**---------------------------------------------------**

**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.

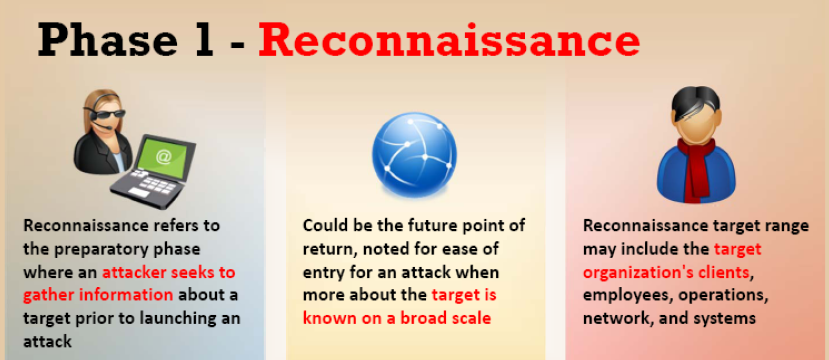
---------------------------------------------------------------------------------

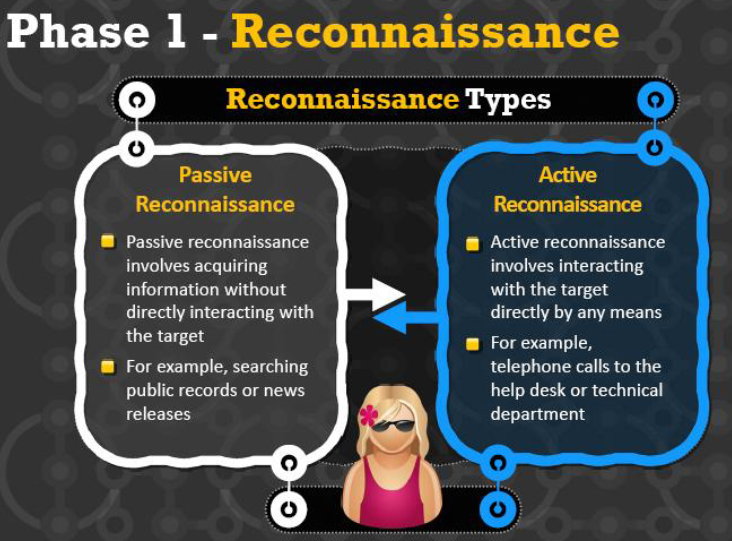
3.) What is hactivism? Explain it.



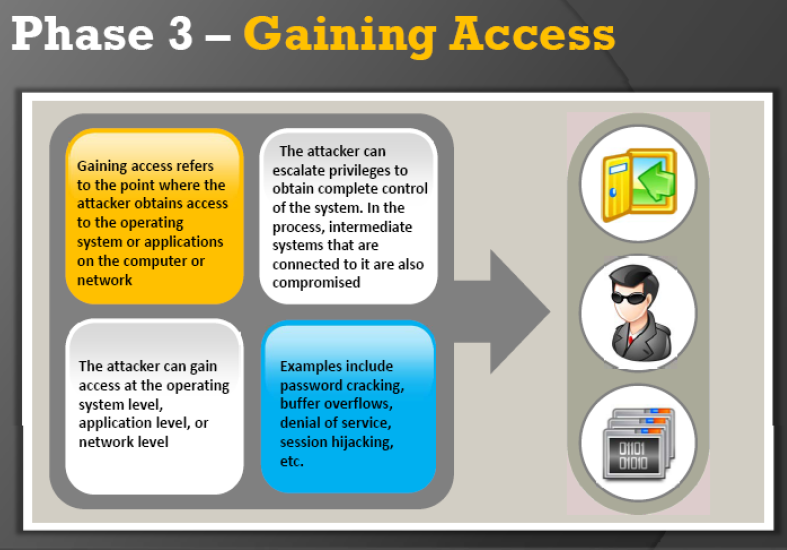
4.) Enumerate different phases of Hacking. Explain each in detail

