



PROJET DE L'ADMINISTRATION SYSTÈME

SUJET :

DYNAMIC HOST CONFIGURATION PROTOCOL « DHCP »

SOUTENU PAR :

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

SOUS LA DIRECTION DE :

- MME ZAYDI MOUNIA

FILIÈRE:

- GENIE INFORMATIQUE _PROMO-18

Année Universitaire 2021-2022

PLAN

1. INTRODUCTION

2. PROTOCOLE DHCP

3. INSTALLATION ET CONFIGURATION DHCP

4. IDENTIFICATION DE VULNÉRABILITÉS LIÉES À DHCP

5. MESURES DE SÉCURITÉ DE DHCP

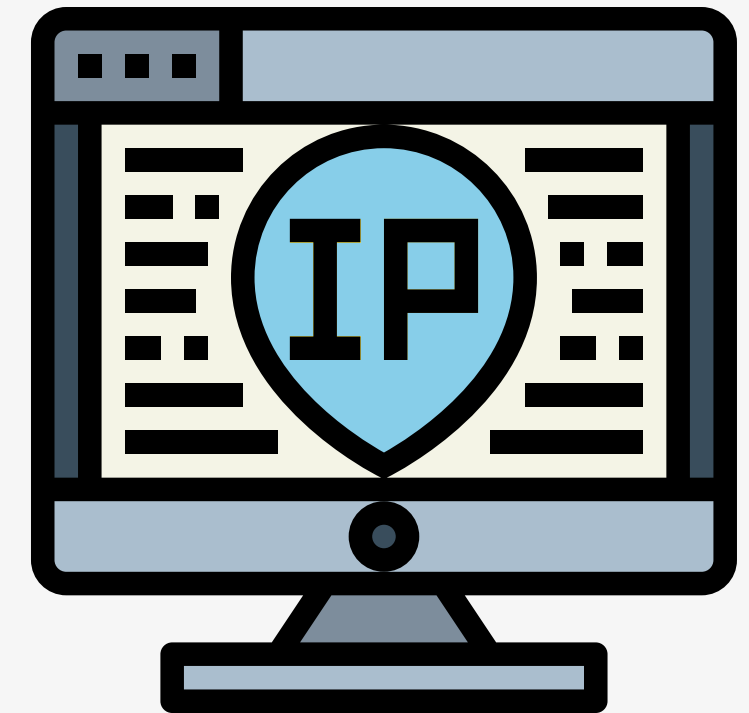
6. CONCLUSION

INTRODUCTION

PROTOCOLE DHCP

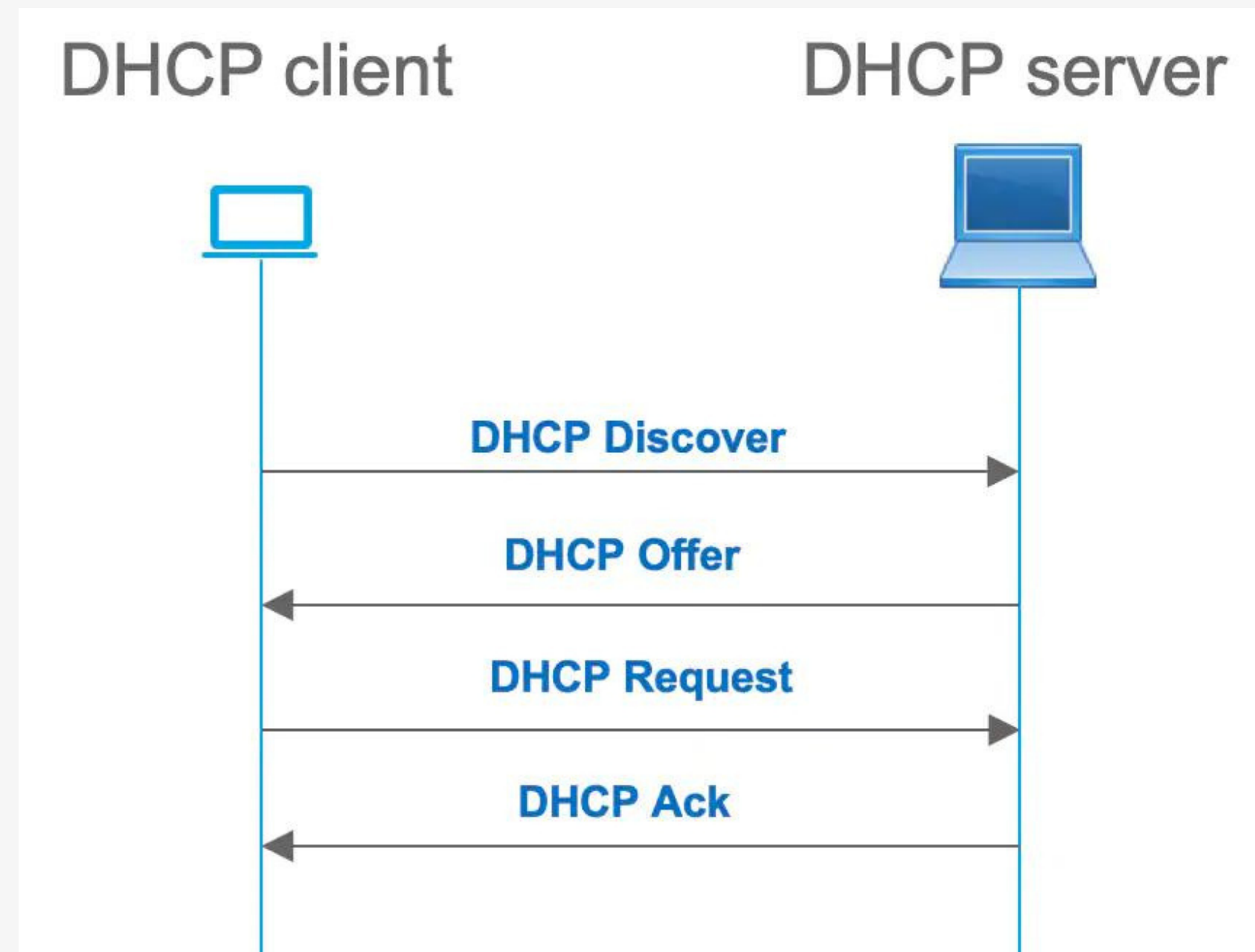
DÉFINITION

DHCP est un protocole qui permet à un ordinateur qui se connecte sur un réseau local d'obtenir dynamiquement et automatiquement sa configuration IP



