Class Assignment

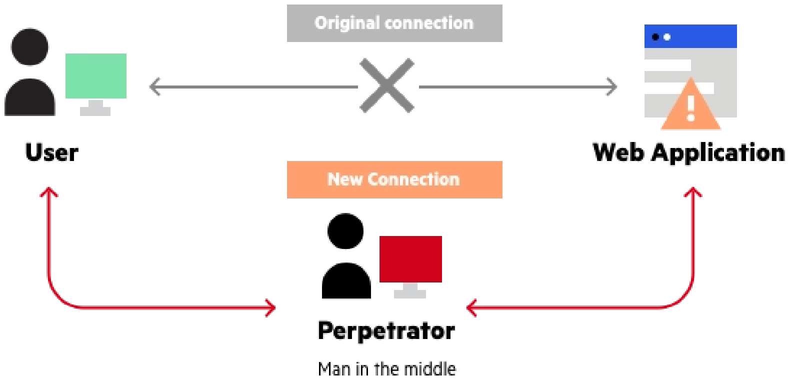
1) What is MiTM and how does it work??

MiTM stands for Man-in-the-Middle Attack.

A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.

The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers. Targets are typically the users of financial applications, SaaS businesses, e-commerce sites and other websites where logging in is required.

Information obtained during an attack could be used for many purposes, including identity theft, unapproved fund transfers or an illicit password change.



The first step intercepts user traffic through the attacker's network before it reaches its intended destination.

This can be achieved by the following approach:

- IP Spoofing
- ARP Spoofing
- DNS Spoofing

By using the above methods, attacker redirects the connection of the website or application to himself and then send that traffic to the user. This makes him capable of reading and checking all the data transferred between 2 parties.

2) What are the types of MiTM?

Types of Man in the Middle Attacks are:

1. IP spoofing

Every device capable of connecting to the internet has an internet protocol (IP) address, which is similar to the street address for your home. By spoofing an IP address, an attacker can trick you into thinking you're interacting with a website or someone you're not, perhaps giving the attacker access to information you'd otherwise not share.

2. DNS spoofing

Domain Name Server, or DNS, spoofing is a technique that forces a user to a fake website rather than the real one the user intends to visit. If you are a victim of DNS spoofing, you may think you're visiting a safe, trusted website when you're actually interacting with a fraudster. The perpetrator's goal is to divert traffic from the real site or capture user login credentials.

3. HTTPS spoofing

When doing business on the internet, seeing "HTTPS" in the URL, rather than "HTTP" is a sign that the website is secure and can be trusted. In fact, the "S" stands for "secure." An attacker can fool your browser into believing it's visiting a trusted website when it's not. By redirecting your browser to an unsecure website, the attacker can monitor your interactions with that website and possibly steal personal information you're sharing.

4. SSL hijacking

When your device connects to an unsecure server — indicated by "HTTP" — the server can often automatically redirect you to the secure version of the server, indicated by "HTTPS." A connection to a secure server means standard security protocols are in place, protecting the data you share with that server. SSL stands for Secure Sockets Layer, a protocol that establishes encrypted links between your browser and the web server.

In an SSL hijacking, the attacker uses another computer and secure server and intercepts all the information passing between the server and the user's computer.

5. Email hijacking

Cybercriminals sometimes target email accounts of banks and other financial institutions. Once they gain access, they can monitor transactions between the institution and its customers. The attackers can then spoof the bank's email address and send their own instructions to customers. This convinces the customer to follow the attackers' instructions rather than the bank's. As a result, an unwitting customer may end up putting money in the attackers' hands.

6. Wi-Fi eavesdropping

Cybercriminals can set up Wi-Fi connections with very legitimate sounding names, similar to a nearby business. Once a user connects to the fraudster's Wi-Fi, the attacker will be able to monitor the user's online activity and be able to intercept login credentials, payment card information, and more. This is just one of several risks associated with using public Wi-Fi. You can learn more about such risks here.

7. Stealing browser cookies

To understand the risk of stolen browser cookies, you need to understand what one is. A browser cookie is a small piece of information a website stores on your computer.

3) What is DDOS and how DDOS works?

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices.

From a high level, a DDoS attack is like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination.

DDoS attacks are carried out with networks of Internet-connected machines.

These networks consist of computers and other devices (such as IoT devices) which have been infected with malware, allowing them to be controlled remotely by an attacker. These individual devices are referred to as bots (or zombies), and a group of bots is called a botnet.

Once a botnet has been established, the attacker is able to direct an attack by sending remote instructions to each bot.

When a victim's server or network is targeted by the botnet, each bot sends requests to the target's IP address, potentially causing the server or network to become overwhelmed, resulting in a denial-of-service to normal traffic.

Because each bot is a legitimate Internet device, separating the attack traffic from normal traffic can be difficult.

4) What are the types of DDOS?

Most common types of DDOS are:

- TCP/UDP Flood
- ICMP (Ping) Flood
- SYN Flood
- Ping of Death
- Slowloris
- NTP Amplification
- HTTP Flood

5) Discuss a Proxy server and what is the difference between a VPN and a Proxy Server?

A proxy server is a computer system or router that functions as a relay between client and server. It helps prevent an attacker from invading a private network and is one of several tools used to build a firewall.

The word proxy means "to act on behalf of another," and a proxy server acts on behalf of the user. All requests to the Internet go to the proxy server first, which evaluates the request and forwards it to the Internet. Likewise, responses come back to the proxy server and then to the user.

While on the other hand, VPN (Virtual Private Network) creates a dedicated encrypted connection to another site or server.

A VPN, or Virtual Private Network, routes all of your internet activity through a secure, encrypted connection, which prevents others from seeing what you're doing online and from where you're doing it. Basically, a VPN provides an extra layer of security and privacy for all of your online activities.