Introduction to Network Security Basics

Network threats.

1. Malware

Cybercriminals use many different types of malicious software, or malware, to carry out their activities. Malware is any code that can be used to steal data, bypass access controls, or cause harm to or compromise a system. Knowing what the different types are and how they spread is key to containing and removing them.
Some most common malware are:

1. **Virus**
   A virus is a type of malicious software that replicates and attaches itself to executable files, often requiring user interaction to activate. Viruses can range from harmless (e.g., displaying images) to destructive (e.g., deleting data). Some are designed to mutate, avoiding detection. They are typically spread via USB drives, optical disks, network shares, or email.

   Example: The ILOVEYOU virus, which spread in 2000, affected many systems in India. Disguised as a love letter in an email attachment, it infected computers, overwrote files, and spread itself to contacts. The virus caused significant disruptions, especially in government and private sectors, leading to data loss and system failures across the country.

2. **Worms**
   A worm is a type of malware that replicates itself to spread between computers without needing a host program. Unlike viruses, worms don't require user interaction and can propagate quickly across networks. They exploit system vulnerabilities and carry malicious payloads to damage systems. For example, the Code Red worm in 2001 infected over 300,000 servers in just 19 hours.

3. **Trojans**

This malware carries out malicious operations by masking its true intent. It might appear legitimate but is, in fact, very dangerous. Trojans exploit your user privileges and are most often found in image files, audio files or games.

Unlike viruses, Trojans do not self-replicate but act as a decoy to sneak malicious software past unsuspecting users. Remote Access Trojans(RATs) are most common trojans and very harmful for the system.

Example: In India, the "Anubis" Trojan targeted mobile banking users in 2017. Disguised as a legitimate app, it stole banking credentials and sensitive information, spreading through third-party app stores and phishing sites, leading to financial theft.

4. **Spyware**

   Designed to track and spy on you, spyware monitors your online activity and can log every key you press on your keyboard, as well as capture almost any of your data, including sensitive personal information such as your online banking details. Spyware does this by modifying the security settings on your devices.

   It often bundles itself with legitimate software or Trojan horses.

5. **Adware**

   Adware is often installed with some versions of software and is designed to automatically deliver advertisements to a user, most often on a web browser. You know it when you see it! It’s hard to ignore when you’re faced with constant pop-up ads on your screen.

   It is common for adware to come with spyware.

6. **Backdoor**
   This type of malware is used to gain unauthorized access by bypassing the normal authentication procedures to access a system. As a result, hackers can gain remote access to resources within an application and issue remote system commands.A backdoor works in the background and is difficult to detect.

7. **Ransomware**

   This malware is designed to hold a computer system or the data it contains captive until a payment is made. Ransomware usually works by encrypting your data so that you can’t access it.

   Some versions of ransomware can take advantage of specific system vulnerabilities to lock it down. Ransomware is often spread through phishing emails that encourage you to download a malicious attachment or through a software vulnerability.

8. **Scareware**

   This is a type of malware that uses 'scare’ tactics to trick you into taking a specific action. Scareware mainly consists of operating system style windows that pop up to warn you that your system is at risk and needs to run a specific program for it to return to normal operation.

   If you agree to execute the specific program, your system will become infected with malware.

9. **Rootkit**

   This malware is designed to modify the operating system to create a backdoor, which attackers can then use to access your computer remotely. Most rootkits take advantage of software vulnerabilities to gain access to resources that normally shouldn’t be accessible (privilege escalation) and modify system files.

   Rootkits can also modify system forensics and monitoring tools, making them very hard to detect. In most cases, a computer infected by a rootkit has to be wiped and any required software reinstalled.

2. Phishing Attacks:

Phishing got its name from “Phish” meaning fish. It’s a common phenomenon to put bait for the fish to get trapped. Similarly, Phishing works. It is an unethical way to make the user or victim click on harmful sites. The attacker makes the harmful site or emails in such a way that the victim feels it to be authentic, thus falling prey to it. The most common phishing attack method is sending emails that appear genuine and thus taking away all credentials from the victim like login credentials, credit card information, personal information, and so on.

How is a phishing attack carried out?

1. Clicking on an unknown file or attachment.
2. Using an open or free wifi hotspot.
3. Responding to social media requests.
4. Clicking on unauthenticated links or ads.

Types of Phishing Attacks.

1. Email Phishing:

A cyberattack is where the attacker sends fraudulent emails that appear to be from a trusted source, aiming to deceive the victim into disclosing sensitive information, such as passwords or credit card details.

2. Spear Phishing:
A targeted phishing attack is where cybercriminals impersonate a trusted individual or organization to steal sensitive information, often using personalized tactics.

