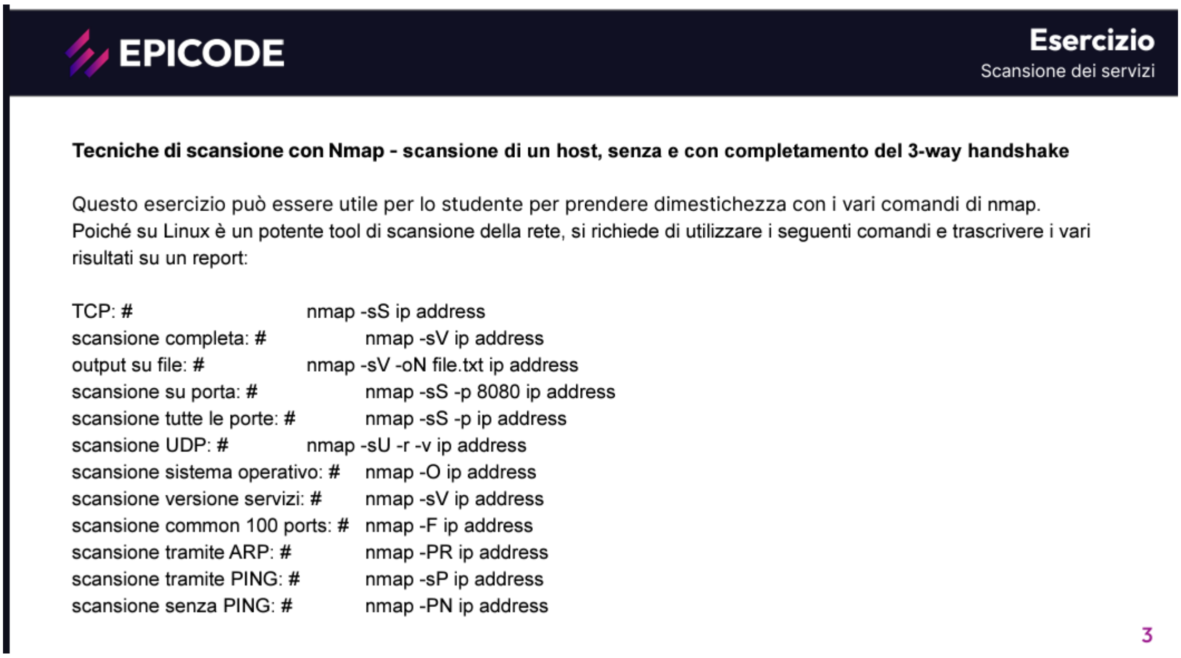
ESERCITAZIONE W11D4



EPICODE

Esercizio

Scansione dei servizi

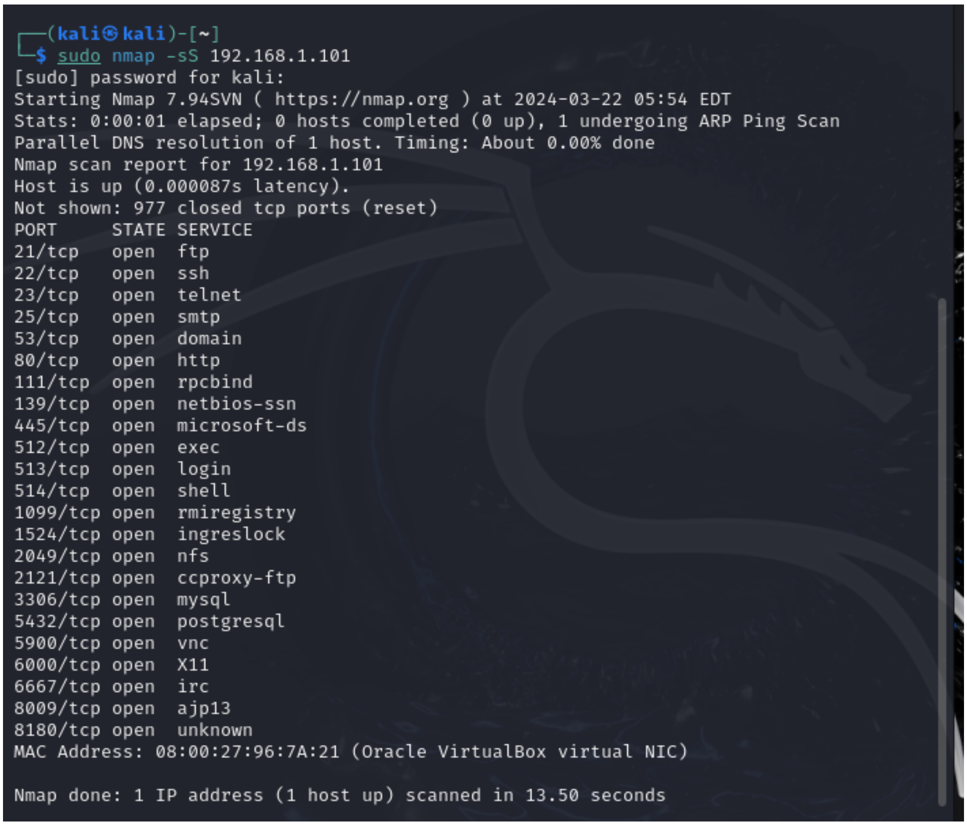
Tecniche di scansione con Nmap - scansione di un host, senza e con completamento del 3-way handshake

