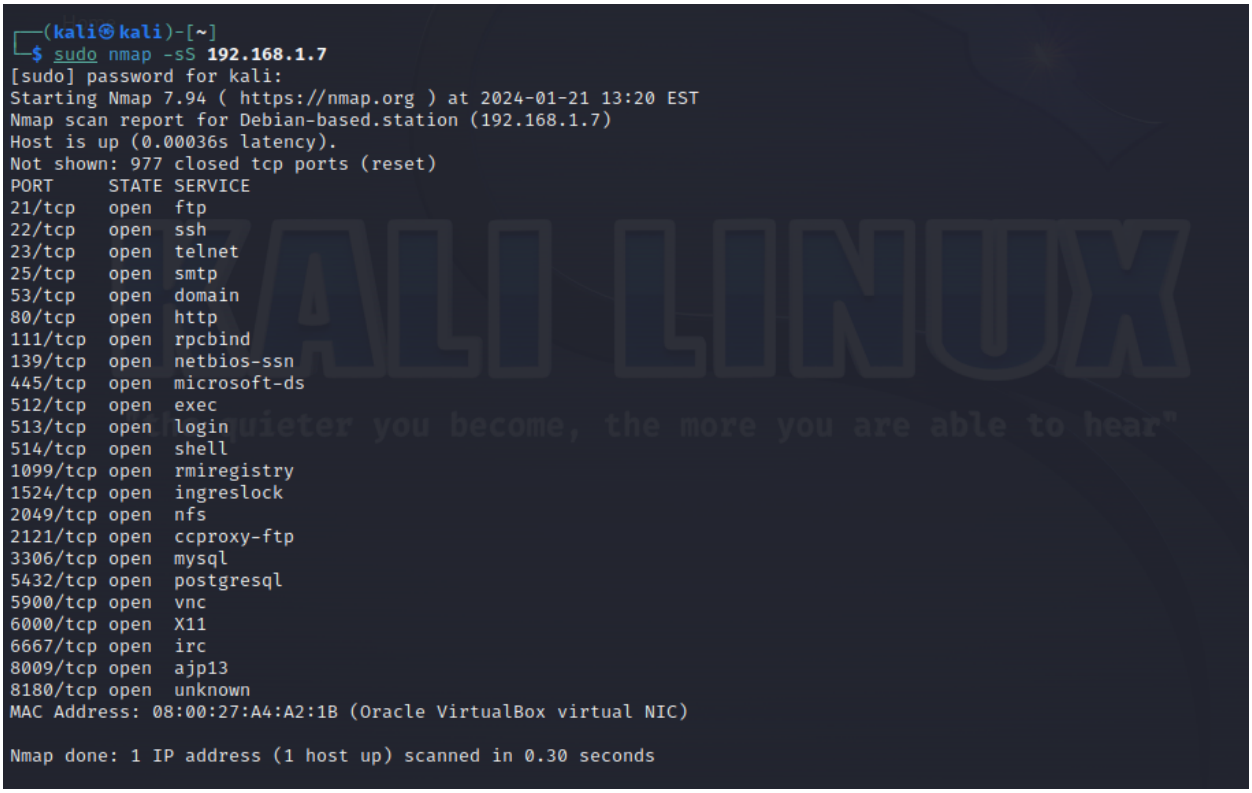
Tecniche di scansione con Nmap - scansione di un host, senza e con completamento del 3-way handshake

Questo esercizio può essere utile per lo studente per prendere dimestichezza con i vari comandi di nmap.

Poiché su Linux è un potente tool di scansione della rete, si richiede di utilizzare i seguenti comandi e trascrivere i vari risultati su un report:

TCP#

Nmap -sS ip address



Scansione completa

Nmap -sV ip address

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.1.7
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-21 13:22 EST
Nmap scan report for Debian-based.station (192.168.1.7)
Host is up (0.00064s 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?
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
MAC Address: 08:00:27:A4:A2:1B (Oracle VirtualBox virtual NIC)
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 64.08 seconds
```

Output su file #

Nmap -sV -oN file.txt ip address