PROTOCOLE DHCP

FONCTIONNEMENT DHCP



INSTALLATION ET CONFIGURATION DHCP

1- INSTALLATION DU SERVEUR DHCP

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

2- CONFIGURATION DU SERVEUR DHCP

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

```
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
```

INSTALLATION ET CONFIGURATION DHCP

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

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

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

INSTALLATION ET CONFIGURATION DHCP

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

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

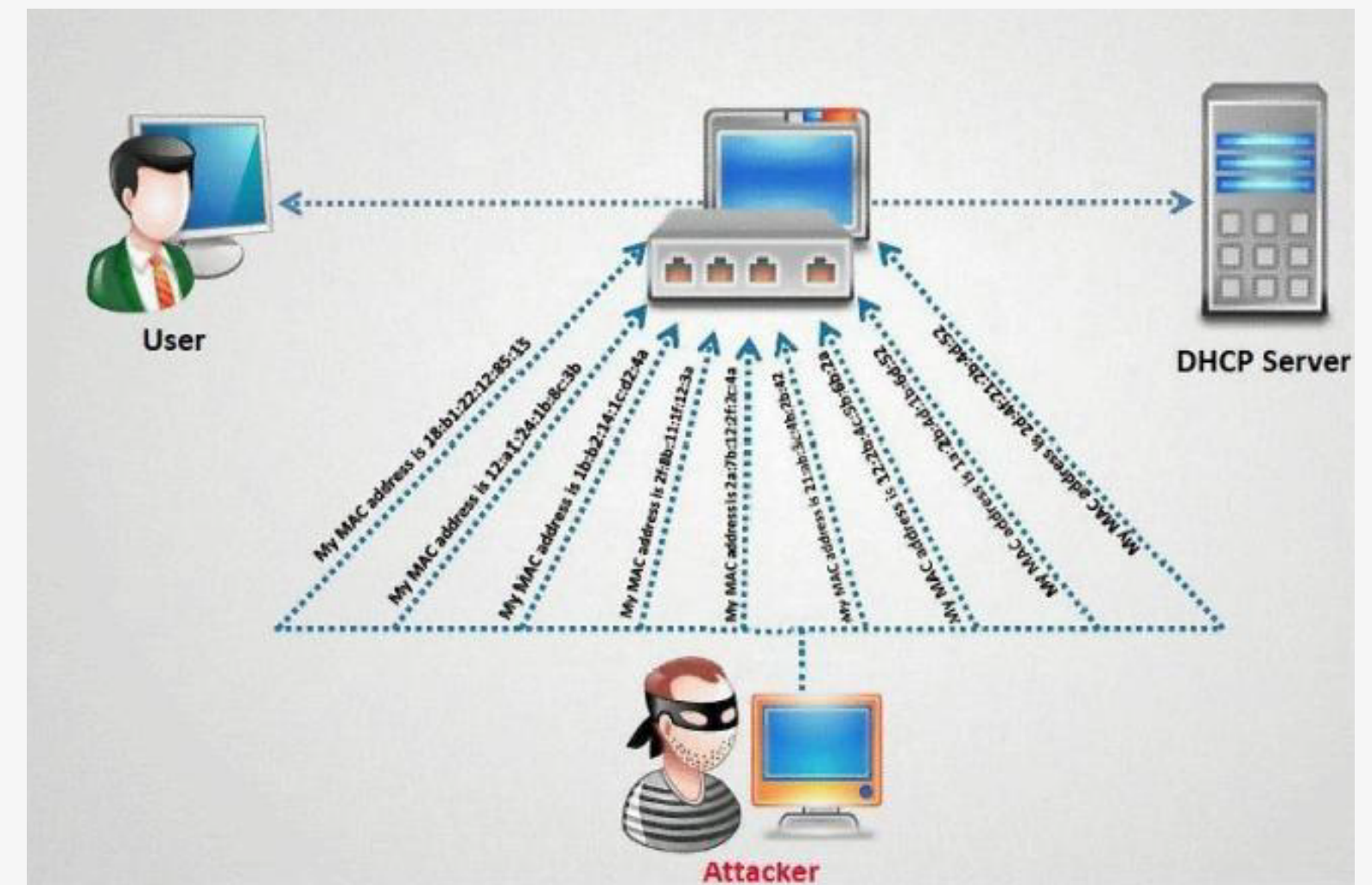
```
aomarmezine@aomarmezine-ubuntu:~$ sudo systemctl status isc-dhcp-server.service  
● isc-dhcp-server.service - ISC DHCP IPv4 server  
   Loaded: loaded (/lib/systemd/system/isc-dhcp-server.service; enabled; vendor  
