Sécurisation du DHCP

Exercice 1 – DHCP snooping

Configuration du serveur DHCP

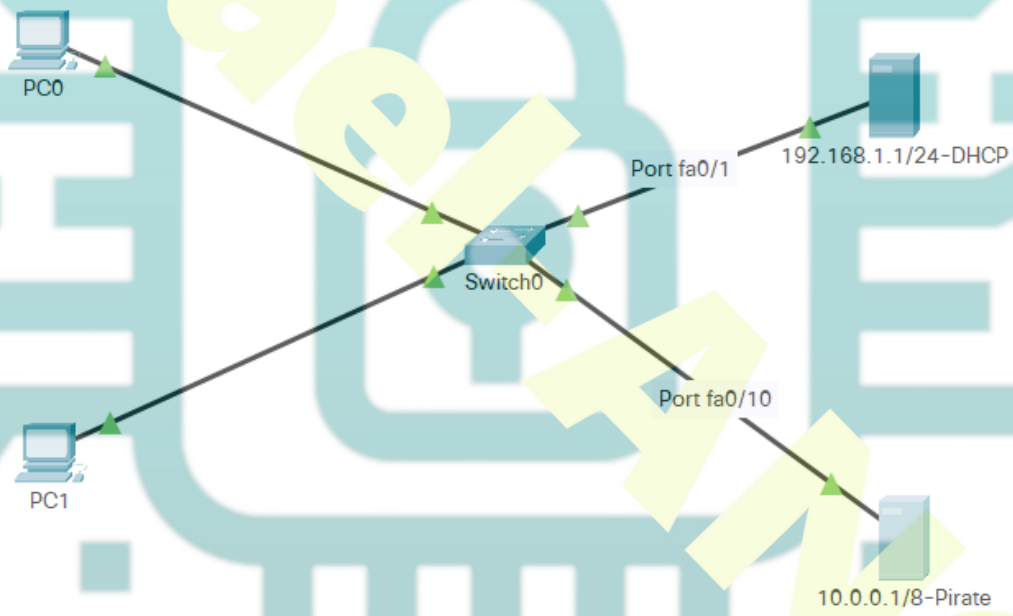
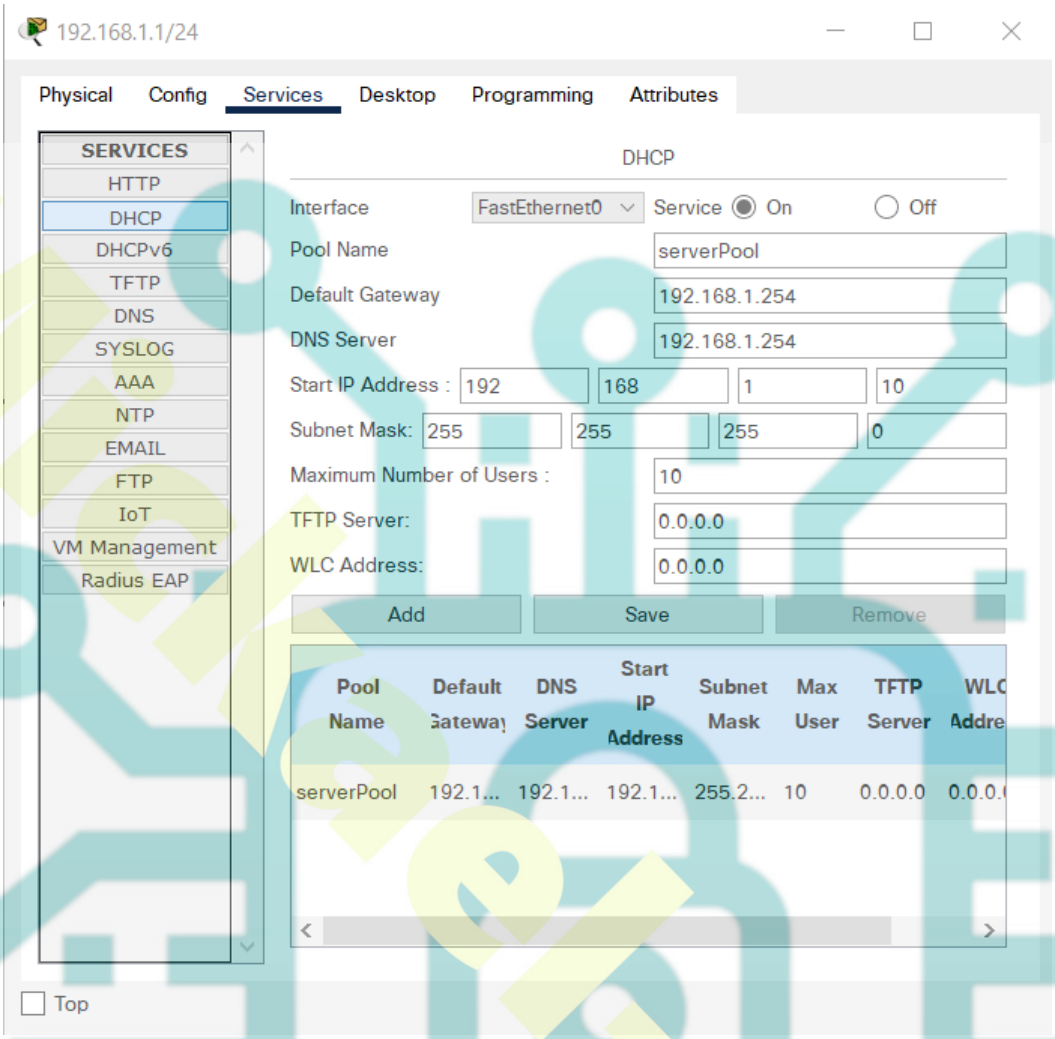


