
Important Questions [Ethical Hacking]

~ Sudha Mam

1.) What are the different attack factors through which attacker can attack information system. Explain them.

There are several attack factors that an attacker can use to target an information system. Here are some of the most common ones:

Malware: Malware is malicious software that can be used to harm an information system. It can include viruses, worms, Trojans, ransomware, and spyware. Malware can be used to steal sensitive information, destroy data, or disrupt normal operations of the system.

Social engineering: Social engineering is the art of manipulating people to divulge sensitive information or to perform actions that can compromise the security of the information system. Social engineering attacks can include phishing, pretexting, baiting, and spear phishing.

Password attacks: Password attacks are designed to crack or steal user passwords. Attackers can use different techniques like brute-force attacks, dictionary attacks, and phishing to obtain passwords.

Denial of service (DoS) attacks: Denial of service attacks are aimed at disrupting the availability of a system by overloading it with traffic or by sending malformed packets. This can lead to the system being unavailable to legitimate users.

Man-in-the-middle (MITM) attacks: Man-in-the-middle attacks occur when an attacker intercepts communication between two parties and can modify, read or inject malicious data into it. This can enable the attacker to steal sensitive data or credentials.

Physical attacks: Physical attacks involve the physical compromise of the system or its components. This can include theft of hardware, unauthorized access to restricted areas, and tampering with the system hardware.

SQL injection attacks: SQL injection attacks are aimed at exploiting vulnerabilities in web applications that use SQL databases. Attackers can insert malicious SQL code in input fields, which can enable them to gain unauthorized access to data or perform unintended operations.

Cross-site scripting (XSS) attacks: XSS attacks are aimed at exploiting vulnerabilities in web applications that allow attackers to inject malicious scripts into web pages viewed by other users. This can enable the attacker to steal sensitive data or to take control of the user's browser.

These are just a few of the many attack factors that can be used by attackers to target information systems. It's important to be aware of these threats and to implement appropriate security measures to protect against them.

2.) Classify the categories of information security threat. Explain each category in detail.

Information security threats can be classified into several categories based on their nature and the impact they can have on an organization. Here are some of the most common categories of information security threats:

Human threats: Human threats are threats that come from employees, contractors, or other authorized individuals who have access to an organization's information systems.

These threats can include intentional actions, such as theft or sabotage, as well as unintentional actions, such as mistakes or negligence.

Malicious software: Malicious software, or malware, is software that is designed to harm a computer system or to steal data. Malware can include viruses, worms, Trojans, ransomware, and spyware. Malware can be introduced into a system through email attachments, downloads, or infected media.

Physical threats: Physical threats are threats that come from physical sources, such as theft, damage, or destruction of hardware or media. Physical threats can include theft of laptops or other mobile devices, destruction of servers, or damage to network infrastructure.

Network threats: Network threats are threats that exploit vulnerabilities in a network or its components. Network threats can include denial-of-service attacks, spoofing attacks, man-in-the-middle attacks, and eavesdropping attacks.

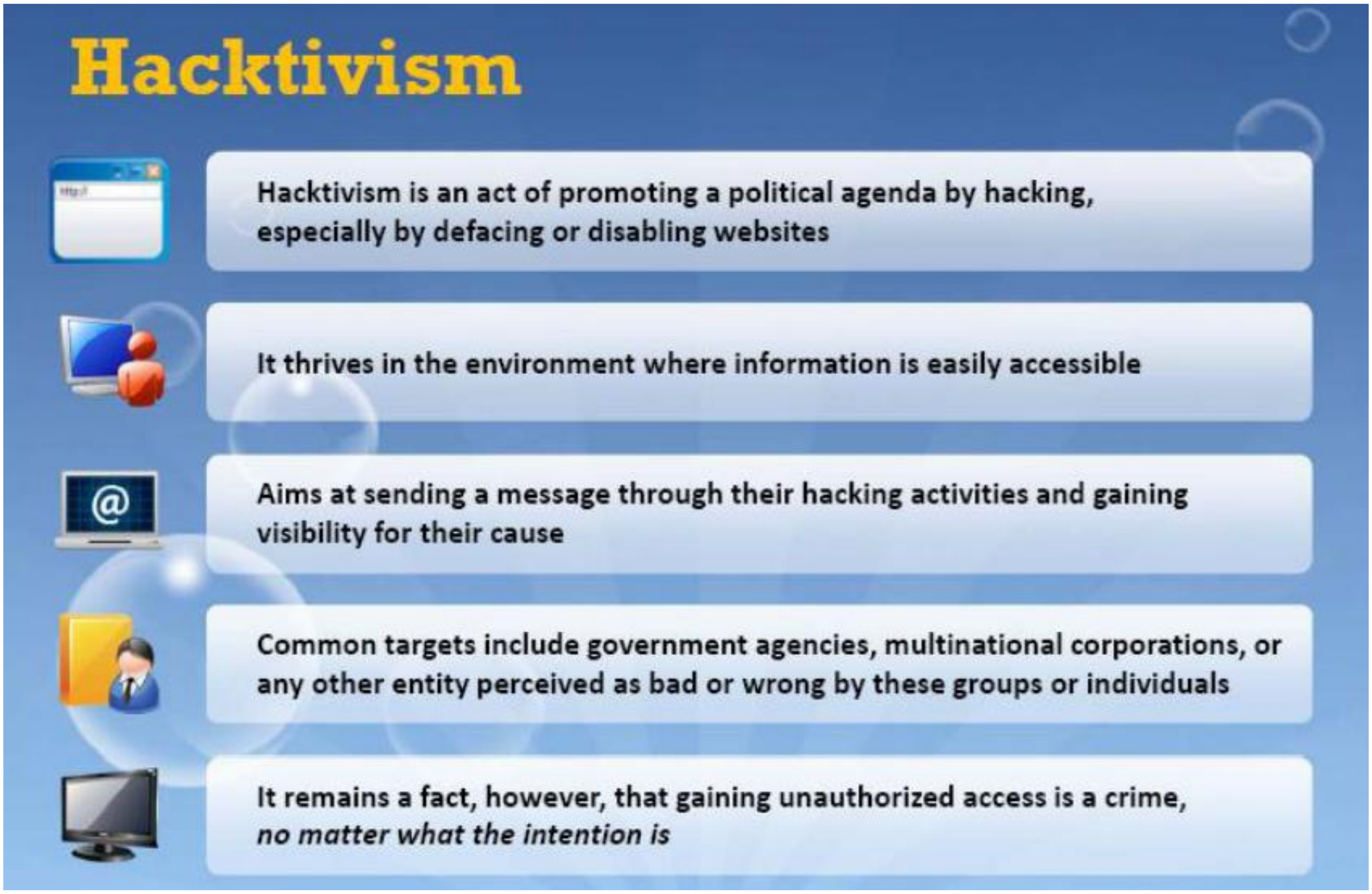
Application threats: Application threats are threats that exploit vulnerabilities in software applications. Application threats can include SQL injection attacks, cross-site scripting (XSS) attacks, and buffer overflow attacks.

Environmental threats: Environmental threats are threats that come from natural or environmental sources, such as floods, earthquakes, fires, or power outages. Environmental threats can cause damage to hardware or media, or they can disrupt network or power infrastructure.

Social engineering: Social engineering is a category of threat that exploits human psychology to trick people into revealing sensitive information or performing actions that compromise the security of a system. Social engineering attacks can include phishing, pretexting, baiting, and spear phishing.

Each of these categories of information security threats represents a different type of threat that an organization may face. It's important for organizations to understand the nature of these threats and to implement appropriate security measures to protect against them.

