

## Traccia:

Tecniche di scansione con Nmap Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

- OS fingerprint.
- Syn Scan.
- TCP connect - trovate differenze tra i risultati delle scansioni TCP connect e SYN?
- Version detection.

E la seguente sul target Windows:

- OS fingerprint.

---

## Report Finale

Per prima cosa, controlliamo i diversi IP e facciamo dei ping di prova per verificare che le due macchine Kali e Metasploitable comunichino tra loro.

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:25:ac:14 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.187/24 brd 192.168.1.255 scope global eth0
    inet6 fd8d:db7a:9800:9046:a00:27ff:fe25:ac14/64 scope global dynamic
        valid_lft 1718sec preferred_lft 1718sec
    inet6 fe80::a00:27ff:fe25:ac14/64 scope link
        valid_lft forever preferred_lft forever
```

Con il comando `<ip a>` controlliamo l'ip della Metasploitable che in questo caso è "192.168.1.187/24"

A questo punto "pinghiamo" su Kali la nostra Metasploitable – e come possiamo vedere c'è risposta al ping.

```
(kali@kali) ~$ ping 192.168.1.187
PING 192.168.1.187 (192.168.1.187) 56(84) bytes of data:
64 bytes from 192.168.1.187: icmp_seq=1 ttl=64 time=2.00 ms
64 bytes from 192.168.1.187: icmp_seq=2 ttl=64 time=0.588 ms
64 bytes from 192.168.1.187: icmp_seq=3 ttl=64 time=0.323 ms
64 bytes from 192.168.1.187: icmp_seq=4 ttl=64 time=0.748 ms
64 bytes from 192.168.1.187: icmp_seq=5 ttl=64 time=1.04 ms
64 bytes from 192.168.1.187: icmp_seq=6 ttl=64 time=0.178 ms
64 bytes from 192.168.1.187: icmp_seq=7 ttl=64 time=0.331 ms
64 bytes from 192.168.1.187: icmp_seq=8 ttl=64 time=1.45 ms
64 bytes from 192.168.1.187: icmp_seq=9 ttl=64 time=0.235 ms
64 bytes from 192.168.1.187: icmp_seq=10 ttl=64 time=1.30 ms
64 bytes from 192.168.1.187: icmp_seq=11 ttl=64 time=0.385 ms
64 bytes from 192.168.1.187: icmp_seq=12 ttl=64 time=0.301 ms
64 bytes from 192.168.1.187: icmp_seq=13 ttl=64 time=0.169 ms
64 bytes from 192.168.1.187: icmp_seq=14 ttl=64 time=0.729 ms
64 bytes from 192.168.1.187: icmp_seq=15 ttl=64 time=0.345 ms
64 bytes from 192.168.1.187: icmp_seq=16 ttl=64 time=0.344 ms
64 bytes from 192.168.1.187: icmp_seq=17 ttl=64 time=0.369 ms
64 bytes from 192.168.1.187: icmp_seq=18 ttl=64 time=0.472 ms
64 bytes from 192.168.1.187: icmp_seq=19 ttl=64 time=0.475 ms
64 bytes from 192.168.1.187: icmp_seq=20 ttl=64 time=0.457 ms
64 bytes from 192.168.1.187: icmp_seq=21 ttl=64 time=1.05 ms
```

Una volta confermata la comunicazione tra le due macchine partiamo con i comandi richiesti nell'esercizio.

## Comando: OS fingerprint (Identificazione del sistema operativo)

```
sudo nmap -O 192.168.1.187
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 09:30 EDT
Nmap scan report for 192.168.1.187
Host is up (0.00060s 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
8000/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:25:AC:14 (PCS Systemtechnik/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 12.50 seconds
```

nmap -O 192.168.1.187

-O: cerca di indovinare il sistema operativo usando tecniche di fingerprinting.

• In questo caso, come da screen, abbiamo scoperto le diverse porte aperte e il sistema operativo evidenziato in rosso:

OS CPE: cpe:/o:linux:linux\_kernel:2.6

OS details: linux 2.6.9 – 2.6.33

- **Perché si usa:** Identifica il sistema operativo in esecuzione su un host remoto (es. Windows, Linux, etc.).
- **Come funziona:** Analizza il comportamento della macchina in risposta a pacchetti TCP/IP particolari.

## Comando: Syn Scan (scansione più veloce e discreta)

