



TP - KALI

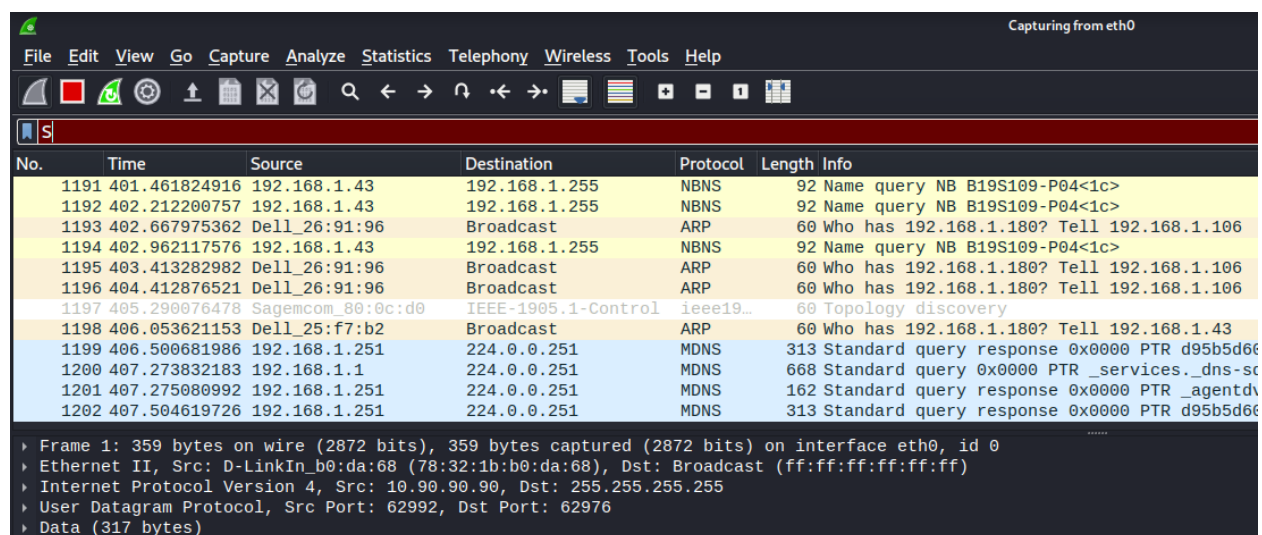
Gomez Gaétan

Travail à faire :

a. Analyse de la capture du ping

➡ A partir de Kali, lancez l'outil wireshark, et lancez la capture de trafic sur l'interface eth0

en lançant l'outil wireshark je suis aller sur capture et start tout en sélectionnant eth0



No.	Time	Source	Destination	Protocol	Length	Info
1191	401.461824916	192.168.1.43	192.168.1.255	NBNS	92	Name query NB B19S109-P04<1c>
1192	402.212200757	192.168.1.43	192.168.1.255	NBNS	92	Name query NB B19S109-P04<1c>
1193	402.667975362	Dell_26:91:96	Broadcast	ARP	60	Who has 192.168.1.180? Tell 192.168.1.106
1194	402.962117576	192.168.1.43	192.168.1.255	NBNS	92	Name query NB B19S109-P04<1c>
1195	403.413282982	Dell_26:91:96	Broadcast	ARP	60	Who has 192.168.1.180? Tell 192.168.1.106
1196	404.412876521	Dell_26:91:96	Broadcast	ARP	60	Who has 192.168.1.180? Tell 192.168.1.106
1197	405.290076478	Sagemcom_80:0c:d0	IEEE-1905.1-Control	ieee19...	60	Topology discovery
1198	406.053621153	Dell_25:f7:b2	Broadcast	ARP	60	Who has 192.168.1.180? Tell 192.168.1.43
1199	406.500681986	192.168.1.251	224.0.0.251	MDNS	313	Standard query response 0x0000 PTR d95b5d66
1200	407.273832183	192.168.1.1	224.0.0.251	MDNS	668	Standard query 0x0000 PTR _services._dns-sc
1201	407.275080992	192.168.1.251	224.0.0.251	MDNS	162	Standard query response 0x0000 PTR _agentdv
1202	407.504619726	192.168.1.251	224.0.0.251	MDNS	313	Standard query response 0x0000 PTR d95b5d66

