



## Hacking : méthodes et pratiques

---

# **Etude, analyse et mise en œuvre des attaques sur les Switch.**

---

*Auteur :*  
EL HADDAD MOUAD

SR2I-203

janvier 2022



## Table des matières

<b>1 Les risques des attaques sur les switches</b>	<b>5</b>
<b>2 GNS3, un outil de simulation</b>	<b>5</b>
<b>3 Première topologie et première attaque sur GNS3</b>	<b>6</b>
3.1 Première topologie : . . . . .	6
3.2 Première attaque : MAC Flooding . . . . .	6
3.2.1 Avant l'attaque . . . . .	8
3.2.2 Après l'attaque . . . . .	9
3.3 Technique de prévention . . . . .	10
<b>4 Deuxième attaque : Arp Spoofing</b>	<b>11</b>
4.1 Mise en oeuvre de l'attaque . . . . .	13
4.2 Technique de prévention . . . . .	15
<b>5 Troisième attaque : DHCP spoofing</b>	<b>16</b>
5.1 Mise en oeuvre de l'attaque : . . . . .	17
5.1.1 Une deuxième topologie : . . . . .	17
5.1.2 Avant l'attaque . . . . .	17
5.1.3 Après l'attaque . . . . .	18
5.2 Technique de prévention . . . . .	20
<b>6 Quatrième attaque : STP Manipulation Attack</b>	<b>20</b>
6.1 Mise en oeuvre de l'attaque : . . . . .	22
6.2 Technique de prévention : . . . . .	24
6.2.1 Protection de la couche 2 avec Root Guard . . . . .	24
6.2.2 Protection de la couche 2 avec BPDU Guard . . . . .	24
<b>7 Cinquième attaque : Vlan hopping</b>	<b>25</b>
7.1 Switched Spoofing . . . . .	26
7.2 Double Tagging . . . . .	26
7.3 Technique de prévention . . . . .	29
7.4 Empêcher le Trunking . . . . .	29
7.5 Prévention de l'utilisation du DTP . . . . .	30
7.6 Empêcher le double tagging . . . . .	30
<b>8 Conclusion</b>	<b>30</b>

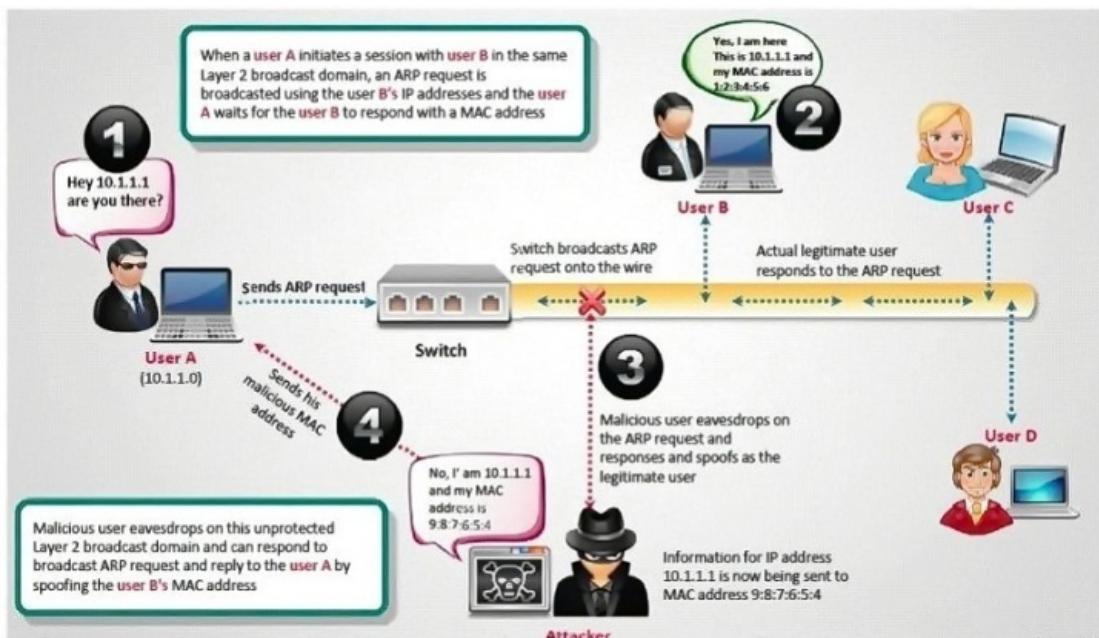
## Table des figures

1	La première topologie sur GNS3 . . . . .	6
2	La table des adresses Mac du switch . . . . .	8
3	Capture des trames avec wireshark avant l'attaque . . . . .	9
4	Capture des trames avec wireshark après l'attaque . . . . .	9
5	Visualisation du cache Arp avant l'attaque . . . . .	13
6	Ettercap scan . . . . .	14
7	Visualisation du cache Arp apres l'attaque . . . . .	14
8	Le résultat de l'attaque . . . . .	15
9	Une deuxieme topologie . . . . .	17
10	Une deuxième topologie . . . . .	18
11	DHCP spoofing avec ettercap . . . . .	18
12	Fake ACK envoyé . . . . .	19
13	Machine windows victime du DHCP spoofing . . . . .	19
14	Une Troisieme topologie . . . . .	22
15	Acces au root bridge à l'aide de yersinia . . . . .	23
16	Root bridge changé . . . . .	23
17	Quatrieme topologie : . . . . .	27
18	Passage en mode trunk à l'aide de yersinia . . . . .	27
19	Trunk port sur le switch . . . . .	28
20	Détection du VLAN du serveur ftp . . . . .	28
21	Ping vers le serveur ftp . . . . .	28
22	Détection du trafic FTP avec wireshark . . . . .	29
23	Intrusion du serveur ftp . . . . .	29

# Introduction

Les commutateurs LAN et Ethernet sont généralement considérés comme de la plomberie. Ils sont faciles à installer et à configurer, mais il est facile d'oublier la sécurité lorsque les choses semblent simples. De multiples vulnérabilités existent dans les commutateurs Ethernet. Des outils d'attaque pour les exploiter ont commencé à apparaître il y a quelques années (par exemple, le paquetage bien connu dsniff). En utilisant ces outils d'attaque, un attaquant peut vaincre le mythe de la sécurité des commutateurs, qui affirme faussement que le reniflage et l'interception de paquets sont impossibles avec un commutateur. En effet, avec dsniff, Cain et d'autres outils conviviaux sur un système Microsoft Windows ou Linux, un attaquant peut facilement détourner n'importe quel trafic vers son propre PC afin de briser la confidentialité ou l'intégrité de ce trafic. La plupart des vulnérabilités sont inhérentes aux protocoles de la couche 2, allant du protocole Spanning Tree à la découverte des voisins IPv6. Si la couche 2 est compromise, il est plus facile d'élaborer des attaques sur les protocoles des couches supérieures en utilisant des techniques telles que les attaques de type "man-in-the-middle" (MITM). Comme un pirate peut intercepter n'importe quel trafic, il peut s'immiscer dans les communications en clair (comme HTTP ou Telnet) et dans les canaux chiffrés (comme Secure Socket Layer [SSL] ou secure shell [SSH]). Pour exploiter les vulnérabilités de la couche 2, un attaquant doit généralement être adjacent à la couche 2 de la cible. Bien qu'il semble impossible pour un pirate externe de se connecter au réseau local d'une entreprise, ce n'est pas le cas. En effet, un pirate peut utiliser l'ingénierie sociale pour accéder aux locaux, ou se faire passer pour un ingénieur appelé sur place pour régler un problème mécanique. En outre, de nombreuses attaques sont menées par un initié, par exemple un employé sur site. Traditionnellement, il existe une règle non écrite et, dans certains cas, écrite, selon laquelle les employés sont des entités de confiance. Cependant, au cours de la dernière décennie, de nombreux cas et statistiques prouvent que cette hypothèse est fausse. L'enquête CSI/FBI 2006 sur la criminalité et la sécurité informatiques<sup>1</sup> a révélé que 68 % des pertes subies par les organisations interrogées étaient partiellement ou totalement dues à un mauvais comportement des employés. Une fois à l'intérieur des locaux physiques de la plupart des organisations, il est relativement facile de trouver une prise Ethernet ouverte sur le mur ou un périphérique en réseau (par exemple, une imprimante réseau) qui peut être déconnecté pour obtenir un accès réseau non autorisé. Avec le DHCP aussi largement déployé qu'il l'est et le faible pourcentage de ports LAN nécessitant une authentification (par exemple, IEEE 802.1X), le PC d'un utilisateur obtient une adresse IP et, dans la

plupart des cas, dispose du même niveau d'accès au réseau que tous les autres utilisateurs autorisés valides. Ayant obtenu une adresse IP de réseau, l'utilisateur mécréant peut maintenant tenter diverses attaques. Avec cette nouvelle vision de la confiance accordée à un utilisateur de réseau, l'exposition aux informations sensibles et confidentielles qui traversent les réseaux est une réalité qui ne peut être négligée. La plupart des organisations, sinon toutes, ont intégré une sécurité d'accès dans leurs applications et dans de nombreux dépôts de documents.



# 1 Les risques des attaques sur les switches

Les menaces et attaques passant par le réseau sont généralement de deux types :

- Menaces passives : activités comme le Wiretapping (écoute en ligne) et l'idle scan (méthode de balayage des ports TCP), conçues pour intercepter le trafic passant par le réseau.
- Menaces actives : activités telles que les attaques par déni de service (Dos, Denial of Service) et les injections SQL, où l'auteur tente d'exécuter des commandes afin de perturber le fonctionnement normal du réseau.

Les deux types de menaces représentent un très grand risque au niveau des piliers de la sécurité à savoir le « CID ». D'un coté, les attaques passives touchent à la confidentialité des informations qui circulent dans un réseau. D'autre part les attaques actives menacent les deux autres piliers, que sont l'intégrité, comme c'est le cas des attaques MITN par exemple, et la disponibilité qui concerne les attaques Dos ou DDos. Les switches ne font pas exception de ces attaques puisque chaque année des dizaines de CVE sont découvertes comme « CVE-2013-0570 » et « CVE-1999-0667 » par exemple. Cependant, la majorité des attaques sont dues aux mauvaises pratiques des ingénieurs réseau et de leur mauvaise configuration. Ainsi, dans la suite de notre projet, nous allons exploiter des failles de sécurité et effectuer des attaques aussi bien qu'introduire des bonnes pratiques et des méthodes de prévention efficaces.