Schéma du TD

Configurer le serveur DHCP 192.168.1.1 comme suit :



Configuration du serveur DHCP

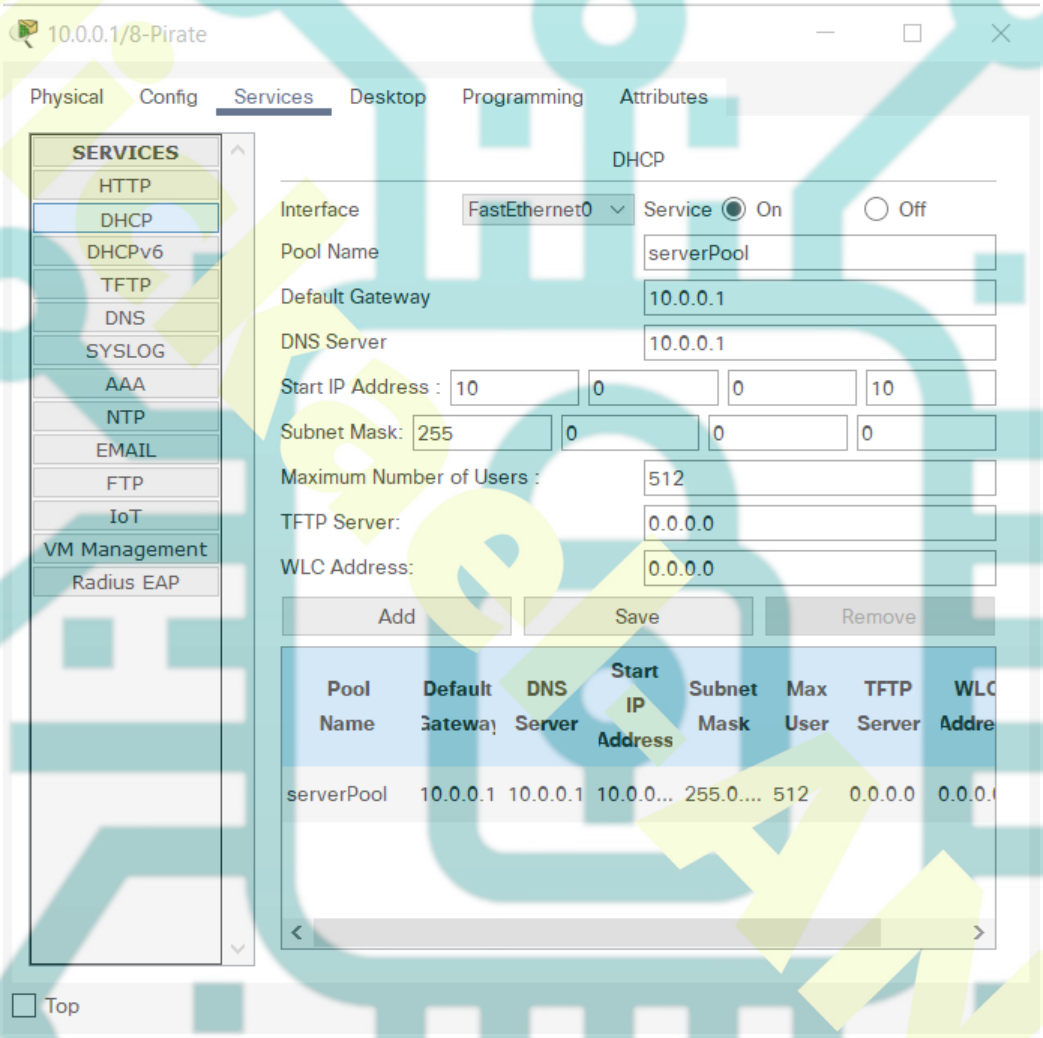
Configuration du switch

```
en
conf t
!activation du snooping sur le switch
ip dhcp snooping
!activation du snooping pour le vlan 1
ip dhcp snooping vlan 1
!Désactivation du champ option-82 (agent relay), si les clients car le DHCP et le serveur DHCP résident sur le même réseau IP.
no ip dhcp snooping information option
!activation du snooping sur l'interface du serveur
interface fastEthernet 0/1
ip dhcp snooping trust
```

