GIANFERMI Matteo

S'initier aux réseaux informatiques

Sommaire :

I. *Découverte des hôtes*

Tout d'abord, j'utilise une VM de Kali Linux sur VirtualBox, que j'ai installé sur mon PC personnel. Dans les réglages réseau de VirtualBox, j'ai modifié le mode d'accès réseau par "accès par pont" pour avoir accès au réseau Wi-Fi de ma maison et de ne pas rester sur la carte réseau virtuel.

1. Lister les interfaces réseaux :

```
┌──(root㉿kali)-[/home/kali]
└─# ip -c addr
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 noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:cb:7e:f5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.72/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
       valid_lft 84159sec preferred_lft 84159sec
    inet6 2a02:842a:8383:2001:eed4:9f24:edaf:401e/64 scope global dynamic noprefixroute
       valid_lft 604627sec preferred_lft 604627sec
    inet6 fe80::acb:8914:7737:a14a/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

La commande “ip –c addr” permet de lister les interfaces réseaux et de mettre en couleur les informations importantes.

2. Pour chaque interface :

(a) Identifier les paramètres réseaux :

```
┌──(root㉿kali)-[/home/kali]
└─# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.72  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::acb:8914:7737:a14a  prefixlen 64  scopeid 0x20<link>
        inet6 2a02:842a:8383:2001:eed4:9f24:edaf:401e  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:cb:7e:f5  txqueuelen 1000  (Ethernet)
        RX packets 8228  bytes 1011895 (988.1 KiB)
        RX errors 0  dropped 19  overruns 0  frame 0
        TX packets 14457  bytes 986288 (963.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- Adresse IP (inet) = 192.168.1.72

- Masque de sous-réseau (netmask) : 255.255.255.0

- Adresse MAC (ether) = 08:00:27:cb:7e:f5

(b) Indiquer l’ensemble des adresses possibles :

La plage d'adresses IP possibles va de 192.168.1.1 à 192.168.1.254 . Il y a 254 adresses possibles.

(c) Lister les routeurs :

```
┌──(kali㉿kali)-[~]
└─$ ip -c route
default via 192.168.1.1 dev eth0 proto dhcp src 192.168.1.72 metric 100
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.72 metric 100
```

L’adresse du routeur est 192.168.1.1

La commande “ip –c route” permet de lister les routeurs et de mettre en couleur les informations importantes

3. Utiliser fping pour lister les adresses utilisées :

```
┌──(root㉿kali)-[/home/kali]
└─# fping -agq 192.168.1.0/24
192.168.1.1
192.168.1.23
192.168.1.26
192.168.1.31
192.168.1.35
192.168.1.61
192.168.1.63
192.168.1.72
192.168.1.65
192.168.1.66
192.168.1.79
192.168.1.80
```