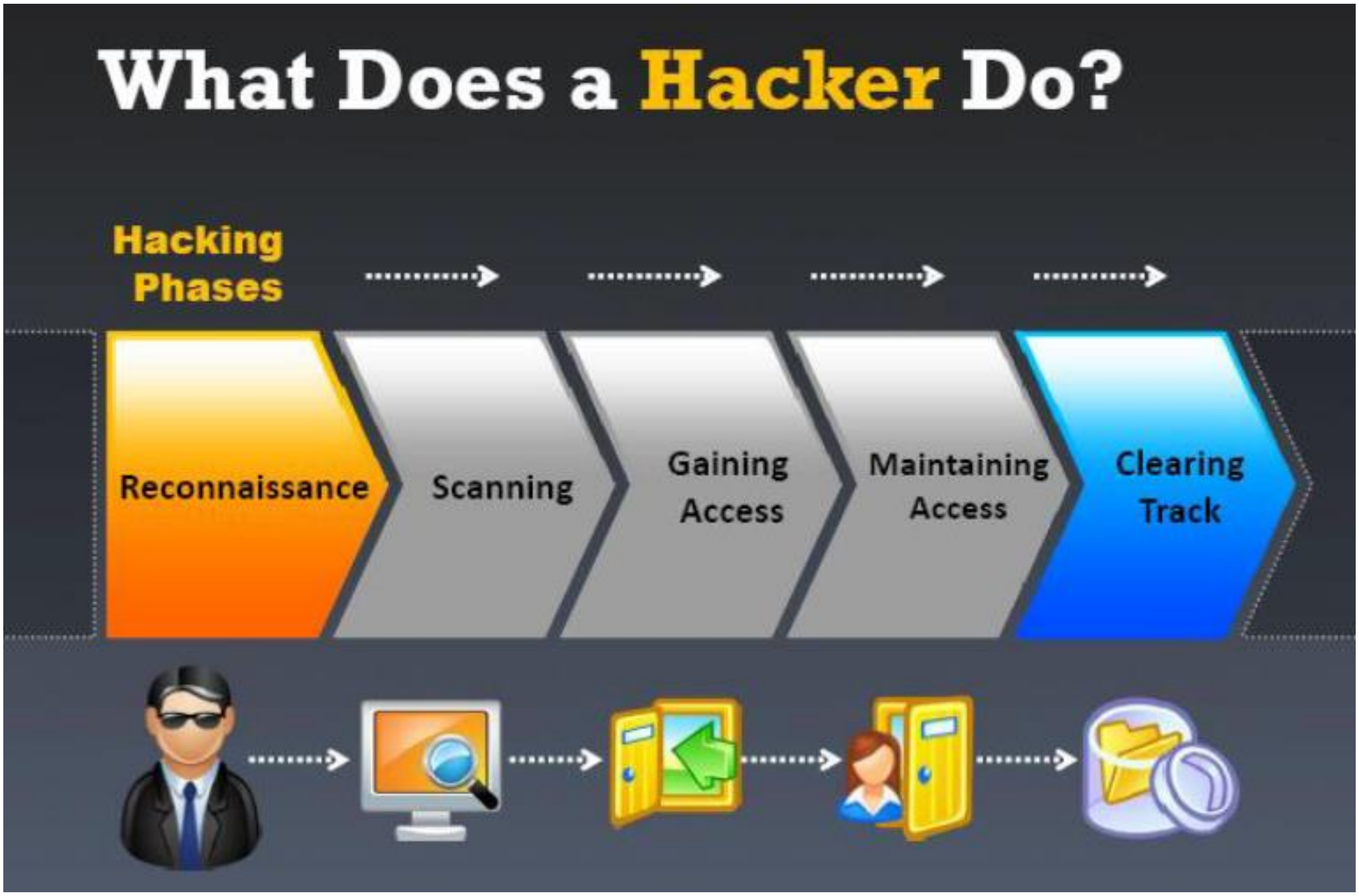
3.) What is hactivism? Explain it.



Hacktivism

- Hacktivism is an act of promoting a political agenda by hacking, especially by defacing or disabling websites
- It thrives in the environment where information is easily accessible
- Aims at sending a message through their hacking activities and gaining visibility for their cause
- Common targets include government agencies, multinational corporations, or any other entity perceived as bad or wrong by these groups or individuals
- It remains a fact, however, that gaining unauthorized access is a crime, *no matter what the intention is*

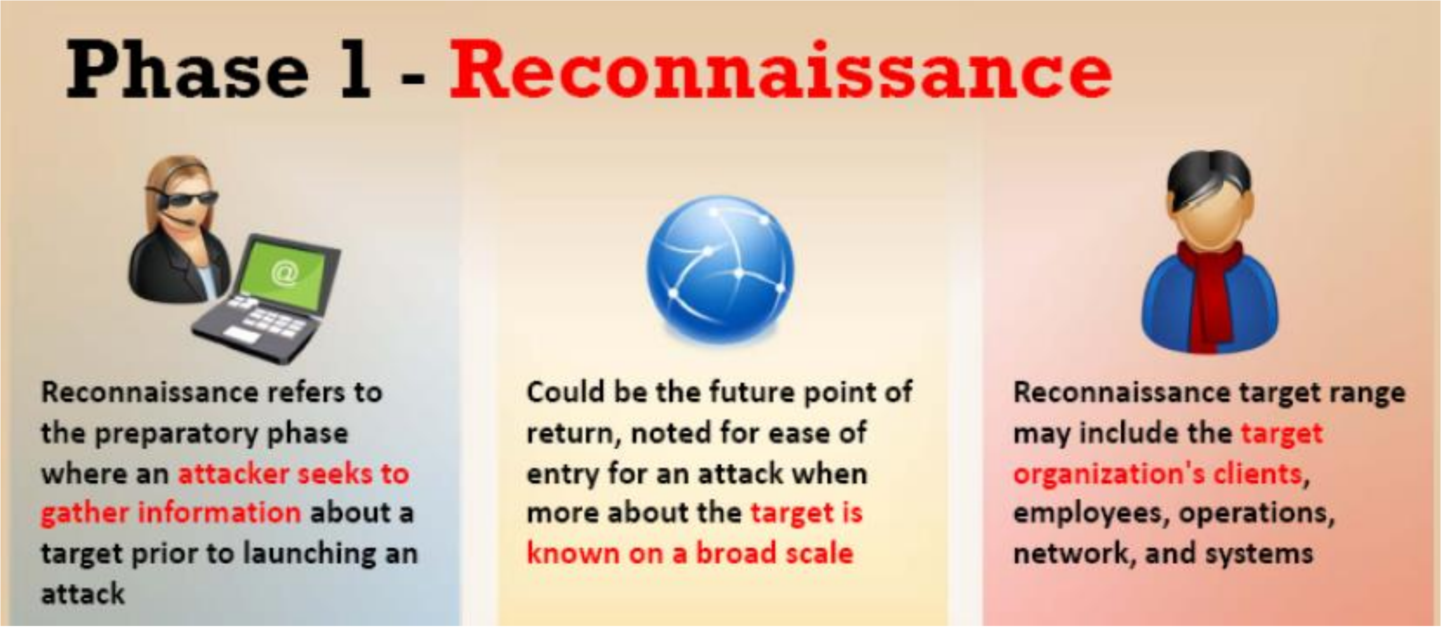
4.) Enumerate different phases of Hacking. Explain each in detail



What Does a Hacker Do?