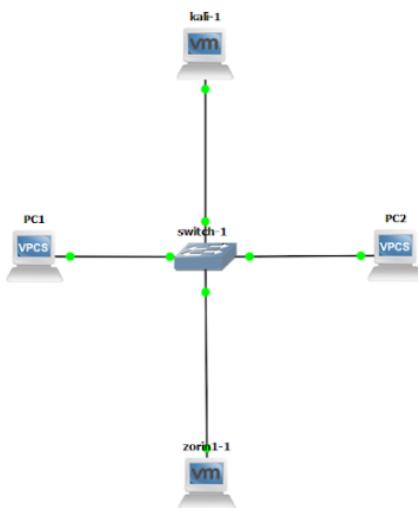
# 2 GNS3, un outil de simulation

GNS3 est utilisé par des centaines de milliers d'ingénieurs réseau dans le monde pour émuler, configurer, tester et dépanner des réseaux virtuels et réels. GNS3 nous permet d'exécuter une petite topologie composée de quelques dispositifs seulement sur votre ordinateur portable, jusqu'à celles qui comportent de nombreux dispositifs hébergés sur plusieurs serveurs ou même hébergés dans le nuage. Ainsi, pour notre projet nous allons utiliser GNS3-all-in-one software (GUI) et GNS3 Virtual machine (VM) pour avoir une CLI du switch afin de visualiser et d'analyser les différentes sorties du switch. En outre, nous allons aussi lier une machine virtuel Kali linux qui servira d'un agent malicieux qui va exercer plusieurs attaques sur nos différentes topologies.

### 3 Première topologie et première attaque sur GNS3

#### 3.1 Première topologie :

Une topologie qui contient 4 PC (2 vPC et 2 machines virtuelles afin d'économiser l'utilisation des ressources en termes de processeur et ram) interconnectés par un switch qui va subir la première attaque malveillante.



**FIGURE 1 –** La première topologie sur GNS3

#### 3.2 Première attaque : *MAC Flooding*

Le MAC Flooding est une méthode d'attaque visant à compromettre la sécurité des commutateurs de réseau. Habituellement, les commutateurs maintiennent une structure de table appelée MAC Table. Celle-ci est constituée des adresses MAC individuelles des ordinateurs hôtes du réseau qui sont connectés aux ports du commutateur. Cette table permet aux commutateurs de diriger les données hors des ports où se trouve le destinataire. Comme nous l'avons déjà vu, les concentrateurs diffusent les données sur l'ensemble du réseau, ce qui permet aux données d'atteindre tous les hôtes du réseau, tandis que les commutateurs envoient les données à la ou aux machines spécifiques auxquelles elles sont destinées. Cet objectif est atteint par l'utilisation de tables MAC. Le but du MAC

Flooding est de détruire cette table MAC.

Dans une attaque typique de MAC Flooding, l'attaquant envoie des trames Ethernet en grand nombre. Lorsqu'il envoie de nombreuses trames Ethernet au commutateur, ces trames auront différentes adresses d'expéditeur. L'intention de l'attaquant est de consommer la mémoire du commutateur qui est utilisée pour stocker la table des adresses MAC. Les adresses MAC des utilisateurs légitimes seront éliminées de la table MAC. Maintenant, le commutateur ne peut pas délivrer les données entrantes au système de destination. Ainsi, un nombre considérable de trames entrantes seront inondées sur tous les ports.

La table des adresses MAC est pleine et ne peut pas enregistrer de nouvelles adresses MAC. Cela conduira le commutateur à entrer dans un mode ouvert en cas de panne et le commutateur se comportera alors comme un hub de réseau. Il transmettra les données entrantes à tous les ports comme une diffusion. Voyons maintenant quels sont les avantages de l'attaquant avec l'attaque MAC Flooding.

Comme l'attaquant fait partie du réseau, il recevra également les paquets de données destinés à la machine victime. Ainsi, l'attaquant sera en mesure de voler des données sensibles à partir de la communication de la victime et d'autres ordinateurs. Un analyseur de paquets est généralement utilisé pour capturer ces données sensibles.

A la suite d'une attaque MAC Flood, l'attaquant pourrait poursuivre avec une attaque ARP spoofing. Cela lui permettra de conserver l'accès aux données privilégiées même après que les commutateurs attaqués se soient remis de l'attaque MAC Flood.

Vous pouvez faire une attaque MAC Flooding avec un outil appelé Macof qui fait partie de Dsniff qui peut être installé avec cette commande sur kali Linux :

```
sudo apt-get install -y dsniff
```

Mais nous avons décidé de développer notre propre code python qui va bombarder la table des adresses Mac du switch.

```
from random import randint
from scapy.all import *
def genMAC():
    #cette
    fonction genere des adresses MAC aleatoire
    Mac = [0x00]+[randint(0x00, 0xff) for i in range(5)]
    return ':' .join(map(lambda x: "%02x" % x, Mac))
```

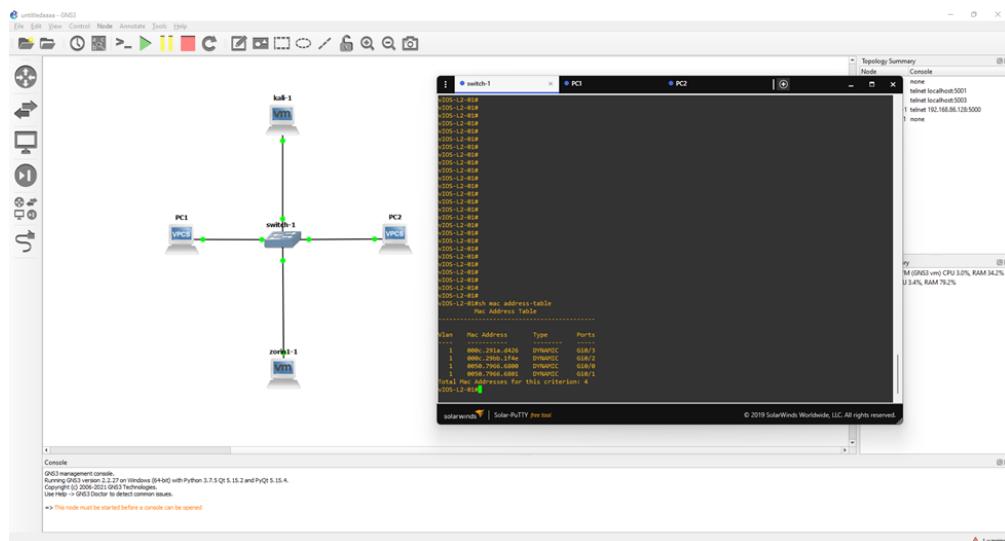
```

for i in range(10000):
    randMAC = genMAC()
    print("the mac sent is : " + randMAC)
10 destMAC = 'FF:FF:FF:FF:FF:FF'
    sendp(Ether(src=randMAC, dst=destMAC) / ARP(op=2, psrc
        ="0.0.0.0", hwdst=destMAC)/Padding(load="X"*18),
    verbose=0)

```

### 3.2.1 Avant l'attaque

Nous avons visualisé la table des adresses Mac du switch et testé le bon fonctionnement de ce dernier en essayant de capturer les trames sur un autre port. Ainsi, nous avons effectué des pings pour dépasser la phase d'apprentissage et remplir la table des adresses Mac du switch avec des adresses légitimes.

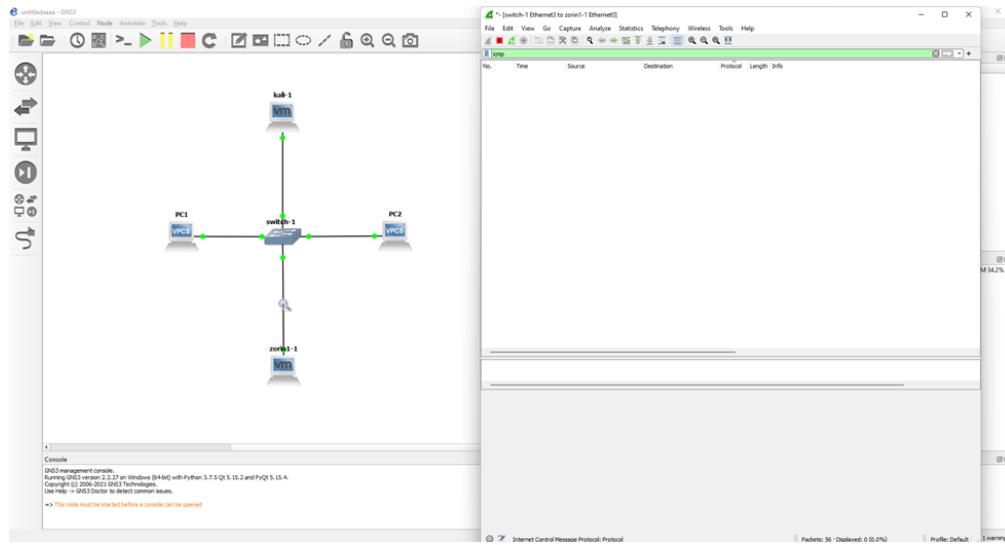


**FIGURE 2 – La table des adresses Mac du switch**

Nous avons effectué un ping entre le vPC1 et le vPC2 après la phase d'apprentissage. Cependant, nous ne pouvons pas intercepter la trame du Protocol ICMP vu que le switch par défaut achemine les trames vers les ports en question.