▶ Frame 1: 359 bytes on wire (2872 bits), 359 bytes captured (2872 bits) on interface eth0, id 0
 ▶ Ethernet II, Src: D-LinkIn_b0:da:68 (78:32:1b:b0:da:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 ▶ Internet Protocol Version 4, Src: 10.90.90.90, Dst: 255.255.255.255
 ▶ User Datagram Protocol, Src Port: 62992, Dst Port: 62976
 ▶ Data (317 bytes)

➡ A partir de la hôte, lancez un ping vers la machine Kali

j'ai ping ma machine kali depuis l'hôte avant tout ça j'ai chercher l'adresse depuis le terminale de la machine kali en faisant "ip a"

```
PS C:\Users\maeva.phan> ping 192.168.1.14

Envoi d'une requête 'Ping' 192.168.1.14 avec 32 octets de données :
Réponse de 192.168.1.14 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.14 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.14 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.14 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.1.14:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

➡ Analysez les PDU capturés et répondez aux questions suivantes :

➡ Quelle est l'adresse source des paquets en destination de Kali ?

l'adresse sources et tout simplement 192.168.1.105 en destination de ma machine kali

```
630 200.792445384 192.168.1.105 192.168.1.14 ICMP 74 Echo (ping) request id=0x0001, seq=10/2560, ttl=128 (reply in 631)
```

➡ Le Ping utilise-t-elle un protocole de la couche transport ? si, oui, lequel ?

Le ping utilise le protocole de la couche transport, ICMP

Protocol
ICMP
ICMP
ICMP
ICMP
ICMP

➡ Quel est le protocole de la couche réseau (IP) utilisés par Ping ?

Le protocole de la couche réseau utilisé par ping et aussi ICMP

Protocol
ICMP
ICMP
ICMP
ICMP
ICMP

➡ Quel est le type de message (icmp) envoyés par ping ?

le type de message icmp envoyeés par ping et request

request

➡ Quel est le type de message (icmp) de réponses envoyés par Kali ?

le type de message icmp envoyeés par kali et reply

reply

b. Analyse de la capture de traceroute

➡ A partir de la hôte, lancez la commande 'tracert @ip Kali' vers la machine Kali

tracert @ip kali & tracert 192.168.1.14 revient au même

```
PS C:\Users\maeva.phan> tracert @ip kali

Détermination de l'itinéraire vers kali.home [192.168.1.14]
avec un maximum de 30 sauts :

    1    <1 ms    <1 ms    <1 ms    kali.home [192.168.1.14]

Itinéraire déterminé.
PS C:\Users\maeva.phan> tracert 192.168.1.14

Détermination de l'itinéraire vers kali.home [192.168.1.14]
avec un maximum de 30 sauts :

    1    <1 ms    <1 ms    <1 ms    kali.home [192.168.1.14]

