



# Nmap

Prove pratiche di scansione su metasploitable 2  
e Windows 7

```

└─# nmap
Nmap 7.94 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3], ...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to give
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery pr
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2], ...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
  Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from

```

# Cos'è Nmap?

Nmap, abbreviazione di "Network Mapper", è uno strumento open-source ampiamente utilizzato per la scansione di reti, la scoperta di dispositivi, la valutazione della sicurezza e l'analisi delle porte

# Scansioni su Metasploitable2

1°

## OS fingerprint

OS fingerprint fornirà informazioni sull'IP target, le porte aperte e una congettura sull'OS in esecuzione.

```
File Actions Edit View Help
(root@kali)-[/home/kali]
# nmap -O 192.168.2.110
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 08:10 EDT
Nmap scan report for 192.168.2.110 (192.168.2.110)
Host is up (0.025s latency).
Not shown: 978 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
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
```

2°

## Syn Scan

Questa scansione mostrerà quali porte sono aperte sull'host target, ma non fornirà informazioni sull'OS in esecuzione.

File Actions Edit View Help

(root@kali)-[/home/kali]

# nmap -sS 192.168.2.110

Starting Nmap 7.94 ( <https://nmap.org> ) at 2023-10-25 08:12 EDT

Nmap scan report for 192.168.2.110 (192.168.2.110)

Host is up (0.073s latency).

Not shown: 978 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
----------	------	------------

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 2.41 seconds

3°

## TCP connect

Questa scansione mostrerà quali porte sono aperte sull'host target.

TCP Connect è meno stealthy rispetto ad altre tecniche di scansione, come la scansione SYN (Scansione SYN), in quanto implica l'apertura di connessioni complete alle porte.

```
(root@kali)-[/home/kali]
# nmap -sT 192.168.2.110
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 09:44 EDT
Nmap scan report for 192.168.2.110 (192.168.2.110)
Host is up (0.083s latency).
Not shown: 978 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
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 1.24 seconds
(root@kali)-[/home/kali]
```



4°

## Version detection

I risultati includeranno non solo le porte aperte, ma anche le informazioni sul servizio in esecuzione su ciascuna porta, compresa la versione del software.

```
(root@kali)-[/home/kali]
# nmap -sV 192.168.2.110
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 08:18 EDT
Nmap scan report for 192.168.2.110 (192.168.2.110)
Host is up (0.068s latency).
Not shown: 978 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  tcpwrapped
445/tcp   open  tcpwrapped
512/tcp   open  exec?
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
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; OS
s: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

# Scansioni su Windows 7

Qua è presente una problematica, il firewall di windows 7 è abbastanza potente da bloccare i tool di nmap, visti da noi fino ad adesso, anche aumentando i gradi di aggressività

```
(root@kali)-[/home/kali]
# nmap -A -T2 192.168.1.19
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 08:37 EDT
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth S
can
SYN Stealth Scan Timing: About 0.20% done
Stats: 0:02:41 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth S
can
SYN Stealth Scan Timing: About 18.70% done; ETC: 08:51 (0:11:36 remaining)
Stats: 0:05:42 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth S
can
SYN Stealth Scan Timing: About 39.95% done; ETC: 08:51 (0:08:33 remaining)
Stats: 0:06:39 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth S
can
SYN Stealth Scan Timing: About 46.70% done; ETC: 08:51 (0:07:35 remaining)
Stats: 0:10:06 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth S
can
SYN Stealth Scan Timing: About 70.90% done; ETC: 08:51 (0:04:09 remaining)
Stats: 0:10:51 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth S
can
SYN Stealth Scan Timing: About 76.20% done; ETC: 08:51 (0:03:23 remaining)
Stats: 0:13:24 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth S
can
SYN Stealth Scan Timing: About 94.10% done; ETC: 08:51 (0:00:50 remaining)
Nmap scan report for 192.168.1.19 (192.168.1.19)
Host is up (0.0070s latency).
All 1000 scanned ports on 192.168.1.19 (192.168.1.19) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:70:53:1A (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: specialized|VoIP phone|general purpose|phone
Running: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7|8|Phone
|XP|2012, Palmmicro embedded, VMware Player
```

Tentativo con  
aggressività elevata

---

In questo caso per ottenere  
un responso, ho disattivato il  
firewall dalla macchina  
Windows 7 e ho rilanciato il  
comando.

