

relazione S5L2

L'esercizio di oggi consisteva nell'utilizzo delle varie funzioni di nmap.

```
(kali㉿kali)-[~]
$ sudo nmap -O 192.168.178.46
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 08:34 EDT
Nmap scan report for 192.168.178.46
Host is up (0.00026s 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: 08:00:27:77:F7:96 (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 1.48 seconds

(kali㉿kali)-[~]
$
```

In questa prima immagine ho usato la funzione -O ovvero l'os fingerprint. L'os fingerprint è una tecnica utilizzata per identificare, inviando pacchetti specifici e analizzando le risposte, di identificare un sistema operativo in esecuzione su un dispositivo di rete.

```
(kali@kali)-[~]
$ sudo nmap -sS 192.168.178.46
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 08:36 EDT
Nmap scan report for 192.168.178.46
Host is up (0.000040s 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: 08:00:27:77:F7:96 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds

(kali@kali)-[~]
$
```

In questa seconda immagine ho utilizzato come da esercizio il comando -sS ovvero il SYN scanner. Il syn scanner di nmap è una tecnica di scansione delle porte mediante l'invio di pacchetti syn per determinare lo stato delle porte di un determinato host.

```
(kali@kali)-[~]
$ sudo nmap -sT 192.168.178.46
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 08:37 EDT
Nmap scan report for 192.168.178.46
Host is up (0.00012s 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: 08:00:27:77:F7:96 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds

(kali@kali)-[~]
$
```

In questa terza immagine ho usato il comando `-sT` ovvero il comando inerente al TCP connect. Come possiamo notare il risultato è il medesimo del Syn scanner perchè ciò che lo contraddistingue dal Syn scanner è che a differenza di esso il TCP connect esegue tutti i passaggi di stretta di mano . Ciò lo rende meno furtivo del Syn scanner.

```

(kali@kali)-[~]
$ sudo nmap -sV 192.168.178.46
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 08:38 EDT
Stats: 0:00:22 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 08:39 (0:00:01 remaining)
Nmap scan report for 192.168.178.46
Host is up (0.00012s 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?
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
MAC Address: 08:00:27:77:F7:96 (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 63.42 seconds

```

In quest'ultima immagine ho utilizzato il comando `-sV` corrispondente alla funzione di Version Detector di nmap. Il Version Detector di nmap è una tecnica che, mediante l'invio di specifici pacchetti e analizzando le risposte ricevute dal target, riesce a determinare i tipi e le versioni dei servizi in esecuzione nelle varie porte aperte di un host.