



Projet de l'Administration Système

Sujet :

Dynamic Host Configuration Protocol

« DHCP »

Filière:

GENIE INFORMATIQUE _ PROMO-18

SOUTENU PAR :

- ALIANI Mohamed
- BARGA Saad
- MEZINE Aomar
- ZEROUK EL Mehdi

Sous la direction de :

- Mme ZAYDI Mounia

Remerciement

Dans le cadre de ce travail, nous tenons à saisir l'occasion pour remercier du fond du cœur tous ceux qui ont participé à la réalisation de ce projet et qui en ont contribué à en faire une expérience enrichissante, en particulier notre encadrante Mme **ZAYDI Mounia** pour son engagement.

Résumé

Ce travail a été réalisé dans le cadre de l'élément administration système. Ce projet a pour but d'installer et configurer un serveur DHCP et le sécuriser en anticipant les diverses attaques auxquelles celui-ci peut être confronté.

Nous donnerons en première étape le contexte général du projet. Dans la deuxième étape, nous introduirons le DHCP afin d'avoir une idée précise sur son rôle et son fonctionnement.

La troisième étape aura pour but d'assurer l'installation et configuration du serveur DHCP sur notre machine virtuelle.

Quatrièmement, on identifiera les diverses vulnérabilités liées au DHCP. Cela nécessitera une documentation sur les sources de menaces au DHCP puis une simulation d'attaque (DHCP Rogue Server).

Dans la dernière étape, nous citerons une mesure de sécurité ainsi que sa configuration sur Cisco Packet Tracer afin de contrer ces attaques et éviter toute fuite d'informations sensibles des clients DHCP.

Abstract

This work was done as part of the system administration element. This project aims to install and configure a DHCP server and secure it by anticipating the various attacks it may face.

We will first give the general context of the project. In the second step, we will introduce the DHCP in order to have a precise idea on its role and its operation.

The third step will aim to ensure the installation and configuration of the DHCP server on our virtual machine.

Fourth, we will identify the various vulnerabilities related to DHCP. This will require documentation of the sources of threats to DHCP and then an attack simulation (DHCP Rogue Server).

In the last step, we will cite a security measure as well as its configuration on Cisco Packet Tracer in order to counter these attacks and avoid any leakage of sensitive information from DHCP clients.

Table de Figures

Figure 0 : Les étapes d'attribution d'une adresse IP.....	14
Figure 1 : Installation DHCP.....	17
Figure 2 : Backup server file	17
Figure 3 : Adresse IP de la machine	17
Figure 4 : Accès au fichier DHCP	17
Figure 5 : Attribution des adresses IP aléatoires	18
Figure 6 : Attribution d'une adresse IP statique au client	18
Figure 7 : Liaison du serveur à une interface	19
Figure 8 : Redémarrage du serveur DHCP	19
Figure 9 : Vérification du statut du serveur DHCP	20
Figure 10 : Vérification du statut du serveur DHCP	20
Figure 11 : Vérification du statut du serveur DHCP	20
Figure 12 : Vérification du statut du serveur DHCP	21
Figure 13 : Vérification du statut du serveur DHCP	21
Figure 14 : Vérification du statut du serveur DHCP	21
Figure 15 : Attribution d'une adresse IP a un client	21
Figure 16 : DHCP starvation attack	23
Figure 17 : Rogue DHCP server attack	24
Figure 18 : Installation de Yersinia	25
Figure 19 : La commande Yersinia -h	25
Figure 20 : La commande Yersinia -G.....	26
Figure 21 : Launch attack	26
Figure 22 : Sending discover packet	27
Figure 23 : Résultat de l'attaque	27

Figure 24 : Creating DHCP rogue server.....	28
Figure 25 : Fenêtre de configuration de DHCP rogue server	29
Figure 26 : DHCP sans rogue server	29
Figure 27 : Configuration de serveur DHCP légitime	30
Figure 28 : DHCP avec rogue server	30
Figure 29 : Configuration de serveur DHCP rogue	31
Figure 30 : La réussite de l'attaque	31
Figure 31 : DHCP Snooping.....	33
Figure 32: Configuration DHCP snooping	35
Figure 33: Configuration DHCP snooping actif	35
Figure 34: Unable to get IP adresse	36
Figure 35 : Configuration des ports de confiance	37
Figure 36 : La réussite de la configuration	37
Figure 37-1 : Pc connecté au serveur légitime.....	37
Figure 37-2 : Pc connecté au serveur légitime.....	38
Figure 38: DHCP binding	38
Figure 39: DHCP rate limit.....	39

Tables de Matières

Tables de figures	6
Tables de matières.....	8
Introduction	9
Chapitre 1 : Contexte générale de projet.....	10
1. Problématique.....	11
2. Description de projet	11
3. Objectif générale de projet.....	11
Chapitre 2 : DHCP Dynamic Host Configuration Protocol	12
1. Définition.....	13
2. Les composants du protocole	13
3. Fonctionnement.....	14
4. Les avantages de DHCP	15
Chapitre 3 : Installation et configuration.....	16
1. Installation du serveur DHCP	17
2. Configuration du serveur DHCP	17
3. Configuration des clients	20
Chapitre 4 : Identification de vulnérabilités liées à DHCP.....	22
I. Sources de menaces	23
1. DHCP starvation attack	23
2. Rogue DHCP Server attack	24
II. Simulation de l'attaque.....	24
1. Installation de Framework yersinia	25
2. DHCP starvation attack.....	26
3. Configuration DHCP rogue server	28
4. Configuration du rogue server sous Packet Tracer	29
Chapitre 5 : Mesures de sécurité pour un usage plus sûr de DHCP	32
1. DHCP Snooping	33
2. Configuration de DHCP Snooping	35
Conclusion.....	40
Bibliographie.....	41

INTRODUCTION :

Face au développement de l'internet et l'émergence des nouvelles technologies lors de cette dernière décennie, le nombre de machines connectées sur un même réseau a rapidement évolué. Or les entreprises utilisent leurs réseaux en permanence. Ils doivent alors être toujours disponibles et garantir la qualité du service. Afin d'assurer la connectivité de toutes les machines, il n'est donc pas possible de leur attribuer manuellement chacun sa propre adresse IP et pouvoir gérer toutes les modifications au sein du réseau. D'où la création du protocole DHCP face au besoin d'un protocole qui va manager l'adressage IP et de manière automatique.

Ce rapport est divisé en deux parties. La première partie contient le premier chapitre, contexte général du projet. Tandis que la deuxième partie sera consacrée entièrement à la conception et réalisation du projet. Cette partie comporte les quatre chapitres restants. Nous verrons d'abord le principe de fonctionnement du DHCP suivi de la configuration du serveur DHCP sur la distribution Linux UBUNTU. Ensuite, on entamera par les attaques sur le serveur DHCP afin de finir par la configuration d'une mesure qui va sécuriser ce serveur.

Chapitre 1

Contexte général du projet

1. Problématique :

De nos jours, le nombre de machines connecté sur un même réseau a grandement augmenté en l'espace de quelques années. Pour assurer la connexion de la totalité des machines tout en gérant le flux des machines entrantes et sortantes, il faudrait avoir des adresses IP disponibles en permanence. Or l'épuisement des adresses IP engendrera plusieurs problèmes surtout au sein de l'entreprise à laquelle cela va coûter cher en temps et argent. D'où la nécessité et l'urgence de mettre en œuvre un protocole qui va pouvoir distribuer les adresses IP automatiquement, gérer le flux des machines et leur configuration à chaque connexion. Néanmoins, une simple configuration du serveur n'est pas suffisante. Il faudrait trouver des moyens pour sécuriser toutes ces données transmises au client pour éviter la pénétration d'un serveur Rogue et le vol de ces informations sensibles.

2. Description du projet :

Afin d'assurer l'attribution automatique des adresses IP, un protocole de gestion du réseau est nécessaire.

C'est dans ce cadre que s'inscrit notre projet. Il s'agit de l'installation et configuration d'un protocole qui va gérer les adresses IP du réseau, nommé DHCP (Dynamic Host Configuration Protocol) et sa sécurisation par la suite.