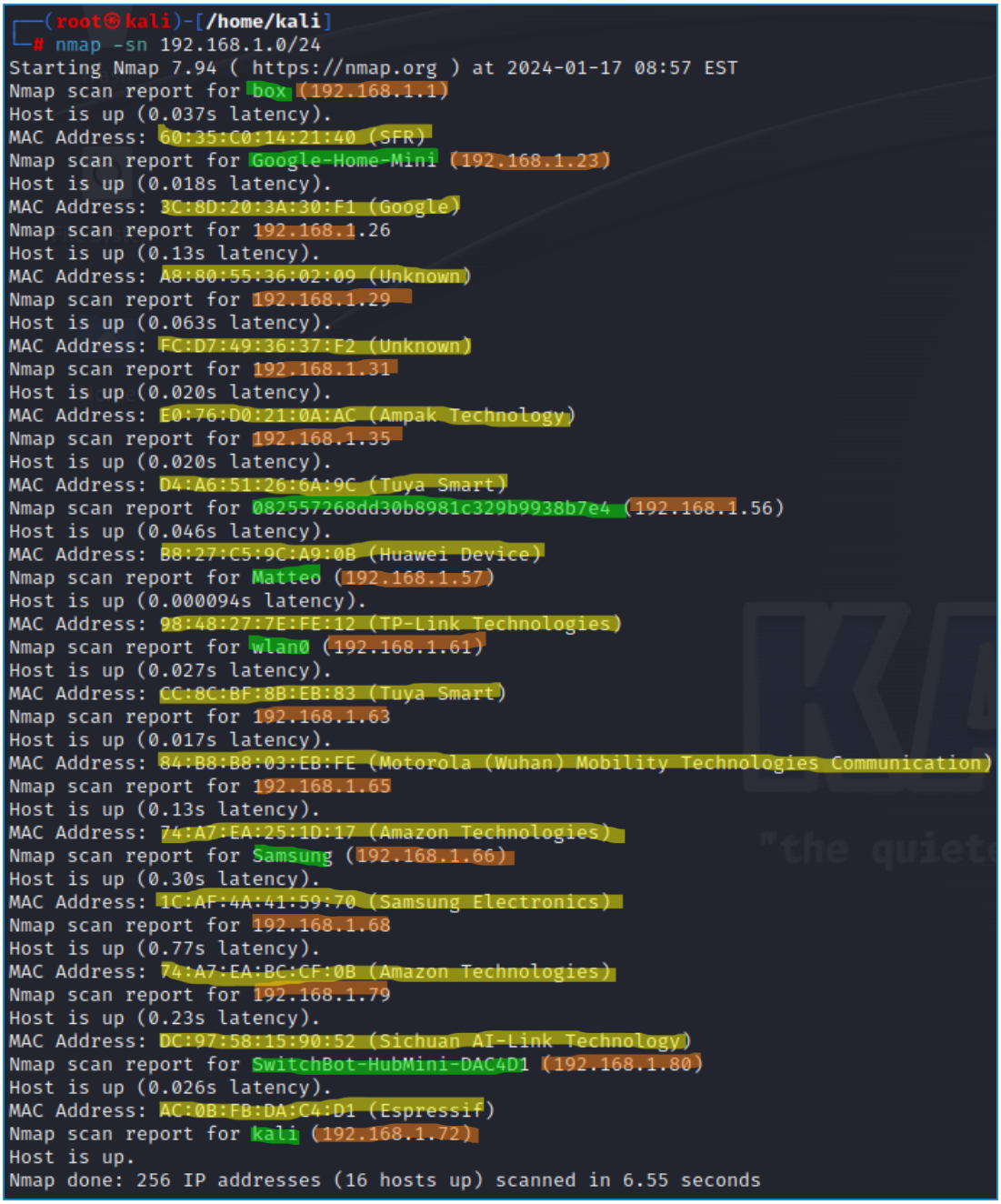
Il y a 12 adresses utilisées

- a : Permet d'afficher uniquement les adresses IP qui sont actives

- g : Permet de sélectionner la plage d'adresses IP à tester.

- q : Permet d'afficher uniquement le résumé final de toutes les requêtes ICMP.

4. Utiliser nmap pour lister les adresses utilisées.



On remarque que Nmap détecte 16 hôtes contrairement à fping qui n'en détecte que 12. On peut en déduire que la méthode de détection entre Nmap et fping n'est pas la même.

II. Identification des hôtes

1. ***Pour chaque hôte détecté :***

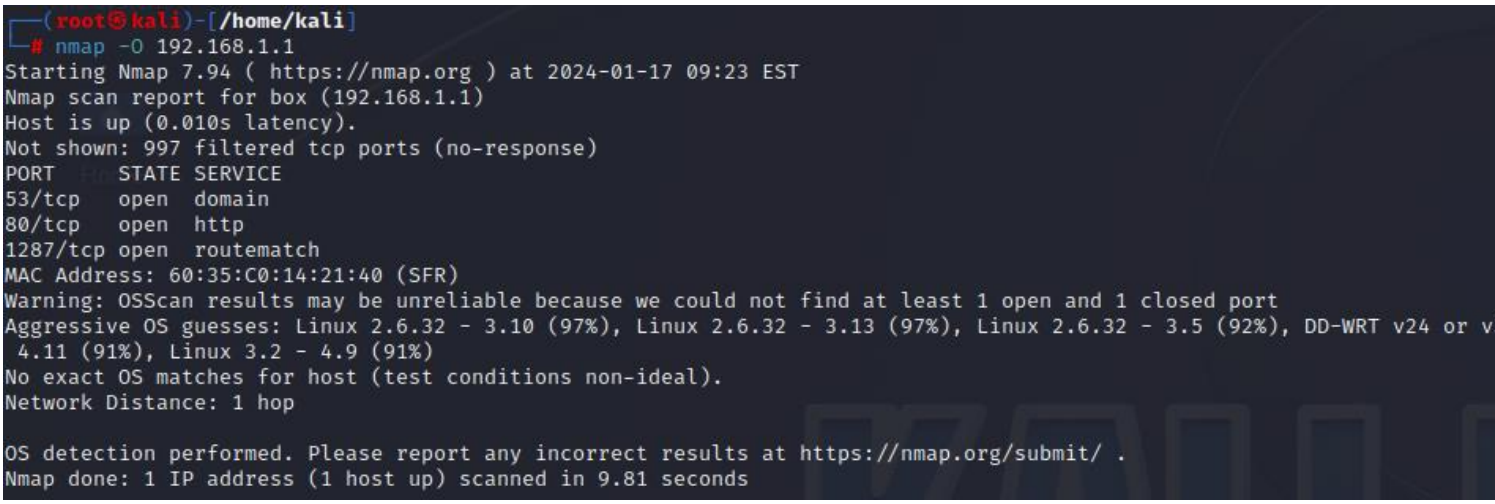
(a). Donner son adresse MAC et identifier le fabricant :