Itinéraire déterminé.
```

➡ Analysez les PDU capturés et répondez aux questions suivantes :

- traceroute utilise-t-il un protocole de la couche transport ?

Traceroute sous Linux utilise UDP comme protocole de transport pour envoyer des paquets IP. ... Lorsque le paquet atteint enfin la destination, il ne doit plus être routé. Ainsi, la destination ne renvoie aucun message d'erreur ICMP à la source.

- quel est le protocole de la couche réseau utilisé par traceroute ?

Le protocole utilisé par traceroute est ICMP

Protocol
ICMP
ICMP
ICMP
ICMP
ICMP
ICMP

- Comment fonctionne la commande traceroute ?

La commande traceroute tente d'effectuer le traçage de la route qu'un paquet IP suit pour accéder à un hôte Internet

- Dans les PDU de la couche réseau envoyés par la hôte, quelle est la valeur du champ Time to Live ?

La valeur du champ time to live est de 64

No.	Time	Source	Destination	Protocol	Length	Info
586	123.458393302	192.168.1.105	192.168.1.14	ICMP	106	Echo (ping) request id=0x0001, seq=20/5120, ttl=1 (reply in 587)
587	123.458412268	192.168.1.14	192.168.1.105	ICMP	106	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64 (request in 586)

c. Analyse de la capture d'une interaction avec un serveur Web

➡ A partir de la Kali, lancez le serveur web apache : `# service apache2 start`
Si il n'est pas installé dans le terminal `#apt-get install apache2`

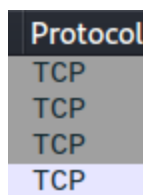
Pour installer apache 2 il faut:

- Aller sur le terminal de kali,
- Se mettre en administrateur avec la commande `sudo su`
- Taper la commande `apt-get install apache2` (toujours sur le terminale)
- Dès qu'il c'est installer il faut tout simplement
- Taper `service apache2 start` (toujours en tant qu'administrateur sur le terminale)
- Nous pouvons ensuite ouvrir apache2 depuis notre système d'exploration (firefox)
- Taper localhost une page devrait apparaître avec apache2



➡ Quel est le protocole de la couche de transport utilisé durant cette interaction

Le protocole de la couche transport utilisé durant cette interaction est le protocole TCP



➡ Identifiez les paquets d'établissements de connexion TCP, et en extraire les numéros de séquences et d'acquittements

Je pense que les numéros de séquences et d'acquittement sont 0 et 0 j'ai trouver ça en taper tcp dans capture wireshark

▶ Transmission Control Protocol, Src Port: 37188, Dst Port: 443, Seq: 0, Len: 0

➡ Quel est le protocole de la couche application utilisé

HTTP

➡ Quel est le port source, et le port de destination

Le port sources est 37188 et le port de destination est 443 j'ai taper http ainsi j'ai cliquer sur l'adresse avec laquelle cela à était envoyer pour le trouver nous le trouvons dans la console. Tout cela s'effectue sur wireshark dans la console.

▶ Transmission Control Protocol, Src Port: 37188, Dst Port: 443

➡ Quel est le type de requête envoyé par le client pour afficher la page web.

HTTP

▶ Transmission Control Protocol, Src Port: 59970, Dst Port: 80, Seq: 1, Ack: 1, Len: 337

➡ Quel est la version du serveur web utilisé.

▶ 353 59.775934939 192.168.1.14 5.22.145.16 HTTP 403 GET //192.168.1.14/ HTTP/1.1

Activité II) nmap : découvertes des machines et des services

➡ A l'invite du terminal, saisissez `man nmap`. `$ man nmap`

Quand j'ai taper `$ man nmap` un guide d'utilisation de la commande c'est afficher

```
NMAP(1)                                Nmap Reference Guide                                NMAP(1)
NAME
    nmap - Network exploration tool and security / port scanner
SYNOPSIS
    nmap [Scan Type ...] [Options] {target specification}
```

➡ Qu'est-ce que Nmap ?

Nmap est un sniffer réseau, un scanner de ports libres.

Ce logiciel est devenu une référence pour les administrateurs réseaux car l'audit des résultats de Nmap fournit des indications sur la sécurité d'un réseau. Il est disponible sous Windows, Mac OS X, Linux, BSD et Solaris.

➡ À quoi Nmap sert-il ?

Il est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant.

Pour scanner les ports d'un ordinateur distant, diverses techniques d'analyse basées sur des protocoles tels que TCP, IP, UDP ou ICMP.

Par défaut Nmap scanne les port de 1 à 1024 et les ports indiqués dans le fichier `nmap-services`.

➡ Saisissez /example et appuyez sur ENTRÉE. Cette opération permet de rechercher le mot exemple vers l'avant dans les pages du manuel.

```

kali@kali: ~
File Actions Edit View Help

A typical Nmap scan is shown in Example 1. The only Nmap arguments
used in this example are -A, to enable OS and version detection,
script scanning, and traceroute; -T4 for faster execution; and then
the hostname.