```
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

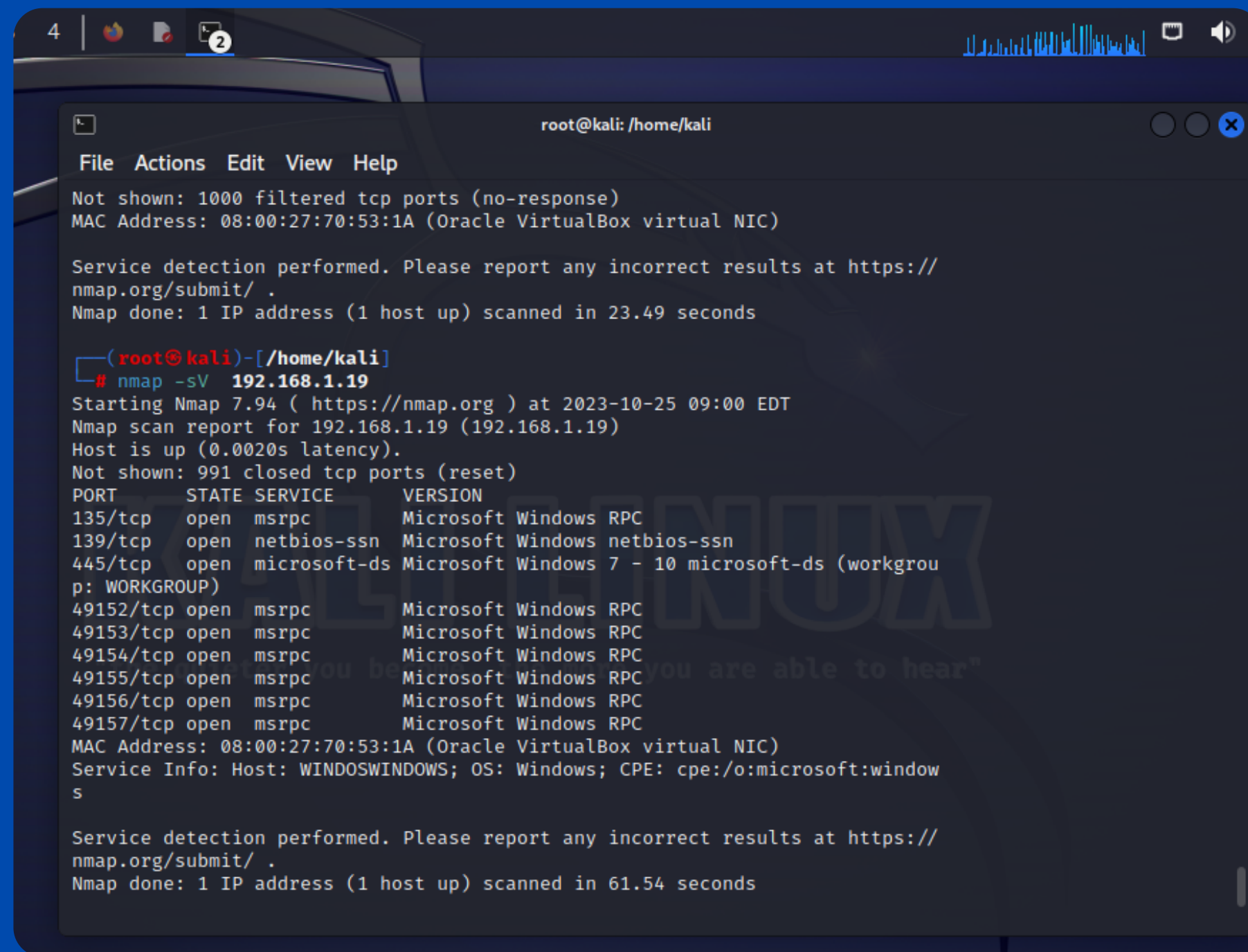
Nmap done: 1 IP address (1 host up) scanned in 1.24 seconds

(root@kali)-[/home/kali]
# nmap -O 192.168.1.19
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 10:00 EDT
Nmap scan report for 192.168.1.19 (192.168.1.19)
Host is up (0.0015s latency).
Not shown: 991 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
49157/tcp  open  unknown
MAC Address: 08:00:27:70:53:1A (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1
t:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, W
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https:
```

Molte informazioni  
risultano ancora  
nascoste





```
root@kali: /home/kali
File Actions Edit View Help
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:70:53:1A (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.49 seconds

(root@kali)-[/home/kali]
# nmap -sV 192.168.1.19
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 09:00 EDT
Nmap scan report for 192.168.1.19 (192.168.1.19)
Host is up (0.0020s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds   Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc          Microsoft Windows RPC
49153/tcp open  msrpc          Microsoft Windows RPC
49154/tcp open  msrpc          Microsoft Windows RPC
49155/tcp open  msrpc          Microsoft Windows RPC
49156/tcp open  msrpc          Microsoft Windows RPC
49157/tcp open  msrpc          Microsoft Windows RPC
MAC Address: 08:00:27:70:53:1A (Oracle VirtualBox virtual NIC)
Service Info: Host: WINDOSWINDOWS; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 61.54 seconds
```

## AUMENTIANO L'AGGRESSIVITÀ PER OTTENERE QUELLO CHE CERCHIAMO

OPZIONE -A DI NMAP È UNA COMBINAZIONE DI DIVERSE OPZIONI, TRA CUI LA SCANSIONE OS FINGERPRINT CON -O, LA SCANSIONE DELLE VERSIONI DEI SERVIZI CON -SV E ALTRE TECNICHE AVANZATE PER RACCOLGERE INFORMAZIONI SUL SISTEMA TARGET

# Scan Indirizzi Ip

[illegible]

Con il comando nell'immagine riusciamo a ottenere una lista degli ip attivi dentro la rete(In questo caso ho impostato un range)

**\*Dati potenzialmente sensibili cancellati**