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
output su file: #	nmap -sV -oN file.txt ip address
scansione su porta: #	nmap -sS -p 8080 ip address
scansione tutte le porte: #	nmap -sS -p ip address
scansione UDP: #	nmap -sU -r -v ip address
scansione sistema operativo: #	nmap -O ip address
scansione versione servizi: #	nmap -sV ip address
scansione common 100 ports: #	nmap -F ip address
scansione tramite ARP: #	nmap -PR ip address
scansione tramite PING: #	nmap -sP ip address
scansione senza PING: #	nmap -PN ip address

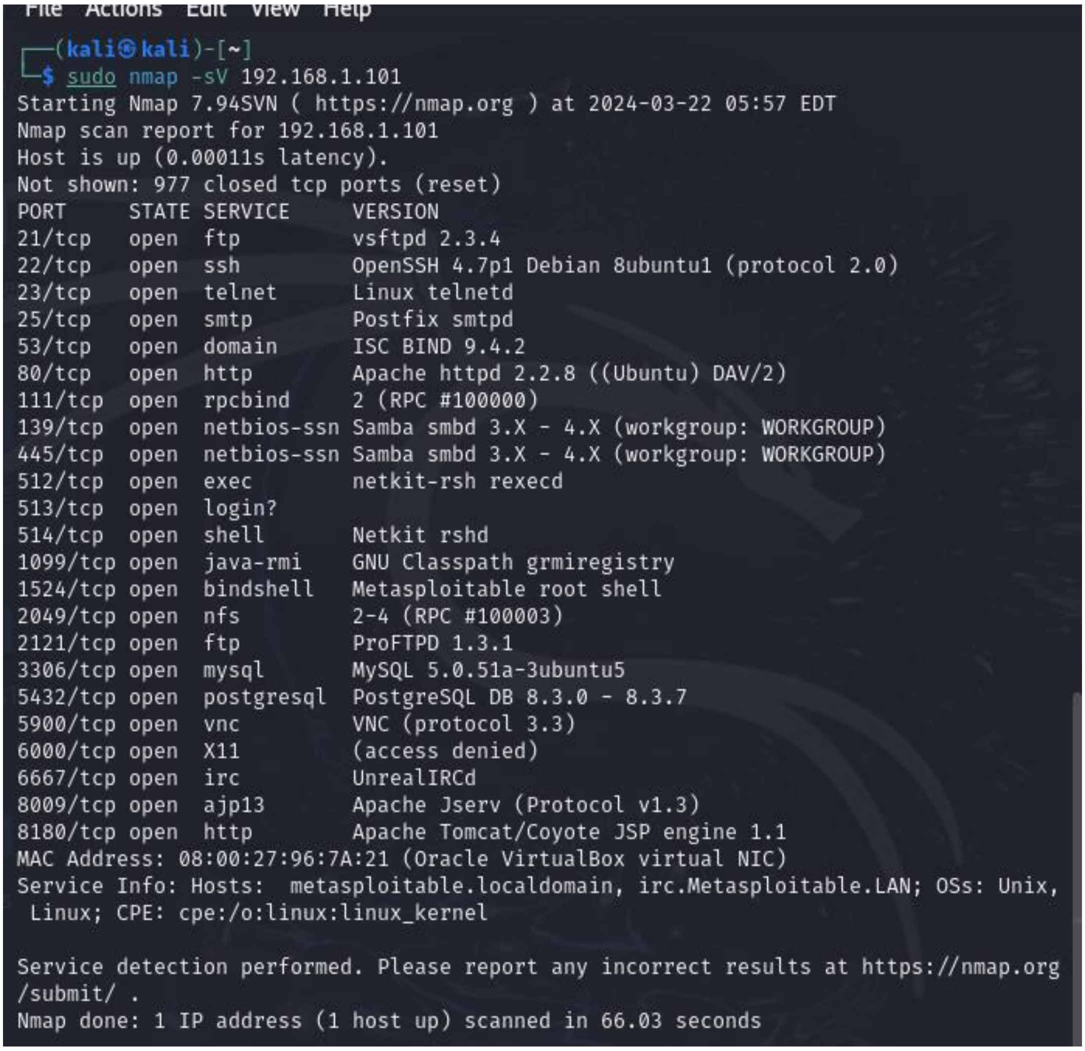
3

1) Scansione TCP



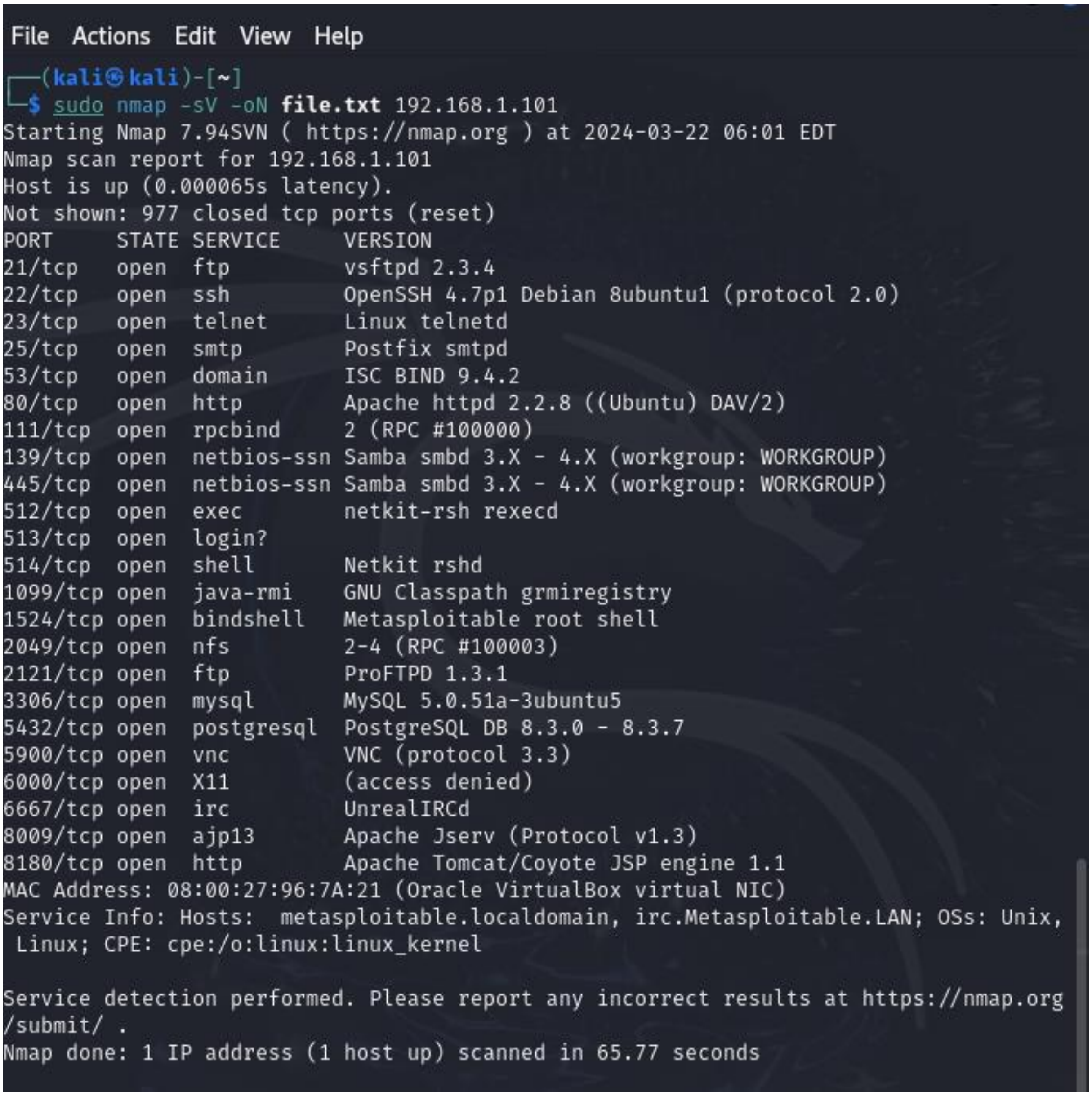
