services running on them, their versions etc. Nmap is the powerful tool used mainly for this purpose.

Enumeration

- Enumeration is defined as the process of extracting user names, machine names, network resources, shares and services from a system.
- the attacker creates an active connection to the system and performs directed queries to gain more information about the target.
- The gathered information is used to identify the vulnerabilities or weak points in system security and tries to exploit in the System gaining phase.

Techniques for Enumeration

- Extracting user names using email ID's
- Extract information using the default password
- Brute Force Active Directory
- Extract user names using SNMP
- Extract user groups from Windows
- Extract information using DNS Zone transfer

System Hacking

- Goals:

1. Gaining Access-Password cracking , password attacks
2. Escalating privileges
3. Executing applications
4. Hiding files
5. Clearing tracks

Escalating privileges

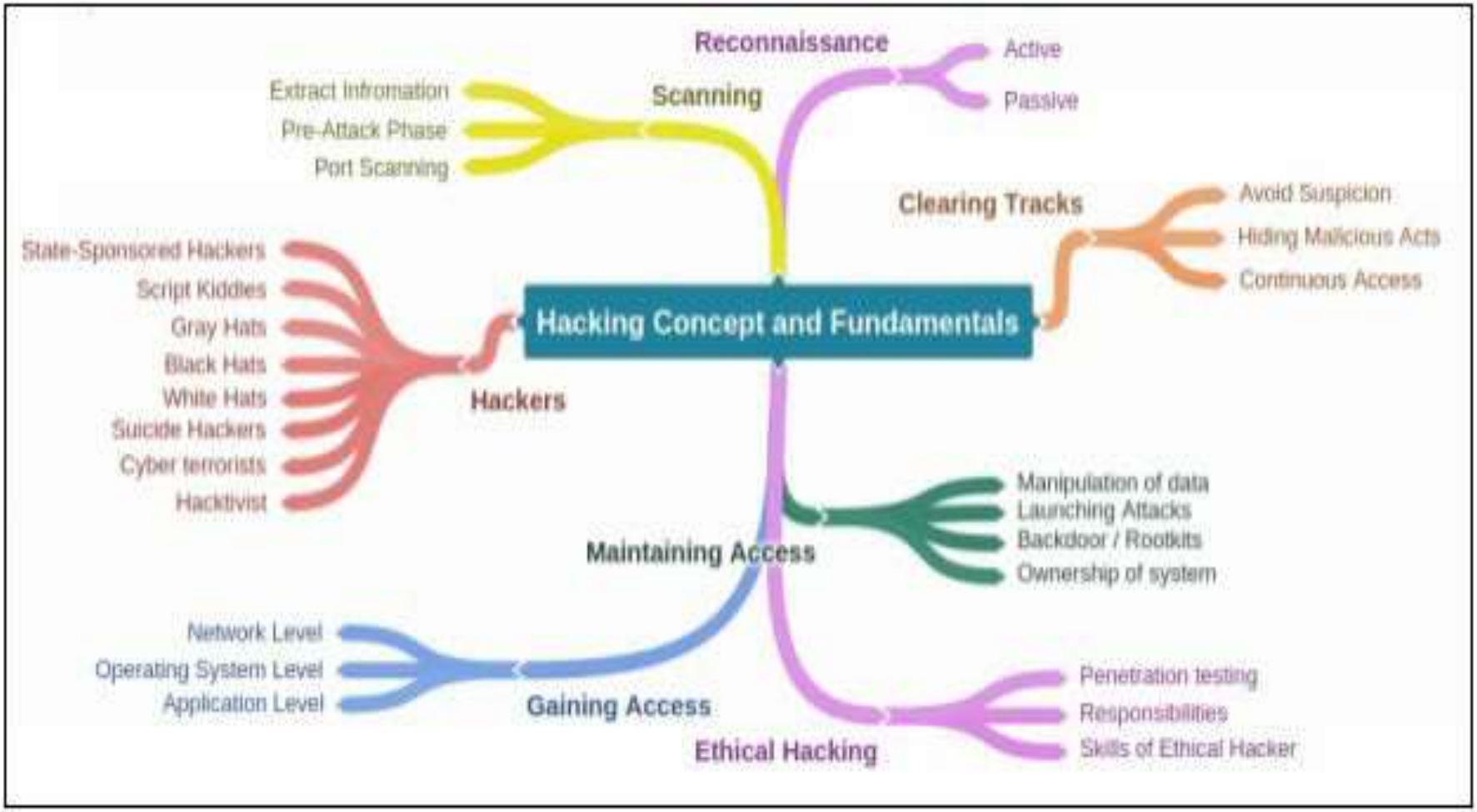
- An attacker can gain access to the network using a non-admin user account, and the next step would be to gain administrative privilege.
- Horizontal
- Vertical

