

S5L2



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 della scansioni TCP connect e SYN?
- Version detection.

E la seguente sul target Windows:

- OS fingerprint.

Per completare l'esercizio, ho impostato gli indirizzi IP delle macchine in modo da averli in una rete locale, in questo modo: Windows = 192.168.50.104 e Metasploitable2 = 192.168.50.101.

Fatto questo possiamo passare alla parte delle scansioni su Metasploitable.

Windows: Ho utilizzato il programma nmap con **-O** per l'OS fingerprint e **-sV** per identificare i programmi che girano dentro l'host e la loro versione. (Sono consapevole che sV non fa parte della richiesta, ma per comodità di digitazione, ho ricopiato la sintassi utilizzata per Metasploitable2.

```
(kali@kali)-[~]
$ nmap -O -sV 192.168.50.104
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:32 EDT
Nmap scan report for 192.168.50.104
Host is up (0.00013s latency).
Not shown: 982 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
7/tcp     open  echo
9/tcp     open  discard?
13/tcp    open  daytime      Microsoft Windows International daytime
17/tcp    open  qotd          Windows qotd (English)
19/tcp    open  chargen
80/tcp    open  http          Microsoft IIS httpd 10.0
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds   Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
1801/tcp  open  msmq?
2103/tcp  open  msrpc         Microsoft Windows RPC
2105/tcp  open  msrpc         Microsoft Windows RPC
2107/tcp  open  msrpc         Microsoft Windows RPC
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5432/tcp  open  postgresql?
8009/tcp  open  ajp13         Apache Jserv (Protocol v1.3)
8080/tcp  open  http          Apache Tomcat/Coyote JSP engine 1.1
8443/tcp  open  ssl/https-alt
MAC Address: 08:00:27:88:CE:24 (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
Service Info: Host: DESKTOP-9K104BT; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 173.92 seconds
```

Metasploitable: Anche qui chiaramente ho utilizzato nmap con **-O** per l'OS fingerprint e **-sV** per identificare i programmi che girano dentro l'host e la loro versione. Ho utilizzato due comandi in un'unica richiesta per comodità. Nello screen troveremo le porte aperte, il tipo di OS e la versione dei programmi che girano al suo interno.

```
(kali@kali)-[~]
$ nmap -O -sV 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:38 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00011s 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?
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  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: 08:00:27:57:52:FB (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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 67.91 seconds
```

Nmap -sS: (Metasploitable2): Questo comando serve per la TCP SYN Scan. Questo comando è una scansione che “bussa” alla porta ma non entra. Da qui deriva il termine “Scansione stealth”.

Questo comando non completa il 3-way-handshake e richiede privilegi da amministratore.

```
(kali@kali)-[~]
$ nmap -sS 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:51 EDT
Nmap scan report for 192.168.50.101
Host is up (0.000091s 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: 08:00:27:57:52:FB (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.26 seconds
```

Nmap -sT (Metaspitable2): Questo comando serve per la TCP connect scan. Questo comando è una scansione che al contrario di -sS non si limita a bussare, ma completa il 3-way-handshake e non richiede privilegi da amministratore.

```
(kali@kali)-[~]
$ nmap -sT 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 09:02 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00016s 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: 08:00:27:57:52:FB (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds
```

Ricapitolando nel corso di questa esercitazione i comandi impiegati sono stati:

OS Fingerprinting: Utilizzando il comando nmap -O, ho ottenuto informazioni dettagliate sui sistemi operativi in esecuzione su entrambe le macchine. Questo ha permesso di confermare le versioni dei sistemi operativi e di identificare potenziali vulnerabilità associate a ciascun sistema.

TCP Connect Scan: Con il comando nmap -sT, ho eseguito una scansione delle porte, scoprendo quali porte erano aperte e quali servizi stavano girando sulla macchina in questione. Questo tipo di scansione è utile per rilevare eventuali servizi non protetti o vulnerabili.

Syn Scan: Con l'uso del comando nmap -sS, ho effettuato una scansione stealth, che permette di raccogliere informazioni senza completare il 3-way handshake, riducendo così la possibilità di essere rilevati.

Version detection: Utilizzando il comando -sV, ho ottenuto la versione dei programmi che girano nel dispositivo e il rispettivo sistema operativo. Tramite questo comando si possono ottenere informazioni dettagliate sul dispositivo.

In generale, l'esercizio mi ha permesso di mettere in pratica diverse tecniche di scansione e raccolta informazioni cruciali per questa fase in un attacco informatico.

L'accuratezza delle informazioni che ho ottenuto da Nmap dimostra l'efficacia degli strumenti di penetration testing nel determinare le caratteristiche di una rete e dei sistemi in essa contenuti, fornendo un punto di partenza fondamentale per l'analisi di sicurezza.

