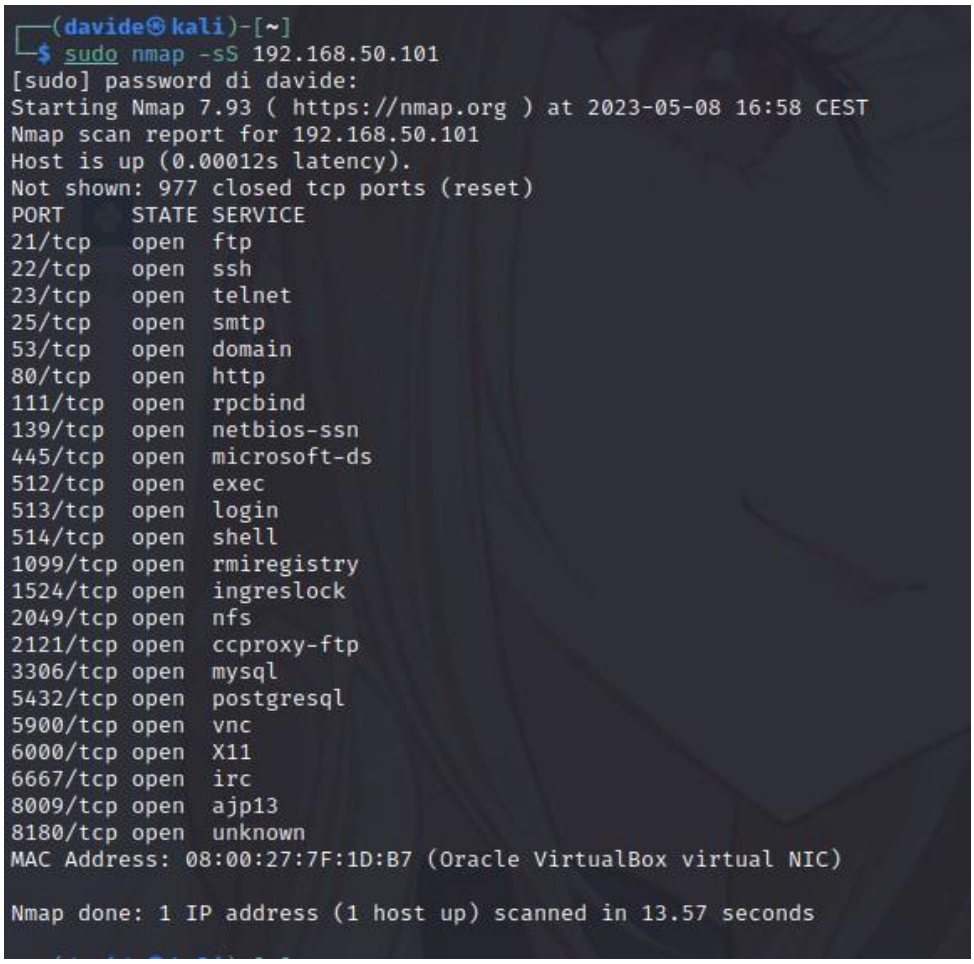
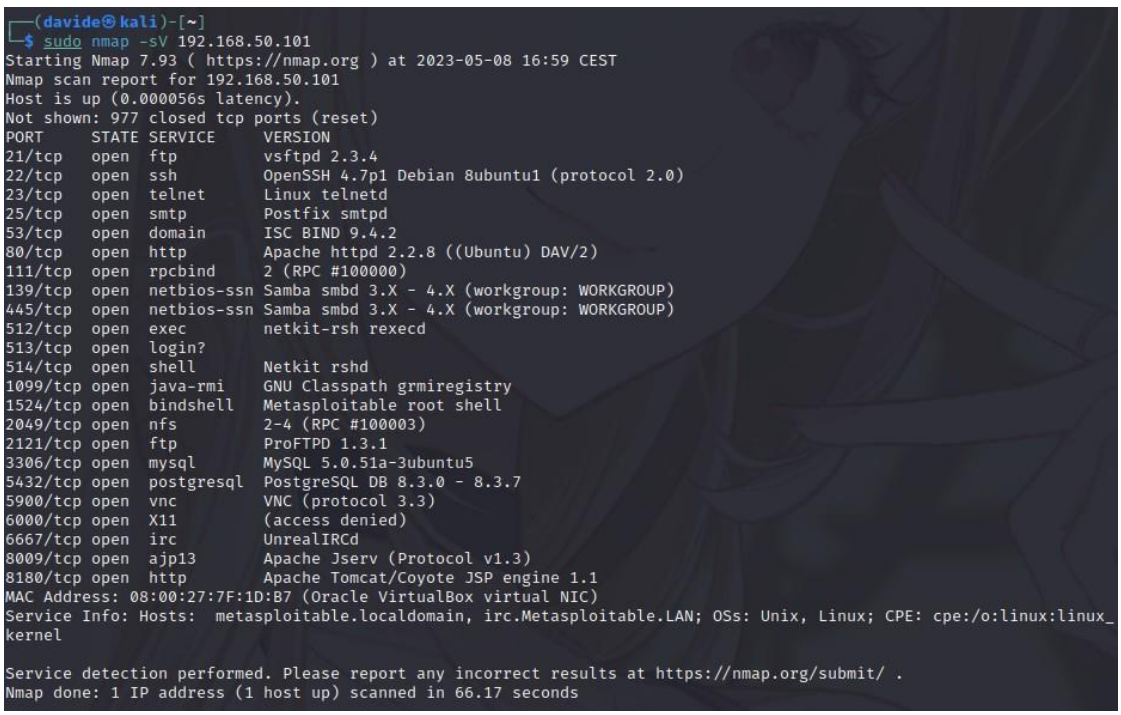
-sS (SYN scan stealth – opzione di base di nmap)



