PROJET 4A

Projet : Émulation d'un réseau pédagogique de sécurité

Présenté par : BOU SABA Elie
NITCHEU-TCHAMI Pagès

Sous l'encadrement de : Mr.N. MBAREK

Table des matières

Liste des figures

Remerciement

Nos remerciements s’adressent à Monsieur MBAREK Nader de nous avoir introduit à ce sujet tout en nous apportant des explications tout au long du module qui nous ont permis de bien mener à ce projet et d’apprendre de nouvelles notions concernant la sécurité et la qualité des réseaux.

Introduction générale

Au cours des dernières années, l'importance des réseaux a évolué au niveau international et l'utilisation de plus en plus de cette technologie pour l'échange et la sécurité des informations à tel point qu'on ne pourrai pas imaginer notre quotidien sans l'existence des réseaux et ses divers services. En fait, l'utilisateur s'intéresse au premier lieu que les données échangées entre autres utilisateurs soient bien transmises et sécurisés.

En revanche, pour qu'un réseau soit fiable et fonctionne comme prévue il faut bien prendre en compte la sécurité informatique qui a pour rôle la protection des différentes informations qui s'échangent entre les divers équipements de ce réseau (routeurs, serveurs, ordinateurs, smartphones…) et mettre en place des méthodes pour faire face à n'importe quel type d'interruptions (usage illicite) ou attaques extérieures sur le réseau qui peuvent le menacer et le rendre vulnérable.

Chapitre 1 : État de l'art sur les attaques de sécurité

Introduction

Dans ce premier chapitre, nous avons pointé sur les différents types d'attaques qui peuvent s'induire sur notre réseau par les attaquants en donnant des exemples sur chacune de ces attaques avec les divers outils que les attaqueurs peuvent utiliser pour pirater. À la fin de ce chapitre, on a designer l'émulateur GNS3 qu'on va utiliser pour appliquer des exemples attaques dans les chapitres qui suivent.

1. Différents types d'attaques :

Il existe deux types d'attaques : Les attaques actives et les attaques passives.

• **Attaque passive :** Ce type d'attaque observe et surveille les informations qui se transmettent entre les équipements informatiques dans un réseau sans faire des modifications sur les données interceptées. Détecter les attaques passives est un défi car les informations transmises ne sont pas modifiées et donc ce n'est pas facile de savoir si quelqu'un a eu accès aux données existantes. On mentionne 2 types d'attaques passives : [2]

- La lecture des messages : Ce sont les données non encryptées et donc sont entièrement visibles pour le lecteur (conversations téléphoniques, emails…)

- Analyse du trafic : Dans le cas où les données ont passé une démarche de cryptage, l'attaquant ayant pas avoir lu les informations, peut appliquer une analyse du trafic sur le réseau en déterminant pour chacun des hôtes qui partagent de messages son identité et son emplacement et peut donc voir les différents aspects de tout ce qui s'échangent comme la fréquence des messages et leurs tailles.

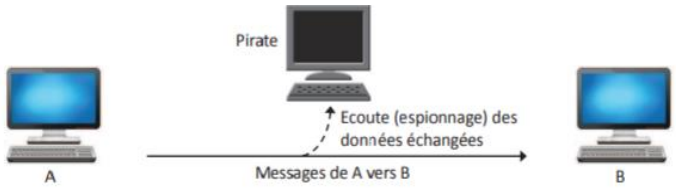


Figure 1 : Attaque passive

• **Attaque active :** Cause des modifications sur les ressources échangées ou créer puis envoyer des messages fausses et donc ce type d'attaque a un effet direct sur le système qui peut causer un fonctionnement anormal. Donc le principe de ces attaques c'est prétendre être une entité différente. Il y a plusieurs catégories des attaques actives : [2]

a) Usurpation d'identité : Le pirate joue le rôle d'une autre entité sur le réseau et commence à envoyer des messages.

Figure 2 : Usurpation d'identité

b) Rejeu : Existence de 2 phases dans cette attaque. L'attaquant capture le message envoyé par un hôte vers un autre et puis retransmet le message vers le destinataire.

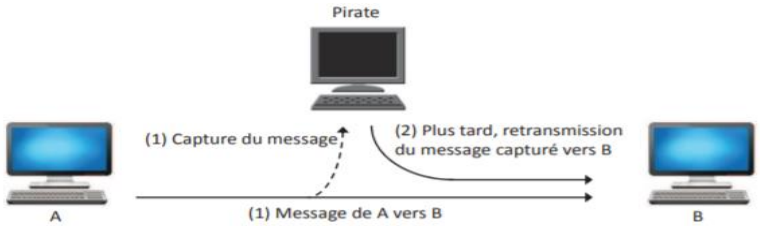


Figure 3 : Rejeu

c) Modification des messages : Il y a un changement par l'attaquant dans le contenu du message qui s'échange entre les 2 équipements.

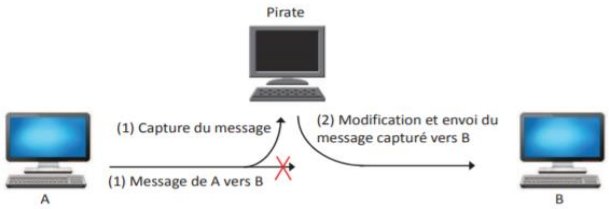


Figure 4 : Modification des messages

d) Déni de service (Interruption de service) : Cette attaque a comme but d'encombrer le service du réseau et sa performance en 2 manières : Soit l'attaquant induit la suppression des messages qui se dirigent vers le destinataire ou il envoi des messages inutiles sur le réseau pour que l'ensemble du système devient surchargé.

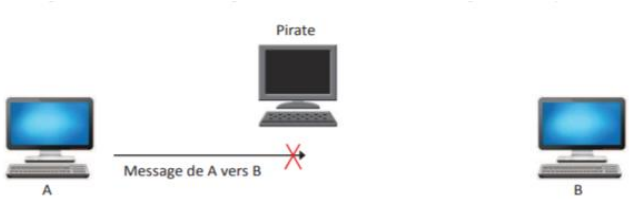


Figure 5 : Déni de service

2. Quelques exemples d'attaques :

a) DoS et DDoS : Ces deux types d'attaques connus par 'attaque par déni de service' pour DoS et 'attaque par déni de service distribué' pour DDoS appliquent presque le même principe. Ces attaques ont un effet indispensable sur le service du réseau et la connexion vers l'internet en attaquant directement un serveur relié à l'internet par exemple ce qui rend impossible pour les machines connectées au réseau d'avoir accès aux ressources installées sur le serveur et être connectées à l'internet. Ce phénomène peut être achevé en appliquant une sorte de saturation d'une machine précise en transmettant beaucoup des messages inutiles ce qui l'empêche d'offrir ces services et devient inactive. Une attaque est dite DDoS quand un déni de service est provoqué par plusieurs machines qui ont été infectés par le malware que l'attaquant à transmit et ils deviennent quelque chose appelé un 'botnet' et tous ces 'botnets' vont participer dans l'attaque vers le serveur. [2]

b) Usurpation d'identité : Cette attaque est définie comme jouer le rôle d'une autre machine en prenant sa place. On indique plusieurs exemples d'usurpations :

- Usurpation de l'adresse IP : Changer l'IP de celui qui envoie des informations en le remplacent par un autre.

