

Scansione dei servizi con Nmap

```
(root@kali)-[/home/kali]
# nmap -sS 192.168.48.93
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 15:46 EST
Nmap scan report for 192.168.48.93
Host is up (0.0081s latency).
Not shown: 977 filtered tcp ports (no-response)
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 5.79 seconds
(root@kali)-[/home/kali]
```

Il comando **nmap -sS 192.168.48.93** è stato utilizzato per eseguire una scansione SYN su tutte le porte della macchina con l'indirizzo IP 192.168.48.93

```

(root@kali)-[/home/kali]
# nmap -sV 192.168.48.93
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 15:48 EST
Nmap scan report for 192.168.48.93
Host is up (0.0045s latency).
Not shown: 977 filtered tcp ports (no-response)
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  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 16.75 seconds

```

Il comando **nmap -sV 192.168.48.93** è stato utilizzato per eseguire una scansione dei servizi sulla macchina con l'indirizzo IP 192.168.48.93.

```

(root@kali)-[/home/kali]
# nmap -sV -oN file.txt 192.168.48.93
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 15:49 EST
Nmap scan report for 192.168.48.93
Host is up (0.0050s latency).
Not shown: 977 filtered tcp ports (no-response)
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  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 16.12 seconds

```

```

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

```



file.txt

Il comando **nmap -sV -oN file.txt 192.168.48.93** è stato utilizzato per

eseguire una scansione dei servizi sulla macchina con l'indirizzo IP 192.168.48.93 e salvare i risultati in un file di testo denominato "file.txt".

```
(root@kali)-[/home/kali]
# nmap -sS -p 8080 192.168.48.93
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 15:51 E
Nmap scan report for 192.168.48.93
Host is up (0.0012s latency).

PORT      STATE      SERVICE
8080/tcp   filtered  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
(root@kali)-[/home/kali]
```

Il comando **nmap -sS -p 8080 192.168.48.93** è stato utilizzato per eseguire una scansione SYN su una specifica porta, nel caso specifico la porta 8080, sulla macchina con l'indirizzo IP 192.168.48.93

```
➜ nmap -sS -p- 192.168.48.93
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 15:51 EST
Nmap scan report for 192.168.48.93
Host is up (0.027s latency).
Not shown: 65509 filtered tcp ports (no-response)
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
514/tcp   open  shell
1099/tcp  open  rmiregistry
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
40983/tcp open  unknown
44296/tcp open  unknown
46185/tcp open  unknown
56450/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 108.59 seconds
```

Il comando **nmap -sS -p 8080 192.168.48.93** è stato utilizzato per eseguire una scansione SYN su tutte le 65535 porte, sulla macchina con l'indirizzo IP 192.168.48.93

```
(root@kali)-[/home/kali]
# nmap -sU -r -v 192.168.48.93
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 15:55 EST
Initiating Ping Scan at 15:55
Scanning 192.168.48.93 [4 ports]
Completed Ping Scan at 15:55, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:55
Completed Parallel DNS resolution of 1 host. at 15:55, 0.01s elapsed
Initiating UDP Scan at 15:55
Scanning 192.168.48.93 [1000 ports]
Discovered open port 53/udp on 192.168.48.93
Discovered open port 111/udp on 192.168.48.93
Discovered open port 137/udp on 192.168.48.93
Increasing send delay for 192.168.48.93 from 0 to 50 due to 11 out of 14 dropped probes since last increase.
Increasing send delay for 192.168.48.93 from 50 to 100 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 15.85% done; ETC: 15:59 (0:02:45 remaining)
Discovered open port 2049/udp on 192.168.48.93
Increasing send delay for 192.168.48.93 from 100 to 200 due to 11 out of 12 dropped probes since last increase.
UDP Scan Timing: About 25.20% done; ETC: 15:59 (0:03:01 remaining)
Increasing send delay for 192.168.48.93 from 200 to 400 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 29.65% done; ETC: 16:00 (0:03:36 remaining)
Increasing send delay for 192.168.48.93 from 400 to 800 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 32.90% done; ETC: 16:01 (0:04:07 remaining)
UDP Scan Timing: About 34.65% done; ETC: 16:03 (0:04:45 remaining)
UDP Scan Timing: About 36.25% done; ETC: 16:04 (0:05:18 remaining)
UDP Scan Timing: About 37.90% done; ETC: 16:05 (0:05:46 remaining)
Increasing send delay for 192.168.48.93 from 800 to 1000 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 39.65% done; ETC: 16:06 (0:06:16 remaining)
UDP Scan Timing: About 41.70% done; ETC: 16:07 (0:06:48 remaining)
UDP Scan Timing: About 44.85% done; ETC: 16:09 (0:07:24 remaining)
UDP Scan Timing: About 64.85% done; ETC: 16:16 (0:07:17 remaining)
UDP Scan Timing: About 72.05% done; ETC: 16:18 (0:06:15 remaining)
UDP Scan Timing: About 78.20% done; ETC: 16:19 (0:05:08 remaining)
UDP Scan Timing: About 83.95% done; ETC: 16:20 (0:03:56 remaining)
UDP Scan Timing: About 89.35% done; ETC: 16:21 (0:02:42 remaining)
UDP Scan Timing: About 94.50% done; ETC: 16:21 (0:01:26 remaining)
Completed UDP Scan at 16:22, 1593.68s elapsed (1000 total ports)
Nmap scan report for 192.168.48.93
Host is up (0.011s latency).
Not shown: 996 open|filtered udp ports (no-response)
PORT      STATE SERVICE
53/udp    open  domain
111/udp   open  rpcbind
137/udp    open  netbios-ns
2049/udp   open  nfs

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1593.90 seconds
Raw packets sent: 2272 (105.660KB) | Rcvd: 10 (1.091KB)
```

