

# ESERCIZIO

## Traccia: Tecniche di scansione con Nmap

Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

- OS fingerprint;
- Syn Scan;
- TCP connect (trovate le differenze tra TCP connect e Syn Scan);
- Version detection

E la seguente sul target Windows:

- OS fingerprint.

Prima di cominciare l'esercizio dovremo assicurarci che il nostro laboratorio sia configurato correttamente. Avremo bisogno delle VM Kali, Metasploitable2 e Windows7 su delle reti interne. Per far questo utilizzeremo Pfsense (che ha funzioni sia router che firewall) e con il quale simuleremo schede di rete aggiuntive.

```
2 - LAN (vtnet0 - static)
3 - OPT1 (vtnet1 - static)
4 - OPT2 (vtnet2 - static)

Enter the number of the interface you wish to configure:
VirtualBox Virtual Machine - Netgate Device ID: 53d22ad2111215aaabe9

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.194/24
LAN (lan)      -> vtnet0    -> v4: 192.168.10.1/24
OPT1 (opt1)    -> vtnet1    -> v4: 192.168.20.1/24
OPT2 (opt2)    -> vtnet2    -> v4: 192.168.30.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system             14) Enable Secure Shell (sshd)
6) Halt system               15) Restore recent configuration
7) Ping host                 16) Restart PHP-FPM
8) Shell

Enter an option: █
```

Come possiamo vedere dall'immagine, abbiamo creato 3 Vlan, che andremo ad assegnare rispettivamente alla Kali, a Metasploitable 2 e Windows 7. Utilizzeremo degli indirizzi IP statici.

```
msfadmin@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.10.101 netmask 255.255.255.0 broadcast 192.168.10.255
    inet6 fe80::9df4:251b:82eb:5ab6 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:04:42:0f txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 22 bytes 2760 (2.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

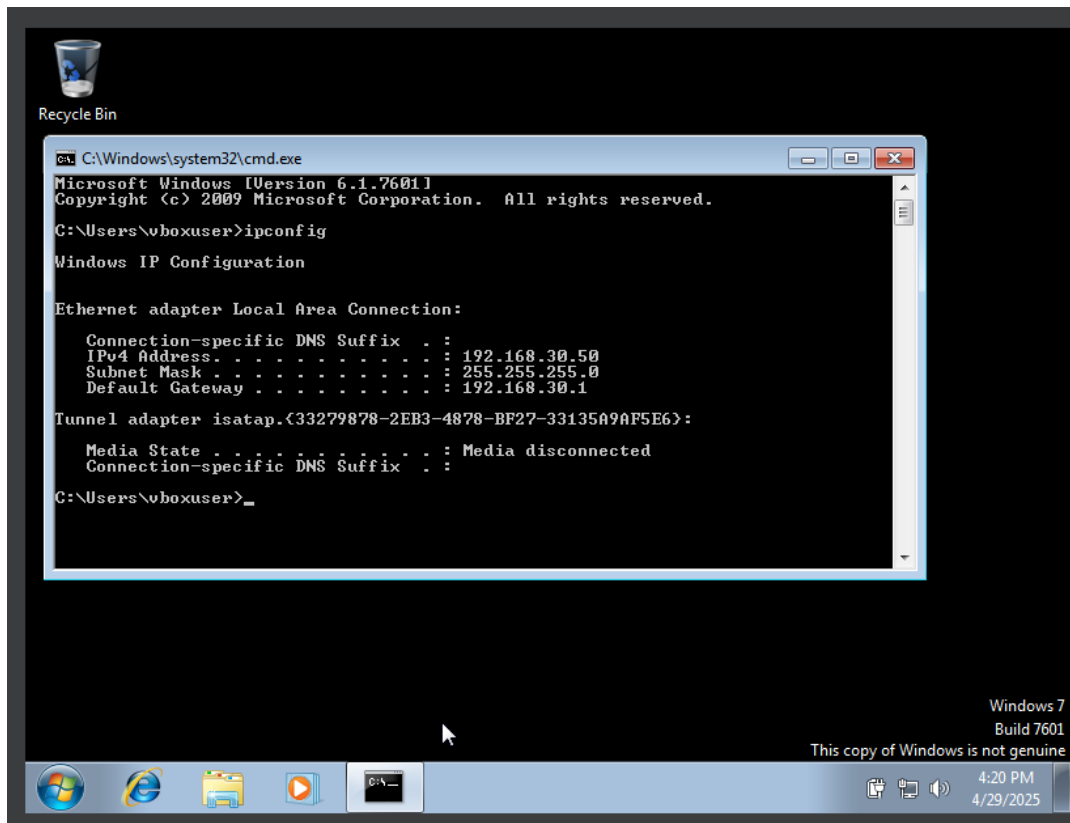
Nell'immagine sopra vediamo l'IP assegnato alla Kali.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:82:19:ea
          inet addr:192.168.20.50 Bcast:192.168.20.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe82:19ea/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:31044 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29483 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3053494 (2.9 MB)  TX bytes:13226312 (12.6 MB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:556 errors:0 dropped:0 overruns:0 frame:0
          TX packets:556 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:231017 (225.6 KB)  TX bytes:231017 (225.6 KB)

msfadmin@metasploitable:~$
```

