Mr JACQUEMIN

07/10/2024

Compte rendu TP

Sécurisation couche 2 et ARP Poisonning

TEWES Arnaud
BTS SIO SISR 1ERE ANNEE

1. Introduction

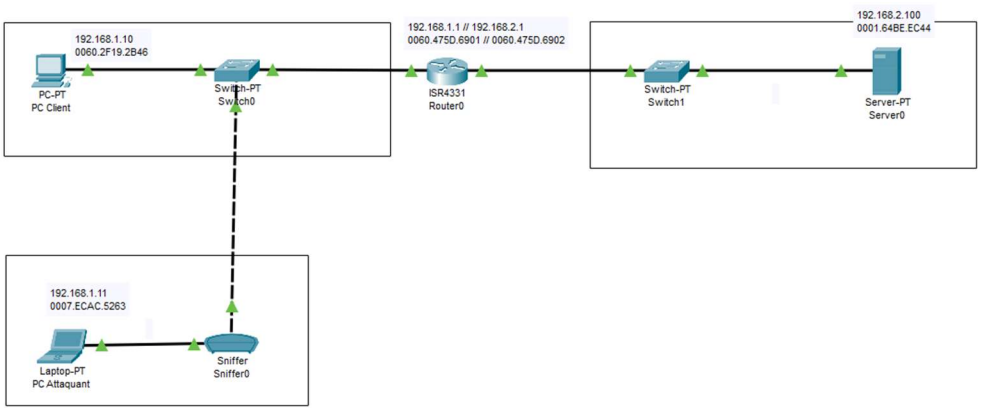
Dans ce TP, nous avons pris le rôle d'un attaquant lors d'une attaque MITM (Man in the Middle) en réalisant une attaque par ARP Poisoning.

Une attaque Man in the Middle consiste à se substituer à un routeur ou à un autre équipement sur un réseau en usurpant son adresse MAC. Cela permet à l'attaquant de se faire passer pour cet équipement et d'intercepter les requêtes qui lui sont normalement destinées. Il existe des logiciels, appelés "mac changers", qui permettent de réaliser cette usurpation dans un contexte réel. Grâce au switch et les mise à jour constante de sa table ARP (table qui lie les adresses MAC aux adresses IP), il est possible de se faire passé pour un équipements sur un réseau.

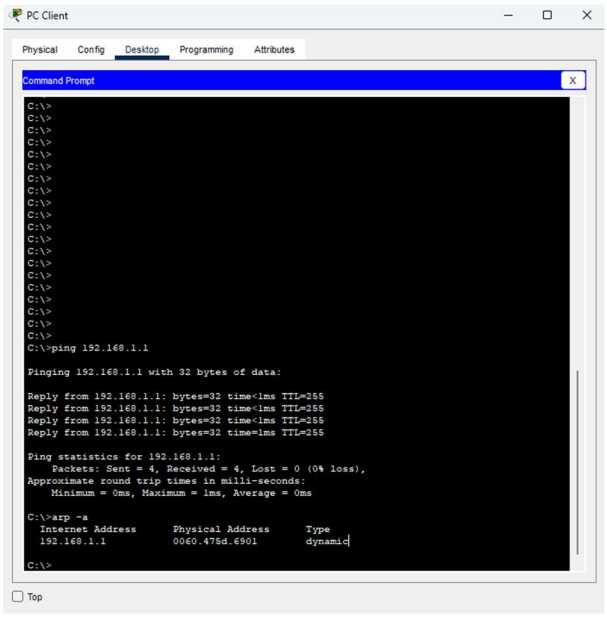
Dans ce TP, nous avons expérimenté cette attaque en utilisant le logiciel Cisco Packet Tracer

