**Chapter-14(Network Threats and Mitigation)**

**1. What types of threats can adversely affect your network?**

**Ans:** The types of threats:

**Denial of Service:** Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users.

Or

Denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

DoS attacks come in a variety of flvors,such as:

**The ping of death:** A ping of death is a type of attack on a computer system that involves sending a malformed or otherwise malicious ping to a computer.

**Smurf:** A smurf attack is a type of denial of service attack in which a system is flooded with spoofed ping messages.

**SYN Flood:** A SYN flod is also a DoS attack that inundates the receiving machine with lots of packets that cause the victim to waste resources by holding connections open.

**Viruses:** A computer virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.

There are several different kinds of viruses, but the most popular ones are:

**File Viruses:** File Viruses is a type of computer virus that inserts its malicious code into executable files on a system. When the infected file is opened or used the virus may overwrite the file and cause permanent damage to the content of the overwritten file.

**Macro Viruses:** A macro virus is a computer virus that "infects" a Microsoft Word or similar application and causes a sequence of actions to be performed automatically when the application is started or something else triggers it.

**Boot-Sector Viruses:** Boot-sector viruses infect computer systems by copying code either to the boot sector on a floppy disk or the partition table on a hard disk.

**Worms:** A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself.

**Buffer Overflow:** A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold.

**Wireless Threats:** Wireless threats are:

War Driving, War Chalking, WEP Cracking, WPA Cracking, Evil Twin

**Rogue Access Points:** A Rogue Access Point (Rogue AP) is a wireless access point installed on a wired enterprise network without authorization from the network administrator.

**2. Write about Attackers and Their Tools?**

**Ans:**

**IP Spoofing:** IP spoofing refers to connection hijacking through a fake Internet Protocol (IP) address.

**Backdoors:** Backdoors are simply paths leading into a computer or network.

**Packet Sniffers:** Packet Sniffers is a sniffer program that targets packets of data transmitted over the Internet.

Other tools are: Application-Layer Attacks, ActiveX Attacks, Autorooters, Network Reconnaissance, Port Scanners, FTP Bounce, Password Attacks, Brute-Force Attacks etc.

**3. What is Social Engineering (Phishing)?**

**Ans:** Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization.

**4. What are the steps to detect intruder and defend?**

**Ans:**

* Active detection, which involves constantly scanning the network for possible break-ins
* Passive detection, which involves logging all network events to a file
* Proactive defense methods, which involve using tools to shore up your network walls against attack

**5. Write the names of policies and procedures?**

**Ans:**

**Policies:**

**Security Policies:** it should precisely defie how security is to be implemented within an organization and include physical security, document security, and network security.

**Security Audit:** A security audit is a thorough examination of your network that includes testing all its components to make sure everything is secure.

**Clean-Desk Policy:** It means requiring that all potentially important documents like books, schematics, confidential letters, notes to self, and so on aren’t left out in the open when someone’s away from their desk.

**Recording Equipment:** Recording equipment—such as tape recorders, cell phones, and small memory devices like USB flash memory keychains—can contain sensitive, confidential information, so a good security policy should prohibit their unauthorized presence and use.

**Security procedures:**

A security procedure defies how to respond to any security event that happens on your network. Here’s a short list of items you might include:

* What to do when someone has locked themselves out of their account
* How to properly install or remove software on servers
* What to do if files on the servers suddenly appear to be “missing” or altered
* How to respond when a network computer has a virus
* Actions to take if it appears that a hacker has broken into the network
* Actions to take if there is a physical emergency such as a fire or flood

**Security procedures:** Security Training, End-User Training, Administrator Training, Patches and Upgrades, Automatic Updates through Windows Update, Downloading Patches and Hotfixes, Updating Antivirus Components, Scanning for Viruses.

**6. What types of threats can adversely affect your network?**

Ans: Threats include denial of service attacks, viruses, worms, rogue access points, phishing, and various other attack methods employed by hackers.

**7. How attackers attempt to get information about your network.**

Ans: Attackers have various methods they can use to gather information. Some of the most common reconnaissance tools are packet sniffers and social engineering.

**8. How to keep your systems automatically updated.**

Ans: Programs such as Windows Update can keep your operating systems current, which will reduce opportunities for attackers to exploit your computers and network.

**9. Where to go to find downloadable software updates.**

Ans: Check the manufacturer’s website for the most current security information, patches, and updates.