Nell'immagine sopra vediamo l'IP assegnato alla Metasploitable2.



Nell'immagine sopra vediamo l'IP assegnato a Windows 7.

Una volta impostato il nostro laboratorio correttamente possiamo verificare che sia funzionante mandando dei ping dalla Kali a Metasploitable 2 e Windows 7.

Se riceveremo risposta ai ping vorrà dire che la configurazione è stata effettuata correttamente.

A questo punto possiamo procedere a fare le scansioni con nmap richieste dalla traccia.

```
(kali@kali)-[~]
$ nmap -O 192.168.20.50
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 08:29 EDT
Nmap scan report for 192.168.20.50
Host is up (0.013s 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    filtered 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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.30 seconds
```

nmap -O 192.168.20.50 --> oltre le porte aperte, ci restituisce il SO utilizzato dalla Metasploitable 2.

```
(kali㉿kali)-[~]  
$ nmap -sS 192.168.20.50  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 08:36 EDT  
Nmap scan report for 192.168.20.50  
Host is up (0.012s 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    filtered  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  
  
Nmap done: 1 IP address (1 host up) scanned in 3.06 seconds
```

nmap -sS 192.168.20.50 --> ci permette di vedere i servizi in esecuzione sull'host.

```
(kali㉿kali)-[~]  
$ nmap -sT 192.168.20.50  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 08:39 EDT  
Nmap scan report for 192.168.20.50  
Host is up (0.0096s 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    filtered   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  
  
Nmap done: 1 IP address (1 host up) scanned in 2.02 seconds
```

nmap -sT 192.168.20.50 --> ci restituisce lo stesso risultato visto in precedenza.

La differenza tra nmap -sS e -sT non è nel risultato che otteniamo. La differenza consiste nella modalità in cui vengono effettuate le due scansioni.

sT: è il metodo di scansione più invasivo, in quanto per controllare se una porta è aperta o meno e recuperare informazioni sul servizio in ascolto, nmap completa tutti i passaggi del 3 way handshake, stabilendo di fatto un canale.

ss: è un metodo meno invasivo, in quanto nmap, una volta ricevuto il pacchetto SYN/ACK dalla macchina target, non conclude il 3 way handshake, ma appurato che la porta è aperta chiude la comunicazione, evitando overload dato dalla creazione del canale.

```
(kali@kali)-[~]
$ nmap -sV 192.168.20.50
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 08:42 EDT
Nmap scan report for 192.168.20.50
Host is up (0.0040s 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    filtered http
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        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
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 14.45 seconds
```

nmap -sV 192.168.20.50 --> identifica i servizi in esecuzione e le loro versioni.

Infine, per quanto riguarda Windows7:

```
(kali@kali)-[~]
$ nmap -O 192.168.30.50
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 10:14 EDT
Nmap scan report for 192.168.30.50
Host is up (0.0046s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
Device type: general purpose
Running: Microsoft Windows 2008/7/Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista:: cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows 7 or Windows Server 2008 R2, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.62 seconds
```

`nmap -O 192.168.30.50` --> oltre le porte aperte, ci restituisce il SO in uso, in questo caso Windows 7.