-**sV** (Abilita il version detection. In alternativa, è possibile utilizzare l'opzione -A che attiva il version detection, tra le altre cose.)



-sV -oN (System version + creazione di file txt)

```
┌──(davide㉿kali)-[~]
└─$ sudo nmap -sV -oN scansione_metasploitable 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 17:01 CEST
Nmap scan report for 192.168.50.101
Host is up (0.000087s 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  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: 08:00:27:7F:1D:B7 (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 65.84 seconds
```

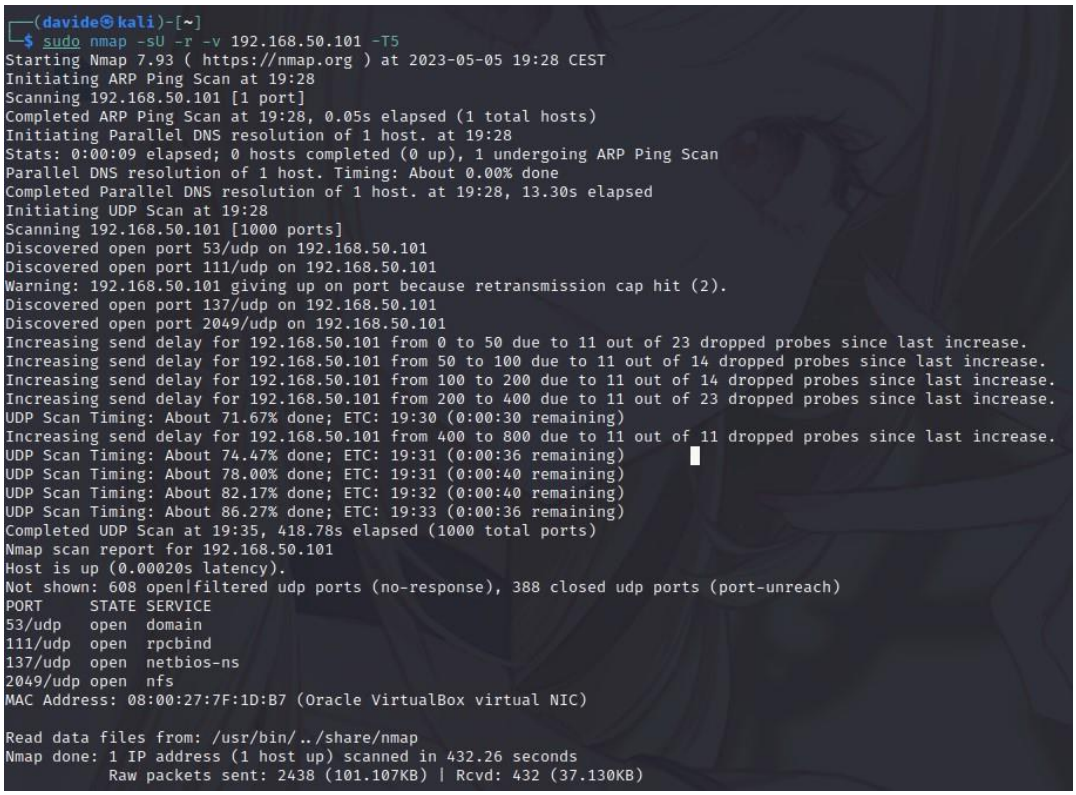
-**sS** porta 8080 (SYN stealth scan su porta singola 8080)