3. Whaling:
A form of spear phishing targeting high-profile individuals, such as

executives or government officials, to gain access to sensitive or financial data.

4. Vishing:
Voice phishing, where attackers use phone calls to trick victims into revealing personal information, often by impersonating legitimate organizations.

5. Smishing:

SMS phishing, where attackers send fraudulent text messages to lure victims into revealing sensitive data, such as login credentials or financial information.

6. Clone Phishing:
A type of phishing attack where a legitimate email is replicated with a malicious link or attachment, and sent to the victim to trick them into clicking it.

3. Distributed Denial of Service (DDoS) Attacks

Attackers flood a network or website with excessive traffic, causing service disruptions.

Example: Indian Government Websites Targeted (2024): Several government websites and banking institutions faced massive DDoS attacks, allegedly from state-sponsored actors.

4. Man-in-the-Middle (MITM) Attacks

Hackers intercept communication between two parties to steal sensitive data.

Example: Public Wi-Fi Interception in India: Cybercriminals set up fake Wi-Fi networks in airports and cafes, intercepting user credentials when they log in to banking websites.

5.SQL Injection & Web Attacks

Attackers manipulate website databases to extract sensitive data.

Example: Data Leak from Indian Banks (2024): Hackers exploited SQL injection vulnerabilities in several Indian financial service providers, leading to leaks of customer financial data on the dark web.

6. Deepfake & AI-Based Cyber Threats

Attackers use AI-generated videos, voices, or images to manipulate victims.

Example: AI-Based Fraud Call (2024):
A businessman in Delhi was scammed after receiving a deepfake video call that appeared to be from his CEO, instructing him to transfer ₹50 lakh.

7. Social Engineering

Social engineering involves manipulating individuals into divulging confidential information by exploiting human psychology rather than technical vulnerabilities.

Example: An attacker might impersonate a trusted colleague to gain access to sensitive information.

8. Zero-Day Exploits

Zero-day exploits target undiscovered vulnerabilities in software or hardware, allowing attackers to exploit them before developers can address the issue.

Example: The **Stuxnet worm** exploited multiple zero-day vulnerabilities to sabotage Iran's nuclear program.

9. Insider Threats

Insider threats originate from individuals within an organization who misuse their access to harm the organization's systems, data, or operations.

Example: An employee might intentionally leak confidential company information to a competitor.

10. Supply Chain Attacks

Supply chain attacks target vulnerabilities in an organization's supply chain, compromising products or services before they reach the end user.

Example: The **SolarWinds attack** in 2020 involved hackers compromising the company's software updates to infiltrate multiple U.S. government agencies.

11. Credential Stuffing

Credential stuffing involves using stolen username and password combinations to gain unauthorized access to user accounts, often by automating login attempts.

Example: If a user reuses passwords across multiple sites, an attacker can use credentials from a breached site to access accounts on other platforms.

12. Clickjacking

Clickjacking tricks users into clicking on something different from what they perceive, potentially revealing confidential information or allowing unauthorized actions.

Example: An attacker might overlay a transparent button over a legitimate webpage element, causing users to click on the hidden button unknowingly.

13. DNS Spoofing

DNS spoofing involves corrupting the Domain Name System data to redirect users to malicious websites without their knowledge.

Example: An attacker might manipulate DNS records to redirect users from a legitimate website, such as a bank, to a malicious clone, stealing login credentials and personal information.

14. Brute Force Attacks

A **brute force attack** involves systematically trying all possible combinations of passwords or encryption keys until the correct one is found. This can be automated to try millions of combinations in a short amount of time.

Example: An attacker might use automated tools to crack a weak password for an online account, gaining unauthorized access.

15. Keyloggers

Keyloggers are malicious software or hardware that track and record the keystrokes made on a device. This data is then sent to the attacker, allowing them to capture sensitive information like passwords, credit card numbers, and personal messages.

Example: A **software-based keylogger** might be installed via a phishing email, silently monitoring the victim's typing activities.

16. Session Hijacking

Session hijacking is when an attacker takes control of a web session between a user and a web application, often after the user has authenticated. The attacker can then impersonate the user and carry out malicious activities.

Example: An attacker intercepts the session cookie of a logged-in user, gaining access to their online banking account without needing to log in themselves.

17. Fake Software Updates (Update Exploits)

Attackers often use fake software updates to trick users into downloading malicious software. These updates may seem legitimate but actually install malware or steal sensitive data.

Example: A user receives a **fake update prompt** for their browser or operating system, and by clicking on it, installs a **trojan** that gives the attacker control of their system.

These are some common network threats we see. There are many other cyber threats present in today's digital era.If you are interested in exploring about more threats you can research.