

PRATICA M2/S1/L2
CS0225IT
MIRKO GERIA



Introduzione

L'esercizio di oggi ci chiede:

Traccia: Tecniche di scansione con Nmap

Si richiede allo studente di effettuare le seguenti scansioni sul target

Metasploitable:

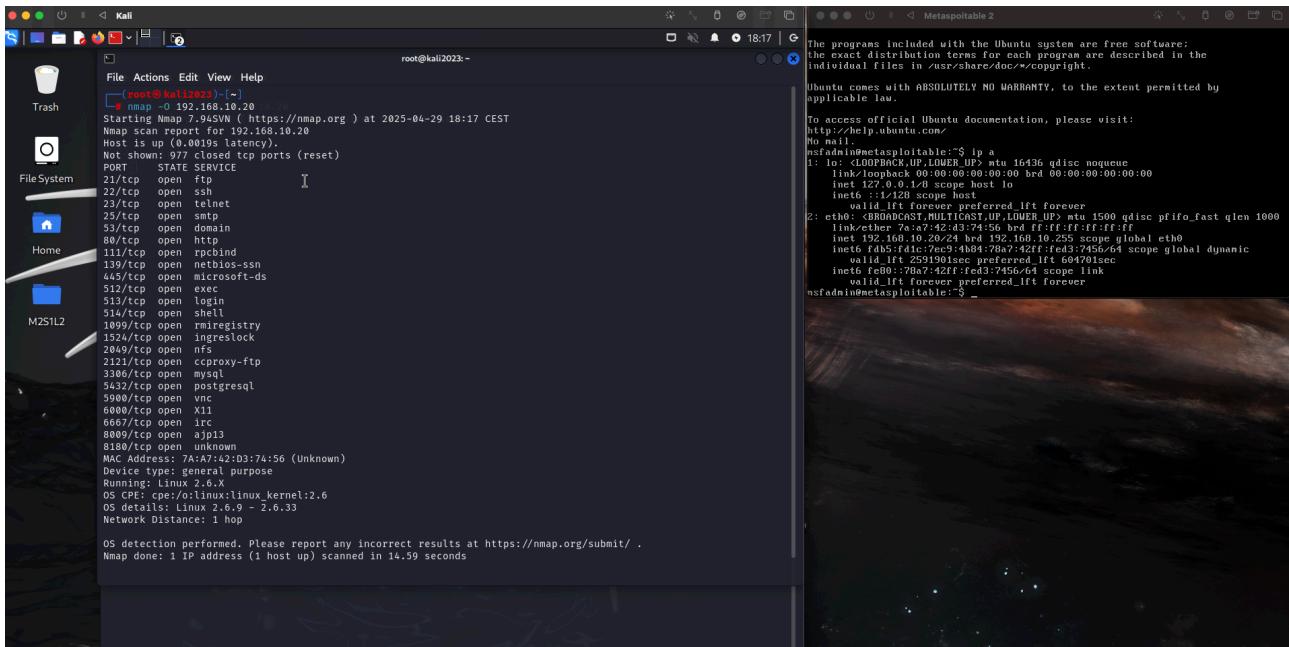
- OS fingerprint.
- Syn Scan.
- TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?
- Version detection.

E la seguente sul target Windows:

- OS fingerprint.

Descrizione del procedimento

Usiamo Kali linux 192.168.10.10 per eseguire la scansione OS su metasploitable 192.168.10.20 con il comando ‘sudo nmap -O 192.168.10.20’ e avremo questo risultato:

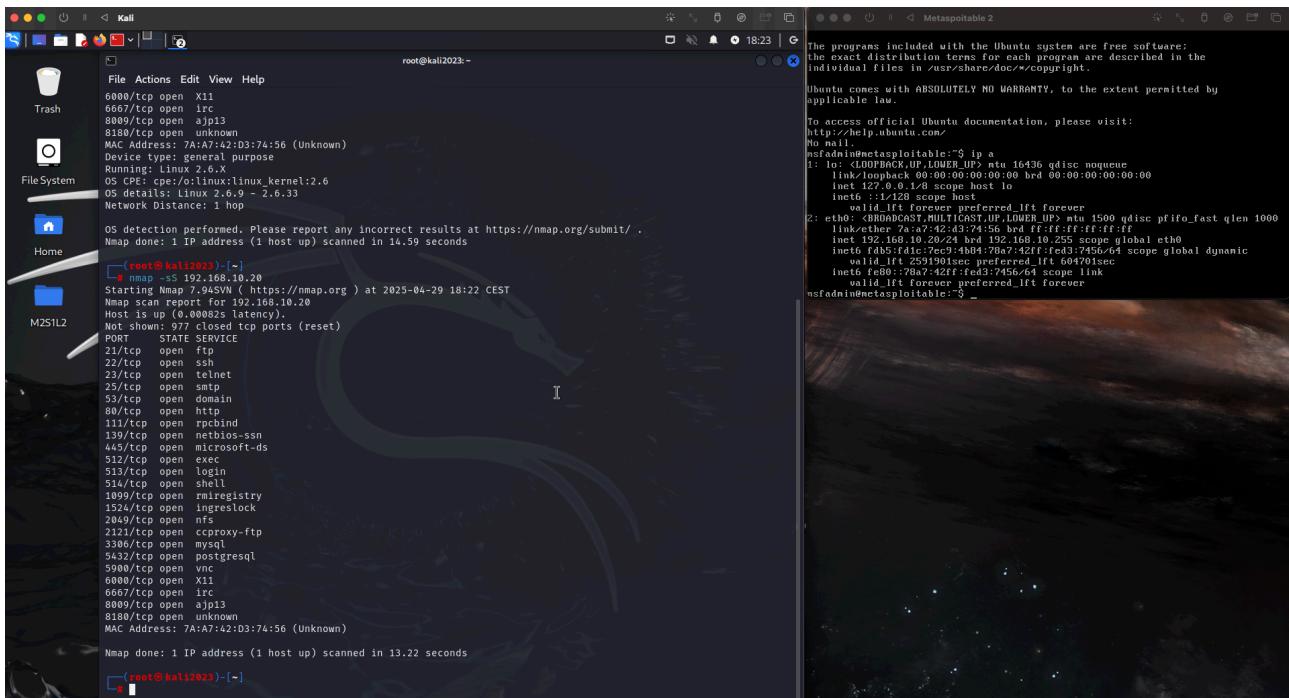


```
root@kali2023:~# nmap -O 192.168.10.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-29 18:17 CEST
Nmap scan report for 192.168.10.20
Host is up (0.00082s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
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
109/tcp   open  rmiregistry
152/tcp   open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-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: 7A:A7:42:D3:74:56 (Unknown)
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 14.59 seconds

root@kali2023:~# nsfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
        link-layer brd ff:ff:ff:ff:ff:ff
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 7a:a7:42:d3:74:56 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.24 brd 192.168.10.255 scope global eth0
        link-layer brd ff:ff:ff:ff:ff:ff
        valid_lft 2591901sec preferred_lft 604701sec
    inet fe80::7a:a7ff:fed3:7456/64 scope link
        link-layer brd ff:ff:ff:ff:ff:ff
        valid_lft forever preferred_lft forever
nsfadmin@metasploitable:~$
```

Per la SYN Scan usiamo il comando ‘nmap -sS 192.168.10.20’ e avremo questo risultato:



```
root@kali2023:~# nmap -sS 192.168.10.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-29 18:23 CEST
Nmap scan report for 192.168.10.20
Host is up (0.00082s 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
109/tcp   open  rmiregistry
152/tcp   open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-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: 7A:A7:42:D3:74:56 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds

root@kali2023:~# nsfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
        link-layer brd ff:ff:ff:ff:ff:ff
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 7a:a7:42:d3:74:56 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.24 brd 192.168.10.255 scope global eth0
        link-layer brd ff:ff:ff:ff:ff:ff
        valid_lft 2591901sec preferred_lft 604701sec
    inet fe80::7a:a7ff:fed3:7456/64 scope link
        link-layer brd ff:ff:ff:ff:ff:ff
        valid_lft forever preferred_lft forever
nsfadmin@metasploitable:~$
```

Per la TCP Connect Scan usiamo il comando ‘nmap -sT 192.168.10.20’ e avremo questo risultato:

```
File Actions Edit View Help
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open cproxy-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: TA:A7:42:D3:74:56 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds

[root@kali2023:~]
# nmap -sT 192.168.10.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-29 18:25 CEST
Nmap scan report for 192.168.10.20
Host is up (0.001s 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  privilege
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-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: TA:A7:42:D3:74:56 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds

[root@kali2023:~]
#
```