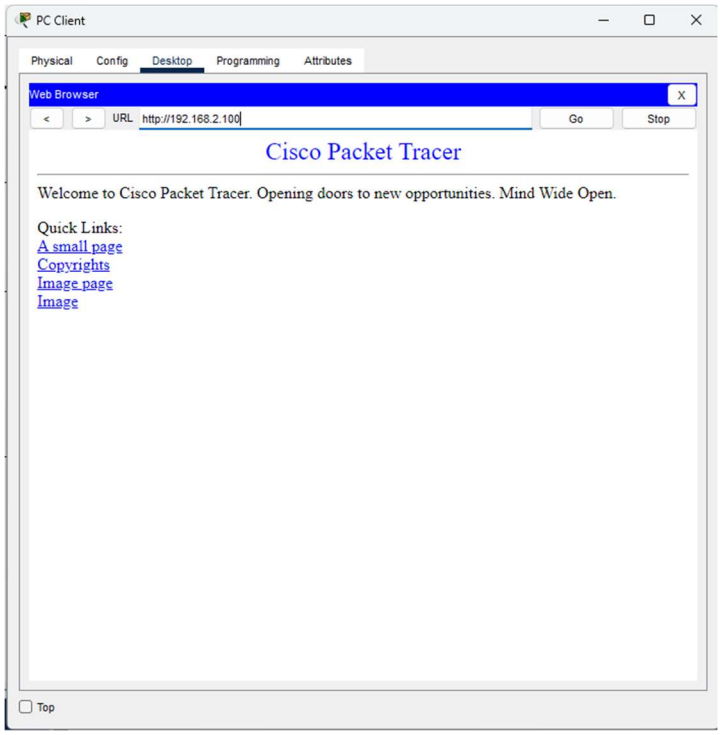
2. Procédé de l'attaque

Dans un premier temps, voici le réseau fictif qui sera la cible ce cette attaque.

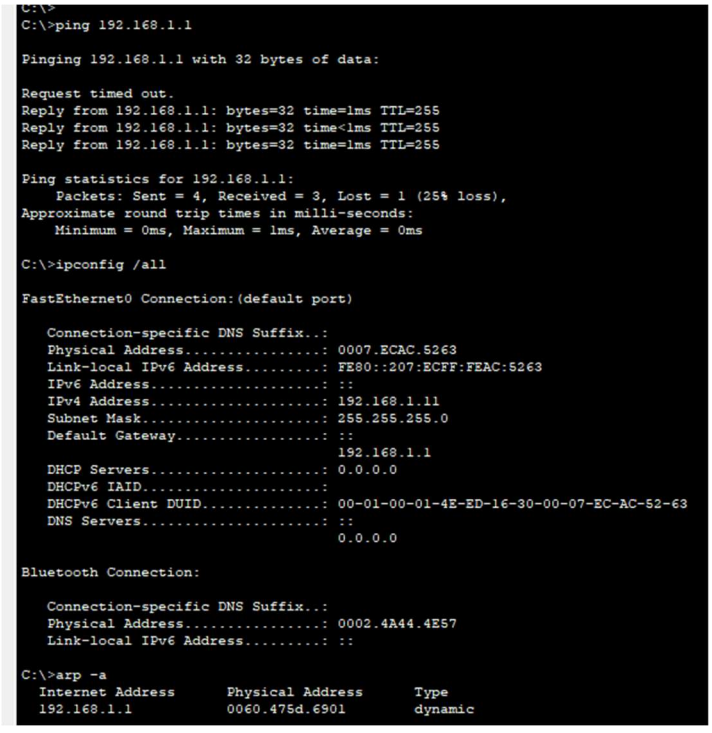


Ensuite, après avoir paramétré tout mes équipements, je vérifie que tout réponde bien et vérifie la table ARP de mon PC client et que j'accède bien à mon serveur WEB



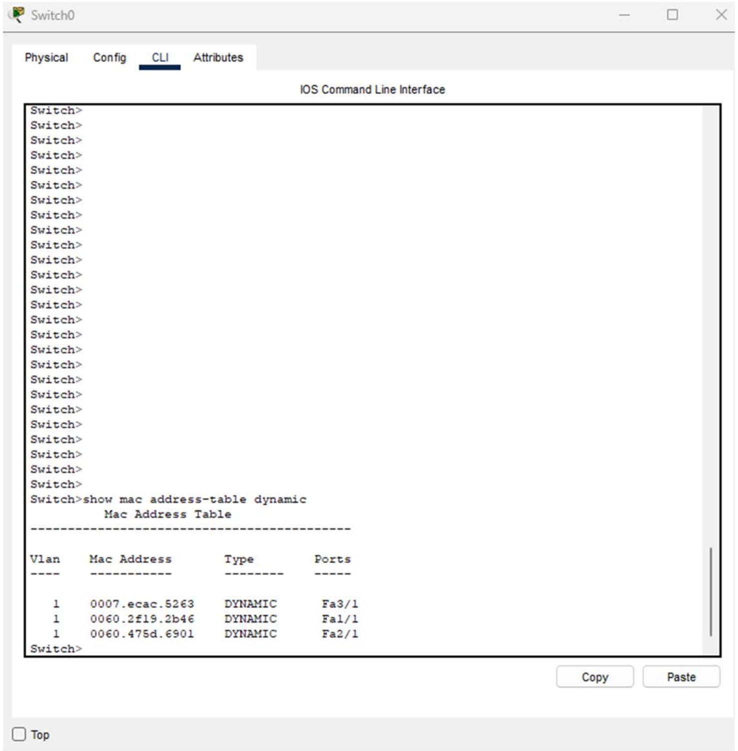


Cela fait, je vérifie l'adresse MAC et la table ARP du pc de l'attaquant avec la commande ipconfig /all

