

# Report S5L2 - Nmap

## Introduzione

L'esercizio richiede di effettuare delle scansioni di servizi tramite Nmap. Le scansioni saranno effettuate dal terminale della kali, e si andranno ad effettuare:

- Sulla VM **metasploitable**:
  - OS Fingerprint;
  - Syn Scan;
  - TCP Connect;
  - Version Detection.
- Sulla VM **Windows 10**:
  - OS Fingerprint.

**Nmap** (Network Mapper) è uno strumento open-source estremamente potente e versatile per la scansione della rete e l'identificazione dei dispositivi e dei servizi.

Funzionalità principali di Nmap:

- Scansione degli Host: Identifica gli host attivi all'interno di una rete;
- Identificazione dei Servizi: Rileva i servizi in esecuzione su ciascun host, inclusi i numeri di porta e i protocolli;
- Rilevamento dei Sistemi Operativi: Utilizza varie tecniche di fingerprinting per determinare il sistema operativo in esecuzione su un host;
- Scansione delle Vulnerabilità: Può essere utilizzato per identificare potenziali vulnerabilità nei dispositivi e nei servizi rilevati.

Il primo step è quello di impostare tutte le macchine virtuali in modo da averne 3 connesse in Bridge con la scheda di rete dell'host.



Scheda 1: Intel PRO/1000 MT Desktop (Scheda con bridge, Realtek PCIe GbE Family Controller)

## Controllare l'indirizzo IP delle 3 macchine attraverso la console:

```
Last login: Tue Jan 6 13:33:04 EST 2026 on tty1
linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
or write to mail.

hsfadmin@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 08:00:27:1a:d4:54 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.127/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe1a:d454/64 scope link
        valid_lft forever preferred_lft forever
hsfadmin@metasploitable:~$
```

```
Prompt dei comandi
C:\Users\user>ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv4. . . . . : 192.168.1.125
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1

Scheda Tunnel isatap.{92D61F82-1D19-45C9-B7CF-2E5AF2D63627}:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6. . . . . : 2001:0:2851:782c:2039:1621:68b6:71b1
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::2039:1621:68b6:71b1%5
    Gateway predefinito . . . . . :
```

```
kali@kali: ~
Session Actions Edit View Help
command 'ifconfig' from deb net-tools
Try: sudo apt install <deb name>

(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:63:b0:05 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.126/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
        valid_lft 40500sec preferred_lft 40500sec
    inet6 fe80::9934:39ab:244:b8a1/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali@kali)-[~]
$
```

Prima di avviare le attività di scansione, è stata verificata la raggiungibilità degli host all'interno della sottorete. La mappatura degli asset ha confermato la seguente distribuzione degli indirizzi IP:

- **Windows 10:** 192.168.1.125;
- **Metasploitable:** 192.168.1.127;
- **Kali Linux:** 192.168.1.126.

Gli indirizzi IP ci saranno necessari per indirizzare i nostri scan, una volta fatto questo si può procedere con le scansioni.

## Target 1: Metasploitable 2

In questa fase abbiamo testato la macchina vulnerabile per eccellenza per osservare come risponde a scansioni aggressive.

### A. OS Fingerprinting

L'**OS Fingerprinting** è la tecnica che Nmap utilizza per determinare il sistema operativo del target senza che questo lo dichiari esplicitamente.

Comando: `sudo nmap -O 192.168.1.127`

```
(kali@kali)-[~]
$ nmap -O 192.168.1.127
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 13:47 EST
Nmap scan report for 192.168.1.127
Host is up (0.0068s 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: 08:00:27:1A:D4:54 (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 1.88 seconds
```

Il comando quindi ci darà come risultato

OS details: Linux 2.6.9 - 2.6.33



## B. SYN Scan vs TCP Connect Scan

Comandi:

- SYN scan: nmap -sS 192.168.1.127
- TCP scan: nmap -sT 192.168.1.127.

```
(kali@kali)-[~]
$ nmap -sS 192.168.1.127
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 13:48 EST
Nmap scan report for 192.168.1.127
Host is up (0.019s 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: 08:00:27:1A:D4:54 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
```

```
(kali@kali)-[~]
$ nmap -sT 192.168.1.127
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 13:48 EST
Nmap scan report for 192.168.1.127
Host is up (0.0089s 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: 08:00:27:1A:D4:54 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
```

Il SYN scan e il TCP scan mostrano sostanzialmente lo stesso risultato, la differenza tra i due risiede nelle performance e nella visibilità.

