

Nel compito odierno era richiesto di eseguire delle scansioni di tipologie differenti tramite l'ausilio del programma nmap.

Sono state eseguite scansioni di 4 tipo per l'esattezza, sulla macchina vulnerabile metasploitable 2, per rilevare il SO fingerprint, una scansione tramite l'invio di un pacchetto SYN, una in cui è stato effettuato il Three Ways Handshake, ed un'ultima per verificare le versioni dei protocolli disponibile sulla macchina attaccata.

```
Nmap scan report for 192.168.178.28
Host is up (0.00018s 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: 08:00:27:7F:97:4E (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

Nmap scan report for kali.fritz.box (192.168.178.27)
Host is up (0.000027s latency).
All 1000 scanned ports on kali.fritz.box (192.168.178.27) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 72.04 seconds

(kali㉿kali)-[~]
└─$
```

In primo luogo è stato eseguito il comando `nmap -O 192.168.178.28/24` (Indirizzo IP della macchina bersaglio) che ci ha consentito di eseguire uno scan in range 192.168.178.1 fino a 192.168.178.255, ciò perché nel comando è stata anche inserita la CIDR. Il risultato è stato una scansione dei dispositivi presenti nel range, tra cui la nostra macchina vittima, sulla quale è stato possibile verificare che il SO presente Linux 2.6.x

```
└─$ sudo nmap -sS 192.168.178.28
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 11:20 EDT
Nmap scan report for 192.168.178.28
Host is up (0.000081s 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: 08:00:27:7F:97:4E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

```
(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.178.28
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 11:21 EDT
Nmap scan report for 192.168.178.28
Host is up (0.00037s 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
```

In seguito, il secondo comando eseguito è stato `nmap -sS` il quale invierà soltanto un pacchetto SYN, senza quindi proseguire con la Three Ways Handshake, che come risultato ha fornito tutte le porte aperte, specificando che le restanti 977 sono chiuse al protocollo TCP.

Subito dopo con il comando `nmap -sT` è stata fatta la stessa verifica, ma questa volta la TWH è avvenuta con successo tramite il SYN/SYN ACK/ACK, mostrando risultati piuttosto simili, specificando però che le 977 porte chiuse anziché “reset” hanno mostrato come risposta “conn-refused”.

```

(kali@kali)-[~]
$ sudo nmap -sV 192.168.178.28
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 11:23 EDT
Nmap scan report for 192.168.178.28
Host is up (0.000093s 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
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: 08:00:27:7F:97:4E (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 64.81 seconds

```

L'ultimo comando inserito tramite il programma nmap è stato `nmap -sV`, il quale identifica e ci mostra tutte le versioni delle porte in ascolto, le porte aperte, informazioni molto importanti in caso di attacco alla macchina vulnerabile.

In seguito allo scan di metasploitable 2, è stato anche effettuato un controllo tramite il comando `sudo nmap -O` su una macchina con SO windows 10. Esso ha confermato il SO peso

```

kali@kali: ~
$ sudo nmap -O 192.168.178.29
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 12:02 EDT
Nmap scan report for DESKTOP-9K104BT.fritz.box (192.168.178.29)
Host is up (0.00025s latency).
Not shown: 981 closed tcp ports (reset)
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
2869/tcp  open  iclslap
3389/tcp  open  ms-wbt-server
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
MAC Address: 08:00:27:60:6F:E6 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Microsoft Windows 10 10586 - 14393 (98%), Microsoft Windows 10 1507 - 1607 (98%), Microsoft Server 2008 R2 SP1 (98%), Microsoft Windows Server 2016 build 10586 - 14393 (95%), Microsoft Windows 7 Professional (95%), Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1 (95%), Microsoft Windows 7 Ultimate (95%), Microsoft Windows 7 or 8.1 R1 or Server 2008 R2 SP1 (95%), Microsoft Windows 10 1703 (95%), Microsoft Windows 7 or Windows Server 2008 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

```

nate.