```
┌──(davide㉿kali)-[~]
└─$ sudo nmap -sS -p 8080 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 17:03 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00016s latency).

PORT     STATE  SERVICE
8080/tcp closed http-proxy
MAC Address: 08:00:27:7F:1D:B7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.41 seconds
```

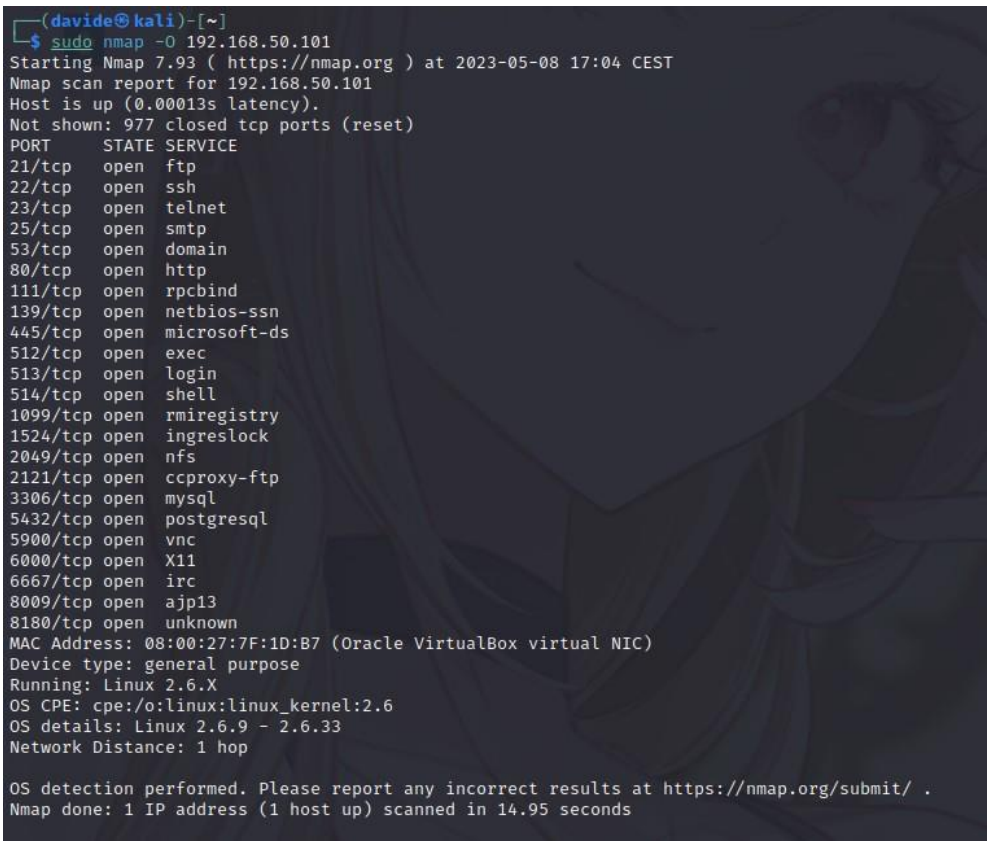
-p senza range di porte

```
┌──(davide㉿kali)-[~]
└─$ sudo nmap -sS -p 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 17:03 CEST
Error #487: Your port specifications are illegal.  Example of proper form: "-100,200-1024,T:3000-4000,U:60000-"
QUITTING!
```

