

Pratica S5L3

Andiamo ad effettuare le scansioni tramite nmap di tipo syn scan, tcp scan e Os fingerprint verso la macchina metasploitable con ip 192.168.1.172:

Syn Scan:

```
(luca@kali)-[~/Desktop]
$ sudo nmap 192.168.1.172 -sS
[sudo] password for luca:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:05 CEST
Nmap scan report for 192.168.1.172
Host is up (0.0081s 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: 08:00:27:72:F6:3C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.56 seconds
```

TCP Scan (qui viene effettuato il 3-way handshake completo):

```
(luca@kali)-[~/Desktop]
$ sudo nmap 192.168.1.172 -sT
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:05 CEST
Nmap scan report for 192.168.1.172
Host is up (0.019s 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: 08:00:27:72:F6:3C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

A livello di output non notiamo nessuna differenza, ma sappiamo che la seconda scansione provocherà più rumore all'interno della rete.

Vediamo ora la scansione di tipo OS Fingerprint:

```
(luca@kali) - [~/Desktop]
$ sudo nmap 192.168.1.172 -O
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:10 CEST
Nmap scan report for 192.168.1.172
Host is up (0.0027s 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: 08:00:27:72:F6:3C (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 1.77 seconds
```

Oltre alla informazioni precedenti nmap ci dice che il sistema operativo target è di tipo Linux, e la sua versione dovrebbe risiedere nell'intervallo 2.6.9 – 2.6.33

Andiamo ora a provare le scansioni verso la macchina Windows 7, con ip 192.168.1.109:

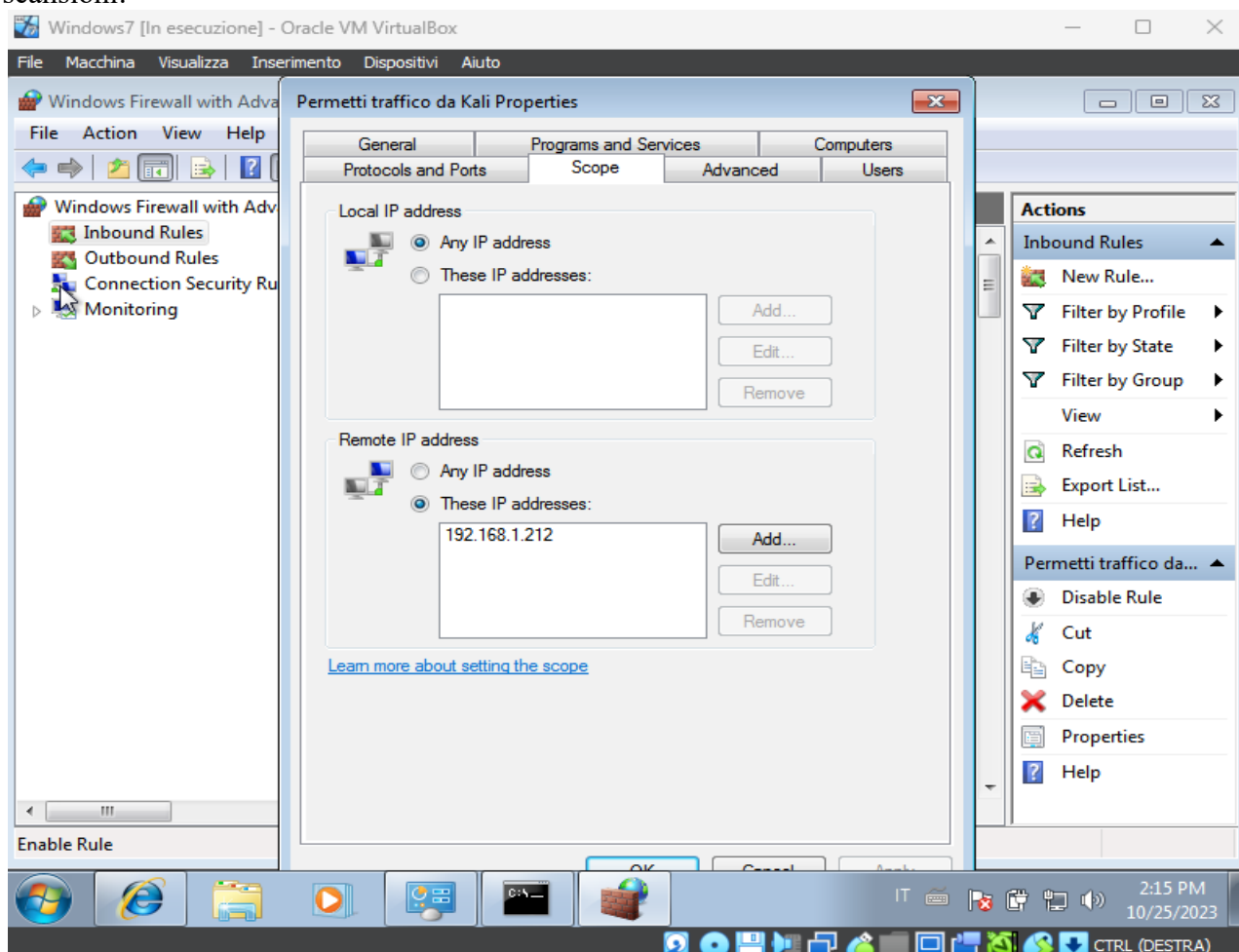
```
(luca@kali)-[~/Desktop]
$ sudo nmap -sS 192.168.1.109
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:14 CEST
Nmap scan report for 192.168.1.109
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.1.109 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:09:7F:E8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 21.49 seconds