3. Objectif général du projet :

L'objectif du projet en premier lieu est d'installer et de configurer le serveur DHCP sur Ubuntu. Et en second lieu, on va identifier les différentes attaques qui visent le serveur et mettre en œuvre une mesure de sécurité pour un usage plus sûr du DHCP.

Chapitre 2

DHCP «Dynamic Host Configuration Protocol »

1 – Définition du protocole DHCP

DHCP signifie Dynamic Host Configuration Protocol. Il s'agit d'un protocole qui permet à un ordinateur qui se connecte sur un réseau local d'obtenir dynamiquement et automatiquement sa configuration IP. Le but principal étant la simplification de l'administration d'un réseau. On voit généralement le protocole DHCP comme distribuant des adresses IP, mais il a été conçu au départ comme complément au protocole BOOTP (Bootstrap Protocol) qui est utilisé par exemple lorsque l'on installe une machine à travers un réseau (on peut effectivement installer complètement un ordinateur, et c'est beaucoup plus rapide que de le faire en à la main). Cette dernière possibilité est très intéressante pour la maintenance de gros parcs machines. Les versions actuelles des serveurs DHCP fonctionnent pour IPv4 (adresses IP sur 4 octets). Une spécification pour IPv6 (adresses IP sur 16 octets) est en cours de développement par l'IETF.

2 – Les composants du protocole

Pour utiliser le DHCP, il est important de comprendre tous ses composants. Voici leur liste :

- **Serveur DHCP** : appareil en réseau exécutant le service DHCP qui contient les adresses IP et les informations de configuration associées.
- **Client DHCP** : le point de terminaison qui reçoit les informations de configuration du serveur.
- **Pool d'adresses IP** : plage d'adresses disponibles pour les clients DHCP.
- **Sous-réseau** : les réseaux IP peuvent être partitionnés en segments appelés sous-réseaux. Ces sous-réseaux aident à garder les réseaux gérables.
- **Location** : la durée pendant laquelle un client DHCP détient les informations d'adresse IP.
- **Relais DHCP** : routeur ou hôte, il reçoit les messages clients diffusés sur ce réseau, puis les transmet à un serveur configuré.

3 – Fonctionnement

DHCP fonctionne sur le modèle client-serveur : un serveur, qui détient la politique d'attribution des configurations IP, envoie une configuration donnée pour une durée donnée à un client donné (typiquement, une machine qui vient de démarrer). Le serveur va servir de base pour toutes les requêtes DHCP (il les reçoit et y répond), aussi doit-il avoir une configuration IP fixe. Dans un réseau, on peut donc n'avoir qu'une seule machine avec adresse IP fixe : le serveur DHCP. Le protocole DHCP s'appuie entièrement sur BOOTP : il en reprend le mécanisme de base (ordre des requêtes, mais aussi le format des messages). DHCP est une extension de BOOTP.

Quand une machine vient de démarrer, elle n'a pas de configuration réseau (même pas de configuration par défaut), et pourtant, elle doit arriver à émettre un message sur le réseau pour qu'on lui donne une vraie configuration. La technique utilisée est le broadcast : pour trouver et dialoguer avec un serveur DHCP, la machine va simplement émettre un paquet spécial, dit de broadcast, sur l'adresse IP 255.255.255.255 et sur le réseau local. Ce paquet particulier va être reçu par toutes les machines connectées au réseau (particularité du broadcast). Lorsque le serveur DHCP reçoit ce paquet, il répond par un autre paquet de broadcast contenant toutes les informations requises pour la configuration. Si le client accepte la configuration, il renvoie un paquet pour informer le serveur qu'il garde les paramètres, sinon, il fait une nouvelle demande.

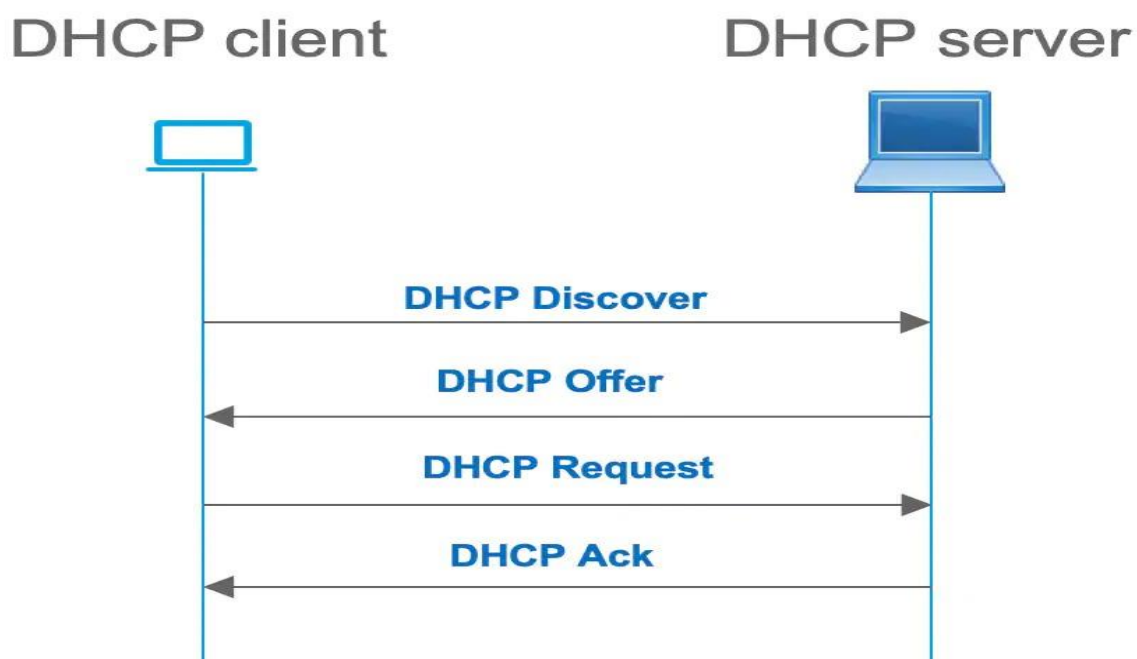


Figure 0 : les étapes d'attribution d'une adresse IP

4 – Les avantages de DHCP

L'un des principaux avantages de l'utilisation de DHCP est la gestion plus facile des adresses IP. Par rapport à d'autres solutions réseau, il permet de configurer un réseau TCP/IP plus rapidement. Ce protocole simplifie l'administration en fournissant aux clients des adresses IP, avec les adresses de la passerelle par défaut, des serveurs DNS, des serveurs WINS et d'autres serveurs utiles au client.

En attribuant des adresses IP automatiquement, les développeurs peuvent se charger des tâches plus transformatrices, plutôt que de perdre du temps aux configurations manuelles.

L'utilisation de ce pool permet également d'éviter les conflits d'adresses qui surviennent quand la même adresse IP est attribuée par erreur à deux hôtes. Il prend en charge tout système d'exploitation, avec une assistance client axée sur PC et Mac. DHCP est particulièrement avantageux pour les réseaux avec des millions de clients DHCP, via le multithreading, ces administrateurs peuvent traiter simultanément de nombreuses demandes de clients.

