

Nmap

L'esercizio di oggi riguarda la creazione di un report con i dettagli di 4 tipi di scansioni sul target Metasploitable(su reti diverse).

La prima scansione è la scansione del sistema operativo, la seconda il syn scan, la terza il tcp scan e l'ultima la version scan.

1)

```
(raul@192)-[~]
$ nmap -O 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-04 17:37 GMT
Nmap scan report for 192.168.51.101
Host is up (0.0012s 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
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 1.71 seconds
```

Raul Pastor

2)

```
(raul@192)-[~]
$ nmap -sS 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-04 17:38 GMT
Nmap scan report for 192.168.51.101
Host is up (0.0016s 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

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

1 0.0000000000	192.168.50.100	192.168.51.101	ICMP	44 Echo (ping) request	id=0x1376, seq=0/0, ttl=41 (reply in 5)
2 0.0000131412	192.168.50.100	192.168.51.101	TCP	69 52416 - 443 [ACK] Seq=0 Win=1024 Len=0 MSS=1460	
3 0.0000131456	192.168.50.100	192.168.51.101	TCP	69 52416 - 80 [ACK] Seq=1 Win=1024 Len=0 MSS=1460	
4 0.0000921505	192.168.50.100	192.168.51.101	ICMP	56 Timestamp request	id=0x0e085, seq=0/0, ttl=48
5 0.001187222	192.168.51.101	192.168.50.100	ICMP	44 Echo (ping) reply	id=0x1376, seq=0/0, ttl=63 (request in 1)
6 0.001187305	192.168.51.101	192.168.50.100	TCP	56 443 - 52416 [RST, ACK] Seq=3 Ack=1 Win=0 Len=0	
7 0.001187347	192.168.51.101	192.168.50.100	ICMP	56 Timestamp reply	id=0x0e855, seq=0/0, ttl=63
8 0.0558100000	192.168.50.100	192.168.50.100	DNS	149 Standard query	id=0xe26, Port=53, Name="168.192.in-addr.arpa", TTL=101.51.168.192.in-addr.arpa
9 0.0558101029	192.168.50.100	192.168.50.100	DNS	149 Standard query	id=0xe26, Port=53, Name="168.192.in-addr.arpa", TTL=101.51.168.192.in-addr.arpa SOA localhost
10 0.084883062	192.168.50.100	192.168.51.101	TCP	69 52672 - 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
11 0.084893564	192.168.50.100	192.168.51.101	TCP	69 52672 - 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
12 0.084096440	192.168.50.100	192.168.51.101	TCP	69 52672 - 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
13 0.0841000000	192.168.50.100	192.168.51.101	TCP	69 52672 - 8880 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
14 0.0841000000	192.168.50.100	192.168.51.101	TCP	69 52672 - 118 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
15 0.084101608	192.168.50.100	192.168.51.101	TCP	69 52672 - 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
16 0.084103490	192.168.50.100	192.168.51.101	TCP	69 52672 - 1028 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
17 0.084104962	192.168.50.100	192.168.51.101	TCP	69 52672 - 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
18 0.084105875	192.168.50.100	192.168.51.101	TCP	69 52672 - 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
19 0.084106875	192.168.50.100	192.168.51.101	TCP	69 52672 - 1028 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
20 0.085023079	192.168.51.101	192.168.50.100	TCP	56 1723 - 52672 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
21 0.085023393	192.168.51.101	192.168.50.100	TCP	56 199 - 52672 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
22 0.085023395	192.168.51.101	192.168.50.100	TCP	69 3306 - 52672 [SYN, ACK] Seq=1 Ack=1 Win=5840 Len=0 MSS=1460	
23 0.085124877	192.168.50.100	192.168.51.101	TCP	56 52672 - 3306 [RST] Seq=1 Win=0 Len=0	
25 0.085152894	192.168.50.100	192.168.51.101	TCP	56 52672 - 52672 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
26 0.085153008	192.168.50.100	192.168.51.101	TCP	56 111 - 52672 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0	
27 0.085153049	192.168.51.101	192.168.50.100	TCP	69 111 - 92672 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460	
28 0.085153049	192.168.51.101	192.168.50.100	TCP	56 554 - 52672 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
29 0.085153091	192.168.51.101	192.168.50.100	TCP	56 443 - 52672 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
30 0.085153091	192.168.51.101	192.168.50.100	TCP	56 587 - 52672 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
31 0.085160259	192.168.50.100	192.168.51.101	TCP	56 52672 - 111 [RST] Seq=1 Ack=1 Win=0 Len=0	
32 0.085193049	192.168.50.100	192.168.51.101	TCP	69 52672 - 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
33 0.085292039	192.168.50.100	192.168.51.101	TCP	69 52672 - 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
34 0.085292039	192.168.50.100	192.168.51.101	TCP	69 52672 - 211 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
35 0.085292609	192.168.50.100	192.168.51.101	TCP	69 52672 - 145 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
36 0.085297581	192.168.50.100	192.168.51.101	TCP	69 52672 - 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
37 0.085298915	192.168.50.100	192.168.51.101	TCP	69 52672 - 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	

Raul Pastor

3)