## 3.2 Première attaque : MAC Flooding

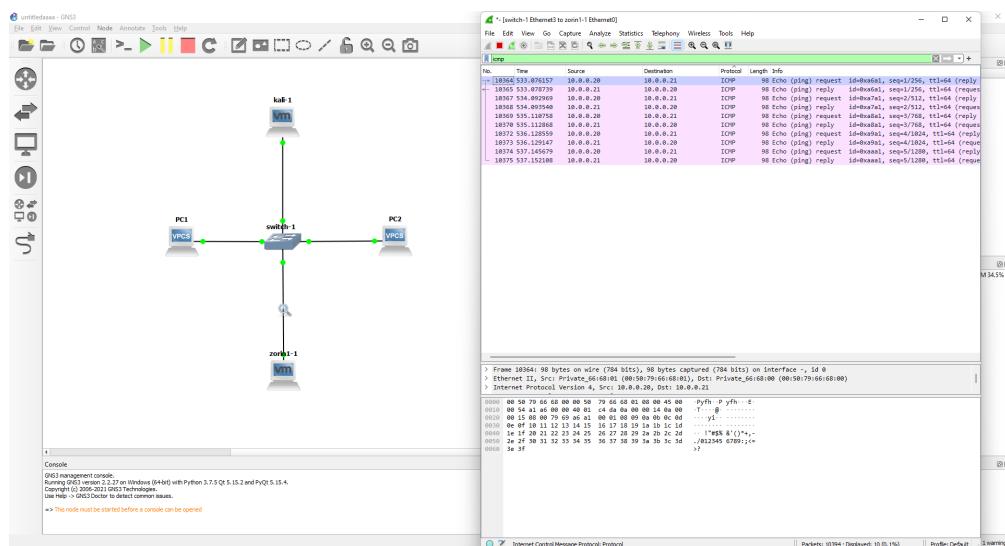
9



**FIGURE 3 –** Capture des trames avec wireshark avant l’attaque

### 3.2.2 Après l’attaque

Nous allons utiliser notre propre script python avec scapy pour bombarder la table des adresses du switch. Ainsi, la table d’apprentissage des adresses mac du switch sera saturée et le switch adoptera un comportement de Hub. Pour tester que le switch adopte bien un comportement de Hub, nous allons effectuer un ping du vPC1 vers vPC2 que nous allons intercepter à l’aide de Wireshark.



**FIGURE 4 –** Capture des trames avec wireshark après l’attaque

Ainsi, on s'aperçoit que le switch ne garantit plus la confidentialité des trames.

### **3.3 *Technique de prévention***

Cisco a mis en place une fonction, appelée switchport port-security, pour se protéger contre ce type d'attaque. Vous pouvez utiliser la fonction de sécurité du port pour restreindre l'entrée sur une interface en limitant et en identifiant les adresses MAC des stations autorisées à accéder au port. Il existe trois types d'adresses MAC sécurisées :

- Les adresses MAC sécurisées statiques : Elles sont configurées manuellement à l'aide de la commande de configuration d'interface switchport port-security mac-address mac-address, enregistrées dans la table d'adresses et ajoutées à la configuration courante du commutateur.
- Adresses MAC dynamiques sécurisées : Elles sont apprises dynamiquement, stockées uniquement dans la table d'adresses et supprimées au redémarrage du commutateur.
- Adresses MAC sécurisées collantes : Elles peuvent être apprises dynamiquement ou configurées manuellement, stockées dans la table d'adresses et ajoutées à la configuration en cours. Si ces adresses sont enregistrées dans le fichier de configuration, l'interface n'a pas besoin de les réapprendre dynamiquement lorsque le commutateur redémarre.

Lorsque le nombre maximum d'adresses MAC sécurisées a été ajouté à la table d'adresses et qu'une station dont l'adresse MAC ne figure pas dans la table d'adresses tente d'accéder à l'interface, une violation de sécurité se produit.

Le commutateur peut réagir à une violation de sécurité de trois manières différentes :

- protéger : Lorsque le nombre d'adresses MAC sécurisées atteint la limite autorisée sur le port, les paquets dont l'adresse source est inconnue sont abandonnés jusqu'à ce que vous supprimiez un nombre suffisant d'adresses MAC sécurisées ou que vous augmentiez le nombre d'adresses maximales autorisées. Vous n'êtes pas informés qu'une violation de sécurité s'est produite.
- restreindre : Lorsque le nombre d'adresses MAC sécurisées atteint la limite autorisée sur le port, les paquets dont l'adresse de source est inconnue sont abandonnés jusqu'à ce que vous supprimiez un nombre suffisant d'adresses MAC sécurisées ou que vous augmentiez le nombre d'adresses maximales autorisées. Dans ce mode, vous êtes informés qu'une violation

de sécurité s'est produite. Plus précisément, un piège SNMP est envoyé, un message syslog est enregistré et le compteur de violation s'incrémente.

- shutdown (arrêt) : Dans ce mode, une violation de la sécurité du port entraîne la désactivation immédiate de l'interface en cas d'erreur et l'extinction de la LED du port. Elle envoie également un piège SNMP, enregistre un message syslog et incrémente le compteur de violations. Lorsqu'un port sécurisé est dans l'état d'erreur désactivé, vous pouvez le faire sortir de cet état en entrant la commande de configuration globale errdisable recovery cause psecure-violation, ou vous pouvez le réactiver manuellement en entrant les commandes de configuration d'interface shutdown et no shutdown. Il s'agit du mode par défaut.

Exemple : Limiter à dix adresses MAC, dont deux sont statiques, sur le port FastEthernet 0/1. La violation requise est "restreinte".

```

Switch-1# conf t
Switch-1(config)# interface fastethernet0/1
Switch-1(config-if)# switchport mode access
Switch-1(config-if)# switchport port-security
5 Switch-1(config-if)# switchport port-security maximum 10
Switch-1(config-if)# switchport port-security violation
      restrict
Switch-1(config-if)# switchport port-security mac-address 8
      C9A.046E.0446
Switch-1(config-if)# switchport port-security mac-address 32
      CE.046E.3CEB

```

## 4 Deuxième attaque : Arp Spoofing

Le protocole de résolution d'adresse (ARP) est un protocole qui permet aux communications réseau d'atteindre un périphérique spécifique sur le réseau. ARP traduit les adresses IP (Internet Protocol) en adresses MAC (Media Access Control), et vice versa. Le plus souvent, les périphériques utilisent ARP pour contacter le routeur ou la passerelle qui leur permet de se connecter à Internet.

Les hôtes maintiennent un cache ARP, une table de correspondance entre les adresses IP et les adresses MAC, et l'utilisent pour se connecter à des destinations sur le réseau. Si l'hôte ne connaît pas l'adresse MAC d'une certaine adresse IP, il

envoie un paquet de requête ARP, demandant aux autres machines du réseau l'adresse MAC correspondante.

Le protocole ARP n'a pas été conçu pour la sécurité, il ne vérifie donc pas qu'une réponse à une requête ARP provient réellement d'une partie autorisée. Il permet également aux hôtes d'accepter les réponses ARP même s'ils n'ont jamais envoyé de demande. Il s'agit là d'un point faible du protocole ARP, qui ouvre la porte aux attaques de type "ARP spoofing".

Le protocole ARP ne fonctionne qu'avec des adresses IP de 32 bits dans l'ancienne norme IPv4. Le nouveau protocole IPv6 utilise un protocole différent, le Neighbor Discovery Protocol (NDP), qui est sécurisé et utilise des clés cryptographiques pour vérifier l'identité des hôtes. Toutefois, comme la majeure partie de l'internet utilise toujours l'ancien protocole IPv4, le protocole ARP reste largement utilisé. L'usurpation ARP, également appelée empoisonnement ARP, est une attaque de type "Man in the Middle" (MitM) qui permet aux attaquants d'intercepter la communication entre les périphériques réseau. L'attaque fonctionne comme suit :

1. L'attaquant doit avoir accès au réseau. Il analyse le réseau pour déterminer les adresses IP d'au moins deux périphériques, disons une station de travail et un routeur.
2. L'attaquant utilise un outil d'usurpation, tel que Arpspoof ou Driftnet, pour envoyer de fausses réponses ARP.
3. Les réponses falsifiées annoncent que l'adresse MAC correcte pour les deux adresses IP, appartenant au routeur et à la station de travail, est l'adresse MAC de l'attaquant. Le routeur et la station de travail sont ainsi trompés et se connectent à la machine de l'attaquant, au lieu de se connecter l'un à l'autre.
4. Les deux appareils mettent à jour leurs entrées de cache ARP et, à partir de ce moment, communiquent avec l'attaquant au lieu de communiquer directement entre eux.
5. L'attaquant est maintenant secrètement au milieu de toutes les communications.

Une fois que l'attaquant a réussi une attaque ARP spoofing, il peut :

- Continuer à acheminer les communications telles quelles - l'attaquant peut renifler les paquets et voler les données, sauf si ces dernières sont transférées sur un canal crypté comme HTTPS.
- Effectuer un détournement de session - si l'attaquant obtient un identifiant de session, il peut accéder aux comptes sur lesquels l'utilisateur est

actuellement connecté.

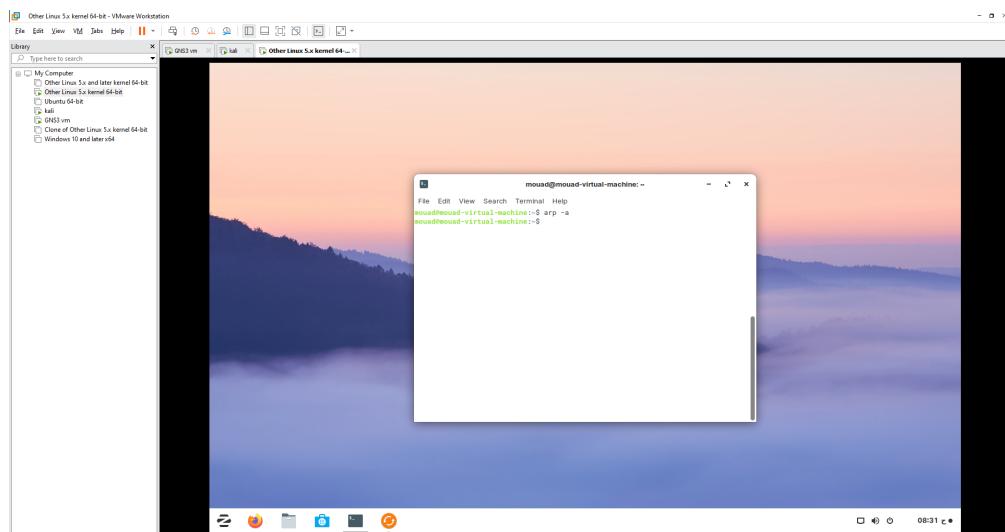
- Modifier la communication, par exemple en envoyant un fichier ou un site Web malveillant sur le poste de travail.
- Déni de service distribué (DDoS) - les attaquants peuvent fournir l'adresse MAC d'un serveur qu'ils souhaitent attaquer par DDoS, au lieu de leur propre machine. S'ils le font pour un grand nombre d'IP, le serveur cible sera bombardé de trafic.