   Active: active (running) since Sun 2022-07-03 01:06:14 CET; 1h 10min ago  
   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


IDENTIFICATION DE VULNÉRABILITÉS LIÉES À DHCP

SOURCE DES MENACES

-DHCP STARVATION ATTACK:

DHCP Starvation attack est une attaque qui cible les serveurs DHCP par laquelle des requêtes DHCP falsifiées sont conçues par un attaquant dans le but d'épuiser toutes les adresses IP disponibles qui peuvent être allouées par le serveur DHCP .

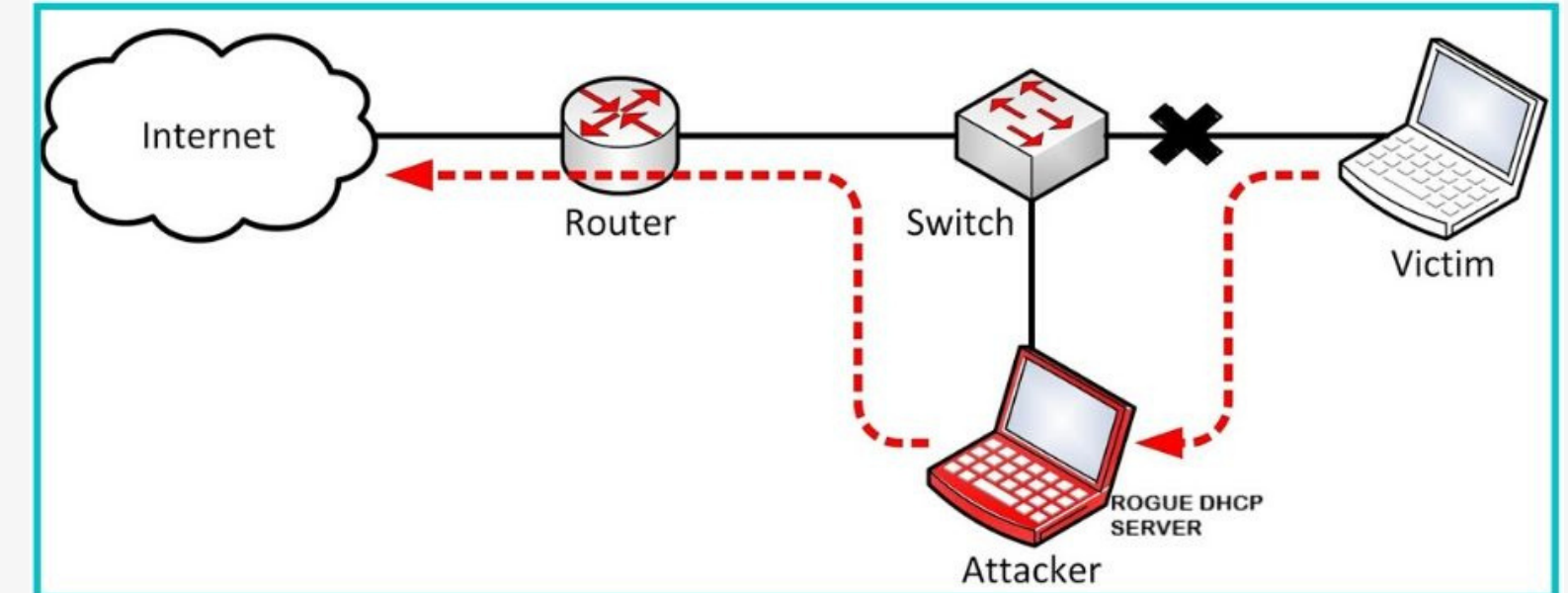


IDENTIFICATION DE VULNÉRABILITÉS LIÉES À DHCP

SOURCE DES MENACES

-DHCP ROGUE SERVER:

Les serveurs DHCP rogue sont des serveurs qui 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.



IDENTIFICATION DE VULNÉRABILITÉS LIÉES À DHCP

SIMULATION D'ATTAQUE

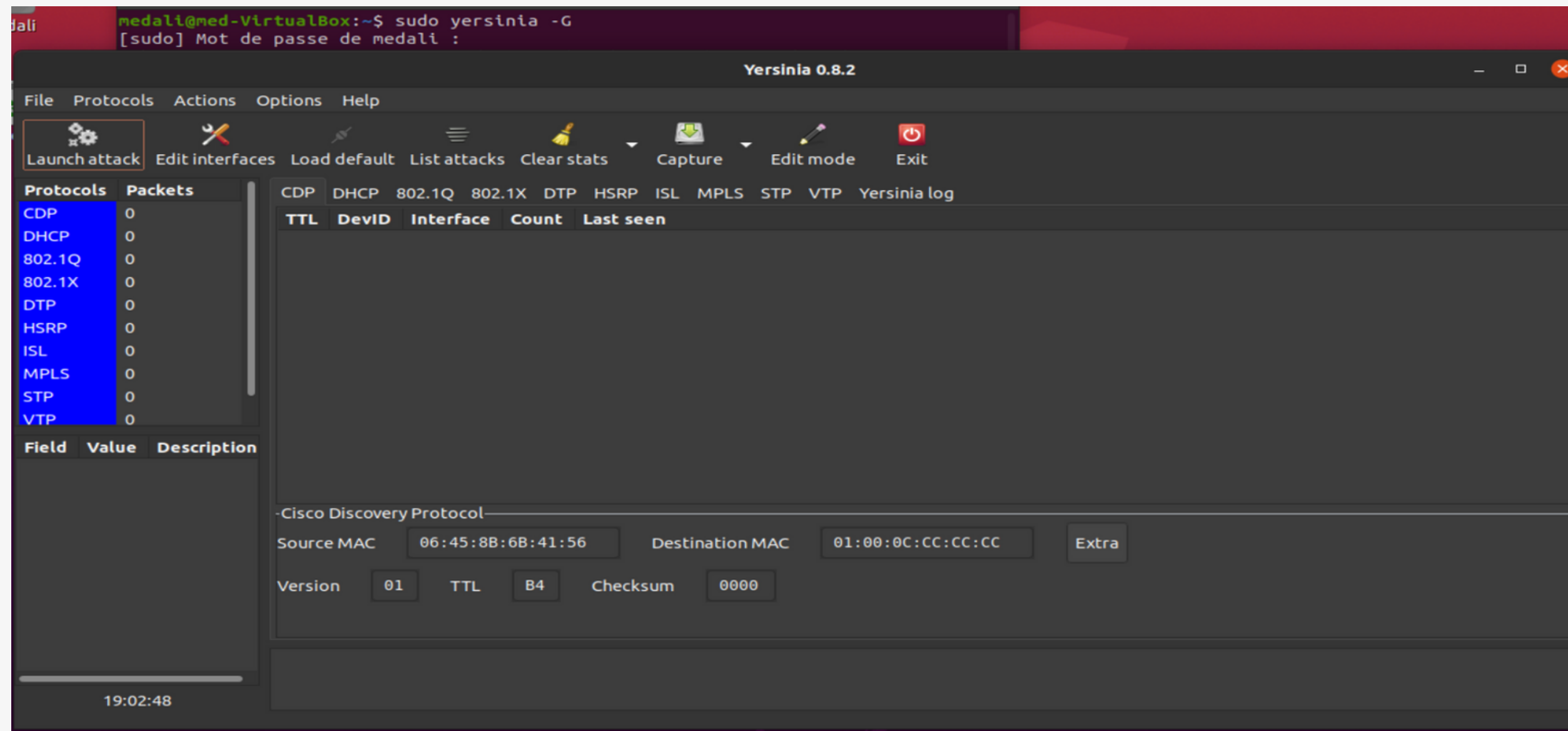
-INSTALLATION DU FRAMEWORK YERSINIA

