

Scansione tcp sulle porte well known:

```
77 14.208795250 192.168.32.100 192.168.32.101 TCP 74 52278 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=119...
78 14.209032199 192.168.32.101 192.168.32.100 TCP 74 445 → 52278 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM...
79 14.209045375 192.168.32.100 192.168.32.101 TCP 66 52278 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=119330427 TSecr=...

(kali㉿kali)-[~]
└─$ nmap -sT 192.168.32.101 444
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 11:39 EST
Nmap scan report for 192.168.32.101
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      tcp    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
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.15 seconds
Nmap done: 2 IP addresses (1 host up) scanned in 14.57 seconds
```

Come possiamo vedere, utilizzando il comando `nmap -sT` si scansionano le porte aperte sul server metasploitable con ip indicato, e si scansiona in maniera piu invasiva, terminando il 3 handshake, dove all'inizio (fra la porta 445 e 52278) precisamente kali linux (in questo caso sorgente:192.168.32.100) mandera `seq=0` a metasploitable(in questo caso destinatario 192.168.32.101), esso rispondera con `seq=0` e `ack=1` ed a sua volta linux aggiungera valore 1 e rispondera `seq=1` e `ack=1` terminando il 3 handshake.

Sacansione SYN:

```
File Actions Edit View Help
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 11:45 EST
Nmap scan report for 192.168.32.101
Host is up (0.00029s 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: 08:00:27:0E:BC:5E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.46 seconds
```

56	25.865812829	192.168.32.101	192.168.32.100	TCP	60 53 → 35644 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
57	25.865833731	192.168.32.100	192.168.32.101	TCP	54 35644 → 53 [RST] Seq=1 Win=0 Len=0

IN Questo caso con il comando nmap -sS abbiamo avviato una scansione meno invasiva evitando di terminare il 3 hand shake: difatti come si puo vedere, le due macchine si rimandano il valore un'unica volta senza terminarlo.

Scansione con switch-a:

23/tcp open telnet

(kali㉿kali)-[~]

\$ nmap st 192.168.32.101 -p1-1024

Starting Nmap 7.93 (<https://nmap.org>) at 2023-02-09 11:11 EST

Failed to resolve "st".

Nmap scan report for 192.168.32.101

Host is up (0.0014s latency).

Not shown: 1012 closed tcp ports (conn-refused)

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

Nmap done: 1 IP address (1 host up) scanned in 19.59 seconds