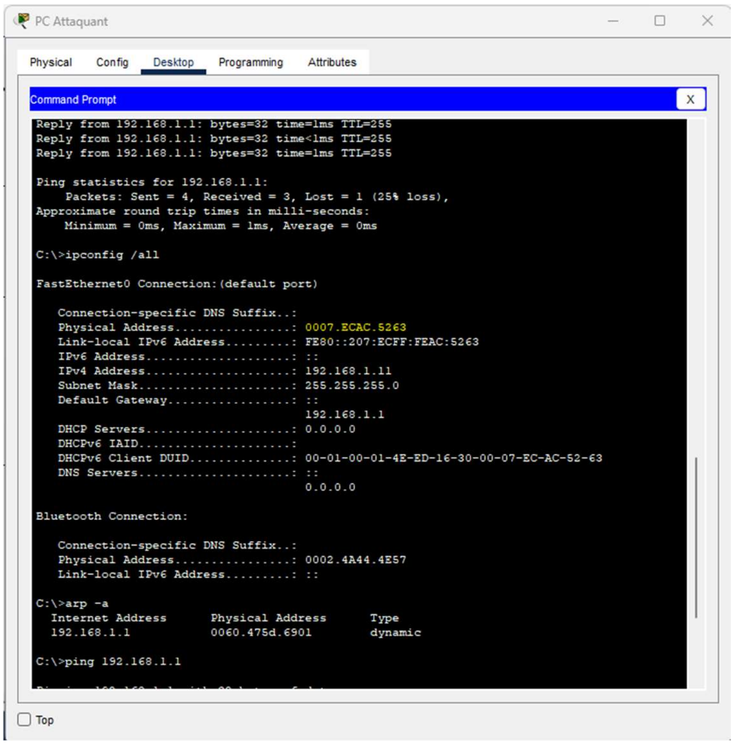


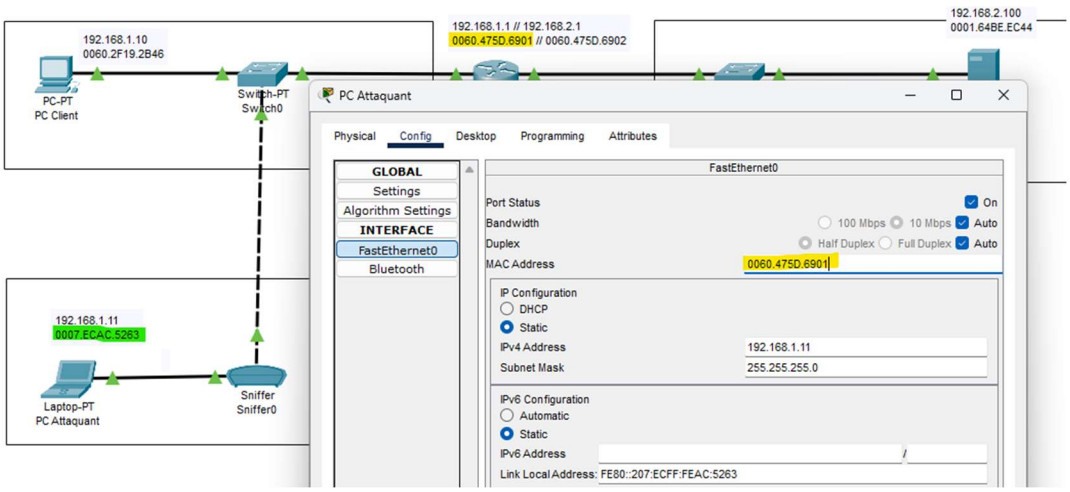
```
C:\>
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.................: 0007.ECAC.5263
   Link-local IPv6 Address.........: FE80::207:ECFF:FEAC:5263
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.11
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.1.1
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-4E-ED-16-30-00-07-EC-AC-52-63
   DNS Servers.....................: ::
                                     0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address.................: 0002.4A44.4E57
   Link-local IPv6 Address.........: ::

C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.1           0060.475d.6901        dynamic
```

Maintenant, je vérifie la table ARP de mon switch pour vérifier que toute mes machines sont bien assignées (pour l'instant, il n'y a eu aucune action malveillante)

