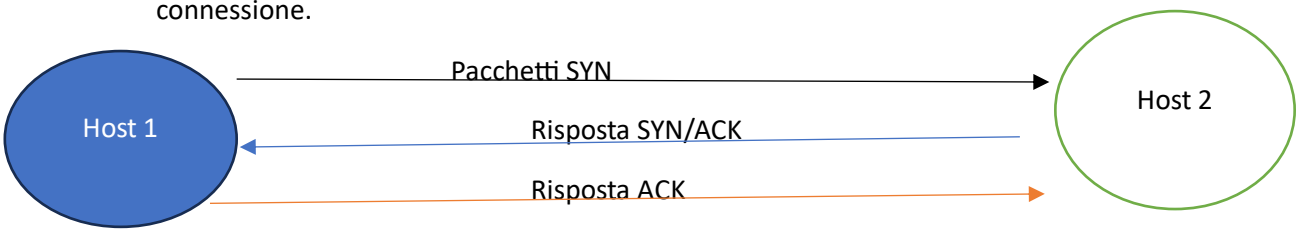
```
# nmap --system-dns -F  192.168.1.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-18 02:55 EDT
Nmap scan report for 192.168.1.103
Host is up (0.00032s latency).
Not shown: 82 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
513/tcp  open  login
514/tcp  open  shell
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
8009/tcp open  ajp13
MAC Address: 08:00:27:5C:EF:24 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

Nella scansione con nmap -F viene eseguita una scansione veloce delle porte più comuni, limitando il numero di porte scansionate. In questo tipo di scansione abbiamo il completamento del 3-way-handshake.

- Nmap invia dei pacchetti SYN alle porte desiderate per verificare se sono aperte
- Se la porta è aperta il server invia una risposta SYN/ACK per indicare che è pronto a stabilire una connessione; le porte chiuse possono inviare un altro tipo di risposta o non rispondere affatto
- Dopo aver ricevuto le risposte nmap invia pacchetti di completamento dell'ACK per completare la connessione.




```
Nmap scan report for 192.168.1.103
Host is up (0.00089s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:5C:EF:24 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

Nella scansione **nmap -O** viene individuato il SO dell'host target.

Nmap invia una serie di pacchetti, tra cui pacchetti TCP SYN a un insieme di porte comuni e ICMP Echo Request (ping) al target.ù

Nmap analizza le risposte ricevute dai pacchetti TCP SYN inviati alle porte target; se una porta risponde con un pacchetto SYN/ACK, è probabile che la porta sia aperta e il servizio sia in ascolto; inoltre analizza le risposte ricevute per determinare caratteristiche specifiche dei pacchetti di risposta.

Basandosi sulle caratteristiche dei pacchetti di risposta nmap cerca di identificare il sistema operativo dell'host.

Nel nostro caso nmap ci dice che è un sistema linux 2.6

```
└─# nmap --system-dns -PN  192.168.1.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-18 03:00 EDT
Nmap scan report for 192.168.1.103
Host is up (0.00030s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:5C:EF:24 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds
```

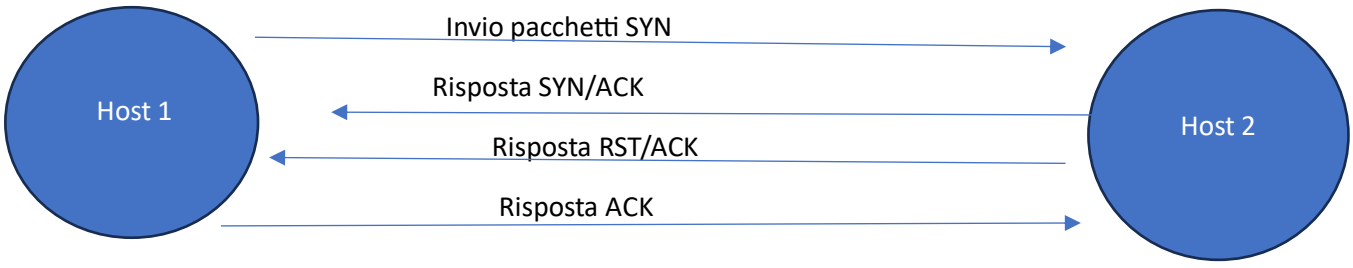
Nmap -PN effettua una scansione senza inviare pacchetti di ping per verificare la disponibilità dell'host, questo è utile quando si vuole bypassare i dispositivi di sicurezza che bloccano il traffico ping.

