

REPORT S5/L2

Si richiede di effettuare le seguenti scansioni sul target Metasploitable:

- OS Fingerprint
- Syn Scan
- TCP Connect
- Version Detection

E la sequent sul target Windows

- Os Fingerprint

Per prima cosa si procede con la scansione per determinare il sistema operativo del primo target, in questo caso la vm Metasploitable, da kali quindi con il comando “**nmap -O**” si tenta di determinare il sistema operativo dell’ host di destinazione. **Figura 1**

```
(kali@kali)-[~]
$ sudo nmap -O 192.168.1.3
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 14:29 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is d
isabled. Try using --system-dns or specify valid servers with --dns-serv
ers
Nmap scan report for 192.168.1.3
Host is up (0.00024s 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: 08:00:27:85:8A:68 (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
```

Figura 1, mediante nmap -O viene determinato il sistema operativo del target.

In questo caso si evidenzia come in seguito alla scansione emerge che il sistema operativo in questione è *Linux* ed in particolare una versione dalla 2.6.9 alla 2.6.33.

Il passo successivo è quello della SYN scan, questa è una scansione “half-open” si invia un SYN al target e si aspetta il SYN/ACK di risposta, la si esegue mediante il comando “**nmap -sS ip-target**”. **Figura 2**

```

(kali@kali)-[~]
$ sudo nmap -sS 192.168.1.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 14:41 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or speci
fy valid servers with --dns-servers
Nmap scan report for 192.168.1.3
Host is up (0.000065s 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: 08:00:27:85:8A:68 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds

```

Figura 2, SYN scan effettuato sull'host METASPLOITABLE.

In questo caso invece, dalla SYN scan, si otterrà come risultato la lista delle porte tcp aperte sull'host. Si procede ora con TCP Connect per evidenziare eventuali differenze, in questo caso a differenza del caso precedente si stabiliranno delle connessioni complete ma con il medesimo risultato. **Figura 3**

```

(kali@kali)-[~]
$ sudo nmap -sT 192.168.1.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 14:49 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or speci
fy valid servers with --dns-servers
Nmap scan report for 192.168.1.3
Host is up (0.00061s 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: 08:00:27:85:8A:68 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds

```

Figura 3, dalla TCP Connect è evidente come il risultato sia lo stesso del caso precedente.

Si procede infine con la **Version detection** del target, lo scopo di quella scansione è quello di identificare i servizi attivi sull'host e le loro versioni, il comando è "**nmap -sV**". **Figura 4**

```

$ sudo nmap -sV 192.168.1.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 14:55 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 14:56 (0:00:02 remaining)
Nmap scan report for 192.168.1.3
Host is up (0.00028s 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-ssr  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssr  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell
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: 08:00:27:85:8A:68 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

```

Figura 4, dal version detection emergono le versioni dei singoli servizi attivi sul target.

Si procede infine andando a scansionare la vm Windows, identificando il sistema operativo in questione. Come avvenuto nel caso precedente il comando da utilizzare sarà "**nmap -O**". **Figura 5**

```

(kali@kali) ~
$ sudo nmap -O 192.168.1.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 15:16 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.15
Host is up (0.00021s 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: 08:00:27:9A:F3:B7 (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_2008::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

```

Figura 5, scansione sistema operativo sull'host Windows 7.

La scansione in questo caso è stata possibile solo dopo aver disabilitato manualmente il firewall di Windows.