Hacking Phases

Reconnaissance → Scanning → Gaining Access → Maintaining Access → Clearing Track

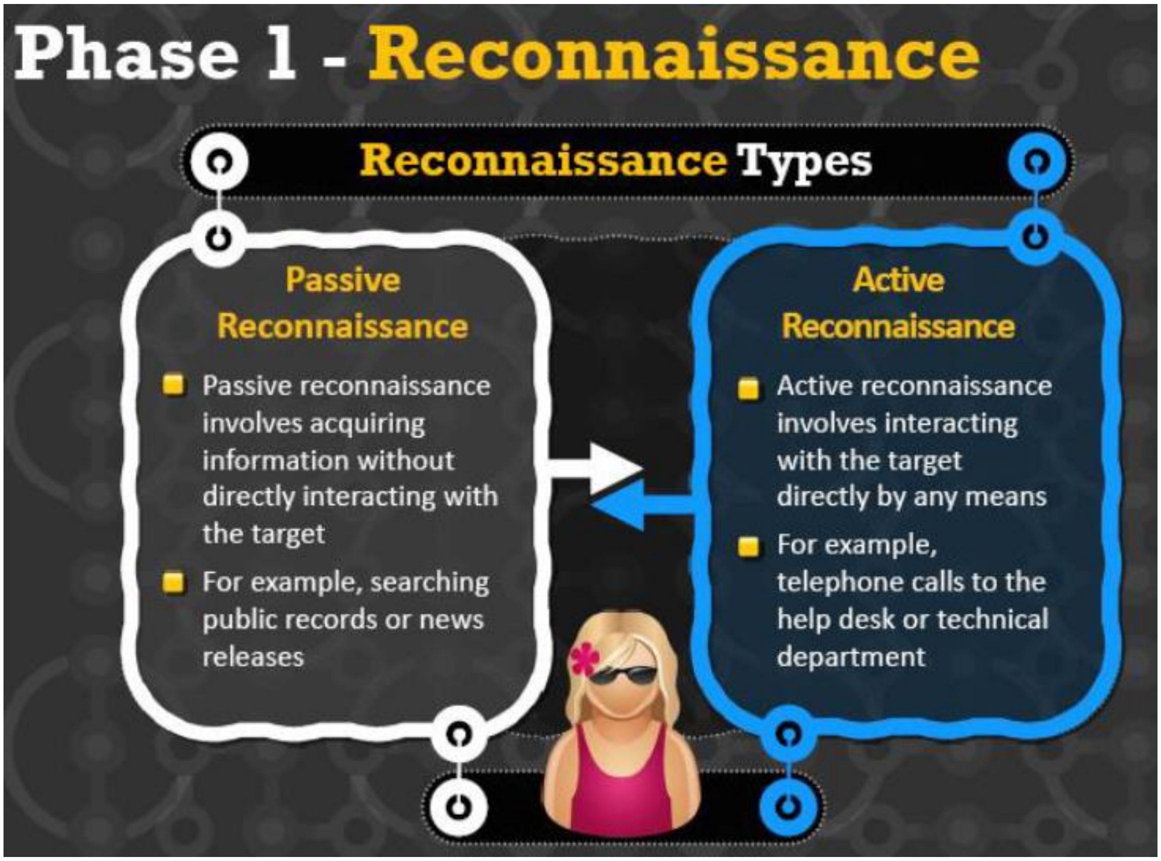


Phase 1 - Reconnaissance

Reconnaissance refers to the preparatory phase where an attacker seeks to gather information about a target prior to launching an attack

Could be the future point of return, noted for ease of entry for an attack when more about the target is known on a broad scale

Reconnaissance target range may include the target organization's clients, employees, operations, network, and systems



Phase 1 - Reconnaissance

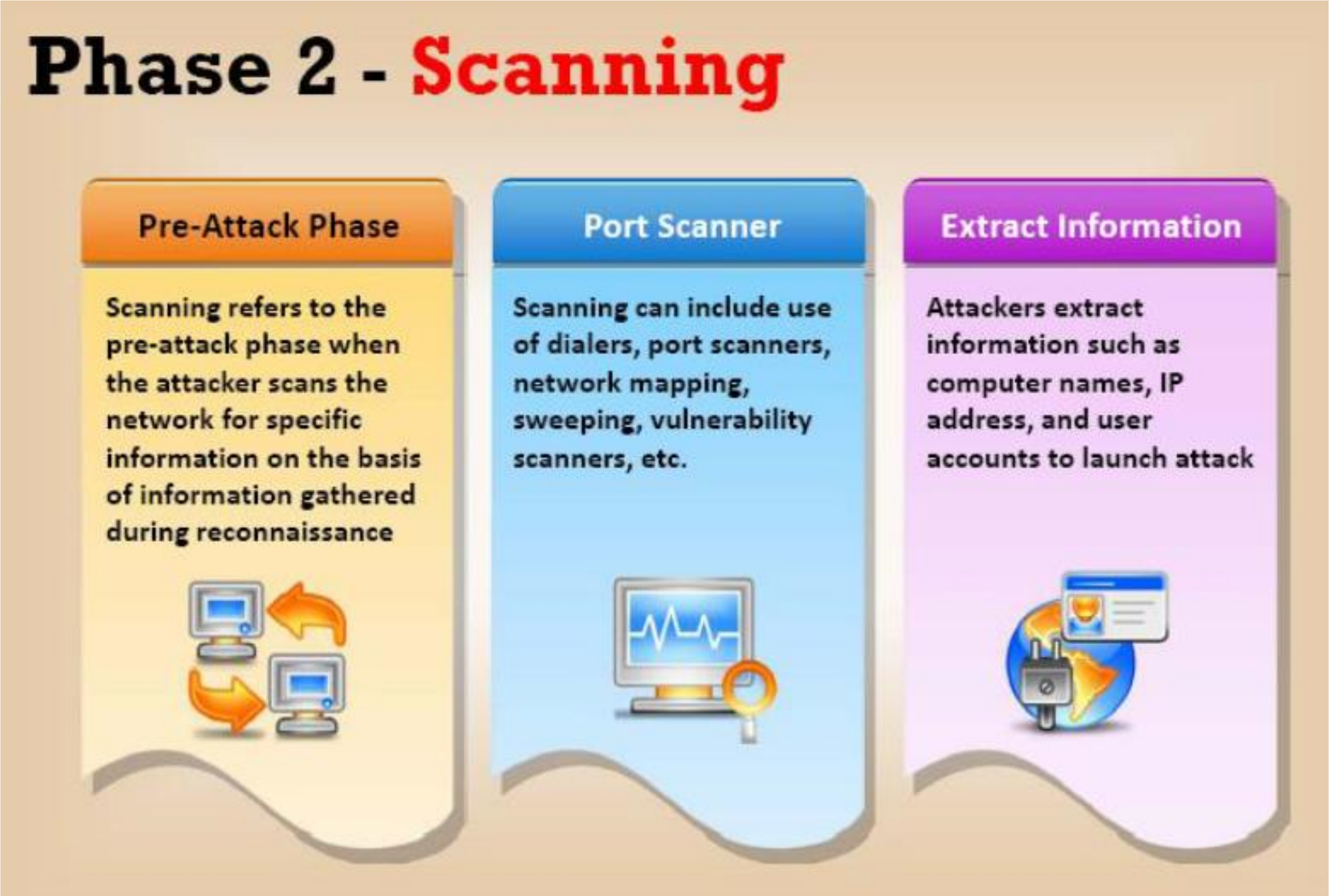
Reconnaissance Types

Passive Reconnaissance

- Passive reconnaissance involves acquiring information without directly interacting with the target
- For example, searching public records or news releases

Active Reconnaissance

- Active reconnaissance involves interacting with the target directly by any means
- For example, telephone calls to the help desk or technical department