Dove non notiamo differenze con SYN Scan

Per la Version detection usiamo il comando ‘nmap -sT 192.168.10.20’ e avremo questo risultato:

```
File Actions Edit View Help
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: 7A:A7:42:D3:74:56 (Unknown)

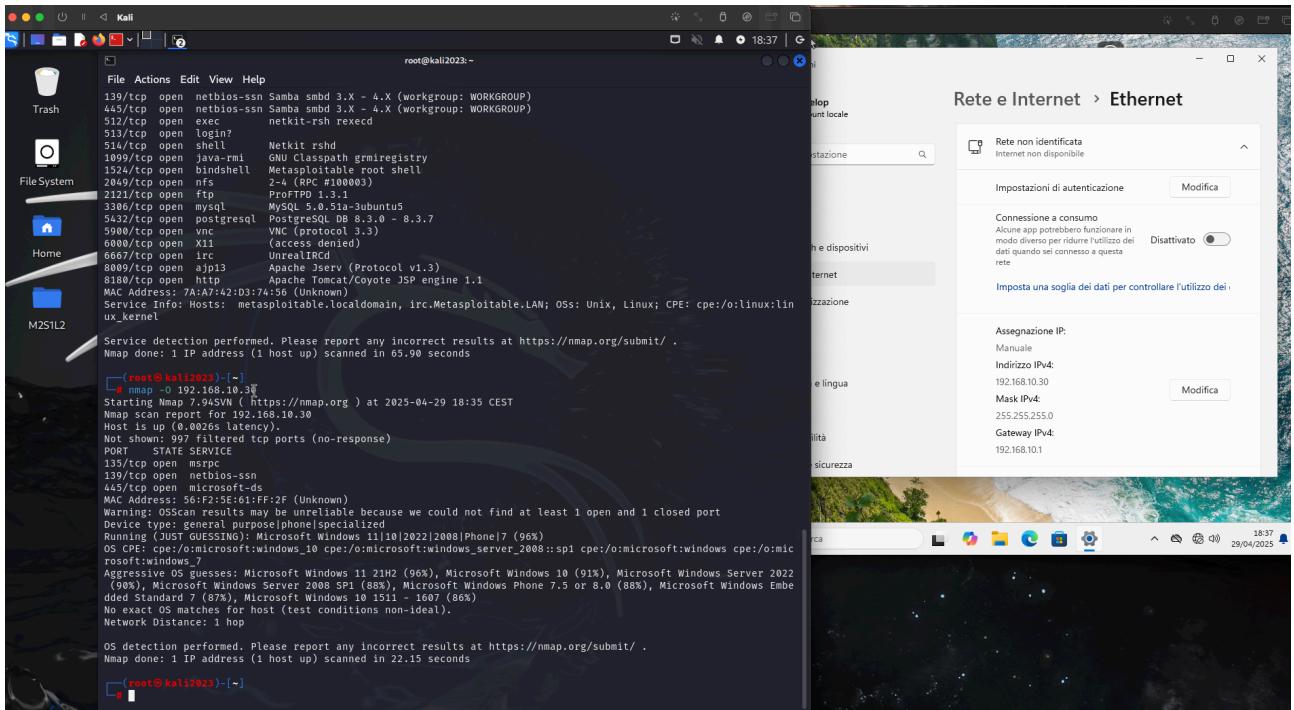
Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds

[root@kali2023:~]
# nmap -sT 192.168.10.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-29 18:32 CEST
Nmap scan report for 192.168.10.20
Host is up (0.001s 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
33/tcp    open  domain       ISC BIND 9.12.1
80/tcp    open  http         Apache Tomcat/Coyote JSP engine 1.1
111/tcp   open  rpcbind     2 (RPC #10000)
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        Netkit rshd
514/tcp   open  shell        Netkit rshd
1099/tcp  open  rmiregistry  Oracle Classpath rmiregistry
1524/tcp  open  ingreslock  Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #10000)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-Subuntu5
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          Unspecified
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 7A:A7:42:D3:74:56 (Unknown)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:lin ux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.90 seconds

[root@kali2023:~]
```

Fatto ciò ci spostiamo a scansionare la VM Windows 11 192.168.10.30 dove eseguiamo solo la scansione OS, tramite Kali Linux 192.168.10.10, con il comando ‘`sudo nmap -O 192.168.10.30`’ e avremo questo risultato:



Dalla scansione su metasploitable 192.168.10.20 possiamo evincere quanto segue:

- IP: 192.168.10.20
- OS: Linux 2.6.9 – 2.6.33
- 23 Porte aperte:

PORTE	OPEN/CLOSED
21/tcp	open
22/tcp	open
23/tcp	open
25/tcp	open
53/tcp	open
80/tcp	open
111/tcp	open
139/tcp	open

445/tcp	open
512/tcp	open
513/tcp	open
514/tcp	open
1099/tcp	open
1524/tcp	open
2049/tcp	open
2121/tcp	open
3306/tcp	open
5432/tcp	open
5900/tcp	open
6000/tcp	open
6667/tcp	open
8009/tcp	open
8180/tcp	open

- Servizi in ascolto con versione:

SERVIZIO	VERSIONE
ftp	vsftpd 2.3.4
ssh	OpenSSH 4.7p1 Debian 8ubuntui (protocol
telnet	Linux telnetd
smtp	Postfix Smtpd
domain	ISC BIND 9.4.2
http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
rpebind	2 (RPC #100000)
netbios-ssn	Samba smbd 3. - 4.X (workgroup:
netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
exec	netkit-rsh rexecd
login?	
shell	Netkit rshd
java- rmi	GNU Classpath grmiregistry
bindshell	Metasploitable root shell
nfs	2-4 (RPC #100003)
ftp	ProFTPD 1.3.1

mysql	MySOL 5.0.51a-3ubuntu5
postgresql	PostgreSQL DB 8.3.0 - 8.3.7
vnG	VNC (protocol 3.3)
X11	(access denied)
irc	UnrealIRCd
ajp13	Apache Jserv (Protocol v1.3)
http	Apache Tomcat/Coyote JSP engine 1.1

Mentre dalla scansione fatta su Windows 11 possiamo evincere quanto segue:

- IP: 192.168.10.30
- OS: Microsoft Windows 11 21H2 (96%)

Autori e contatti

Mirko Geria

mirkogeria@gmail.com

+39 33318****