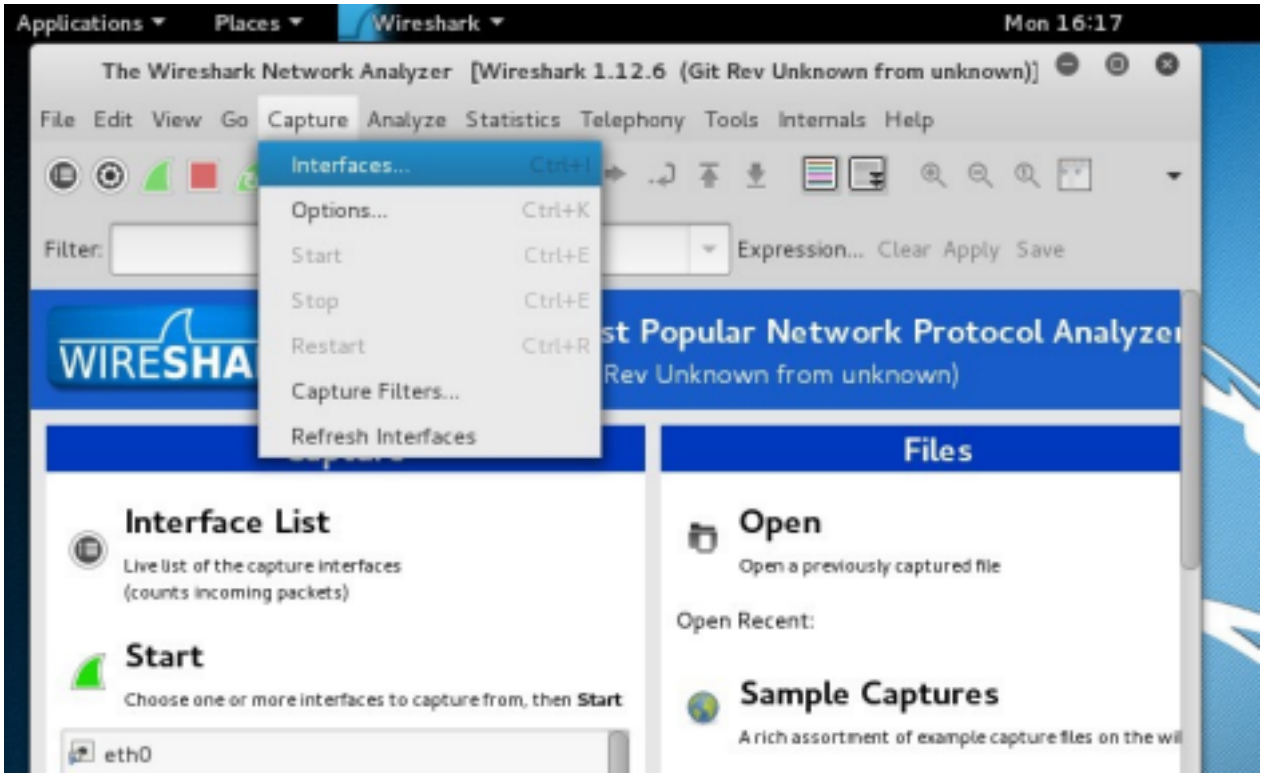
Installation et utilisation Kali Linux

Informer les utilisateurs et mettre en œuvre les défenses appropriées.

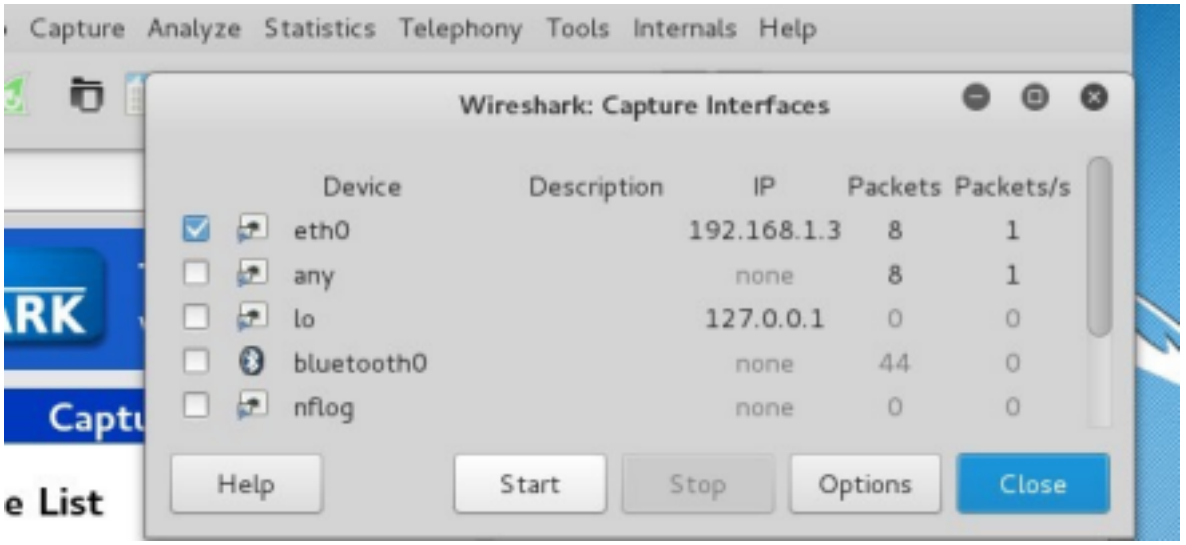
Wireshark, nmap

Activité I) Wireshark : Lancer une capture de trames ?