```
(kali@kali)~$ nmap -sS 192.168.1.187
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 10:00 EDT
Nmap scan report for 192.168.1.187
Host is up (0.00014s 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
8000/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:25:AC:14 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 11.22 seconds
```

nmap -sS 192.168.1.187

-sS: Syn scan, detta anche "half-open scan", invia solo pacchetti SYN.

È rapida e furtiva (molti firewall la rilevano con più difficoltà).

- **Perché si usa:** È il tipo di scansione più veloce e discreto per identificare porte aperte.
- **Come funziona:** Invia un pacchetto SYN (inizio handshake) e legge la risposta, senza completare la connessione (stealth scan).

## TCP Connect Scan (per inviare pacchetti raw)

```
(kali@kali)~$ nmap -sT 192.168.1.187
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 10:16 EDT
Nmap scan report for 192.168.1.187
Host is up (0.00009s latency).
Not shown: 977 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
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: 08:00:27:25:AC:14 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 11.12 seconds
```

nmap -sT 192.168.1.187

**-sT**: usa la chiamata di sistema completa connect() per aprire le connessioni TCP.

È più facile da rilevare, ma non richiede privilegi di root.

- **Perché si usa**: È usato quando non hai i permessi per inviare pacchetti raw (es. senza privilegi di root).
- **Come funziona**: Esegue il normale handshake TCP completo (SYN, SYN-ACK, ACK).

## Differenze tra i due comandi -sS -sT

Nel risultato della riga quattro del comando -sS notiamo:

- Not Shown: 977 closed tcp ports (reset) – ovvero 977 porte chiuse che non vengono mostrate.

**-sS (SYN scan)**: È una **scansione "half-open"**, cioè Nmap invia solo un pacchetto SYN per vedere se la porta è aperta. Se è chiusa, riceve un pacchetto **RST (reset)** in risposta. → Mostrato come **(reset)** evidenziato nello screenshot (in arancione)

Mentre nel risultato del comando nmap -sT notiamo:

- Not Shown: 977 closed tcp ports (conn-refused) – indicazione che se la porta è chiusa, il sistema target rifiuta la connessione, e quindi si ottiene un **Connection Refused (conn-refused)**.

**-sT (TCP connect scan)**: È una **scansione completa**, che utilizza la funzione connect () del sistema operativo per aprire una vera connessione TCP. Se la porta è chiusa, il sistema target rifiuta la connessione, e quindi si ottiene un **Connection Refused**. → Mostrato come **(conn-refused)** evidenziato nello screenshot (in arancione).

Anche le tempistiche di risposta tra i due comandi sono diverse, il comando nmap -sS oltre ad essere più veloce è anche più "stealth" e lascia meno log nei target. Nonostante il metodo diverso, **entrambi hanno elencato le stesse porte aperte** e indicano che 977 porte erano chiuse (ma non mostrate in dettaglio).

## Version Detection (servizi in esecuzione delle porte aperte)

```
(kali@kali)~$ sudo nmap -sV 192.168.1.187
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 10:37 EDT
Nmap scan report for 192.168.1.187
Host is up (0.00031s latency).
Not shown: 977 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
53/tcp    open  domain         ISC BIND 9.4.2
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           netkit-rsh rshexec
513/tcp   open  login          OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi       GNU Classpath grmiregistry
1524/tcp  open  bindshell      Metasploitable root shell
2049/tcp  open  nfs            2-4 (RPC #100003)
2121/tcp  open  ftp            ProFTPD 1.3.1
3306/tcp  open  mysql          MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql     PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc            VNC (protocol 3.3)
6000/tcp  open  X11            (access denied)
6667/tcp  open  irc            UnrealIRCd
8009/tcp  open  ajp13          Apache Jserv (Protocol v1.3)
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:25:AC:14 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; 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 22.48 seconds
```

`sudo nmap -sV 192.168.1.187`

**-sV:** cerca di determinare le versioni dei servizi in esecuzione sulle porte aperte.

- **Perché si usa:** Identifica il tipo e la versione precisa dei servizi in esecuzione su una porta
- **Come funziona:** Interroga le porte aperte e analizza le risposte dei servizi.

**Sintesi finale:** il target presenta numerosi servizi attivi, alcuni dei quali obsoleti e a rischio.

L'implementazione tempestiva di contromisure (chiusura porte inutilizzate, aggiornamenti, cifratura dei servizi) porterà ad un significativo innalzamento della postura di sicurezza complessiva.

E la seguente sul target Windows: OS fingerprint.

