

## Scansione con Nmap

In questa relazione ho descritto in modo dettagliato l'attività di laboratorio svolta utilizzando lo strumento Nmap, con l'obiettivo di apprendere le principali tecniche di scansione di rete.

### strumenti utilizzati

L'attività è stata svolta utilizzando la macchina virtuale Kali Linux come macchina attaccante. Come target di Linux ho utilizzato la macchina virtuale Metasploitable. Poi è stata utilizzata una macchina Windows solo per il OS fingerprinting.

### Individuazione degli indirizzi IP

Prima di procedere con le scansioni era necessario individuare gli indirizzi IP dei target. Una volta avviate le macchine virtuali, ho identificato i seguenti indirizzi:

Metasploitable:	192.168.60.10
Windows:	192.168.50.152

Questi indirizzi sono stati utilizzati come riferimento per tutte le successive scansioni Nmap.

### OS Fingerprinting su Metasploitable

La prima scansione che ho effettuato su Metasploitable è stata l'OS fingerprinting, con lo scopo di individuare il sistema operativo del target. Per eseguire questa operazione è stato utilizzato il comando:

```
[root@kali]~[/home/kali]
# nmap -O 192.168.60.10
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-07 11:54 EST
Nmap scan report for 192.168.60.10
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    filtered 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)
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 3.35 seconds
```

nmap

-O

192.168.60.10

Questo comando consente a Nmap di inviare una serie di pacchetti TCP/IP appositamente costruiti e di analizzare le risposte del sistema target. Dal comportamento dello stack di rete Nmap è stato in grado di determinare che il sistema operativo del target è Linux, con kernel della serie 2.6.X.

## SYN Scan

Successivamente è stata eseguita una scansione SYN, nota anche come stealth scan. Il comando utilizzato è stato:

```
[root@kali] ~
# nmap -sS 192.168.60.10
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-07 11:59 EST
Nmap scan report for 192.168.60.10
Host is up (0.0016s 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    filtered 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 1.46 seconds
```

nmap

-sS

192.168.60.10

Questa tecnica prevede l'invio di pacchetti TCP SYN alle porte del target senza completare il three-way handshake. Se una porta risponde con SYN/ACK, viene considerata aperta. Questa scansione è particolarmente efficiente perché veloce e meno rilevabile dai sistemi di logging. Il risultato ha mostrato un elevato numero di porte aperte, tra cui FTP, SSH, Telnet, HTTP e database.

## TCP Connect Scan e confronto

Per confrontare i risultati ottenuti con il SYN Scan, ho eseguito una scansione TCP Connect utilizzando il comando:

```
└─(root㉿kali)-[~/home/kali]
└─# nmap -sT 192.168.60.10
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-07 12:03 EST
Nmap scan report for 192.168.60.10
Host is up (0.0016s 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    filtered 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 1.47 seconds
```

nmap -sT 192.168.60.10

A differenza del SYN Scan, questa tecnica completa interamente il three-way handshake TCP. Dal punto di vista dei risultati le porte aperte individuate coincidono con quelle del SYN Scan, tuttavia questa scansione risulta più rumorosa e facilmente tracciabile poiché le connessioni vengono registrate nei log del sistema target. Questo confronto evidenzia come il SYN Scan sia preferibile in contesti di penetration testing.

## Version Detection

Una volta individuate le porte aperte, ho fatto la scansione di rilevamento delle versioni dei servizi in ascolto mediante il comando:

```

└─(root㉿kali㉿kali)-[~/home/kali]
# nmap -sV 192.168.60.10
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-07 12:06 EST
Stats: 0:01:21 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.45% done; ETC: 12:07 (0:00:04 remaining)
Stats: 0:02:29 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.45% done; ETC: 12:08 (0:00:07 remaining)
Stats: 0:02:43 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.90% done; ETC: 12:09 (0:00:00 remaining)
Stats: 0:02:47 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.90% done; ETC: 12:09 (0:00:00 remaining)
Stats: 0:02:49 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.92% done; ETC: 12:09 (0:00:00 remaining)
Stats: 0:02:55 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.92% done; ETC: 12:09 (0:00:00 remaining)
Nmap scan report for 192.168.60.10
Host is up (0.0021s 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    filtered http
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?
514/tcp   open      shell        Netkit rshd
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      ccproxy-ftp?
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 176.21 seconds

```

nmap

-sV

192.168.60.10

Questa scansione permette a Nmap di interrogare direttamente i servizi attivi e di analizzarne i banner. I risultati hanno mostrato la presenza di servizi obsoleti e vulnerabili, come vsftpd 2.3.4 per il servizio FTP, Apache 2.2.8 per il servizio HTTP e MySQL 5.0.51a per il database.

## OS Fingerprinting sul target Windows

Infine ho fatto l'OS fingerprinting sul target Windows, utilizzando il comando:

```
[root@kali] /home/kali]
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-07 12:18 EST
Nmap scan report for 192.168.50.152
Host is up (0.00030s latency).
Not shown: 555 closed ports
PORT      STATE SERVICE
7/tcp      open  echo
9/tcp      open  discard
13/tcp     open  systime
17/tcp     open  gopher
19/tcp     open  chargen
80/tcp     open  http
113/tcp    open  nntp
139/tcp    open  netbios-ssn
445/tcp   open  microsoft-ds
8080/tcp  open  http-proxy
843/tcp  open  https-alt
MAC Address: 08:00:27:7C:F2:D0 (PC Systemtechnik/Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Microsoft Windows 10 1507 - 1607 (98%), Microsoft Windows 10 1511 - 1607 (98%), Microsoft Server 2008 R2 SP1 (98%), Microsoft Windows 10 (95%), Microsoft Windows Vista SP2 or Windows 7 or Windows Server 2008 R2 or Windows 8.1 (95%), Microsoft Windows Server 2016 or Server 2019 (95%), Microsoft Windows 7 Professional (95%), Microsoft Windows 7 Ultimate (95%), Microsoft Windows 7 or 8.1 R1 or Server 2008 R2 SP1 (95%), Microsoft Windows 10 1703 (95%)
No exact OS matches for host (test conditions non-ideal).
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 6.07 seconds
```

nmap -O 192.168.50.152

Analizzando le risposte del sistema, Nmap ha identificato il target come un sistema operativo Microsoft Windows. Questo dimostra come il fingerprinting permetta di distinguere chiaramente sistemi Linux e Windows sulla base del loro comportamento di rete.

## Risultati finali

Per il target Metasploitable sono state individuate numerose porte aperte, tra cui la 21 (FTP), la 22 (SSH), la 23 (Telnet), la 80 (HTTP) e la 3306 (MySQL). Il sistema operativo identificato è Linux. Per il target Windows è stato identificato come un sistema operativo Microsoft Windows. I risultati ottenuti rispettano gli obiettivi della traccia.

## Conclusione

L'attività ha permesso di comprendere l'importanza delle tecniche di scansione di rete nell'ambito della sicurezza informatica. L'utilizzo di Nmap ha dimostrato come è possibile ottenere informazioni dettagliate su un sistema remoto, evidenziando potenziali rischi di sicurezza.

