## Report

L'esercizio richiede di fare delle scansioni.

Come richiesto sono state eseguite le scansioni sul target Metasploitable.

Con il comando nmap -O, questo ci permette di stimare il sistema operativo del target.

```
)-[/usr/share/nmap/scripts]
    nmap -0 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 16:36 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0014s latency).
Not shown: 977 closed tcp ports (reset)
PORT
          STATE SERVICE
         open ftp
open ssh
open telnet
21/tcp
22/tcp
23/tcp
         open smtp
25/tcp
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: 16:FE:53:6E:26:5A (Unknown)
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 14.75 seconds
```

# Syn Scan

Con il comando sS di nmap andiamo a fare un scansione poco invasiva sul target segue una scansione Syn che non va a chiudere il 3 way handshake.

```
| kali)-[/usr/share/nmap/scripts]
    nmap -sS 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 16:44 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00092s 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
                                                 Ī
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 16:FE:53:6E:26:5A (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
```

### **TPC Connect**

Con il comando sT di nmap andiamo a fare un scansioneinvasiva sul target segue una scansione completa sul tcp eseguendo il 3 way handshake.

```
kali)-[/usr/share/nmap/scripts]
 -# nmap -sT 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 16:46 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0030s latency).
Not shown: 977 closed tcp ports (conn-refused)
        STATE SERVICE
PORT
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: 16:FE:53:6E:26:5A (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 13.21 seconds
```

### **Version Detection**

Con il comando sV di nmap andiamo a fare un scansione molto invasiva sul target simile a quella che fa sT, ma con l'aggiunta di test specifici che rilevano i servizi in ascolto su un target.

```
)-[/usr/share/nmap/scripts]
       nmap -sV 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 16:48 CEST
 Nmap scan report for 192.168.50.101
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
                                            VERSION
PORT
              STATE SERVICE
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 exec netkit-rsh rexecd
512/tcp open exec
513/tcp open login?
514/tcp open shell
                                               netkit-rsh rexecd
514/tcp open togin;
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 ync VNC (protocol 3.3)
                          vnc VNC (protocol 3.3)
X11 (access denied)
5900/tcp open
6000/tcp open X11
                                               UnrealIRCd
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
                                               Apache Jserv (Protocol v1.3)
MAC Address: 16:FE:53:6E:26:5A (Unknown)
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 186.98 seconds
```

### Scansioni su Windows 7

Le non hanno riportato nessuna risposta. Scansione con il comando nmap -O:

```
(root@kali)-[/usr/share/nmap/scripts]
# nmap -0 192.168.50.102

Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 18:18 CEST

Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn

Nmap done: 1 IP address (0 hosts up) scanned in 1.74 seconds
```

Scansione con il comando nmap -Pn -O, si usa per un host ch'è attivo ma che non risponde al ping.

```
(root@kali)-[/usr/share/nmap/scripts]
# nmap -Pn -0 192.168.50.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 18:19 CEST
Nmap done: 1 IP address (0 hosts up) scanned in 1.72 seconds
```

Scansione con il comando nmap -sS:

```
(root@kali)-[/usr/share/nmap/scripts]
# nmap -sS 192.168.50.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 18:32 CEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.55 seconds

(root@kali)-[/usr/share/nmap/scripts]
# nmap -Pn -sS 192.168.50.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 18:32 CEST
Nmap done: 1 IP address (0 hosts up) scanned in 1.54 seconds
```

Scansione con il comando nmap -sT:

```
(root@ kall)-[/usr/share/nmap/scripts]
// nmap -sT 192.168.50.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 18:35 CEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.56 seconds

(root@ kall)-[/usr/share/nmap/scripts]
// nmap -Pn -sT 192.168.50.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 18:35 CEST
Nmap scan report for 192.168.50.102
Host is up (0.045s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 990 filtered __cp ports (no-response), 10 filtered tcp ports (host-unreach)

Nmap done: 1 IP address (1 host up) scanned in 19.00 seconds
```

Scansione con il comando nmap -sV:

```
(root@kali)-[/usr/share/nmap/scripts]
# nmap -sV 192.168.50.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 18:37 CEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.76 seconds

(root@kali)-[/usr/share/nmap/scripts]
# nmap -Pn -sV 192.168.50.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 18:37 CEST
Nmap done: 1 IP address (0 hosts up) scanned in 1.66 seconds
```