

COMPTE RENDU

MAN IN THE MIDDLE



💧 **Réalise par**


OTHMANE TAYBI


💧 **Encadré par**

M. OMOR




Qu'est-ce qu'une attaque MITM :






 Une attaque d'homme du milieu (MITM) est un terme général désignant le moment où un auteur se positionne dans une conversation entre un utilisateur et une application, soit pour écouter, soit pour se faire passer pour l'une des parties, ce qui donne l'impression qu'il s'agit d'un échange normal d'informations. Est en cours.

 Le but d'une attaque est de voler des informations personnelles, telles que les informations de connexion, les détails du compte et les numéros de carte de crédit. Les cibles sont généralement les utilisateurs d'applications financières, les entreprises SaaS, les sites de commerce électronique et d'autres sites Web où la connexion est requise.



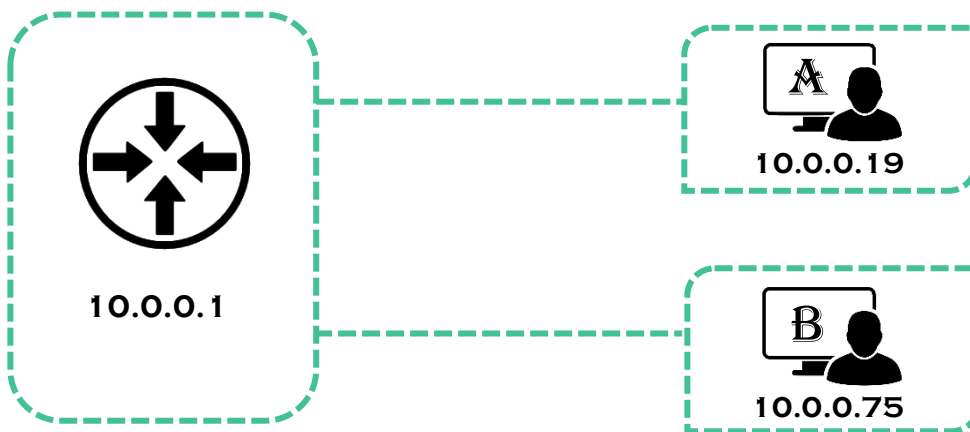
Concepts clés d'une attaque Man-in-the-Middle :

 Attaques de l'homme du milieu :

-  Sont un type de détournement de session.
-  Impliquer des attaquants s'insérant en tant que relais ou mandataires dans une conversation ou un transfert de données en cours et légitimes.
-  Exploitez la nature en temps réel des conversations et des transferts de données pour passer inaperçus.
-  Autoriser les attaquants à intercepter des données confidentielles.
-  Autoriser les attaquants à insérer des données et des liens malveillants d'une manière indiscernable des données légitimes.

Test MITM [Man-in-the-Middle] :

CONFIGURATION DU RÉSEAU :



ATTAQUANT/VICTIME :

Dans ce scénario, l'attaquant **A** [10.0.0.19] attaquera le Victime **B** [10.0.0.75]



APERÇU DE L'ATTAQUE :

- Attaque [ARP Poisoning](#), cela attaque la table de recherche que chaque routeur contient des adresses MAC adresses IP. Si nous pouvons modifier les entrées de cette table, elle peut recevoir tout le trafic destiné à une autre partie, établir une connexion avec cette partie, la rediriger et manipuler les informations des Victime.
- L'attaque utilisera [Ettercap](#) pour automatiser la transmission des paquets ARP corrects. Cela incitera le routeur à mettre à jour sa liste d'adresses MAC et d'adresses IP, et tentera également de renvoyer le trafic vers le MAC de l'attaquant.



