# Topic-5

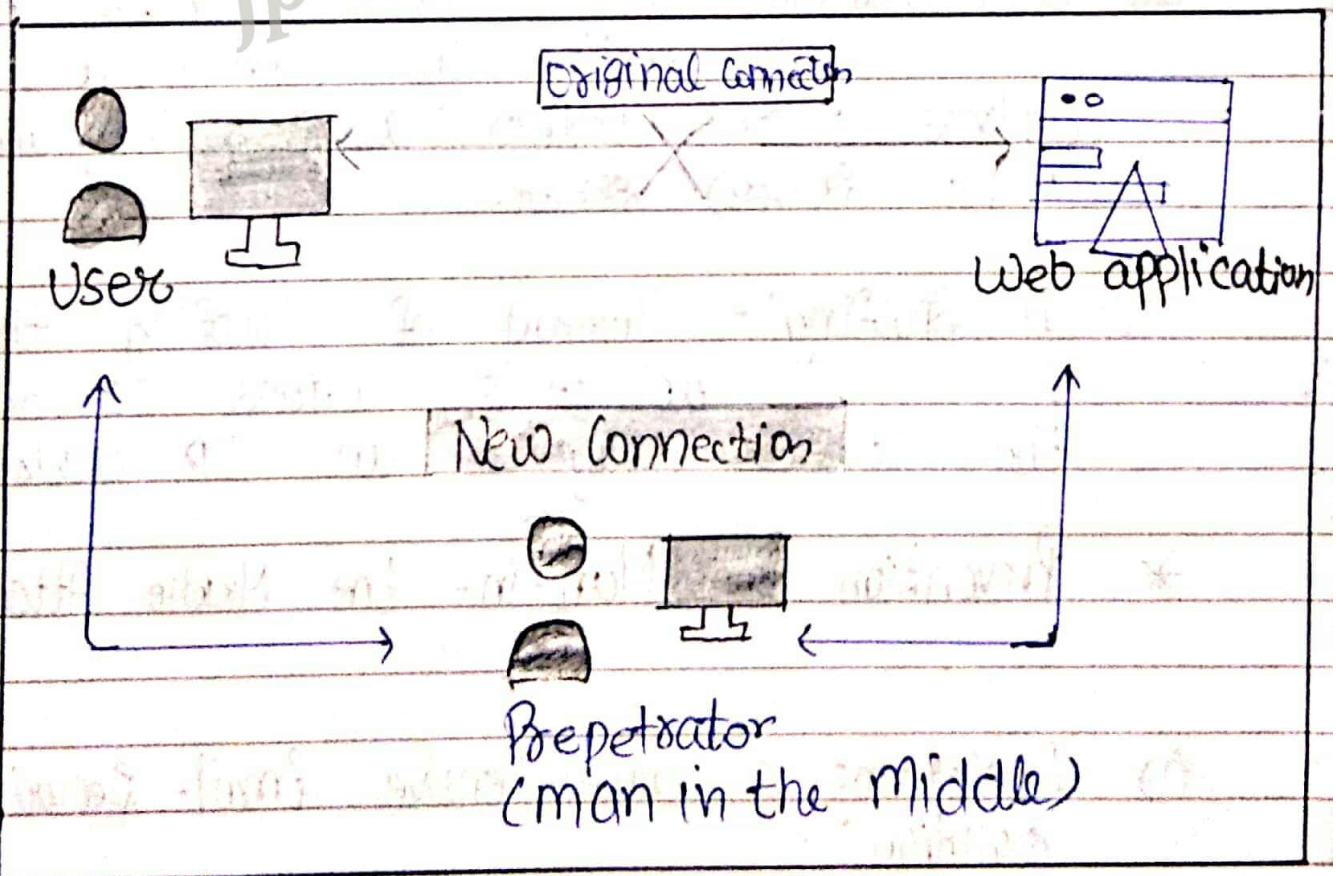
Notes by jpwebdevelopers

## * Man in the Middle Attack :-

→ A man-in-the-middle attack is a type of evastropping attack, where attacks interrupt an existing conversation of data transfer.

→ The goal of an attack is to steal Personal information, such as logic information, account details and credit card numbers.

→ Information obtained during an attack could be used as 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 suspecting 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 attemped on their Organization.

(IV) Keep Credentials Secure:-

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