## 4.1 Mise en oeuvre de l'attaque

Il existe deux types d'attaques ARP :

- Usurpation ARP : un pirate envoie de faux paquets ARP reliant l'adresse MAC d'un attaquant à l'adresse IP d'un ordinateur déjà sur le LAN.
- Empoisonnement ARP : après une usurpation ARP réussie, un pirate modifie la table ARP d'une entreprise afin de falsifier les correspondances entre adresses MAC et IP. L'attaque se propage.

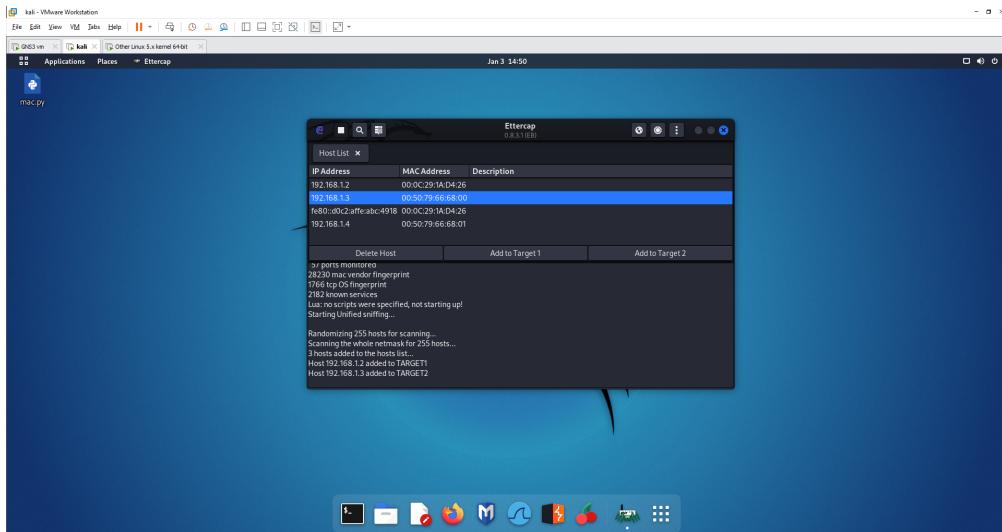
L'objectif est de relier l'adresse MAC d'un pirate au réseau. Ainsi, tout trafic envoyé au réseau compromis sera redirigé vers le cybercriminel. Sur la machine Zorin, nous allons visualiser le cache Arp qui doit être vide :



**FIGURE 5 –** Visualisation du cache Arp avant l'attaque

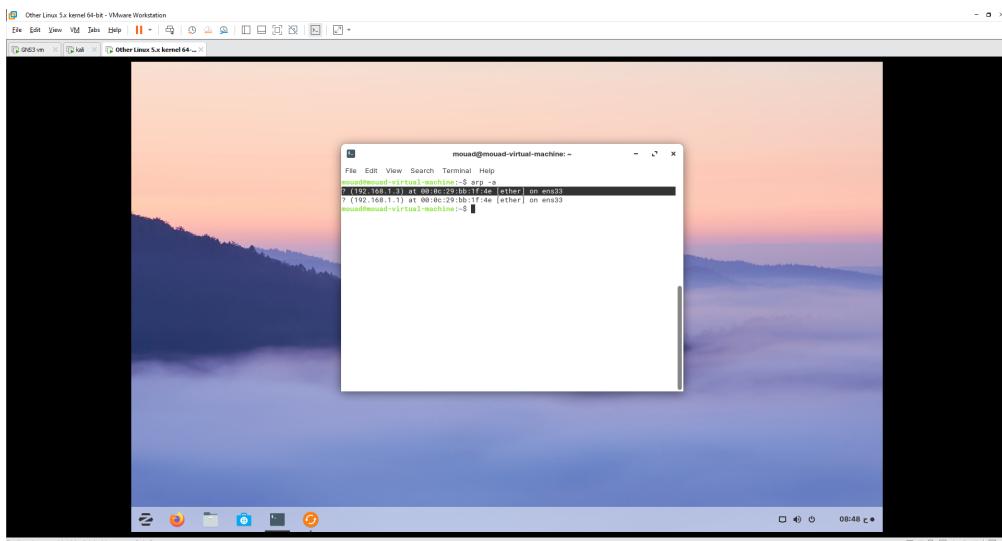
Avec Ettercap nous allons faire un scan pour trouver les hôtes sur notre segment réseau, nous avons trouvé 3 hôtes. Nous choisissons la machine Zorin

comme victime (@IP 192.168.1.2) et le PC1 (@IP 192.168.1.3) pour faire un man in the middle.



**FIGURE 6 – Ettercap scan**

Sur Zorin on effectue un Arp -a et on constate que @IP du PC1 est liée à l'adresse Mac du kali.



**FIGURE 7 – Visualisation du cache Arp apres l'attaque**

Nous effectuons un ping qui fonctionne correctement. On remarque que c'est Kali qui nous répond.

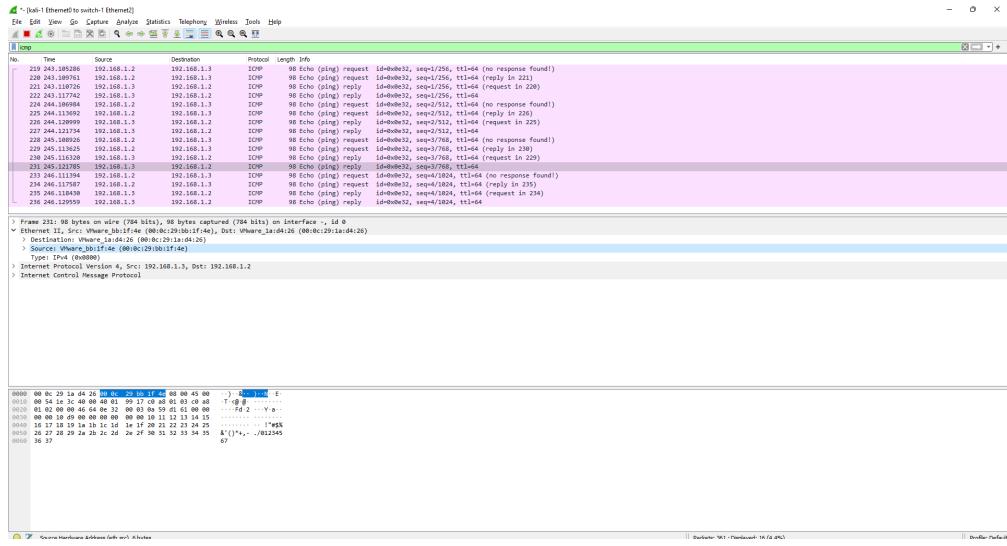


FIGURE 8 – Le résultat de l'attaque

## 4.2 Technique de prévention

Pour prévenir les attaques ARP Spoofing, les configurations suivantes sont disponibles sur les outils cisco.

- Activation de l'anti-spoofing ARP
- Configuration de la protection de l'hôte
- Configuration du contrôle de cohérence de l'adresse MAC source
- Configuration de l'anti-spoofing de la passerelle
- Configuration du port de confiance

Exemple : Configuration de la protection de l'hôte La configuration de la protection de l'hôte sur un port permet à ce dernier de rejeter les paquets ARP inconnus. Configurez la liaison IP-port lorsque vous configurez le dispositif pour rejeter les paquets ARP inconnus. Cela permet au paquet ARP de cette adresse IP d'inonder les autres ports uniquement via ce port configuré. Si le paquet ARP de cette adresse IP entre par un autre port, il sera rejeté.

```
Switch-1# configure terminal
Switch-1# host-guard bind ip 192.168.5.13 interface ethernet
      1/2
```

## 5 Troisième attaque : DHCP spoofing

DHCP (Dynamic Host Configuration Protocol) est un protocole de gestion de réseau de la couche application qui fournit un système rapide, automatique et central pour la distribution et l'attribution d'adresses IP et d'informations de configuration TCP/IP pour les clients d'un réseau.

Le protocole DHCP peut être utilisé pour attribuer des informations de masque de sous-réseau, des adresses IP de passerelle par défaut, des adresses de système de nom de domaine (DNS), etc. Une autre caractéristique des configurations DHCP est qu'elles sont limitées dans le temps par le DHCP Lease Time, qui détermine la fréquence à laquelle elles doivent être renouvelées. Avant de décrire les techniques d'usurpation et d'empoisonnement du protocole DHCP, passons en revue le fonctionnement de base du protocole DHCP. Dans un scénario normal, lorsqu'un client se connecte pour la première fois à un nouveau réseau DHCP, le processus est le suivant :

- Le client envoie une requête DHCPDISCOVER par diffusion.
- La demande comprend des informations sur le client, telles que l'adresse MAC, afin que le serveur sache quel client a envoyé la demande.
- Le serveur DHCP répond par un DHCPOFFER. Le DHCPOFFER propose au client une adresse IP provenant du pool d'adresses disponibles du serveur DHCP et définit l'IP de destination sur l'adresse proposée.
- Le client répond avec un DHCPREQUEST pour confirmer l'adresse fournie par le serveur et demande des détails supplémentaires au serveur.
- Le serveur DHCP répond par un DHCPACK pour accuser réception de la demande du client et confirmer l'adresse IP demandée. Des informations supplémentaires sont fournies, notamment l'adresse du serveur DNS, le nom de domaine et la durée du bail.
- Lorsque la période de location est terminée, le client envoie un message DHCPRELEASE pour informer le serveur que l'adresse peut maintenant être redistribuée à un autre client.

Il va sans dire que le protocole DHCP est un outil de configuration réseau puissant qui peut simplifier la vie des administrateurs réseau. Le problème survient lorsque des administrateurs réseau peu méfiants ne sont pas conscients de tout ce qui rend le protocole DHCP vulnérable aux attaques. Par défaut, le protocole DHCP n'utilise aucune forme d'authentification et est envoyé en diffusion, de sorte que n'importe quel dispositif du réseau peut potentiellement recevoir et éventuellement altérer les messages.