Mise en œuvre :



INSTALLER DES OUTILS :

Nous utiliserons plusieurs outils différents pour effectuer l'attaque de MITM :

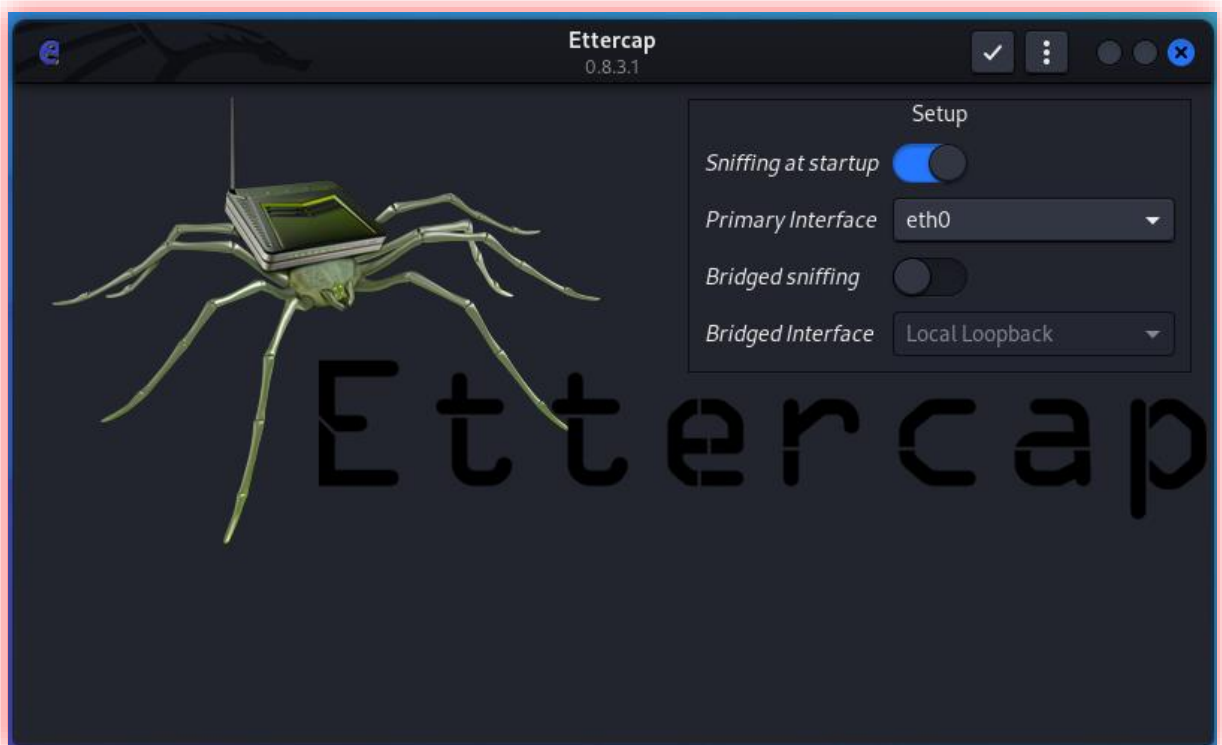
- Dans cette attaque, nous aurons besoin [Ettercap](#) et de [Wireshark](#) pour démarrer et exécuter l'attaque.
- Nous devons peut-être utiliser [Driftnet](#) pour analyser le trafic pendant l'attaque.

INSTALLATION ETTERCAP :

Pour installer Ettercap en taper la commande `sudo apt install ettercap-common`

```
(root@serverDNS)~# apt install ettercap-common
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ettercap-common is already the newest version (1:0.8.3.1-4).
ettercap-common set to manually installed.
```

- Viola l'interface de Ettercap :

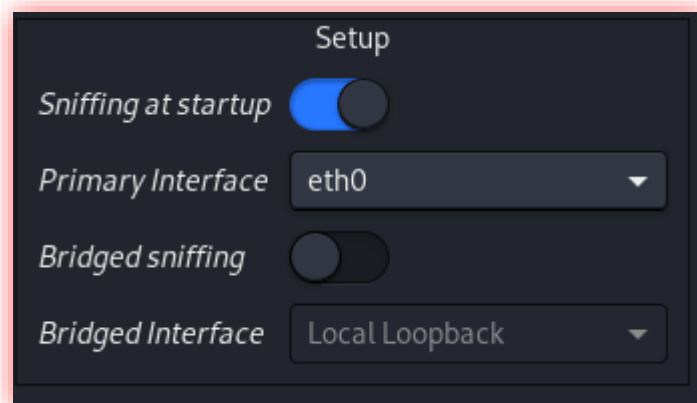


- L'étape suivante consiste à effectuer un **ARP poisoning** avec **Ettercap**.
 - Avec la commande **Ettercap -G** :

```
(root@serverDNS)-[~]  
# ettercap -G  
  
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
```

TYPE DE RENIFLEMENT À ETTERCAP :

- Nous allons maintenant spécifier le type de reniflement que nous voulons qu'Ettercap fasse.
- Nous ferons du reniflement unifié. Sélectionnez Sniff > Unified Sniffing dans le menu.