Example 1. A representative Nmap scan

# nmap -A -T4 scanme.nmap.org

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.3p1 Debian 3ubuntu7 (proto
col 2.0)
Manual page nmap(1) line 46 (press h for help or q to quit)

```

a. Dans le premier exemple, trois correspondances s'affichent. Pour accéder à la correspondance suivante, appuyez sur n.

Pour descendre d'un article à l'autre il faut taper n.

➡ Quelle est la commande nmap utilisée ?

La commande nmap utilisée pour pouvoir afficher l'exemple 1 c'est /example.

➡ Utilisez la fonction de recherche pour répondre aux questions suivantes.

- À quoi sert le commutateur -A ?

- À quoi sert le commutateur -T4 ?

Sert à regarder les port ouvert et nous pouvons même voir sur qu'elle système d'exploitation

➡ Faites défiler la page pour en savoir plus sur nmap. Saisissez « q » lorsque vous avez terminé

Quand on fait défiler la page pour en savoir plus sur nmap on peut voir, option summary, target specification etc...

II.1 Découverte du réseau avec map

➡ Effectuez une découverte d'hôtes, et déterminez les adresses IP+MAC des hôtes en ligne se trouvant dans le même réseau que Kali (utilisez l'option -sP)

```
(root@kali)~[/home/kali]
# nmap -sP 192.168.1.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-31 05:15 EST
Nmap scan report for lan.home (192.168.1.1)
Host is up (0.00054s latency).
MAC Address: D4:F8:29:80:0C:D0 (Sagemcom Broadband SAS)
Nmap scan report for ilocz162500hl.home (192.168.1.18)
Host is up (1.1s latency).
MAC Address: D0:BF:9C:3A:D2:CF (Hewlett Packard)
Nmap scan report for pc-3.home (192.168.1.24)
Host is up (0.74s latency).
MAC Address: D0:BF:9C:3A:D2:CC (Hewlett Packard)
Nmap scan report for b19s109-p15.home (192.168.1.28)
Host is up (0.00068s latency).
MAC Address: 70:B5:E8:25:F9:5F (Dell)
Nmap scan report for b19s109-p20.home (192.168.1.34)
Host is up (0.00051s latency).
MAC Address: 70:B5:E8:26:92:3C (Dell)
Nmap scan report for desktop-a7svcce.home (192.168.1.40)
Host is up (0.00045s latency).
MAC Address: 70:B5:E8:26:91:38 (Dell)
Nmap scan report for b19s109-p01.home (192.168.1.44)
Host is up (0.00033s latency).
MAC Address: 70:B5:E8:25:F7:DD (Dell)
Nmap scan report for 211-9.home (192.168.1.47)
Host is up (0.00055s latency).
MAC Address: 70:B5:E8:26:91:98 (Dell)
Nmap scan report for desktop-gvuhj4h.home (192.168.1.56)
Host is up (0.00055s latency).
MAC Address: 70:B5:E8:25:F7:99 (Dell)
Nmap scan report for D109-2.home (192.168.1.105)
Host is up (0.00012s latency).
MAC Address: 70:B5:E8:2A:62:DC (Dell)
Nmap scan report for pc-150.home (192.168.1.115)
Host is up (0.0052s latency).
MAC Address: 74:59:09:DA:E6:2C (Huawei Technologies)
Nmap scan report for redmi7-redmi.home (192.168.1.156)
Host is up (0.095s latency).
```

➡ Lancer un scan en ciblant la machine locale (Kali) et déterminez les services ouverts ainsi que le système d'exploitation, lancez ftp et http ensuite relancez le scan

```
(root@kali)-[/home/kali]
# nmap -sS -O 192.168.1.14
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-31 05:18 EST
Nmap scan report for kali.home (192.168.1.14)
Host is up (0.000023s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.97 seconds
```

➡ Lancer un scan en ciblant le routeur :

```
(root@kali)-[/home/kali]
# nmap -sS -O 192.168.1.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-31 05:19 EST
Nmap scan report for lan.home (192.168.1.1)
Host is up (0.0020s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
113/tcp   closed ident
135/tcp   closed msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
631/tcp   open  ipp
MAC Address: D4:F8:29:80:0C:D0 (Sagemcom Broadband SAS)
Device type: general purpose|media device|storage-misc|firewall
Running (JUST GUESSING): Linux 2.6.X|3.X|4.X (96%), Dish embedded (93%), Excito embedded (89%), WatchGuard Firewall 11.X (89%), Synology DiskStation Manager 5.X (88%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/h:dish:hopper cpe:/o:linux:linux_kernel:3 cpe:/h:excito:b3 cpe:/o:watchguard:fireware:11.8 cpe:/o:linux:linux_kernel cpe:/a:synology:diskstation_manager:5.1 cpe:/o:linux:linux_kernel:4
Aggressive OS guesses: Linux 2.6.32 (96%), Dish Network Hopper media device (93%), Linux 3.2 - 3.8 (91%), Linux 2.6.32 - 3.10 (90%), Linux 2.6.32 - 3.0 (90%), Linux 3.0 (90%), Excito B3 file server (Linux 2.6.39) (89%), Linux 2.6.39 (89%), Linux 3.4 (89%), WatchGuard Firewall 11.8 (89%)
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 9.13 seconds
```

➡ De quelle façon peut-on cibler plusieurs machines avec une seule exécution de la commande ?

en faisant un nmap -sP et l'adresse ip du réseau.

➡ Comment scanner une plage d'adresses IP de classe C?

une plage d'adresse IP de classe C, est réseaux 192.0.0 à 223.255.255