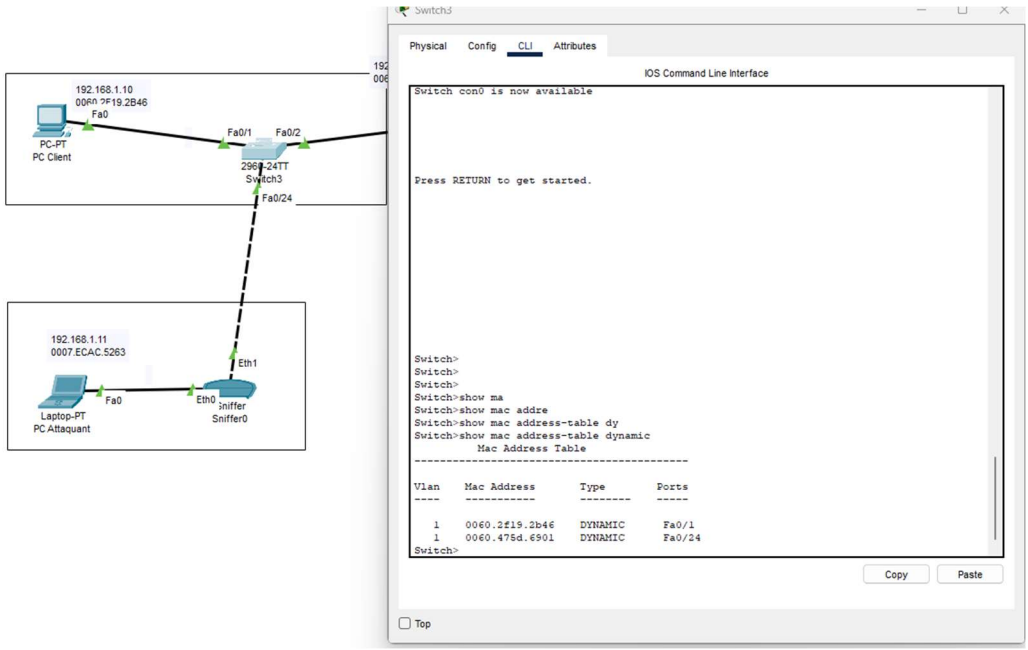


Il faut maintenant modifier l'adresse MAC du pc de l'attaquant (qui serait fait dans un cas réel avec un « mac changer ») étant sous Cisco Packet Tracer, je peux modifier directement dans les paramètres de la carte réseau



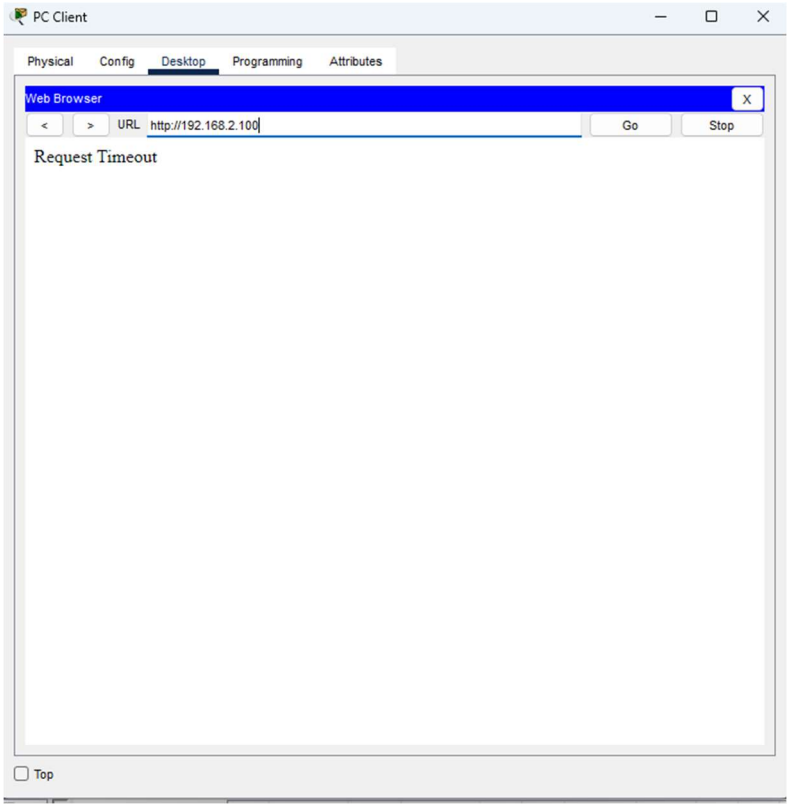


Le PC de mon attaquant a donc maintenant usurpé l'adresse MAC de mon routeur, si je fais un ping depuis le pc de mon attaquant vers le PC client, la table ARP du switch va donc se mettre à jour comme suit :