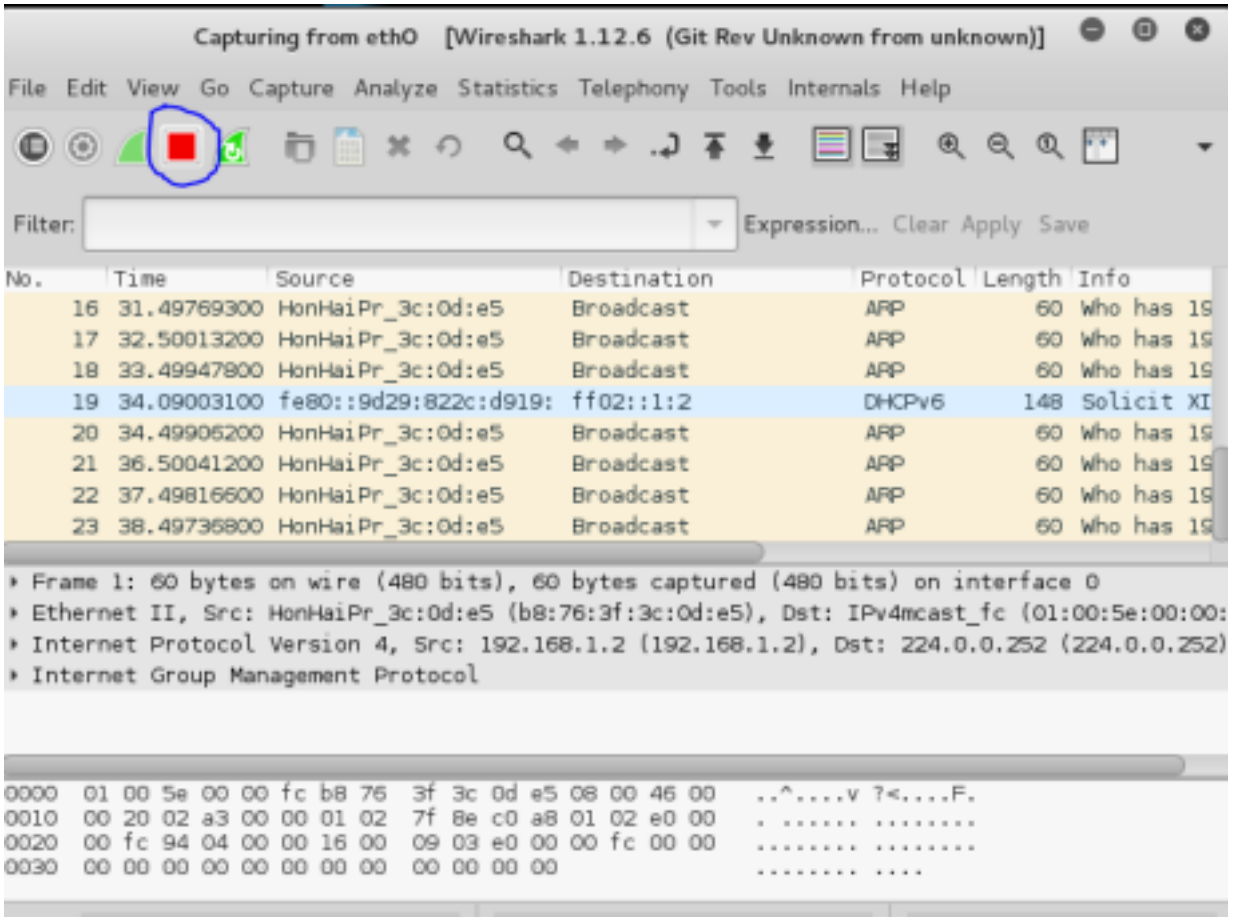
Lancer l'application Wireshark. Vous devriez voir apparaître une fenêtre similaire à celle-ci :



Dans le menu `capture`, sélectionner le sous-menu `Interfaces` et lancer une capture de trame sur la carte réseau portant votre adresse IP et appuyer sur `Start`



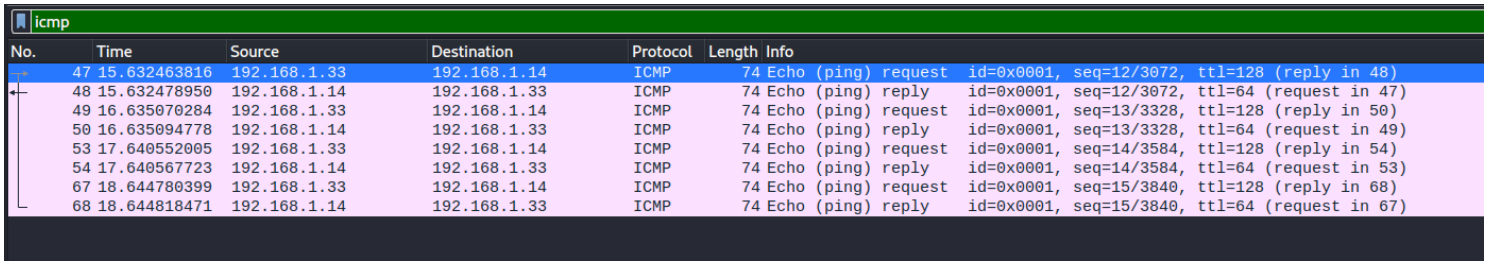
Arrêter la capture en cliquant sur le bouton arrêter en rouge (voir image ci-dessous).
Une fois la capture effectuée, vous obtiendrez la fenêtre suivante :



Travail à faire :

a. Analyse de la capture du ping

- Démarrer la machine virtuelle Kali en mode « *host only* »
- A partir de Kali, lancez l'outil wireshark, et lancez la capture de trafic sur l'interface eth0
- A partir de la hôte, lancez un ping vers la machine Kali
- Attendez jusqu'à ce que le ping soit terminé, ensuite arrêtez la capture wireshark sur Kali



➡ Analysez les PDU capturés et répondez aux questions suivantes :

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

C'est l'adresse 192.168.1.33

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

Oui il utilise le protocole ICMP

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

  C'est le protocole ICMP.

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

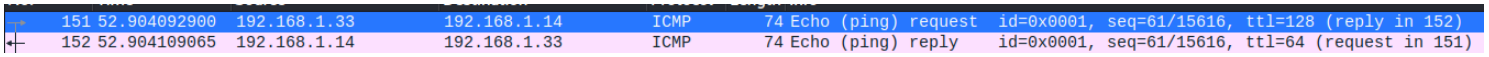
  Le type de message est un echo request

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

  Le type de message est un echo reply

b. Analyse de la capture de traceroute

- A partir de Kali, lancez l'outil Wireshark, et lancez la capture de trafic sur eth0
- A partir de la hôte, lancez la commande 'tracert @ip Kali' vers la machine Kali
- Attendez jusqu'à ce que tracert soit terminé, ensuite arrêtez la capture Wireshark sur Kali



- Analysez les PDU capturés et répondez aux questions suivantes :

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

  Oui, il utilise le protocole ICMP.

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

  Il utilise le protocole ICMP.

- Comment fonctionne la commande traceroute ?

