PR Cyber Attacks Documentation

1. Types of cyber-attacks:
   1. Malware attacks:
      1. Viruses:
         1. File Infector Virus: This type of virus infects executable files such as .exe and .dll files. When a user runs an infected file, the virus activates and infects other files on the system.
         2. Boot Sector Virus: This virus infects the boot sector of a hard drive, making it difficult to detect and remove. The virus loads before the operating system and can infect other bootable devices.
         3. Macro Virus: This virus infects files created in applications such as Microsoft Word, Excel, and PowerPoint. The virus is embedded in the macro code and activates when the file is opened.
         4. Polymorphic Virus: This type of virus changes its code every time it replicates, making it difficult to detect with traditional antivirus software.
         5. Resident Virus: This virus stays in memory even after the infected file is closed, allowing it to infect other files as they are opened.
         6. Multipartite Virus: This virus infects both the boot sector and executable files, making it difficult to detect and remove.
         7. Direct Action Virus: This virus only infects executable files and activates when the infected file is executed.
         8. Worms: Worms are self-replicating viruses that spread over a network or the internet, causing damage to computer systems and networks.
      2. Trojans - A Trojan virus (also known as a Trojan horse) is a type of malware that appears to be a legitimate program or file, but contains malicious code that allows hackers to gain unauthorized access to a computer system or network, all types of viruses can be disguised as a trojan horse, but the main types of trojans are:
         1. Backdoor Trojans: allow hackers to control a system remotely;
         2. banking Trojans: steal login credentials and financial information
      3. Ransomware - type of malicious software that encrypts a victim's files or system and demands payment in exchange for restoring access to the data or removing the restriction.
      4. Spyware - type of malicious software that secretly collects a user's personal information or internet usage data and sends it to a third-party without the user's knowledge or consent.
   2. Phishing attacks: Phishing is a type of social engineering attack where attackers attempt to trick victims into giving up sensitive information such as login credentials, credit card details, or other personal information through email, text messages, or fake websites.
      1. Deceptive Phishing: The most common type of phishing attack, where attackers send fraudulent emails, text messages, or social media messages to trick victims into providing personal information, such as login credentials, credit card details, or social security numbers.
      2. Spear Phishing: A targeted phishing attack that is directed towards a specific individual or organization. Attackers use personal information gathered from social media or other sources to create a personalized message that appears to be from a trusted source.
      3. Whaling: A type of spear phishing attack that is directed at high-level executives or individuals in an organization, with the aim of stealing sensitive information or gaining access to confidential data.
      4. Clone Phishing: A type of attack where attackers create a replica of a legitimate email or website, with the aim of stealing login credentials or personal information from the victims.
      5. Smishing: A type of phishing attack that is conducted through text messages, where attackers send a message with a link to a fake website or a malicious app.
      6. Vishing: A type of phishing attack that is conducted over the phone, where attackers impersonate a legitimate entity and use social engineering tactics to trick victims into revealing sensitive information.
   3. Denial of Service (DoS) attacks: A DoS attack is an attempt to make a website or network unavailable to users by overwhelming it with traffic from multiple sources.
      1. TCP SYN Flood: This attack exploits the way that a TCP connection is established, by flooding a server with a high volume of SYN packets, which results in the server becoming unresponsive or crashing.
      2. UDP Flood: This attack involves flooding a server with a high volume of UDP packets, which can consume network resources and cause the server to become unavailable.
      3. Ping of Death: This attack involves sending an oversized ping packet to a server or network device, which causes the device to crash or become unresponsive.
      4. Smurf Attack: This attack involves sending a high volume of ICMP echo requests to a network's broadcast address, causing all devices on the network to respond and overload the network.
      5. Application Layer DoS: This attack targets the application layer of a network, by overwhelming the server with requests that are designed to consume resources or crash the application.
      6. Distributed DoS (DDoS): A DDoS attack involves using multiple compromised devices (often through botnets) to simultaneously target a single server or network, overwhelming it with traffic and making it unavailable, which is probably the most common one.
   4. Man-in-the-middle (MITM) attacks: MITM attacks occur when an attacker intercepts communication between two parties, allowing them to eavesdrop or modify the communication without either party knowing.
      1. IP Spoofing: This attack involves an attacker sending a packet to a network with a false source IP address, making it appear as if the packet originated from a trusted source. This can be used to intercept traffic or launch other types of attacks.
      2. ARP Spoofing: This attack involves an attacker sending falsified Address Resolution Protocol (ARP) messages to a network, causing traffic to be redirected to the attacker's device instead of its intended destination.
      3. DNS Spoofing: This attack involves an attacker intercepting Domain Name System (DNS) requests and redirecting them to a fake website or server, allowing the attacker to steal sensitive information or launch other attacks.
      4. HTTPS Spoofing: This attack involves an attacker intercepting HTTPS traffic and using a fake SSL certificate to make the victim's browser believe that the website or server is legitimate, allowing the attacker to steal sensitive information.
