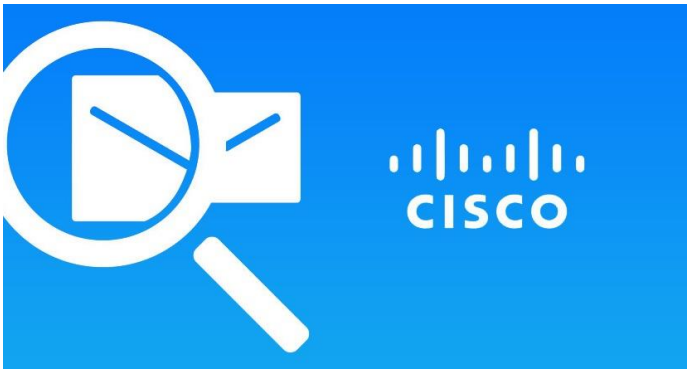


TP SECURISATION COUCHE 2

RESUME

Veuillez trouver ci-dessous mon TP sur l'analyse de risques réalisé grâce à Cisco Packet Tracer.

TEDE Sacha

Cisco Packet Tracer

Introduction

Aujourd'hui, nous allons réaliser un TP intitulé "Sécurisation de la couche 2" à l'aide de Cisco Packet Tracer. Ce logiciel permet de construire un réseau virtuel et de simuler le comportement des protocoles réseaux.

Objectif : Intercepter les paquets du PC client vers un serveur Web en utilisant une attaque de type "Man in the Middle" (MITM) via l'ARP Poisoning. Cette attaque consiste à ce qu'un attaquant intercepte les paquets de données du client envoyés au serveur en se faisant passer pour un participant légitime.

Cisco Packet Tracer est un logiciel de CISCO permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs.

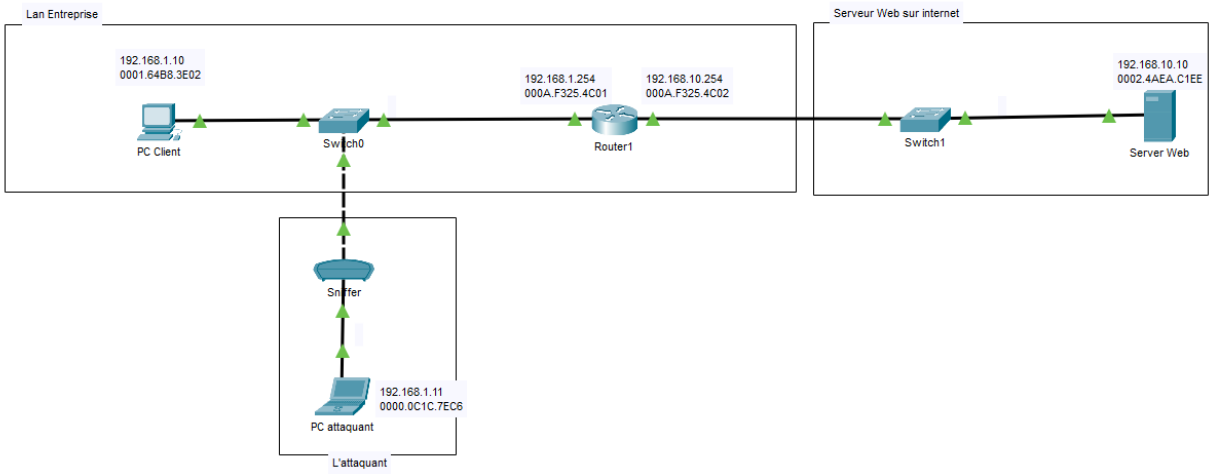
« MITM » est un type de cyberattaque où les attaquants interceptent une conversation ou un transfert de données existant, soit en écoutant, soit en se faisant passer pour un participant légitime. Pour la victime, il semblera qu'un échange standard d'informations est en cours, mais en s'insérant au « milieu » de la conversation ou du transfert de données, l'attaquant peut discrètement détourner des informations. »

Matériel utilisé :

- 2 switches
- 1 routeur
- 1 PC client
- 1 serveur Web
- 1 sniffeur (comme WireShark)
- 1 PC attaquant