  Elle indique tous les routeurs dont le ping passe pour atteindre sa cible.

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

  La valeur du champ TTL est de 64

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

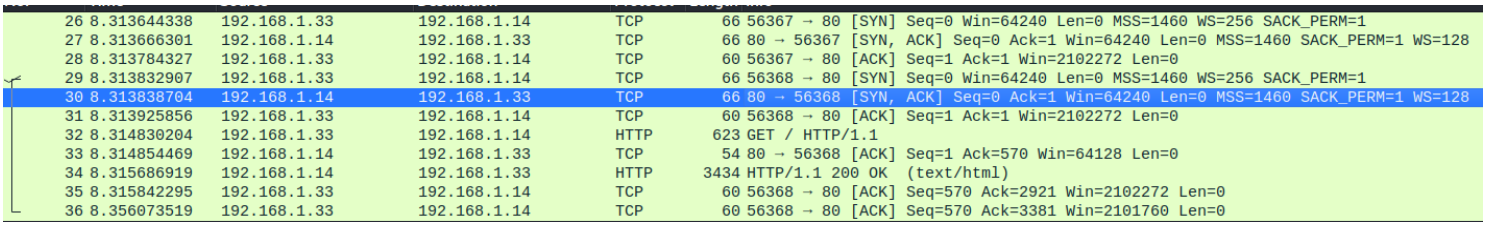
Si il n'est pas installé dans le terminal #apt-get install apache2

```
┌──(kali㉿kali)-[~]
└─$ sudo su

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
┌──(root💀kali)-[/home/kali]
└─# apt-get install apache2
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
apache2 is already the newest version (2.4.51-2).
apache2 set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 377 not upgraded.

┌──(root💀kali)-[/home/kali]
└─# service apache2 status
o apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
     Active: inactive (dead)
       Docs: https://httpd.apache.org/docs/2.4/

┌──(root💀kali)-[/home/kali]
└─# service apache2 start

┌──(root💀kali)-[/home/kali]
└─# service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
     Active: active (running) since Mon 2022-01-24 05:27:14 EST; 4s ago
```

- Vérifiez que le serveur web est lancé par la commande : netstat -antp

```
┌──(root💀kali)-[/home/kali]
└─# netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 192.168.1.14:51442      93.184.220.29:80        TIME_WAIT   -
tcp        0      0 192.168.1.14:51440      93.184.220.29:80        ESTABLISHED 15513/firefox-esr
tcp        0      0 192.168.1.14:54362      142.250.178.138:443     ESTABLISHED 15513/firefox-esr
tcp        0      0 192.168.1.14:53890      52.222.174.28:443       ESTABLISHED 15513/firefox-esr
tcp        0      0 192.168.1.14:54080      142.250.74.227:80       TIME_WAIT   -
tcp        0      0 192.168.1.14:36894      54.191.212.31:443       ESTABLISHED 15513/firefox-esr
tcp        0      0 192.168.1.14:49950      35.244.181.201:443      ESTABLISHED 15513/firefox-esr
tcp6       0      0 :::80                   :::*                    LISTEN      15440/apache2
```

- A partir de la Kali, lancez l'outil Wireshark, et lancez la capture de trafic sur eth0
- A partir de la hôte, ouvrez le navigateur web, et taper l'adresse http://@ip-de-Kali pour accéder au serveur web de Kali.
- Attendez jusqu'à ce qu'une page web s'affiche sur le navigateur web, ensuite arrêtez la capture Wireshark.



26	8.313644338	192.168.1.33	192.168.1.14	TCP	66	56367 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
27	8.313666301	192.168.1.14	192.168.1.33	TCP	66	80 → 56367 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
28	8.313784327	192.168.1.33	192.168.1.14	TCP	60	56367 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
29	8.313832907	192.168.1.33	192.168.1.14	TCP	66	56368 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
30	8.313838704	192.168.1.14	192.168.1.33	TCP	66	80 → 56368 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
31	8.313925856	192.168.1.33	192.168.1.14	TCP	60	56368 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
32	8.314830204	192.168.1.33	192.168.1.14	HTTP	623	GET / HTTP/1.1
33	8.314854469	192.168.1.14	192.168.1.33	TCP	54	80 → 56368 [ACK] Seq=1 Ack=570 Win=64128 Len=0
34	8.315686919	192.168.1.14	192.168.1.33	HTTP	3434	HTTP/1.1 200 OK (text/html)
35	8.315842295	192.168.1.33	192.168.1.14	TCP	60	56368 → 80 [ACK] Seq=570 Ack=2921 Win=2102272 Len=0
36	8.356073519	192.168.1.33	192.168.1.14	TCP	60	56368 → 80 [ACK] Seq=570 Ack=3381 Win=2101760 Len=0

➡ Analysez les PDU capturés par Wireshark et répondez aux questions suivantes :

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

  C'est le protocole HTTP

- Quel est le protocole de la couche application utilisé

  C'est le protocole TCP

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

  Le port source est le port 80 et le port destination est le port 56368

- Quel est la version du serveur web utilisé.

Fichier auto capture :
https://www.wireshark.org/download/automated/captures/

Activité II) nmap : découvertes des machines et des services

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

$ man nmap

➡ Qu'est-ce que Nmap ?

