TP – Séance 9 – RS2P
Sécurité de couche 2 et Réseaux sans fil

Objectif général : le but de ce TP est de mettre en évidence certains problèmes de sécurité au niveau 2 (écoute de trafic tierce avec la technique de port mirroring et attaque par inondation de la table de commutation), de mettre en place des politiques de sécurité sur un commutateur, et de configurer un réseau sans fil.

Ressources requises (par trois ou quatre)

- 1 commutateur
- 3 ordinateurs fixes (sous Ubuntu)
- câbles pour configurer et pour relier les périphériques
- le simulateur Packet Tracer (utilisé individuellement)

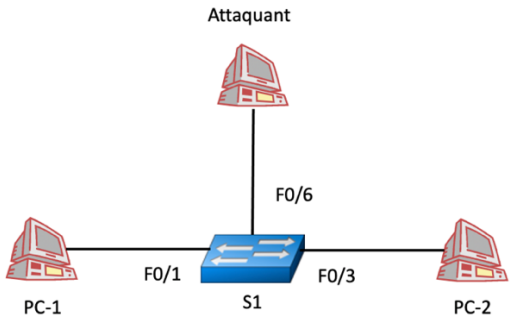
Si vous le souhaitez, vous pouvez essayer de travailler par binôme. Dans ce cas, l'attaquant sera un attaquant virtuel placé sur le PC2 et associé à la 2e interface réseau. Il faudra bien jouer le jeu et n'écouter que sur l'interface de l'attaquant.

1ère partie : Étude de quelques problèmes de sécurité de couche 2

Cette partie s'appuie sur les modules 10 et 11 -Concepts de sécurité du réseau local LAN & Configuration de la sécurité du commutateur- du CCNA SRWE.

Pourquoi la sécurité de la couche 2 (couche Liaison de données) est importante ?

Topologie considérée pour cette partie



Dans cette partie, vous utilisez des équipements réels.

Étape 1 : Connectez les équipements et configurez les interfaces IP des stations

selon le plan d'adressage suivant.

Station	IPv4
PC-1	192.168.10.1/24
PC-2	192.168.10.2/24

La 3e station est un attaquant qui se connecte, à votre insu, sur le commutateur du réseau local que vous administrez.

Étape 2 : L'attaquant écoute tout le trafic traversant le commutateur

Pour cela, il utilise la technique du *port mirroring*. Il s'agit de dupliquer le trafic qui passe par un port vers un autre port qui peut être relié à un outil d'analyse du trafic (par exemple la station de l'attaquant sur laquelle Wireshark fonctionne).

L'attaquant accède en mode console au commutateur S1 et met en place la technique de port mirroring du port f0/1 vers le port f0/6 avec les commandes suivantes :

```
S1(config)#monitor session 1 source interface fa0/1 both
S1(config)#monitor session 1 destination interface fa0/6
```

Faites la même chose pour récupérer le trafic passant par l'interface f0/3 de S1. Notez les commandes utilisées :

L'attaquant lance Wireshark sur l'interface sur laquelle il désire écouter le trafic.

Faites un **telnet** du PC-1 vers le PC-2 (qui sera le serveur telnet). Si le serveur telnet n'est pas installé, faites les commandes suivantes :

```
PC-2> apt-get update
PC-2> apt-get install telnetd
PC-2> systemctl start inetd
```

Ajouter un compte utilisateur sur PC-2 avec la commande **adduser**.

Étudier les trames reçues par l'attaquant suite au telnet effectué entre PC-1 et PC-2. Qu'observez-vous ?

Indiquer deux politiques de sécurité qui pourraient être mises en place pour éviter l'attaque ci-dessus.

Supprimer le port mirroring sur S1 avec la commande :

```
S1(config)#no monitor session 1
```

Étape 3 : L'attaquant inonde la table d'adresses MAC de S1

Nettoyez la table de commutation (table d'adresses MAC) de S1 avec la commande :

```
S1# clear mac address-table dynamic
```

Vérifier que la table est bien vide. Notez la commande utilisée :

Quelle est la taille de la table de commutation ? Vous utiliserez la commande :

```
S1(config)#show mac address-table count
```

L'attaquant utilise l'outil **macof** (https://manpages.ubuntu.com/manpages/trusty/man8/macof.8.html) pour envoyer à saturation des trames avec des adresses MAC aléatoires.

