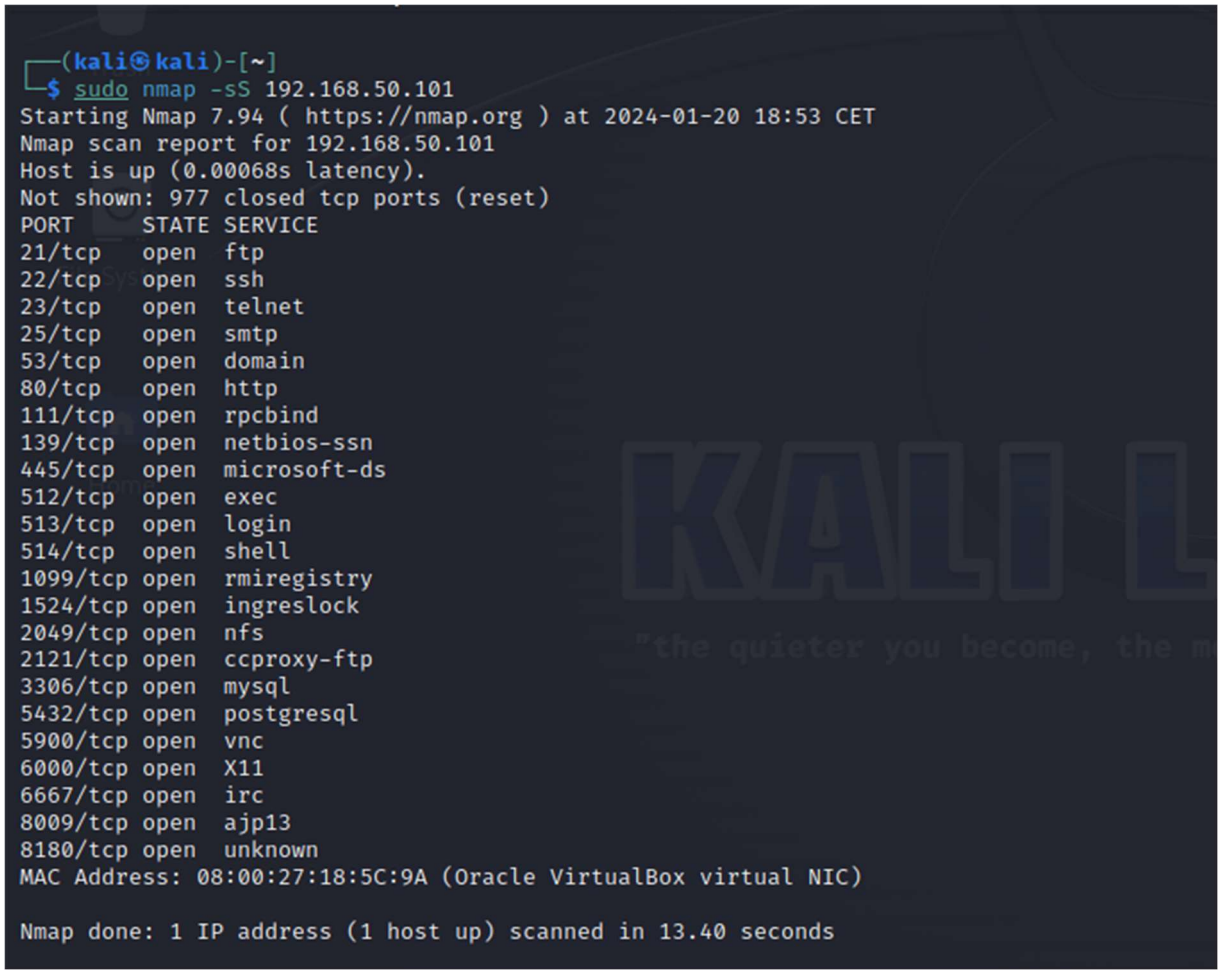
Traccia

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:

1. TCP: # nmap -sS ip address,sT
2. scansione completa: # nmap -sV ip address
3. output su file: # nmap -sV -oN file.txt ip address
4. scansione su porta: # nmap -sS -p 8080 ip address
5. scansione tutte le porte: # nmap -sS -p ip address
6. scansione UDP: # nmap -sU -r -v ip address
7. scansione sistema operativo: # nmap -O ip address
8. scansione versione servizi: # nmap -sV ip address
9. scansione common 100 ports: # nmap -F ip address
10. scansione tramite ARP: # nmap -PR ip address
11. scansione tramite PING: # nmap -sP ip address
12. scansione senza PING: # nmap -PN ip address

1.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-20 18:54 CET
Nmap scan report for 192.168.50.101
Host is up (0.0013s 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: 08:00:27:18:5C:9A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.40 seconds
```

2.