Skills of an Ethical Hacker

- ***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. 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.


Hacking Concept and Fundamentals
Reconnaissance
Active
Passive
Scanning
Extract Information
Pre-Attack Phase
Port Scanning
Clearing Tracks
Avoid Suspicion
Hiding Malicious Acts
Continuous Access
Hackers
State-Sponsored Hackers
Script Kiddies
Gray Hats
Black Hats
White Hats
Suicide Hackers
Cyber terrorists
Hacktivist
Maintaining Access
Manipulation of data
Launching Attacks
Backdoor / Rootkits
Ownership of system
Gaining Access
Network Level
Operating System Level
Application Level
Ethical Hacking
Penetration testing
Responsibilities
Skills of Ethical Hacker

Vulnerability Assessment

- Vulnerability assessment is the procedure of examination, identification, and analysis of system or application abilities including security processes running on a system

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

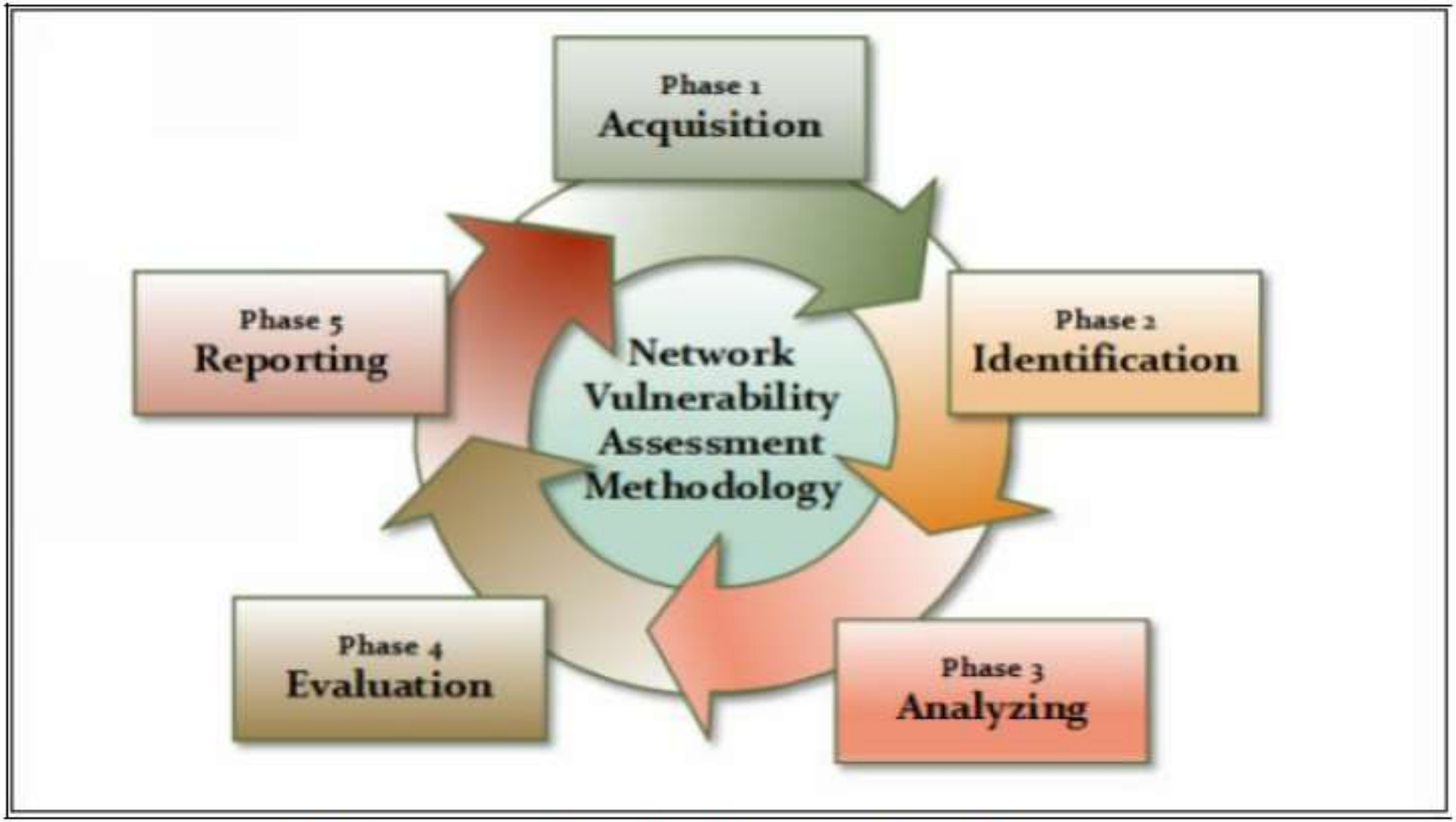
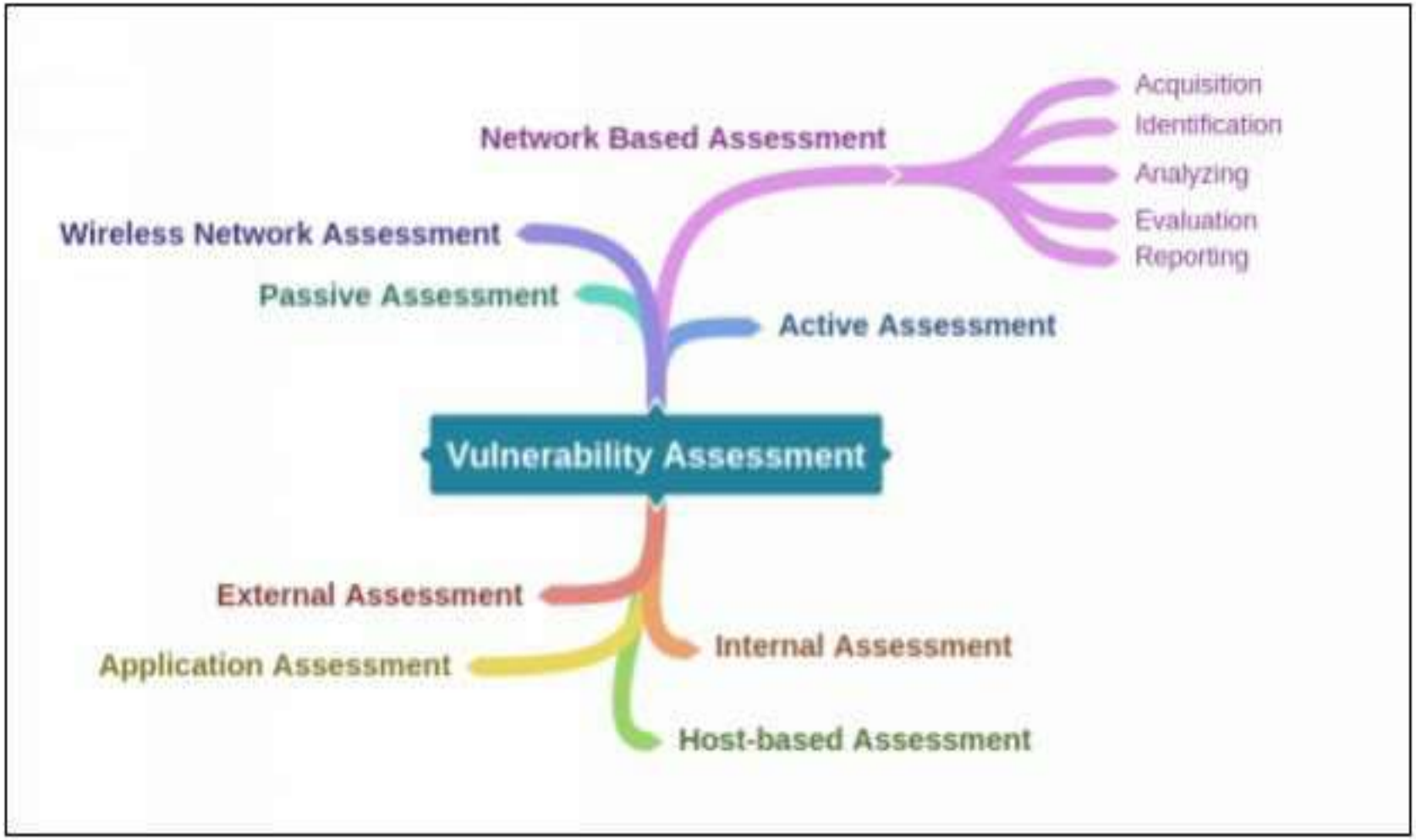