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.1.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-22 05:54 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.1.101
Host is up (0.000087s 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: 08:00:27:96:7A:21 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.50 seconds
```

2) Scansione completa



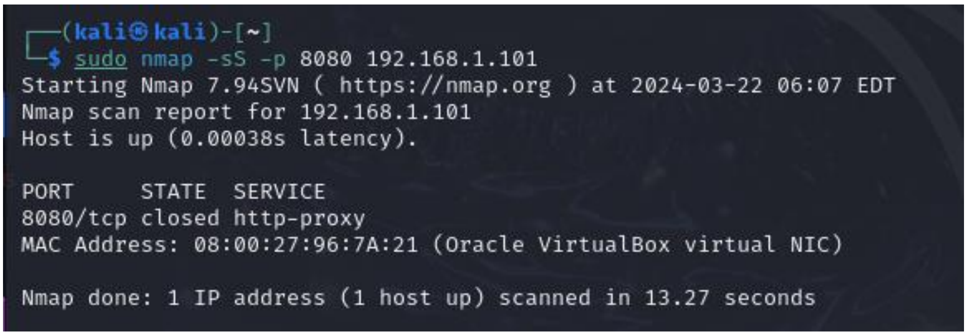
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-22 05:57 EDT
Nmap scan report for 192.168.1.101
Host is up (0.00011s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
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: 08:00:27:96:7A:21 (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 66.03 seconds
```