Le code couleur est situé sur la capture Nmap :

	= Adresse MAC et fabricant
	= Adresse IP
	= Nom de l'hôte

(b). Utiliser Nmap pour identifier, si possible, le système d'exploitation :

On utilise la commande "nmap -O 192.168.1.<hôte>" pour identifier le système d'exploitation d'un hôte.



La commande détecte Linux 2.6.32 - 3.10 comme OS avec 97% de fiabilité sur mon routeur SFR

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -O 192.168.1.23
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-17 10:11 EST
Nmap scan report for Google-Home-Mini (192.168.1.23)
Host is up (0.042s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
8008/tcp  open  http
8009/tcp  open  ajp13
8443/tcp  open  https-alt
9000/tcp  open  cslistener
10001/tcp open  scp-config
MAC Address: 3C:8D:20:3A:30:F1 (Google)
Aggressive OS guesses: Linux 2.6.32 - 3.10 (99%), Linux 3.10 (97%), Linux 3.2 - 3.16 (97%), Linux 3.6 (96%), Linux 3.7 (96%), Linu
.4) (96%), Android 4.1.1 (96%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.39 seconds
```

La commande détecte Linux 2.6.32 - 3.10 et Android 4.1.1 comme OS avec 99% de fiabilité et 96% sur mon Google Home Mini

Le reste de mes hôtes n'affiche pas les OS :

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -O 192.168.1.79
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-17 10:22
Nmap scan report for 192.168.1.79
Host is up (0.0091s latency).
All 1000 scanned ports on 192.168.1.79 are in ignored states
Not shown: 1000 closed tcp ports (reset)
MAC Address: DC:97:58:15:90:52 (Sichuan AI-Link Technology)
Too many fingerprints match this host to give specific OS de
Network Distance: 1 hop

OS detection performed. Please report any incorrect results
Nmap done: 1 IP address (1 host up) scanned in 1.92 seconds
```

II. Découverte des services disponibles

nmap -sT = Pour vérifier les ports TCP ouverts.

nmap –sU = Pour vérifier les ports UDP ouverts

Option “-p-” = Cette option permet de scanner tous les ports (de 1 à 65535)

Scan TCP parmi les plus souvent utilisés de mon IPhone

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.1.81
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-17 10:31 EST
Nmap scan report for 192.168.1.81
Host is up (0.11s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
49152/tcp open  unknown
62078/tcp open  iphone-sync
MAC Address: 32:AB:5F:A1:C2:58 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 301.26 seconds
```

Scan UDP parmi les plus souvent utilisés de mon IPhone

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sU 192.168.1.81
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-17 10:38 EST
Nmap scan report for 192.168.1.81
Host is up (0.018s latency).
Not shown: 999 closed udp ports (port-unreach)
PORT     STATE         SERVICE
5353/udp open|filtered zeroconf
MAC Address: 32:AB:5F:A1:C2:58 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.31 seconds
```

