

## S5/L3

### Tecniche di scansione con Nmap

Nell'esercizio di oggi ci è stato richiesto di effettuare le seguenti scansioni con nmap 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 7:

- OS fingerprint

### OS fingerprint

```
(root@kali)-[/home/kali]
# nmap -O 192.168.60.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 11:03 EST
Nmap scan report for 192.168.60.101
Host is up (0.0033s 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
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 1.80 seconds
```

Abbiamo effettuato questa scansione con il comando:

**nmap -O 192.168.60.101**

Eseguendo questo comando, oltre a vedere le porte TCP aperte, ci fornisce anche il sistema operativo del target. (Linux 2.6.15 - 2.6.26).

## Syn Scan

```
(root@kali)-[/home/kali]
# nmap -sS 192.168.60.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 11:05 EST
Nmap scan report for 192.168.60.101
Host is up (0.0021s 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

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

Abbiamo effettuato questa scansione con il comando:

**nmap -sS 192.168.60.101**

È un metodo meno invasivo in quanto una volta appurato che una porta è aperta chiude la comunicazione. Più difficile da individuare.

## TCP connect

```
(root@kali)-[/home/kali]
# nmap -sT 192.168.60.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 11:06 EST
Nmap scan report for 192.168.60.101
Host is up (0.0055s 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

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

Abbiamo effettuato questa scansione con il comando:

**nmap -sT 192.168.60.101**

A differenza del Syn Scan, il TCP Connect è un metodo molto invasivo oltre a controllare se una porta è aperta crea un canale e per questo è facilmente individuabile.

Come possiamo notare non ci sono differenze tra il Syn Scan e il TCP Connect.

## Version detection

```
(root@kali)-[/home/kali]
# nmap -sV 192.168.60.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 11:06 EST
Nmap scan report for 192.168.60.101
Host is up (0.0047s 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        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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; O
Ss: 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 12.59 seconds
```

Abbiamo effettuato questa scansione con il comando:

**<< nmap -sV 192.168.60.101>>**

Con questa scansione possiamo identificare i servizi attivi sulle specifiche porte e le versioni. Possiamo anche notare che rispetto alle altre scansioni i tempi aumentano notevolmente.

## OS fingerprint su Windows7

Nel primo tentativo, il firewall era attivo, e non siamo riusciti ad ottenere nessuna informazione.

```
(root@kali)-[/home/kali]
# nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 11:50 EST
Nmap scan report for 192.168.50.102
Host is up (0.0074s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: A2:9A:F0:88:06:2A (Unknown)
Too many fingerprints match this host to give specific OS details
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 24.42 seconds
```

Mentre nel secondo tentativo, abbiamo disattivato il firewall, e come possiamo notare la scansione è avvenuta in modo corretto restituendoci le informazioni disponibili tra cui il sistema operativo Windows7.

Da notare i tempi molto più lunghi nel primo tentativo.

```
(root@kali)-[/home/kali]
# nmap -O -Pn 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 11:25 EST
Nmap scan report for 192.168.50.102
Host is up (0.0014s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsddapi
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
MAC Address: A2:9A:F0:88:06:2A (Unknown)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/
o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r
2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows
Server 2008 R2, Windows 8, or Windows 8.1 Update 1
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 2.49 seconds
```