      5. Wi-Fi Eavesdropping: This attack involves an attacker intercepting Wi-Fi traffic by setting up a rogue access point or by eavesdropping on a public Wi-Fi network, allowing the attacker to intercept and steal sensitive information.
   5. SQL injection attacks: SQL injection is a technique used to exploit vulnerabilities in web applications that use databases. Attackers use malicious SQL statements to gain unauthorized access to the database, steal data, or modify it.
      1. In-band SQLi: This is the most common type of SQL injection attack, where an attacker uses the same communication channel (such as a web form or URL parameter) to send the malicious SQL query and receive the results.
      2. Blind SQLi: In this type of attack, the attacker does not receive any feedback from the application, but can still infer information from the database by sending SQL queries and analyzing the responses.
      3. Out-of-band SQLi: This type of attack involves using a separate channel (such as email or DNS) to send the malicious SQL query and receive the results, without relying on the application's feedback.
      4. Error-based SQLi: This attack exploits SQL errors that occur when a malicious query is executed, allowing the attacker to infer information about the database or the application.
      5. Union-based SQLi: This attack involves injecting a UNION operator into a legitimate SQL query, allowing the attacker to combine the results of two different queries and extract information from the database.
      6. Time-based SQLi: This attack involves exploiting a time delay in the application's response to infer information from the database, by injecting a query that causes a delay in the application's response time.
   6. Cross-site scripting (XSS) attacks: XSS attacks are another type of web application vulnerability. Attackers inject malicious code into a website to steal user data, gain control of user sessions, or redirect users to malicious websites.
      1. Reflected XSS: This type of attack involves injecting malicious code into a web page that is reflected back to the user, often through a search box or a URL parameter.
      2. Stored XSS: This attack involves injecting malicious code into a web page that is permanently stored on the server and served to all users who access the page.
      3. DOM-based XSS: This attack involves injecting malicious code into the Document Object Model (DOM) of a web page, often through client-side scripting, such as JavaScript.
      4. Blind XSS: This attack involves injecting malicious code into a web page that is stored on the server but not directly displayed to the user, such as in a database or log file.
      5. Multipart/form-data XSS: This attack involves injecting malicious code into a form that accepts file uploads, allowing an attacker to upload a file with malicious code and execute it on the server.
   7. Advanced persistent threat (APT) attacks: APT attacks are sophisticated, long-term attacks on a specific target by a skilled attacker. They often involve multiple stages, including reconnaissance, infiltration, and exfiltration of data.
      1. Password Attacks: Password attacks involve the use of brute-force techniques to crack passwords or trick users into revealing their passwords. Once the attacker gains access to a user's account, they can use it to access the organization's network.
      2. Watering Hole Attacks: In this type of attack, the attacker infects a website that the targeted organization's employees frequently visit with malware. When an employee visits the site, the malware infects their computer and gives the attacker access to the organization's network.
      3. Malware Attacks: This involves the use of malware to infiltrate an organization's network. The attacker sends an email with a malicious attachment or a link to a website that installs the malware onto the victim's computer.
      4. Supply Chain Attacks: In this type of attack, the attacker infiltrates a supplier or partner of the targeted organization and then uses their access to gain entry to the targeted organization's network.
      5. Zero-Day Exploits: These are attacks that take advantage of previously unknown vulnerabilities in software or systems. The attacker exploits the vulnerability before the developer has had a chance to patch it, giving them access to the organization's network.
2. Cyber-attacks affecting casual internet user:
   1. Malware:
      1. Viruses: All types of viruses can be accidentally downloaded from the internet by a careless internet user.
      2. Trojans: Just like any other virus, this one can be easily downloaded from anywhere. It can stay undetected by the user, if it doesn’t cause any harm to the computer, but instead allow the hacker to remotely control the computer or steal login details to all types of websites. Every virus can be disguised as a trojan.
      3. Ransomware: Also very harmful to the casual user, who probably has lots of important photos and videos on the computer.
      4. Spyware: Dangerous, because of its lack of instant harm to the user. By the time the spyware is detected, it could have already collected enough personal information.
   2. Phishing attacks: All types of Phishing are similar to one another, and they are mostly used on careless users and organization executives, who don’t check the legitimacy of a website, email or message. They can lead to leaks of personal and confidential company information.
   3. Denial of Service (DoS) attacks: Just as they can overwhelm and crash a website, they can also do that to a home router and stop access to the internet for the whole household.
   4. Man-in-the-middle (MITM) attacks: These attacks are also able to affect all types of users. They can steal important information or intercept connections.
   5. Cross-site scripting (XSS) attacks: These attacks are hard to detect and be prevented by a careful user, they can contain any type of malware.
   6. Advanced persistent threat (APT) attacks:
      1. Password Attacks: Most common way of hacking different types of accounts. Most users use passwords with their name or birthday contained in it, which makes it a lot easier to guess. A common practice is also to use the same password for every website, which makes it even more dangerous.