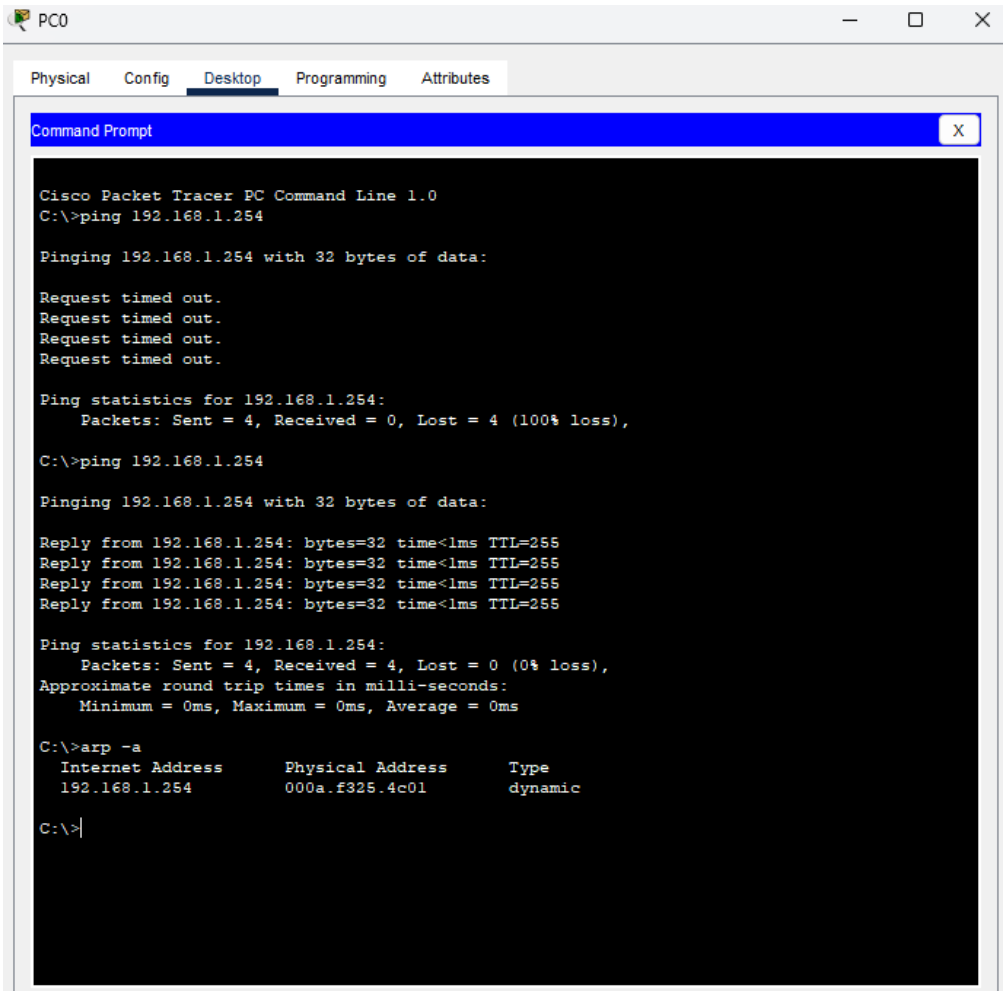
Étapes :

1. Configuration des équipements avec des adresses IP et des passerelles.
2. Test de connectivité via des pings et vérification des tables ARP.
3. Accès au serveur Web depuis le PC client.
4. Modification de l'adresse MAC du PC attaquant pour correspondre à celle du routeur.
5. Vérification de l'interception des paquets via le sniffeur