- Usurpation des courriers électroniques : Remplacer l'adresse de l'expéditeur par un autre.

c) ARP spoofing et Flooding:

- ARP spoofing : L'attaquant intercepte le Protocol ARP entre deux machines et effectue des modifications de données dans la requête d'ARP et puis il la transmet vers la machine recevant cette requête. Donc les tables ARP des deux machines vont être remplis par des informations fausses qui sont bénéficiaires pour le pirate et lui permet de recevoir tous les messages envoyés par l'un des deux périphériques.

- ARP flooding : Le logiciel utilisé par le pirate va envoyer un vaste nombre de messages sur un commutateur ce qui induit la surcharge de la table ARP d'un commutateur et quand un commutateur devient surchargé il va diffuser tout le trafic réseau sur ses ports ce qui permet à l'attaquant de voire tout ce qui est transmis comme donnée sur le réseau.

d) DHCP starvation : C'est une attaque directe sur le protocole DHCP où l'attaquant va éliminer les adresses disponibles à donner par le DHCP en les réservant donc les utilisateurs du réseau vont échouer en essayant de connecter vers un réseau car ils n'auront pas d'adresses IP en utilisant le Protocol DHCP.

d) CAM overflow : Une attaque de CAM overflow s'applique lorsqu'un pirate se connecte à un ou plusieurs ports d'un commutateur puis exécute un outil qui permet la création de milliers d'adresses MAC aléatoires sur ces ports. Le commutateur va intégrer les adresses qui a reçu dans son table CAM ce qui va induire au remplissage ce cette table. Lorsqu'un commutateur est dans cet état, aucune nouvelle adresse MAC ne peut être apprise. Par conséquent, le commutateur commence à transmettre tout trafic provenant de nouveaux hôtes vers tous les ports du commutateur.

3. Etude de l'émulateur GNS3

La réussite d'une bonne implémentation d'un réseau informatique nécessite un pré travail très précis et bien détaillé sur la construction et la configuration des différentes branches de ce réseau et suivie après par des tests pour optimiser au fur et à mesure ce réseau et éviter que les erreurs encombrent les pratiques quotidiennes de l'utilisateur. Plusieurs outils sont offerts au niveau de ce travail et on mentionne le simulateur GNS3 (Graphical Network Simulator). Ce logiciel permet d'implémenter et de paramétrer des serveurs, commutateurs, routeurs... et effectuer des tests sur ces composants. Cependant, le simulateur GNS3 permet en effet de connecter également notre hyperviseur de machines virtuelles depuis VMWare ou VirtualBox et donc nous pourrions architecturer un réseau complexe et le simuler virtuellement.

Conclusion

En conclusion, on indique que les pirates se placent dans 2 catégories. On a les experts qui forment la minorité et l'autre type sont les amateurs qui prennent l'avantages des aides et des outils(logiciels) pour succéder dans leurs attaques et donc bénéficier soit du part de vol d'informations qui sont personnelles ou confidentielles et parfois gouvernementaux soit pour voler d'argent (voler la clé des cartes bancaires par exemple)

Chapitre 2 : Application de quelques attaques à notre réseau et mettre en place les remèdes :

Introduction

Dans ce second chapitre, nous avons appliqués 3 attaques différentes (ARP spoofing, DHCP starvation, Cam overflow) en mettant un remède pour chaque attaque dans le but de protéger notre réseau de se piratage. Pour achever ces attaques, nous avons utilisé l'émulateur GNS3 qui nous a permis d'implémenter un réseau composé d'un pirate (Kali Linux), de 2 PCs clients, d'un routeur et d'un commutateur.

1. ARP spoofing :

a) Attaque :

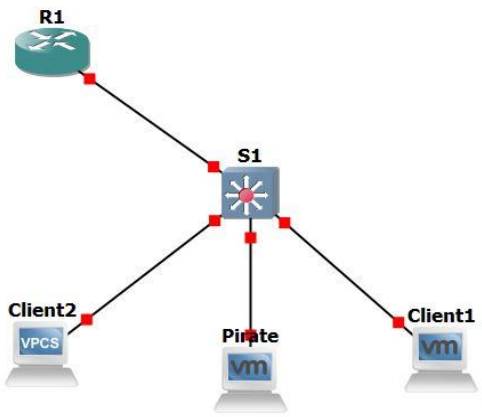
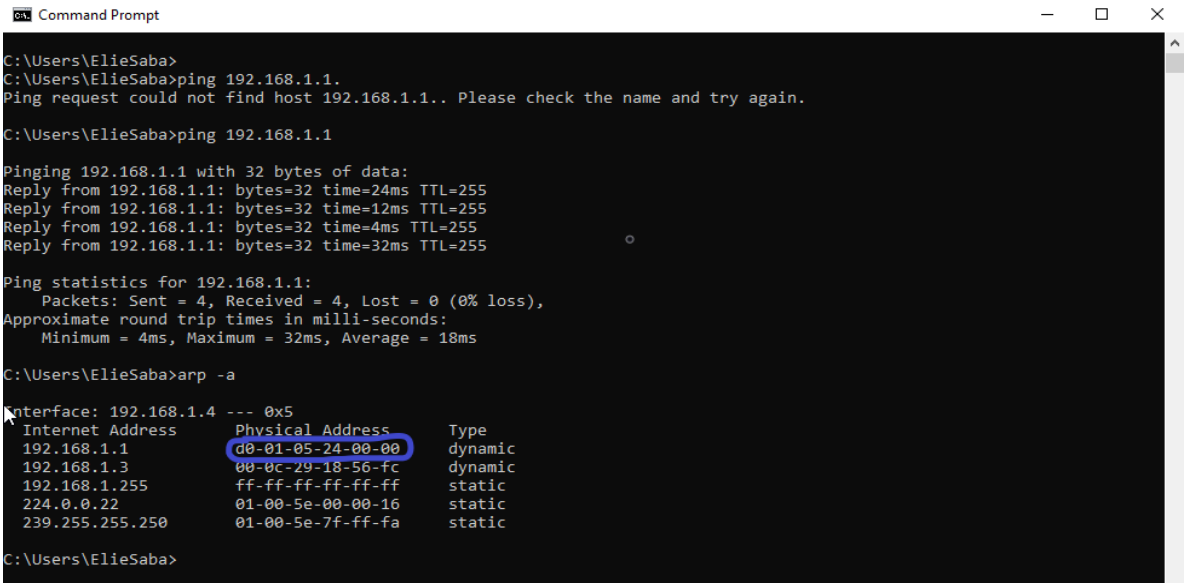


