Understanding Cyber Security:

MAN-IN-THE-MIDDLE (MitM) ATTACK

is a form of cyberattack that happens when attackers eavesdrop on the communication between two parties. This results in important data being intercepted by the attacker in the process of them being an active or passive participant in the conversation. For instance, they may either impersonate a legitimate user or quietly listen in on the conversation.

Attack Techniques

Sniffing

Attackers deploy tools that inspect packets – units of data that are transferred over a network. The data collected is then used to intercept (or "sniff") unencrypted information such as passwords and usernames.

Packet Injection

Malicious packets are being injected into data communication streams to disrupt the user's network access. These packets appear to be part of the communication, but are malicious in nature.

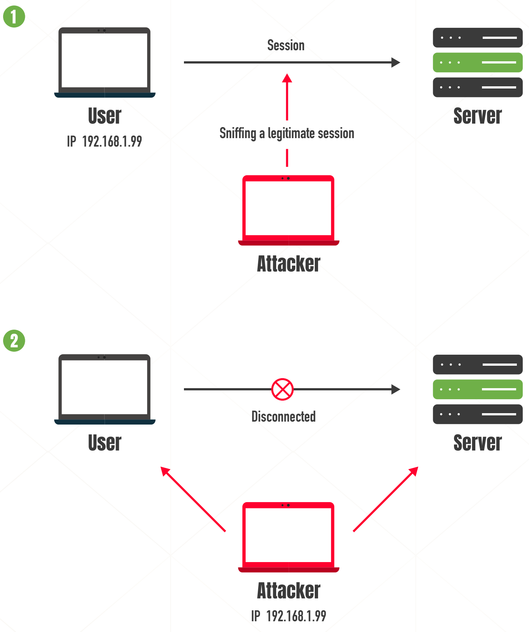
Session Hijacking

An attacker sniffs data packets to steal session cookies from the user's device, allowing them to hijack a user session through the identification of the session token.

SSL Stripping

Traffic is intercepted from a HTTPS website though interception of packets and alteration of their address to direct the user to the less secure HTTP equivalent. This forces the host to make requests to the server unencrypted, and sensitive data is leaked as a result.

How It Works? - An Example on Session Hijacking



1. A client connects to a server.
2. The attacker's computer gains control of the client.
3. The attacker's computer disconnects the client from the server.
4. The attacker's computer replaces the client's IP address with its own IP address and spoofs the client's sequence numbers.
5. The attacker's computer continues dialog with the server and the server believes it is still communicating with the client.

Prevention Tips

Strong WEP/WAP Encryption

Having a strong encryption mechanism on wireless access points prevents unwanted users from joining your network due to proximity. The stronger the encryption implementation, the safer.

Strong Router Login Credentials

Ensure that you change your default router login credentials to lessen the chances of the attacker accessing your network to change your DNS servers to their malicious servers.

Virtual Private Network

VPN is used to mask your IP address as it goes through a private server. VPN uses key-based encryption to create a subnet for secure communication. This makes your network less penetrable to the attackers.

Force HTTPS

HTTPS can be used to securely communicate over HTTP using public-private key exchange to preventing sniffing. Websites should only use HTTPS. Users can install browser plugins to enforce always using HTTPS on requests.