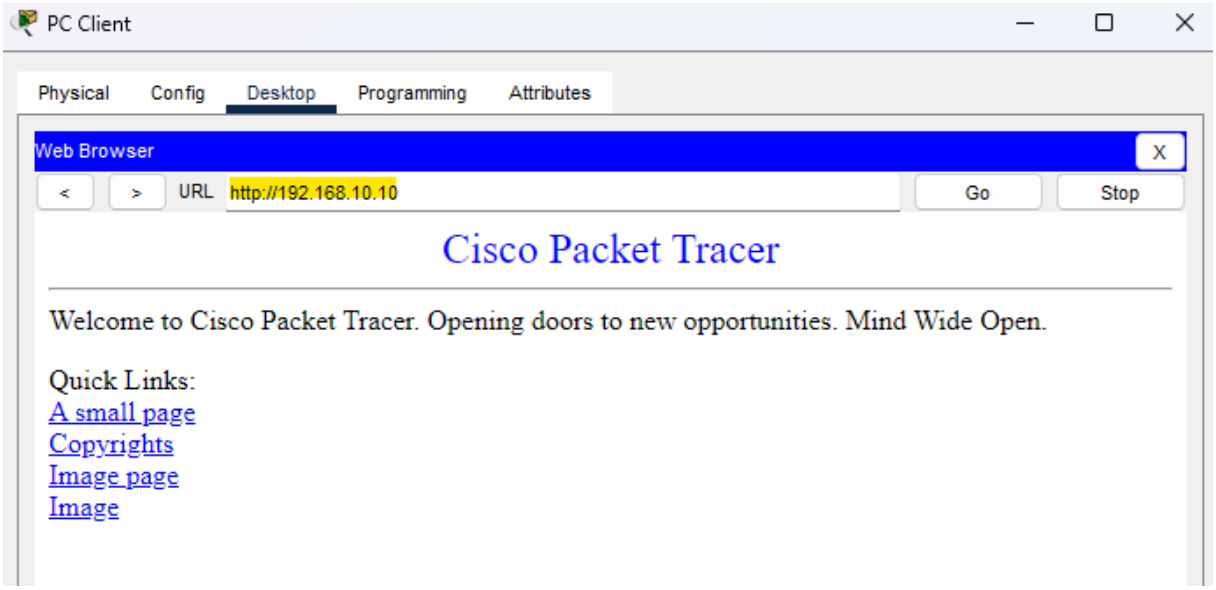
Par la suite, une fois qu'on a connecté nos équipements, on réalise un ping depuis notre Pc attaquant vers notre routeur pour voir si la connectivité est bonne.

Puis grâce à la commande « arp -a », nous pouvons voir la table ARP. Donc à voir les adresses MAC liés à leurs adresses IP.

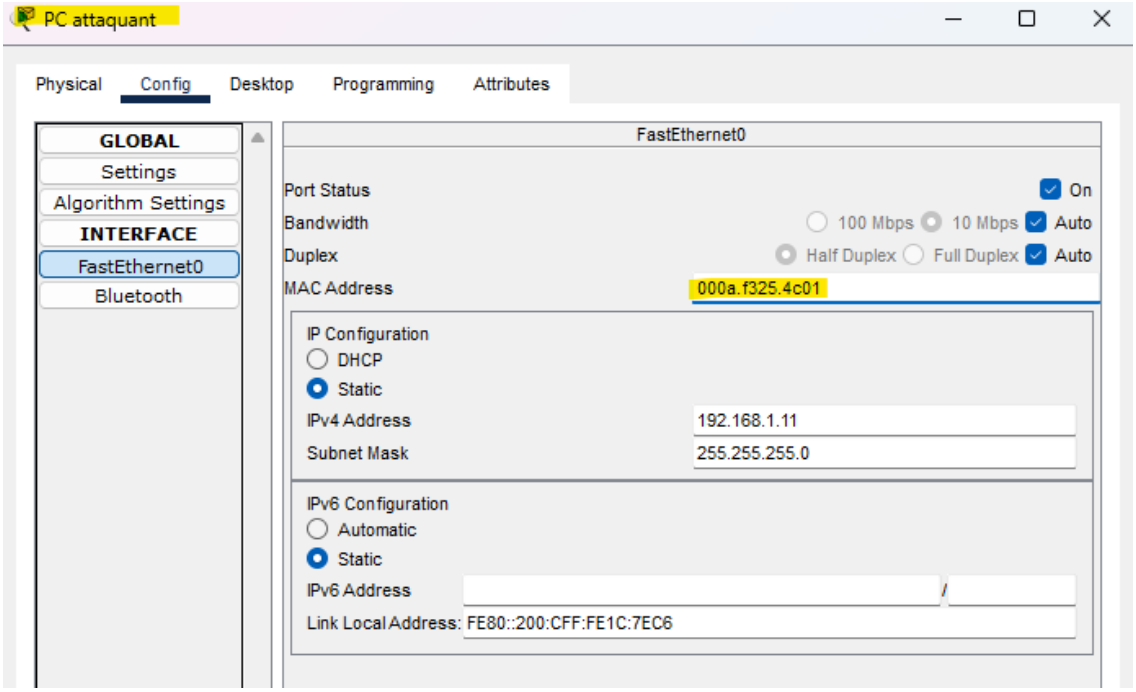


Ensuite, on rentre l'adresse IP de notre serveur Web sur notre PC client. On trouve grâce à l'URL, la page du site demandé.