Nmap est un scanner de ports libre

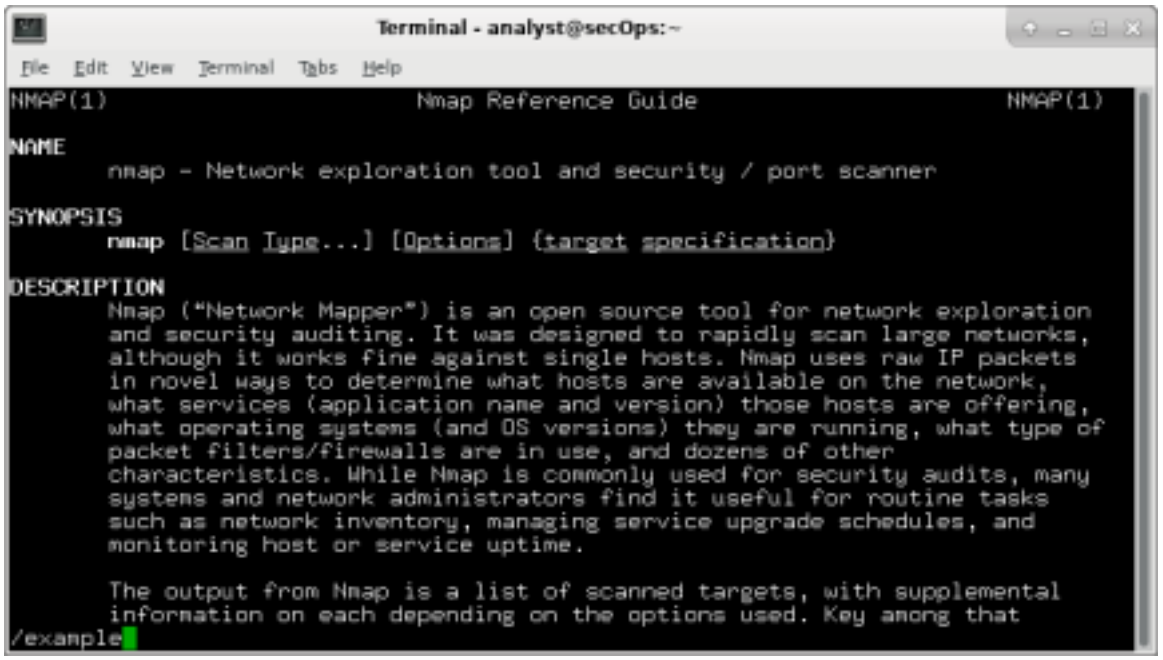
➡ À quoi Nmap sert-il ?

Il sert à savoir quel port sont ouvert

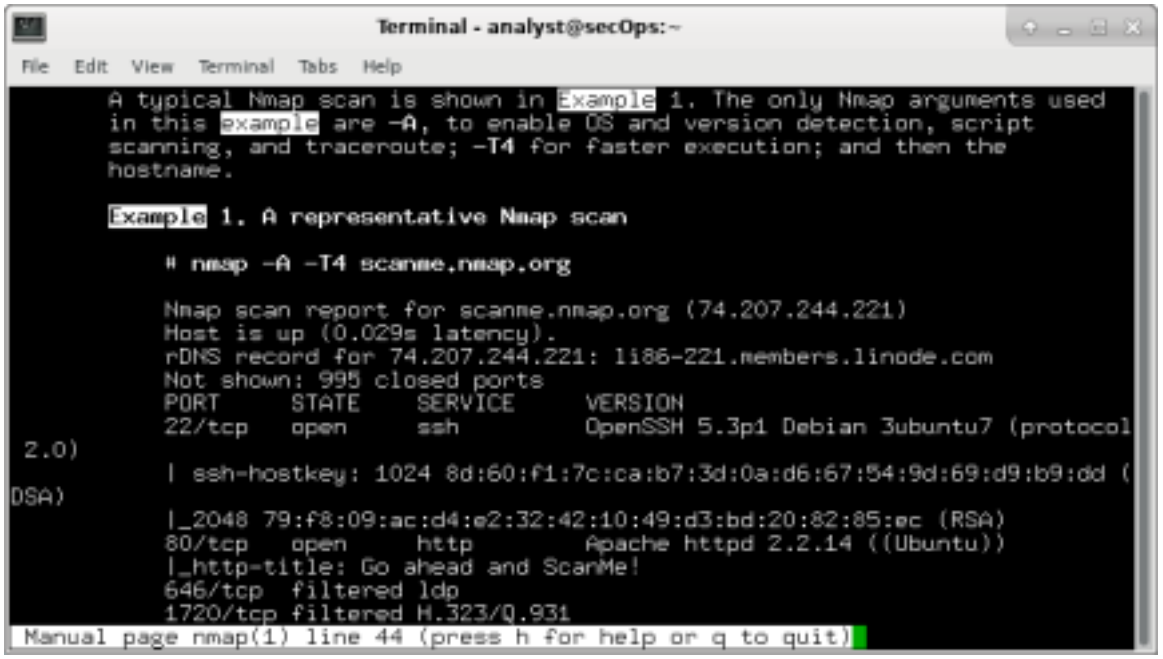
Lorsque vous êtes sur la page du manuel, vous pouvez utiliser les touches fléchées haut/bas pour faire défiler les pages. Vous pouvez également appuyer sur la barre d'espace pour avancer d'une page à la fois.

Pour rechercher un terme ou une expression spécifique, saisissez une barre oblique (/) ou un point d'interrogation (?) suivi de ce terme ou de cette expression. La barre oblique permet d'effectuer une recherche vers l'avant dans tout le document, tandis que le point d'interrogation effectue une recherche en arrière dans le document. La touche n permet d'accéder à la correspondance suivante.

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



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



Regardez l'exemple 1.

➡ Quelle est la commande nmap utilisée ?

/example

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)
nmap –sP 192.168.1.0/24

```
┌──(root💀kali)-[/home/kali]
└─# nmap -sP 192.168.1.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-31 04:39 EST
Nmap scan report for lan.home (192.168.1.1)
Host is up (0.0012s 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 (0.0016s 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 (0.0014s 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 (0.0013s latency).
MAC Address: 70:B5:E8:25:F9:5F (Dell)
Nmap scan report for b19s109-p10.home (192.168.1.33)
Host is up (0.00035s latency).
MAC Address: 70:B5:E8:25:F7:79 (Dell)
Nmap scan report for b19s109-p20.home (192.168.1.34)
Host is up (0.0015s latency).
MAC Address: 70:B5:E8:26:92:3C (Dell)
Nmap scan report for b19s109-p24.home (192.168.1.36)
Host is up (0.0014s latency).
MAC Address: 70:B5:E8:25:F7:A2 (Dell)
Nmap scan report for 192.168.1.40
Host is up (0.0022s latency).
MAC Address: 70:B5:E8:26:91:38 (Dell)
Nmap scan report for b19s109-p01.home (192.168.1.44)
Host is up (0.0021s latency).
MAC Address: 70:B5:E8:25:F7:DD (Dell)
Nmap scan report for 211-1.home (192.168.1.47)
Host is up (0.0020s latency).
MAC Address: 70:B5:E8:26:91:98 (Dell)
Nmap scan report for desktop-gvuhj4h.home (192.168.1.56)
Host is up (0.0024s latency).
MAC Address: 70:B5:E8:25:F7:99 (Dell)
Nmap scan report for b19s109-p18.home (192.168.1.106)
Host is up (0.0012s latency).
MAC Address: 70:B5:E8:26:91:96 (Dell)
Nmap scan report for pc-150.home (192.168.1.115)
Host is up (0.0099s 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 (0.18s latency).
MAC Address: BC:7F:A4:D4:05:14 (Xiaomi Communications)
Nmap scan report for d-211.home (192.168.1.250)
Host is up (0.0070s latency).
MAC Address: 00:1B:A9:21:AA:9D (Brother industries)
Nmap scan report for kali.home (192.168.1.14)
Host is up.
Nmap done: 256 IP addresses (16 hosts up) scanned in 10.44 seconds
```