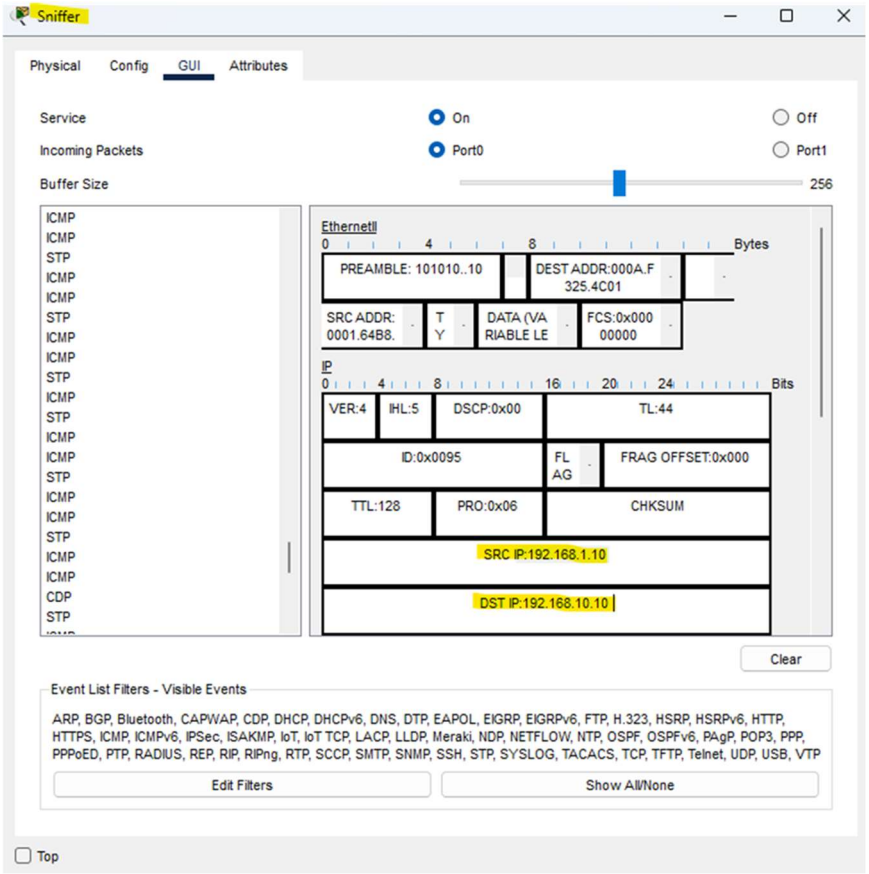


On voit bien que maintenant l'adresse MAC du routeur redirige bien vers le port du switch ou le PC de l'attaquant est connecté.

Je vais faire un test pour vérifier que je récupère bien via mon sniffer les paquets envoyés vers mon serveur WEB depuis mon pc client.



Le serveur WEB est maintenant inaccessible. Allons voir dans le sniffer si nous avons récupéré des informations sur ces paquets envoyés



Nous avons bien récupéré certains paquets TCP envoyé depuis mon PC client et qui devait normalement arriver vers mon serveur WEB grâce à l'usurpation d'adresse MAC de mon routeur.

3. Conclusion

Pour conclure, l'attaque de Man in the Middle est une attaque facile à réaliser mais également facilement contrôlable en respectant certaines règles simples de sécurité comme :

- Verrouiller les ports inutilisés sur notre switch
- Laisser nos machines en IP fixe sans DHCP sur le réseau (pas très pratique)
- Créer des VLANs pour segmenter le réseau
- Utiliser des switchs avec inspection ARP dynamique
- Former les utilisateurs

En se mettant à la place de l'attaquant, nous avons pu voir de l'intérieur comment se déroule une attaque de ce type. Cela nous permet de mieux comprendre les vulnérabilités de notre réseau et de mettre en place des mesures de sécurité efficaces pour le protéger. En appliquant ces bonnes pratiques, nous pouvons considérablement réduire les risques d'attaques et assurer une meilleure protection de nos données et de nos infrastructures.

De plus, il est crucial de maintenir une vigilance constante et de mettre à jour régulièrement nos systèmes et logiciels pour combler les failles de sécurité potentielles. La sensibilisation et la formation des utilisateurs jouent également un rôle clé dans la prévention des attaques. En comprenant les méthodes utilisées par les attaquants, les utilisateurs peuvent adopter des comportements plus sûrs, comme éviter de se connecter à des réseaux Wi-Fi publics non sécurisés ou vérifier l'authenticité des sites web avant de saisir des informations sensibles.