Esercitazione nmap

1. Target Metasploitable2 (**192.168.50.10**)

- OS fingerprinting:

  Utilizzando il comando **-O** sulla macchina metasploitable2, oltre a vedere eventuali porte aperte, si trovano informazioni riguardanti il sistema operativo in uso sulla macchina bersaglio

```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.50.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 07:53 EDT
Nmap scan report for 192.168.50.10
Host is up (0.00037s 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:CF:CA:E8 (PCS Systemtechnik/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
```

  Il risultato della scansione ci dà come sistema operativo Linux 2.6.x con dettaglio di versione tra la 2.6.9 e la 2.6.33

- Syn Scan:

  Con il comando **-sS** sulla macchina bersaglio inizializzo un Syn Scan, nel quale Nmap non completerà il 3-way-handshake con la macchina bersaglio, riuscendo comunque a recuperare informazioni sullo stato delle porte.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.50.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:01 EDT
Nmap scan report for 192.168.50.10
Host is up (0.00011s 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:CF:CA:E8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.56 seconds
```

  Il risultato della scansione ci mostra tutte le porte che hanno risposto all'inizio del 3-way-handshakes e che quindi sono aperte. Nel risultato troviamo varie porte, tra cui la 21 e la 80 aperte le quali sono poco sicure.

- TCP connect:

  La connessione tramite TCP connect si differenzia dal SYN Scan perché in questo tipo di scansione il 3-way-handshake viene completato.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.50.10

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:16 EDT
Nmap scan report for 192.168.50.10
Host is up (0.00047s 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:CF:CA:E8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds
```

  Questa scansione ha come output lo stesso del SYN Scan; infatti, notiamo le stesse porte in entrambe le scansioni. L'unica differenza che c'è sta nel motivo con cui vengono trovate le porte chiuse, ovvero in questa scansione abbiamo il messaggio "**Not shown: 977 closed tcp ports (conn-refused)**" mentre nella scansione SYN abbiamo "**Not shown: 977 closed tcp ports (reset)**". La differenza è dovuta dal fatto che nella scansione SYN troviamo delle porte chiuse quando in risposta al pacchetto SYN riceviamo dalla porta bersaglio il pacchetto RST (reset). Mentre nella scansione TCP connect, dopo il tentativo di stabilire la connessione TCP completa, riceve come messaggio il Connection Refused.

- Version Detection:

  Utilizziamo il comando nmap -sV sull'ip bersaglio, verranno mandati dei pacchetti che, in base alle risposte ottenute, possono identificare il servizio con la versione corrispondente.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:33 EDT
Nmap scan report for 192.168.50.10
Host is up (0.000082s 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        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  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:CF:CA:E8 (PCS Systemtechnik/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 65.52 seconds
```

  L'output ci mostra tutti i servizi e la relativa versione.

2. Target Windows 10 (**192.168.50.20**)
   - OS fingerprinting:

```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.50.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:56 EDT
Nmap scan report for 192.168.50.20
Host is up (0.00033s latency).
Not shown: 982 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
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: 08:00:27:94:14:74 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Microsoft Windows 10 1507 - 1607 (98%), Microsoft Windows 10 1511 - 1607 (98%), Microsoft Windows Server 2008 R2 SP1 (98%), Microsoft Windows 10 (95%), Microsoft Windows Vista SP2 or Windows 7 or
 Windows Server 2008 R2 or Windows 8.1 (95%), Microsoft Windows Server 2016 or Server 2019 (95%), Microsoft Windows 7 Professional (95%), Microsoft Windows 7 Ultimate (95%), Microsoft Windows 7 or 8.1 R1 or Ser
ver 2008 R2 SP1 (95%), Microsoft Windows 10 1703 or Windows 11 21H2 (95%)
No exact OS matches for host (test conditions non-ideal).
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 28.62 seconds
```

In questo caso. effettuando l'OS fingerprinting sulla macchina Windows, otteniamo delle **Aggressive OS guesses**, ovvero delle stime sul sistema operativo con relativa percentuale di accuratezza. Succede questo perché non si è trovata una corrispondenza al 100% per il sistema operativo del target.