Phase 2 - Scanning

Pre-Attack Phase

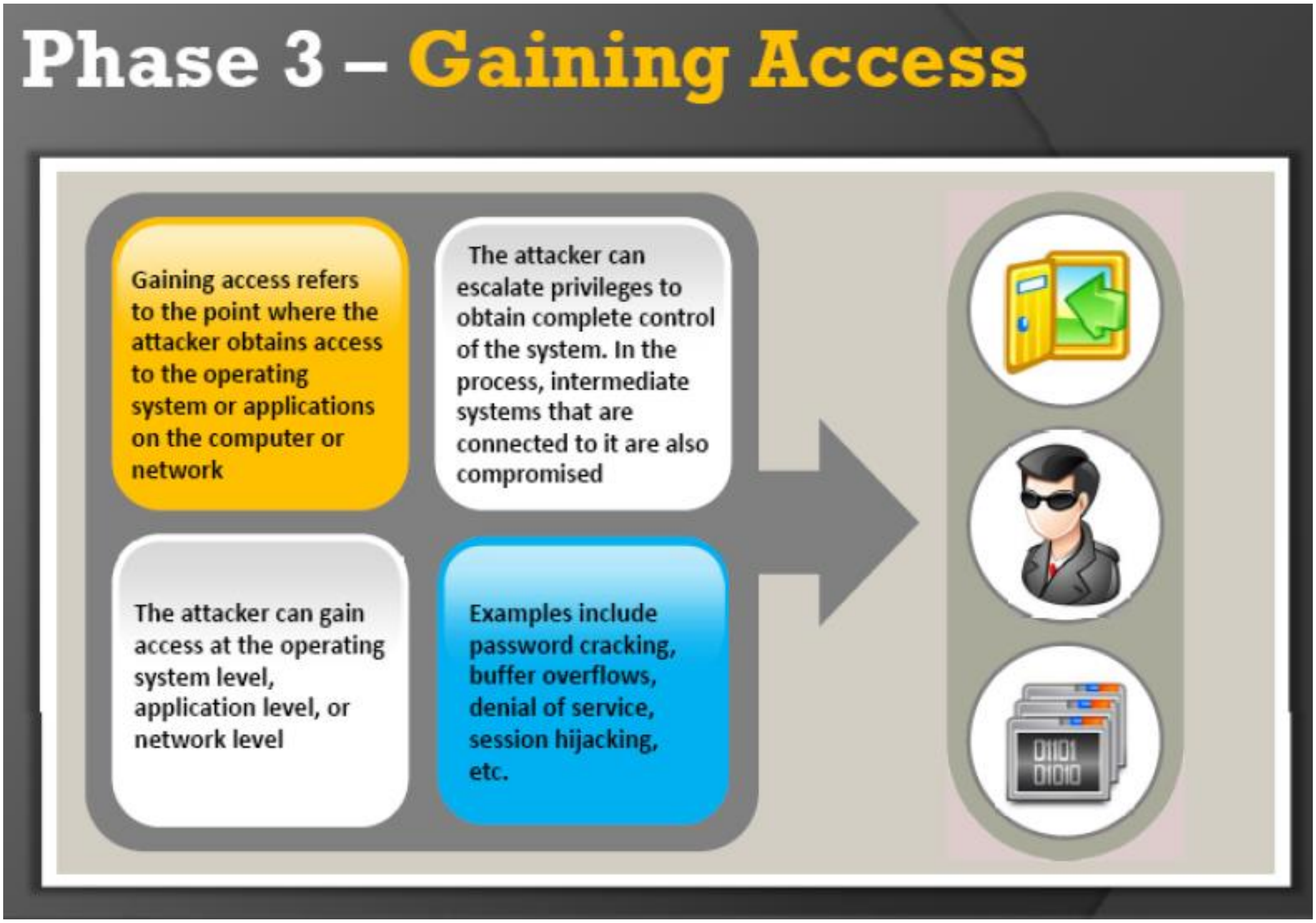
Scanning refers to the pre-attack phase when the attacker scans the network for specific information on the basis of information gathered during reconnaissance

Port Scanner

Scanning can include use of dialers, port scanners, network mapping, sweeping, vulnerability scanners, etc.

Extract Information

Attackers extract information such as computer names, IP address, and user accounts to launch attack



Phase 3 – Gaining Access

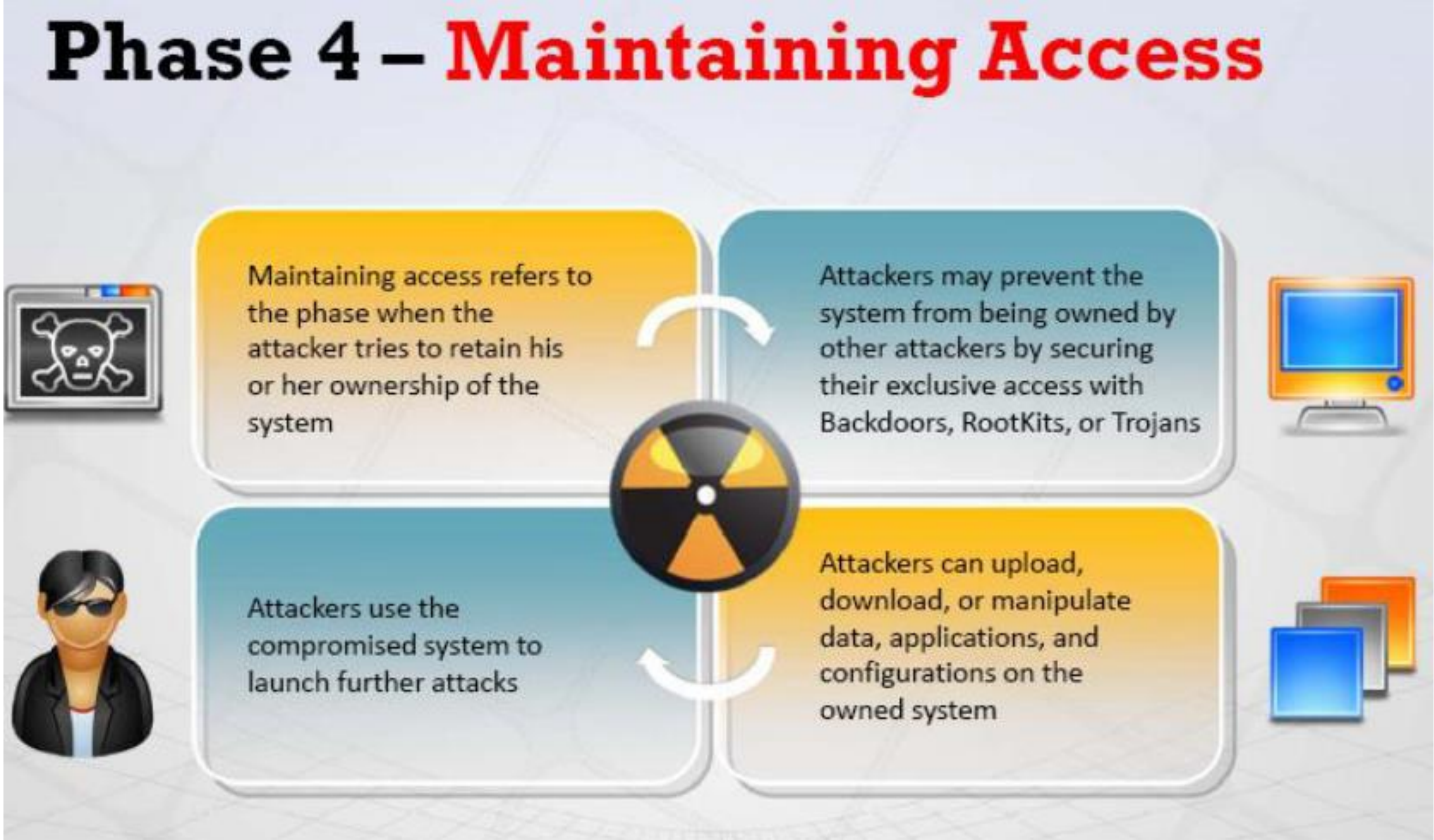
Gaining access refers to the point where the attacker obtains access to the operating system or applications on the computer or network

The attacker can escalate privileges to obtain complete control of the system. In the process, intermediate systems that are connected to it are also compromised

The attacker can gain access at the operating system level, application level, or network level

Examples include password cracking, buffer overflows, denial of service, session hijacking, etc.