```
(kali@kali)~$ ping 192.168.1.60
PING 192.168.1.60 (192.168.1.60) 56(84) bytes of data.
64 bytes from 192.168.1.60: icmp_seq=1 ttl=128 time=0.239 ms
64 bytes from 192.168.1.60: icmp_seq=2 ttl=128 time=0.424 ms
64 bytes from 192.168.1.60: icmp_seq=3 ttl=128 time=0.331 ms
64 bytes from 192.168.1.60: icmp_seq=4 ttl=128 time=0.341 ms
64 bytes from 192.168.1.60: icmp_seq=5 ttl=128 time=0.439 ms
64 bytes from 192.168.1.60: icmp_seq=6 ttl=128 time=0.731 ms
^C
--- 192.168.1.60 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5113ms
rtt min/avg/max/mdev = 0.239/0.417/0.731/0.154 ms
```

Come sempre controlliamo che le due macchine pinghino tra loro.

In questo caso l'ip di Windows è 192.168.1.60.

```
(kali@kali)~$ nmap -O 192.168.1.60
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 10:59 EDT
Nmap scan report for 192.168.1.60
Host is up (0.00056s latency).
Not shown: 980 closed tcp ports (reset)
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
80/tcp    open  http
135/tcp   open  mspc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1801/tcp  open  msmsg
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2187/tcp  open  msmsg-mgmt
2869/tcp  open  iclslap
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdaapi
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8443/tcp  open  https-alt

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.90 seconds
```

Andiamo ora ad usare il comando OS Fingerprint: `nmap -O 192.168.1.60` – verificando il sistema operativo che come possiamo constatare nello screenshot di sinistra, il risultato del comando, conferma il OS della nostra VM, in questo caso Windows 10.

## Conclusioni

**IP Target:** 192.168.1.187

Sistema Operativo:

Sistema Rilevato: Linux 2.6.x

Dettagli: Linux 2.6.9 - 2.6.33

MAC Address: 08:00:27:25:AC:14

Vendor NIC: PCS Systemtechnik / Oracle VirtualBox (virtual NIC)

### Porte Aperte e Servizi:

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

### Servizi aperti con Versione:

```
SERVICE      VERSION
ftp           vsftpd 2.3.4
ssh           OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
telnet        Linux telnetd
smtp          Postfix smtpd
domain        ISC BIND 9.4.2
http          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
rpcbind       2 (RPC #100000)
netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
exec          netkit-rsh rexecd
login
tcpwrapped
java-rmi      GNU Classpath grmiregistry
bindshell     Metasploitable root shell
nfs           2-4 (RPC #100003)
ftp           ProFTPD 1.3.1
mysql         MySQL 5.0.51a-3ubuntu5
postgresql    PostgreSQL DB 8.3.0 - 8.3.7
vnc           VNC (protocol 3.3)
X11           (access denied)
irc           UnrealIRCd
ajp13         Apache Jserv (Protocol v1.3)
http          Apache Tomcat/Coyote JSP engine 1.1
```

Le scansioni effettuate tramite Nmap sono state eseguite con l'obiettivo di identificare e documentare le caratteristiche principali degli host attivi all'interno della rete analizzata.

In particolare, l'attività ha permesso di raccogliere informazioni relative agli indirizzi IP, ai sistemi operativi rilevati, alle porte aperte e ai servizi in ascolto con le relative versioni.

Questi dati costituiscono la base informativa necessaria per una successiva fase di analisi nel nostro caso di pentesting.