Chapitre 3

Installation et configuration du DHCP

1- Installation du serveur DHCP

Pour installer *dhcpcd*, exécutez la commande *apt* suivante dans le terminal :

```
aomarmezine@aomarmezine-ubuntu:~$ sudo apt install isc-dhcp-server
[sudo] password for aomarmezine:
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

Figure 1 : Installation DHCP

2- Configuration du serveur DHCP

On sauvegarde les fichiers de configuration d'origine. En cas de problème, la configuration d'origine peut facilement être restaurée. On utilise ci-dessous la commande *cp* ou la commande *mv* pour créer une sauvegarde :

```
aomarmezine@aomarmezine-ubuntu:~$ sudo mv /etc/dhcp/dhcpd.conf{,.backup}
```

Figure 2 : Backup server file

On aura besoin de l'adresse MAC de notre machine pour configurer le serveur DHCP par la suite.

Pour obtenir l'adresse MAC, nous pouvons utiliser la commande *ip* sur la machine :

```
aomarmezine@aomarmezine-ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether ac:b5:7d:dd:12:b0 brd ff:ff:ff:ff:ff:ff
    altname wlp2s0
    inet 10.30.253.181/16 brd 10.30.255.255 scope global dynamic noprefixroute wlo1
        valid_lft 12407sec preferred_lft 12407sec
    inet6 fe80::d005:9f25:c052:b703/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Figure 3 : Adresse IP de la machine

On utilise l'éditeur *nano* afin de configurer le fichier */etc/dhcp/dhcpd.conf* :

```
aomarmezine@aomarmezine-ubuntu:~$ sudo nano /etc/dhcp/dhcpd.conf
```

Figure 4 : Accès au fichier DHCP

NB : « */etc/dhcp/dhcpd.conf* », ce fichier sert à la configuration du serveur (plage d'adresses, paramètres distribués).



```
GNU nano 4.8 /etc/dhcp/dhcpd.conf Modified
# a simple /etc/dhcp/dhcpd.conf
default-lease-time 600;
max-lease-time 7200;
authoritative;

subnet 10.30.253.0 netmask 255.255.255.0 {
    range 10.30.253.100 10.30.253.254;
    option routers 10.30.253.254;
    option domain-name-servers 10.30.253.1, 10.30.253.2;
}
```

Figure 5 : Attribution des adresses IP aléatoires

Les paramètres utilisés sont :

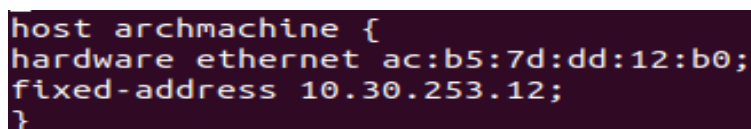
- 1- **max-lease-time** <secondes> : durée maximal d'un bail
- 2- **default-lease-time** <secondes> : valeur par défaut attribuée à un bail
- 3- **Option domain-name-servers** <liste d'adresse> : liste des serveurs DNS
- 4- **Option routers** <liste d'adresse> : liste d'adresse de passerelles, la première est la passerelle par défaut.
- 5- **Paragraphe subnet** : décrit un réseau physique.
- 6- **Le paramètre range** : à l'intérieur du paragraphe indique la plage d'adresse IP utilisée pour les clients de ce réseau.

On peut spécifier plusieurs *range* à l'intérieur d'un paragraphe *subnet*
Dans un *subnet* on peut spécifier des paramètres spécifiques pour les machines de ce réseau.

Pour garantir qu'un client particulier obtiendra toujours la même adresse IP, le serveur DHCP aura besoin de l'adresse MAC de ce client.

Pour obtenir l'adresse MAC d'un client, nous pouvons utiliser la commande *ip* comme précédemment sur la machine cliente.

On fixe l'adresse du client sur 10.30.253.12 :

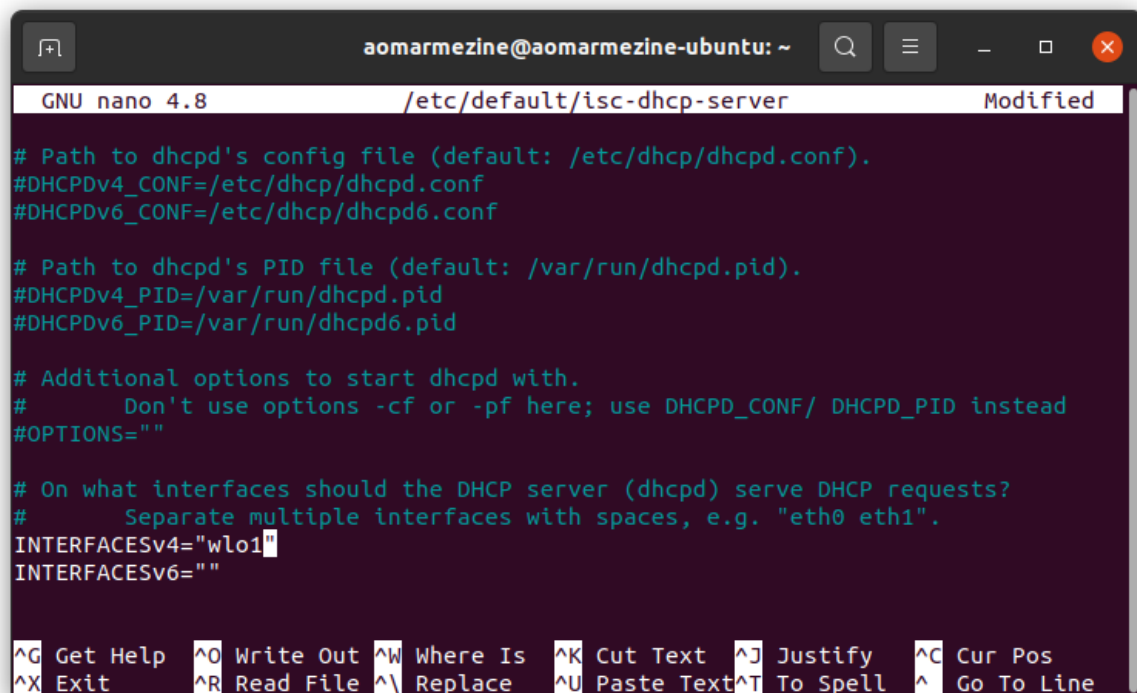


```
host archmachine {
    hardware ethernet ac:b5:7d:dd:12:b0;
    fixed-address 10.30.253.12;
}
```

Figure 6 : Attribution d'une adresse IP statique au client

Le serveur DHCP peut avoir de nombreuses interfaces. On définit l'interface qu'il doit écouter. On affiche les interfaces sur le serveur en utilisant **ip -a** tout comme le client.

L'interface avec laquelle établir la liaison est définie dans le fichier **/etc/default/isc-dhcp-server**. On l'ouvre à l'aide de l'éditeur **nano**. L'interface de notre serveur est wlo1. On obtient le fichier ci-dessous :



```
GNU nano 4.8 /etc/default/isc-dhcp-server Modified

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

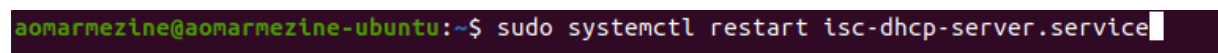
# Additional options to start dhcpd with.
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="wlo1"
INTERFACESv6=""

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Paste Text ^T To Spell  ^_ Go To Line
```

Figure 7 : Liaison du serveur à une interface

Maintenant que les modifications nécessaires ont été apportées à la configuration, nous devons redémarrer le service pour activer ces modifications. Pour cela nous allons utiliser la commande **systemctl** :



```
aomarmezine@aomarmezine-ubuntu:~$ sudo systemctl restart isc-dhcp-server.service
```

