L'attaque de l'homme du milieu

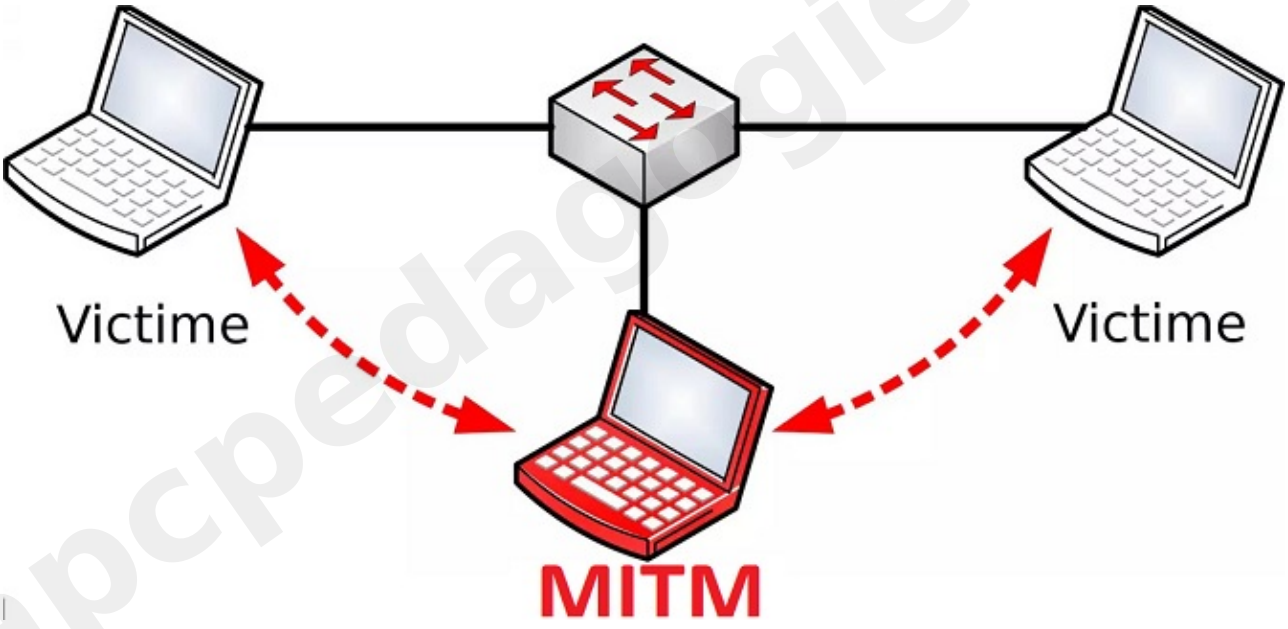
[sommaire]

1. **Objectifs**

- Connaitre et se protéger contre une attaque dite de l'homme du milieu

- **Qu’est-ce qu’une attaque Man-in-the-Middle**

  - Une attaque man in the middle (littéralement "attaque de l'homme au milieu" ou "attaque de l’intercepteur"), parfois notée MITM, est un scénario d’attaque dans lequel un pirate écoute une communication entre deux interlocuteurs et falsifie les échanges afin de se faire passer pour l’une des parties.



  - L’attaque de l’homme du milieu (MITM) est un terme général désignant le fait pour un attaquant de se positionner dans une conversation entre un utilisateur et une application, ou bien entre deux utilisateurs, soit pour écouter, soit pour se faire passer pour l’une des parties, en donnant l’impression qu’un échange normal d’informations est en cours.
  - *L'**attaque de l'homme du milieu** (HDM) ou man-in-the-middle attack (MITM), parfois appelée attaque de l'intercepteur, est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis.*

- Une **attaque de l’homme du milieu** désigne un modèle de cyberattaque dans lequel un cybercriminel installe, physiquement ou logiquement, un système contrôlé entre le système de la victime et une ressource Internet qu’elle utilise.
- L'objectif de l'attaquant est d’intercepter, de lire ou de manipuler toute communication entre la victime et sa ressource sans se faire remarquer.
- Une attaque de type "**Man in The Middle**" (MiTM) est une attaque dans laquelle l’agresseur intercepte et relaie secrètement des messages entre deux parties qui croient communiquer directement l’une avec l’autre.
- Une attaque de l'homme du milieu est une technique de hacking par laquelle un pirate informatique intercepte les communications entre deux parties, sans que ni l’une ni l’autre ne puisse se douter que le canal de communication entre elles a été compromis. Dans le cas d’une attaque qui pourrait vous concerner, cela affecterait votre PC, votre mobile ou encore le réseau WiFi que vous utilisez.

