

Report S5/L2

Scansione Nmap

La traccia ci chiede di effettuare le seguenti scansioni utilizzando Nmap sul target Metasploitable:

- OS fingerprint
- Syn Scan
- TCP connect - trovate differenze tra i risultati della scansione TCP connect e SYN?
- Version detection

Inoltre sul target Windows:

- OS fingerprint

Nmap(Network Mapper):

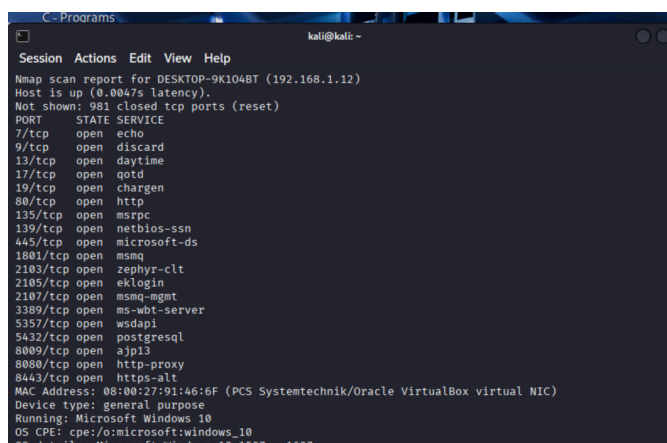
è uno strumento open-source estremamente potente per la scansione della rete e l'identificazione dei dispositivi e dei servizi. Utilizzato nella fase 2 del Penetration Testing per la mappatura di rete:

- Identificazione dei dispositivi: Rilevare e identificare tutti i dispositivi collegati alla rete, inclusi client, server, router, switch e altri dispositivi di rete.
- Rilevamento dei protocolli: Determinare quali protocolli di rete vengono utilizzati dai dispositivi, come HTTP, HTTPS ecc.
- Scansione delle Porte: Identificare le porte aperte e i servizi in esecuzione su ciascun dispositivo
- Analisi della Topologia: Comprendere la disposizione e le interconnessioni tra i vari dispositivi nella rete.

-Test sulla Metasploitable:

OS fingerprint

nmap -O 192.168.1.12 (analizza come risponde la rete per capire il sistema operativo dell'Host)



```
C:\Programs
kali@kali: ~
Session Actions Edit View Help
Nmap scan report for DESKTOP-9K104BT (192.168.1.12)
Host is up (0.0047s 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  mstpc
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  wsdapi
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
MAC Address: 08:00:27:91:46:6F (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
```

- Test SYN SCAN :

nmap -sS 192.168.1.10 Questo tipo di tecnica di scansione è più veloce e furtiva rispetto a TCP (La SYNSCAN non chiude la connessione)

```
(kali@kali)-[~]
$ nmap -sS 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 12:26 EST
Nmap scan report for PC192.168.1.10.homenet.telecomitalia.it (192.168.1.10)
Host is up (0.0012s 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: 08:00:27:49:97:E2 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 1.20 seconds
```

- Test TCP Connect:

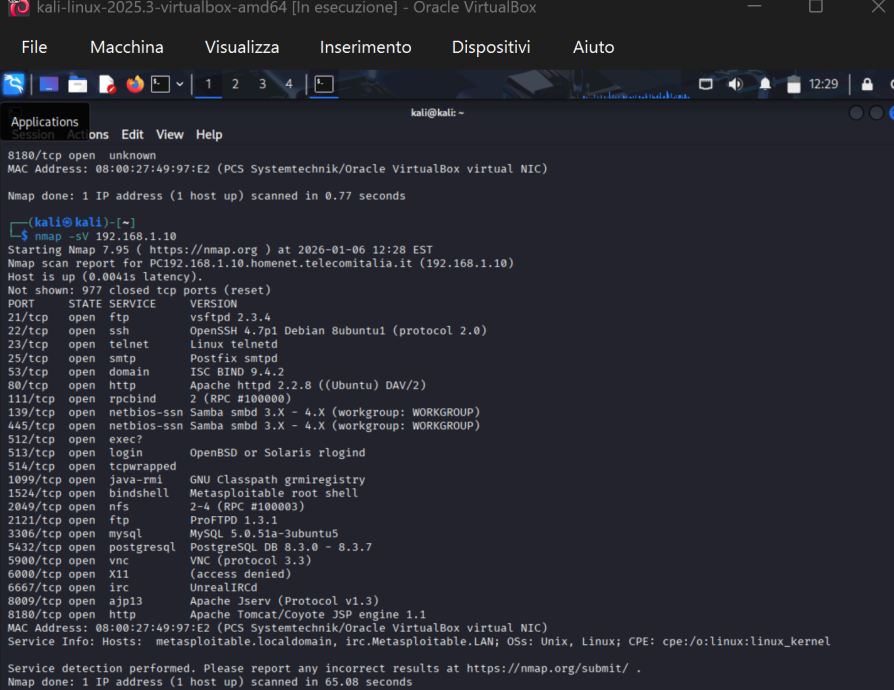
nmap -sT 192.168.1.10

La differenza che notiamo subito è che **Nmap -sT** risulta meno veloce (completa il three-way handshake di TCP)

```
(kali@kali)-[~]
$ nmap -sT 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 12:27 EST
Nmap scan report for PC192.168.1.10.homenet.telecomitalia.it (192.168.1.10)
Host is up (0.0056s 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: 08:00:27:49:97:E2 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds
```

- Test Version Detection:

nmap -sV 192.168.1.10 questo comando serve per vedere la versioni dei servizi tramite le porte aperte



```
kali-linux-2025.3-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

Applications
Session Actions Edit View Help

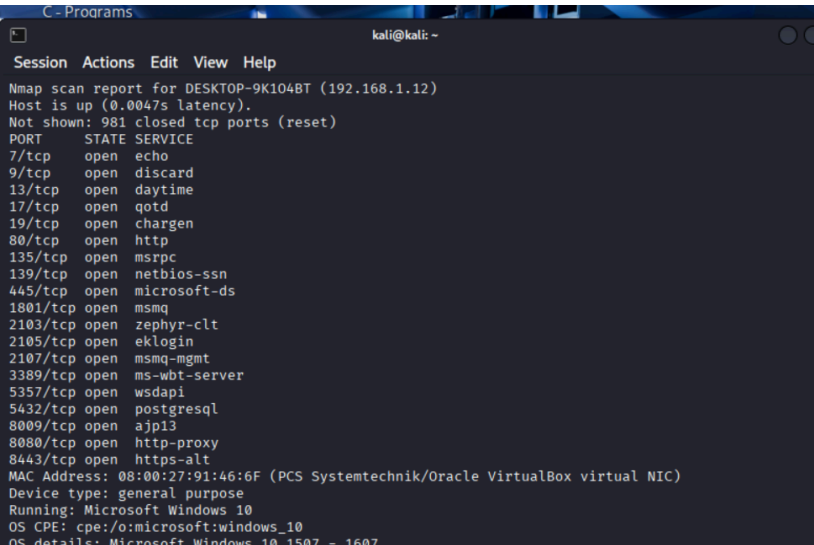
8180/tcp open  unknown
MAC Address: 08:00:27:49:97:E2 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds

(kali@kali)-[~]
└─$ nmap -sV 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 12:28 EST
Nmap scan report for PC192.168.1.10.homenet.telecomitalia.it (192.168.1.10)
Host is up (0.0041s 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?
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: 08:00:27:49:97:E2 (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 65.08 seconds
```

- Test target Windows:

nmap -O 192.168.1.12



```
C:\Programs
kali@kali: -

Session Actions Edit View Help

Nmap scan report for DESKTOP-9K104BT (192.168.1.12)
Host is up (0.0047s 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  wsdapi
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
MAC Address: 08:00:27:91:46:6F (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
```