Figure 1-13 Network Vulnerability Assessment Methodology

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*** 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


Vulnerability Assessment
Network Based Assessment
Acquisition
Identification
Analyzing
Evaluation
Reporting
Wireless Network Assessment
Passive Assessment
Active Assessment
External Assessment
Application Assessment
Internal Assessment
Host-based Assessment

Penetration Testing

- 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.

Pentester

- Pentesters are the penetration tester that has permission to hack a system by owner

Pentesting Comparison

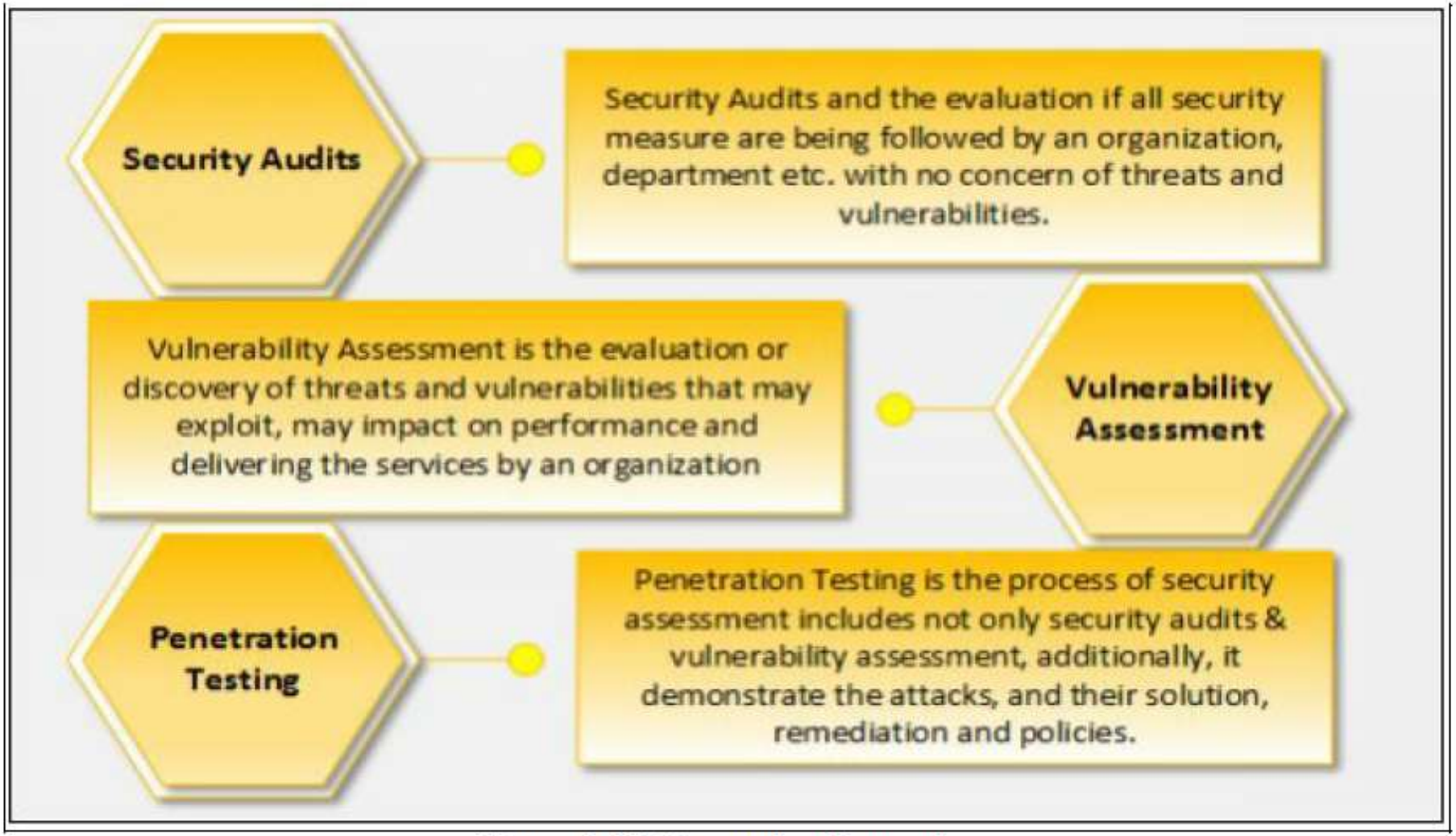


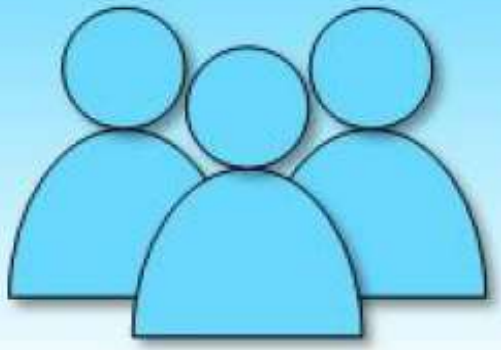
Figure 1-13 Comparing Pentesting

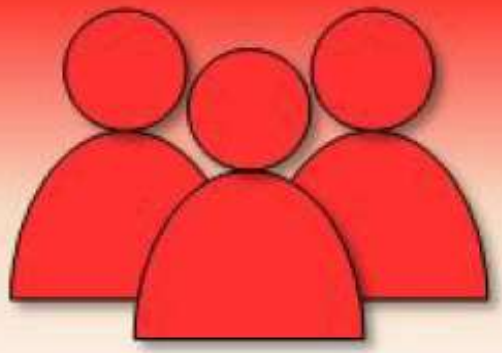
Pentesting Advantages

- 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).

Blue and Red Teaming

Blue teaming is an approach, in which a security team is responsible for performing analysis of security control & efficiency of an information security system. They detect and mitigate red team attacks.





In Red teaming approach, a team of ethical hacker or pen testers are responsible for system penetration with limited or without any granted access to internal resources. security control & efficiency of an information security system. They detect and evaluate vulnerabilities form an attackers perspective.

Figure 1-14 Comparing Blue & Red Teaming

	Red Team	Blue Team
Role	Attackers	Defenders
Objective	Identify vulnerabilities, test defenses, and find ways to breach security.	Protect systems, detect attacks, respond to incidents, and recover from breaches.
Methodology	Simulate real-world attacks and use tactics similar to those used by real attackers.	Use preventive measures, detect suspicious activities, and respond to security incidents.
Tools	Penetration testing tools, exploit development, social engineering techniques, etc.	Firewalls, IDS/IPS, SIEM, threat hunting tools, patch management, log analyzers, etc.
Mindset	Offensive - to find weak points in security and exploit them.	Defensive - to secure systems, networks, and data, and react appropriately to any threats.
Outcome	Provide a detailed report of findings and suggest improvements.	Secure organization's assets, ensure compliance with security policies, and manage risks.