Quelques types d’attaques MiTM

- En règle générale, une attaque **MiTM** peut se faire de quatre manières principales :

1. **Le reniflage de paquets (packet sniffing)**

- Le reniflage de paquets est l’une des méthodes d’attaque MiTM les plus courantes et constitue une forme d’écoute ou de mise sur écoute, sauf que ce ne sont pas des conversations téléphoniques que les pirates essayent d’obtenir. Il s’agit de paquets de données envoyés entre les deux systèmes.
- Le reniflage de paquets est la pratique consistant à collecter, collecter et enregistrer certains ou tous les paquets qui transitent par un réseau informatique, quelle que soit la manière dont le paquet est adressé.
- Un renifleur de paquets, parfois appelé analyseur de paquets, est composé de deux parties principales.

1. Une carte réseau qui connecte le renifleur au réseau existant.
2. Un logiciel qui permet de consigner, de voir ou d'analyser les données collectées par l'appareil.

- La capture de données sur un réseau entier peut nécessiter plusieurs renifleurs de paquets.
- Étant donné que chaque collecteur ne peut collecter que le trafic réseau reçu par la carte réseau, il peut ne pas être en mesure de voir le trafic qui existe de l'autre côté des routeurs ou des commutateurs.
- Sur les réseaux sans fil, la plupart des adaptateurs sont capables de se connecter à un seul canal à la fois.

apcpedagogie.com

- Afin de capturer des données sur plusieurs segments de réseau ou plusieurs canaux sans fil, un renifleur de paquets est nécessaire sur chaque segment du réseau.
- La plupart des solutions de surveillance de réseau fournissent le reniflage de paquets comme l'une des fonctions de leurs agents de surveillance.

- **L’injection de paquets**

  - L'injection de paquets (également appelée falsification de paquets ou usurpation de paquets) dans les réseaux informatiques , est le processus d'interférence avec une connexion réseau établie au moyen de la construction de paquets pour apparaître comme s'ils faisaient partie du flux de communication normal.
  - Le processus d' **injection de paquets** permet à un tiers inconnu de perturber ou d'intercepter les paquets des parties consentantes qui communiquent, ce qui peut entraîner une dégradation ou un blocage de la capacité des utilisateurs à utiliser certains services ou protocoles réseau .
  - L'injection de paquets est couramment utilisée dans les attaques de type "homme du milieu" et les attaques par déni de service .

- **Le détournement de session TCP**

  - Le vol de **session TCP** (également appelé **détournement de session TCP** ou TCP **session hijacking**) est une technique consistant à intercepter une session TCP initiée entre deux machines afin de la détourner.
  - Dans la mesure où l'authentification s'effectue uniquement à l'ouverture de la session, un pirate réussissant cette attaque parvient à prendre possession de la connexion pendant toute la durée de la session.
  - Le détournement de session se produit lorsqu'un attaquant prend le contrôle d'une session valide entre deux ordinateurs. L'attaquant vole un identifiant de session valide afin de pénétrer dans le système et de fouiller les données.
  - Le plus souvent, l'authentification se produit seulement au début d'une session TCP. Dans un détournement de session TCP, un attaquant obtient l'accès en prenant en charge une session TCP entre deux machines en milieu de session.
  - **Le processus de piratage de session**

1. **Sniffez**, c'est-à-dire effectuez une attaque d'homme-dans-le-milieu (MitM), placez-vous entre la victime et le serveur.
2. **Surveillez** les paquets circulant entre le serveur et l'utilisateur.
3. **Brisez** la connexion de la machine victime.
4. **Prenez** le contrôle de la session.

apcpedagogie.com

5. **Injectez** de nouveaux paquets au serveur en utilisant l'ID de session de la victime.