(luca@kali)-[~/Desktop]
$ sudo nmap -O 192.168.1.109
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:15 CEST
Nmap scan report for 192.168.1.109
Host is up (0.00084s latency).
All 1000 scanned ports on 192.168.1.109 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:09:7F:E8 (Oracle VirtualBox virtual NIC)
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 24.04 seconds
```

Come vediamo nmap non riceve risposta ai tentativi di SYN nel primo caso, mentre nel secondo ci informa anche che ha rilevato troppe fingerprint diverse per poter stabilire il sistema operativo target. Ricordiamo però che la macchina W7 ha un firewall abilitato di default, quindi andiamo a creare una regola che permetterà il traffico dalla macchina Kali verso quella W7 e riproviamo con le scansioni:



Riproviamo a scansionare, aggiungendo l'opzione -V per andare a recuperare informazioni anche sulla versione dei protocolli corrispondenti alle porte eventualmente aperte:

```
(luca@kali)-[~/Desktop]
$ sudo nmap -sV 192.168.1.109
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:23 CEST
Nmap scan report for 192.168.1.109
Host is up (0.0010s latency).
Not shown: 992 filtered tcp ports (no-response)
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
MAC Address: 08:00:27:09:7F:E8 (Oracle VirtualBox virtual NIC)
Service Info: Host: WINDOWS7; 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 63.25 seconds

(luca@kali)-[~/Desktop]
$ sudo nmap -O 192.168.1.109
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:24 CEST
Nmap scan report for 192.168.1.109
Host is up (0.0015s latency).
Not shown: 992 filtered tcp ports (no-response)
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
MAC Address: 08:00:27:09:7F:E8 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|phone
Running: Microsoft Windows 7|Phone
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0
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 6.51 seconds
```

Notiamo come ora vengano restituite anche diverse informazioni nella colonna “version” nel primo caso, e anche sulla versione del sistema operativo che viene rilevato essere W7. Nel secondo caso, con l'opzione -O, nel campo **OS Details** vengono restituite più possibilità in quanto le fingerprint probabilmente sono comuni anche ai sistemi Windows Phone 7.5 e 8.0

Infine, eseguiamo anche la scansione con opzione -V verso la macchina Metasploitable:

```
(luca@kali)~[~/Desktop]
$ sudo nmap 192.168.1.172 -sV
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:30 CEST
Nmap scan report for 192.168.1.172
Host is up (0.0055s 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  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
MAC Address: 08:00:27:F6:3C (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 12.15 seconds
```

Anche in questo caso nella colonna version possiamo recuperare più informazioni, spesso anche la versione supportata dal protocollo (es. ftp 2.3.4).