```
medali@med-VirtualBox:~$ sudo apt-get install yersinia
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libnet1
Les NOUVEAUX paquets suivants seront installés :
  libnet1 yersinia
0 mis à jour, 2 nouvellement installés, 0 à enlever et 151 non mis à jour.
Il est nécessaire de prendre 207 ko dans les archives.
Après cette opération, 624 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] O
Réception de :1 http://ma.archive.ubuntu.com/ubuntu focal/main amd64 libnet1 amd64 1.1.6+dfsg-3.1build1 [43.3 kB]
Réception de :2 http://ma.archive.ubuntu.com/ubuntu focal/universe amd64 yersinia amd64 0.8.2-2build1 [164 kB]
207 ko réceptionnés en 1s (317 ko/s)
Sélection du paquet libnet1:amd64 précédemment désélectionné.
(Lecture de la base de données... 189365 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../libnet1_1.1.6+dfsg-3.1build1_amd64.deb ...
Dépaquetage de libnet1:amd64 (1.1.6+dfsg-3.1build1) ...
Sélection du paquet yersinia précédemment désélectionné.
Préparation du dépaquetage de .../yersinia_0.8.2-2build1_amd64.deb ...
Dépaquetage de yersinia (0.8.2-2build1) ...
Paramétrage de libnet1:amd64 (1.1.6+dfsg-3.1build1) ...
Paramétrage de yersinia (0.8.2-2build1) ...
Traitement des actions différées (« triggers ») pour man-db (2.9.1-1) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.31-0ubuntu9.7) ...
```

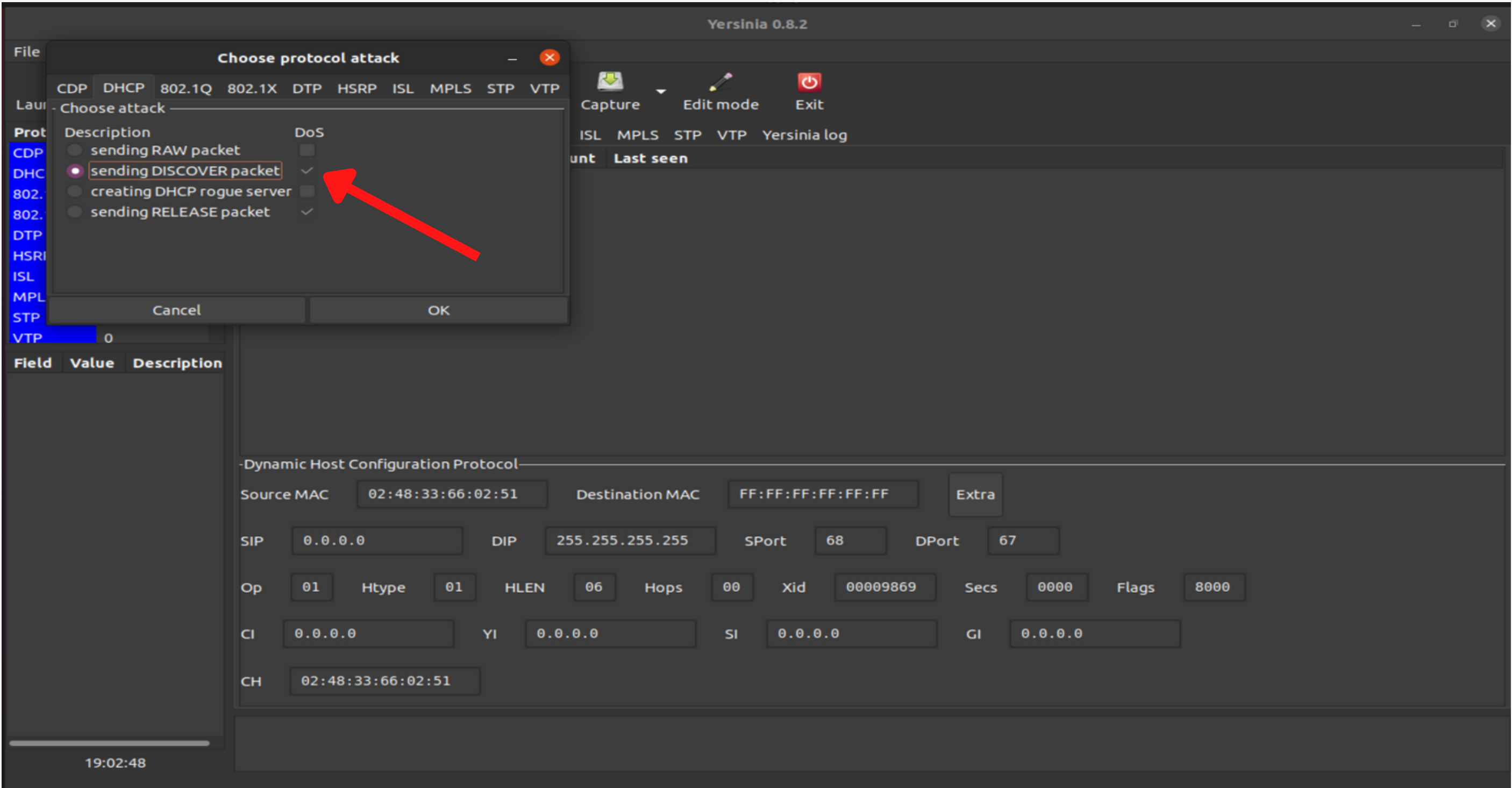
IDENTIFICATION DE VULNÉRABILITÉS LIÉES À DHCP

SIMULATION D'ATTAQUE

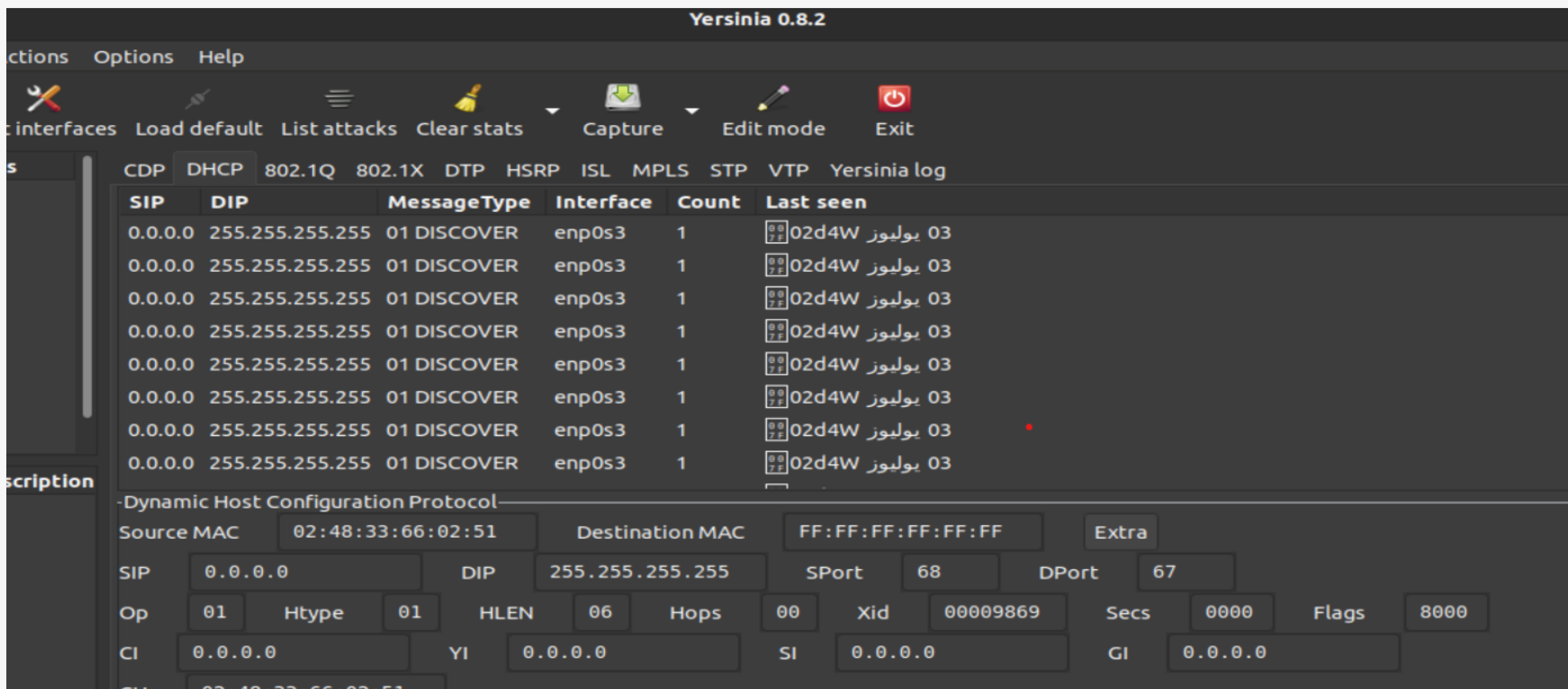
-CONFIGURATION STARVATION ATTACK



IDENTIFICATION DE VULNÉRABILITÉS LIÉES À DHCP