- **La redirection des utilisateurs des sites malveillants**

  - Si des pirates informatiques compromettent votre site, ils peuvent insérer du code malveillant qui redirige les visiteurs vers des sites de phishing ou de logiciels malveillants.

- ## Analyseur de trames

  - Pour pénétrer un réseau sur lequel ils veulent mener ce type d'attaque, les pirates utilisent un analyseur de trames (sniffer en anglais) qui permet d'écouter le trafic d'un réseau et de capter les informations qui circulent.
  - Pour réaliser cette attaque, voici une liste de logiciels utiles :

  - **nemesis**

    Sous Linux, permet de forger des requêtes ARP, entre autres ;

  - **scapy**

    Sous Linux également, est un outil très pratique en réseau, il permet de faire beaucoup de choses comme forger des requêtes ou faire de l'analyse réseau par exemple ;

  - **Wireshark**

    Sous Linux et Windows, permet d'analyser les requêtes qui passent par votre carte réseau ; Autrefois connu sous le nom d'Ethereal, Wireshark est un "sniffer" ou analyseur de protocoles réseau et applicatif. C'est-à-dire qu'il va capturer des paquets IP transitant sur un réseau de manière transparente pour qu'ils soient ensuite analysés. Des filtres de capture peuvent être appliqués afin de recueillir des paquets correspondants à des besoins particuliers. Distribué sous licence GNU GPL, Wireshark est utilisé par les administrateurs réseau et les experts en sécurité lors de tests d'intrusion, notamment pour des scénarios d'attaque man-in-the-middle.

  - **Cain&Abel**

    Pour Windows, est un outil très puissant et potentiellement très dangereux, car il permet en quelques clics de notamment casser des mots de passe, de cracker des réseaux Wi-Fi et (c'est ce qui nous intéresse ici) de mettre en œuvre une attaque MITM très facilement ! Ce logiciel est génial car il est redoutable et facile d'utilisation, mais il peut être détecté

apcpedagogie.com

comme dangereux par les antivirus. Et pour cause ! Il permet même de prendre discrètement le contrôle d'une machine à distance !

- ## Comment vous protéger contre les attaques de MITM

  - L'essentiel est de faire en sorte de naviguer en toute sécurité. En chiffrant le trafic entre le réseau et votre appareil à l'aide d'un logiciel de chiffrement de navigation, vous pouvez repousser les éventuelles attaques dites de l'homme du milieu.
  - Vérifiez toujours que les sites que vous visitez sont sécurisés. La plupart des navigateurs affichent un symbole de cadenas à côté de l'URL lorsqu'un site Web est sécurisé. Si vous ne voyez pas ce symbole, vérifiez que l'adresse Web commence par « https ». Le « S » signifie sécurisé et garantit que vos données ne seront pas susceptibles d'être interceptées par un pirate.
  - Utiliser un pare-feu est également un moyen fiable de protéger vos données de navigation. Sans être infaillible, un pare-feu fournit un degré de sécurité supplémentaire lorsque vous utilisez un réseau wifi public. Si vous naviguez souvent sur un réseau wifi public, il est conseillé de configurer un réseau privé virtuel (VPN). Ce type de réseau protège votre trafic et complique la tâche des pirates qui voudrait l'intercepter.
  - Mettez vos logiciels de sécurité à jour. Les cybercriminels ne cessent de s'adapter et de se perfectionner, vous devriez en faire de même. En mettant à jour votre solution de sécurité, vous avez accès en permanence à des outils dernier cri qui surveillent votre activité en ligne pour une navigation sécurisée et agréable.
  - **Commande:** `Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Windows-Subsystem-Linux`

Sources:

- *https://www.kaspersky.fr/resource-center/threats/man-in-the-middle-attack*

Sommaire du cours Administration et sécurité des sites web

Source : https://apcpedagogie.com/lattaque-de-lhomme-du-milieu · téléchargé le 04/11/2026 · © APC Pédagogie · apcpedagogie.com