Figure 8 : Redémarrage du serveur DHCP

Comme précédemment, on utilise la commande **systemctl** pour vérifier si le serveur est actif. L'état actif indique que le serveur DHCP a récupéré avec succès la configuration et est prêt à distribuer les adresses IP.

```
aomarmezine@aomarmezine-ubuntu: ~  
aomarmezine@aomarmezine-ubuntu:~$ sudo systemctl status isc-dhcp-server.service  
● isc-dhcp-server.service - ISC DHCP IPv4 server  
   Loaded: loaded (/lib/systemd/system/isc-dhcp-server.service; enabled; vendor  
   Active: active (running) since Sun 2022-07-03 01:06:14 CET; 1h 10min ago  
     Docs: man:dhcpcd(8)  
    Main PID: 25681 (dhcpcd)  
      Tasks: 4 (limit: 9370)  
     Memory: 4.9M  
    CGroup: /system.slice/isc-dhcp-server.service  
            └─25681 dhcpcd -user dhcpcd -group dhcpcd -f -4 -pf /run/dhcp-server/dhcp  
  
Jul 03 02:16:24 aomarmezine-ubuntu dhcpcd[25681]: DHCPREQUEST for 10.30.105.125 fro  
Jul 03 02:16:24 aomarmezine-ubuntu dhcpcd[25681]: DHCPNAK on 10.30.105.125 to ce:28  
Jul 03 02:16:24 aomarmezine-ubuntu dhcpcd[25681]: DHCPDISCOVER from ce:28:56:60:b0:  
Jul 03 02:16:24 aomarmezine-ubuntu dhcpcd[25681]: DHCPPOFFER on 10.30.253.189 to ce:  
Jul 03 02:16:25 aomarmezine-ubuntu dhcpcd[25681]: DHCPREQUEST for 10.30.105.125 (10  
Jul 03 02:16:25 aomarmezine-ubuntu dhcpcd[25681]: DHCPNAK on 10.30.105.125 to ce:28  
Jul 03 02:16:41 aomarmezine-ubuntu dhcpcd[25681]: DHCPDISCOVER from 28:39:26:d1:9a:  
lines 1-17
```

Figure 9 : Vérification du statut du serveur DHCP

3- Configuration du client

Maintenant, utilisez la syntaxe suivante pour configurer le client DHCP :

```
aomarmezine@aomarmezine-ubuntu:~$ sudo nano /etc/network/interfaces
```

Figure 10 : Vérification du statut du serveur DHCP

Ici, le nom de l'interface réseau est 'wlo1' ; nous avons modifié les lignes ci-dessus au format suivant :

```
GNU nano 4.8 /etc/network/interfaces Modified  
auto wlo1  
iface wlo1 inet dhcp
```

Figure 11 : Vérification du statut du serveur DHCP

Enregistrez et fermez le fichier de configuration ci-dessus. Maintenant, redémarrez les services du gestionnaire de réseau en exécutant la commande suivante :

```
aomarmezine@aomarmezine-ubuntu:~$ sudo systemctl restart NetworkManager.service
```

Figure 12 : Vérification du statut du serveur DHCP

Ou

```
aomarmezine@aomarmezine-ubuntu:~$ sudo systemctl restart networking
```

Figure 13 : Vérification du statut du serveur DHCP

Vérifiez l'état d'exécution du service NetworkManager en exécutant la commande suivante :

```
● NetworkManager.service - Network Manager
   Loaded: loaded (/lib/systemd/system/NetworkManager.service; enabled; vendor pre>
   Active: active (running) since Sun 2022-07-03 03:00:13 CET; 1min 10s ago
     Docs: man:NetworkManager(8)
   Main PID: 29700 (NetworkManager)
    Tasks: 3 (limit: 9370)
   Memory: 3.1M
    CGroup: /system.slice/NetworkManager.service
            └─29700 /usr/sbin/NetworkManager --no-daemon

Jul 03 03:00:13 aomarmezine-ubuntu NetworkManager[29700]: <info> [1656813613.7893] >
Jul 03 03:00:13 aomarmezine-ubuntu NetworkManager[29700]: <info> [1656813613.7938] >
Jul 03 03:00:13 aomarmezine-ubuntu NetworkManager[29700]: <info> [1656813613.7941] >
Jul 03 03:00:13 aomarmezine-ubuntu NetworkManager[29700]: <info> [1656813613.7976] >
Jul 03 03:00:13 aomarmezine-ubuntu NetworkManager[29700]: <info> [1656813613.7984] >
Jul 03 03:00:13 aomarmezine-ubuntu NetworkManager[29700]: <warn> [1656813613.7992] >
Jul 03 03:00:13 aomarmezine-ubuntu NetworkManager[29700]: <info> [1656813613.8294] >
Jul 03 03:00:13 aomarmezine-ubuntu NetworkManager[29700]: <info> [1656813613.8296] >
lines 1-18
```

Figure 14 : Vérification du statut du serveur DHCP

Lors du processus de démarrage, ce système doit demander les paramètres réseau au serveur DHCP.

Pour exécuter manuellement le processus DHCP, la commande **dhclient** peut être utilisée. Si le serveur DHCP n'attribue aucune adresse IP au client DHCP, utilisez la commande suivante pour renouveler ou libérer l'adresse IP. Attendez un moment ; le serveur DHCP attribuera automatiquement des adresses IP à la machine cliente.

```
mehdiz@ubuntu:~$ sudo dhclient -r ens33
```

Figure 15 : Attribution d'une adresse IP à un client

L'utilisation de la commande 'ifconfig' permet d'afficher le nom de l'interface.

Chapitre 4

Identification des vulnérabilités liées à DHCP

I – Sources de menaces

Les cyberattaques sont de plus en plus fréquentes. DHCP est devenu un point d'entrée pour les cybercriminels. DHCP simplifie l'adressage IP et la configuration du réseau, mais peut aussi créer des problèmes de sécurité. Parmi les attaques les plus répandues on cite :

1- DHCP starvation attack

Une attaque starvation DHCP est une attaque numérique malveillante qui cible les serveurs DHCP. Lors d'une attaque DHCP, un acteur hostile inonde un serveur DHCP de faux paquets DISCOVER jusqu'à ce que le serveur DHCP épuise son approvisionnement en adresses IP. Une fois que cela se produit, l'attaquant peut refuser le service aux utilisateurs légitimes du réseau, ou même fournir une connexion DHCP alternative qui mène à une attaque Man-in-the-Middle (MITM).

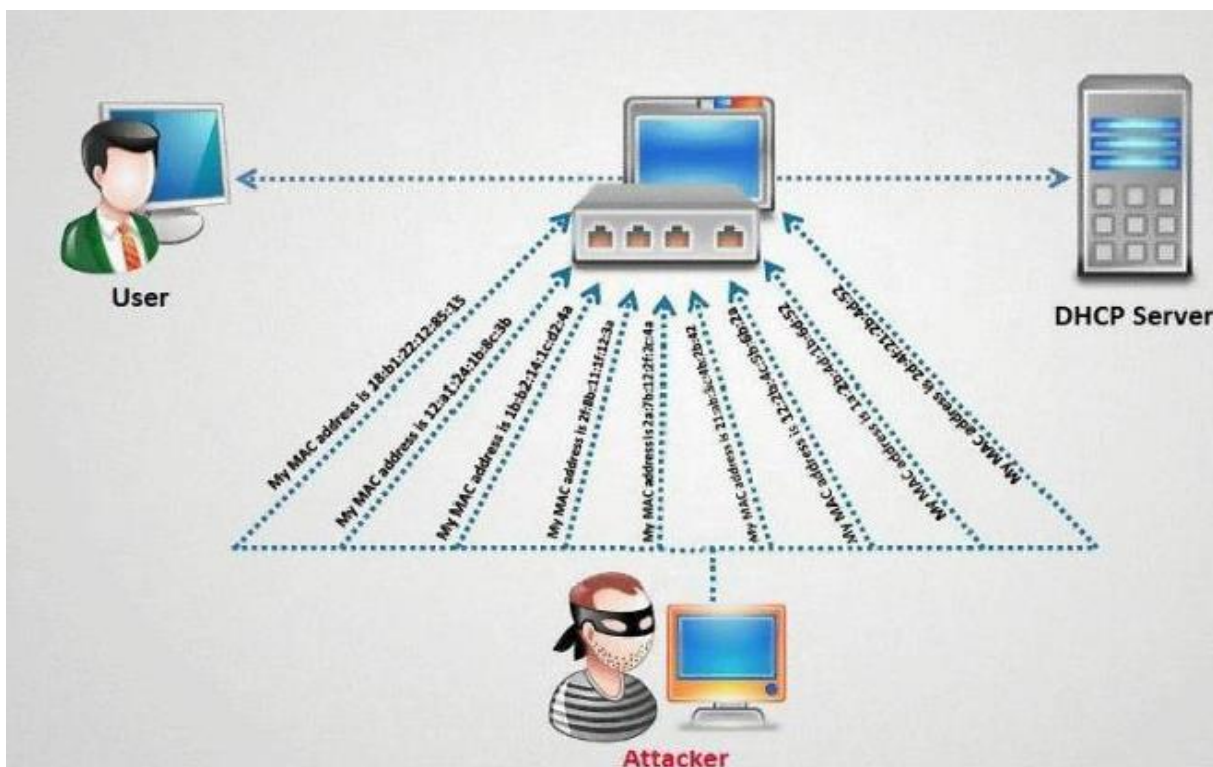


Figure 16 : DHCP starvation attack

2- Rogue DHCP server attack

Les serveurs DHCP rogue sont des serveurs qui ne sont pas sous le contrôle des administrateurs réseau. Ils ont tendance à se faire passer pour un serveur légitime, offrant des adresses IP et d'autres informations réseau aux côtés du serveur DHCP légal lorsque le client compatible DHCP envoie un message de diffusion.