3) Scansione output su file



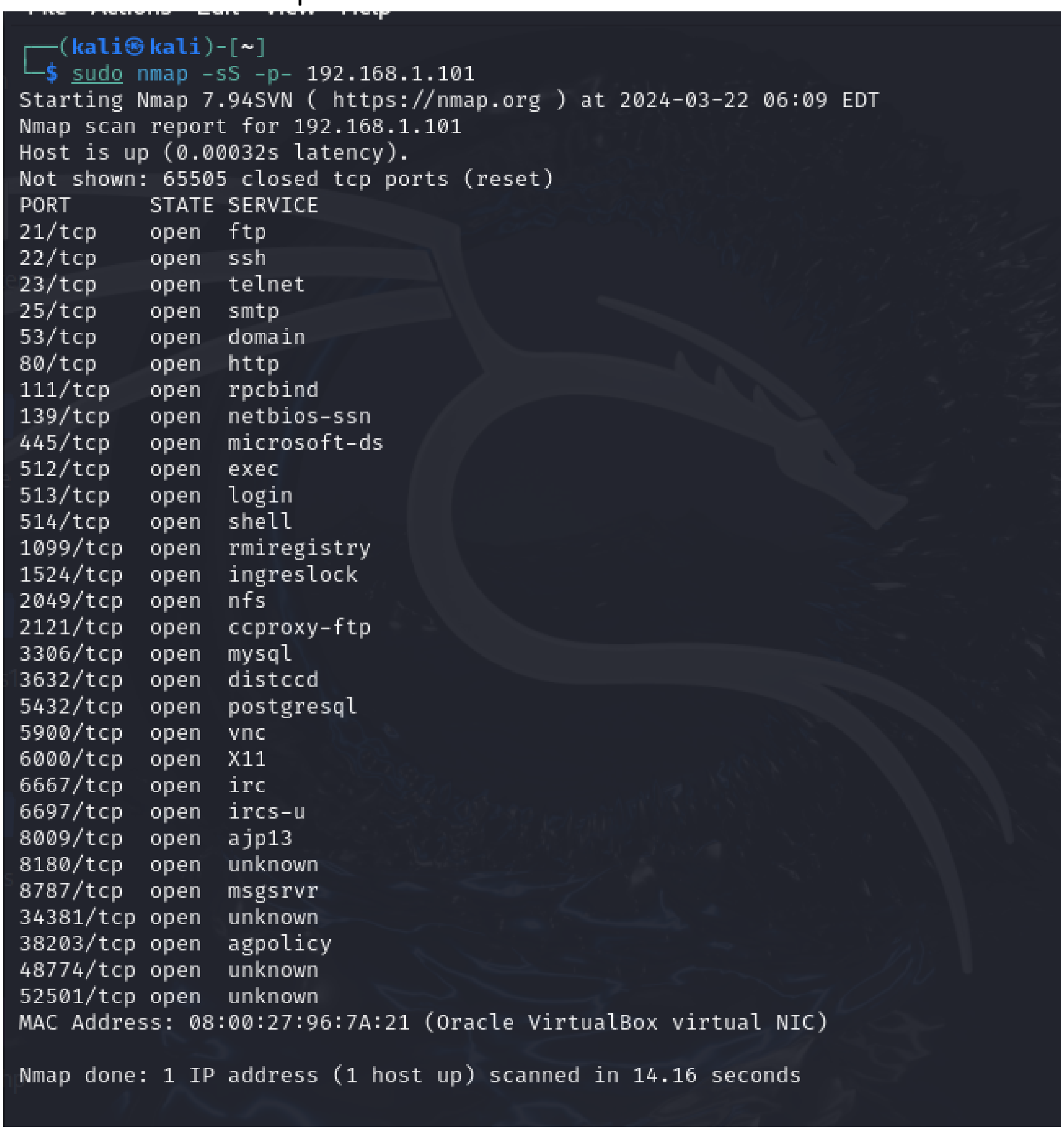
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -oN file.txt 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-22 06:01 EDT
Nmap scan report for 192.168.1.101
Host is up (0.000065s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         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: 08:00:27:96:7A:21 (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 65.77 seconds
```

4) Scansione su porta



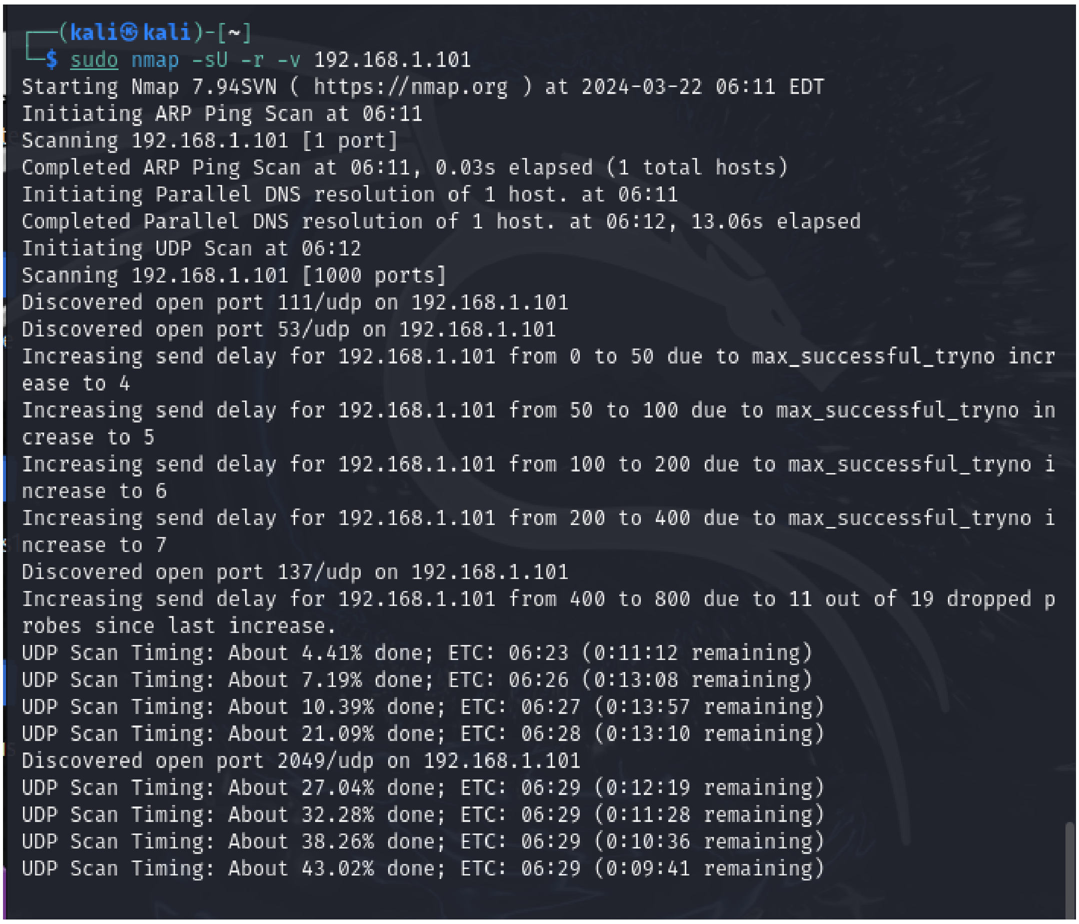
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p 8080 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-22 06:07 EDT
Nmap scan report for 192.168.1.101