0110I
01010



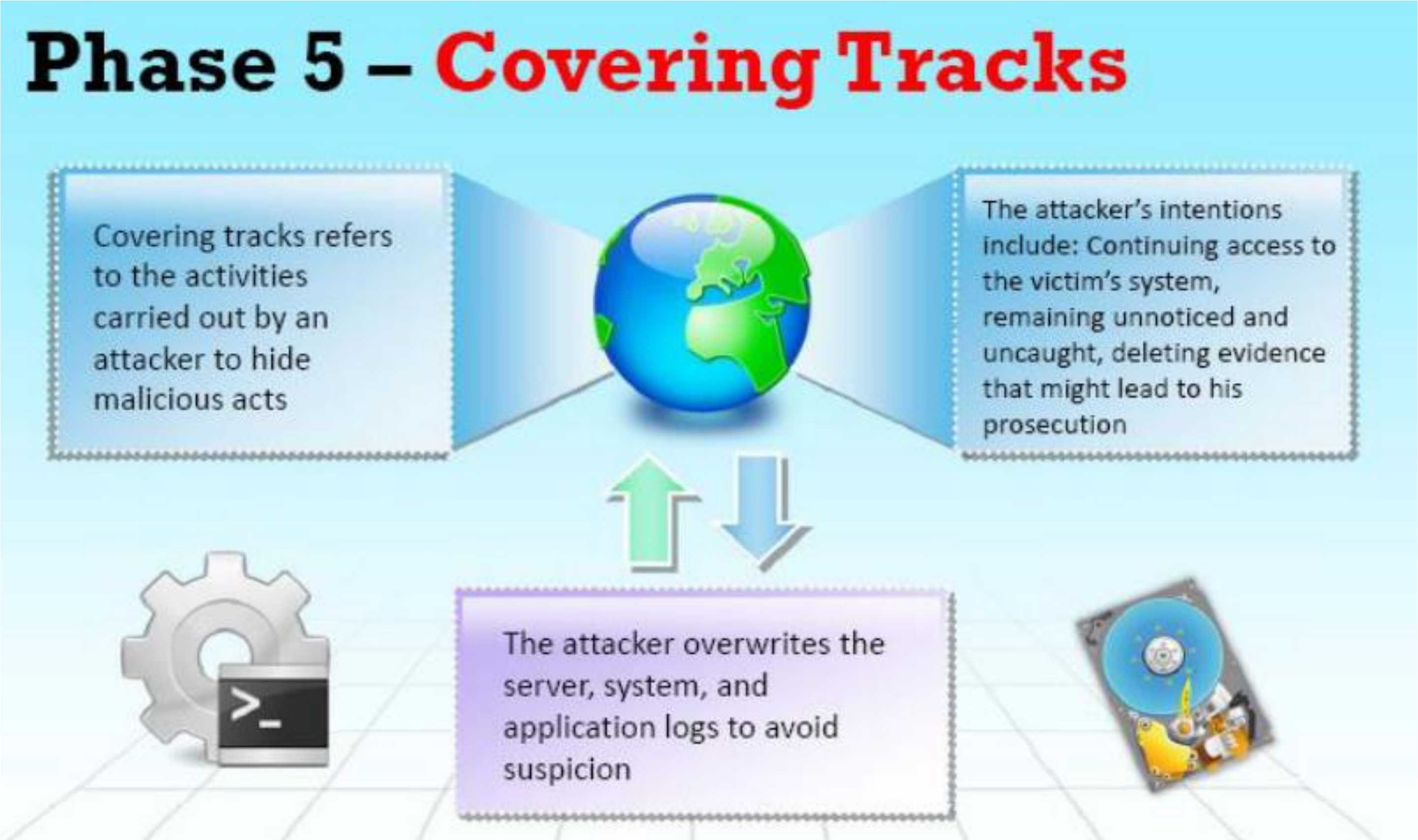
Phase 4 – Maintaining Access

Maintaining access refers to the phase when the attacker tries to retain his or her ownership of the system

Attackers may prevent the system from being owned by other attackers by securing their exclusive access with Backdoors, RootKits, or Trojans

Attackers use the compromised system to launch further attacks

Attackers can upload, download, or manipulate data, applications, and configurations on the owned system



Phase 5 – Covering Tracks

Covering tracks refers to the activities carried out by an attacker to hide malicious acts

The attacker's intentions include: Continuing access to the victim's system, remaining unnoticed and uncaught, deleting evidence that might lead to his prosecution

The attacker overwrites the server, system, and application logs to avoid suspicion

5.) What is foot printing. & explain following terminology

a. Open source or passive information gathering

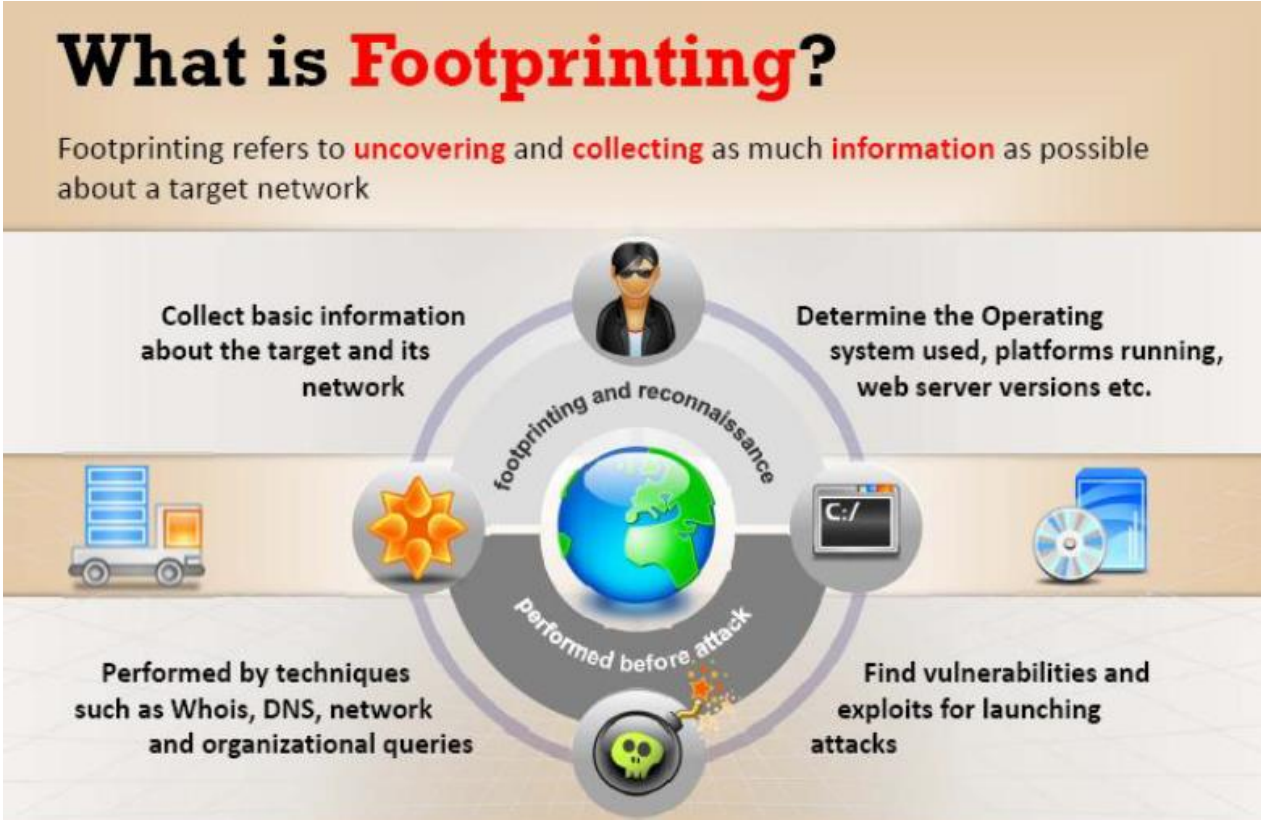
b. Anonymous foot printing

C. Org foot printing

D. Active info gathering

E. Pseudonimous foot printing

F. Internet foot printing



What is Footprinting?