```
┌──(kali㉿kali)-[~/Documents/Epicode]
└─$ sudo nmap -sV -oN nmap-file.txt 192.168.1.7\
>
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-21 14:29 EST
Nmap scan report for Debian-based.station (192.168.1.7)
Host is up (0.00051s 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?
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
MAC Address: 08:00:27:A4:A2:1B (Oracle VirtualBox virtual NIC)
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 63.70 seconds
```

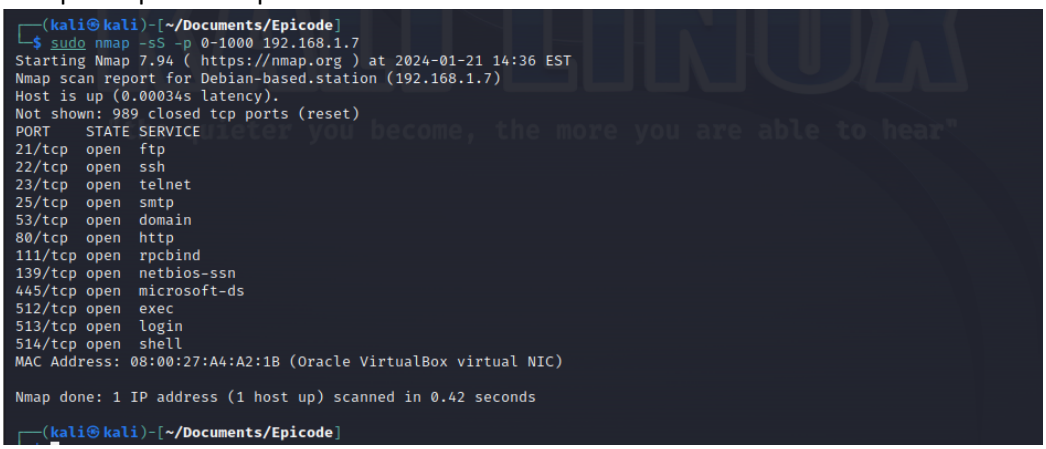
Scansione su porta

Nmap -sS -p 8080 ip address

```
┌──(kali㉿kali)-[~/Documents/Epicode]
└─$ sudo nmap -sS -p 8080  192.168.1.7

Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-21 14:32 EST
Nmap scan report for Debian-based.station (192.168.1.7)
Host is up (0.0018s latency).

PORT     STATE  SERVICE
8080/tcp closed http-proxy
MAC Address: 08:00:27:A4:A2:1B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
```

Scansion tutte le porte

Nmap -sS -p 0-1000 ip address



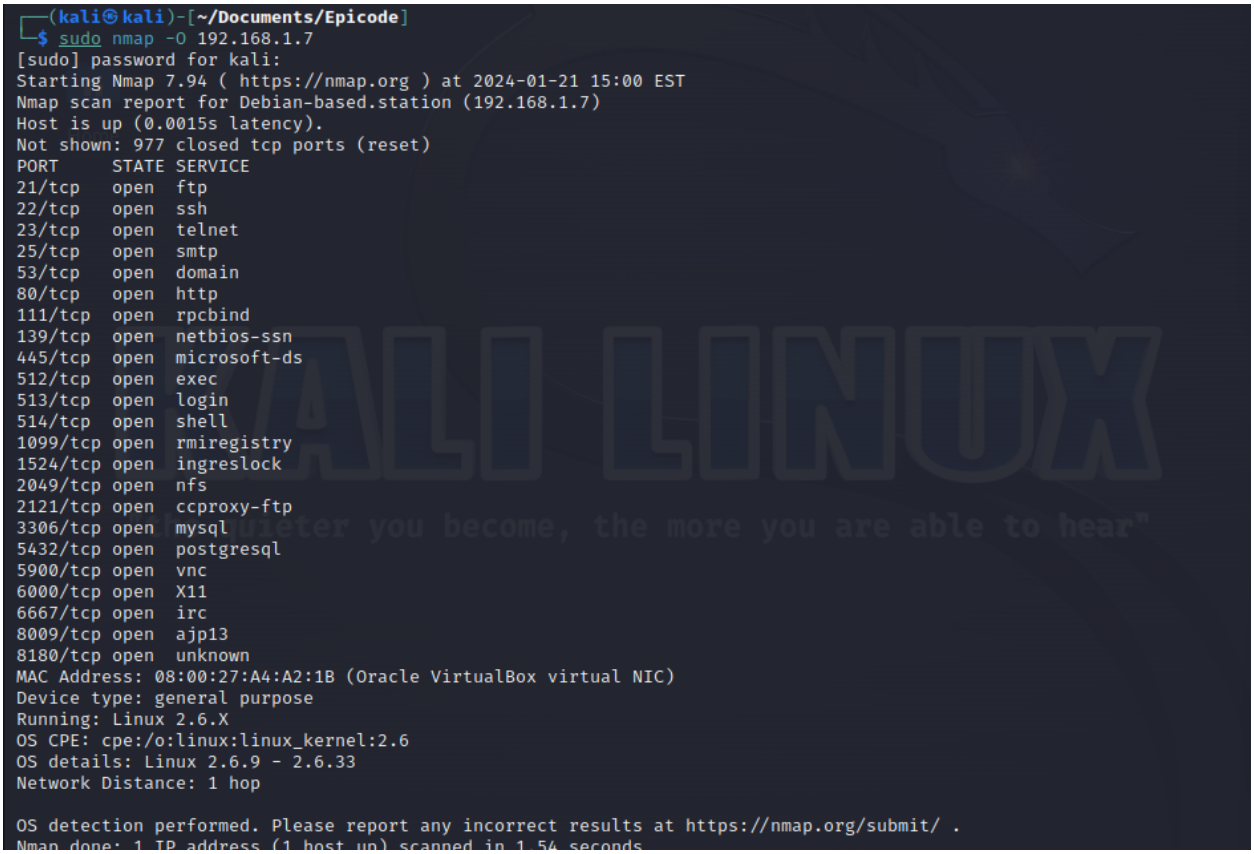
Scansion UDP

Nmap -sU -r -v ip address

