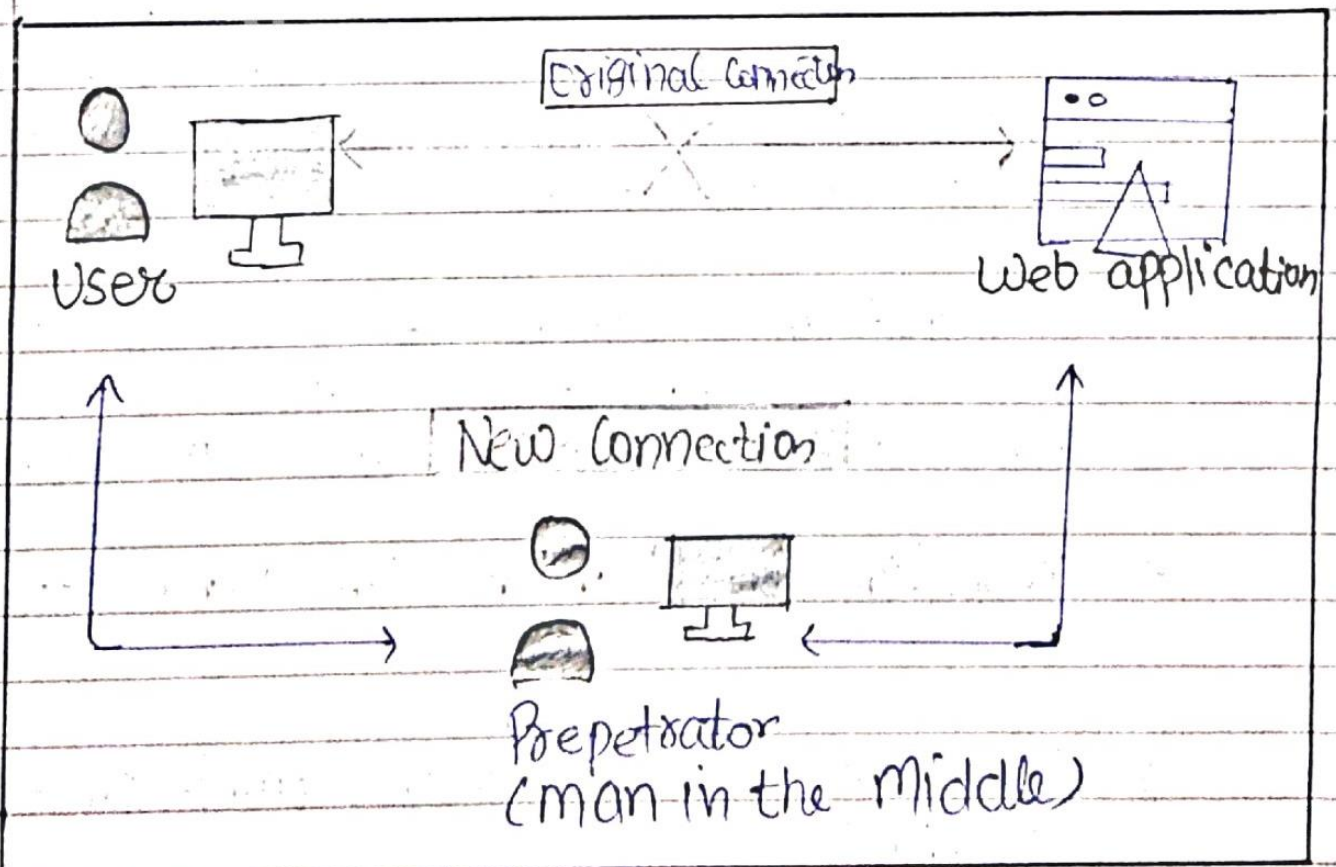


* Man in the Middle Attack :-

- A man-in-the-middle attack is a type of eavesdropping attack, where attacks intercept an existing conversation of data transfer.
- The goal of an attack is to steal Personal information, such as login information, account details and credit card numbers.
- Information obtained during an attack could be used for many purposes, including identity theft, unapproved fund transfers etc.



(Man in the middle attack example)

_ / _ / _

* Types of Man-in-the-Middle Attacks:-

(i) E-mail-Hijacking :- In this, attackers gain access to a user's email account and watch transactions to and from the account.

(ii) Wi-fi Eavesdropping :- Wifi eavesdropping involves cyber hackers setting up public Wi-fi connections, typically with an unsuspecting name and gain access.

(iii) DNS Spoofing :- An attacker engages in DNS Spoofing by altering a website's address record within a DNS (Domain Name Server) server.

(iv) IP Spoofing :- Instead of spoofing the website's address record, the attacker disguises an IP address.

* Prevention for Man-in-the-Middle Attacks:-

(i) Implement a Comprehensive Email-Security Solution :-

→ It will help minimize the risk associated with MITM.

→ It secures email activity while staff focuses efforts elsewhere.

(ii) Implement a Web Security Solution:-

→ It is similar to an email security tool, this implementation protects your organization's web traffic so the security team can cover more ground.

(iii) Educate Employees:-

→ Prepare your workforce for these advanced attacks by educating them on the dynamics, patterns, samples and frequency of attack methods attempted on their organization.

(iv) Keep Credentials Secure :-

→ Make sure your passwords are secure, complex and updated every three months at minimum.