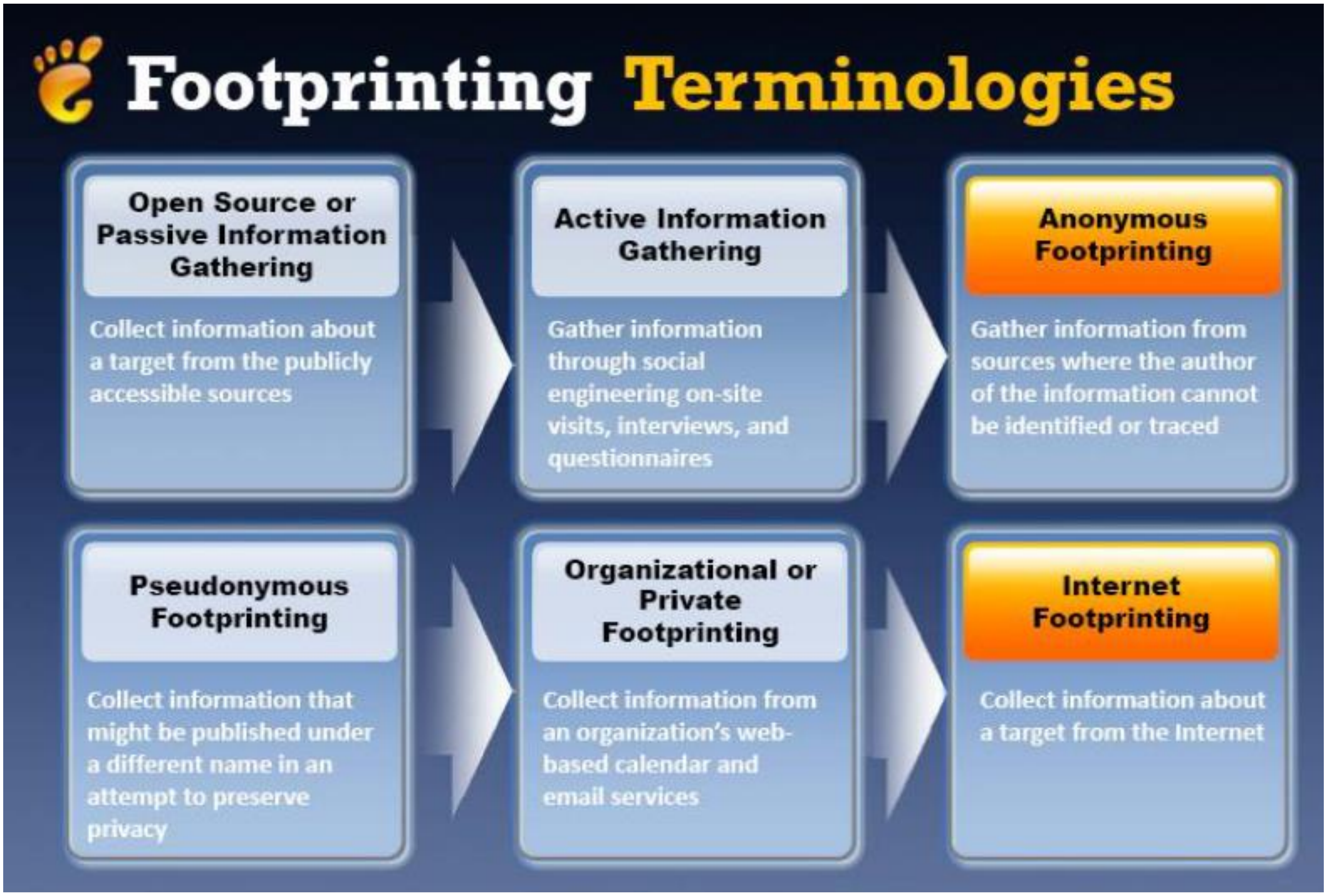
Footprinting refers to **uncovering** and **collecting** as much **information** as possible about a target network

Collect basic information about the target and its network

Determine the Operating system used, platforms running, web server versions etc.

Performed by techniques such as Whois, DNS, network and organizational queries

Find vulnerabilities and exploits for launching attacks



Footprinting Terminologies

Open Source or Passive Information Gathering

Collect information about a target from the publicly accessible sources

Active Information Gathering

Gather information through social engineering on-site visits, interviews, and questionnaires

Anonymous Footprinting

Gather information from sources where the author of the information cannot be identified or traced

Pseudonymous Footprinting

Collect information that might be published under a different name in an attempt to preserve privacy

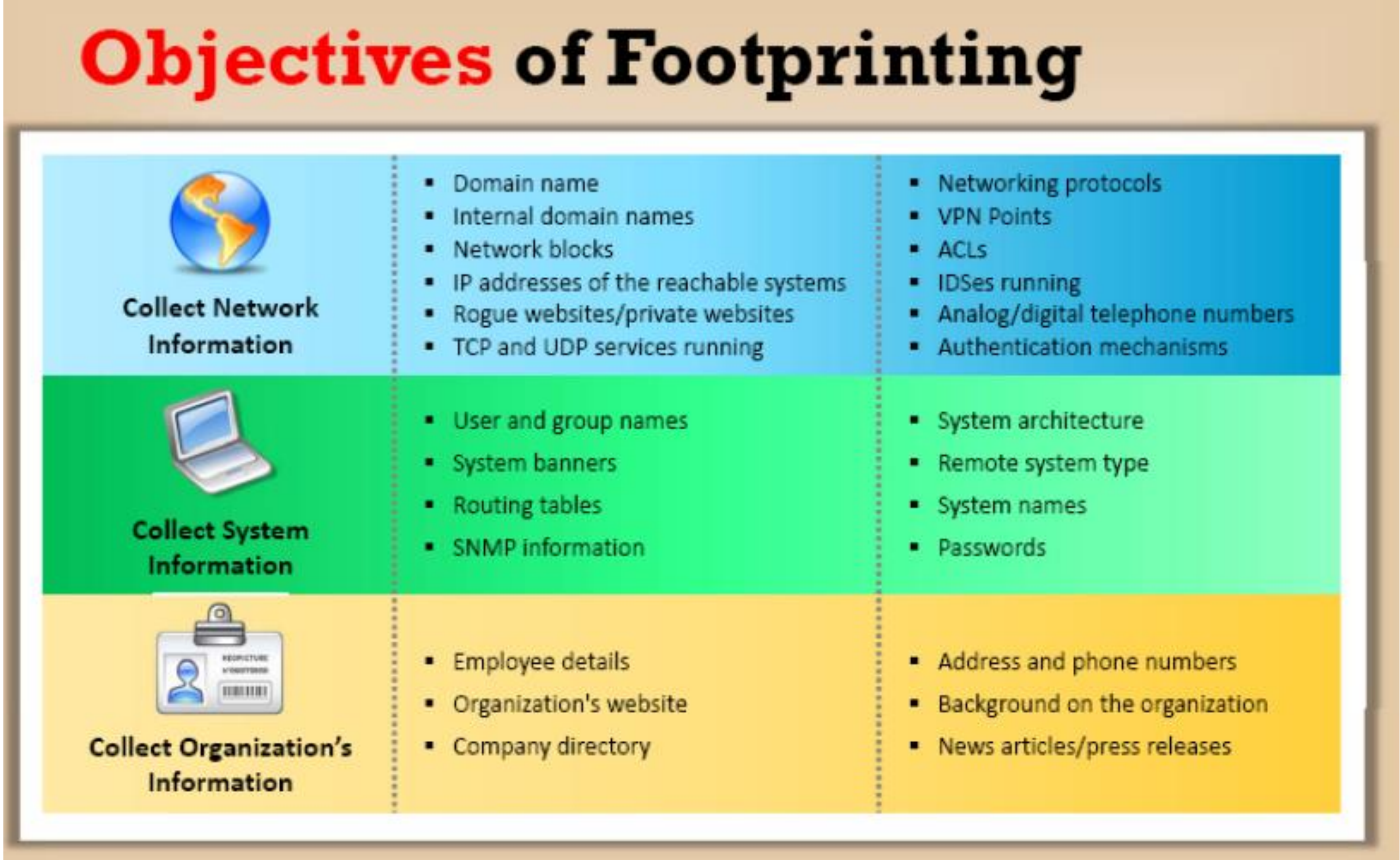
Organizational or Private Footprinting

Collect information from an organization's web-based calendar and email services

Internet Footprinting

Collect information about a target from the Internet

6.) Why do attacker need footprinting. What are the objective behind it.