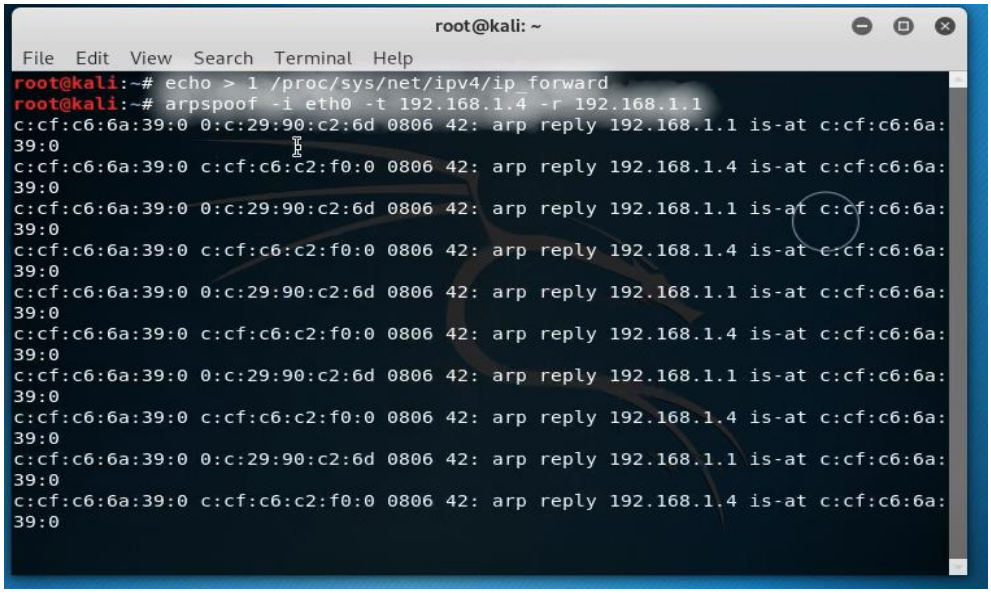
Figure 6 : Le réseau informatique



```
C:\Users\ElieSaba>
C:\Users\ElieSaba>ping 192.168.1.1.
Ping request could not find host 192.168.1.1.. Please check the name and try again.

C:\Users\ElieSaba>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=24ms TTL=255
Reply from 192.168.1.1: bytes=32 time=12ms TTL=255
Reply from 192.168.1.1: bytes=32 time=4ms TTL=255
Reply from 192.168.1.1: bytes=32 time=32ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 32ms, Average = 18ms

C:\Users\ElieSaba>arp -a

Interface: 192.168.1.4 --- 0x5
  Internet Address      Physical Address      Type
  192.168.1.1           d0-01-05-24-00-00     dynamic
  192.168.1.3           00-0c-29-18-56-fc     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

C:\Users\ElieSaba>
```

Figure 7 : Affichage de la table des adresses MAC

Dans la figure (7) nous avons appliqué la commande ‘arp -a’ sur le client Windows pour accéder au ARP cache et voir les adresses MAC du routeur R1 qu’on va remplacer par l’adresse MAC du pirate pour qu’il reçoit tous les paquets envoyés par le client Windows vers le routeur.



```
root@kali:~# echo > 1 /proc/sys/net/ipv4/ip_forward
root@kali:~# arpspoof -i eth0 -t 192.168.1.4 -r 192.168.1.1
c:cf:c6:6a:39:0 0:c:29:90:c2:6d 0806 42: arp reply 192.168.1.1 is-at c:cf:c6:6a:
39:0
c:cf:c6:6a:39:0 c:cf:c6:c2:f0:0 0806 42: arp reply 192.168.1.4 is-at c:cf:c6:6a:
39:0
c:cf:c6:6a:39:0 0:c:29:90:c2:6d 0806 42: arp reply 192.168.1.1 is-at c:cf:c6:6a:
39:0
c:cf:c6:6a:39:0 c:cf:c6:c2:f0:0 0806 42: arp reply 192.168.1.4 is-at c:cf:c6:6a:
39:0
c:cf:c6:6a:39:0 0:c:29:90:c2:6d 0806 42: arp reply 192.168.1.1 is-at c:cf:c6:6a:
39:0
c:cf:c6:6a:39:0 c:cf:c6:c2:f0:0 0806 42: arp reply 192.168.1.4 is-at c:cf:c6:6a:
39:0
c:cf:c6:6a:39:0 0:c:29:90:c2:6d 0806 42: arp reply 192.168.1.1 is-at c:cf:c6:6a:
39:0
c:cf:c6:6a:39:0 c:cf:c6:c2:f0:0 0806 42: arp reply 192.168.1.4 is-at c:cf:c6:6a:
39:0
c:cf:c6:6a:39:0 0:c:29:90:c2:6d 0806 42: arp reply 192.168.1.1 is-at c:cf:c6:6a:
39:0
c:cf:c6:6a:39:0 c:cf:c6:c2:f0:0 0806 42: arp reply 192.168.1.4 is-at c:cf:c6:6a:
39:0
```

Figure 8 : Exécution de l'attaque par Kali Linux

Ensuite, on a exécuté la commande ‘arpspoof -i eth0 -t 192.168.1.4 -r 192.168.1.1’ sur le logiciel kali linux qui est le pirate et qui permet d’envoyer des messages ARP vers le client Windows et lui donne des informations incorrectes concernant le routeur et par la suite le mac adresse de l’ip ‘192.168.1.1’ qui est ‘d0-01-05-24-00-00’ du routeur va être remplacé par le mac adresse du pirate qui est ’00-0c-29-18-56-fc’.

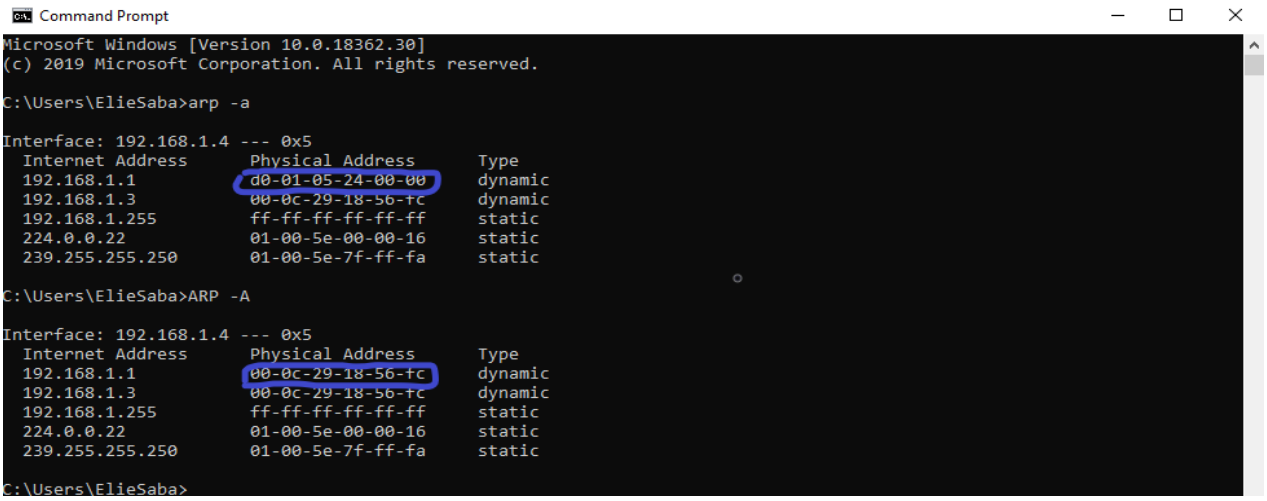


Figure 9 : Affichage du tableau des adresses MAC

On remarque qu’après l’attaque, le mac adresse de l’ip du routeur a été remplacé par celui du pirate pour le client Windows.