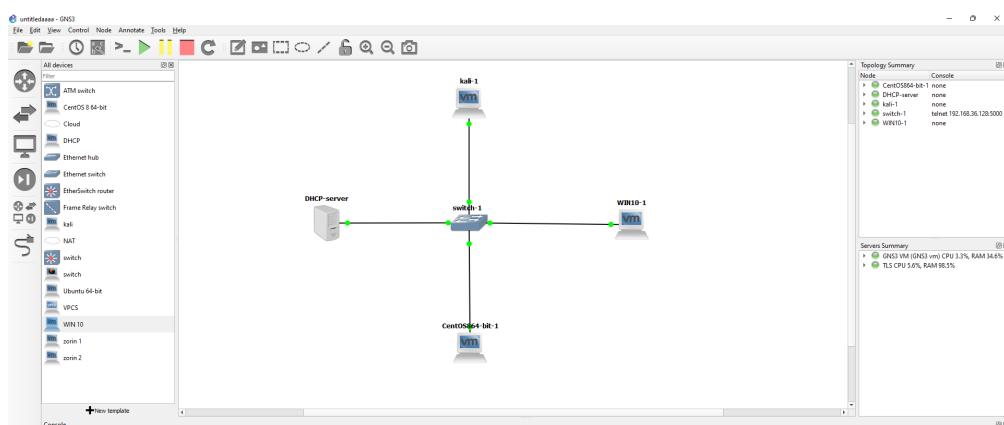
DHCP Spoofing (usurpation d'identité DHCP) se produit lorsqu'un attaquant tente de répondre aux demandes DHCP et tente de se faire passer (spoof) pour la passerelle (Gateway) ou le serveur DNS par défaut, ce qui déclenche une attaque de l'homme du milieu (Man In The Middle ou MITM). Il est donc possible qu'ils puissent intercepter le trafic des utilisateurs avant de le rediriger vers la passerelle (Gateway) réelle ou effectuer des Dos (Denial of Service Attack, Attaque par déni de service en français) en inondant le serveur DHCP réel de demandes visant à étouffer les ressources en adresses IP.

### **5.1 Mise en oeuvre de l'attaque :**

Nous allons maintenant configurer notre propre serveur DHCP, écouter les demandes de diffusion entrantes et envoyer des réponses usurpées avec des configurations malveillantes. En général, nous cherchons à se définir comme serveur DNS et passerelle par défaut pour les clients.

#### **5.1.1 Une deuxième topologie :**

Afin de mettre en oeuvre cette attaque, nous allons avoir besoin d'un serveur DHCP sur notre topologie. Ainsi pour cette attaque, nous allons introduire un serveur DHCP sur notre maquette.



**FIGURE 9 – Une deuxième topologie**

#### **5.1.2 Avant l'attaque**

Sur notre machine victime windows 10 nous avons testé le bon fonctionnement de notre serveur DHCP.

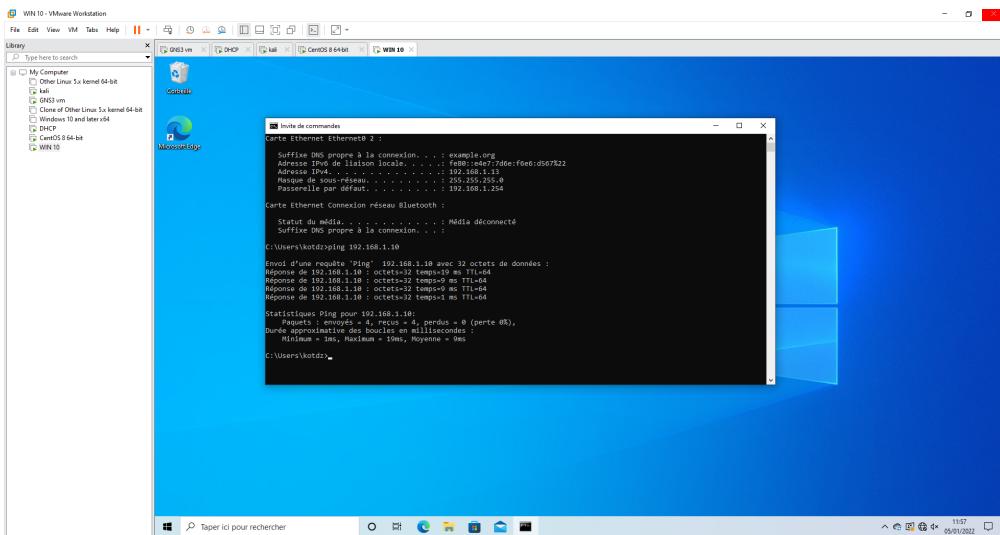


FIGURE 10 – Une deuxième topologie

Nous commençons notre attaque à l'aide de Ettercap :

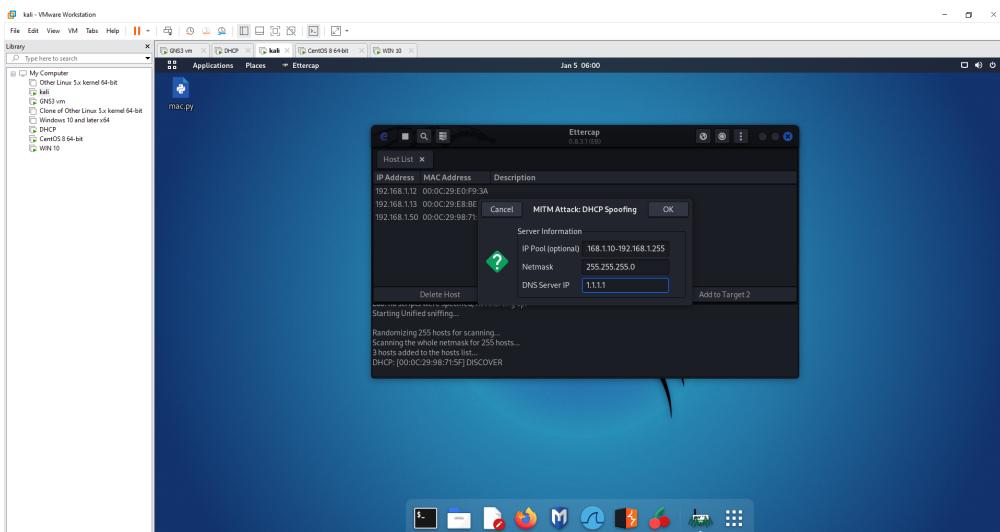
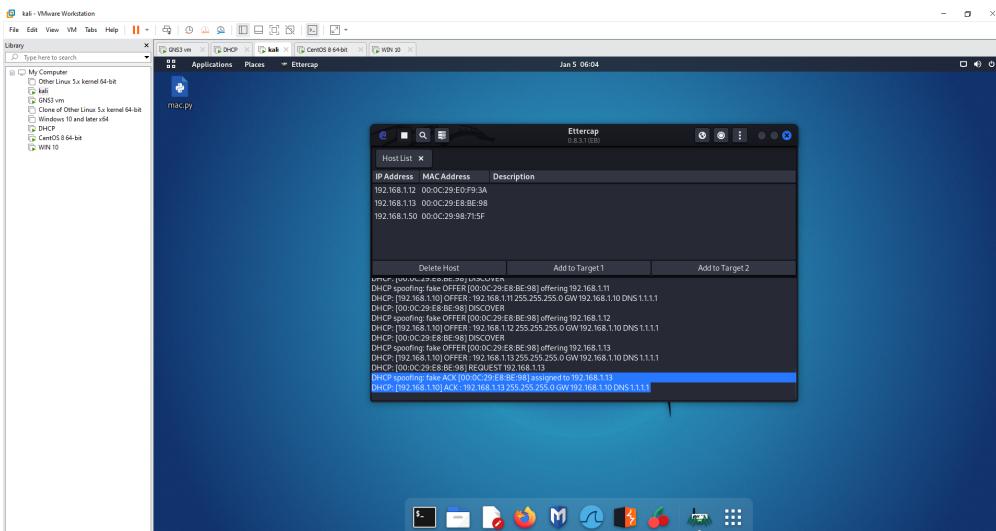


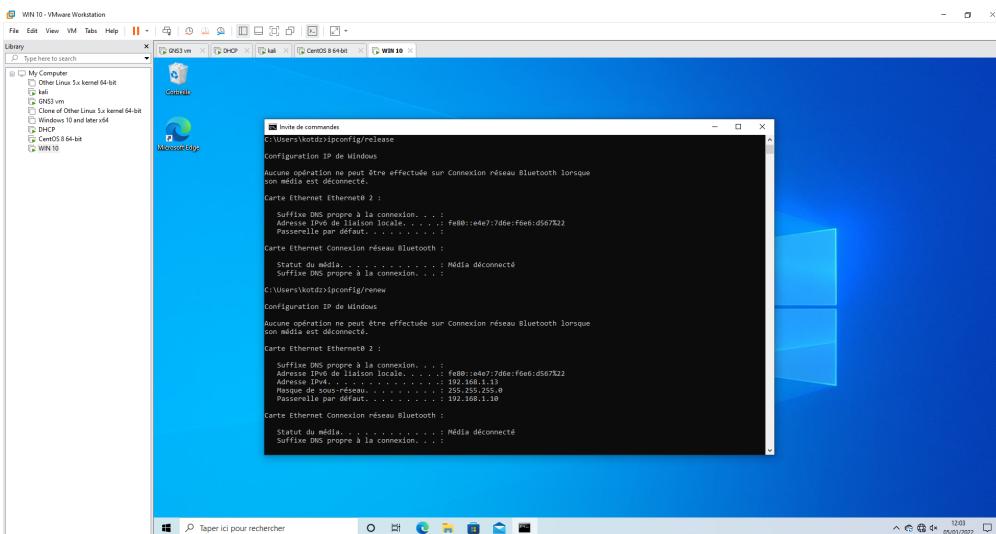
FIGURE 11 – DHCP spoofing avec ettercap

### 5.1.3 Après l'attaque

Nous détections sur Ettercap que la machine windows a bien subi l'attaque.

**FIGURE 12 – Fake ACK envoyé**

Ainsi, nous remarquons que la passerelle par défaut ainsi que @IP du DNS a changé. On en conclut que notre attaque a redirigé la machine Windows vers la machine attaquante qui se présente comme un serveur DHCP .