Si le DHCP rogue propose un paquet différent de celui du vrai serveur DHCP, accepter l'offre, surtout si elle vient en premier, causera toutes sortes de ravages pour le client.

La plupart du temps, les attaquants sont ceux qui se cachent derrière les serveurs DHCP rogue. Si le client reçoit une adresse IP et d'autres informations d'un serveur DHCP non autorisé, cela signifie que l'adresse IP recevra tout le trafic du client - cela, l'attaquant peut acquérir et envoyer à la passerelle par défaut appropriée.

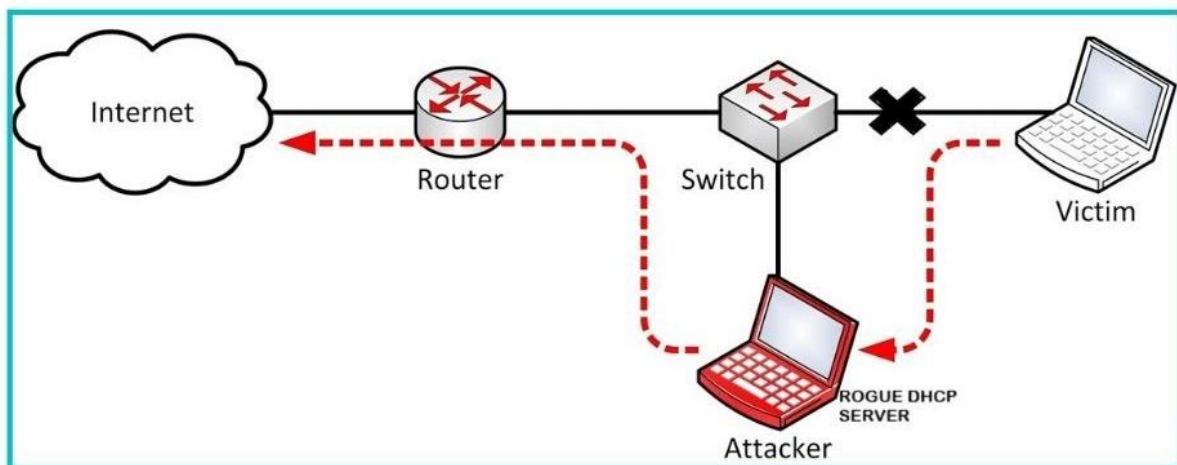


Figure 17 : Rogue DHCP server attack

II – Simulation d'attaque

Afin de simuler l'attaque sur le serveur DHCP, on fait appel au framework YERSINIA qui est conçu pour effectuer des attaques de couche 2. Ce framework tire parti de certaines faiblesses des différents protocoles réseau comme le DHCP. Il prétend être un cadre solide pour analyser et tester les réseaux et systèmes déployés.

2- DHCP starvation attack

Lancement de l'outil « Yersinia » en mode graphique.

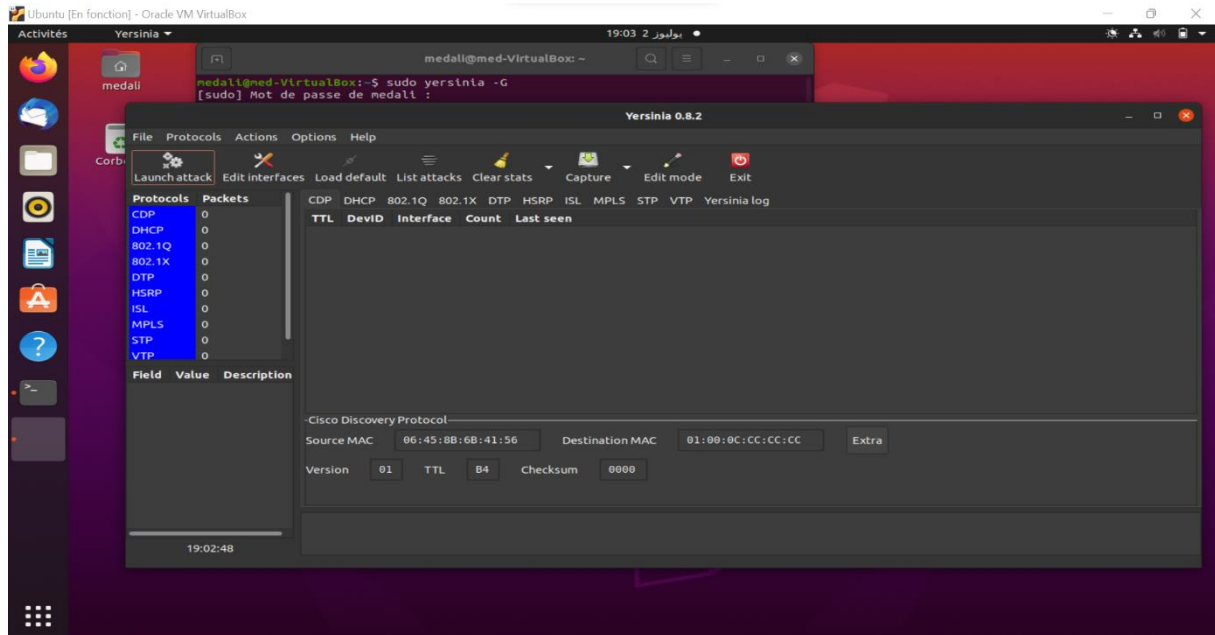


Figure 20 : La commande Yersinia -G

Une fenêtre s'affiche. Cliquez sur « Launch Attack » (Lancer l'attaque)

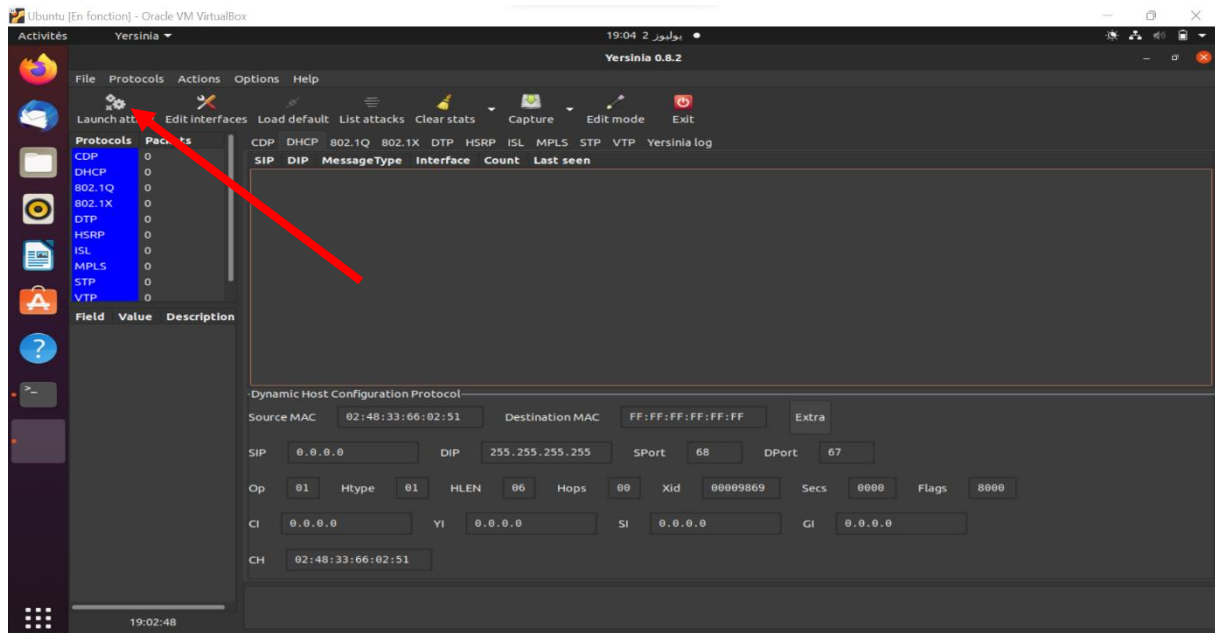


Figure 21 : Launch attack

Une nouvelle fenêtre s'affiche. Cliquez sur « DHCP » puis choisissez « Sending Discover packet ».