```
Nmap scan report for Debian-based.station (192.168.1.7)
Host is up (0.0012s latency).
Not shown: 955 closed udp ports (port-unreach)
PORT     STATE         SERVICE
21/udp   open|filtered ftp
37/udp   open|filtered time
38/udp   open|filtered rap
49/udp   open|filtered tacacs
53/udp   open          domain
67/udp   open|filtered dhcps
68/udp   open|filtered dhcpc
69/udp   open|filtered tftp
80/udp   open|filtered http
111/udp  open          rpcbind
112/udp  open|filtered mcidas
113/udp  open|filtered auth
120/udp  open|filtered cfdptkt
136/udp  open|filtered profile
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
139/udp  open|filtered netbios-ssn
161/udp  open|filtered snmp
162/udp  open|filtered snmptrap
192/udp  open|filtered osu-nms
199/udp  open|filtered smux
207/udp  open|filtered at-7
363/udp  open|filtered rsvp_tunnel
389/udp  open|filtered ldap
402/udp  open|filtered genie
427/udp  open|filtered svrloc
434/udp  open|filtered mobileip-agent
443/udp  open|filtered https
464/udp  open|filtered kpasswd5
497/udp  open|filtered retrospect
502/udp  open|filtered mbap
512/udp  open|filtered biff
513/udp  open|filtered who
515/udp  open|filtered printer
518/udp  open|filtered ntalk
539/udp  open|filtered apertus-ldp
593/udp  open|filtered http-rpc-epmap
626/udp  open|filtered serialnumberd
639/udp  open|filtered msdp
657/udp  open|filtered rmc
682/udp  open|filtered xfr
684/udp  open|filtered corba-iiop-ssl
686/udp  open|filtered hcp-wismar
688/udp  open|filtered realm-rusd
2049/udp open          nfs
MAC Address: 08:00:27:A4:A2:1B (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1018.97 seconds
           Raw packets sent: 1737 (79.201KB) | Rcvd: 1044 (76.219KB)
```

Scansione Sistema operativo

Nmap -O ip address



Scansione versione servizi

Nmap -sV ip address

```
┌──(kali㉿kali)-[~/Documents/Epicode]
└─$ sudo nmap -sV 192.168.1.7
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-21 15:02 EST
Nmap scan report for Debian-based.station (192.168.1.7)
Host is up (0.0012s 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?
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
MAC Address: 08:00:27:A4:A2:1B (Oracle VirtualBox virtual NIC)
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 64.85 seconds
```

Scansione common 100 port

Nmap -F ip address

```
┌──(kali㉿kali)-[~/Documents/Epicode]
└─$ sudo nmap -F 192.168.1.7
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-21 15:07 EST
Nmap scan report for Debian-based.station (192.168.1.7)
Host is up (0.00034s latency).
Not shown: 82 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
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
MAC Address: 08:00:27:A4:A2:1B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

Scansione tramite ARP

Nmap -PR ip address

```
┌──(kali㉿kali)-[~/Documents/Epicode]
└─$ sudo nmap -PR 192.168.1.7
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-21 15:08 EST
Nmap scan report for Debian-based.station (192.168.1.7)
Host is up (0.0014s 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:A4:A2:1B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds

┌──(kali㉿kali)-[~/Documents/Epicode]
```

Scansione tarmite ping nmap -sP ip Address

```
┌──(kali㉿kali)-[~/Documents/Epicode]
└─$ sudo nmap -sP 192.168.1.7
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-21 15:09 EST
Nmap scan report for Debian-based.station (192.168.1.7)
Host is up (0.00085s latency).
MAC Address: 08:00:27:A4:A2:1B (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds

┌──(kali㉿kali)-[~/Documents/Epicode]
└─$
```

Scansione senza ping nmap -PN ip address

```
┌──(kali㉿kali)-[~/Documents/Epicode]
└─$ sudo nmap -PN 192.168.1.7
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-21 15:09 EST
Nmap scan report for Debian-based.station (192.168.1.7)
Host is up (0.00055s 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:A4:A2:1B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
```