```
(root@kali)-[/home/kali]
# nmap -sS -O 192.168.1.1 192.168.1.250
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-16 07:11 EST
Packet Tracing enabled.
SENT (23.1487s) TCP 192.168.1.35:59000 > 192.168.1.1:1089 S ttl=53 id=
```

➡ Lancez un sniffing Wireshark sur Kali, ensuite effectuez deux scan nmap de types « scan TCP

➡ SYN » et « scan Xmas » respectivement. Examinez les paquets capturés associés à chacune des deux techniques de scan et déterminez la différence entre elles.

nmap

Pour le scan TCP de SYN j'a effectuer un nmap -sS + adresse ip

```
(root@kali)-[/home/kali]
# nmap -sS 192.168.1.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-16 07:28 EST
Nmap scan report for livebox.home (192.168.1.1)
Host is up (0.0095s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
113/tcp   closed ident
135/tcp   closed msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
631/tcp   open  ipp
MAC Address: D4:F8:29:80:0C:D0 (Sagemcom Broadband SAS)

Nmap done: 1 IP address (1 host up) scanned in 4.58 seconds
```

Pour le scan Xmas j'ai effectué un nmap -sX + adresse ip (192.168.1.1) j'ai alors obtenue des résultats depuis wireshark.

```
(root@kali)-[/home/kali]
# nmap -sX 192.168.1.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-16 07:32 EST
Nmap scan report for livebox.home (192.168.1.1)
Host is up (0.0020s latency).
Not shown: 998 open|filtered tcp ports (no-response)
PORT      STATE SERVICE
113/tcp    closed ident
135/tcp    closed msrpc
MAC Address: D4:F8:29:80:0C:D0 (Sagemcom Broadband SAS)

Nmap done: 1 IP address (1 host up) scanned in 4.77 seconds
```

Les résultats obtenus avec wireshark en recherchant "TCP" voici les protocole TCP obtenu

35	4.099382750	192.168.1.35	192.168.1.1	TCP	54 43132 → 5900 [FIN, PSH]
36	4.099393754	192.168.1.35	192.168.1.1	TCP	54 43132 → 3389 [FIN, PSH]
37	4.099405349	192.168.1.35	192.168.1.1	TCP	54 43132 → 23 [FIN, PSH]
38	4.099416879	192.168.1.35	192.168.1.1	TCP	54 43132 → 256 [FIN, PSH]
39	4.100906058	192.168.1.1	192.168.1.35	TCP	60 113 → 43132 [RST, ACK]
40	4.101581936	192.168.1.1	192.168.1.35	TCP	60 135 → 43132 [RST, ACK]
41	4.103950800	192.168.1.35	192.168.1.1	TCP	54 43132 → 993 [FIN, PSH]
42	4.103983880	192.168.1.35	192.168.1.1	TCP	54 43132 → 1025 [FIN, PSH]
43	4.103995886	192.168.1.35	192.168.1.1	TCP	54 43132 → 8888 [FIN, PSH]
44	4.104006002	192.168.1.35	192.168.1.1	TCP	54 43132 → 8080 [FIN, PSH]

II.2 Analyse des ports ouverts sur un réseau

b. Si nécessaire, ouvrez un terminal sur la machine virtuelle. À l'invite, saisissez nmap -A -T4 localhost. Selon votre réseau local et vos périphériques, l'analyse peut durer de quelques secondes à quelques minutes.