Activation du DHCP sur le client PC0

Le clients doit récupérer une adresse fourni par le serveur

Installation d'un DHCP pirate



Puis désactiver le DHCP du serveur DHCP 192.168.1.1

Ensuite activer le client PC1, il ne doit pas récupérer d'adresse IP du serveur 10.0.0.1. La protection est active.

Vérifier par la commande **show ip dhcp snooping**

Exercice 2 – ARP inspection

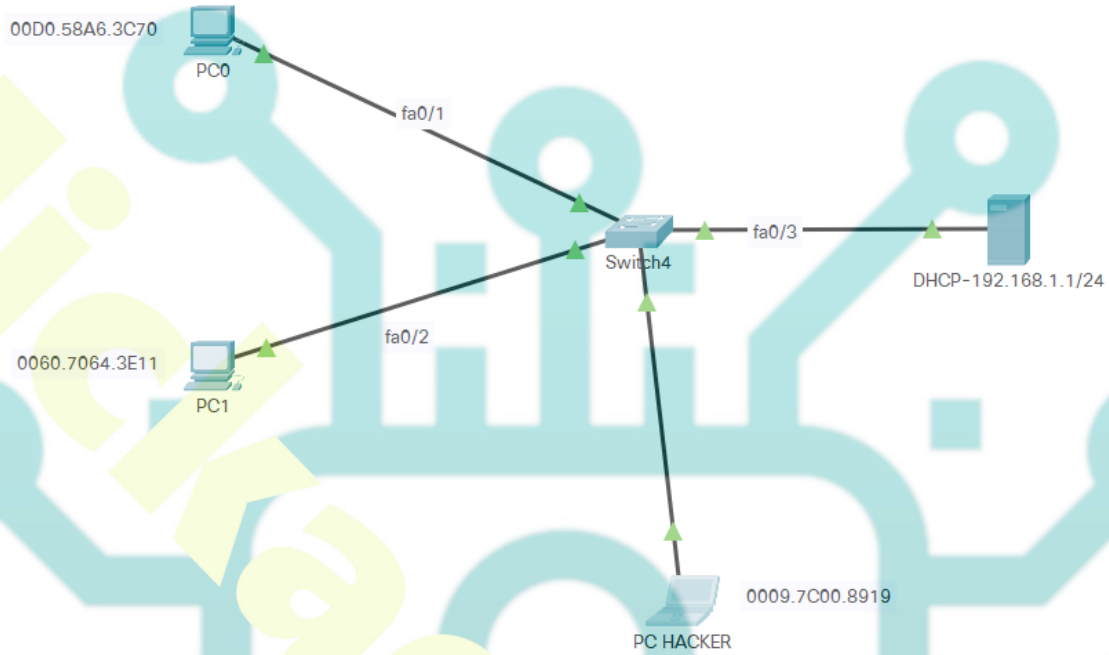
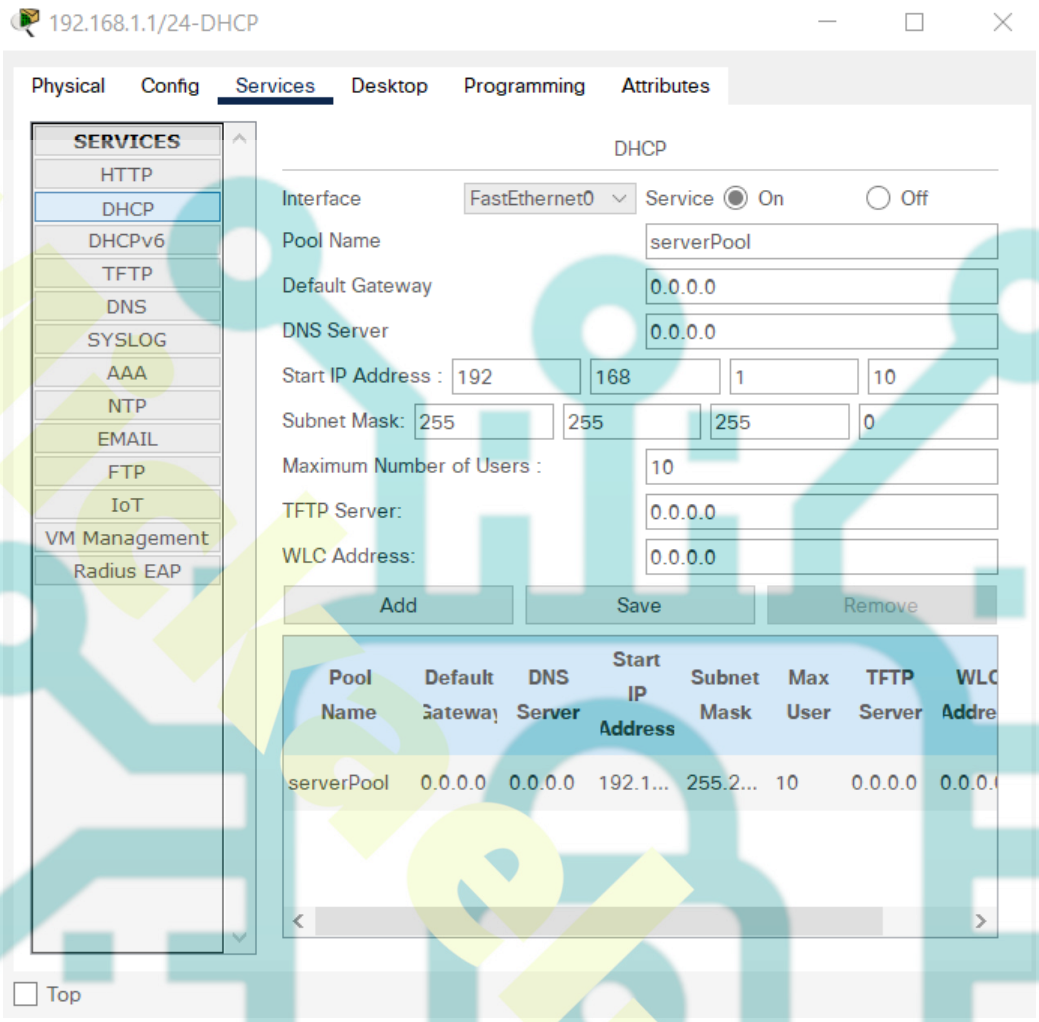


