

# Report 29 Aprile

In questa esercitazione andremo a raccogliere informazioni tramite delle scansioni con nmap. In particolare

Scansioni con target

## Metasploitable:

- OS fingerprint
- Syn Scan.
- TCP connect.
- Version detection.

E la seguente con target Windows:

- OS fingerprint.

Andiamo ad eseguire il comando: **nmap -O 192.168.1.10**, utilizzando l'IP della macchina target. Questo comando ci permette di rilevare il sistema operativo (e quale versione) è in esecuzione sul nostro target.

```
valid_lft forever preferred_lft forever
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:df:56:46 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.10/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fedf:5646/64 scope link
    valid_lft forever preferred_lft forever
sfadmin@metasploitable:~$
```

Quello che otteniamo è una sfilza di informazioni molto utili, come il MAC address, le porte aperte, ma soprattutto il **sistema operativo** dalla macchina target.

```

(kali@kali)-[~]
$ nmap -O 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 09:20 EDT
Nmap scan report for METASPLOITABLE.station (192.168.1.10)
Host is up (0.00027s 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:DF:56:46 (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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.11 seconds

```

Ora procediamo allo stesso modo con windows.

```

Scheda Ethernet Ethernet:

Suffisso DNS specifico per connessione: station
Indirizzo IPv6 locale rispetto al collegamento . : fe80::18e1:bae7:33a6:a5d6%4
Indirizzo IPv4. . . . . : 192.168.1.11
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.1.1

```

Come possiamo notare in “Running” troviamo stampato **Windows 10**, mentre nello screen precedente troviamo “**Linux 2.6.X**”

```

(kali@kali)-[~]
$ nmap -O 192.168.1.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 09:30 EDT
Nmap scan report for DESKTOP-9K104BT.station (192.168.1.11)
Host is up (0.00022s 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
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdisapi
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
MAC Address: 08:00:27:37:43:AB (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
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 16.54 seconds

```

Ora per il secondo punto del nostro esercizio, andiamo a fare una scansione tramite il comando: **nmap -sS 192.168.1.10** (da qui il nostro target sarà sempre **Metasploitable**). La -sS permette di vedere le porte aperte, e utilizza pacchetti **SYN** e attende una risposta **SYN/ACK** per vedere quali porte sono aperte. E' una **scansione Stealth** poiché non stabilisce una connessione completa, rendendo meno probabile che venga rilevata dal firewall.

```
(kali㉿kali)-[~]
$ nmap -sS 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 09:46 EDT
Nmap scan report for METASPLOITABLE.station (192.168.1.10)
Host is up (0.000087s 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:DF:56:46 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

Per il terzo punto andiamo a fare una scansione tramite il comando: **nmap -sT 192.168.1.10**. Questo comando utilizza la chiamata di sistema **connect()** per stabilire una connessione TCP completa a ciascuna porta di destinazione.

```
(kali㉿kali)-[~]
$ nmap -sT 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 10:13 EDT
Nmap scan report for METASPLOITABLE.station (192.168.1.10)
Host is up (0.00043s 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:DF:56:46 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

La differenza tra **-sS** e **-sT** la notiamo nella riga 4 di entrambi i codici: in **-sS** troviamo “Not shown 977 closed tcp ports (**reset**)”, mentre in **-sT** alla riga 4 del comando notiamo che alla fine è scritto (**conn-refused**), questo perche “**SYN scan**” invia un pacchetto RST di risposta per terminare la connessione, senza completare l’hand-shacke, **mentre “-TCP connect scan”** stabilisce una connessione TCP completa, completando l’handshake

A differenza di **-sS**, **-sT** è meno “**stealth**”, perché stabilisce connessioni complete, ma è utile in ambienti in cui lo stealth non è una preoccupazione.

Per l'ultimo punto andiamo ad utilizzare il comando: **nmap -sV 192.168.1.10**. Questo comando ci permette di eseguire la rilevazione della versione dei servizi in esecuzione sulle porte aperte.

```
(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 10:44 EDT
Nmap scan report for METASPLOITABLE.station (192.168.1.10)
Host is up (0.00016s 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:DF:56:46 (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 64.75 seconds
```

Notiamo infatti accanto alle porte aperte lo loro relativa versione, eccetto per le porte 512 e 514