Host is up (0.00038s latency).

PORT     STATE  SERVICE
8080/tcp closed http-proxy
MAC Address: 08:00:27:96:7A:21 (Oracle VirtualBox virtual NIC)

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

5) Scansione su tutte le porte



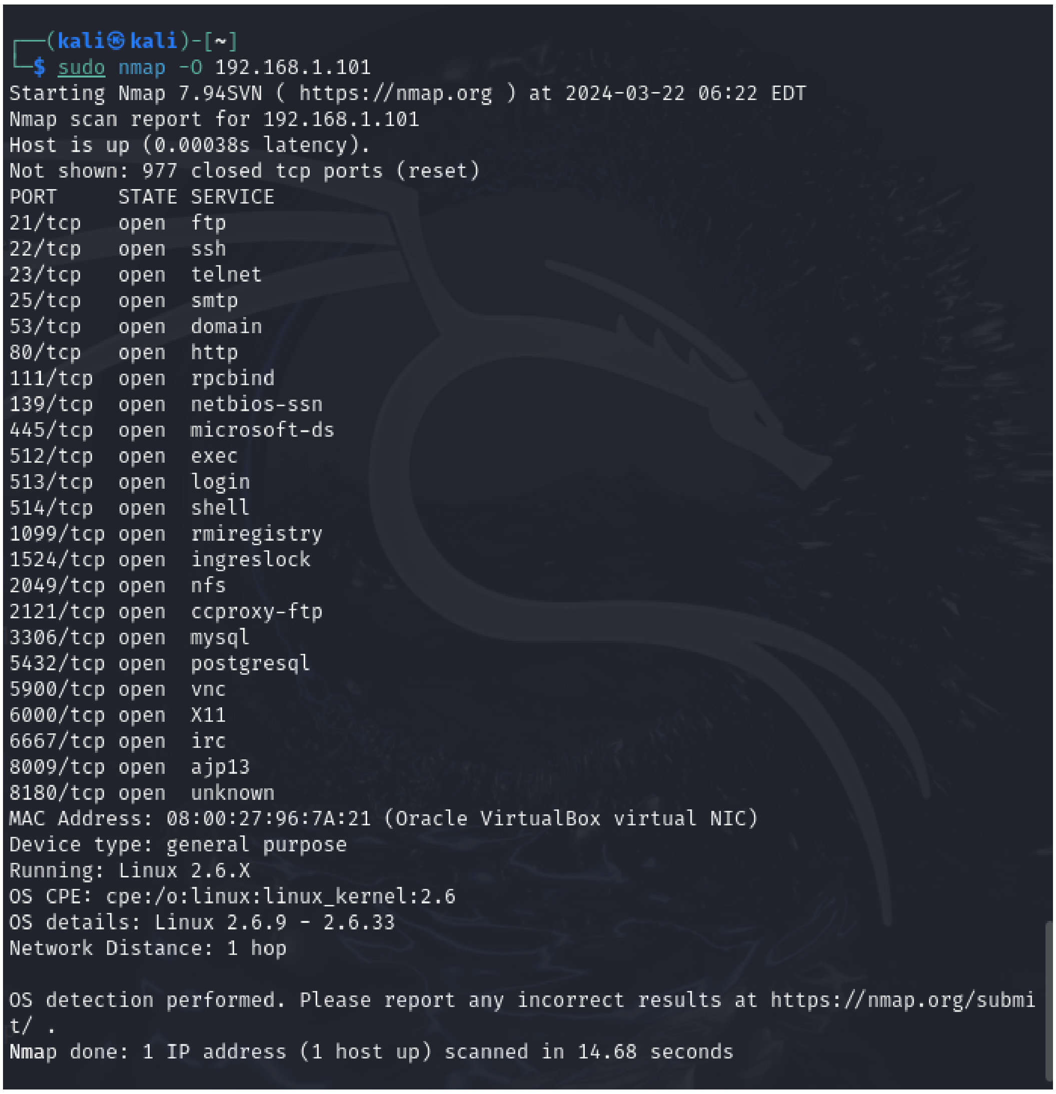
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p- 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-22 06:09 EDT
Nmap scan report for 192.168.1.101
Host is up (0.00032s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
34381/tcp open  unknown
38203/tcp open  agpolicy
48774/tcp open  unknown
52501/tcp open  unknown
MAC Address: 08:00:27:96:7A:21 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.16 seconds
```

