Footprints and Social Engineering

Define foot print

Footprinting means gathering information about a target system that can be used to execute a successful cyber attack. To get this information, a hacker might use various methods with variant tools. This information is the first road for the hacker to crack a system. There are two types of footprinting as following below.

- **Active Footprinting:** Active footprinting means performing footprinting by getting in direct touch with the target machine.
- **Passive Footprinting:** Passive footprinting means collecting information about a system located at a remote distance from the attacker.

Advantages:

- Footprinting allows Hackers to gather the basic security configurations of a target machine along with network route and data flow.
- Once the attacker finds the vulnerabilities he/she focuses on a specific area of the target machine.
- It allows the hacker to identify as to which attack is handier to hack the target system.

Define DNS

The domain name system (DNS) is a naming database in which internet domain names are located and translated into Internet Protocol (IP) addresses. The domain name system maps the name people use to locate a website to the IP address that a computer uses to locate that website.For example, if someone types "example.com" into a web browser, a server behind the scenes maps that name to the corresponding IP address.

What is Web Bugs

Also called a "Web beacon," "pixel tag," "clear GIF" and "invisible GIF," it is a method for passing information from the user's computer to a third party website. Used in conjunction with cookies, Web bugs enable information to be gathered and tracked in the stateless environment of the Internet. The Web bug is typically a one-pixel, transparent GIF image, although it can be a visible image as well. As the HTML code for the Web bug points to a site to retrieve the image, it can pass along information at the same time.Web bugs can be placed into an HTML page used for email messages as most mail programs support the display of HTML pages.

Explain what is Ethical Hacking?

Ethical Hacking is when a person is allowed to hacks the system with the permission of the product owner to find weakness in a system and later fix them.

What is a penetration test?

- Penetration testing is also known as pen testing or ethical hacking. It describes the intentional launching of simulated cyber attacks that seek out exploitable vulnerabilities in computer systems, networks, websites, and applications

Define Social engineering

Social engineering is the art of convincing people to reveal confidential information. By taking advantage of, basic human nature like trust or a lack of knowledge, the attacker deceives people to reveal sensitive information.

The social engineering attacks can be grouped into three types:

- Human-based
- Mobile-based
- Computer-based

Define zone transfer

Zone Transfer (in a DNS Server) is the process of transferring information in the zone file on a primary name server to a secondary name server. It is one of several mechanisms available for administrators to replicate DNS databases across a set of DNS servers.

Define Port scanning

Ports are points at which information comes and goes from a computer, so by scanning for open ports, attackers can find weakened pathways with which to enter your computer.Port scanning is one of the most popular techniques attackers use to discover services they can exploit to break into your computer system, according to the SANS Institute.It's important to note that port scanning is not solely used for nefarious purposes. It also has legitimate uses in managing networks.

Tcpdump

tcpdump is a most powerful and widely used command-line packets sniffer or package analyzer tool which is used to capture or filter TCP/IP packets that are received or transferred over a network on a specific interface

What are the types of ethical hackers?

The types of ethical hackers are

- Grey Box hackers or Cyber warrior
- Black Box penetration Testers
- White Box penetration Testers
- Certified Ethical hacker

Explain what is DOS (Denial of service) attack? What are the common forms of DOS attack?
Denial of Service, is a malicious attack on network that is done by flooding the network with useless traffic. Although, DOS does not cause any theft of information or security breach, it can cost the website owner a great deal of money and time.

- Buffer Overflow Attacks
- SYN Attack
- Teardrop Attack
- Smurf Attack
- Viruses

Explain what is Network Sniffing?

A network sniffer monitors data flowing over computer network links. By allowing you to capture and view the packet level data on your network, sniffer tool can help you to locate network problems. Sniffers can be used for both stealing information off a network and also for legitimate network management.

Types of Sniffing Sniffing can be primarily divided into two main categories:

1. Active sniffing 2. Passive sniffing

Active Sniffing Active sniffing is where we directly interact with our target machine, by sending packets and requests. ARP spoofing and MAC flooding are common examples.

Passive Sniffing In passive sniffing, the attacker does not interact with the target. They just sit on the network and capture the packets sent and received by the network. This happens in the case of hub-based networks or wireless networks

What can an ethical hacker do?

An ethical hacker is a computer system and networking master who systematically endeavours to infiltrate a PC framework or network for the benefit of its owners to find security vulnerabilities that a malicious hacker could potentially exploit.

What are the advantages and disadvantages of hacking?

Advantages	Disadvantages
It can be used to foil security attacks	It creates massive security issues
To plug the bugs and loopholes	Get unauthorized system access
It helps to prevent data theft	Stealing private information
Hacking prevents malicious attacks	Violating privacy regulations

Distinguish between phishing and spoofing?

Phishing and spoofing are totally different beneath the surface. One downloads malware to your PC or network, and the other part tricks you into surrendering sensitive monetary data to a cyber-crook. Phishing is a technique for recovery, while spoofing is a method for delivery.

What are the tools used for ethical hacking?

There are several moral hacking tools out there within the marketing for different purposes, they are:

- **NMAP** – NMAP stands for Network plotter. It's an associate degree open-source tool that's used widely for network discovery and security auditing.
- **Metasploit** – Metasploit is one of the most powerful exploit tools to conduct basic penetration tests.
- **Burp Suit** – Burp Suite could be a widespread platform that's widely used for playing security testing of internet applications.
- **Angry IP Scanner** – Angry information processing scanner could be a lightweight, cross-platform information processing address and port scanner.
- **Cain & Abel** – Cain & Abel is a password recovery tool for Microsoft operational Systems.
- **Ettercap** – Ettercap stands for local area network Capture. It is used for a Man-in-the-Middle attack using a network security tool.

What is MAC Flooding?

MAC Flooding is a kind of a technique wherever the protection of given network switch is compromised. In MAC flooding the hacker floods the switch with sizable amounts of frames, than what a switch can handle. This makes switch behaving as a hub and transmits all packetsto all the ports existing. Taking the advantage of this the attacker can attempt to send his packet within the network to steal the sensitive information.

Differentiate Between a MAC and an IP Address?

All networks across devices are assigned a number which is unique, which is termed as MAC or Machine Access Control address. This address may be a personal mail box on the net. The network router identifies it. the amount may be modified anytime.All devices get their distinctive information processing address so they can be located easily on a given laptop and network. Whoever is aware of your distinctive information processing address will contact you through it.