

ESERCIZIO S5 L2

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.

A valle delle scansioni è prevista la produzione di un report contenente le seguenti info (dove disponibili):

- IP.
- Sistema Operativo.
- Porte Aperte.
- Servizi in ascolto con versione.

RISPOSTA

Durante questa sessione, ho condotto una serie di scansioni Nmap su due target distinti: una macchina Metasploitable e un sistema Windows 10 . L'obiettivo era quello di testare diverse tecniche di scansione e confrontarne i risultati.

Come primo passo, procedo con impostare gli indirizzi IP delle VM che si troveranno sulla stessa rete interna:

Kali : 192.168.70.100

Metasploitable : 192.168.70.101

Windows 10 : 192.168.70.102

Prendo **Metasploitable** come target iniziale e procedo con la scansione **OS fingerprint**

Utilizzo il comando:

nmap -O >>> Rileva il sistema operativo del target

```
(kali㉿kali)-[~]
$ nmap -O 192.168.70.100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:15 EDT
Nmap scan report for 192.168.70.100
Host is up (0.00073s latency).
Not shown: 982 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
111/tcp   open  rpcbind
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
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: 08:00:27:72:CE:0F (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 14.73 seconds
```

I risultati ci mostrano le varie porte ed infine i dettagli che riguardano il sistema operativo del target.

Passo alla seconda scansione **Syn Scan**. Utilizzo il comando:

nmap -sS >>> Scansione “stealth” delle porte che non completa il three-way-handshake

```

(kali㉿kali)-[~]
$ nmap -sS 192.168.70.100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:17 EDT
Nmap scan report for 192.168.70.100
Host is up (0.00057s latency).
Not shown: 982 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
111/tcp   open  rpcbind
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
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: 08:00:27:72:CE:0F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.35 seconds

```

Successivamente, procedo con la scansione **TCP connect**, utilizzando il comando:

nmap -sT >>> Scansione porte TCP che a differenza del Syn Scan completa il three-way-handshake.

```

(kali㉿kali)-[~]
$ nmap -sT 192.168.70.100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:18 EDT
Nmap scan report for 192.168.70.100
Host is up (0.0011s latency).
Not shown: 982 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
111/tcp   open  rpcbind
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
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: 08:00:27:72:CE:0F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds

```

Come ultima scansione procedo con la Version detection utilizzando il comando:

nmap -sV >>> Identifica software e versioni dei servizi

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.70.100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:19 EDT
Nmap scan report for 192.168.70.100
Host is up (0.00032s latency).
Not shown: 982 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
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
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
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: 08:00:27:72:CE:0F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: 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 112.66 seconds
```

Le differenze che ho notato tra le due scansioni **Syn Scan e TCP connect** :

La Syn Scan risulta più safe o meglio “stealth” dato che raccoglie informazioni senza essere rilevata (non completa il three-way-handshake) dunque non completa la connessione al contrario di TCP connect che esegue una connessione completa e di conseguenza è più rilevabile ma potrebbe ritornare alcuni risultati non accurati sullo status delle porte a causa del firewall o ips.

Le velocità di scansione sono state prevalentemente identiche con una leggerissima differenza: Syn Scan (generalmente più veloce) : **13.35s**, mentre TCP connect **13.34s**.

Ora passo all'ultimo target : Windows 10 con IP 192.168.70.102

Eseguo il comando **nmap -O**, rilevando il sistema operativo del target.

```
(kali@kali)-[~]
$ nmap -O 192.168.70.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:55 EDT
Nmap scan report for 192.168.70.102
Host is up (0.0017s 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: 08:00:27:86:54:F0 (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 16.34 seconds
```

CONCLUSIONE

Con questa esercitazione ho potuto fare pratica con i vari comandi di **Nmap**, raccogliendo informazioni importanti che riguardano le reti e i sistemi target, e comprendendo le tecniche di scansione ed il loro utilizzo, aspetti molto importanti per la seconda fase del Penetration Testing chiamata Enumeration.