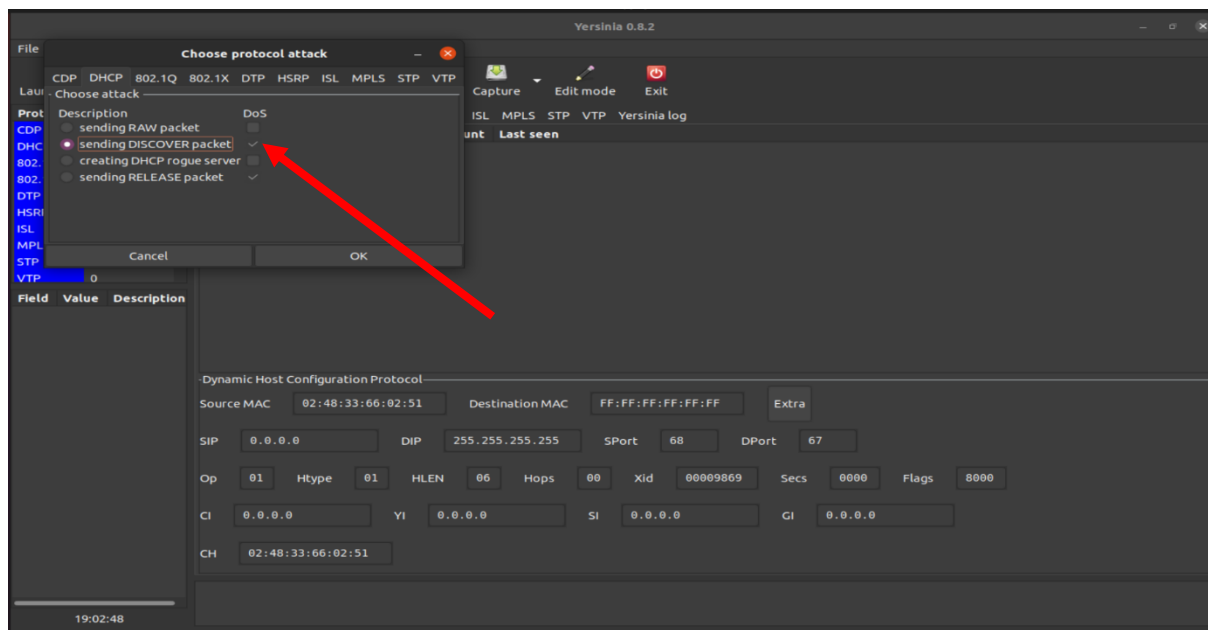


Figure 22 : Sending discover packet

Cette attaque est une attaque par « déni de service par saturation » qui consiste à envoyer beaucoup de paquets « DHCP DISCOVER » au serveur DHCP afin d'épuiser toutes ses ressources.

Une fois les ressources du DHCP sont épuisées, aucun client ne peut obtenir une adresse IP.

Après avoir cliqué sur « OK », l'attaque est lancée et le résultat suivant s'affiche.

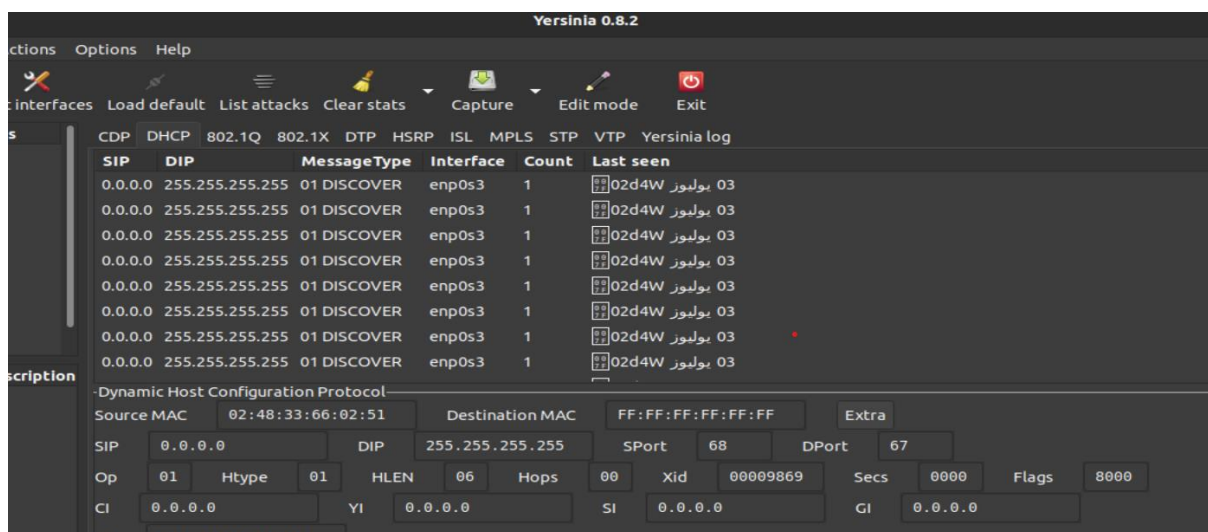


Figure 23 : Résultat de l'attaque

3- Configuration DHCP rogue server

On clique sur « Launch Attack », Une nouvelle fenêtre s'affiche. Après on clique sur « DHCP » puis on choisit «creating DHCP rogue server ».