```
(raul㉿192)-[~]
$ nmap -sT 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-04 17:38 GMT
Nmap scan report for 192.168.51.101
Host is up (0.0034s 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

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

1659 0.090134868	192.168.50.100	192.168.51.101	TCP	76 56132 → 513 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=3386287391 TSecr=0 WS=1024
1806 0.094064623	192.168.51.101	192.168.50.100	TCP	76 513 → 56132 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TStamp=3709582 TSecr=3386287391
1807 0.094064665	192.168.51.101	192.168.50.100	TCP	56 2638 → 45592 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1808 0.094064665	192.168.51.101	192.168.50.100	TCP	56 2383 → 49064 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1809 0.094064249	192.168.50.100	192.168.51.101	TCP	68 56132 → 513 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TStamp=3386287395 TSecr=3709582
1810 0.094064276	192.168.50.100	192.168.50.100	TCP	56 603 → 60029 [ACK] Seq=2 Ack=2 Win=64512 Len=0

4)

```
(raul@192) [~]
$ nmap -sV 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-04 17:52 GMT
Nmap scan report for 192.168.51.101
Host is up (0.0019s 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         netkit-rsh rexecd
513/tcp   open  login?      -
514/tcp   open  shell        Netkit rshd
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  ccproxy-ftp?
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 172.67 seconds
```

Notiamo attraverso una cattura con wireshark che nella seconda scansione (syn-scan) con nmap il three-way handshake non viene completato mentre nella terza (tcp-scan) viene completato.

REPORT

Indirizzo ip target: 192.168.51.101

Sistema operativo: Linux 2.6

Informazioni sulle porte:

PORTA	STATO	SERVIZIO	VERSIONE
21	open	ftp	vsftpd 2.3.4
22	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23	open	telnet	Linux telnetd
25	open	smtp	Postfix smtpd
53	open	domain	ISC BIND 9.4.2
80	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111	open	rpcbind	2 (RPC #100000)
139	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512	open	exec	netkit-rsh rexecd
513	open	login?	-
514	open	shell	Netkit rshd
1099	open	java-rmi	GNU Classpath grmiregistry

1524	open	bindshell	Metasploitable root shell
2049	open	nfs	2-4 (RPC #100003)
2121	open	ccproxy-ftp?	—
3306	open	mysql	MySQL 5.0.51a-3ubuntu5
5432	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900	open	vnc	VNC (protocol 3.3)
6000	open	X11	access denied
6667	open	irc	UnrealIRCd
8009	open	ajp13	Apache Jserv (Protocol v1.3)
8180	open	http	Apache Tomcat/Coyote JSP engine 1.1

PARTE FACOLTATIVA:

La parte facoltativa prevedeva di estendere le 4 scansioni sulla macchina Metasploitable presente nella stessa rete di Kali e verificarne le differenze.

1)

```
(raul@192)-[~]
$ nmap -o 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-04 19:45 GMT
Nmap scan report for 192.168.50.101 (192.168.50.101)
Host is up (0.0016s 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
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
8180/tcp  open  unknown
MAC Address: 52:9D:95:FD:5F:3E (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 1.56 seconds
```

Raul Pastor

2)

```
(raul@192)-[~]
$ nmap -sS 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-04 19:45 GMT
Nmap scan report for 192.168.50.101 (192.168.50.101)
Host is up (0.00046s 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: 52:9D:95:FD:5F:3E (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

3)

```
(raul@192)-[~]
$ nmap -sT 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-04 19:45 GMT
Nmap scan report for 192.168.50.101 (192.168.50.101)
Host is up (0.00042s 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: 52:9D:95:FD:5F:3E (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

4)

```
(raul@192)-[~]
$ nmap -sV 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-04 19:45 GMT
Nmap scan report for 192.168.50.101 (192.168.50.101)
Host is up (0.00049s 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         netkit-rsh rexecd
513/tcp   open  login?      Netkit rshd
514/tcp   open  shell        Netkit rshd
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: 52:9D:95:FD:5F:3E (Unknown)
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 52.79 seconds
```

Le differenze principali sono:

- Nella prima scansione (OS scan), diversamente da quanto previsto, viene trovata una porta aggiuntiva nella versione scan su 2 reti diverse.
- Nelle restanti scansioni la versione sulla stessa rete ci ha impiegato relativamente molto meno tempo e ha indicato il mac address della macchina target, diversamente dalla scansione su reti diverse.