Different types of cyber attacks

Two basic types based on the nature of invasion :

- Passive attack : The attacker does not alter the data content. Type of network security breach where the attacker observes or monitors data being transmitted without altering or interfering with the communication. The goal is to gather sensitive information without detection.
- Active attack : Type of network security breach where the attacker actively interferes with the communication by modifying, disrupting, or injecting malicious data into the system. The goal is to alter or damage the communication process.

Passive attacks

- Eavesdropping
- Traffic analysis

Active attacks

- Man-in-the-middle (MITM) attacks can be of many types, which can be either
  - Masquarade or spoofing attacks
  - Repudiation attacks
- Denial of Service (DoS) attacks
- Replay attacks
- Data modification

Man-in-the-Middle Attack

In Man-in-the-middle or MitM attacks,

- the attacker either poses himself as a genuine user or subscriber and gets permission to log in to classified servers, or takes services which are classified, or steals classified data (Masquarade attack) or
- The attacker can perform a passive attack to evesdrop on any ongoing session to steal credentials to be used for a later masquarade, or
- sets up forged websites or portals to masquarade as a genuine service provider to steal subscribers confidential information when they connect to the forged site,
- sets up rogue network equipments in between the route of the packets from subscriber to service providers and lures subscribers to connect through them to steal informtion, or
- sets up dubious websites to provide lucrative services and advertizes to potential targets to lure them to connect to the website and provide their personal info.
- Uses spoofing to gain access to restricted services.

Masquarade attacks

Different types of masquarades are possible, i.e

- Username and Password Masquerade: In this masquerade attack, a person uses either stolen or even forged credentials to authenticate themselves as a valid user while gaining access to the system or application.
- IP address masquerade: This is an attack where the IP address of a malicious user is spoofed or forged such that the source from which the system or the application is accessed appears to be trusted.
- Website masquerade: A hacker creates a fake website that resembles as a legitimate one in order to gain user information or even download malware.
- Email masquerade: This is an e-mail masquerade attack through which an attacker sends an apparently trusted source email so that the recipient can mistakely share sensitive information or download malware.

Spoofing and Evesdropping attacks

1. Wi-Fi Eavesdropping : The attacker sets up a rogue Wi-Fi hotspot to capture data transmitted over the network. Users unknowingly connect to the fake hotspot, exposing sensitive information.
2. Packet Sniffing : The attacker uses tools like Wireshark to capture and analyze packets sent over unsecured or improperly secured networks, gaining access to sensitive data such as passwords or private messages.
3. Session Hijacking : The attacker intercepts session cookies to take over a user's session with a website or service, potentially granting access to sensitive accounts.
4. SSL Stripping : The attacker downgrades a secure HTTPS connection to an unsecured HTTP connection, making the communication vulnerable to interception.
5. DNS Spoofing : The attacker redirects users to a fake website by altering the Domain Name System (DNS) resolution process. Users believe they are visiting a legitimate site but are instead interacting with the attacker.
6. ARP Spoofing : ARP is used in many data network backbones to resolve the hardware address of the physical network from the knowledge of IP addresses, and maintains a cache for later referencing. The attacker sends fake Address Resolution Protocol (ARP) messages to a local network, linking their MAC address with the IP address of another device (e.g., a gateway). This allows interception of data meant for the intended device.
7. Email Hijacking : Attackers gain access to email communications, often in corporate environments, to intercept or manipulate sensitive information like invoices or confidential documents.
8. HTTP Spoofing : By intercepting and manipulating HTTP communications, attackers can inject malicious scripts or redirect users to malicious websites.
9. Man-in-the-Browser (MitB) The attacker installs malware on a victim's browser, enabling them to intercept or alter data during online transactions or communications without the user's awareness.
10. IoT-Based MitM : Intercepting communications between IoT devices and their control systems, exploiting the often weak security protocols in IoT ecosystems.
11. Bluetooth Interception : Exploiting vulnerabilities in Bluetooth connections to eavesdrop or inject malicious data into a communication.
12. Fake Certificate-Based Attacks : The attacker uses fraudulent digital certificates to impersonate a trusted entity and intercept secure communication.
13. Voice over IP (VoIP) Interception : Intercepting or altering VoIP communications, such as phone calls, to eavesdrop or inject malicious audio.
14. Phishing : It is an unethical way to dupe the user or victim to click on harmful sites. The attacker crafts the harmful site in such a way that the victim feels it to be an authentic site, thus falling prey to it. The most common mode of phishing is by sending spam emails that appear to be authentic and thus, taking away all credentials from the victim.