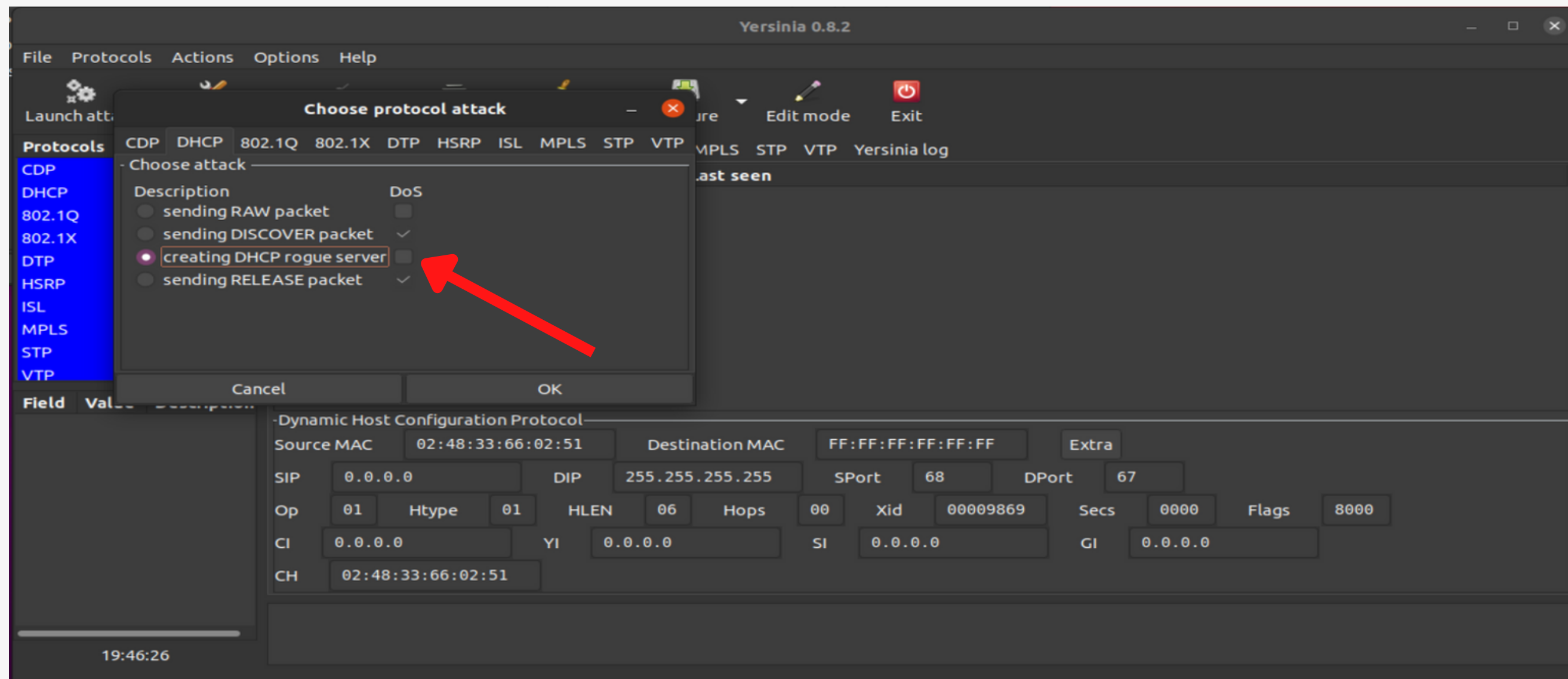
IDENTIFICATION DE VULNÉRABILITÉS LIÉES À DHCP



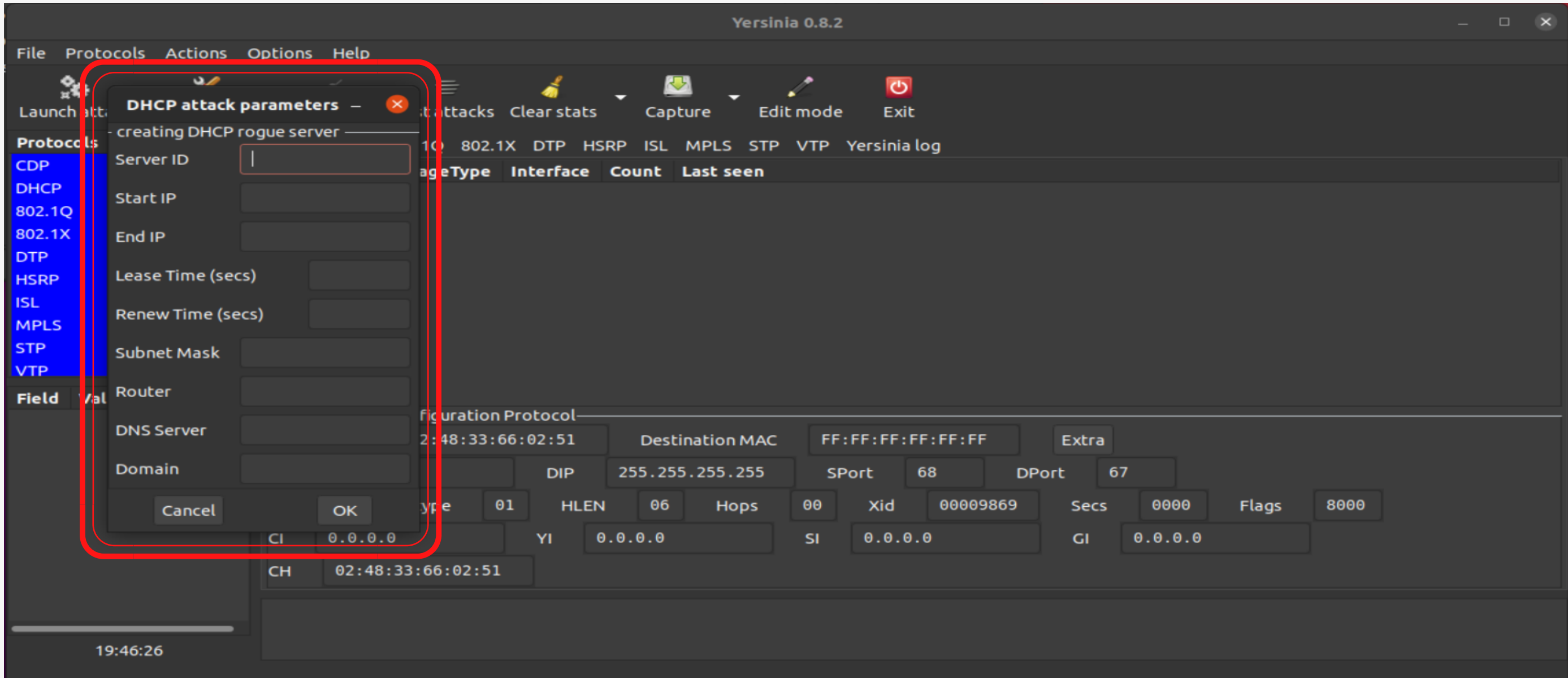
IDENTIFICATION DE VULNÉRABILITÉS LIÉES À DHCP

SIMULATION D'ATTAQUE

-CONFIGURATION DHCP ROGUE SERVER:



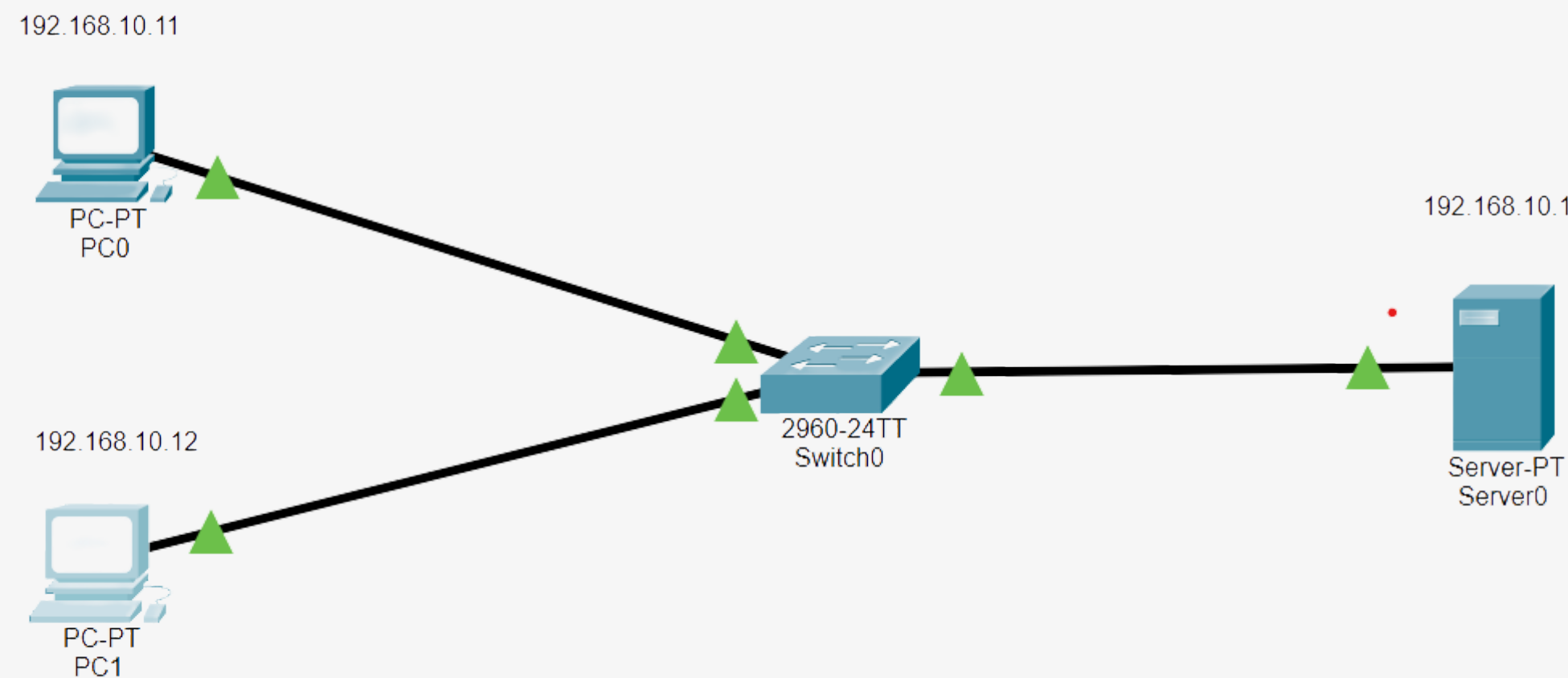
IDENTIFICATION DE VULNÉRABILITÉS LIÉES À DHCP



IDENTIFICATION DE VULNÉRABILITÉS LIÉES À DHCP

SIMULATION D'ATTAQUE

-CONFIGURATION DHCP ROGUE SERVER SOUS PACKET TRACER:



Réseau sans rogue server

IDENTIFICATION DE VULNÉRABILITÉS LIÉES À DHCP

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

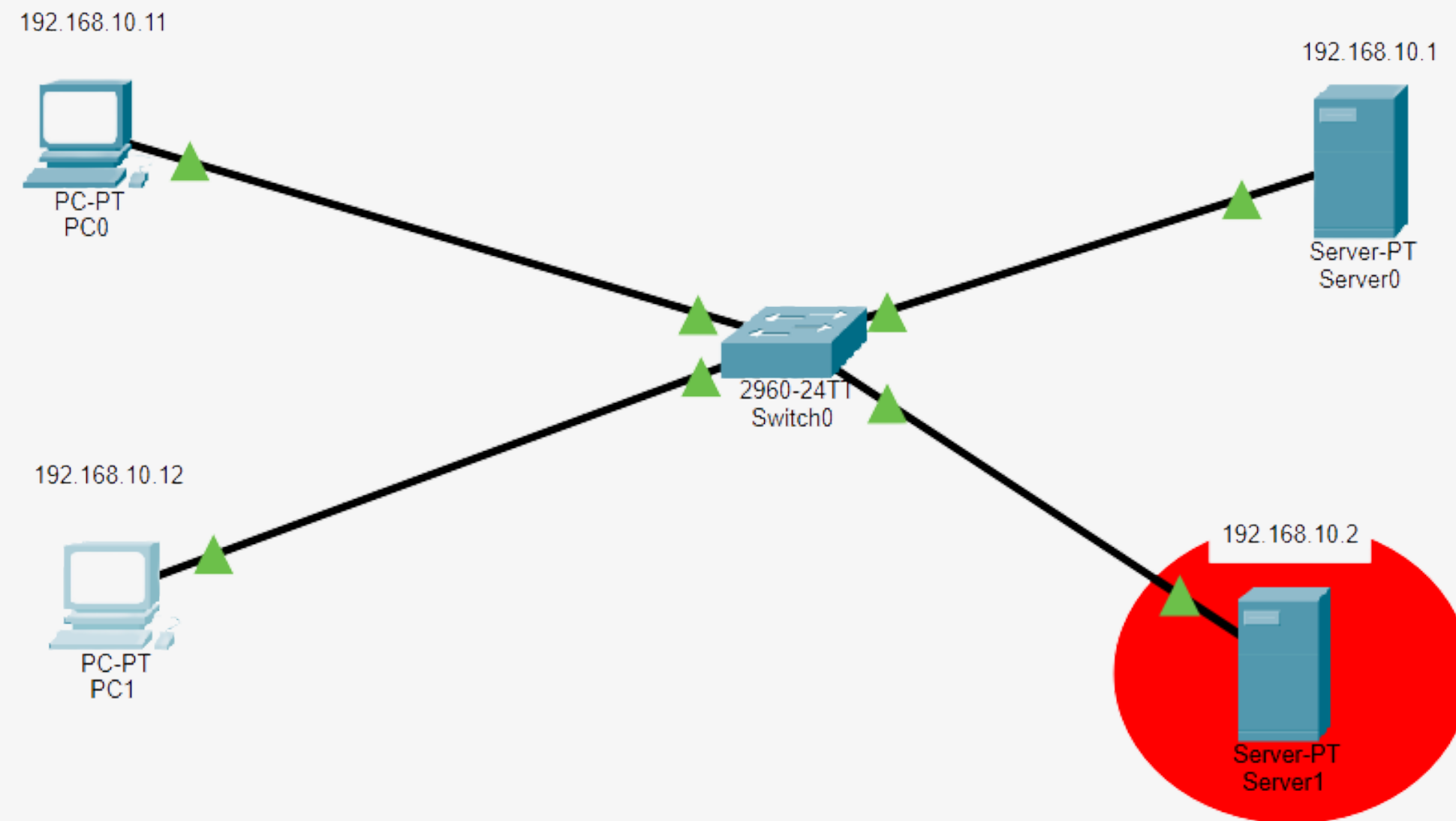
Add

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

IDENTIFICATION DE VULNÉRABILITÉS LIÉES À DHCP



Réseau avec rogue server

IDENTIFICATION DE VULNÉRABILITÉS LIÉES À DHCP