-sU -r -v (scan UDP in ordine numerico -r e aumento della verbosità della scansione con -v)



-O (Abilita la OS detection). In alternativa, è possibile utilizzare l'opzione -A per attivare sia l'OS detection, tra le altre cose.



-sV (version detection – alias: *-sR*)

```
┌──(davide㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 16:59 CEST
Nmap scan report for 192.168.50.101
Host is up (0.000056s 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  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: 08:00:27:7F:1D:B7 (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 66.17 seconds
```

-f (fast scan)

```
┌──(davide㉿kali)-[~]
└─$ sudo nmap -f 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 17:06 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00011s 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: 08:00:27:7F:1D:B7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.31 seconds
```

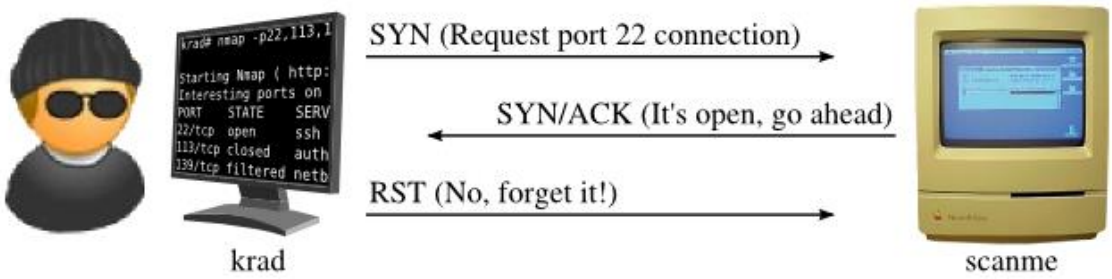
-PR (ARP/Neighbor Discovery)

```
┌──(davide㉿kali)-[~]
└─$ sudo nmap -PR 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 17:06 CEST
Nmap scan report for 192.168.50.101
Host is up (0.000099s 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: 08:00:27:7F:1D:B7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
```

-sP (opzione -sn, ovvero senza port scan).

Port scan dopo un host discovery e di mostrare gli host che hanno risposto. Quest'opzione è spesso conosciuta come «ping scan», ma si può anche richiedere il traceroute ed eseguire script host NSE. Quest'azione è un gradino più invadente della List Scan, e spesso può essere usata per lo stesso scopo. Essa permette una mappatura di una rete obiettivo senza attrarre molta attenzione. Sapere quanti host sono attivi è più utile ad un attaccante rispetto ad una semplice List Scan di ogni indirizzo IP e nome di host.

```
┌──(davide㉿kali)-[~]
└─$ nmap -sP 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 17:20 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00041s latency).
Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds
```


krad# nmap -p22,113,1
Starting Nmap (http:
Interesting ports on
PORT STATE SERV
22/tcp open ssh
113/tcp closed auth
139/tcp filtered netb
SYN (Request port 22 connection)
SYN/ACK (It's open, go ahead)
RST (No, forget it!)
krad
scanme