**FIGURE 13 – Machine windows victime du DHCP spoofing**

## 5.2 *Technique de prévention*

DHCP Snooping est une technologie de sécurité de couche 2 du modèle OSI intégrée dans le système d'exploitation d'un commutateur réseau qui connecte les clients aux serveurs DHCP et supprime le trafic DHCP jugé inacceptable. Il empêche les serveurs DHCP non autorisés de distribuer des adresses IP aux clients DHCP. La fonction DHCP Snooping permet d'effectuer les actions suivantes :

- Valider les messages DHCP provenant de sources non fiables et filtrer les messages invalides.
- Construire et maintenir la base de données de liaison DHCP Snooping, qui contient des informations sur les hôtes non fiables avec des adresses IP louées.
- Utiliser la base de données de liaison DHCP Snooping pour valider les requêtes ultérieures des hôtes non fiables.

Ainsi, nous aurons une liste des ports "trusted" et "untrusted". Seuls les ports Trusted pourront émettre des DHCP OFFER et ACK, et donc, la machine pirate du schéma ci-dessus, n'étant pas sur un port trusted, ne pourra pas émettre de DHCP OFFER et ACK. C'est très simple à mettre en place :

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 3 15
Switch(config)# ip dhcp snooping information option
Switch(config)# interface fastethernet0/0
5 Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate 50
```

## 6 Quatrième attaque : STP Manipulation Attack

Les liens redondants sont toujours les bienvenus dans la topologie des commutateurs car ils augmentent la disponibilité et la robustesse du réseau.

Les liens redondants, si nous les considérons du point de vue de la couche 2, peuvent provoquer des boucles de couche 2. C'est simplement parce que le champ TTL (Time To Live) du paquet se trouve dans l'en-tête de la couche 3 et que la couche 2 ne possède pas un tel champ.

Sur L3, cela signifie que le nombre de TTL ne sera diminué que lorsque le paquet passera par le routeur. Il n'y a aucun moyen de "tuer" un paquet qui est

---

coincé dans une boucle de couche 2. Cette situation peut entraîner des tempêtes de diffusion.

Heureusement, le protocole STP (Spanning Tree Protocol) peut vous permettre d'avoir des liens redondants tout en ayant une topologie sans boucle, empêchant ainsi le potentiel d'une tempête de diffusion.

Le protocole STP réalise cette topologie sans boucle en sélectionnant un commutateur comme pont racine. Si nécessaire, l'administrateur réseau peut influencer le choix du commutateur qui devient le pont racine. Cela se fait en manipulant la priorité du commutateur, la priorité du pont la plus basse signifiant le pont racine.

Tous les autres commutateurs du réseau choisissent un port racine, le port STP du réseau convergé "le plus proche" du commutateur du pont racine, en termes de "coût". Les commutateurs prennent des dispositions pour l'élection du pont racine par l'échange d'unités de données du protocole de pont (BPDU). Tous les ports des commutateurs de la topologie sont soit dans l'état de blocage, soit dans l'état de transmission.

Si le pont racine tombe, la topologie STP doit trouver un nouveau pont racine et l'élection commence à ce moment-là. Un port ne passe pas immédiatement de l'état de blocage à l'état de transfert. Il passe plutôt de l'état bloqué à l'état d'écoute, puis à l'état d'apprentissage, et enfin à l'état de transfert. Le délai avant que le port ne commence à transmettre des paquets peut aller jusqu'à une minute.

Si un attaquant a accès aux ports du commutateur qui peuvent devenir des ports de jonction, il peut introduire un commutateur pirate dans le réseau.

N'oubliez pas que les commutateurs Cisco ont tous les ports en mode "désirable dynamique" par défaut. Cela signifie que si les ports sont toujours dans ce mode, l'attaquant peut connecter le commutateur rouge dans la prise murale du réseau de son cubicule et le commutateur négociera le lien trunk avec le commutateur de l'entreprise.

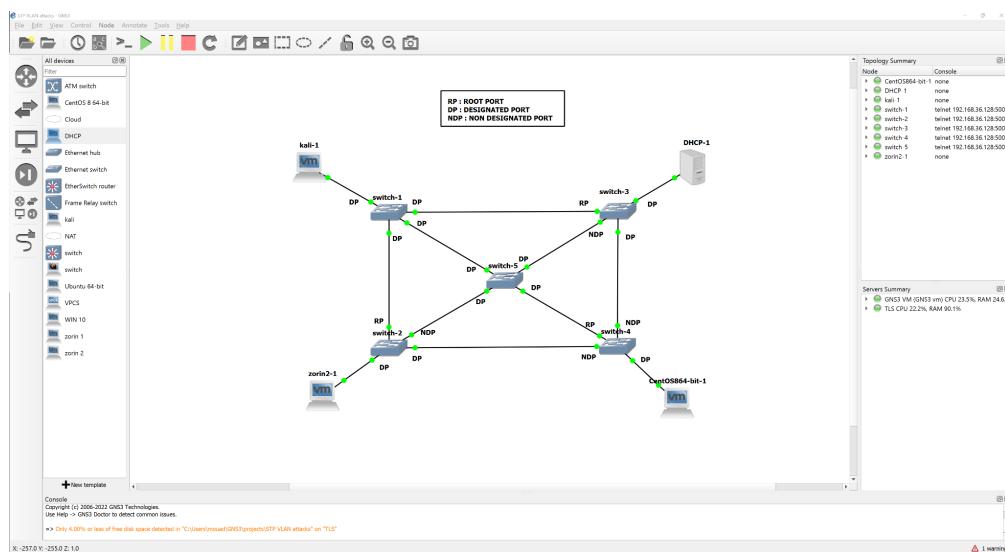
À ce moment-là, il a la possibilité de former une autre connexion avec le deuxième commutateur de cette entreprise et il est alors en mesure de manipuler la priorité spanning tree du commutateur rouge. S'il configure son commutateur pirate pour qu'il ait une priorité inférieure à celle de tout autre commutateur de l'entreprise, la plupart du trafic passera théoriquement par ce commutateur.

Le commutateur pirate avec par exemple la priorité 0 annonce ses "BPDUs supérieurs", et la topologie STP se reconvertis. Son commutateur rouge devient le pont racine et tout le trafic passe par ce commutateur. Cela lui donne la possibilité de renifler tout le trafic dans l'entreprise. Il va également rediriger le trafic des liens à large bande passante entre les autres commutateurs vers un lien de 100

Mbps sur le commutateur rouge. Cela réduira considérablement la vitesse du réseau.

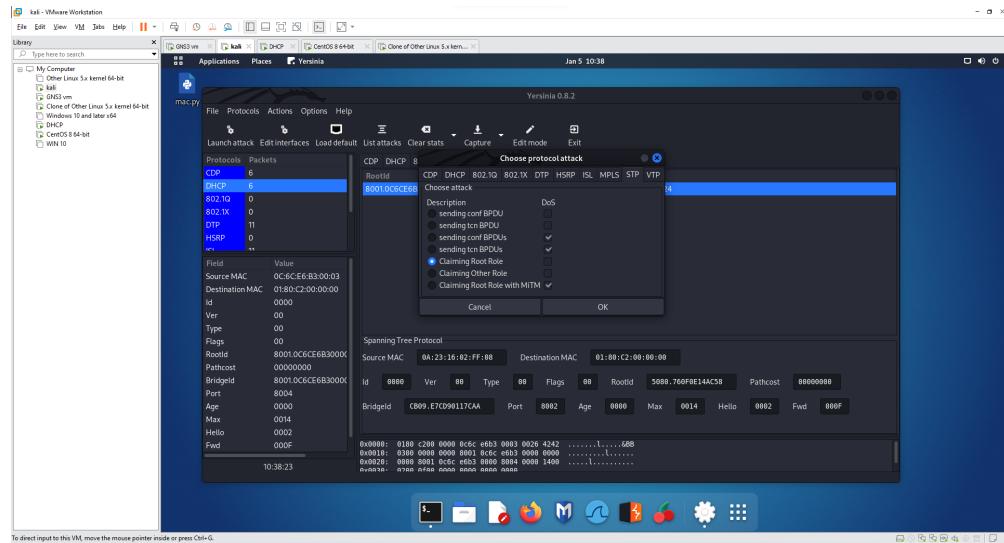
### 6.1 Mise en oeuvre de l'attaque :

Une attaque STP implique un attaquant qui usurpe le pont racine dans la topologie. L'attaquant diffuse un BPDU de changement de configuration/topologie STP dans le but de forcer un recalcul STP. Le BPDU envoyé annonce que le système de l'attaquant a une priorité de pont inférieure. L'attaquant peut alors voir une variété de trames qui proviennent d'autres commutateurs. Le recalcul STP peut également provoquer une condition de déni de service (Dos) sur le réseau en provoquant une interruption de 30 à 45 secondes chaque fois que le pont racine change. Nous allons configurer le STP, après la convergence du STP on a la maquette suivante :



**FIGURE 14 – Une Troisième topologie**

Notre attaque va consister à bombarder le root bridge qui est le switch 1. À l'aide de yersinia nous avons détecté l'adresse mac du root bridge. Ainsi, nous allons essayer de passer en root bridge.



**FIGURE 15 – Acces au root bridge à l'aide de yersinia**

Nous remarquons que le root bridge mac adresse a changé et que le switch 1 n'est plus le root bridge.