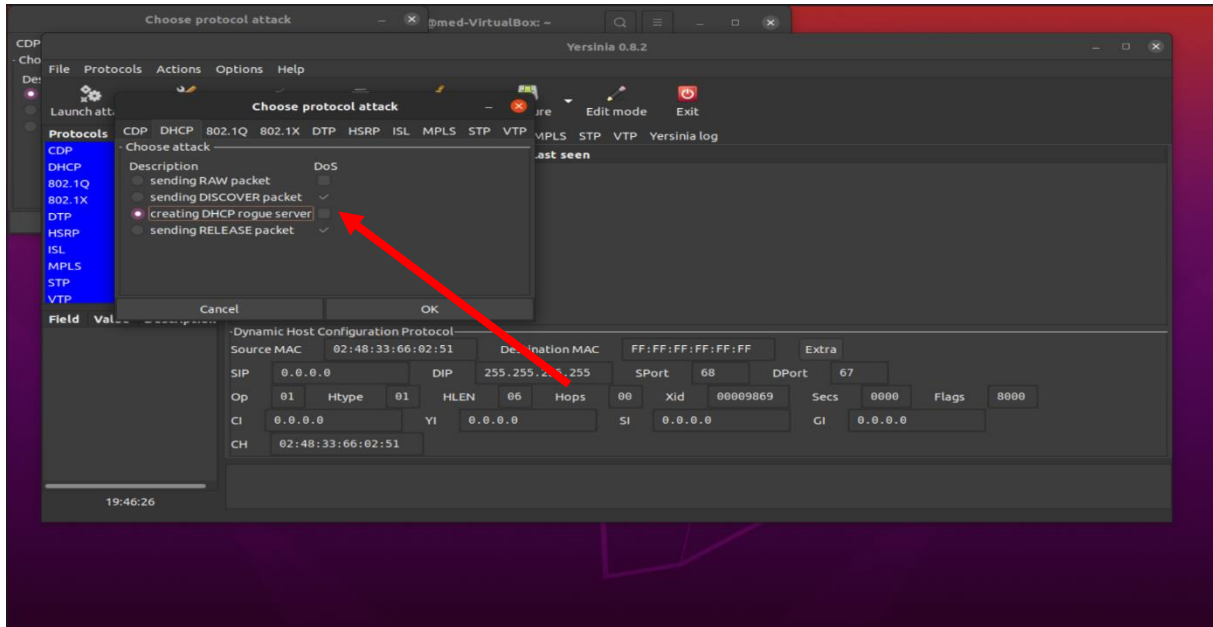


Figure 24 : Creating DHCP rogue server

The screenshot shows the Yersinia 0.8.2 application window. The 'DHCP attack parameters' dialog is open, displaying various configuration fields. The 'Field' tab is selected, showing a table of fields and their values. The table includes columns for Field, Value, and other parameters like Type, HLEN, Hops, SPort, DPort, Xid, Secs, and Flags.

Field	Value	Type	HLEN	Hops	SPort	DPort	Xid	Secs	Flags
CI	0.0.0.0	YI	0.0.0.0				0.0.0.0		
CH	02:48:33:66:02:51								

4- Configuration du rogue server sous packetracer

The diagram illustrates a network topology where two PCs, PC0 and PC1, are connected to a central switch, Switch0. PC0 has the IP address 192.168.10.11 and PC1 has 192.168.10.12. Switch0 is a 2960-24TT model. The switch is then connected to a server, Server0, which has the IP address 192.168.10.1. All connections are shown as black lines with green triangle markers at the endpoints.

29

On configure de la passerelle par défaut du serveur DHCP tout en précisant l'adresse IP de début et le nombre maximum d'adresses à attribuer.

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 192.168.10.10

DNS Server: 0.0.0.0

Start IP Address: 192 168 10 11

Subnet Mask: 255 255 255 0

Maximum Number of Users: 10

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Buttons: Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168.10.10	0.0.0.0	192.168.10.11	255.255.255.0	10	0.0.0.0	0.0.0.0

Figure 27 : Configuration de serveur DHCP légitime

Maintenant on introduit un serveur DHCP malicieux (rogue DHCP server) qui va prendre la place du serveur légitime et commence à attribuer des adresses IP aux pcs.

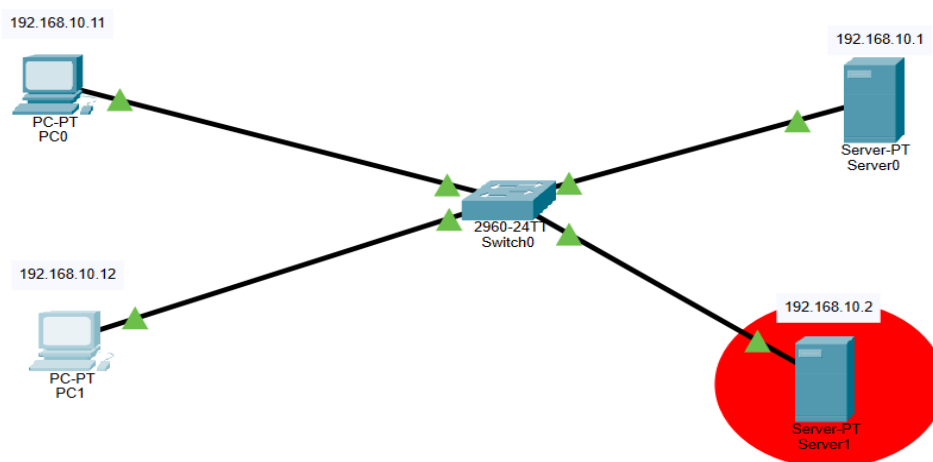


Figure 28 : DHCP avec rogue server

On configure de la passerelle par défaut du serveur DHCP rogue tout en précisant l'adresse IP de début et le nombre maximum d'adresses à attribuer.

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 192.168.10.5

DNS Server: 0.0.0.0

Start IP Address: 192 168 10 11

Subnet Mask: 255 255 255 0

Maximum Number of Users: 10

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Buttons: Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168....	0.0.0.0	192.168....	255.255....	10	0.0.0.0	0.0.0.0

Figure 29 : Configuration de serveur DHCP rogue

Après l'envoi du message de DISCOVER par le deuxième pc, c'est le DHCP Rogue serveur qui va attribuer l'adresse IP (d'après la passerelle).

IP Configuration

Interface: FastEthernet0

IP Configuration

☒ DHCP ☐ Static

IP Address: 192.168.10.11

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.10.5

DNS Server: 0.0.0.0

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address: /

Link Local Address: FE80::201:42FF:FE04:5AE2

IPv6 Gateway:

IPv6 DNS Server:

802.1X

☐ Use 802.1X Security

Figure 30 : La réussite de l'attaque

Chapitre 5

Mesures de sécurité pour un usage plus sûr de DHCP

1 – DHCP snooping

Le DHCP snooping est une fonction de sécurité intervenant au deuxième niveau du modèle OSI. Cette fonction est intégrée dans le commutateur connectant les clients aux serveurs DHCP. En d'autres termes, il s'agit d'un protocole qui contrôle tout d'abord l'ensemble des informations DHCP passant par le commutateur. Seuls les paquets autorisés provenant de serveurs dignes de confiance sont transmis aux clients.

De cette façon, un serveur DHCP non autorisé peut certes recevoir le paquet DHCPDISCOVER (la requête du client visant à obtenir un serveur DHCP) puisqu'il surveille le broadcast. Il peut aussi envoyer un paquet DHCPOFFER (la réponse à la recherche), mais ce paquet n'atteindra jamais le client. Placé dans le commutateur, le DHCP snooping identifie le fait que le paquet ne provient pas d'un serveur digne de confiance et contient de fausses informations et procède donc au blocage de la transmission.

