

# EPICODE-CS0124

## S5/L3 - Pratica

Flaviano Sedici

---

### Pratica

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.

---

### 1. Target Metasploitable (192.168.60.101)

#### 1.1. OS Fingerprint

```
(root@kaliArm)-[/home/flaviano]
# nmap -O 192.168.60.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 13:34 CET
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    filtered 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 2.93 seconds
```

Sulla VM di Metasploitable è stato effettuato uno scan per il riconoscimento del SO, che ha restituito il sistema operativo nell'immagine.

## 1.2. Syn Scan

Per effettuare il SYN Scan è stato utilizzato il comando:

***nmap -O -Pn -sS --osscan-limit 192.168.60.101***

```
(root@kaliArm)-[/home/flaviano]
# nmap -O -Pn -sS --osscan-limit 192.168.60.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 13:21 CET
Nmap scan report for 192.168.60.101
Host is up (0.0045s 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    filtered 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 2.96 seconds
```

Si è utilizzato lo switch -sS per completare la richiesta ma è stato deciso di aggiungere anche gli switch -Pn per evitare di utilizzare il ping.

Inoltre è stato ampliato lo switch -O con lo switch --osscan-limit per rilevare eventuale differenze con --osscan-guess (vedi paragrafi successivi).

Lo switch -sS genera meno traffico e quindi ha minore probabilità di essere rilevato.

## 1.3. TCP Connect

Per effettuare il TCP Connect è stato utilizzato il comando:

***nmap -O -Pn -sT --osscan-limit 192.168.60.101***

Si è utilizzato lo switch -sT per completare la richiesta ma è stato deciso di aggiungere anche gli switch -Pn per evitare di utilizzare il ping.

Inoltre è stato ampliato lo switch -O con lo switch --osscan-limit per rilevare eventuale differenze con --osscan-guess (vedi paragrafi successivi).

Come è possibile notare i risultati della scansione sono identici ma il tempo è inferiore di 0,2 secondi rispetto alla scansione effettuata con lo switch -sS, è più invasiva e nello stesso tempo leggermente più veloce con maggiore generazione di traffico (facilmente individuabile).

```
(root@kaliArm)-[/home/flaviano]
# nmap -O -Pn -sT --osscan-limit 192.168.60.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 13:22 CET
Nmap scan report for 192.168.60.101
Host is up (0.0026s 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    filtered 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 2.76 seconds
```

#### 1.4. Version Detection

Per effettuare il Version Detection è stato utilizzato il comando:

***nmap -O -Pn -sV --osscan-limit 192.168.60.101***

Si è utilizzato lo switch -sV per completare la richiesta ma è stato deciso di aggiungere anche gli switch -Pn per evitare di utilizzare il ping.

Inoltre è stato ampliato lo switch -O con lo switch --osscan-guess e in questo caso non è stata rilevata alcuna differenza rispetto alla --osscan-limit.

```
(root@kaliArm)-[/home/flaviano]
# nmap -O -Pn -sV --osscan-guess 192.168.60.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 13:26 CET
Nmap scan report for 192.168.60.101
Host is up (0.0032s latency).
Not shown: 977 closed tcp ports (refused)
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    filtered http
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
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
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 14.65 seconds
```

Come è possibile notare i risultati della scansione oltre che i dati aggiuntivi sul versionamento delle applicazioni collegate alle porte, ma il tempo di scansione è aumentato notevolmente fino a 14,65 secondi.

## 2. Windows 7 (192.168.60.102)

### 2.1. OS Fingerprint (Firewall)

Eseguendo il comando per effettuare il discover del sistema operativo target, il firewall di Windows blocca lo scan di nmap.

Abbiamo inserito il comando -Pn per eludere il blocco del firewall di Windows sul ping.

```
(root@kaliArm)-[/home/flaviano]
# nmap -O -Pn 192.168.60.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 13:28 CET
Stats: 0:00:54 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 53.14% done; ETC: 13:29 (0:00:48 remaining)
```

### 2.2. OS Fingerprint (no Firewall)

Eseguendo lo stesso comando avendo disabilitato il firewall di Windows, nmap restituisce dei risultati in breve tempo 2.95 secondi.

```
(root@kaliArm)-[/home/Flaviano]
# nmap -O -Pn 192.168.60.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 13:29 CET
Nmap scan report for 192.168.60.102
Host is up (0.0034s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
554/tcp    open  rtsp
2869/tcp   open  iclslap
5357/tcp   open  wsdapi
10243/tcp  open  unknown
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7
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 2.95 seconds
```

### 2.3. OS Fingerprint (Firewall) soluzioni alternative

Al fine di aggirare i controlli del firewall di Windows, è stato utilizzato lo switch -T1 per rallentare la frequenza della scansione di nmap in modo che il firewall non cataloghi la scansione come una possibile minaccia.

```
(root@kaliArm)-[/home/flaviano]
# nmap -O -Pn -T1 --osscan-guess -p 135-138 192.168.60.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 13:33 CET
Nmap scan report for 192.168.60.102
Host is up.

PORT      STATE SERVICE
135/tcp    filtered msrpc
136/tcp    filtered msrpc
137/tcp    filtered netbios-ns
138/tcp    filtered netbios-dgm
Too many fingerprints match this host to give specific OS details

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2638.91 seconds
```

Il -Pn è stato aggiunto per evitare di effettuare il ping che normalmente viene bloccato dal firewall di Windows.

L'azione è stata circoscritta alle porte comprese tra la 135 e la 138 in modo da accelerare il processo di ricerca.

Come si evince dal test lo stato delle porte è comunque filtrato (quindi protetto da firewall) e nmap non riesce ad identificare il sistema operativo, oltre che ad impiegare 2.638 secondi.

La **porta 135** riporta comunque il servizio **msrpc** che è legato a **Microsoft Security Event Log** su **protocollo MSRPC** e possiamo quindi ragionevolmente ipotizzare che il sistema operativo sia Windows.

<https://www.ibm.com/docs/it/dsm?topic=options-microsoft-security-event-log-over-msrpc-protocol>