Schéma du TD

Configuration du DHCP sur le serveur



Serveur DHCP 192.168.1.1

Activation du snooping sur le switch

!activation du snooping sur le switch
ip dhcp snooping
!activation du snooping pour le vlan 1
ip dhcp snooping vlan 1
!Désactivation du champ option-82 (agent relay), si les clients car le DHCP et le serveur DHCP résident sur le même réseau IP.
no ip dhcp snooping information option
!activation du snooping sur l'interface du serveur
interface fastEthernet 0/3
ip dhcp snooping trust

- Mettre les clients en dhcp

- Puis saisir la commande **show ip dhcp snooping binding**

```
00:D0:58:A6:3C:70 192.168.1.11 86400 dhcp-snooping 1 FastEthernet0/1
00:60:70:64:3E:11 192.168.1.10 86400 dhcp-snooping 1 FastEthernet0/2
```

On voit bien notre entrée, qui contient **les adresses mac** et **les adresses IP** des hôtes client DHCP

Connexion du hacker

- Configurer le PC hacker en prenant une adresse donnée par le DHCP 192.168.1.10 dans mon exemple
- Connecter ensuite le PC du hacker sur le port 6 du switch
- Faire un ping vers le poste 192.168.1.11, cela fonctionne et c'est une faille.
- Faire également un arp -a sur le 192.168.1.11

```
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.10          0009.7c00.8919        dynamic
```

C'est l'adresse MAC du hacker qui apparait.

Nous sommes maintenant prêts à configurer **l'inspection dynamique de l'ARP** sur le switch.

```
!Activation dynamic ARP inspection sur le vlan.
ip arp inspection vlan 1
!activation du ARP trust sur l'interface du serveur
interface fastEthernet 0/3
ip arp inspection trust
```

Vider le cache ARP du serveur et de la machine 192.168.1.11 (**arp -d**)

A partir du PC du hacker, faire un ping vers le poste 192.168.1.11 cela ne fonctionne plus.

Vérifier via la commande

```
sh ip arp inspection
```