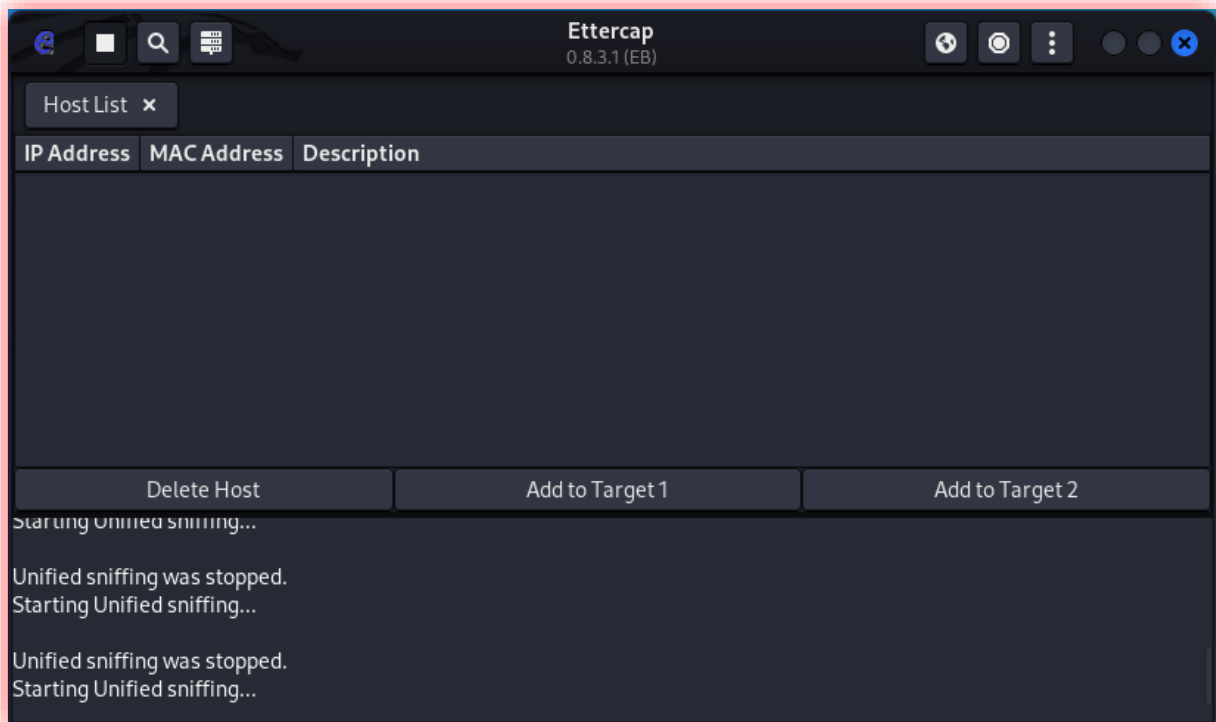




TROUVER DES HÔTES À ETTERCAP :

🔥 Une fois que nous avons choisi notre méthode de reniflement, nous devons choisir une cible, puis lancer notre attaque.

🔥 Nous pouvons exécuter une analyse rapide des différents hôtes agissant en tant que parties dans le trafic réseau. Cliquez sur Hôtes > Rechercher des hôtes pour exécuter une analyse rapide et obtenir une liste des hôtes cibles. Vous devriez voir Ettercap remplir une liste d'adresses IP et MAC hôtes.