Installez la commande macof si ce n'est pas le cas :

```
PC> apt-get update
PC> apt-get install dsniff
```

Notez la commande utilisée pour que l'attaquant lance cette attaque SEULEMENT SUR L'INTERFACE CONNECTÉE AU PORT F0/6 :

L'attaquant vérifie que les trames sont bien transmises sur cette interface grâce à Wireshark.

Observez aussi l'évolution de la table de commutation de S1.

Au bout de quelque temps (durant lequel on espère que la table de commutation de S1 soit complètement remplie), faites un **telnet** du PC-1 vers le PC-2 (qui sera le serveur telnet). Pendant ce temps, l'attaquant continue à capturer les trames qui transitent sur son interface. Est-ce que l'attaquant peut observer des trames concernant l'échange entre PC-1 et PC-2 ?

En quoi cette attaque est différente de l'attaque précédente (hormis le fait que les commandes utilisées sont différentes) ?

2e partie : Mise en place de politiques de sécurité de niveau 2 sur un commutateur

Étape 4 : Rappelez les configurations qui doivent être réalisées sur le commutateur pour sécuriser l'accès au commutateur pour son administration

N'hésitez pas à faire ces configurations sur S1 et à noter ces commandes.

Étape 5 : Sécuriser les ports non utilisés sur S1

dont le port f0/6 afin qu'aucun attaquant ne puisse s'y connecter. Notez la commande utilisée :

Est-ce que l'attaquant peut faire un ping sur une des stations une fois le port f0/6 sécurisé ?

Étape 6 : Activez la sécurité des ports (actifs)

Dans quel mode doivent être les ports pour pouvoir activer la sécurité des ports ?

Entrez les commandes nécessaires pour activer la sécurité des ports actifs (sur f0/1 et f0/3) et observez les paramètres de sécurité de ports. Notez les commandes utilisées et ce que vous observez, par exemple pour le port f0/1. Est-ce qu'un périphérique est associé à ce port ? Quel est le nombre maximal d'adresses MAC possible ?

Est-il possible de changer le nombre maximal d'adresses MAC ? Quelle est la valeur maximale possible ?

Configurez le port f0/1 de telle sorte que seule l'adresse MAC de PC-1 puisse être connectée à ce port. Notez la commande utilisée :

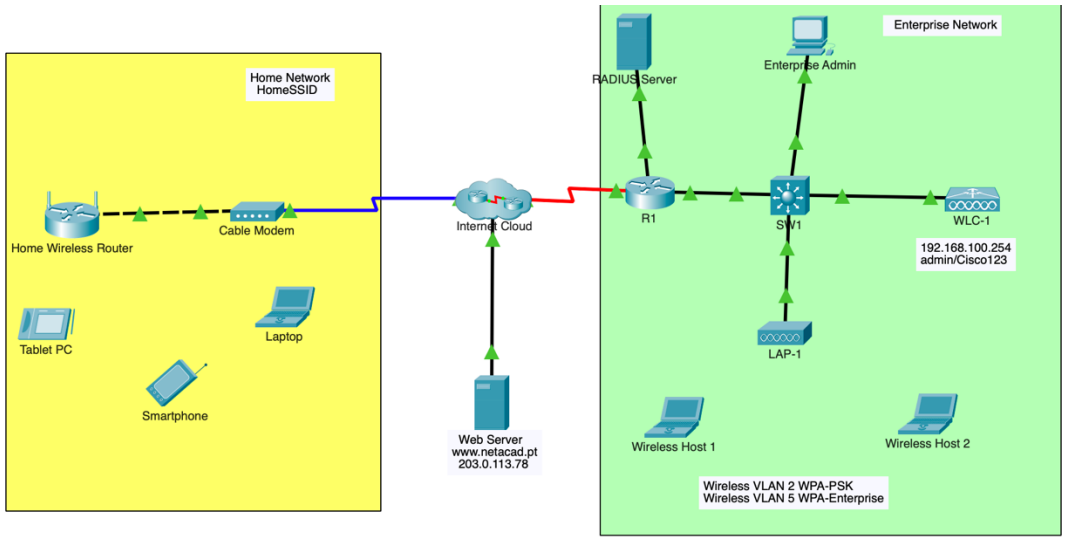
Étape 7 : Vérifiez que l'attaque par inondation de table MAC ne fonctionne pas