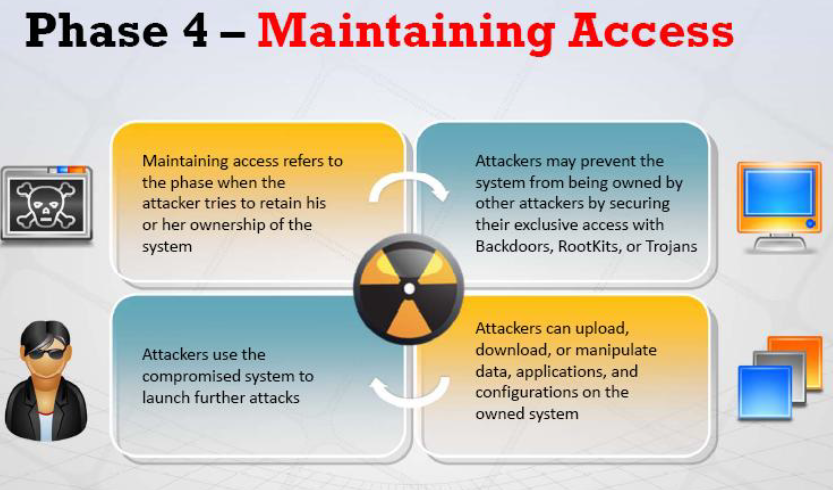














5.) What is foot printing. & explain following terminology

a. Open source or passive information gathering

b. Anonymous foot printing

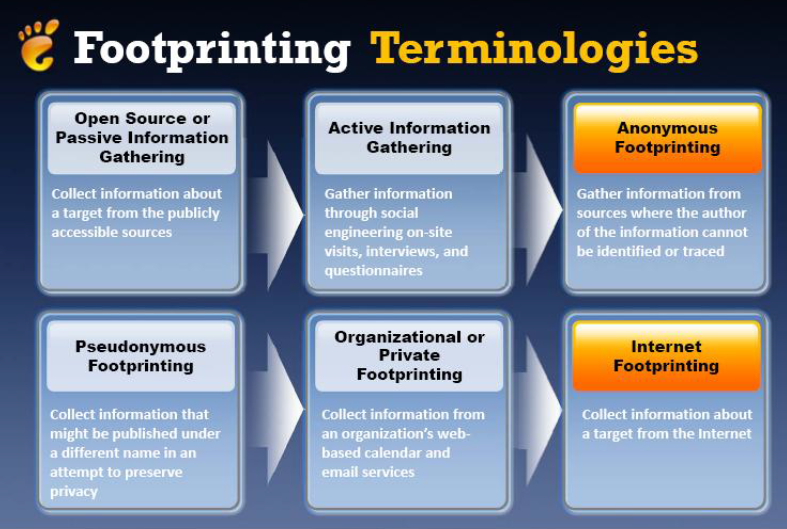
C. Org foot printing

D. Active info gathering

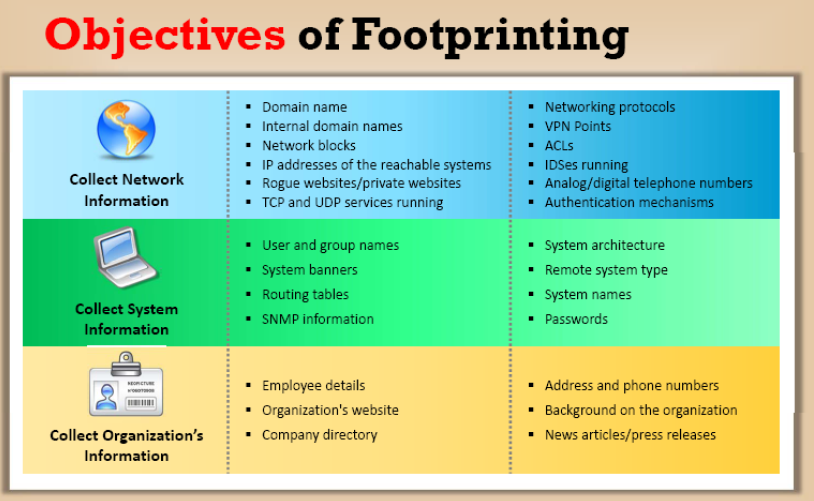
E. Pseudonimous foot printing

F. Internet foot printing





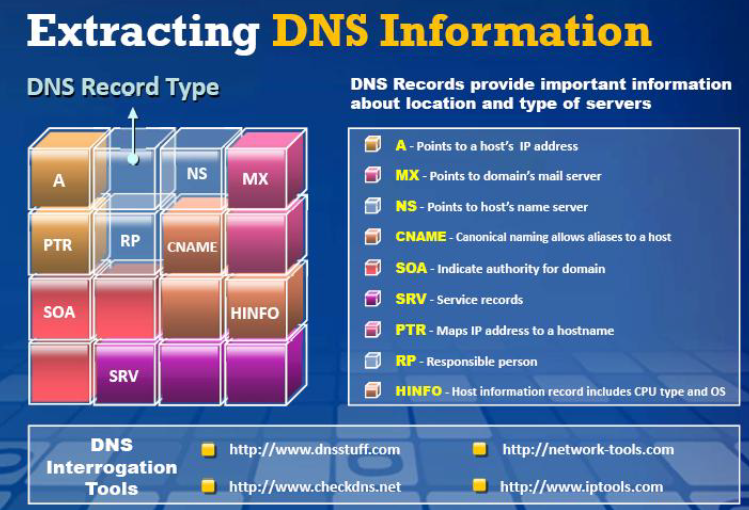
6.) Why do attacker need footprinting. What are the objective behind it.

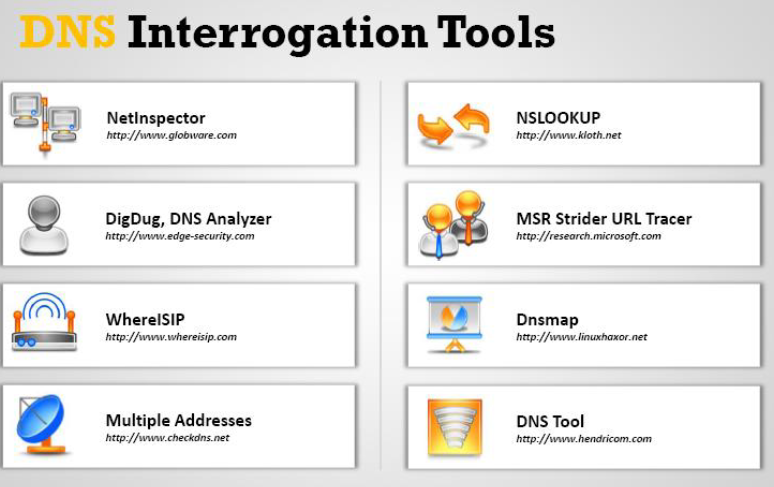


7.) Explain website foot printing

PPT

8.) Explain DNS foot printing





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

