Esercizio S5/L3 di Ciaschini Giorgio del 21/02/2024

Come si evince dallo screen-shot siamo andati a fare un OS fingerprint verso l'indirizzo ip 192.168.49.101 appartenente alla macchina Metasploitable. Si nota che il sistema operativo utilizzato è Linux con versione tra la 2.6.15 e la 2.6.26.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:18 EST
Nmap scan report for 192.168.49.101
Host is up (0.0025s 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), Linux 2.6.20 - 2.6.24 (Ubuntu 7.04 - 8.04)
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 3.13 seconds
```

In quest'altro invece grazie al comando "-sS" abbiamo visto quali sono le porte aperte. Da notare che questo comando non restituisce un "Three-way-Handshake" ma restituisce come ultima risposta un reset.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:13 EST
Nmap scan report for 192.168.49.101
Host is up (0.0020s 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

Nmap done: 1 IP address (1 host up) scanned in 1.50 seconds
```

Successivamente si è effettuato un TCP connect dove possiamo notare, che a differenza del SYN oltre alla differenza del tempo di esecuzione non compaiono grosse disuguaglianze.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:14 EST
Nmap scan report for 192.168.49.101
Host is up (0.0053s 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

Nmap done: 1 IP address (1 host up) scanned in 1.30 seconds
```

Con la “Version detection” siamo andati a studiare la tipologia di servizio

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:16 EST
Nmap scan report for 192.168.49.101
Host is up (0.0011s 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   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?
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     ccproxy-ftp?
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; 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 174.19 seconds
```

Sul target Windows 7 abbiamo come OS fingerprint due diversi risultati scaturiti, il primo con il firewall attivo e il secondo togliendo tutte le difese della macchina Windows 7.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.50.102 -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 11:02 EST
Nmap scan report for 192.168.50.102
Host is up (0.012s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:8B:3F:23 (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 34.06 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.50.102 -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 11:04 EST
Nmap scan report for 192.168.50.102
Host is up (0.00074s 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  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49161/tcp open  unknown
MAC Address: 08:00:27:8B:3F:23 (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_server_2
008::sp1 cpe:/o:microsoft:windows_server_2008:r2 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 16.04 seconds
```

Sulla macchina Windows7 abbiamo visto che con il firewall attivo le informazioni non vengono rilasciate. Una soluzione a questo potrebbe essere utilizzare un'altra tecnica per carpire altre informazioni come ad esempio con il comando "--osscan-guess"

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --osscan-guess 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 11:57 EST
Nmap scan report for 192.168.50.102
Host is up (0.00082s 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: 08:00:27:8B:3F:23 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.91 seconds
```

Altrimenti esistono anche altri metodi di evasione dei firewall come il comand "-f".

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -f 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 12:01 EST
Nmap scan report for 192.168.50.102
Host is up (0.00038s 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: 08:00:27:8B:3F:23 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.53 seconds
```