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

#nmap –sS -O @VMKali

```
┌──(root💀kali)-[/home/kali]
└─# nmap -sS -O 192.168.1.14
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-31 04:41 EST
Nmap scan report for kali.home (192.168.1.14)
Host is up (0.000060s 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 2.35 seconds
```

➡ Lancer un scan en ciblant le routeur :

#nmap –sS -O 192.168.1.1

```
┌──(root💀kali)-[/home/kali]
└─# nmap -sS -O 192.168.1.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-31 04:42 EST
Nmap scan report for lan.home (192.168.1.1)
Host is up (0.0013s 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 (
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/h:dish:hopper cpe:/o:linux:linux_kernel:3 cp
Aggressive OS guesses: Linux 2.6.32 (96%), Dish Network Hopper media device (93%), Linux 2
.39) (89%), Linux 2.6.39 (89%), WatchGuard Fireware 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 9.64 seconds
```

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

On peut cibler plusieur machines grâce à l'adresse de broadcast.

II.2 Analyse des ports ouverts sur un réseau

Dans cette partie, vous allez utiliser les commutateurs issus de l'exemple des pages de manuel Nmap pour analyser votre hôte local, votre réseau local et un serveur distant.

AVERTISSEMENT : avant d'utiliser Nmap sur un réseau, demandez l'autorisation des propriétaires du réseau. En particulier le scan d'un hôte distant n'est pas autorisé sauf s'il s'agit d'un « bac à sable », d'un « pot de miel » ou tout hôte pour lequel vous en avez l'autorisation.

a. Analysez votre hôte local

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. `$ nmap -A -T4 localhost`

```
Starting Nmap 7.40 ( https://nmap.org ) at 01/05/2017 17:20 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000056s latency).
Other addresses for localhost (not scanned): ::1
rDNS record for 127.0.0.1: localhost.localdomain
Not shown: 996 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r-- 1 0 0 0 Apr 19 15:23 ftp_test
```

```
<some output omitted>
```

```
┌──(root💀kali)-[/home/kali]
└─# nmap -A -T4 localhost
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-31 05:24 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000060s latency).
Other addresses for localhost (not scanned): ::1
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
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 3.46 seconds
```

c. Vérifiez les résultats et répondez aux questions suivantes.

➡ Quels sont les ports et les services ouverts ?

Il n'y a qu'un seul port ouvert.

➡ Pour chacun des ports ouverts, notez le nom de l'application qui fournit le service.

C'est le port 80 (port http).

II.3 Analysez le réseau local

AVERTISSEMENT : avant d'utiliser Nmap sur un réseau, demandez l'autorisation des propriétaires du réseau.

d. À l'invite de commande du terminal, saisissez **ip address** pour déterminer l'adresse IP et le masque de sous-réseau de cet hôte. Dans cet exemple, l'adresse IP de cette machine virtuelle est 192.168.1.xx et le masque de sous-réseau est 255.255.255.0.

```
$ ip address
<output omitted>
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
qlen 1000
 link/ether 08:00:27:ed:af:2c brd ff:ff:ff:ff:ff:ff
 inet 192.168.1.xx/24 brd 192.168.1.255 étendue dynamique globale enp0s3
 valid_lft 85777sec preferred_lft 85777sec
 inet6 fe80::a 00:27 ff:feed:af2c/64 lien de portée
 valid_lft forever preferred_lft forever
```

Enregistrez l'adresse IP et le masque de sous-réseau de votre machine virtuelle.

➡ À quel réseau votre machine virtuelle appartient-elle ?

e. Pour localiser les autres hôtes sur ce réseau local, saisissez **nmap -A -T4** ***network address/prefix***. Le dernier octet de l'adresse IP doit être remplacé par un zéro. Par exemple, l'adresse IP 192.168.1.xx, où .15 correspond au dernier octet. Par conséquent, l'adresse réseau est 10.0.2.0. /24 est le préfixe. Il s'agit du raccourci pour le masque de sous réseau 255.255.255.0. Si le masque de réseau votre machine virtuelle est différent, recherchez votre préfixe dans le «tableau de conversion CIDR» sur Internet. Par exemple, 255.255.0.0 correspond à /16. L'adresse réseau 10.0.2.0/24 est utilisée dans cet exemple

Remarque : cette opération peut prendre un certain temps, surtout si plusieurs périphériques sont connectés au réseau. Dans l'environnement de test, l'analyse a pris environ 4 minutes.

```
$ nmap -A -T4 192.168.1.0/24
Starting Nmap 7.40 ( https://nmap.org ) at 01/05/2017 17:13 EDT
<output omitted>
Nmap scan report for 192.168.1.xx
Host is up (0.00019s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r—r— 1 0 0 0 26 mars 2018 ftp_test
| ftp-syst:
| STAT:
| FTP server status:
| Connected to 192.168.1.xx
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| At session startup, client count was 1

| vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open ssh OpenSSH 8.2 (protocol 2.0)
23/tcp open telnet Openwall GNU/*/Linux telnetd
Service Info: Host: Welcome; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Post-scan script results:
| clock-skew:
| 0s:
|_ …
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (x hosts up) scanned in 346.89 seconds
```

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

Il y a 3 ports actifs.

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

Les ports 21, 22 et 23 sont ouverts.

➡ Dans vos résultats Nmap, **nmap -A -T4** ***network address/prefix*** avec *address* et *prefix* correspondants au réseau de la machine virtuelle

Cette commande m’a permis de découvrir tous les ports ouverts du réseaux.

➡ Combien d'hôtes sont actifs ?

Il y a 25 hôtes qui sont actifs.

➡ Répertoriez les adresses IP des hôtes qui se trouvent sur le même réseau local que votre machine virtuelle.
➡ Répertoriez les services qui sont disponibles sur les ordinateurs hôtes détectés.