Jusque-là tout va bien, nos paquets ne sont pas intercepter par le PC attaquant.



Pour continuer, nous changeons d'adresse MAC sur notre PC attaquant, prenant la même que celle du routeur afin que celle-ci s'intègre à la table ARP de notre PC Client.



Grâce à la commande « show mac ad », on peut voir la table ARP également sur le switch connecté à notre PC attaquant.

```
Switch>show mac ad
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0000.0c1c.7ec6    DYNAMIC     Fa1/1
   1    0001.64b8.3e02    DYNAMIC     Fa0/1
   1    000a.f325.4c01    DYNAMIC     Fa2/1
```

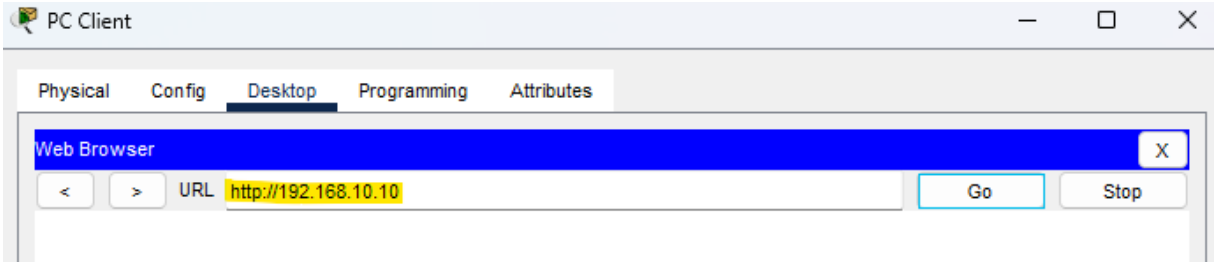
Après un « ipconfig /all », on peut donc voir que l'adresse MAC de 192.168.1.11 est la même que celle de notre routeur.