```

VIOS-L2-01>en
VIOS-L2-01#sh span vlan 1

VLAN0001
  Spanning tree enabled protocol ieee
    Root ID  Priority    32769
              Address      0c6c.e6b2.0000
              Cost         4
              Port        4 (GigabitEthernet0/3)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

    Bridge ID Priority    32769 (priority 32768 sys-id-ext 1)
              Address      0c6c.e6b3.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time   300 sec

    Interface      Role Sts Cost      Prio.Nbr Type
    -----+-----+-----+-----+-----+-----+
    Gi0/0        Desg FWD 4       128.1  Shr
    Gi0/1        Desg FWD 4       128.2  Shr
    Gi0/2        Desg FWD 4       128.3  Shr
    Gi0/3        Root FWD 4      128.4  Shr
    Gi1/0        Desg FWD 4       128.5  Shr
    Gi1/1        Desg FWD 4       128.6  Shr
    Gi1/2        Desg FWD 4       128.7  Shr
    Gi1/3        Desg FWD 4       128.8  Shr
  
```

**FIGURE 16 – Root bridge changé**

Dans ce cas là, nous avons deux alternatives pour continuer l'attaque :

- Root ownership attack : Alternative 1. Cette attaque consiste à s'emparer d'abord du pont racine, puis à ne jamais activer le bit TC-ACK dans les BPDU lors de la réception d'un BPDU TCN. Il en résulte un vieillissement prématûr constant des entrées dans les tables de transfert des commutateurs, ce qui peut entraîner une inondation inutile.

- Root ownership attack : Alternative 2. Pour un effet encore plus négatif, une séquence où l'outil d'attaque génère une BPDU supérieure prétendant être la racine, suivie d'une rétractation de cette information quelques secondes plus tard (voir la fonction "claiming other role" de Yersinia) pourrait être utilisée. Il est garanti que cela provoquera un grand nombre de processus en raison des transitions constantes de la machine d'état, avec pour résultat une utilisation élevée du CPU et un Dos potentiel.

## 6.2 *Technique de prévention :*

Il existe deux principaux mécanismes de protection contre les attaques sur le processus STP : la protection avec Root Guard et la protection de la couche 2 avec BPDU Guard.

### 6.2.1 Protection de la couche 2 avec Root Guard

Le Root Guard peut être activé sur tous les ports du commutateur qui ne doivent pas devenir des ports racine. Cela signifie donc sur chaque port qui n'est pas un port racine. Juste pour vous rappeler, le port racine sur chaque commutateur est le port considéré comme étant le plus proche du commutateur pont racine. Si un port configuré pour Root Guard reçoit un BPDU supérieur, il ne croira pas le BPDU, et alors au lieu de devenir le nouveau port racine, le port passe dans un état root-inconsistent. Tant qu'un port est dans l'état root-inconsistent, il est complètement bloqué pour les données utilisateur, ce qui signifie qu'aucune donnée utilisateur n'est envoyée à travers lui. Cependant, il y a un peu d'espoir pour lui, après l'arrêt des BPDUs supérieurs, le port retourne à l'état de forwarding.

```
Switch-1(config)# interface gigabitethernet 0/1
Switch-1(config-if)# spanning-tree guard root
```

### 6.2.2 Protection de la couche 2 avec BPDU Guard

Le BPDU Guard doit être activé sur tous les ports pour lesquels la fonction Cisco PortFast est configurée. La fonction PortFast est activée sur les ports qui se connectent aux périphériques hôtes, tels que les PC des utilisateurs finaux. Elle permet de sauter presque tout le temps d'attente nécessaire pour que le port passe à l'état de transfert après avoir été connecté.

N'oubliez pas que le processus de convergence STP classique est trop lent pour les réseaux actuels. Avant que le port ne passe à l'état de transfert, le STP le place dans l'état de blocage pendant 20 secondes, dans l'état d'écoute pendant 15 secondes, dans l'état d'apprentissage pendant les 15 secondes restantes, puis le fait finalement passer à l'état de transfert. Tout cela parce que STP doit être sûr que ce port ne fera pas une boucle de couche 2 quand il entre dans l'état de transfert.

La logique de PortFast est qu'un port qui se connecte à un appareil d'utilisateur final n'a pas le potentiel de créer une boucle topologique. Pour cette raison, le port peut devenir actif plus rapidement en sautant les états d'écoute et d'apprentissage du STP. Comme ces ports PortFast sont connectés à des dispositifs d'utilisateur final, ils ne devraient jamais recevoir de BPDU (les BPDU sont envoyés uniquement par les commutateurs). Par conséquent, si un port activé pour BPDU Guard reçoit un BPDU, le port est désactivé et la violation de cette politique est signalée et arrêtée de cette manière.

Configuration de BPDU Guard :

```
Switch-1(config)# interface gigabitetherent 0/2
Switch-1(config-if)# spanning-tree port fast bpduguard
```

## 7 Cinquième attaque : Vlan hopping

Un réseau local virtuel (VLAN) est utilisé pour partager le réseau physique tout en créant des segmentations virtuelles pour diviser des groupes spécifiques. Par exemple, un hôte sur le VLAN 1 est séparé de tout hôte sur le VLAN 2. Tous les paquets envoyés entre les VLAN doivent passer par un routeur ou d'autres dispositifs de couche 3. La sécurité est l'une des nombreuses raisons pour lesquelles les administrateurs réseau configurent les VLAN. Cependant, grâce à un exploit connu sous le nom de "VLAN Hopping", un attaquant est capable de contourner ces implémentations de sécurité. VLAN Hopping permet à un attaquant de contourner toute restriction de couche 2 construite pour diviser les hôtes. Avec une configuration correcte des ports de commutation, un attaquant devrait passer par un routeur et tout autre dispositif de couche 3 pour accéder à sa cible. Cependant, de nombreux réseaux ont une mauvaise implémentation des VLAN ou sont mal configurés, ce qui permet aux attaquants de réaliser cet exploit. Dans cet article, je vais passer en revue les deux principales

méthodes de saut de VLAN, connues sous le nom de "switched spoofing" et de "double tagging".

## 7.1 *Switched Spoofing*

Un attaquant se fait passer pour un commutateur afin d'inciter un commutateur légitime à créer une liaison interréseaux entre eux. Comme mentionné précédemment, les paquets de n'importe quel VLAN sont autorisés à passer par un lien de jonction. Une fois la liaison trunk établie, l'attaquant a accès au trafic de n'importe quel VLAN. Cet exploit ne réussit que si le commutateur légitime est configuré pour négocier un trunk. Cela se produit lorsqu'une interface est configurée en mode "dynamic desirable", "dynamic auto" ou "trunk". Si l'un de ces modes est configuré sur le commutateur cible, l'attaquant peut alors générer un message DTP à partir de son ordinateur et un lien interurbain peut être formé.

## 7.2 *Double Tagging*

Le double tagging se produit lorsqu'un attaquant ajoute et modifie des balises sur une trame Ethernet pour permettre l'envoi de paquets à travers n'importe quel VLAN. Cette attaque tire parti de la façon dont de nombreux commutateurs traitent les balises. La plupart des commutateurs ne retirent que la balise extérieure et transmettent la trame à tous les ports VLAN natifs. Cela dit, cet exploit n'est efficace que si l'attaquant appartient au VLAN natif de la liaison trunk. Un autre point important est que cette attaque est strictement à sens unique car il est impossible d'encapsuler le paquet de retour.

Pour cette attaque, nous allons créer 3 VLANs. VLAN 2 : consacré à l'administration. VLAN 3 : consacré aux profs. VLAN 4 : consacré aux étudiants. Sur le VLAN 2 il y a un serveur ftp qui contient les notes des élèves.

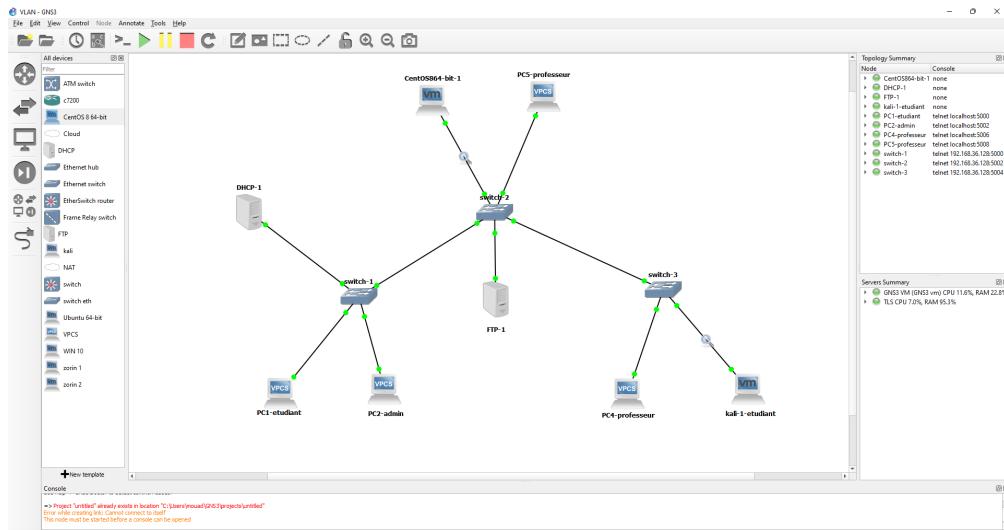


FIGURE 17 – Quatrième topologie :

L’objectif de l’attaque est d’être capable de faire du VLAN hopping, C-à-d accéder à un VLAN non autorisé. Par exemple, le PC kali-1 qui est un étudiant dans le VLAN 4 va essayer de se connecter à l’autre VLAN. Ainsi, à l’aide de yersinia nous allons nous faire passer pour un port Trunk.

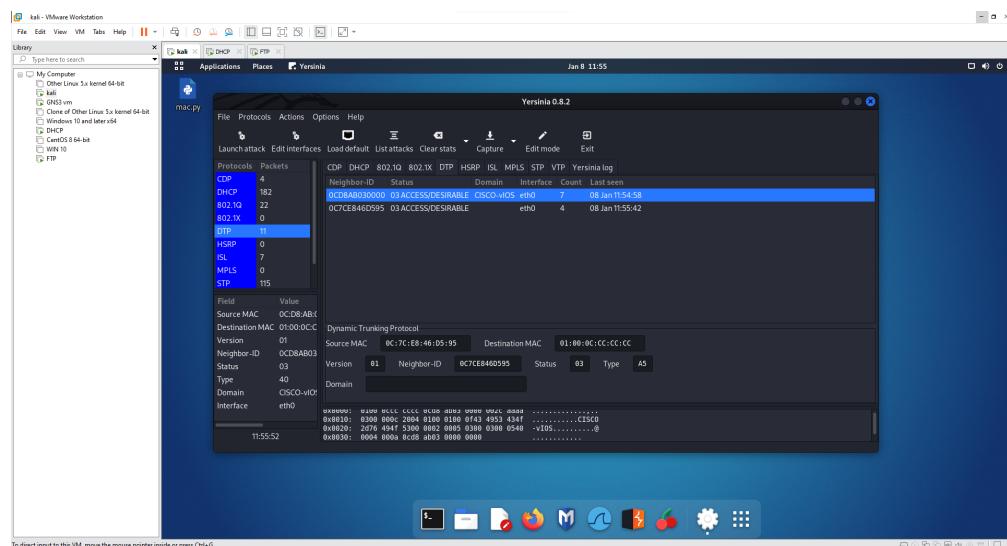


FIGURE 18 – Passage en mode trunk à l'aide de yersinia

Sur le switch nous pouvons bien confirmer que le port est trunk.