Pour cela, réactivez le port f0/6 et activez la sécurité de port sur ce port. Lancez l'attaque par inondation d'adresse MAC et observez la table de commutation de S1. Qu'observez-vous ?

3e partie : Configuration d'un réseau sans fil

Cette partie se base sur les modules 12 et 13 -Concepts WLAN et Configuration WLAN- du CCNA SRWE. L'objectif de cette partie est de configurer un réseau domestique sans fil.

Topologie considérée pour cette partie



Étape 8 : Récupérez le fichier Packet Tracer « Configuration de réseau sans fil »

Dans la section 10.5.1. Attention, le sujet proposé dans ce document est différent de celui proposé avec ce fichier Packet Tracer. On ne s'intéressera qu'au réseau domestique (partie gauche de la figure).

Étape 9 : Configurez le routeur sans fil dans le réseau domestique

En général, que fournit un routeur sans fil ? Quelle est la technologie de communication sans fil utilisée par ce routeur sans fil ?

Configurez les interfaces du routeur (via l'interface graphique GUI) selon le plan d'adressage suivant :

Interface routeur	IPv4
Internet	DHCP
Réseau local sans fil	192.168.6.1/27

Quelle est l'adresse IP obtenue par son interface connectée à l'Internet ?

Configurez un serveur DHCP sur le routeur de telle sorte que 20 appareils sans fil puissent obtenir une adresse IPv4 et que la première adresse possible soit 192.168.6.3.

Toujours sur le routeur, indiquez l'adresse IP d'un serveur DNS. L'adresse 10.100.100.252 sera attribuée.

Étape 10 : Configurez les paramètres de la partie sans fil sur le routeur domestique

Combien de bandes de fréquences sont possibles ?

Le routeur utilisera la bande de fréquences des 2,4 GHz. Indiquez le SSID qui aura comme nom **SSID domestique**. Et configurez le routeur pour qu'il opère sur le canal 6.

Combien de canaux sont disponibles dans la bande des 2,4 GHz ? Quelles sont les largeurs de bande possibles ?

Faites en sorte que le SSID soit diffusé sur le médium sans fil.

Étape 11 : Configurez la sécurité sur le routeur

de telle sorte que le protocole de sécurité WP2 Personal soit utilisé. Vous choisirrez une clé de chiffrement (passphrase).

Étape 12 : Connectez les clients sans fil au réseau sans fil

Cliquez sur l'ordinateur portable, puis cliquez sur Desktop et icône PC Wireless. Est-ce que cet ordinateur voit bien le réseau sans fil avec le SSID 'SSID Domestique' ? Si oui, connectez l'ordinateur à ce réseau sans fil. Qu'est-ce qui vous est demandé ?

Vérifiez les informations obtenues par l'ordinateur (adresse IP, adresse de la passerelle par défaut, adresse d'un serveur DNS). Est-ce que cela vous semble cohérent ?

Quelle est la capacité d'émission de ce lien sans fil ?

Cliquez sur la tablette (ou sur le smartphone), puis sur Config et choisissez Wireless0. Entrez le SSID, choisissez l'authentification WPA2-PSK et entrez la clé. Est-ce que la connexion s'effectue ? Quelle est l'adresse IP obtenue ?

Vérifiez la connectivité entre les équipements sans fil. Est-ce que ces équipements peuvent pinger le serveur Web ?