Invio dei pacchetti SYN sulle porte senza verificare che l'host è attivo tramite ping.

Risposta SYN/ACK: se una porta è aperta e in ascolto, l'host destinatario risponde con un pacchetto SYN/ACK. Nmap rileva queste risposte e identifica le porte aperte.

Risposte RST/ACK: se una porta è chiusa, l'host destinatario risponde con un pacchetto RST/ACK. Nmap identifica queste risposte e le registra come porte chiuse

Risposta ACK l'host mittente risponderà con un pacchetto ACK al server per confermare il completamento del 3-way handshake.



```
└─# nmap --system-dns -PR  192.168.1.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-18 02:56 EDT
Nmap scan report for 192.168.1.103
Host is up (0.00077s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:5C:EF:24 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

La scansione Nmap con l'opzione **-PR** ha lo scopo di determinare quali host sono attivi in una rete specifica. Questa scansione si basa su pacchetti ICMP e ARP per determinare la presenza degli host. Se il 3-way handshake viene completato, non verranno effettuate fasi SYN/ACK o connessioni.

Quindi abbiamo l’invio dei pacchetti di Ping o richieste ARP

Gli Host risponderanno

Nmap analizza le risposte per determinare gli host attivi

```
└─# nmap --system-dns -sP  192.168.1.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-18 02:57 EDT
Nmap scan report for 192.168.1.103
Host is up (0.00065s latency).
MAC Address: 08:00:27:5C:EF:24 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

La scansione **-SP** di Nmap è una scansione di tipo "Ping Scan" che serve a verificare la disponibilità degli host nella rete senza eseguire una scansione di porte. Questa scansione invia pacchetti di ping agli host target e, se il 3-way handshake viene completato, significa che l'host è attivo e risponde.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --system-dns -sS -p 8080 192.168.1.103/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-17 03:48 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0030s latency).

PORT     STATE    SERVICE
8080/tcp filtered http-proxy
MAC Address: 08:00:27:F3:4E:2E (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.103
Host is up (0.00081s latency).

PORT     STATE  SERVICE
8080/tcp closed http-proxy
MAC Address: 08:00:27:5C:EF:24 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.101
Host is up (0.000036s latency).

PORT     STATE  SERVICE
8080/tcp closed http-proxy

Nmap done: 256 IP addresses (3 hosts up) scanned in 2.46 seconds
```

il flusso di una scansione Nmap con l'opzione **-sS** prevede l'invio di un pacchetto SYN, la ricezione di un pacchetto SYN/ACK e l'invio di un pacchetto ACK per completare la connessione. Questo processo con l'aggiunta dell'opzione -p 80808 è una tecnica comune utilizzata da Nmap per rilevare lo stato della porta 8080 sull' host indicato.

```
└─# nmap --system-dns -sS -p-  192.168.1.103/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-17 03:51 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0011s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
MAC Address: 08:00:27:F3:4E:2E (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.103
Host is up (0.00056s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
50740/tcp open  unknown
51162/tcp open  unknown
58796/tcp open  unknown
59178/tcp open  unknown
MAC Address: 08:00:27:5C:EF:24 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.101
Host is up (0.0000020s latency).
```

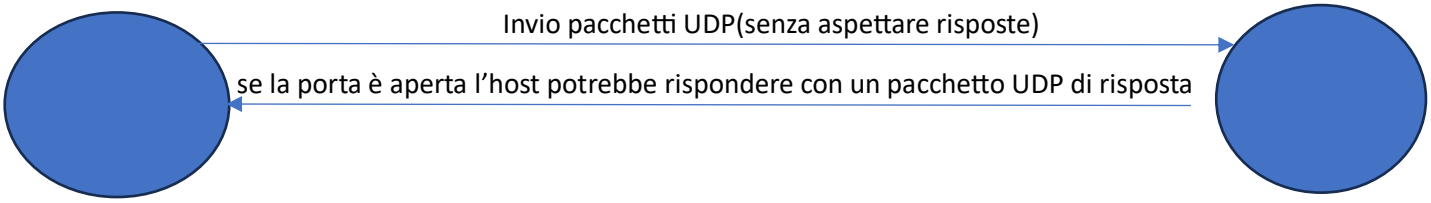
Con l'opzione -p- si esegue una scansione TCP/SYN su tutte le porte.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --system-dns -sS 192.168.1.103/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-17 03:47 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0024s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
MAC Address: 08:00:27:F3:4E:2E (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.103
Host is up (0.00080s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:5C:EF:24 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.101
Host is up (0.0000020s latency).
All 1000 scanned ports on 192.168.1.101 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (3 hosts up) scanned in 6.80 seconds
```