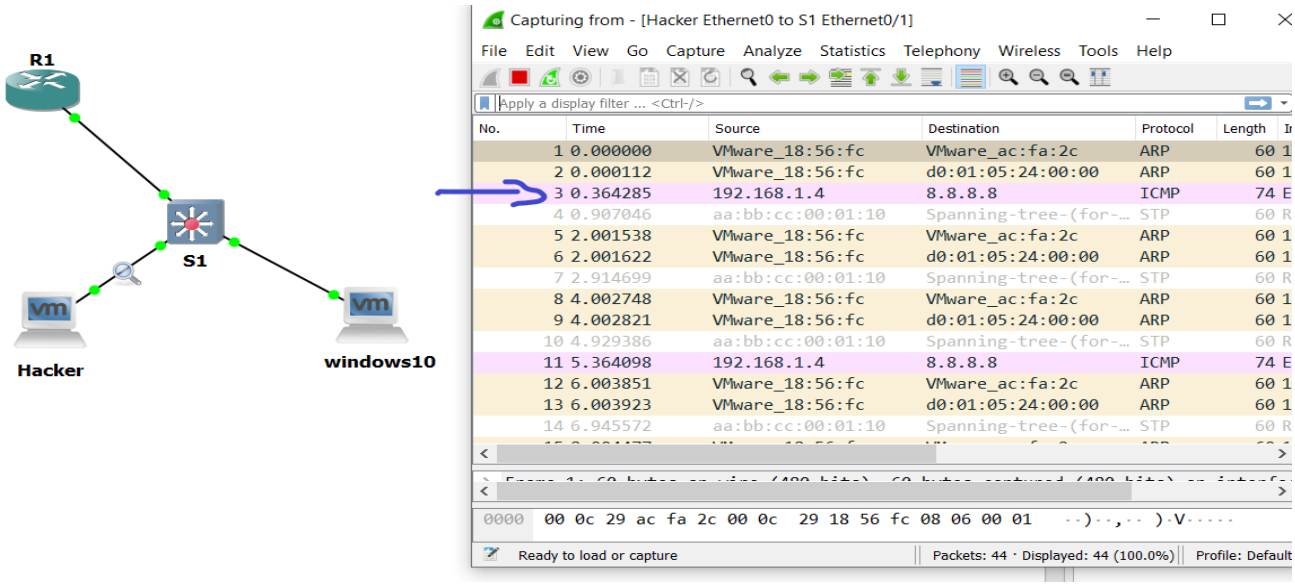


Figure 10 : Surveillance de la liaison entre le commutateur et le pirate

En plus, nous avons capturé le lien connectant le commutateur s1 et le pirate, et on remarque bien que quand le client Windows envoi des paquets vers le routeur R1, ces paquets vont arriver vers le pirate.

b) Remède pour cette attaque : DAI (Dynamic ARP inspection)

Cette fonction nécessite DHCP snooping qui possède une base de données fiable contenant les liaisons d'adresses IP à MAC et donc L'inspection ARP dynamique détermine la validité d'un paquet ARP en la comparant avec celle qui est stockée dans la base de données du DHCP snooping.

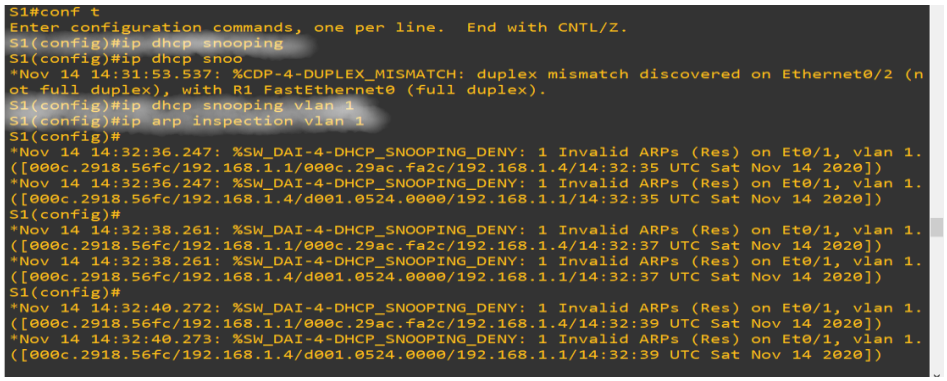


Figure 11 : Application du remède pour l'attaque

L’exécution des commandes marqués en blanc va permettre au commutateur S1 d’utiliser la fonction DHCP snooping et après on va implémenter l’inspection ARP dynamique.