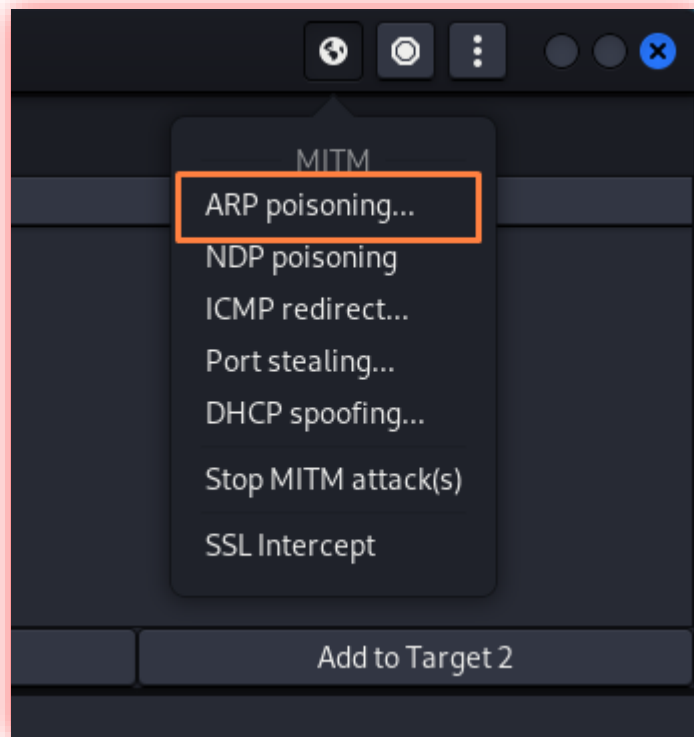
SÉLECTIONNEZ LA ETTERCAP POISON TARGET :

• Maintenant que nous avons une liste d'hôtes, nous recherchons notre cible dans la liste



ON COMMENCE L'ATTAQUE MITM :

• Nous cliquons sur **MITM** > **Arp Poisoning** pour sélectionner l'attaque Arp Poisoning :



• Cela imprimera un message nous indiquant qu'une attaque d'empoisonnement ARP a commencé. Lorsque des informations intéressantes/excitantes apparaissent sur le fil, Ettercap les extraira et les affichera, juste au cas où elles n'auraient pas été capturées ou trouvées avec Wireshark.

HTTPS/SSL :

♦ Parlons de la façon de gérer HTTPS lors d'une attaque par ARP poisoning par MITM.

♦ Si vous utilisez Ettercap et laissez Ettercap gérer les certificats SSL, ils seront faux et invalides, et éveilleront les soupçons du Victime.

♦ Pour éviter ce genre d'avertissements, nous pouvons utiliser **SSLStrip**.

UTILISATION DE SSLSTRIP :

♦ SSLStrip est un service qui détournera de manière transparente une session HTTP, et chaque fois qu'il y aura une redirection HTTPS ou un lien HTTPS, il le transformera en son équivalent HTTP.

♦ Cela permet à un attaquant de forcer un Victime sur des connexions HTTP au lieu de connexions HTTPS.

♦ Cependant, cela n'affectera que les liens et les redirections. Il ne forcera pas HTTP si la cible tape réellement "https://" dans la barre d'adresse du navigateur.



UTILISATION DU PARE-FEU :

🔥 Nous allons configurer une règle de pare-feu qui recherchera tout trafic lié au port 80 et le redirigera vers le port sur lequel SSLStrip écoute.

```
(root@serverDNS)~  
# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-ports 6666
```

🔥 Et pour nous assurer que cela fonctionne, nous faisons une liste de nos règles :

```
(root@serverDNS)~  
# iptables --list -t nat
```

🔥 Ou on supprime toutes les règles :

```
(root@serverDNS)~  
# iptables --flush -t nat
```

🔥 Nous avons donc maintenant une règle de pare-feu qui dirige tout trafic destiné au port 80 vers le port 6666, où SSLStrip l'attend.



DÉMARRER SSLSTRIP :

🔥 Maintenant que nous avons notre règle de pare-feu, nous pouvons démarrer SSLStrip :

```
Command 'sslststrip' not found, but can be installed with:  
apt install sslstrip  
  
(root@serverDNS)-[~]  
# sslstrip -l 6666
```

127 ✕