Il comando **nmap -sU -r -v 192.168.48.93** è stato utilizzato per eseguire una scansione UDP approfondita sulla macchina con l'indirizzo IP 192.168.48.93.

```
(root@kali)-[/home/kali]
# nmap -O 192.168.48.93
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 16:23 EST
Nmap scan report for 192.168.48.93
Host is up (0.0032s latency).
Not shown: 977 filtered tcp ports (no-response)
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
5999/tcp  open  rmiregistry
5524/tcp  open  ingreslock
6049/tcp  open  nfs
6121/tcp  open  ccproxy-ftp
8306/tcp  open  mysql
8432/tcp  open  postgresql
8900/tcp  open  vnc
9000/tcp  open  X11
9667/tcp  open  irc
9809/tcp  open  ajp13
9180/tcp  open  unknown
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (95%), QEMU (92%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (95%), QEMU user mode network gateway (92%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.64 seconds
```

Il comando **nmap -O 192.168.48.93** è stato
utilizzato per eseguire una scansione per
l'identificazione del sistema operativo sulla
macchina con l'indirizzo IP 192.168.48.93.

```
(root@kali)-[/home/kali]
# nmap -F 192.168.48.93
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 16:34 EST
Nmap scan report for 192.168.48.93
Host is up (0.0042s latency).
Not shown: 82 filtered tcp ports (no-response)
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
513/tcp   open  login
514/tcp   open  shell
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
8009/tcp  open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 1.86 seconds
```

Il comando **nmap -F 192.168.48.93** è stato utilizzato per eseguire una scansione rapida delle porte più comuni sulla macchina con l'indirizzo IP 192.168.48.93.


```

(root@kali)-[/home/kali]
# nmap -sV -p- 192.168.48.93
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 16:30 EST
Stats: 0:02:22 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.00% done; ETC: 16:32 (0:00:01 remaining)
Stats: 0:03:37 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.00% done; ETC: 16:33 (0:00:04 remaining)
Nmap scan report for 192.168.48.93
Host is up (0.015s latency).
Not shown: 65510 filtered tcp ports (no-response)
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
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)
6697/tcp  open  irc          UnrealIRCd (Admin email admin@Metasploitable.LAN)
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
40983/tcp open  nlockmgr     1-4 (RPC #100021)
44296/tcp open  java-rmi     GNU Classpath grmiregistry
46185/tcp open  mountd       1-3 (RPC #100005)
Service Info: Host: metasploitable.localdomain; 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 238.15 seconds

```

La scansione completa delle porte e il rilevamento delle versioni dei servizi eseguiti con il comando **nmap -sV -p- 192.168.48.93** hanno fornito un dettagliato elenco dei servizi in esecuzione sulla macchina con l'indirizzo IP 192.168.48.93.

```

(root@kali)-[/home/kali]
# nmap -sP 192.168.48.93
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 16:40 EST
Nmap scan report for 192.168.48.93
Host is up (0.0011s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds

```

Il comando **nmap -sP 192.168.48.93** è stato utilizzato per eseguire una scansione di discovery di host utilizzando pacchetti di tipo ping (ICMP echo request).


```
(root@kali)-[/home/kali]
# nmap -PN 192.168.48.93
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 16:42 EST
Nmap scan report for 192.168.48.93
Host is up (0.0049s latency).
Not shown: 977 filtered tcp ports (no-response)
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 4.39 seconds
```

Il comando **nmap -PN 192.168.48.93** è stato utilizzato per eseguire una scansione della rete senza considerare il ping.

```
L-$ sudo nmap -PR 192.168.157.93
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-25 05:28
Nmap scan report for 192.168.157.93
Host is up (0.00047s 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: 08:00:27:77:28:8F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.97 seconds
```

Il comando **nmap -PR 192.168.157.93**
è stato utilizzato per eseguire una
scansione di discovery di host
mediante l'invio di pacchetti ARP
(Address Resolution Protocol).

IP TARGET	OS	TIPO SCANSIONE	COMAN DO	PORTE APERTE	PORTE CHIUSE	MAC ADDRESS
192.168.48.93	METASPLOITABLE	TCP	nmap -sS	23	977	08:00:27:CE:D2:42
192.168.48.93	METASPLOITABLE	scansione completa	nmap -sV	23	977	08:00:27:CE:D2:42

192.168.48.93	METASPLOITABLE	output su file	nmap -sV -oN file.txt	23	977	08:00:27:CE:D2:42
192.168.48.93	METASPLOITABLE	scansione su pola	nmap -sS ip -p 8080	23	977	08:00:27:CE:D2:42
192.168.48.93	METASPLOITABLE	scansione tutte le porte	nmap -sS -p-	30	65505	08:00:27:CE:D2:42
192.168.48.93	METASPLOITABLE	scansione udp	nmap -sU -r -v	3		08:00:27:CE:D2:42
192.168.48.93	METASPLOITABLE	scansione sistema operativo	nmap -O	-	-	08:00:27:CE:D2:42
192.168.48.93	METASPLOITABLE	scansione versione servizi	nmap -sV	23	977	08:00:27:CE:D2:42
192.168.48.93	METASPLOITABLE	scansione common 100 ports	nmap -F	18	82	08:00:27:CE:D2:42
192.168.157.93	METASPLOITABLE	scansione ARP	nmap -PR	23	977	08:00:27:CE:D2:42