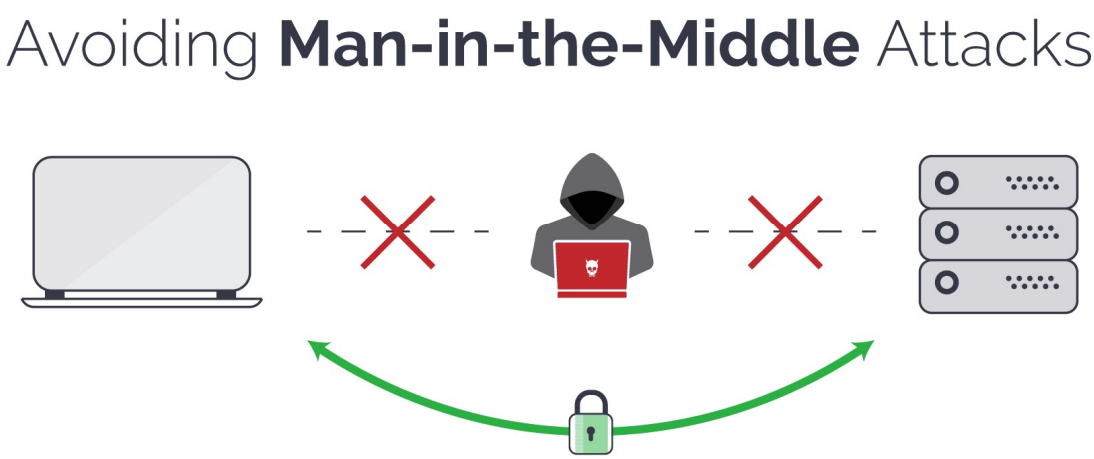
Man In The Middle (MITM)

Une attaque Man In The Middle signifie en français Homme du milieu. C'est une attaque d'**interception** ou un pirate s'intercale entre deux interlocuteurs pour écouter, modifier ou voler les données échangées sans que les victimes s'en rendent compte. L'attaquant peut lire, insérer ou altérer les communications entre deux parties qui croient encore parler entre eux.

Mais comment ça fonctionne ?



La victime tente de se connecter à un serveur (par exemple une banque), l'attaquant intercepte la connexion et agis comme un relais. A ce moment l'attaquant se fait soit passer pour le serveur aux yeux de la victime ou il se fait passer pour la victime auprès du serveur. Et résultat l'attaquant à accès aux données sensibles comme (mots de passes, numéro carte bancaire…).

Voici les différentes techniques courantes pour effectuer un MITM :

Technique	Description
ARP Spoofing	Falsification des tables ARP pour détourner le trafic local.
DNS Spoofing	Fausse réponse DNS pour rediriger la victime vers un faux site
Wi-Fi Evil Twin	Création d'un faux point Wi-Fi pour piéger les victimes
SSL Stripping	Suppression du chiffrement HTTPS pour forcer du HTTP
Session Hijacking	Vol de cookies de session pour usurper l'identité de la victime

ARP Spoofing généralement, l'objectif est d'associer l' adresse MAC de l'attaquant à l' adresse IP d'un autre hôte, comme la passerelle par défaut, ce qui provoque l'envoi à l'attaquant de tout trafic destiné à cette adresse IP.

L'usurpation d'identité ARP peut permettre à un attaquant d'intercepter des trames de données sur un réseau, de modifier le trafic ou de l'interrompre complètement. Cette attaque est souvent utilisée comme une ouverture pour d'autres attaques, telles que le déni de service, l'attaque de l'homme du milieu ou le détournement de session .

L'usurpation DNS , également appelée empoisonnement du cache DNS , est une forme de piratage informatique consistant à introduire des données corrompues du système de noms de domaine (DNS) dans le cache du résolveur DNS , ce qui amène le serveur de noms à renvoyer un enregistrement de résultat incorrect, par exemple une adresse IP . Le trafic est alors redirigé vers l'ordinateur de son choix. En d'autres termes, un pirate fait croire à l'appareil de la victime qu'il se connecte au site web choisi, alors qu'en réalité, il est redirigé vers un autre site web en modifiant l'adresse IP associée au nom de domaine dans le serveur DNS.

Wi-Fi Evil Twin consiste à créer un faux réseau WiFi, pour piéger les internautes et capturer leurs données personnelles. Lors d'une attaque Evil Twin, un hacker met en place **un faux réseau WiFi légitime en apparence**. Dès qu'un internaute s'y connecte, ses données personnelles et identifiants de connexion sont dérobés.

SSL Stripping : Lorsqu'un utilisateur tente d'accéder à un site HTTPS sécurisé, son navigateur recherche généralement le certificat de sécurité du site web concerné afin de garantir une connexion sécurisée. Le décryptage SSL perturbe ce processus, forçant le site à se charger via HTTP. Ce déclassement signifie que les données transférées entre le navigateur et le site web ne sont plus chiffrées et sont donc vulnérables aux interceptions.

Session Hijacking : L'attaque de détournement de session consiste à exploiter le mécanisme de contrôle de session Web, qui est normalement géré pour un jeton de session.

La communication HTTP utilisant de nombreuses connexions TCP différentes, le serveur web a besoin d'une méthode pour reconnaître les connexions de chaque utilisateur. La méthode la plus efficace repose sur un jeton que le serveur web envoie au navigateur client après une authentification réussie. Un jeton de session est généralement composé d'une chaîne de longueur variable et peut être utilisé de différentes manières : dans l'URL, dans l'en-tête de la requête HTTP (cookie), dans d'autres parties de l'en-tête de la requête HTTP, ou encore dans le corps de la requête HTTP.

L'attaque par détournement de session compromet le jeton de session en volant ou en prédisant un jeton de session valide pour obtenir un accès non autorisé au serveur Web.

Le jeton de session peut être compromis de différentes manières ; les plus courantes sont :

- Jeton de session prévisible ;
- Reniflage de session
- MITM

Pour se protéger d'une attaque MITM il faut vérifier que la connexion est sécurisée avec HTTPS, ne jamais se connecter à des réseaux publics sans protections. L'utilisation d'un VPN est aussi une solution pour chiffrer la communication, authentification à double facteur…