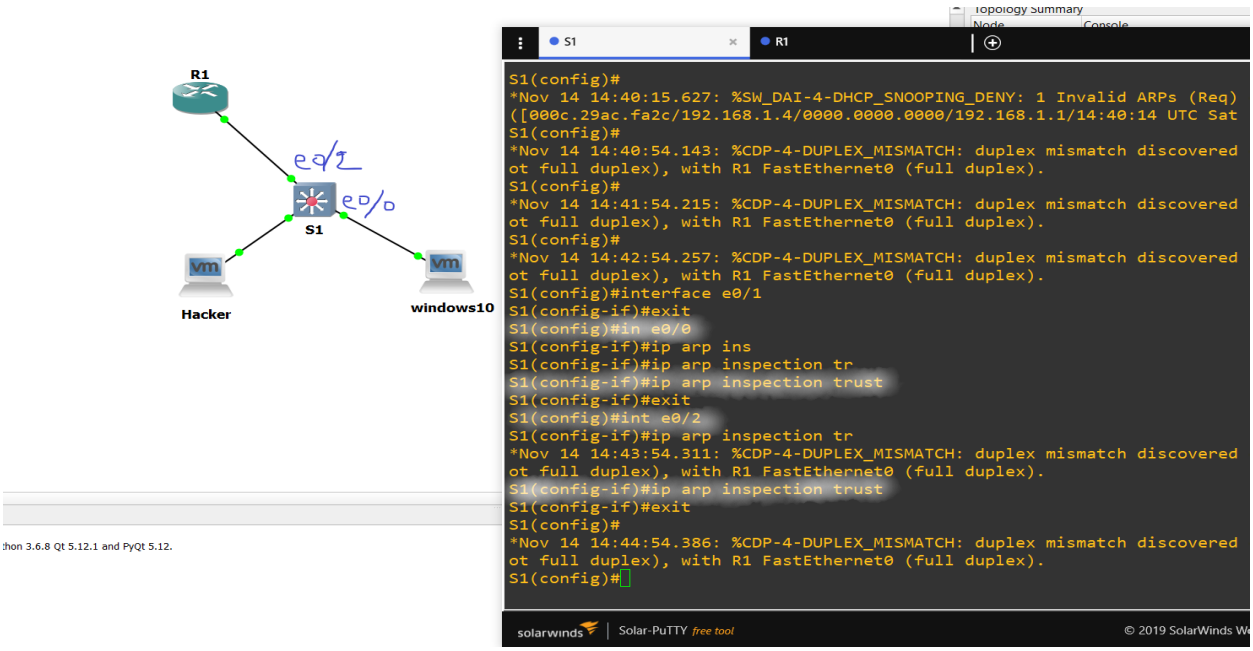


Figure 12 : Application du remède pour l'attaque

Après ça, on va choisir les ports qu'on les fait confiance. Dans notre architecture on va donner confiance à tous les ports du commutateur en excluant le port liant le commutateur au pirate. Cependant, les ARP réponses ou demandes qui arrivent sur le port exclus du commutateur vont obligatoirement passer par le test de l'inspection ARP dynamique qui compare l'ARP et l'ip de l'équipement avec celle qui se trouve dans la base de données du DHCP snooping et si l'ARP ne convient pas, le commutateur va la refuser.

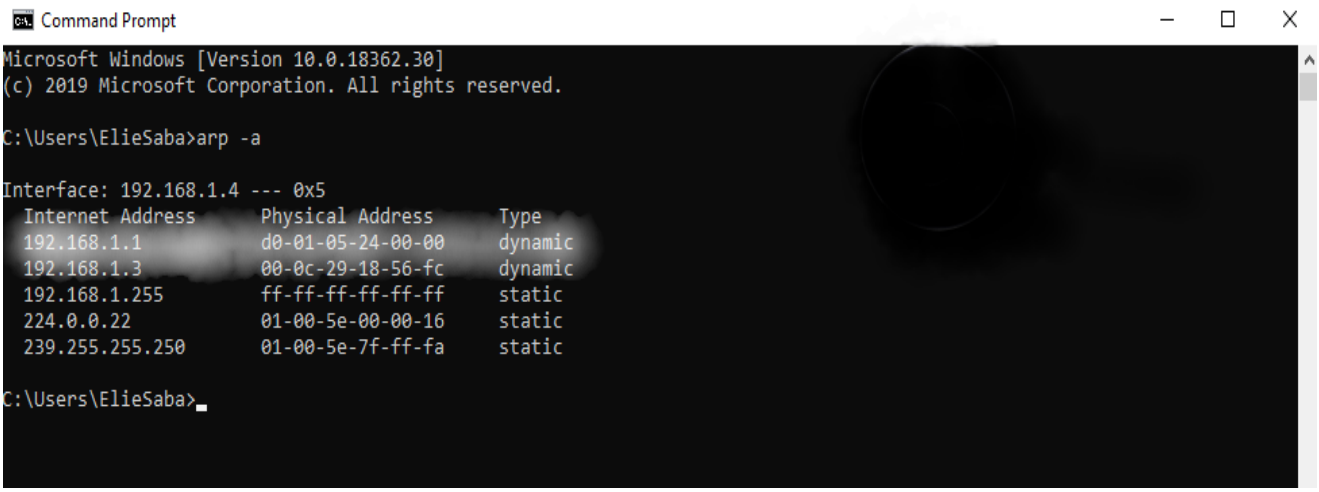


Figure 13 : Affichage de la table des adresses MAC

Après la mise en place de cette fonction de sécurité, l'adresse MAC du routeur dans le MAC cache du client Windows est celle qui convient et par la suite l'adresse n'a pas changer après l'attaque appliqué par le pirate donc on a bien sécurisé le réseau des attaques d'ARP spoofing.

2. DHCP starvation :

a) Attaque :

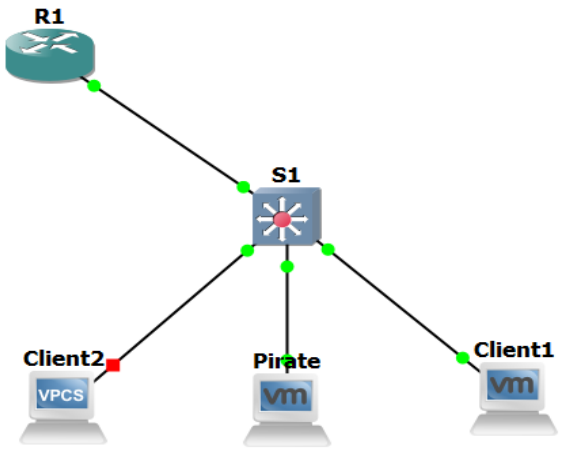


Figure 14 : Le réseau informatique

Dans la figure (14) on a le router R1 configuré avec le service DHCP. Le pirate et le client1 ont déjà eu une adresse ip du router en utilisant le service DHCP. Maintenant, on va faire l'attaque DHCP starvation par le pirate pour saturer tous les ip adresses du DHCP disponibles et empêcher le client2 d'accéder au réseau car il ne va pas avoir un ip du DHCP.

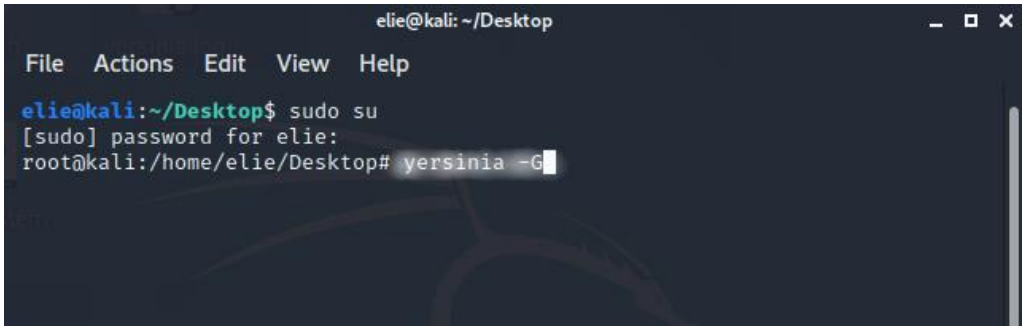


Figure 15 : Lancement du logiciel 'yersinia' pour faire l'attaque

Sur Kali Linux, on a exécuté la commande 'yersinia -G' pour ouvrir le logiciel 'Yersinia' qu'on utilise pour faire l'attaque.