Types of Penetration Testing

- 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
- 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

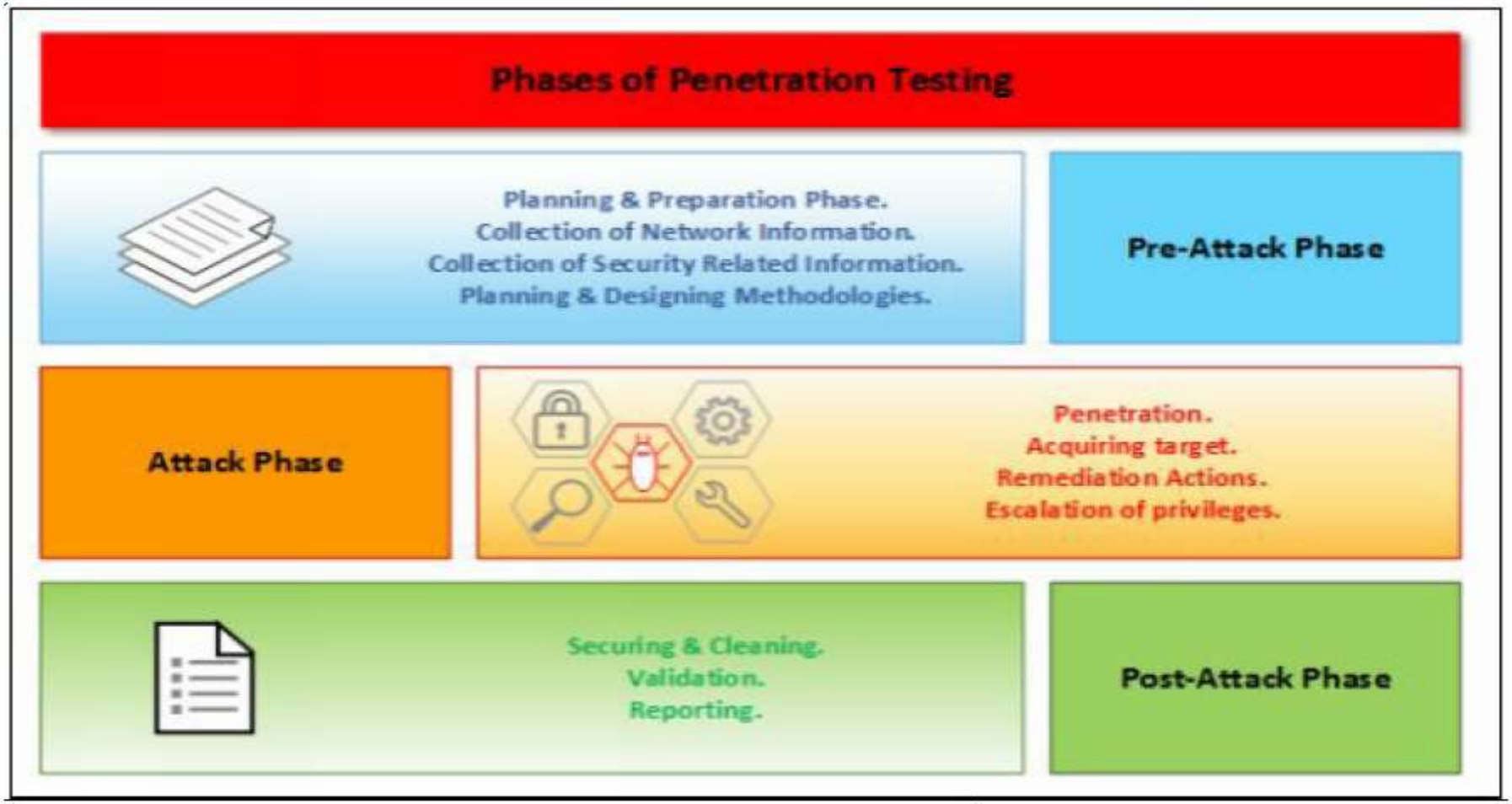


Figure 1-15 Penetration Testing Phases

Security Testing Methodology

- 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

Information Security Laws and Standards

- Payment Card Industry Data Security Standard (PCI-DSS)
- ISO/IEC 27001:2013
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes Oxley Act (SOX)