Il **SYN scan** infatti è più rapido del **TCP scan** ed anche meno visibile. Se analizzassimo il traffico con **Wireshark**, vedremmo che il TCP Connect lascia tracce complete nei log dei servizi (es. un server HTTP loggherà una connessione), mentre il SYN scan no, in quanto non completa il **Three-Way Handshake**.

Il **Three-Way Handshake** è la "stretta di mano" in **tre passaggi** necessaria per stabilire una connessione affidabile tra due computer.

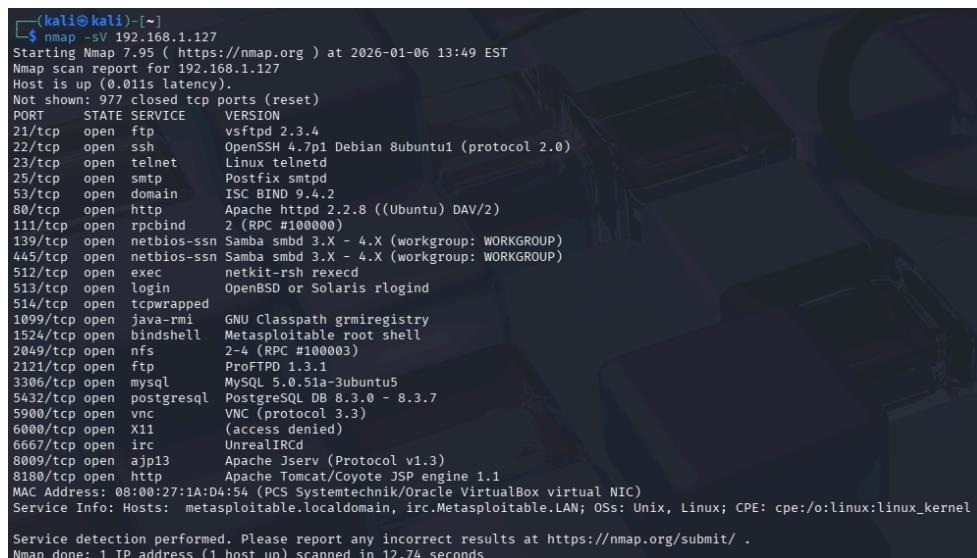
1. **SYN (Synchronize)**: Il Client invia un pacchetto per dire: *"Ehi, vorrei connettermi alla porta X, ecco il mio numero di sequenza"*.
2. **SYN-ACK (Synchronize-Acknowledge)**: Se la porta è aperta, il Server risponde: *"Ricevuto! Anche io sono pronto, ecco il mio numero di sequenza"*.
3. **ACK (Acknowledge)**: Il Client risponde: *"Ok, ho ricevuto tutto, ora iniziamo a scambiare dati"*.

Il SYN Scan è chiamato infatti anche **"Half-Open Scan"** (scansione semi-aperta) proprio perché interrompe bruscamente la procedura dell'handshake al secondo passaggio.

### C. Version Detection

La **Version Detection** è il processo con cui Nmap cerca di capire esattamente **quale software** e **quale versione** specifica stanno girando su una porta aperta.

Comando: `nmap -sV 192.168.1.127`



```
(kali@kali)~$ nmap -sV 192.168.1.127
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 13:49 EST
Nmap scan report for 192.168.1.127
Host is up (0.011s 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
MAC Address: 08:00:27:1A:D4:54 (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 12.74 seconds
```

Come possiamo notare dallo screenshot, questo processo ci ha fornito informazioni su quale software e quale versione giri su una determinata porta.

Prendiamo come esempio la **porta 3306** che ospita il servizio **mysql** con la versione **MySQL 5.0.51a-3ubuntu5**.

# Target 2: Windows

Ora si effettuerà l'OS Fingerprinting su Windows10 per confrontarne le differenze.

## A. OS Fingerprinting

Comando: `sudo nmap -O 192.168.1.125`

```
(kali@kali)-[~]
$ nmap -O 192.168.1.125
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 13:51 EST
Nmap scan report for 192.168.1.125
Host is up (0.0016s latency).
Not shown: 981 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
5357/tcp  open  wsddapi
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
MAC Address: 08:00:27:0F:7D:95 (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 2.65 seconds
```

Contrariamente a quanto avviene solitamente con i target **Windows**, caratterizzati da poche porte aperte e firewall restrittivi che costringono **Nmap** a formulare delle stime (**Guess**), in questo test l'identificazione è risultata univoca. La presenza di servizi accessibili ha permesso a **Nmap** di raccogliere un numero sufficiente di campioni (*fingerprints*), portando a un'identificazione certa del sistema come **Microsoft Windows 10 (versioni 1507 - 1607)** senza la necessità di proporre ipotesi alternative.