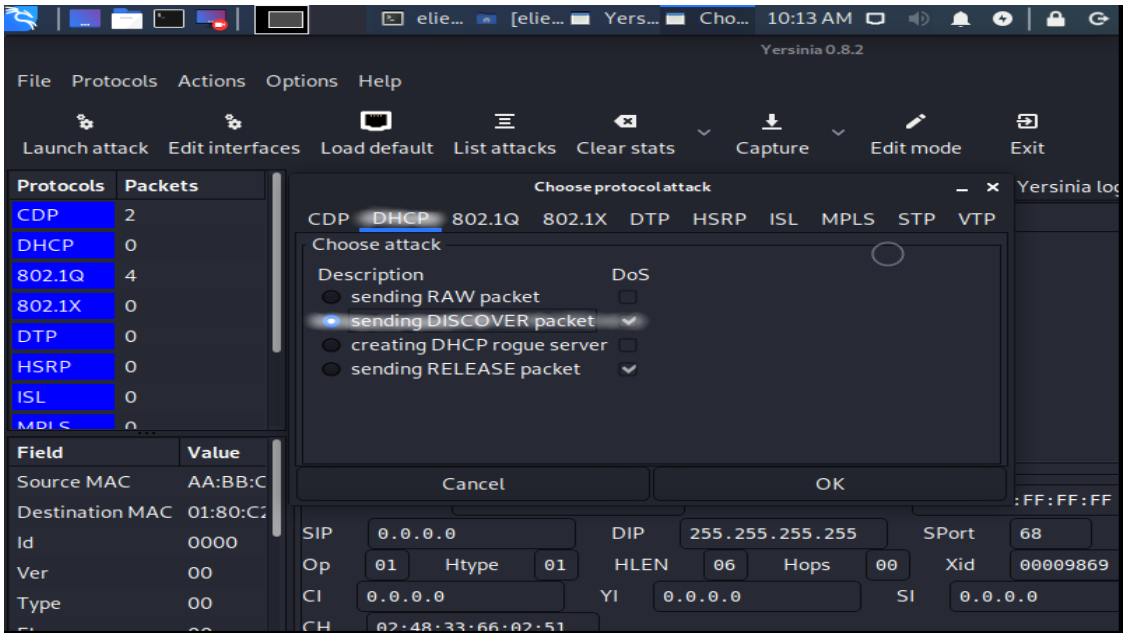


Figure 16 : Exécution de l'attaque en utilisant l'outil 'yersinia'

Ensuite, on a choisi d'envoyer des paquets de découverte DHCP dans le logiciel 'Yersinia' et cela va créer des adresses MAC en les implémentant dans les paquets de découverte pour prendre tous les adresses ip disponibles du DHCP du router.

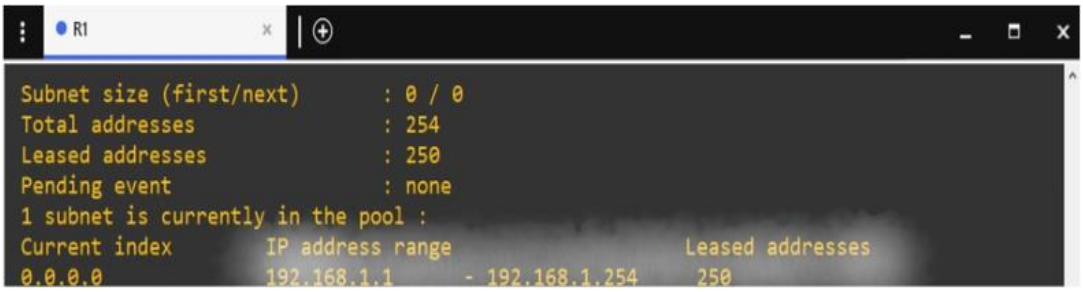


Figure 17 : Affichage des adresses ip loués par DHCP

Après l'attaque, on remarque que tous les ip adresses qui étaient disponibles ne sont plus et par la suite, le client2 ne pourra pas prendre un ip adresse pour se connecter au réseau.

b) Remède pour cette attaque :

```
S1(config-if)#switch mode access
S1(config-if)#switch port-security
S1(config-if)#switch port-security mac-address sticky
S1(config-if)#swic
*Nov 21 16:22:54.759: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet0/2 (n
ot full duplex), with R1 FastEthernet0 (full duplex).
S1(config-if)#switch port-security max 1
S1(config-if)#
```


Figure 18 : Application du remède pour cette attaque

Pour interdire une attaque de DHCP starvation, il faut limiter le nombre d'adressés MAC permis à diffuser sur une interface du commutateur et on réalise ça par les commandes executés dans la figure (18)

3. CAM overflow:

a) Attaque:

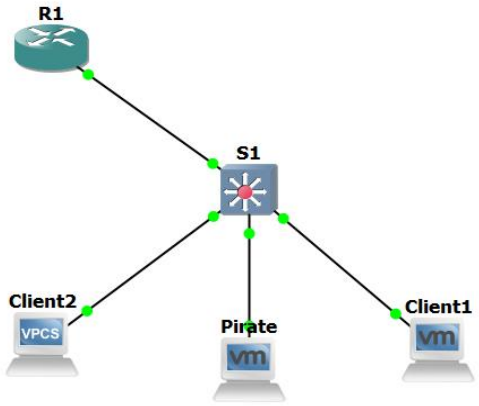


Figure 19 : Le réseau informatique

```
S1#show mac address-table count

Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count  : 5
Static  Address Count  : 0
Total Mac Addresses    : 5

Total Mac Address Space Available: 176842276

S1#
```


Figure 20 : Affichage du nombre total d'adresses MAC possibles à apprendre par le commutateur

Nous remarquons qu'après l'exécution de la commande 'show mac address-table count' le nombre total d'adresses MAC que le commutateur peut remplir et appréhender est limité à un nombre précis qui est de 176842276 adresses MAC pour notre commutateur.