Scan TCP parmi les plus souvent utilisés de ma box SFR

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.1.1
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-17 13:36 EST
Nmap scan report for box (192.168.1.1)
Host is up (0.019s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
1287/tcp open  routematch
MAC Address: 60:35:C0:14:21:40 (SFR)

Nmap done: 1 IP address (1 host up) scanned in 7.59 seconds
```

Scan UDP parmi les plus souvent utilisés de ma box SFR

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sU 192.168.1.1
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-17 13:37 EST
Nmap scan report for box (192.168.1.1)
Host is up (0.021s latency).
Not shown: 995 open|filtered udp ports (no-response)
PORT     STATE  SERVICE
53/udp   open   domain
67/udp   open   dhcps
68/udp   closed dhcpc
123/udp  open   ntp
1900/udp open   upnp
MAC Address: 60:35:C0:14:21:40 (SFR)

Nmap done: 1 IP address (1 host up) scanned in 7.11 seconds
```

Scan TCP parmi TOUS ports utilisés de ma box SFR

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT -p- 192.168.1.1
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-17 11:21 EST
Nmap scan report for box (192.168.1.1)
Host is up (0.013s latency).
Not shown: 65531 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
1287/tcp open  routematch
1288/tcp open  navbuddy
MAC Address: 60:35:C0:14:21:40 (SFR)

Nmap done: 1 IP address (1 host up) scanned in 140.11 seconds
```

Scan UDP parmi TOUS ports utilisés de ma box SFR

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sU -p- 192.168.1.1
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-17 11:27 EST
Nmap scan report for box (192.168.1.1)
Host is up (0.060s latency).
Not shown: 65530 open|filtered udp ports (no-response)
PORT     STATE  SERVICE
53/udp   open   domain
67/udp   open   dhcps
68/udp   closed dhcpc
123/udp  open   ntp
1900/udp open   upnp
MAC Address: 60:35:C0:14:21:40 (SFR)

Nmap done: 1 IP address (1 host up) scanned in 549.33 seconds
```

Scan TCP parmi les plus souvent utilisés de ma caméra IP : Grace à ce scan je peux aller sur le site de ma caméra car je connais le port pour se connecter : 88

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.1.31
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-18 00:58 EST
Nmap scan report for 192.168.1.31
Host is up (0.013s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE
88/tcp  open  kerberos-sec
443/tcp open  https
888/tcp open  accessbuilder
MAC Address: E0:76:D0:21:0A:AC (Ampak Technology)

Nmap done: 1 IP address (1 host up) scanned in 0.70 seconds
```

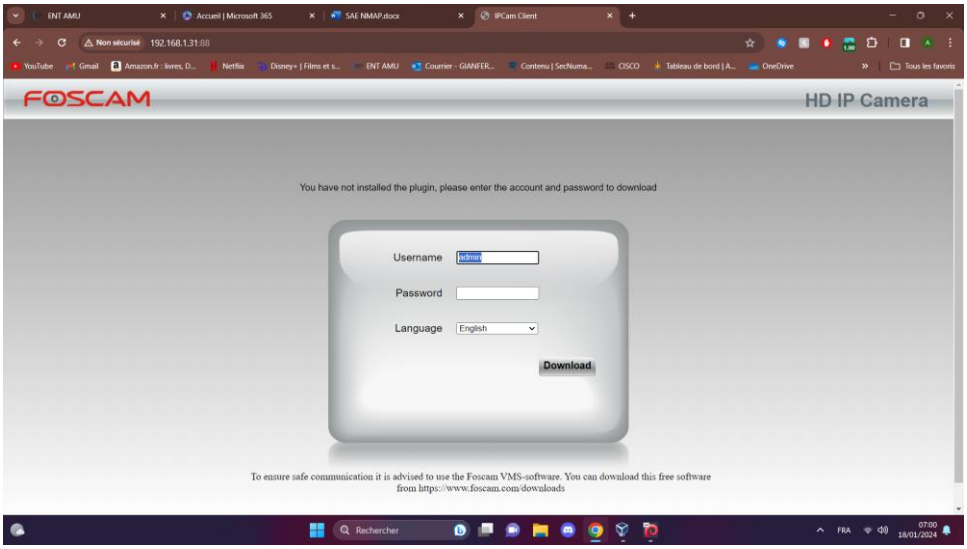


Schéma de mon réseaux privé :