II.3 Analyse d'un site web de votre choix

Ping l'hôte avec la commande ping pour obtenir l'adresse IP
ping "www.nom d'hôte.com"
Entrer la commande suivante :nmap -sV adresse ip de votre cible
Il affichera tous les détails capturés de l'hôte.

Question de réflexion

Nmap est un outil puissant pour l'exploration et la gestion du réseau. Comment Nmap peut-il contribuer à la sécurité du réseau ?
➡ Comment Nmap peut-il être utilisé par un hacker comme outil néfaste ?
Portqry est un outil microsoft en ligne de commandes équivalent à nmap qui peut être utilisé sur un ordinateur windowshttps://docs.microsoft.com/fr-fr/troubleshoot/windows-server/networking/portqry-command-line-port-scanner-v2 **Zenmap** est la version « graphique » de nmap disponible pour Linux, Mac, Windows https://nmap.org/zenmap/

Code pénal

Pour rappel, l'article 323-1 du code pénal stipule que le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.
Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000030939438/

Prolongation Pentest :

- **Netdiscover:**
- Quelle est le protocole utilisé ?

```
272 Captured ARP Req/Rep packets, from 26 hosts.   Total size: 16320
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.1.61    70:b5:e8:25:fc:57     21    1260  Dell Inc.
192.168.1.33    70:b5:e8:25:f7:79     30    1800  Dell Inc.
192.168.1.42    70:b5:e8:26:91:86     23    1380  Dell Inc.
192.168.1.24    d0:bf:9c:3a:d2:cc      7     420  Hewlett Packard
192.168.1.1     d4:f8:29:80:0c:d0      4     240  Sagemcom Broadband SAS
192.168.1.18    d0:bf:9c:3a:d2:cf      1      60  Hewlett Packard
192.168.1.28    70:b5:e8:25:f9:5f      1      60  Dell Inc.
192.168.1.34    70:b5:e8:26:92:3c     15     900  Dell Inc.
192.168.1.44    70:b5:e8:25:f7:dd      2     120  Dell Inc.
192.168.1.49    70:b5:e8:26:91:68     10     600  Dell Inc.
192.168.1.54    70:b5:e8:2a:64:53     20    1200  Dell Inc.
192.168.1.55    70:b5:e8:26:18:5f      1      60  Dell Inc.
192.168.1.56    70:b5:e8:25:f7:99      7     420  Dell Inc.
192.168.1.57    70:b5:e8:2a:60:94     16     960  Dell Inc.
192.168.1.59    a8:1e:84:d8:44:a2      1      60  Quanta Computer Inc.
192.168.1.60    f4:39:09:76:08:9b      4     240  Hewlett Packard
192.168.1.62    c8:d9:d2:e0:3e:5f      1      60  Hewlett Packard
192.168.1.65    30:52:cb:26:72:91     13     780  Liteon Technology Corporation
192.168.1.103   70:b5:e8:25:fb:3e      1      60  Dell Inc.
192.168.1.106   70:b5:e8:26:91:96     20    1200  Dell Inc.
192.168.1.250   00:1b:a9:21:aa:9d      3     180  Brother industries, LTD.
192.168.1.52    70:b5:e8:26:91:2a     31    1860  Dell Inc.
192.168.1.71    70:b5:e8:26:91:97     12     720  Dell Inc.
192.168.1.43    70:b5:e8:25:f7:b2     13     780  Dell Inc.
192.168.1.105   70:b5:e8:2a:62:dc     13     780  Dell Inc.
192.168.1.12    de:b2:0f:e7:c7:01      2     120  Unknown vendor
```

Il s'agit d'une requête ARP.

- Cibler votre instruction avec l'IP de la VM Kali

```
53 Captured ARP Req/Rep packets, from 26 hosts.   Total size: 3180
_____________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________
192.168.1.61    70:b5:e8:25:fc:57      7     420  Dell Inc.
192.168.1.106   70:b5:e8:26:91:96      3     180  Dell Inc.
192.168.1.105   70:b5:e8:2a:62:dc      1      60  Dell Inc.
192.168.1.42    70:b5:e8:26:91:86      4     240  Dell Inc.
192.168.1.1     d4:f8:29:80:0c:d0      2     120  Sagemcom Broadband SAS
192.168.1.18    d0:bf:9c:3a:d2:cf      1      60  Hewlett Packard
192.168.1.16    64:6e:69:89:08:f7      5     300  Liteon Technology Corporation
192.168.1.24    d0:bf:9c:3a:d2:cc      1      60  Hewlett Packard
192.168.1.21    4c:02:20:48:45:79      4     240  Xiaomi Communications Co Ltd
192.168.1.28    70:b5:e8:25:f9:5f      1      60  Dell Inc.
192.168.1.33    70:b5:e8:25:f7:79      1      60  Dell Inc.
192.168.1.34    70:b5:e8:26:92:3c      1      60  Dell Inc.
192.168.1.44    70:b5:e8:25:f7:dd      1      60  Dell Inc.
192.168.1.49    70:b5:e8:26:91:68      1      60  Dell Inc.
192.168.1.54    70:b5:e8:2a:64:53      1      60  Dell Inc.
192.168.1.55    70:b5:e8:26:18:5f      1      60  Dell Inc.
192.168.1.56    70:b5:e8:25:f7:99      1      60  Dell Inc.
192.168.1.57    70:b5:e8:2a:60:94      1      60  Dell Inc.
192.168.1.59    a8:1e:84:d8:44:a2      4     240  Quanta Computer Inc.
192.168.1.62    c8:d9:d2:e0:3e:5f      1      60  Hewlett Packard
192.168.1.65    30:52:cb:26:72:91      1      60  Liteon Technology Corporation
192.168.1.103   70:b5:e8:25:fb:3e      1      60  Dell Inc.
192.168.1.13    3c:06:30:55:84:69      1      60  Apple, Inc.
192.168.1.250   00:1b:a9:21:aa:9d      2     120  Brother industries, LTD.
0.0.0.0         64:6e:69:89:08:f7      3     180  Liteon Technology Corporation
192.168.1.52    70:b5:e8:26:91:2a      3     180  Dell Inc.
```

