

Pratica S5/L2:

Esercizio: 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?

E la seguente sul target Windows:

- OS fingerprint

Sistema Operativo	IPv4
Kali(source)	192.168.50.100/24
Metasploitable(destination)	192.168.60.101/24
Windows10(destination)	192.168.50.101/24

Metasploitable:

OS Fingerprinting (riconoscimento del sistema operativo) è una tecnica usata per identificare il sistema operativo in esecuzione su un host remoto analizzando il comportamento della rete o delle risposte ai pacchetti. Comando utilizzato:

- `sudo nmap -O 192.168.60.101`

Os rilevato: Linux 2.6.X

```
(kali@kali)-[~]
└─$ sudo nmap -O 192.168.60.101
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:01 EDT
Nmap scan report for 192.168.60.101
Host is up (0.00072s 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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded), Linux 2.6.20 - 2.6.24
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.72 seconds
```

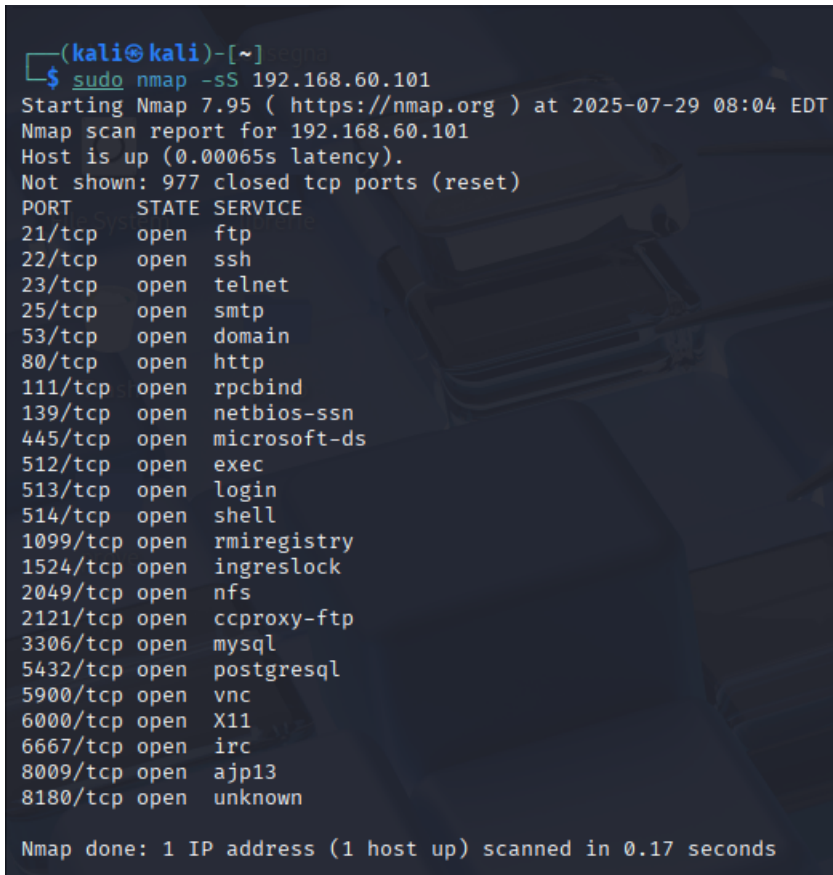
Syn Scan: Il SYN Scan è una tecnica di scansione delle porte TCP che permette di determinare lo stato (aperta, chiusa, filtrata) delle porte di un sistema senza stabilire una connessione completa. È

anche noto come "half-open scan" perché la connessione viene interrotta prima di completare il classico handshake TCP a tre vie:

- 1) L'attaccante invia un pacchetto **SYN** (synchronization) alla porta di destinazione.
- 2) Se la porta è **aperta**, il sistema risponde con un pacchetto **SYN-ACK**
- 3) Invece di completare la connessione con un ACK (come avviene nel normale handshake TCP), il client invia un pacchetto **RST** (reset) per interrompere la connessione.
- 4) Se la porta è **chiusa**, il sistema risponde direttamente con un **RST**.

Comando utilizzato:

- `sudo nmap -sS 192.168.60.101`



```
(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.60.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:04 EDT
Nmap scan report for 192.168.60.101
Host is up (0.00065s 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

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

TCP connect: Il TCP Connect Scan è una tecnica di scansione delle porte che utilizza il completo handshake TCP per determinare se una porta è aperta. È il metodo più semplice e affidabile, perché sfrutta direttamente le funzioni di connessione del sistema operativo:

- 1) Il client invia un pacchetto **SYN** alla porta di destinazione.
- 2) Se la porta è **aperta**, il server risponde con **SYN-ACK**.
- 3) Il client completa la connessione con un **ACK** (completando il **3-way handshake** TCP).
- 4) Dopo aver stabilito la connessione, il client la chiude subito (con un **FIN** o **RST**).

Comando utilizzato:

- `sudo nmap -sT 192.168.60.101`

```
(kali@kali)-[~]
$ sudo nmap -sT 192.168.60.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:09 EDT
Nmap scan report for 192.168.60.101
Host is up (0.00080s 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

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

Version detection: La Version Detection è una funzionalità di Nmap che consente di identificare il software esatto (nome, versione, a volte anche sistema operativo) in esecuzione su una porta aperta.

Comando utilizzato:

- Sudo nmap -sV 192.168.60.101

```
(kali@kali)-[~]
$ sudo nmap -sV 192.168.60.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:10 EDT
Nmap scan report for 192.168.60.101
Host is up (0.00078s 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 rexecd
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
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 11.69 seconds
```

Windows:

OS Fingerprinting (riconoscimento del sistema operativo) è una tecnica usata per identificare il sistema operativo in esecuzione su un host remoto analizzando il comportamento della rete o delle risposte ai pacchetti. Comando utilizzato:

- `sudo nmap -O 192.168.50.101`

Os rilevato: Microsoft Windows10

```
(kali@kali)-[~]
$ sudo nmap -O 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:11 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00027s latency).
Not shown: 982 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  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
3389/tcp  open  ms-wbt-server
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
MAC Address: 08:00:27:DF:AE:4B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
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 11.61 seconds
```