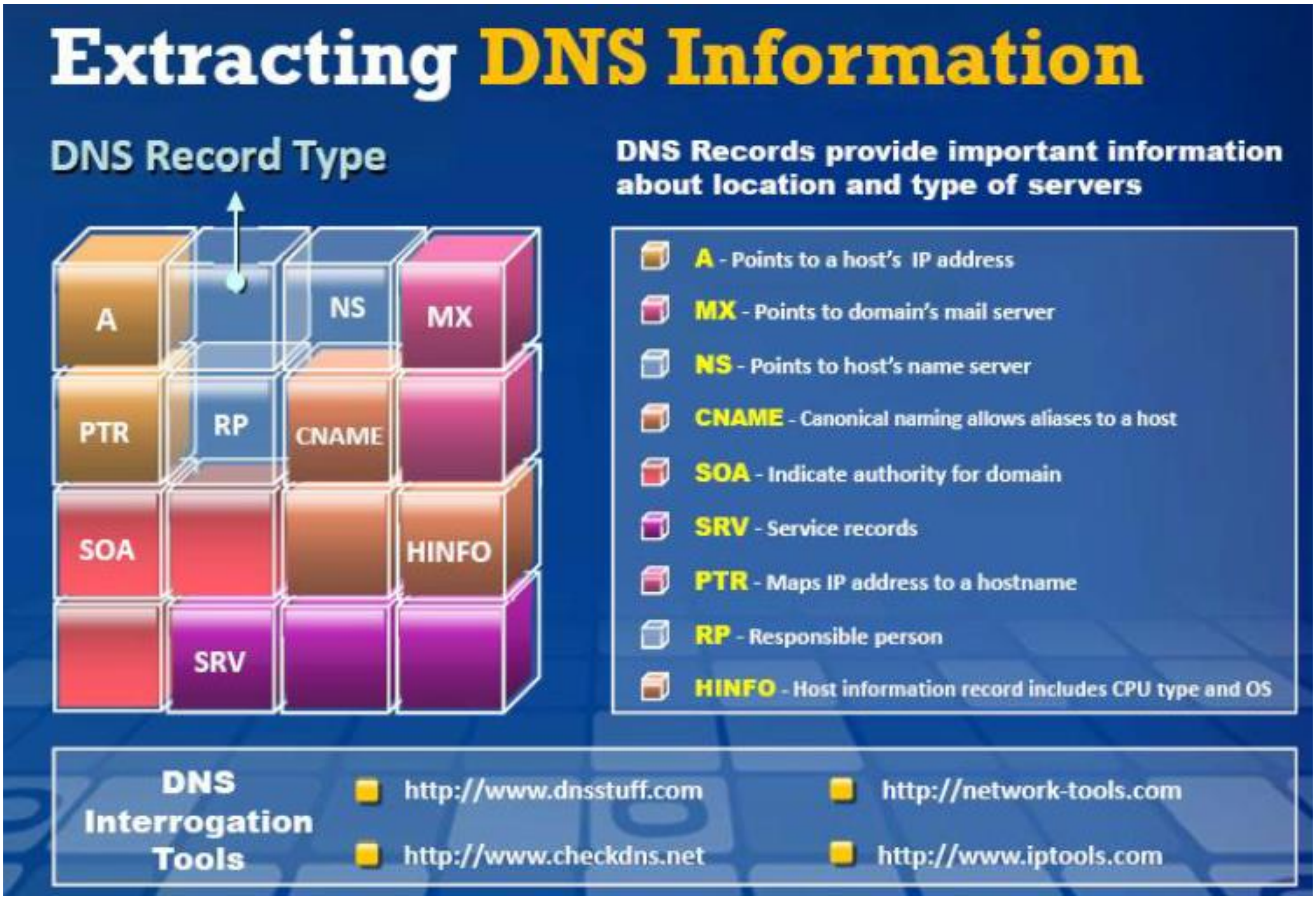
Objectives of Footprinting

Collect Network Information	▪ Domain name ▪ Internal domain names ▪ Network blocks ▪ IP addresses of the reachable systems ▪ Rogue websites/private websites ▪ TCP and UDP services running	▪ Networking protocols ▪ VPN Points ▪ ACLs ▪ IDSes running ▪ Analog/digital telephone numbers ▪ Authentication mechanisms
Collect System Information	▪ User and group names ▪ System banners ▪ Routing tables ▪ SNMP information	▪ System architecture ▪ Remote system type ▪ System names ▪ Passwords
Collect Organization's Information	▪ Employee details ▪ Organization's website ▪ Company directory	▪ Address and phone numbers ▪ Background on the organization ▪ News articles/press releases