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.................: 000A.F325.4C01
   Link-local IPv6 Address.........: FE80::200:CFF:FE1C:7EC6
```

Donc le PC client a bien assimilé le PC attaquant qui a pour adresse IP 192.168.1.11. Preuve qu'il a bien fusionné avec l'adresse MAC du routeur.

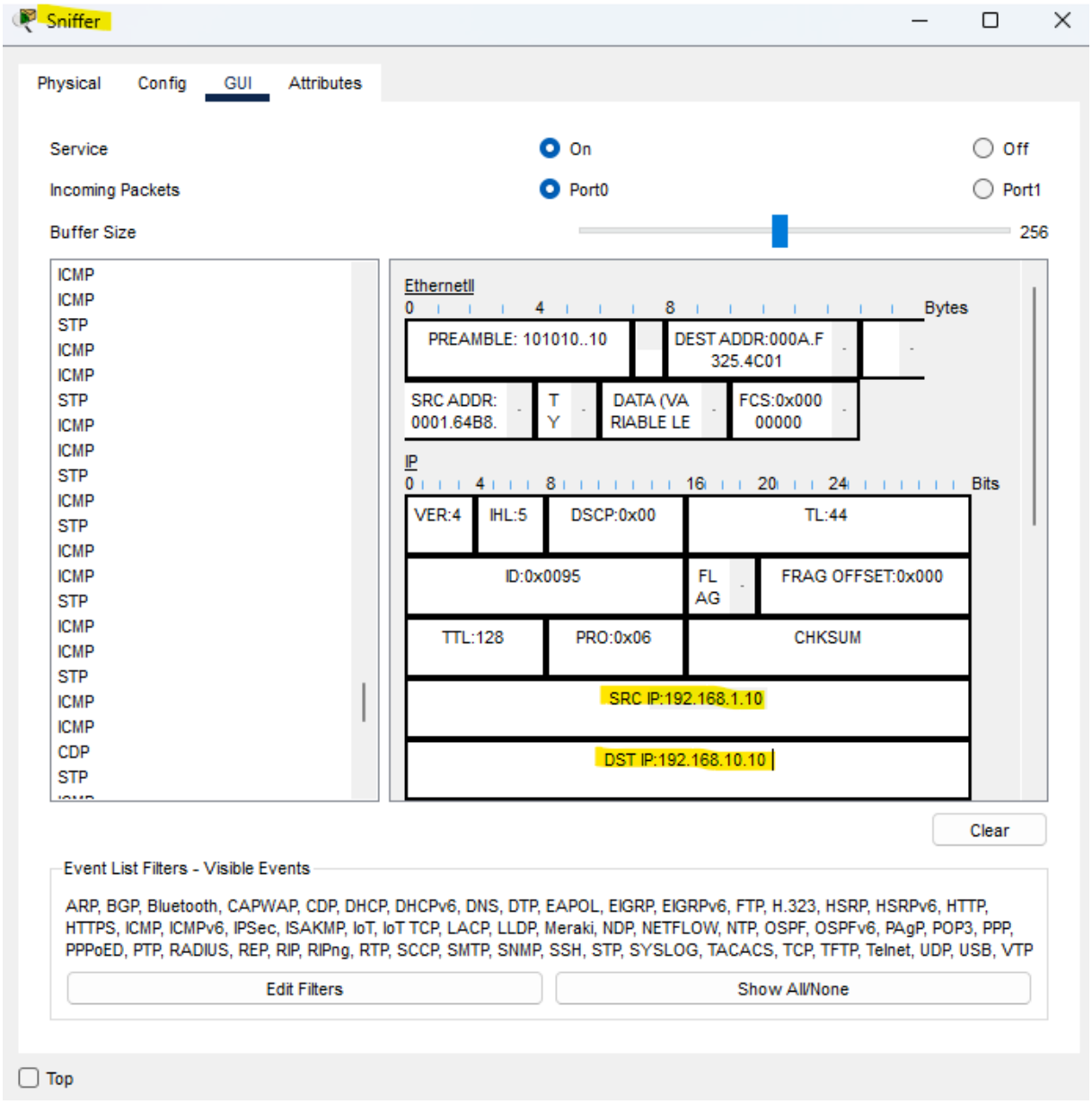
```
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.11          000a.f325.4c01        dynamic
  192.168.1.254         000a.f325.4c01        dynamic
```

Pour finir cette manipulation, l'attaque MITM est censé fonctionner si les paquets du client ne passent plus que par le routeur mais aussi par le PC attaquant, de ce fait l'accès au serveur Web ne devrait plus être disponible (voir screen ci-dessous)



Ainsi, pour confirmer que le MITM a bien été réaliser, nous devons nous rendre sur notre sniffeur, qui permet de tout surveiller, analyser, que ce soient les entrées ou les sorties.

Une fois rendu sur notre sniffeur, nous pouvons nous apercevoir que lorsque nous observons un Protocol TCP, alors en s'y rendant dessus, nous trouvons le paquet de données initialement envoyé au Serveur Web. Cela prouve que le Sniffeur a pu intercepter le paquet.



Conclusion

Ce TP sur la sécurisation de la couche 2 à l'aide de Cisco Packet Tracer nous a permis de mettre en pratique une attaque de type « Man in the Middle » en utilisant la technique de l'ARP Poisoning. Voici les points clés et les apprentissages de cette expérience :

1. Objectif atteint : Nous avons réussi à intercepter les paquets de données entre le PC client et le serveur Web, démontrant ainsi la faisabilité de l'attaque MITM dans un environnement simulé.
2. Configuration et connectivité : La configuration des adresses IP, des passerelles et la connectivité des équipements ont été réalisées avec succès, permettant une communication fluide entre les différents dispositifs du réseau.
3. Manipulation de la table ARP : En modifiant l'adresse MAC du PC attaquant pour qu'elle corresponde à celle du routeur, nous avons pu insérer le PC attaquant dans la table ARP du PC client, prouvant ainsi la vulnérabilité des réseaux à ce type d'attaque.
4. Interception des paquets : L'utilisation d'un sniffeur a permis de confirmer l'interception des paquets de données initialement destinés au serveur Web, validant ainsi l'efficacité de l'attaque MITM.
5. Apprentissages : Ce TP a mis en lumière l'importance de sécuriser les réseaux contre les attaques de type MITM. Il a également permis de renforcer nos compétences en configuration réseau, en diagnostic de connectivité et en analyse de trafic réseau.

En conclusion, cette expérience a souligné la nécessité de mettre en place des mesures de sécurité suffisamment importantes pour protéger les réseaux contre les attaques potentielles.

Ce TP m'a pris environ une heure pour réaliser un attaque MITM.