6) Scansione UDP



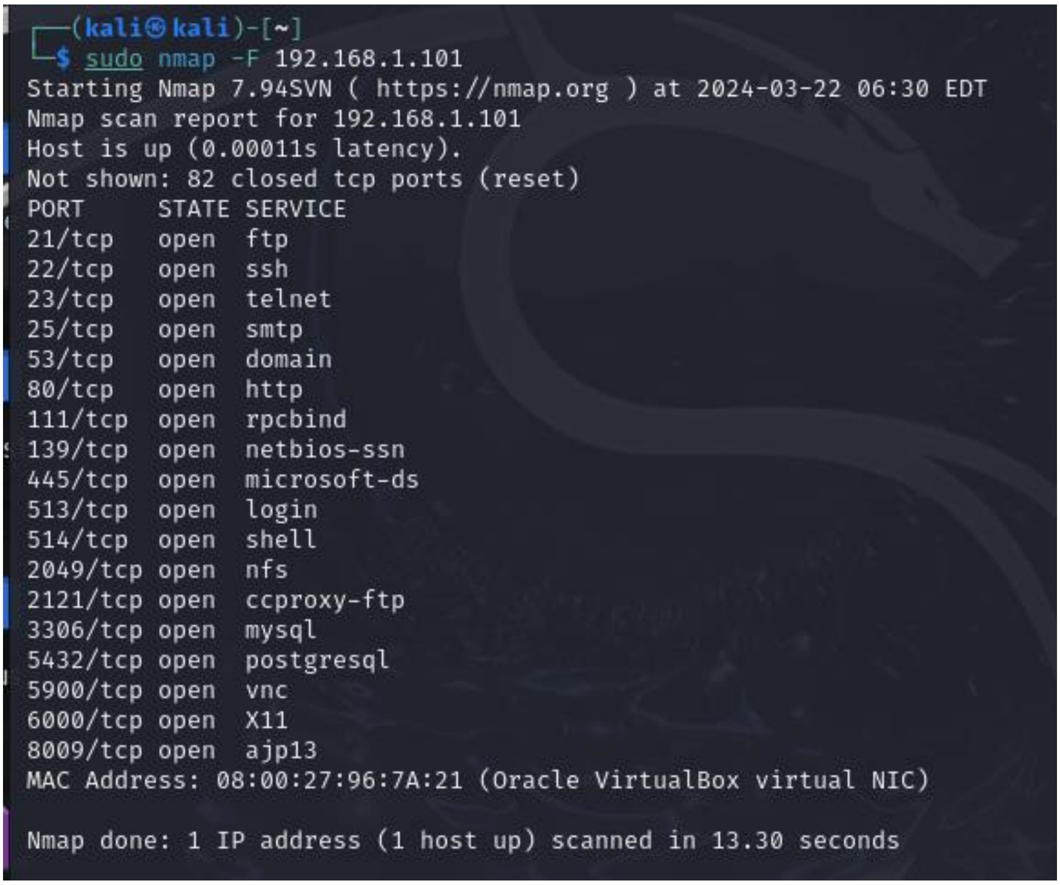
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU -r -v 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-22 06:11 EDT
Initiating ARP Ping Scan at 06:11
Scanning 192.168.1.101 [1 port]
Completed ARP Ping Scan at 06:11, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:11
Completed Parallel DNS resolution of 1 host. at 06:12, 13.06s elapsed
Initiating UDP Scan at 06:12
Scanning 192.168.1.101 [1000 ports]
Discovered open port 111/udp on 192.168.1.101
Discovered open port 53/udp on 192.168.1.101
Increasing send delay for 192.168.1.101 from 0 to 50 due to max_successful_tryno incr
ease to 4
Increasing send delay for 192.168.1.101 from 50 to 100 due to max_successful_tryno in
crease to 5
Increasing send delay for 192.168.1.101 from 100 to 200 due to max_successful_tryno i
ncrease to 6
Increasing send delay for 192.168.1.101 from 200 to 400 due to max_successful_tryno i
ncrease to 7
Discovered open port 137/udp on 192.168.1.101
Increasing send delay for 192.168.1.101 from 400 to 800 due to 11 out of 19 dropped p