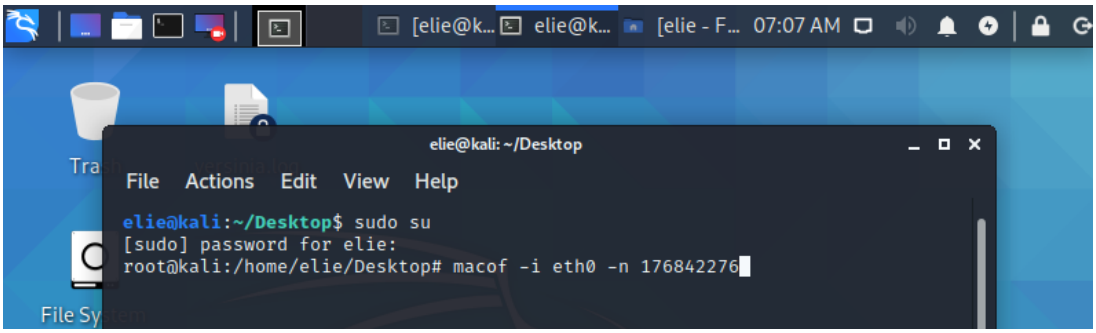


Figure 21 : Exécution de l'attaque par Kali Linux

Dans la figure (21) nous avons appliqué la commande 'macof -i eth0 -n 176842276' qui va envoyer des adresses MAC aléatoires sur l'interface ethernet0 qui vont saturer le commutateur et cela va induire le fait que le commutateur ne pourra plus apprendre des nouvelles adresses MAC des équipements et va donc diffuser les paquets reçus sur une interface vers toutes les équipements connectés sur les différentes interfaces du commutateur.

b) Remède pour cette attaque :

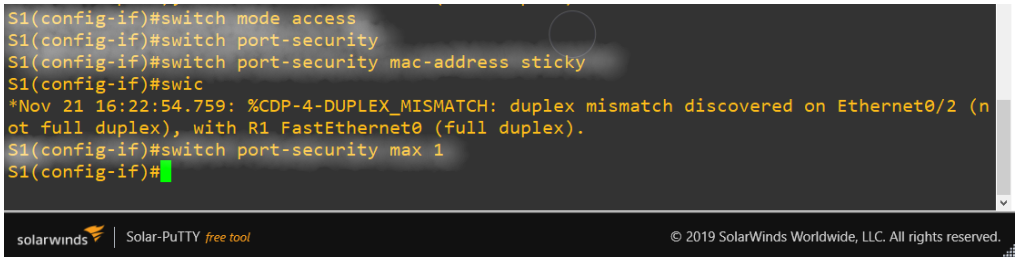


Figure 22 : Mettre en place le remède pour cette attaque

Pour interdire une attaque de CAM overflow, il faut limiter le nombre d'adresses MAC permis à diffuser sur une interface du commutateur et on réalise ça par les commandes exécutées dans la figure (22)

Conclusion

Pour conclure, on remarque qu'il y a une solution pour sécuriser notre réseau contre n'importe quelle attaque qui peut se passer et empêcher les pirates l'infraction de notre infrastructure informatique en implémentant les remèdes précises et possibles pour chaque type d'attaque effectué par l'attaquant sur notre réseau.

Conclusion Générale

Finalement, les données informatiques qui existent et circulent entre les différents équipements du réseau peuvent être très précieuse et par la suite ces informations doivent être bien sécurisé pour empêcher toute intrusion qui provoque des surcoûts considérables pouvant mettre en péril l'intégrité du système informatique.

En outre, sécuriser le système informatique est une tâche assez complexe parce qu'on ne peut pas prévoir les types d'attaques qui peuvent endommager notre système et donc il est totalement nécessaire d'être prêt à n'importe quel type d'attaque en intégrant au système les remèdes possibles pour garantir en permanence la confidentialité, l'intégrité, l'authentification et disponibilité du système.

Références bibliographiques

[1] https://openclassrooms.com/fr/courses/2581701-simulez-des-architectures-reseaux-avec-gns3

[2] https://yd-fsm.weebly.com/uploads/4/6/7/1/46716243/cours_mr2_ch1.pdf

[3] https://waytolearnx.com/2018/07/difference-entre-attaque-active-et-attaque-passive.ht

Annexe

Tutoriel d'installation et guide d'utilisation de l'émulateur GNS3 :

Bénéficier des fonctionnalités applicables dans l'émulateur GNS3 nécessite l'utilisation des 2 composants essentiels : Windows client et la machine virtuelle GNS3. Windows client s'exécute localement sur le système d'exploitation. La machine virtuelle c'est Ubuntu qui s'installe sur VMWare Workstation Pro ou sur VirtualBox. On utilise l'interface graphique de GNS3 implémenté sur le client Windows pour contrôler la machine virtuelle.

Installation et utilisation de GNS3 GUI application :

- Télécharger l'application GNS3 GUI du site : www.gns3.com

- Choisir les outils que vous souhaitez télécharger avec l'application GUI GNS3 :

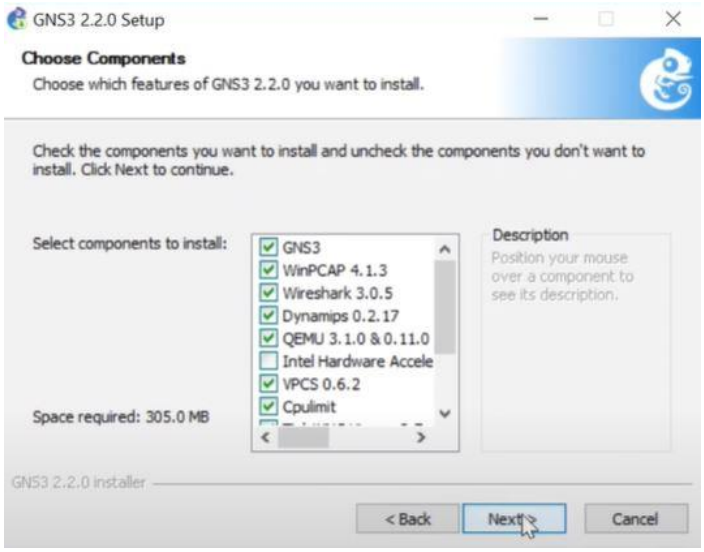


Figure 23 : Services téléchargeables avec GNS3

- Télécharger VMware Workstation Pro du site : www.vmware.com

- Télécharger la machine virtuelle GNS3 du site : www.gns3.com (la version de la machine virtuelle doit obligatoirement être la même que la version de l'application GUI GNS3)

- Lancer l'application VMware Workstation Pro et ouvrir le fichier contenant la machine virtuelle GNS3