```
vios-l2-01#sh int trunk
Port      Mode       Encapsulation  Status      Native vlan
Gi0/0    desirable    n-802.1q     trunking    1
Gi0/1    on          802.1q      trunking    1

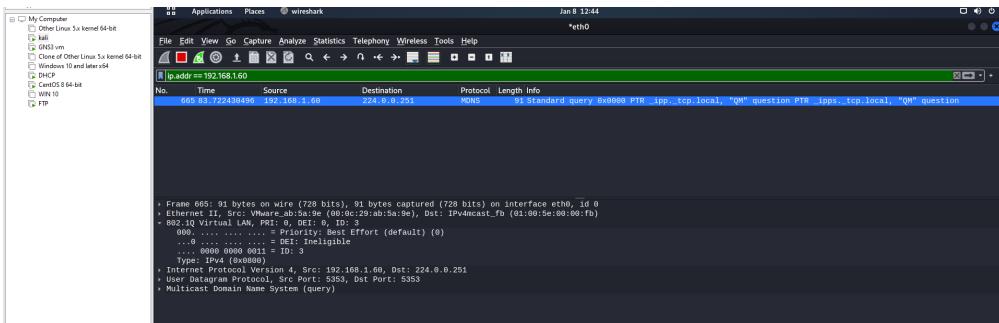
Port      Vlans allowed on trunk
Gi0/0    1-4094
Gi0/1    1-1000

Port      Vlans allowed and active in management domain
Gi0/0    1,3-5,100,200,300
Gi0/1    1,3-5,100,200,300

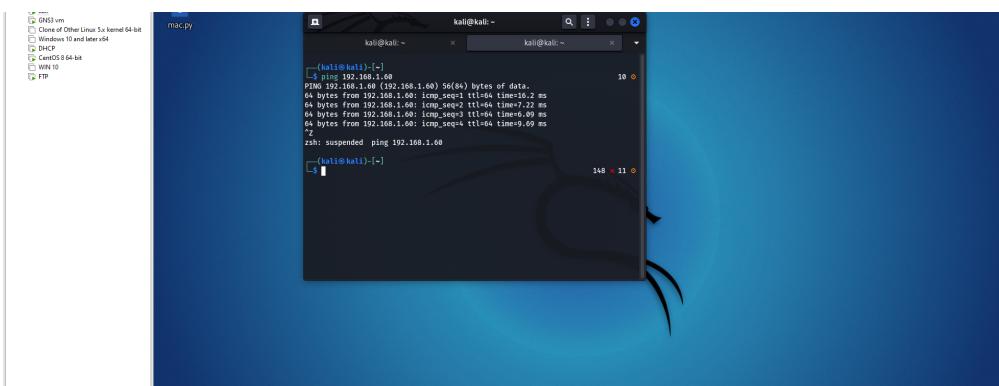
Port      Vlans in spanning tree forwarding state and not pruned
Gi0/0    none
Gi0/1    1,3-5,100,200,300
vios-l2-01#
```

**FIGURE 19 – Trunk port sur le switch**

Et à l'aide de wireshark nous allons faire du sniffing pour détecter le VLAN du serveur ftp.

**FIGURE 20 – Détection du VLAN du serveur ftp**

En outre, nous allons créer une interface virtuelle et nous allons rattacher cette dernière au Vlan 3. Apres, nous effectuons un ping vers une machine du Vlan 3.

**FIGURE 21 – Ping vers le serveur ftp**

Ainsi, nous détectons un trafic FTP non crypté :

94 40.478244	192.168.1.12	192.168.1.60	FTP	78 Request: USER admin
96 40.479699	192.168.1.60	192.168.1.12	FTP	100 Response: 331 Please specify the password.
104 44.893465	192.168.1.12	192.168.1.60	FTP	85 Request: PASS telecomparis

FIGURE 22 – Détection du trafic FTP avec wireshark

Enfin, nous avons mis la main sur les notes depuis le serveur ftp

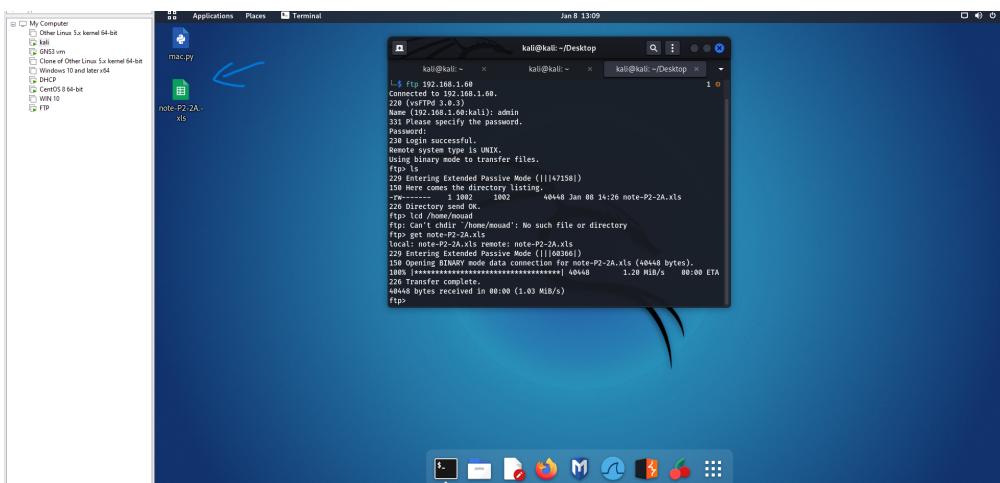


FIGURE 23 – Intrusion du serveur ftp

### 7.3 Technique de prévention

Certains ports de commutateurs Cisco passent par défaut en mode automatique pour le trunking. Cela signifie que les ports deviennent automatiquement des ports de jonction s'ils reçoivent des trames DTP (Dynamic Trunking Protocol) sur certains des ports du commutateur. Il s'agit d'un grand problème de sécurité car un attaquant peut faire en sorte que le port de son commutateur devienne un tronc commun, ce qui lui permet de réaliser facilement des attaques par saut de VLAN. Il peut accéder à tous les VLAN sur le commutateur sans avoir besoin de faire passer les paquets par un routeur. Pour rendre l'usurpation de commutateur impossible, vous pouvez désactiver le trunking sur tous les ports qui n'ont pas besoin de former des trunks, et désactiver le DTP sur les ports qui doivent être des trunks.

### 7.4 Empêcher le Trunking

```
Switch-1(config)# interface gigabitethernet 0/3
Switch-1(config-if)# switchport mode access
Switch-1(config-if)# exit
```

## 7.5 Prévention de l'utilisation du DTP

```
Switch-1(config)# interface gigabitethernet 0/4
Switch-1(config-if)# switchport trunk encapsulation dot1q
Switch-1(config-if)# switchport mode trunk
Switch-1(config-if)# switch port nonegotiate
```

## 7.6 Empêcher le double tagging

```
Switch-1(config)# interface gigabitethernet 0/4
Switch-1(config-if)# switchport trunk native vlan 400
```

# 8 Conclusion

Une récente enquête CSI/FBI a montré que le vol d'informations est la première tendance croissante et que 75 % de toutes les attaques ayant entraîné des pertes financières provenaient de l'intérieur du réseau. Par conséquent, l'intérieur des réseaux d'entreprise doit être approvisionné de manière plus innovante. Si chaque port du réseau est considéré comme un port "périmétrique" auquel des entités potentiellement hostiles peuvent accéder, les administrateurs réseau doivent être conscients de la nature de ces menaces potentielles et des nouvelles fonctions de sécurité, telles que celles présentées dans ce projet , qui doivent être déployées pour verrouiller ces ports et empêcher ces attaques de sécurité de couche 2 potentiellement dommageables.

## Références

- [1] "Security Configuration, Cisco Catalyst PON Series Switches", Cisco Systems, Inc.[Enligne]. Disponible : [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst\\_pon/software/configuration\\_guide/sec/b-gpon-config-security/preventing\\_arf\\_spoofing\\_and\\_flood\\_attack.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst_pon/software/configuration_guide/sec/b-gpon-config-security/preventing_arf_spoofing_and_flood_attack.html)
- [2] Louis Senecal, "Layer 2 Attacks and Their Mitigation", Cisco Systems, Inc.[Enligne]. Disponible : <https://www.cisco.com/c/dam/global/fr-ca/training-events/pdfs/L2-security-Bootcamp-final.pdf>
- [3] Hany EL Mokadem, "Switch Attacks and Countermeasures", Cisco Systems, Inc.[Enligne]. Disponible : [https://www.cisco.com/c/dam/en\\_us/training-events/le31/le46/cln/promo/share\\_the\\_wealth\\_contest/finalists/Hany\\_EL\\_Mokadem\\_Switch\\_Attacks\\_and\\_Countermeasures.pdf](https://www.cisco.com/c/dam/en_us/training-events/le31/le46/cln/promo/share_the_wealth_contest/finalists/Hany_EL_Mokadem_Switch_Attacks_and_Countermeasures.pdf)
- [4] E. Vyncke and C. Paggen, "LAN Switch Security : What Hackers Know About Your Switches. Indianapolis", IN : Cisco Press, 2008.
- [5] S. A. Rouiller, "Virtual LAN Security : weaknesses and countermeasures", SANS Institute InfoSec Reading Room, 2003 [Enligne]. Disponible : <https://www.sans.org/readingroom/whitepapers/networkdevs/virtual-lan-security-weaknesses-countermeasures-1090>
- [6] "VLAN-Based Network Attacks : Switching Security : LAN Switching First-Step" ,eTutorials.org. [Enligne]. Disponible : <http://etutorials.org/Networking/Lan+switching+first-step/Chapter+9.+Switching+Security/VLAN-Based+Network+Attacks/>