robes since last increase.
UDP Scan Timing: About 4.41% done; ETC: 06:23 (0:11:12 remaining)
UDP Scan Timing: About 7.19% done; ETC: 06:26 (0:13:08 remaining)
UDP Scan Timing: About 10.39% done; ETC: 06:27 (0:13:57 remaining)
UDP Scan Timing: About 21.09% done; ETC: 06:28 (0:13:10 remaining)
Discovered open port 2049/udp on 192.168.1.101
UDP Scan Timing: About 27.04% done; ETC: 06:29 (0:12:19 remaining)
UDP Scan Timing: About 32.28% done; ETC: 06:29 (0:11:28 remaining)
UDP Scan Timing: About 38.26% done; ETC: 06:29 (0:10:36 remaining)
UDP Scan Timing: About 43.02% done; ETC: 06:29 (0:09:41 remaining)
```

7) Scansione sistema operativo



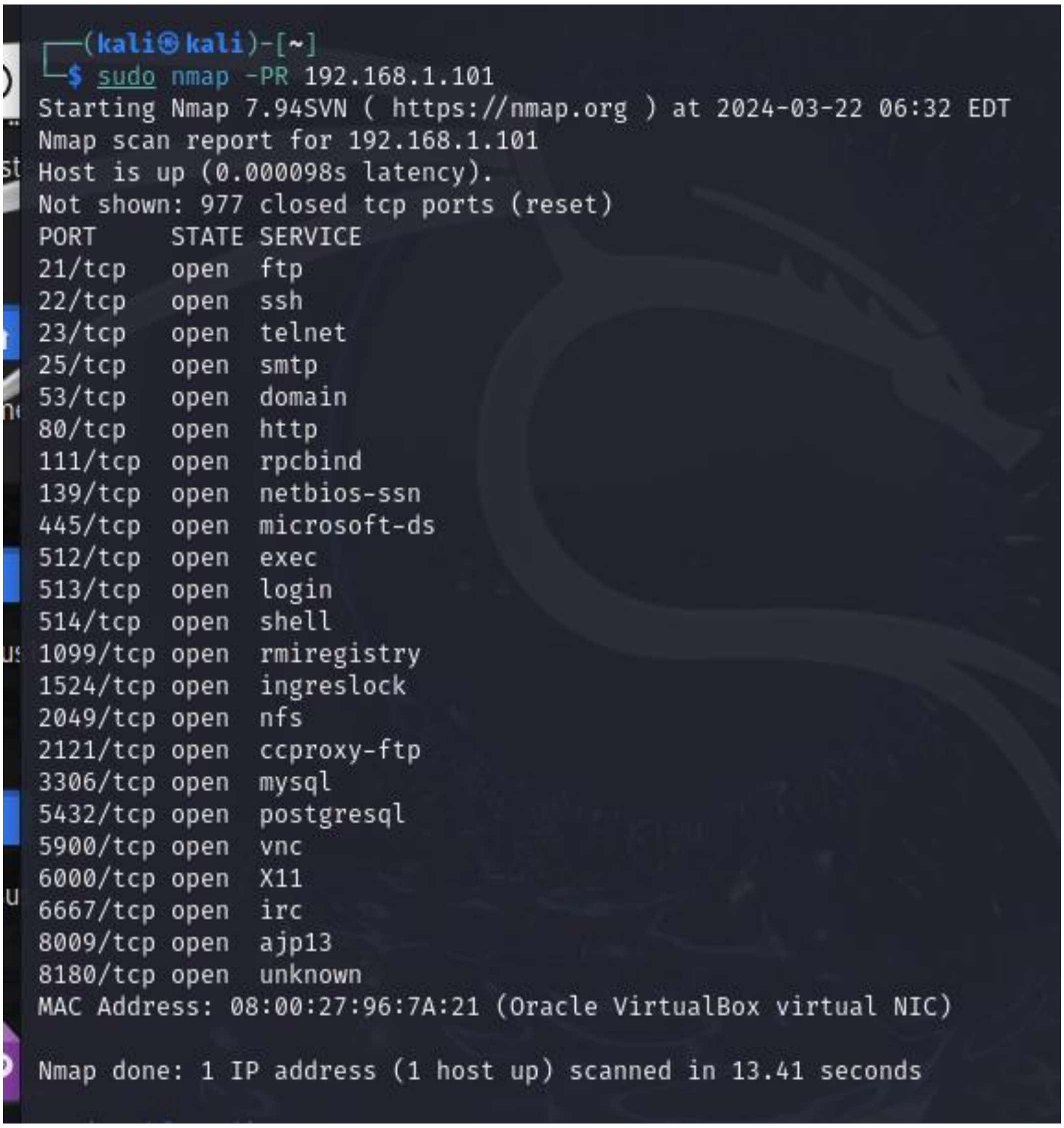
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-22 06:22 EDT
Nmap scan report for 192.168.1.101
Host is up (0.00038s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  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: 08:00:27:96:7A:21 (Oracle VirtualBox virtual NIC)
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/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 14.68 seconds
```