```
(root@kali)-[/home/kali]
# nmap -A -T4 localhost
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-16 07:46 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000043s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.51 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.51 (Debian)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

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 8.82 seconds
```

c. Vérifiez les résultats et répondez aux questions suivantes.

Questions :

- ➡ Quels sont les ports et les services ouverts ?
- ➡ Pour chacun des ports ouverts, notez le nom de l'application qui fournit le service.

Le port ouvert est 80/tcp et le services et http l'application qui fourni le service est apache.

```
80/tcp open  http    Apache httpd 2.4.51 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.51 (Debian)
```

II.3 Analysez le réseau local

- ➡ À quel réseau votre machine virtuelle appartient-elle ?

Ma machine virtuelle appartient au réseau est 127.0.0.1

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
   link/ether 08:00:27:50:4c:14 brd ff:ff:ff:ff:ff:ff
   inet 192.168.1.35/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
       valid_lft 82799sec preferred_lft 82799sec
   inet6 fe80::a00:27ff:fe50:4c14/64 scope link dadfailed tentative noprefixroute
       valid_lft forever preferred_lft forever
```



```
(root@kali)~[/home/kali]
# nmap -A -T5 192.168.1.250
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-16 08:24 EST
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Warning: 192.168.1.250 giving up on port because retransmission cap hit (2).
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 08:25 (0:00:06 remaining)
Stats: 0:01:30 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 83.33% done; ETC: 08:26 (0:00:17 remaining)
Nmap scan report for 192.168.1.250
Host is up (0.0024s latency).
Not shown: 969 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
1/tcp     filtered tcpmux
21/tcp    open  ftp      Brother/HP printer ftpd 1.13
|ftp-anon: Anonymous FTP login allowed (FTP code 230)
|total 1
|_--r--r-- 1 root      printer  4096 Sep 28  2001 CFG-PAGE.TXT
|_--r--r-- 1 root      printer    0 Sep 28  2001 VEILLE
|_
23/tcp    open  telnet   Brother/HP printer telnetd
80/tcp    open  http     Debut embedded httpd 1.08 (Brother/HP printer http admin)
|_http-title: Brother HL-5350DN series
|_Requested resource was /printer/main.html
|_http-server-header: debut/1.08
515/tcp   open  printer
631/tcp   open  ipp?
1062/tcp  filtered veracity
1082/tcp  filtered amt-esd-prot
1216/tcp  filtered etebac5
1433/tcp  filtered ms-sql-s
1500/tcp  filtered vlsi-lm
1805/tcp  filtered enl-name
2107/tcp  filtered msmq-mgmt
2500/tcp  filtered rtsserv
2718/tcp  filtered pn-requester2
2920/tcp  filtered roboeda
3011/tcp  filtered trusted-web
3071/tcp  filtered csd-mgmt-port
3077/tcp  filtered csd-mgmt-port
3827/tcp  filtered netmpi
5566/tcp  filtered westec-connect
5922/tcp  filtered unknown
7070/tcp  filtered realserv
9090/tcp  filtered zeus-admin
9100/tcp  open  jetdirect?
9101/tcp  filtered jetdirect
10215/tcp filtered unknown
15000/tcp filtered hydap
49154/tcp filtered unknown
49157/tcp filtered unknown
50000/tcp filtered ibm-db2
65389/tcp filtered unknown
MAC Address: 00:1B:A9:21:AA:9D (Brother industries)
Device type: printer|webcam
Running: HP embedded, Brother embedded, Sony embedded
OS CPE: cpe:/h:sony:snc-rz30n
OS details: HP LaserJet (1020-, 2010-, 2600-, 2800-, 3050-, or 3390-series), or Brother (DCP-375CW, HL-5250DN, HL-22700W, MFC-7840N, MFC-8860DN, or MFC-9970CDW) printer; or Sony SNC-RZ30N network camera
Network Distance: 1 hop
Service Info: Device: printer

TRACEROUTE
HOP RTT      ADDRESS
1   2.41 ms  192.168.1.250

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 115.83 seconds
```

➡ Dans l'exemple ci-dessus, combien d'hôtes sont actifs ?

Il y a sur l'exemple ci-dessus 3 hôtes actifs.

➡ Quelles adresses IP et quels ports et services sont ouverts ?

Il y a 3 ports ouverts,

qui ont pour adresse ip 21,22 et 23.