**ASSIGNMENT 1**

**Q1. What are the different kinds of security attacks possible?**

**A:** Cybersecurity attacks can take many forms, targeting various aspects of computer systems, networks, and data. Here are some of the different types of cyber attacks:

1. Malware Attacks:
   * Viruses: Programs that can replicate themselves and spread to other files and systems.
   * Worms: Self-replicating malware that can spread across networks.
   * Trojans: Malicious programs disguised as legitimate software.
   * Ransomware: Malware that encrypts data and demands a ransom for decryption.
   * Spyware: Software designed to gather information without the user's knowledge.
2. Phishing Attacks:
   * Phishing: Sending fraudulent emails or messages to trick users into revealing sensitive information.
   * Spear Phishing: Targeted phishing attacks that personalize the message based on the victim.
   * Whaling: Phishing attacks specifically targeting high-profile individuals or executives.
3. Denial of Service (DoS) Attacks:
   * DoS Attacks: Flooding a system or network with traffic to overwhelm and disrupt services.
   * Distributed DoS (DDoS) Attacks: Coordinated attacks using multiple compromised devices to amplify the impact.
4. Man-in-the-Middle (MitM) Attacks:
   * Intercepting and altering communication between two parties without their knowledge.
5. SQL Injection Attacks:
   * Exploiting vulnerabilities in database input to execute unauthorized SQL commands.
6. Cross-Site Scripting (XSS) Attacks:
   * Injecting malicious scripts into websites that are then executed by users' browsers.
7. Zero-Day Exploits:
   * Exploiting software vulnerabilities that are unknown to the vendor and have not been patched.
8. Drive-By Downloads:
   * Infecting a user's system by visiting a compromised website, often without the user's knowledge.
9. Password Attacks:
   * Brute Force: Trying all possible combinations to guess a password.
   * Dictionary Attack: Using a list of commonly used passwords to guess a password.
   * Credential Stuffing: Using stolen usernames and passwords from one site to gain unauthorized access to other sites.
10. Social Engineering Attacks:
    * Manipulating individuals into revealing confidential information or performing actions that compromise security.
11. IoT (Internet of Things) Attacks:
    * Exploiting vulnerabilities in connected devices to gain access to networks or data.
12. Cryptojacking:
    * Illegally using someone else's computer to mine cryptocurrency.
13. Eavesdropping/Sniffing:
    * Unauthorized interception of network traffic to gather sensitive information.
14. Malvertising:
    * Distributing malware through online advertising networks.
15. Insider Threats:
    * Malicious actions by individuals with authorized access to systems and data.
16. Watering Hole Attacks:
    * Compromising a website frequented by the target audience to infect visitors with malware.
17. Fileless Attacks:
    * Exploiting vulnerabilities in software and applications without writing files to the system's disk.

These are just some examples of the various cyber attacks that can occur. Cybersecurity professionals work to prevent, detect, and respond to these threats to safeguard systems, networks, and data.

Top of Form

**Q2. Difference between Worms , Trojans and Virus.**

**A:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Aspect** | **Worms** | **Trojans** | **Viruses** |
| **Propagation** | Self-replicating, spread automatically | Rely on user interaction for execution | Attach to executable files, spread through user actions |
| **Spread** | Over networks, exploiting vulnerabilities | Often delivered through social engineering | Attach to files, require user interaction to spread |
| **Purpose** | Rapid spread, causing congestion | Carry various payloads (backdoors, keyloggers, etc.) | Carry various payloads, may corrupt data or execute other actions |
| **Delivery** | Exploits network vulnerabilities | Emails, malicious links, compromised software | Attach to files, delivered through user actions |
| **Example** | Conficker, Code Red, Blaster | Zeus, Emotet, Remote Access Trojans (RATs) | Melissa, ILOVEYOU, Sasser |