- Toujours dans le terminal tapez : **p0f -i eth0 -p**

```
┌──(root💀kali)-[/home/kali]
└─# p0f -i eth0 -p
Command 'p0f' not found, but can be installed with:
apt install p0f
Do you want to install it? (N/y)y
apt install p0f
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  p0f
0 upgraded, 1 newly installed, 0 to remove and 377 not upgraded.
Need to get 81.0 kB of archives.
After this operation, 224 kB of additional disk space will be used.
Get:1 http://ftp.free.fr/pub/kali kali-rolling/main amd64 p0f amd64 3.09b-3 [81.0 kB]
Fetched 81.0 kB in 13s (6,289 B/s)
Selecting previously unselected package p0f.
(Reading database ... 267880 files and directories currently installed.)
Preparing to unpack .../archives/p0f_3.09b-3_amd64.deb ...
Unpacking p0f (3.09b-3) ...
Setting up p0f (3.09b-3) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for kali-menu (2021.4.2) ...
```

```
┌──(root💀kali)-[/home/kali]
└─# p0f -i eth0 -p
--- p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> ---

[+] Closed 1 file descriptor.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Intercepting traffic on interface 'eth0'.
[+] Default packet filtering configured [+VLAN].
[+] Entered main event loop.
```

- **Nmap:**
- Utiliser le sur le réseau local de votre Box

```
┌──(root💀kali)-[/home/kali]
└─# nmap -sP 192.168.1.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-16 08:15 EST
Nmap scan report for livebox.home (192.168.1.1)
Host is up (0.00078s latency).
MAC Address: D4:F8:29:80:0C:D0 (Sagemcom Broadband SAS)
Nmap scan report for pc-58.home (192.168.1.12)
Host is up (0.016s latency).
MAC Address: DE:B2:0F:E7:C7:01 (Unknown)
Nmap scan report for macbook-pro-de-maeva.home (192.168.1.13)
Host is up (0.23s latency).
MAC Address: 3C:06:30:55:84:69 (Apple)
Nmap scan report for desktop-5gb19rq.home (192.168.1.16)
Host is up (2.3s latency).
MAC Address: 64:6E:69:89:08:F7 (Liteon Technology)
Nmap scan report for ilocz162500hl.home (192.168.1.18)
Host is up (0.0016s 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 (0.0012s 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 (0.00071s latency).
MAC Address: 70:B5:E8:25:F9:5F (Dell)
Nmap scan report for b19s109-p10.home (192.168.1.33)
Host is up (0.00030s latency).
MAC Address: 70:B5:E8:25:F7:79 (Dell)
Nmap scan report for b19s109-p20.home (192.168.1.34)
Host is up (0.00059s latency).
MAC Address: 70:B5:E8:26:92:3C (Dell)
Nmap scan report for d211-22.home (192.168.1.42)
Host is up (0.00050s latency).
MAC Address: 70:B5:E8:26:91:86 (Dell)
Nmap scan report for b19s109-p01.home (192.168.1.44)
Host is up (0.0026s latency).
MAC Address: 70:B5:E8:25:F7:DD (Dell)
Nmap scan report for desktop-hl4l57o.home (192.168.1.49)
Host is up (0.00058s latency).
MAC Address: 70:B5:E8:26:91:68 (Dell)
Nmap scan report for pc-59.home (192.168.1.53)
Host is up (0.0080s latency).
MAC Address: 5A:ED:87:25:45:F0 (Unknown)
Nmap scan report for pc-211-108-hugo.home (192.168.1.54)
Host is up (0.00053s latency).
MAC Address: 70:B5:E8:2A:64:53 (Dell)
Nmap scan report for b19s211p05.home (192.168.1.55)
Host is up (0.00052s latency).
MAC Address: 70:B5:E8:26:18:5F (Dell)
Nmap scan report for desktop-gvuhj4h.home (192.168.1.56)
Host is up (0.00051s latency).
MAC Address: 70:B5:E8:25:F7:99 (Dell)
Nmap scan report for b19s211p07.home (192.168.1.57)
Host is up (0.00050s latency).
MAC Address: 70:B5:E8:2A:60:94 (Dell)
Nmap scan report for desktop-5gb19rq-1.home (192.168.1.59)
Host is up (0.00066s latency).
MAC Address: A8:1E:84:D8:44:A2 (Quanta Computer)
Nmap scan report for itsweeazie.home (192.168.1.60)
Host is up (0.00046s latency).
MAC Address: F4:39:09:76:08:9B (Hewlett Packard)
```

```
42301 853.007361025 192.168.1.35 192.168.1.34 TCP 54 9100 → 65301 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42320 853.049220771 192.168.1.34 192.168.1.35 TCP 66 [TCP Retransmission] 65405 → 15002 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
42321 853.049260854 192.168.1.35 192.168.1.34 TCP 54 15002 → 65405 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42322 853.155790226 192.168.1.34 192.168.1.35 TCP 66 [TCP Retransmission] 65430 → 15002 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
42323 853.155823058 192.168.1.35 192.168.1.34 TCP 54 15002 → 65430 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42327 853.297123739 192.168.1.34 192.168.1.35 TCP 66 [TCP Retransmission] 65458 → 10617 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
42328 853.297184616 192.168.1.35 192.168.1.34 TCP 54 10617 → 65458 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42329 853.398513215 192.168.1.34 192.168.1.35 TCP 66 [TCP Retransmission] 65478 → 10617 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
42330 853.398550613 192.168.1.35 192.168.1.34 TCP 54 10617 → 65478 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42331 853.416317628 192.168.1.34 192.168.1.35 TCP 66 [TCP Retransmission] 65286 → 9100 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
42332 853.416357916 192.168.1.35 192.168.1.34 TCP 54 9100 → 65286 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42333 853.507952093 192.168.1.34 192.168.1.35 TCP 66 [TCP Retransmission] 65301 → 9100 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
42334 853.507973689 192.168.1.35 192.168.1.34 TCP 54 9100 → 65301 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42375 853.657241689 192.168.1.34 192.168.1.35 TCP 66 [TCP Retransmission] 65430 → 15002 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
42376 853.657281471 192.168.1.35 192.168.1.34 TCP 54 15002 → 65430 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42377 853.797539832 192.168.1.34 192.168.1.35 TCP 66 [TCP Retransmission] 65458 → 10617 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
42378 853.797555103 192.168.1.35 192.168.1.34 TCP 54 10617 → 65458 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42380 853.900255834 192.168.1.34 192.168.1.35 TCP 66 [TCP Retransmission] 65478 → 10617 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
42381 853.900276495 192.168.1.35 192.168.1.34 TCP 54 10617 → 65478 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42399 854.050715775 192.168.1.34 192.168.1.35 TCP 66 [TCP Retransmission] 65405 → 15002 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
42400 854.050754375 192.168.1.35 192.168.1.34 TCP 54 15002 → 65405 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42401 854.158894952 192.168.1.34 192.168.1.35 TCP 66 [TCP Retransmission] 65430 → 15002 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
42402 854.158915777 192.168.1.35 192.168.1.34 TCP 54 15002 → 65430 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42403 854.172767910 192.168.1.34 192.168.1.35 TCP 66 49398 → 666 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
42405 854.172800467 192.168.1.35 192.168.1.34 TCP 54 666 → 49398 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42407 854.229087668 192.168.1.34 192.168.1.35 TCP 66 49412 → 666 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
42408 854.229104338 192.168.1.35 192.168.1.34 TCP 54 666 → 49412 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42411 854.297439255 192.168.1.34 192.168.1.35 TCP 66 [TCP Retransmission] 65458 → 10617 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
42412 854.297458568 192.168.1.35 192.168.1.34 TCP 54 10617 → 65458 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42413 854.400974486 192.168.1.34 192.168.1.35 TCP 66 [TCP Retransmission] 65478 → 10617 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
42414 854.401013039 192.168.1.35 192.168.1.34 TCP 54 10617 → 65478 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42438 854.674265130 192.168.1.34 192.168.1.35 TCP 66 [TCP Retransmission] 49398 → 666 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
42439 854.674304863 192.168.1.35 192.168.1.34 TCP 54 666 → 49398 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42440 854.730079150 192.168.1.34 192.168.1.35 TCP 66 [TCP Retransmission] 49412 → 666 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
42441 854.730118198 192.168.1.35 192.168.1.34 TCP 54 666 → 49412 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42463 855.175233945 192.168.1.34 192.168.1.35 TCP 66 [TCP Retransmission] 49398 → 666 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
42464 855.175270525 192.168.1.35 192.168.1.34 TCP 54 666 → 49398 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42466 855.231762045 192.168.1.34 192.168.1.35 TCP 66 [TCP Retransmission] 49412 → 666 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
42467 855.231801386 192.168.1.35 192.168.1.34 TCP 54 666 → 49412 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42576 856.779042162 192.168.1.34 192.168.1.35 TCP 66 49601 → 800 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
42577 856.779094342 192.168.1.35 192.168.1.34 TCP 54 800 → 49601 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42580 856.929446393 192.168.1.34 192.168.1.35 TCP 66 49575 → 800 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
42581 856.929463084 192.168.1.35 192.168.1.34 TCP 54 800 → 49575 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42582 856.965784797 192.168.1.34 192.168.1.35 TCP 66 49577 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
42583 856.965821630 192.168.1.35 192.168.1.34 TCP 54 993 → 49577 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

- **SMBMap :**
- Utiliser le sur la cible : **smbmap -H <IP>** en mode anonyme