7.) Explain website foot printing

PPT

8.) Explain DNS foot printing



Extracting DNS Information

DNS Record Type

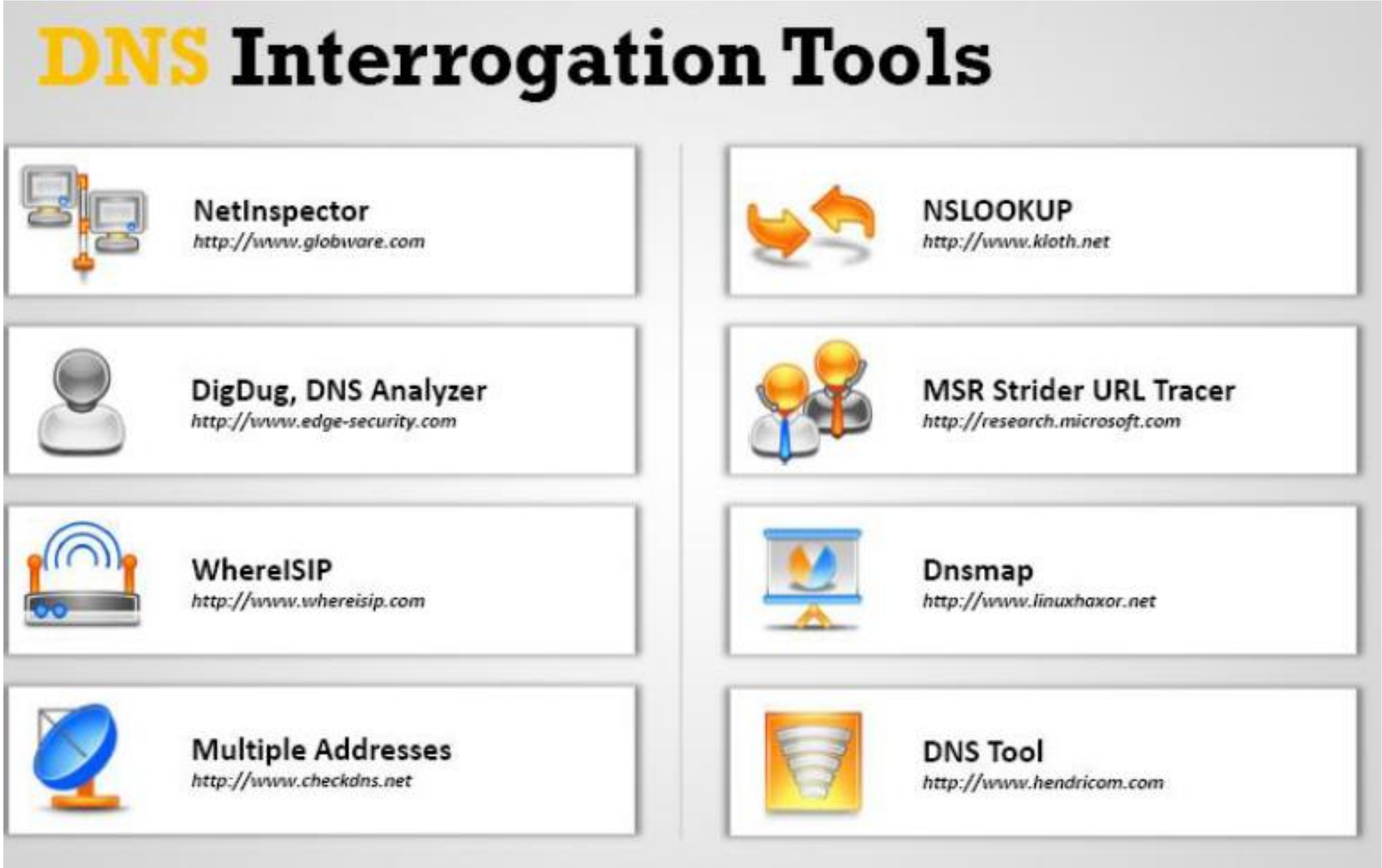
A
NS
MX
PTR
RP
CNAME
SOA
HINFO
SRV

DNS Records provide important information about location and type of servers

- **A** - Points to a host's IP address
- **MX** - Points to domain's mail server
- **NS** - Points to host's name server
- **CNAME** - Canonical naming allows aliases to a host
- **SOA** - Indicate authority for domain
- **SRV** - Service records
- **PTR** - Maps IP address to a hostname
- **RP** - Responsible person
- **HINFO** - Host information record includes CPU type and OS

DNS Interrogation Tools

- http://www.dnsstuff.com
- http://www.checkdns.net
- http://network-tools.com
- http://www.iptools.com



DNS Interrogation Tools

NetInspector
http://www.globware.com

DigDug, DNS Analyzer
http://www.edge-security.com

WhereISIP
http://www.whereisip.com

Multiple Addresses
http://www.checkdns.net

NSLOOKUP
http://www.kloth.net

MSR Strider URL Tracer
http://research.microsoft.com

Dnsmap
http://www.linuxhaxor.net

DNS Tool
http://www.hendricom.com

9.) How is foot printing done through social engineering?

Footprinting through Social Engineering:

Social media like twitter, facebook are searched to collect information like personal details, user credentials, other sensitive information using various social engineering techniques. Some of the techniques include

Eavesdropping: It is the process of intercepting unauthorized communication to gather information

Shoulder surfing: Secretly observing the target to gather sensitive information like passwords, personal identification information, account information etc

Dumpster Diving: This is a process of collecting sensitive information by looking into the trash bin. Many of the documents are not shredded before disposing them into the trash bin . Retrieving these documents from trash bin may reveal sensitive information regarding contact information, financial information, tender information etc.

10.) explain any 5 foot printing tools.

Refer PPT

11.) What is virus and what are its characteristics. Stages in life cycle of virus

A virus is a self-replicating program that produces its own copy by attaching itself to another program, computer boot sector or document.

It infects other programs,

Alters Data

Transforms itself

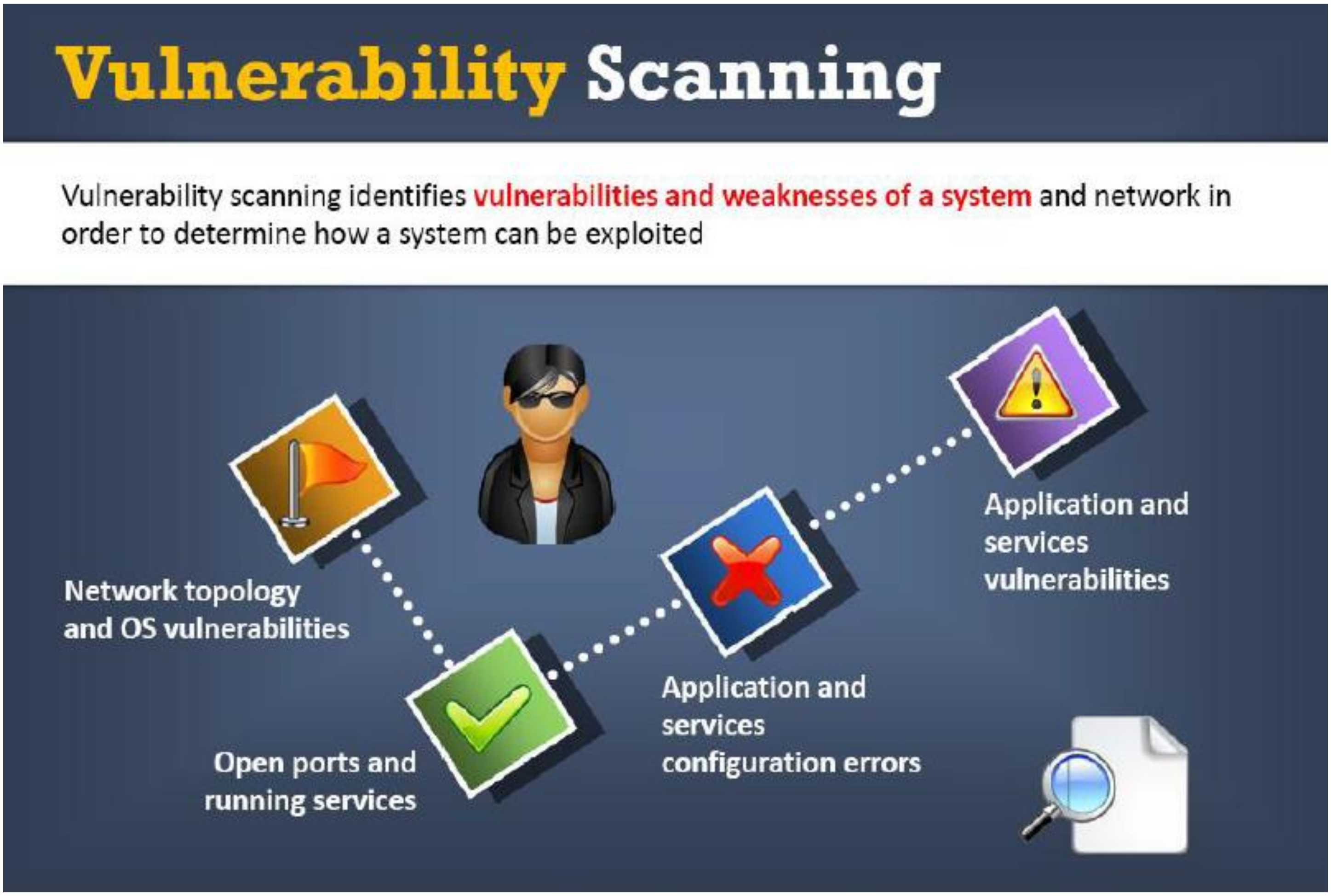
Encrypts Itself

Corrupt files and Programs

Self Propagates

https://www.educative.io/answers/what-is-the-structure-and-life-cycle-of-a-computer-virus

12.) what is vulnerability scanning



Vulnerability Scanning

Vulnerability scanning identifies vulnerabilities and weaknesses of a system and network in order to determine how a system can be exploited

Network topology and OS vulnerabilities
Open ports and running services
Application and services configuration errors
Application and services vulnerabilities