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

192.168.10.5

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

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

IDENTIFICATION DE VULNÉRABILITÉS LIÉES À DHCP

IP Configuration

X

InterfaceFastEthernet0

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

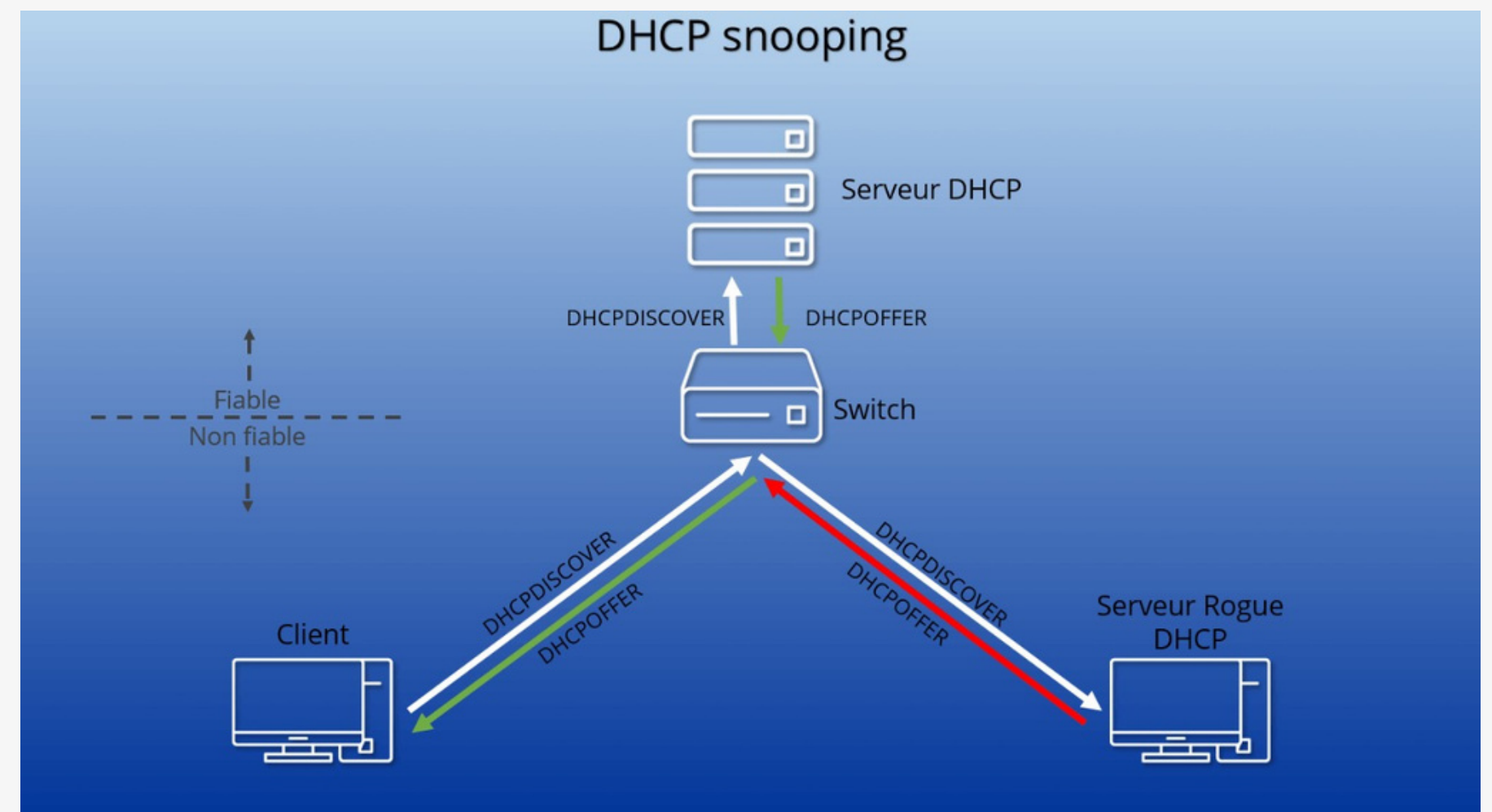
☐ Use 802.1X Security

AuthenticationMDE

MESURES DE SÉCURITÉ DE DHCP

DÉFINITION DHCP SNOOPING

Le DHCP snooping est une fonction de sécurité intervenant au deuxième niveau du modèle OSI. 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.

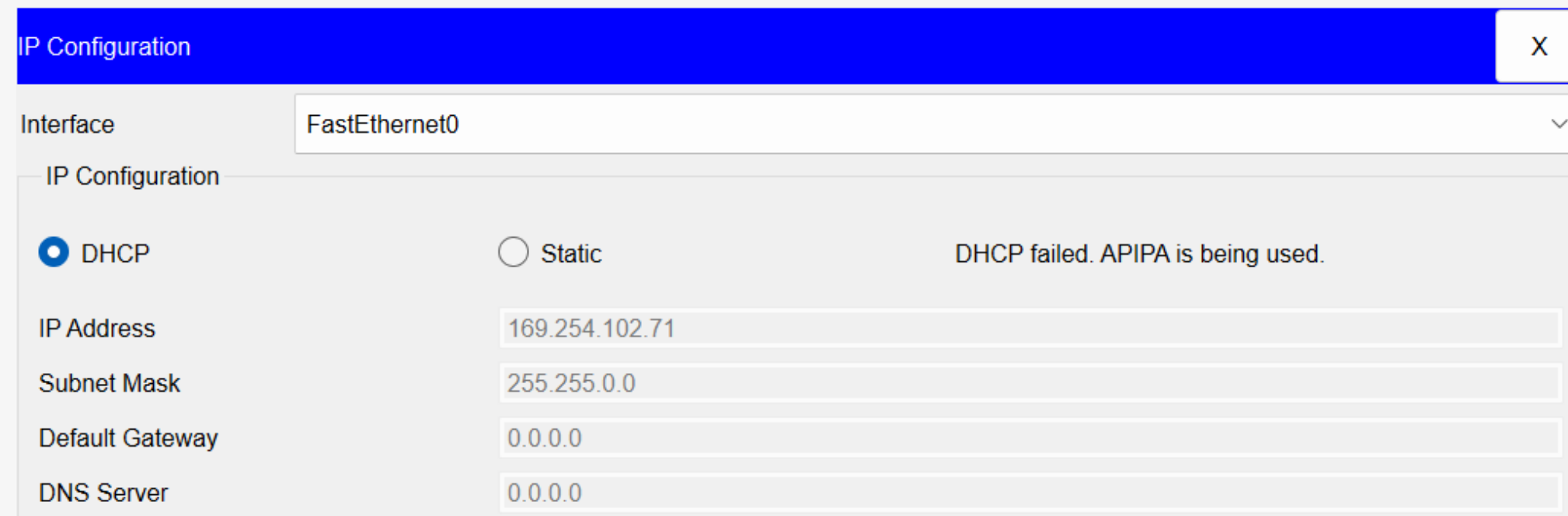


MESURES DE SÉCURITÉ DE DHCP

CONFIGURATION DE DHCP SNOOPING (PACKET TRACER)

-ACTIVATION DU 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)#
```



