

Scan su Metasploitable:

OS FINGERPRINT: (-O)

(ip source: 192.168.1.28)

(ip destination: 192.168.1.26)

OS details: Linux 2.6.9 - 2.6.33

```
(kali㉿10)-[~]
$ sudo nmap -O 192.168.1.26
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 08:48 EDT
Nmap scan report for Host-002.homenet.telecomitalia.it (192.168.1.26)
Host is up (0.00051s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
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:C8:15:2E (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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.84 seconds

(kali㉿10)-[~]
$
```

SYN SCAN: (-sS)

(ip source: 192.168.1.28)

(ip destination: 192.168.1.26)

```
(kali@10)-[~]
$ sudo nmap -sS 192.168.1.26
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 09:02 EDT
Nmap scan report for Host-002.homenet.telecomitalia.it (192.168.1.26)
Host is up (0.00063s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
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:C8:15:2E (Oracle VirtualBox virtual NIC)

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

TCP CONNECT: (-sT)

(ip source: 192.168.1.28)

(ip destination: 192.168.1.26)

```
(kali@10)-[~]
$ nmap -sT 192.168.1.26
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 09:14 EDT
Nmap scan report for Host-002.homenet.telecomitalia.it (192.168.1.26)
Host is up (0.0037s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
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: 1 IP address (1 host up) scanned in 0.12 seconds
```

La differenza tra Syn Scan e TCP Connect risiede nel fatto che Syn Scan non completa il 3-way-handshake, ovvero la comunicazione SYN-SYN/ACK-ACK, ma chiude con RST la comunicazione creando meno disturbo in rete.

TCP Connect (nmap -sT)

192.168.1.28	192.168.1.30	TCP	74 49088 → 9 [SYN] Seq=0 Win=32120 Len=0 M
192.168.1.30	192.168.1.28	TCP	74 5357 → 35264 [SYN, ACK] Seq=0 Ack=1 Win
192.168.1.28	192.168.1.30	TCP	66 35264 → 5357 [ACK] Seq=1 Ack=1 Win=3212
192.168.1.28	192.168.1.30	TCP	66 35264 → 5357 [RST, ACK] Seq=1 Ack=1 Win
192.168.1.28	192.168.1.30	TCP	74 51478 → 10628 [SYN] Seq=0 Win=32120 Len

Syn Scan (nmap -sS)

192.168.1.28	192.168.1.30	TCP	58 33306 → 139 [SYN] Seq=0 Wi
192.168.1.28	192.168.1.30	TCP	58 33295 → 9999 [SYN] Seq=0 W
192.168.1.30	192.168.1.28	TCP	60 139 → 33306 [SYN, ACK] Seq
192.168.1.28	192.168.1.30	TCP	54 33306 → 139 [RST] Seq=1 Wi
192.168.1.28	192.168.1.30	TCP	58 33295 → 9999 [SYN] Seq=0 W

VERSION DETECTION: (-sV)

(ip source: 192.168.1.28)

(ip destination: 192.168.1.26)

```
(kali@10)~[~]
$ sudo nmap -sV -p 0-1024 192.168.1.26
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 09:26 EDT
Nmap scan report for Host-002.homenet.telecomitalia.it (192.168.1.26)
Host is up (0.00040s latency).
Not shown: 1014 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login?
514/tcp   open  tcpwrapped
MAC Address: 08:00:27:C8:15:2E (Oracle VirtualBox virtual NIC)
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.09 seconds
```

Scan su Windows 7:

OS Fingerprint

(ip source: 192.168.1.28)

(ip destination: 192.168.1.30)

OS details: Microsoft Windows Embedded Standard 7

```
(kali@10)-[~]  
$ sudo nmap -O 192.168.1.30  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 10:00 EDT  
Nmap scan report for okay-PC.homenet.telecomitalia.it (192.168.1.30)  
Host is up (0.00047s latency).  
Not shown: 993 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
135/tcp    open  msrpc  
139/tcp    open  netbios-ssn  
445/tcp    open  microsoft-ds  
554/tcp    open  rtsp  
2869/tcp   open  iclslap  
5357/tcp   open  wsdapi  
10243/tcp  open  unknown  
MAC Address: 08:00:27:27:DA:4B (Oracle VirtualBox virtual NIC)  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: specializedIpPhone  
Running: Microsoft Windows 7|Phone  
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows  
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0  
Network Distance: 1 hop
```

REPORT:

IP(source and destination)

(ip source: 192.168.1.28) on Kali Linux

(ip destination: 192.168.1.26) on Metasploitable

(ip destination: 192.168.1.30) on Windows 7

OS:

(ip destination: 192.168.1.26) on Metasploitable

OS details: Linux 2.6.9 - 2.6.33

(ip destination: 192.168.1.30) on Windows 7

OS details: Microsoft Windows Embedded Standard 7

PORTE APERTE:

(ip source: 192.168.1.28)

(ip destination: 192.168.1.26) on Metasploitable

```
└─$ sudo nmap -sT -T5 -p 0-65000 192.168.1.26
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 09:38 EDT
Nmap scan report for Host-002.homenet.telecomitalia.it (192.168.1.26)
Host is up (0.00069s latency).
Not shown: 64972 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
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
38497/tcp open  unknown
46560/tcp open  unknown
46855/tcp open  unknown
49033/tcp open  unknown
MAC Address: 08:00:27:C8:15:2E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.55 seconds
```