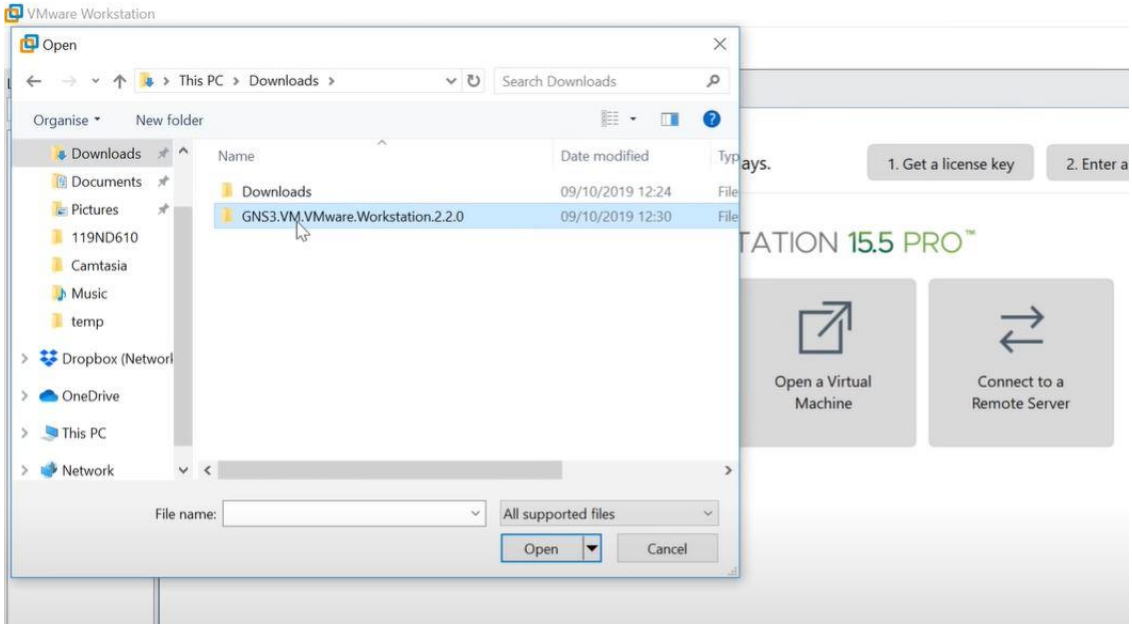


Figure 24 : Lien entre VMware Workstation pro et la machine virtuelle GNS3

- Fermer VMware Workstation Pro et lancer l'application GNS3 GUI pour faire le lien entre l'application et la machine virtuelle GNS3 intégrée dans VMware Workstation Pro.

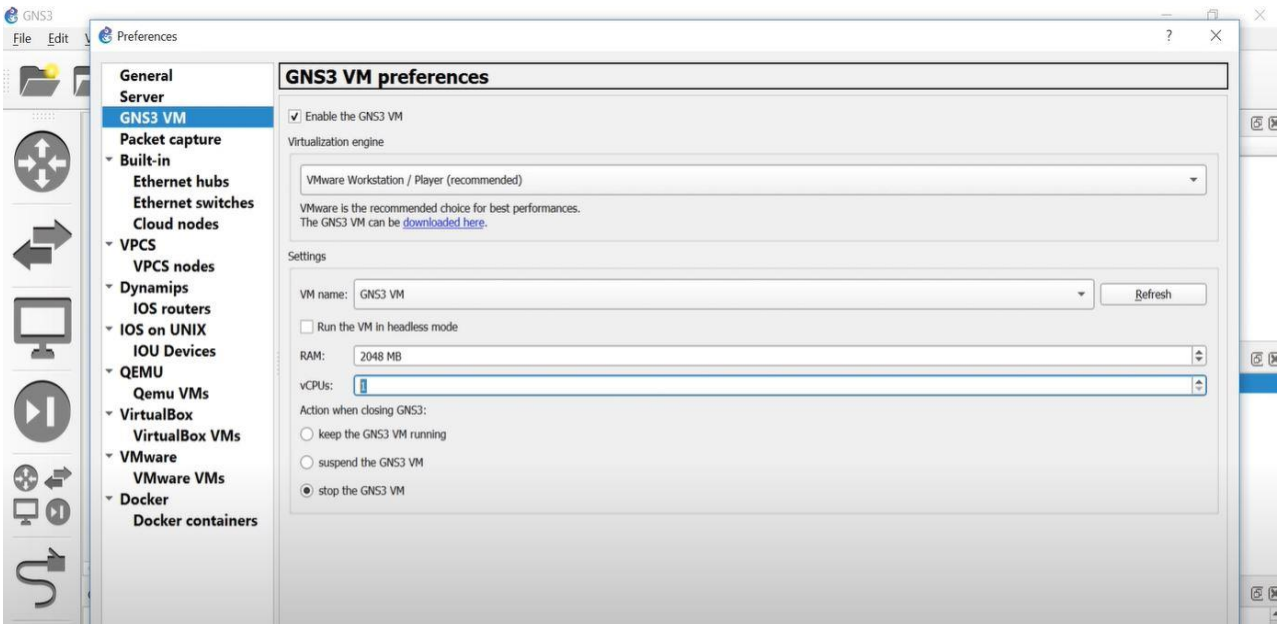


Figure 25 : Lien entre L'application GNS3 GUI et la machine virtuelle GNS3

- Implémenter des équipements Cisco en téléchargeant leurs images et les faire ajouter dans l'application GNS3 GUI qui va les installer sur la machine virtuelle GNS3.

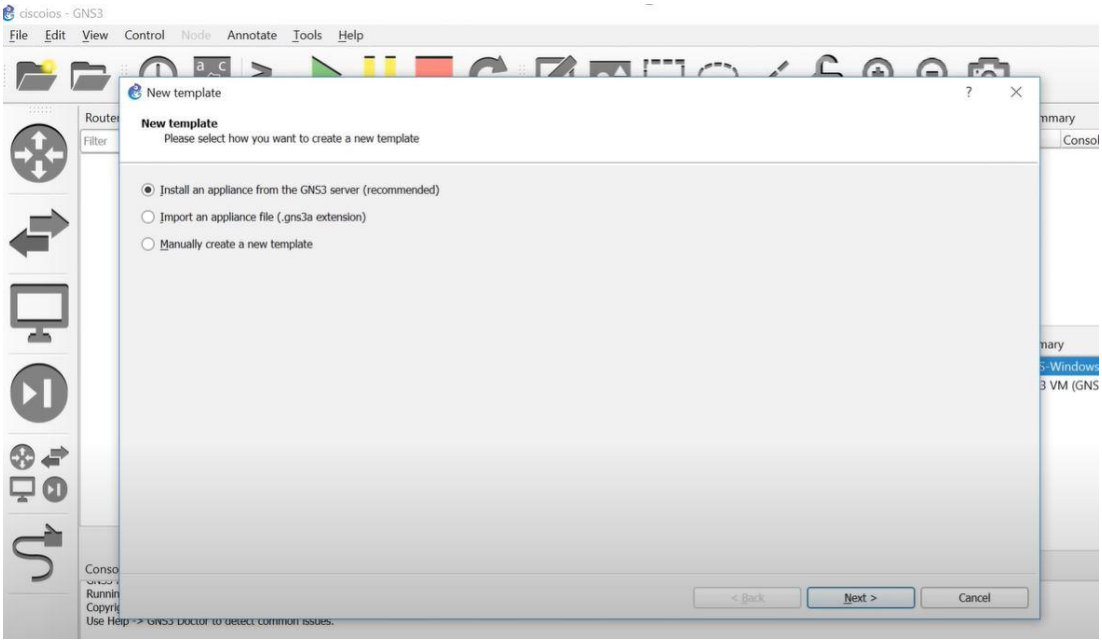


Figure 26 : Ajout des équipements Cisco