

**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 7:

- OS fingerprint.

## SCAN SU METASPLOITABLE 2

1. Procediamo con le scansioni di OS Fingerprint con il comando `nmap -O` per l'identificazione del Sistema Operativo:

```
(root@kali)-[/home/kali]
# nmap -O 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 18:24 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00078s 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: 08:00:27:6E:F3:5C (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 14.56 seconds
```

2. Proseguiamo con le scansioni di OS Fingerprint con il comando `nmap -sV` per l'identificazione delle versioni disponibili sulle porte scansionate del Sistema Operativo (Version Detection):

```
(root@kali)~[/home/kali]
# nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 18:29 EDT
Nmap scan report for 192.168.50.101
Host is up (0.000079s 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 rshcd
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: 08:00:27:6E:F3:5C (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 65.56 seconds
```

3. Proseguiamo con le scansioni di OS Fingerprint con il comando `nmap -PR` per l'identificazione delle richieste ARP sul Sistema Operativo in esame:

```
(root@kali)~[/home/kali]
# nmap -PR 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 18:33 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00012s 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: 08:00:27:6E:F3:5C (Oracle VirtualBox virtual NIC)

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

4. Proseguiamo con le scansioni di OS Fingerprint con il comando `nmap -sS` per effettuare un SYN SCAN, un metodo di Scannerizzazione mono-invasivo che non completa il 3 Way Handshake:

```
(root@kali)-[/home/kali]
# nmap -sS 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 18:42 EDT
Nmap scan report for 192.168.50.101
Host is up (0.000069s 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: 08:00:27:6E:F3:5C (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
```

5. Proseguiamo con le scansioni di OS Fingerprint con il comando `nmap -sT`, effettua uno scan più invasivo completando il 3 Way Handshake creando il canale di comunicazione:

```
(root@kali)-[/home/kali]
# nmap -sT 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 18:45 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00020s 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: 08:00:27:6E:F3:5C (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
```



## SCAN SU WIN 7

1. Procediamo ora con le scansioni di OS Fingerprint con il comando `nmap -O` per l'identificazione del Sistema Operativo di Win 7:

```
(root@kali)-[/home/kali]
# nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 19:09 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00081s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
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: 08:00:27:0C:68:4A (Oracle VirtualBox virtual NIC)
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_7::sp2
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2 SP1
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 24.69 seconds
```

2. Proseguiamo con le scansioni di OS Fingerprint con il comando `nmap -sV` per l'identificazione delle versioni disponibili sulle porte scansionate del Sistema Operativo (Version Detection):

```
(root@kali)-[/home/kali]
# nmap -sV 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 19:11 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00010s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
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)
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
49155/tcp  open  msrpc        Microsoft Windows RPC
49156/tcp  open  msrpc        Microsoft Windows RPC
49157/tcp  open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:0C:68:4A (Oracle VirtualBox virtual NIC)
Service Info: Host: MARIO-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 73.42 seconds
```

3. Proseguiamo con le scansioni di OS Fingerprint con il comando `nmap -PR` per l'identificazione delle richieste ARP sul Sistema Operativo in esame:

```
(root@kali)-[/home/kali]
# nmap -PR 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 19:14 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00092s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
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: 08:00:27:0C:68:4A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.57 seconds
```

4. Proseguiamo con le scansioni di OS Fingerprint con il comando `nmap -sS` per effettuare un SYN SCAN, un metodo di Scannerizzazione mono-invasivo che non completa il 3 Way Handshake:

```
(root@kali)-[/home/kali]
# nmap -sS 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 19:16 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00086s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
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: 08:00:27:0C:68:4A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 31.45 seconds
```

5. Proseguiamo con le scansioni di OS Fingerprint con il comando `nmap -sT`, effettua uno scan più invasivo completando il 3 Way Handshake creando il canale di comunicazione:

```
(root@kali)-[/home/kali]
# nmap -sT 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 19:19 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00062s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
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: 08:00:27:0C:68:4A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 15.16 seconds
```