8) Scansione common 100 ports



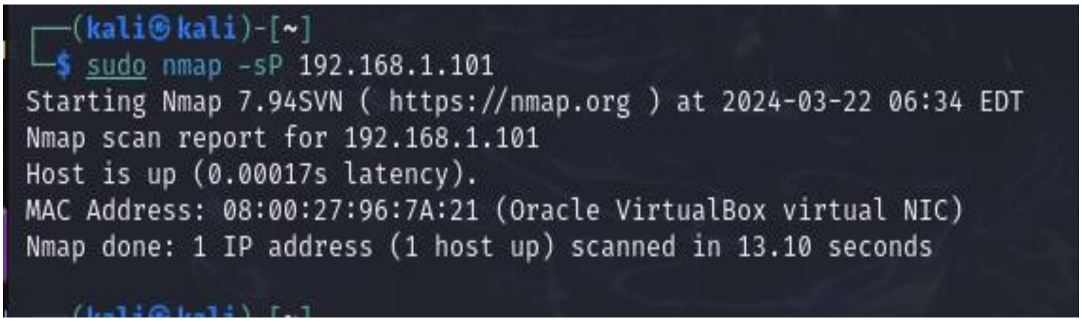
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -F 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-22 06:30 EDT
Nmap scan report for 192.168.1.101
Host is up (0.00011s latency).
Not shown: 82 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  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: 08:00:27:96:7A:21 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
```

9) Scansione tramite ARP



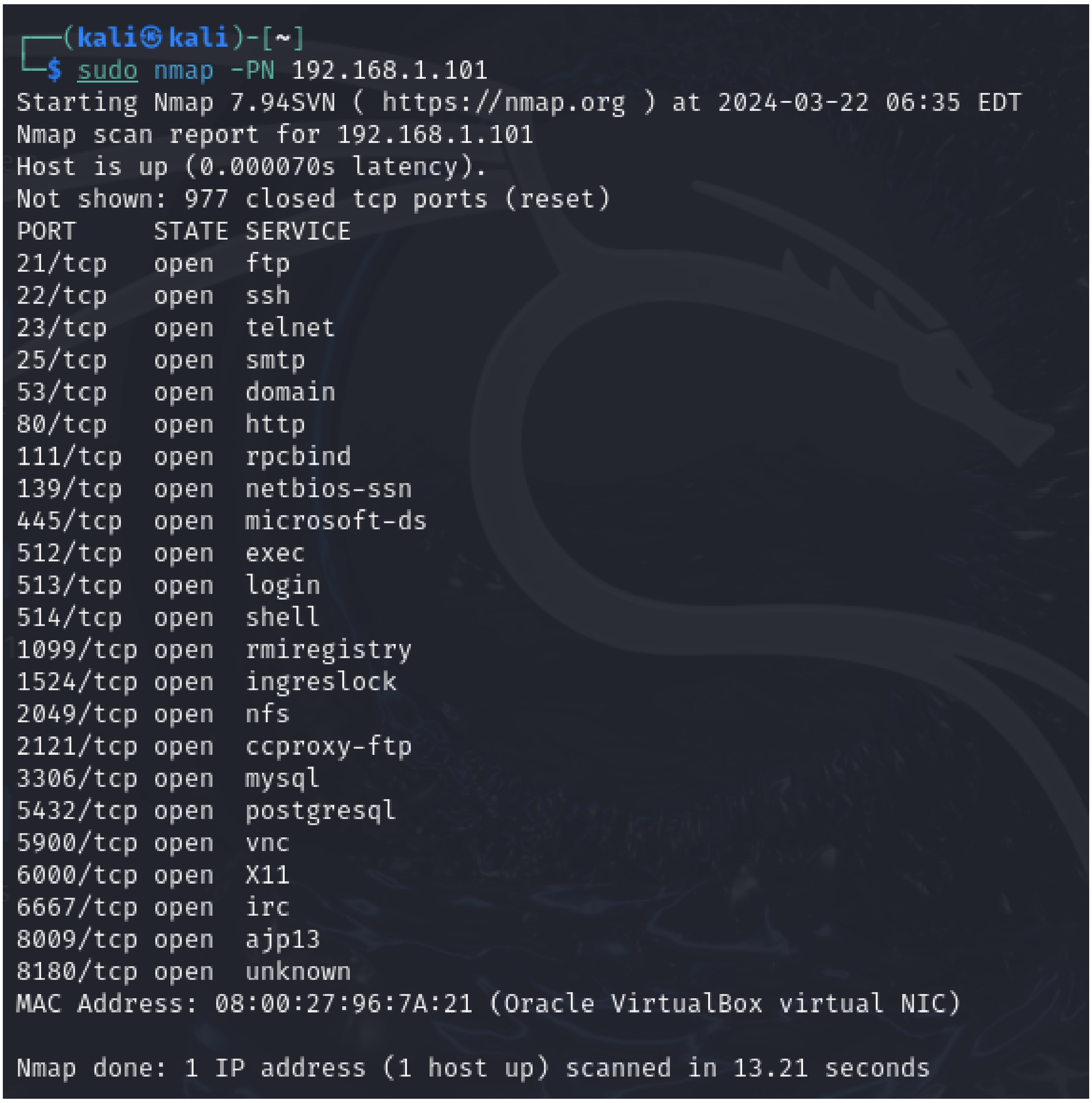
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -PR 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-22 06:32 EDT
Nmap scan report for 192.168.1.101
Host is up (0.000098s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  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: 08:00:27:96:7A:21 (Oracle VirtualBox virtual NIC)

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

10) Scansione tramite PING



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sP 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-22 06:34 EDT
Nmap scan report for 192.168.1.101
Host is up (0.00017s latency).
MAC Address: 08:00:27:96:7A:21 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.10 seconds

┌──(kali㉿kali)-[~]
```

11) Scansione senza PING



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -PN 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-22 06:35 EDT
Nmap scan report for 192.168.1.101
Host is up (0.000070s 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: 08:00:27:96:7A:21 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.21 seconds
```

IP TARGET	OS	TIPO SCANSIONE	COMANDO	PORTE APERTE	PORTE CHIUSE	MAC ADDRESS
192.168.1.101	METASPLOITABLE	TCP	Nmap -sS	23	977	08:00:27:96:7A:21
192.168.1.101	METASPLOITABLE	completa	Nmap -sV	23	977	08:00:27:96:7A:21
192.168.1.101	METASPLOITABLE	Output su file	Nmap –sV –oN file.txt	23	977	08:00:27:96:7A:21
192.168.1.101	METASPLOITABLE	su porta	Nmap –sS –p 8080	23	977	08:00:27:96:7A:21
192.168.1.101	METASPLOITABLE	Su tutte le porte	Nmap –sS -p	30	65505	08:00:27:96:7A:21
192.168.1.101	METASPLOITABLE	UDP	Nmap –sU –r -v	3	-	08:00:27:96:7A:21
192.168.1.101	METASPLOITABLE	Sistema operativo	Nmap -O	-	-	08:00:27:96:7A:21
192.168.1.101	METASPLOITABLE	Common 100 ports	Nmap -F	18	82	08:00:27:96:7A:21
192.168.1.101	METASPLOITABLE	ARP	Nmap -PR	23	977	08:00:27:96:7A:21
192.168.1.101	METASPLOITABLE	Tramite PING	Nmap -sP	-	-	08:00:27:96:7A:21
192.168.1.101	METASPLOITABLE	Senza PING	Nmap -PN	23	977	08:00:27:96:7A:21