Report 29 Aprile

In questa esercitazione andremo a raccogliere informazion trami delle scansioni con nmap. In particolare

Scansioni con target

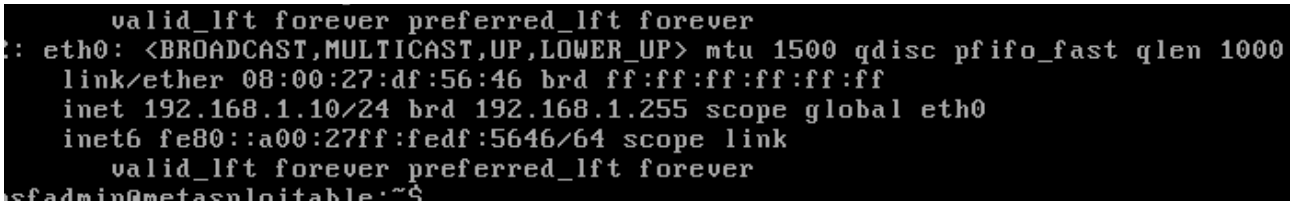
Metasploitable:

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

E la seguente con target Windows:

- OS fingerprint.

Andimo 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.



Quello che otteniamo e una sfilza di informazioni molto utili, come il MAC addres, 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
```

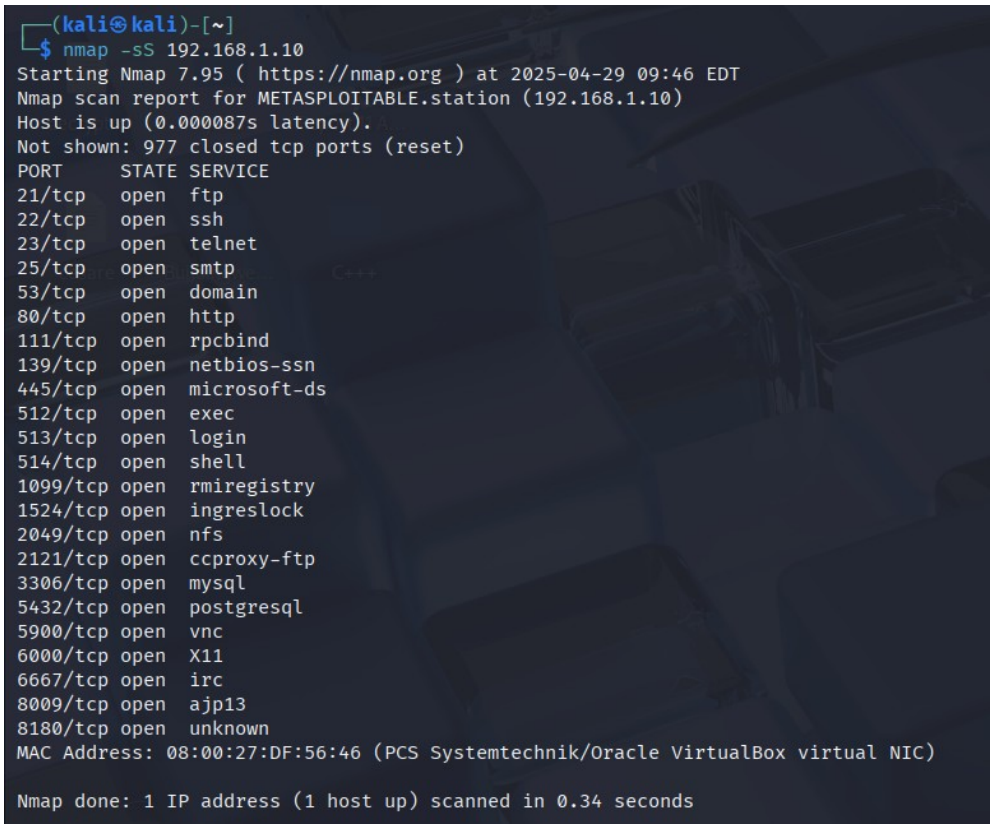
Ora procediamo allo stesso modo con windows.

```
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
```

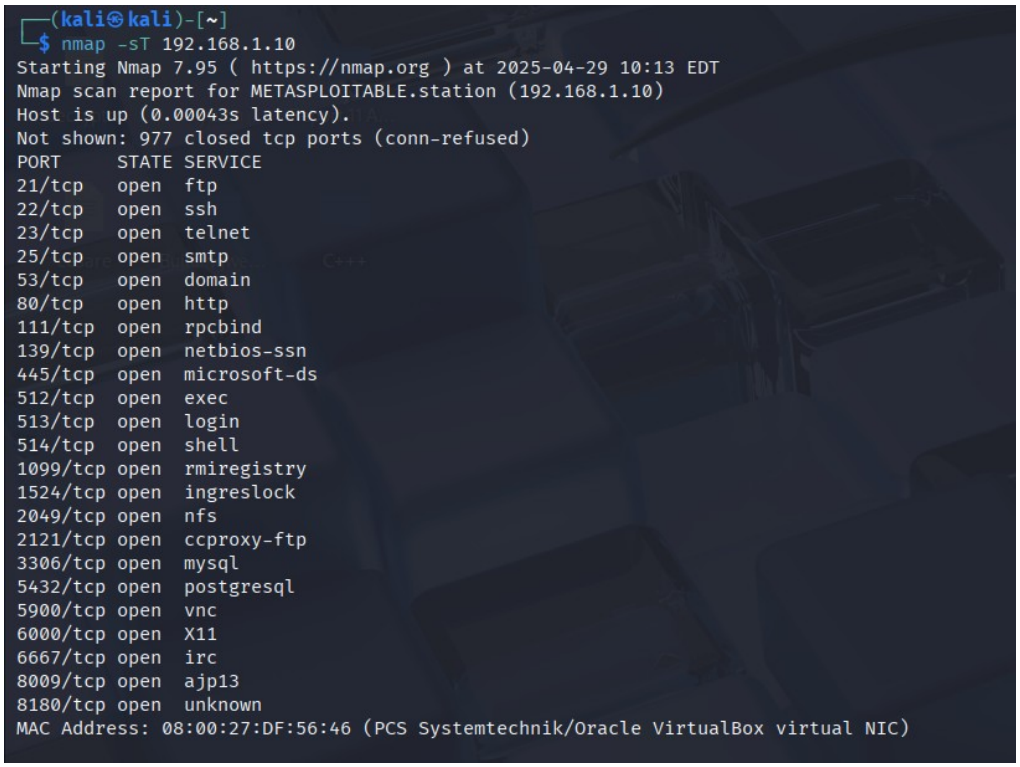
Come possiamo notare in “Running” troviamo stampato **Windows 10,** mentre nello screen precedente troviamo **“Linux 2.6.X”**

```
┌──(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-9K1O4BT.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  wsdapi
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 **scansioni Stealth** poiché non stabilisce una connessione completa, rendendo meno probabile che venga rilevata dal firewall.



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.



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’handshacke

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.

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