```
┌──(root㉿kali)-[/home/kali]
└─# smbmap -h 192.168.1.0

usage: smbmap [-h] (-H HOST | --host-file FILE) [-u USERNAME] [-p PASSWORD] [-s SHARE] [-d DOMAIN] [-P PORT] [-v] [--admin] [-x COMMAND] [--mode CMDMODE] [-L | -R [PATH]
              [-q] [--depth DEPTH] [--exclude SHARE [SHARE ...]] [-F PATTERN] [--search-path PATH] [--search-timeout TIMEOUT] [--download PATH] [--upload SRC DST] [--del

SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com

optional arguments:
  -h, --help            show this help message and exit

Main arguments:
  -H HOST               IP of host
  --host-file FILE      File containing a list of hosts
  -u USERNAME           Username, if omitted null session assumed
  -p PASSWORD           Password or NTLM hash
  -s SHARE              Specify a share (default C$), ex 'C$'
  -d DOMAIN             Domain name (default WORKGROUP)
  -P PORT               SMB port (default 445)
  -v                    Return the OS version of the remote host
  --admin               Just report if the user is an admin

Command Execution:
  Options for executing commands on the specified host

  -x COMMAND            Execute a command ex. 'ipconfig /all'
  --mode CMDMODE        Set the execution method, wmi or psexec, default wmi

Shard drive Search:
  Options for searching/enumerating the share of the specified host(s)

  -L                    List all drives on the specified host
  -R [PATH]             Recursively list dirs, and files (no share\path lists ALL shares), ex. 'C$\Finance'
  -r [PATH]             List contents of directory, default is to list root of all shares, ex. -r 'C$\Documents and Settings\Administrator\Documents'
  -A PATTERN            Define a file name pattern (regex) that auto downloads a file on a match (requires -R or -r), not case sensitive, ex '(web|global).(asax|config)'
  -g                    Make the output grep friendly, used with -r or -R (otherwise it outputs nothing)
  --dir-only            List only directories, ommit files.
  --no-write-check      Skip check to see if drive grants WRITE access.
  -q                    Quiet verbose output. Only shows shares you have READ or WRITE on, and suppresses file listing when performing a search (-A).
  --depth DEPTH         Traverse a directory tree to a specific depth. Default is 5.
  --exclude SHARE [SHARE ...]
                        Exclude share(s) from searching and listing, ex. --exclude ADMIN$ C$'

File Content Search:
  Options for searching the content of files (must run as root)

  -F PATTERN            File content search, -F '[Pp]assword' (requires admin access to execute commands, and PowerShell on victim host)
  --search-path PATH    Specify drive/path to search (used with -F, default C:\Users), ex 'D:\HR\'
  --search-timeout TIMEOUT
                        Specifcy a timeout (in seconds) before the file search job gets killed. Default is 300 seconds.

Filesystem interaction:
  Options for interacting with the specified host's filesystem

  --download PATH       Download a file from the remote system, ex.'C$\temp\passwords.txt'
  --upload SRC DST      Upload a file to the remote system ex. '/tmp/payload.exe C$\temp\payload.exe'
  --delete PATH TO FILE
                        Delete a remote file, ex. 'C$\temp\msf.exe'
  --skip                Skip delete file confirmation prompt
```

- Utiliser le sur la cible : **smbmap -H <IP> -u <user> -p <password>** en mode authentifié