IP Configuration	
Interface	FastEthernet0
IP Configuration	
<input checked="" type="radio"/> DHCP	<input type="radio"/> Static
DHCP failed. APIPA is being used.	
IP Address	169.254.102.71
Subnet Mask	255.255.0.0
Default Gateway	0.0.0.0
DNS Server	0.0.0.0

MESURES DE SÉCURITÉ DE DHCP

CONFIGURATION DE DHCP SNOOPING (PACKET TRACER)

-CONFIGURATION DES PORTS DE CONFIANCE:

```
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#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

MESURES DE SÉCURITÉ DE DHCP

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static DHCP request successful.

IP Address 192.168.10.12

Subnet Mask 255.255.255.0

Default Gateway 192.168.10.10

DNS Server 0.0.0.0

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

MESURES DE SÉCURITÉ DE DHCP

CONFIGURATION DE DHCP SNOOPING (PACKET TRACER)

-AFFICHAGE DES INFORMATIONS DE LA BASE DE DONNÉES DE SURVEILLANCE :

```
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#
```

-CONFIGURATION DE LA LIMITE DE DÉBIT:

```
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
```

CONCLUSION

BIBLIOGRAPHIE

- ① PROTOCOLE DHCP: <https://www.frameip.com/dhcp/>
- ② A Step-by-Step Guide to Set up a DHCP Server on Ubuntu:
<https://www.linuxfordevices.com/tutorials/ubuntu/dhcp-server-on-ubuntu>
- ③ CCNA Sécurité : Attaque 2 : Épuisement des ressources DHCP (DHCP Starvation):
<https://www.nticprof.com/2019/06/dhcp-starvation.html>
- ④ DHCP Snooping: Stop Kali DHCP Hacks and MITM:
<https://www.youtube.com/watch?v=S6KI6VsvDuU&t=211s>
- ⑤ Sue Miller, (January 2001), DHCP for Windows 2000: Managing the Dynamic Host Configuration Protocol