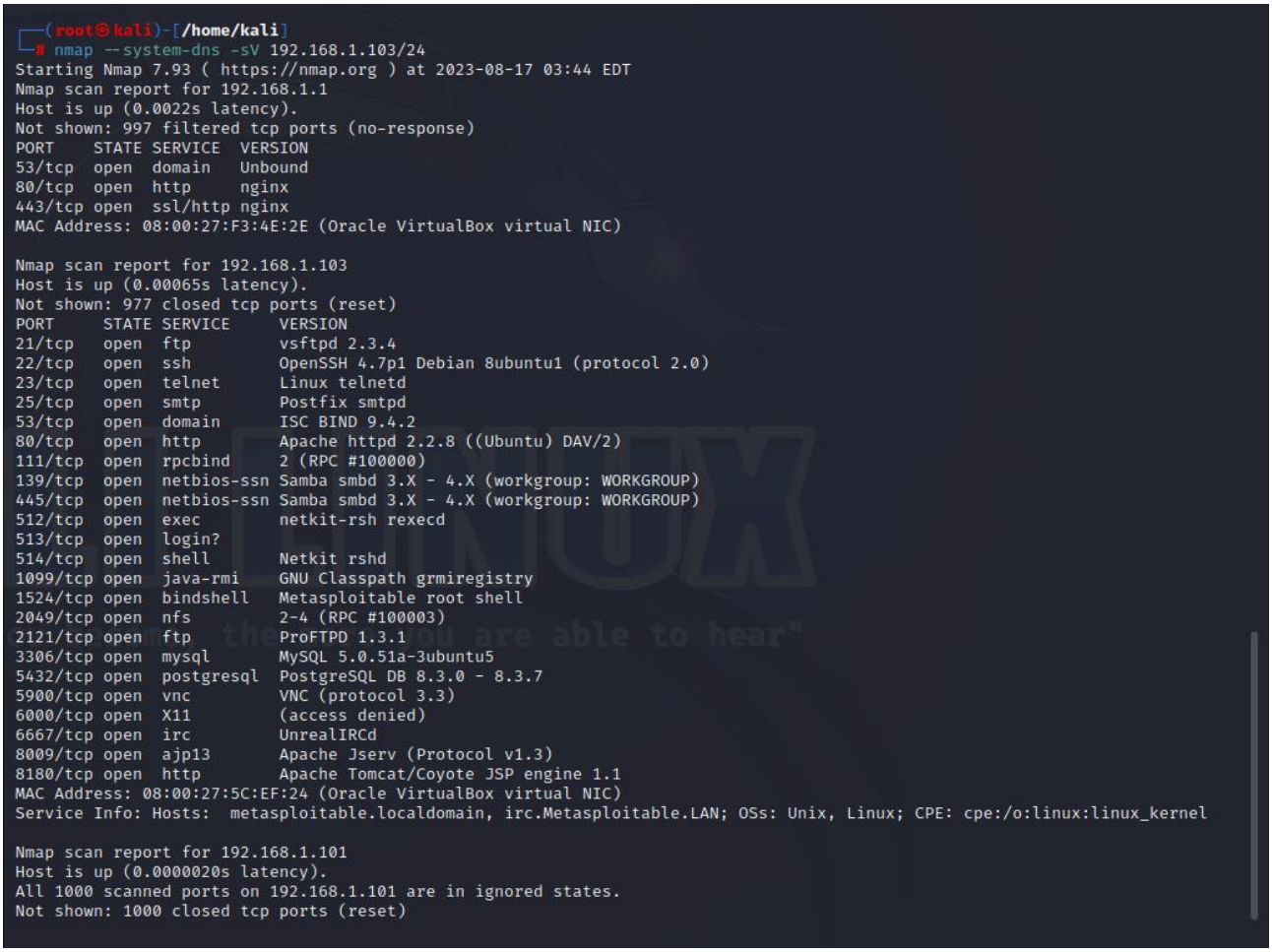
```
Discovered open port 137/udp on 192.168.1.103
Increasing send delay for 192.168.1.103 from 200 to 400 due to 11 out of 18 dropped probes since last increase.
UDP Scan Timing: About 52.61% done; ETC: 03:59 (0:00:31 remaining)
Increasing send delay for 192.168.1.103 from 400 to 800 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 54.01% done; ETC: 04:00 (0:00:54 remaining)
UDP Scan Timing: About 55.46% done; ETC: 04:00 (0:01:16 remaining)
UDP Scan Timing: About 56.85% done; ETC: 04:01 (0:01:34 remaining)
UDP Scan Timing: About 58.25% done; ETC: 04:02 (0:01:50 remaining)
UDP Scan Timing: About 60.13% done; ETC: 04:03 (0:02:06 remaining)
Discovered open port 2049/udp on 192.168.1.103
UDP Scan Timing: About 62.32% done; ETC: 04:04 (0:02:22 remaining)
UDP Scan Timing: About 66.04% done; ETC: 04:06 (0:02:41 remaining)
UDP Scan Timing: About 73.71% done; ETC: 04:08 (0:02:49 remaining)
UDP Scan Timing: About 81.72% done; ETC: 04:11 (0:02:25 remaining)
UDP Scan Timing: About 88.33% done; ETC: 04:13 (0:01:44 remaining)
UDP Scan Timing: About 93.27% done; ETC: 04:14 (0:01:05 remaining)
UDP Scan Timing: About 96.45% done; ETC: 04:14 (0:00:35 remaining)
Completed UDP Scan at 04:16, 1075.12s elapsed (2000 total ports)
Nmap scan report for 192.168.1.1
Host is up (0.0017s latency).
Not shown: 998 open|filtered udp ports (no-response)
PORT    STATE SERVICE
53/udp  open  domain
123/udp open  ntp
MAC Address: 08:00:27:F3:4E:2E (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.103
Host is up (0.00076s latency).
Not shown: 994 closed udp ports (port-unreach)
PORT     STATE         SERVICE
53/udp   open          domain
69/udp   open|filtered tftp
111/udp  open          rpcbind