Types of Phishing attacks

There are several types of Phishing Attacks, some of which are mentioned below. Below

- Email Phishing: The most common type where users are tricked into clicking unverified spam emails and leaking secret data. Hackers impersonate a legitimate identity and send emails to mass victims. Apart from stealing personal info, another intention is to install spyware or malware in the users' system which would periodically keep sending confidential data of the user to a rogue site.
- Spear Phishing: In spear phishing a phishing attack, a particular user(organization or individual) is targeted. In this method, the attacker first gets the full information of the target and then sends malicious emails to his/her inbox to trap him into typing confidential data.
- Smishing: In this type of phishing attack, the medium of phishing attack is SMS. Smishing works similarly to email phishing.
- Vishing: Vishing is also known as voice phishing. In this method, the attacker calls the victim using modern caller ID spoofing to convince the victim that the call is from a trusted source. Attackers also use IVR to make it difficult for legal authorities to trace the attacker.
- Clone Phishing: Email messages that were sent from a trusted source are copied and then the mail is altered to add as attachment a hyperlink to a malicious or fake website. This altered mail is sent to a larger number of users. Once clicked, the user is directed to the malicious site and the mail is forwarded to all the contacts of the affected user's contact list.

Mitigation of MitM attacks

- Use encrypted connections (e.g., HTTPS, VPNs).
- Implement strong network authentication methods.
- Regularly update software and firmware.
- Employ security tools like firewalls and intrusion detection systems.
- Use DNSSEC to protect against DNS spoofing.
- Educate users about phishing and rogue networks. There are anti-phishing tools like Anti-Phishing Domain advertizer (APDA), Phishtank, Webroot anti-Phishing, MAlwarebytes anti-phishing, Kaspersky anti-phishingi tool etc.These anti-phishing tools can provide an additional layer of protection against phishing attacks, but it is important to remember that they are not a complete solution.

Repudiation attack

Repudiation attack are a type of cyber attack wherein some person does some unauthorized transaction or usage of resources, and there is no trace to prove that unauthorised access. Such attacks can seriously hinder the ability to trace down the origin of the attack or to identify who is responsible for a given action, making it tricky to hold responsible the right person.

Types of repudiation attacks :

- Message repudiation attacks: In this attack, a message has been sent by an attacker, but the attacker later denies the sending of the message. This can be achieved either through spoofed or modified headers or even by exploiting vulnerabilities in the messaging system.
- Transaction repudiation attacks: Here, in this type of attack, a transaction-for example, monetary transaction-is made, and at after some time when the evidence regarding the same is being asked to be give then the attacker

denies ever performing that particular transaction. This can be executed either by taking advantage of the vulnerability in the transaction processing system or by the use of stolen and forged credentials.

- Data repudiation attacks: In a data repudiation attack, data is changed or deleted. Then an attacker will later pretend he has never done this. This can be done by exploiting vulnerabilities in the data storage system or by using stolen or falsified credentials.

Denial of Service attack

Denial of Service (DoS) is a form of cybersecurity attack that involves denying the intended users of the system or network access by flooding traffic or requests. In this DoS attack, the attacker floods a target system or network with traffic or requests in order to consume the available resources such as bandwidth, CPU cycles, or memory and prevent legitimate users from accessing them.

There are several types of DoS attacks, including:

- Flood attacks: Here, an attacker sends such a large number of packets or requests to a system or network that it cannot handle them all and the system gets crashed.
- Amplification attacks: In this category, the attacker increases the power of an attack by utilizing another system or network to increase traffic then directs it all into the target to boost the strength of the attack.

To Prevent DoS attacks, organizations can implement several measures, such as:

1. Using firewalls and intrusion detection systems to monitor network traffic and block suspicious activity.

2. Limiting the number of requests or connections that can be made to a system or network.

3. Using load balancers and distributed systems to distribute traffic across multiple servers or networks.

4. Implementing network segmentation and access controls to limit the impact of a DoS attack.