

Report di Scansione di Rete e Analisi dei Servizi

Data: 29 Luglio 2025

Autore: Marco Falchi

Obiettivo: Eseguire scansioni di rete sui target forniti per identificare sistemi operativi, porte aperte e servizi attivi, come richiesto dall'esercizio.

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.
-

Target 1: Metasploitable

A seguito delle scansioni effettuate sul target Metasploitable, sono state raccolte le seguenti informazioni dall'ip:

- **IP: 192.168.50.101**

1.1 OS Fingerprinting

Questa scansione identifica il sistema operativo del target:

- **Comando:** `nmap -O 192.168.50.101`

```
(kali㉿kali)-[~]
$ nmap -O 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:45 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00039s 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: 08:00:27:12:FF:6C (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 14.82 seconds
```

- **Sistema Operativo trovato:** Linux 2.6.9 – 2.6.33

1.2 SYN Scan

Lo SYN scan è un tipo di scansione furtiva che non completa la connessione TCP, rendendola meno facilmente rilevabile

- **Comando:** `nmap -sS 192.168.50.101`

```
(kali㉿kali)-[~]  
$ nmap -sS 192.168.50.101  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:34 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.00015s 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: 08:00:27:12:FF:6C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.38 seconds
```

1.3. TCP Connect Scan

A differenza dello SYN scan, questa tecnica completa la connessione TCP a tre vie. È più rumorosa ma può essere più affidabile in certi contesti.

- **Comando:** `nmap -sT 192.168.50.101`

```
(kali㉿kali)-[~]  
$ nmap -sT 192.168.50.101  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:37 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.00014s 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: 08:00:27:12:FF:6C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds
```

Differenze tra i risultati di TCP Connect e SYN Scan:

Le differenze tra queste due scansioni sono generalmente:

-Velocità: Lo SYN scan è spesso più veloce perché non completa la connessione.

-Rilevabilità: Lo SYN scan è considerato "stealth" o furtivo perché non stabilisce una sessione TCP completa, generando meno log sui sistemi target. Il TCP Connect scan, invece, è facilmente registrabile dai firewall e dai sistemi di rilevamento delle intrusioni.

-Privilegi: Per eseguire uno SYN scan (-sS) sono necessari i privilegi di root (o amministratore), mentre un TCP Connect scan (-sT) può essere eseguito da un utente standard.

I risultati in termini di porte aperte dovrebbero essere identici. Qualsiasi differenza potrebbe indicare la presenza di un firewall o di un IDS/IPS che blocca specificamente i pacchetti SYN.

1.4 Version Detection

Questa scansione non solo rileva le porte aperte, ma interroga anche i servizi in esecuzione per determinarne la versione software

- **Comando:** `nmap -sV 192.168.50.101`

```
(kali@kali)-[~]
$ nmap -sV 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:33 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00014s 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: 08:00:27:12:FF:6C (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 24.62 seconds
```


Target 2: Windows

A seguito delle scansioni effettuate sul target Metasploitable, sono state raccolte le seguenti informazioni dall'ip:

- **IP:** 192.168.50.102

2.1 OS Fingerprinting

Comando: nmap -O 192.168.50.102

```
(kali@kali)-[~]
$ nmap -O 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:46 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00039s 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: 08:00:27:76:3B:86 (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 31.87 seconds
```

- **Sistema Operativo trovato:** Windows 10 1507-1607