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
2049/udp open          nfs
MAC Address: 08:00:27:5C:EF:24 (Oracle VirtualBox virtual NIC)

Initiating UDP Scan at 04:16
Scanning 192.168.1.101 [1000 ports]
Completed UDP Scan at 04:16, 0.05s elapsed (1000 total ports)
Nmap scan report for 192.168.1.101
Host is up (0.0000050s latency).
All 1000 scanned ports on 192.168.1.101 are in ignored states.
Not shown: 1000 closed udp ports (port-unreach)

Read data files from: /usr/bin/../share/nmap
Nmap done: 256 IP addresses (3 hosts up) scanned in 1077.20 seconds
           Raw packets sent: 5114 (225.215KB) | Rcvd: 3264 (208.273KB)
```

La scansione **nmap -sU -r -v** utilizza le opzioni per eseguire una scansione UDP (**-sU**) in modo ricorsivo (**-r**) e con output verboso (**-v**).

Poiché la scansione UDP non coinvolge il tradizionale 3-way handshake come le scansioni TCP, il flusso sarà diverso.



poiché è stata usata l'opzione -r e -v nmap potrebbe eseguire ulteriori passaggi ricorsivi, inoltre mostrerà dettagli aggiuntivi durante il processo di scansione e sulle porte aperte



La scansione Nmap con l'opzione **-sV** (scansione di versione) viene utilizzata per determinare le versioni dei servizi in ascolto sulle porte aperte di un host.

- La fase 1 (SYN) coinvolge l'invio di un pacchetto SYN da parte di Nmap.
- Nella fase 2 (SYN/ACK), l'host di destinazione risponde con un pacchetto SYN/ACK per indicare che la porta è aperta.
- Nella fase 3 (ACK), Nmap invia un pacchetto ACK per completare il 3-way handshake e stabilire una connessione temporanea.

Questo processo consente a Nmap di determinare se una porta è aperta o chiusa e, nell'opzione **-sV**, consente anche di raccogliere informazioni sulla versione del servizio in ascolto su quella porta.