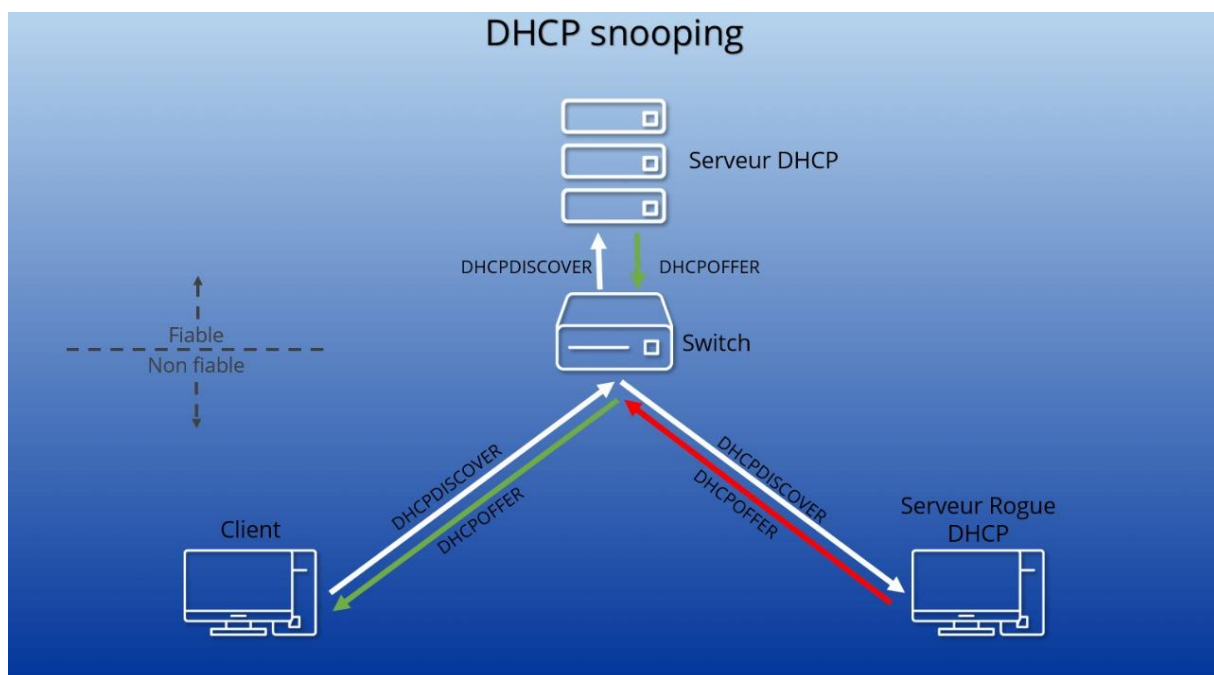


Figure 31 : DHCP Snooping

- **Ports dignes de confiance**

Pour garantir que seuls les serveurs fiables puissent intervenir dans l'attribution d'informations de configuration, le DHCP snooping procède en plusieurs étapes. Dans un premier temps, il détermine un port de confiance pour le serveur ou les serveurs propres. Tous les autres appareils essayant d'accéder au réseau via un autre port sont considérés comme non dignes de confiance. Tous les clients en font également partie. Cela implique donc qu'un hôte sur lequel tourne un serveur DHCP mais qui n'est pas approuvé par l'administrateur sera considéré comme non digne de confiance. Mais si un paquet DHCP ne pouvant être envoyé que par un serveur (DHCP OFFER, DHCP ACK, DHCP REQUEST) arrive par le biais d'un port qui n'est pas digne de confiance, le commutateur bloque la transmission. Le client ne recevra pas l'information.

- **La DHCP snooping Binding Database**

Néanmoins, un hacker peut également essayer de détruire le réseau en se faisant passer pour l'un des clients existants et en rejetant ces offres du serveur DHCP. C'est pourquoi le DHCP snooping utilise une base de données créée et actualisée de façon autonome par le système. Le protocole lit toutes les informations DHCP (mais pas les données effectives après la réussite de la connexion) et en extrait des détails pour la DHCP snooping Binding Database.

Le système enregistre dans la base de données tous les hôtes ne passant pas par un port digne de confiance. Les informations accumulées comprennent l'adresse MAC, l'adresse IP attribuée, le port du commutateur utilisé, le sous-réseau logique (VLAN) et la durée du Lease Time. Le DHCP snooping peut ainsi garantir que seuls les clients originaux ayant participé à la communication peuvent envoyer des ordres au serveur, car l'adresse MAC et le port du commutateur de l'appareil ne coïncident avec les informations enregistrées dans la base de données que pour ces clients originaux.

2 – Configuration de DHCP snooping

▪ Activation du DHCP snooping :

Ici, nous allons activer DHCP Snooping sur le commutateur. DHCP Snooping fonctionnera dessus. DHCP Snooping peut être activé globalement avec la commande « ip dhcp snooping » ou il peut être activé sur un VLAN spécifique qui correspond dans notre cas au VLAN 1.

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#
```

Figure 32 : Configuration DHCP snooping

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#no ip dhcp snooping information option
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is disabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                Trusted      Rate limit (pps)
-----
Switch#
```

Figure 33 : Configuration DHCP snooping actif

Au début de la configuration, les ports requis sont définis comme "non approuvés". Ces ports sont généralement des ports utilisateur. Simplement, nous configurons tous les ports plutôt que le serveur DHCP du réseau comme "non approuvés" avec DHCP Snooping.

The screenshot shows a network configuration window titled "IP Configuration" for the interface "FastEthernet0". Under "IP Configuration", the "DHCP" radio button is selected, but a message indicates "DHCP failed. APIPA is being used." The IP Address is 169.254.102.71, Subnet Mask is 255.255.0.0, Default Gateway is 0.0.0.0, and DNS Server is 0.0.0.0. Under "IPv6 Configuration", the "Static" radio button is selected, and the Link Local Address is FE80::20C:CFFF:FE0A:6647. The "802.1X" section shows "Use 802.1X Security" unchecked and "Authentication" set to MD5.

Figure 34: Unable to get IP adresse

- **Configuration des ports de confiance (trusted ports) :**

Dans les mécanismes DHCP Snooping, il existe deux types de ports L'un d'eux est fiable et l'autre n'est pas fiable. Ici, nous allons définir les ports de confiance. Ici, nous allons simplement définir un port de confiance. Le port du commutateur qui est connecté au serveur DHCP (routeur).

Nous allons accéder à l'interface connectée au routeur et la définir comme port de confiance avec la commande "ip dhcp snooping trust".

```

Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fa0/6
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#|

```

Figure 35 : Configuration des ports de confiance

```

Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is disabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                Trusted      Rate limit (pps)
-----
FastEthernet0/6          yes         unlimited
FastEthernet0/1          no          unlimited
FastEthernet0/2          no          unlimited
FastEthernet0/4          no          unlimited
Switch#|

```

Figure 36 : La réussite de la configuration

Figure 37-1 : Pc connecte au serveur légitime

IP Configuration [X]

Interface: FastEthernet0

IP Configuration

☒ DHCP ☐ Static DHCP request successful.

IP Address: 192.168.10.13

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.10.10

DNS Server: 0.0.0.0

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address: /

Link Local Address: FE80::201:42FF:FE04:5AE2

IPv6 Gateway:

IPv6 DNS Server:

Figure 37-2 : Pc connecte au serveur légitime

Affichez les informations de la base de données de surveillance DHCP. (IP adresse ; bail ; type ; Vlan ; Interface)

```
Switch#show ip dhcp snooping binding
MacAddress      IpAddress      Lease(sec)  Type           VLAN  Interface
-----
00:0C:CF:0A:66:47  192.168.10.12  86400      dhcp-snooping  1     FastEthernet0/2
00:01:42:04:5A:E2  192.168.10.13  86400      dhcp-snooping  1     FastEthernet0/4
Total number of bindings: 2
Switch#
```

Figure 38 : DHCP binding

- **Configuration de la limite de débit :**

Il y a une autre étape de configuration importante ici. Nous pouvons également définir des requêtes DHCP pouvant être reçues en une seconde. Si ce débit dépasse celui configuré, le trafic est abandonné. Ici, mettons-le à 10.

```
Switch#  
Switch#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)#interface fa0/1  
Switch(config-if)#ip dhcp snooping limit rate 10  
Switch(config-if)#end  
Switch#  
%SYS-5-CONFIG_I: Configured from console by console  
Switch#
```

Figure 39 : DHCP rate limit

Conclusion

Le projet de DHCP (Dynamic Host Configuration Protocol) nous a permis de développer nos connaissances sur le domaine de réseau. Tout au long du projet, nous avons pu avoir une idée plus claire sur les menaces auxquelles le serveur DHCP est confronté en permanence et trouver des mesures fiables qui garantissent la sécurité du réseau et la confidentialité des données des clients du serveur DHCP. Cette sécurisation est devenue de nos jours primordiaux au sein des entreprises car toute infraction va coûter cher en temps et argent.

Ce projet a été une réelle opportunité pour mettre en défi notre travail d'équipe et compétences acquises lors de cette année, ce qui nous a permis de développer nos connaissances.

Bibliographie

- Protocole DHCP :

<https://www.frameip.com/dhcp/>

- A Step-by-Step Guide to set up a DHCP Server on Ubuntu:

<https://www.linuxfordevices.com/tutorials/ubuntu/dhcp-server-on-ubuntu/>

- CCNA Sécurité : Attaque 2 : Épuisement des ressources DHCP (DHCP Starvation) :

<https://www.nticprof.com/2019/06/dhcp-starvation.html>

- DHCP Snooping: Stop Kali DHCP Hacks and MITM:

<https://www.youtube.com/watch?v=S6KI6VsvDuU&t=211s>

- Sue Miller, (January 2001), DHCP for Windows 2000: Managing the Dynamic Host Configuration Protocol

Fin.