```
└─$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-20 18:57 CET
Nmap scan report for 192.168.50.101
Host is up (0.00028s 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: 08:00:27:18:5C:9A (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 66.67 seconds
```

3.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -oN file.txt 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-20 19:11 CET
Nmap scan report for 192.168.50.101
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (conn-refused)
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
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 66.48 seconds
```

4.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p 8080 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-20 19:15 CET
Nmap scan report for 192.168.50.101
Host is up (0.00054s latency).

PORT     STATE  SERVICE
8080/tcp closed http-proxy
MAC Address: 08:00:27:18:5C:9A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.28 seconds
```

5.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -P 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-21 10:14 CET
Nmap scan report for 192.168.50.101
Host is up (0.00031s 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: 08:00:27:18:5C:9A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.46 seconds
```

6.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU -r -v 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-20 19:21 CET
Initiating ARP Ping Scan at 19:21
Scanning 192.168.50.101 [1 port]
Completed ARP Ping Scan at 19:21, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:21
Completed Parallel DNS resolution of 1 host. at 19:21, 13.00s elapsed
Initiating UDP Scan at 19:21
Scanning 192.168.50.101 [1000 ports]
Discovered open port 53/udp on 192.168.50.101
Discovered open port 111/udp on 192.168.50.101
Increasing send delay for 192.168.50.101 from 0 to 50 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.50.101 from 50 to 100 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.50.101 from 100 to 200 due to max_successful_tryno increase to 6
Increasing send delay for 192.168.50.101 from 200 to 400 due to max_successful_tryno increase to 7
Increasing send delay for 192.168.50.101 from 400 to 800 due to 11 out of 12 dropped probes since last increase.
Discovered open port 137/udp on 192.168.50.101
UDP Scan Timing: About 3.66% done; ETC: 19:35 (0:13:37 remaining)
UDP Scan Timing: About 19.99% done; ETC: 19:37 (0:12:53 remaining)
Discovered open port 2049/udp on 192.168.50.101
UDP Scan Timing: About 26.14% done; ETC: 19:37 (0:12:03 remaining)
UDP Scan Timing: About 32.72% done; ETC: 19:37 (0:11:08 remaining)
UDP Scan Timing: About 38.48% done; ETC: 19:38 (0:10:16 remaining)
UDP Scan Timing: About 44.14% done; ETC: 19:38 (0:09:23 remaining)
UDP Scan Timing: About 49.38% done; ETC: 19:38 (0:08:32 remaining)
UDP Scan Timing: About 54.52% done; ETC: 19:38 (0:07:41 remaining)
UDP Scan Timing: About 59.76% done; ETC: 19:38 (0:06:49 remaining)
UDP Scan Timing: About 65.11% done; ETC: 19:38 (0:05:56 remaining)
UDP Scan Timing: About 69.98% done; ETC: 19:38 (0:05:04 remaining)
UDP Scan Timing: About 75.31% done; ETC: 19:38 (0:04:10 remaining)
UDP Scan Timing: About 80.67% done; ETC: 19:38 (0:03:17 remaining)
UDP Scan Timing: About 85.90% done; ETC: 19:38 (0:02:23 remaining)
UDP Scan Timing: About 91.04% done; ETC: 19:38 (0:01:31 remaining)
```

```
UDP Scan Timing: About 85.90% done; ETC: 19:38 (0:02:23 remaining)
UDP Scan Timing: About 91.04% done; ETC: 19:38 (0:01:31 remaining)
UDP Scan Timing: About 96.19% done; ETC: 19:38 (0:00:39 remaining)
Completed UDP Scan at 19:38, 1053.17s elapsed (1000 total ports)
Nmap scan report for 192.168.50.101
Host is up (0.00071s latency).
Not shown: 994 closed udp ports (port-unreach)
PORT     STATE         SERVICE
53/udp   open          domain
69/udp   open|filtered tftp
111/udp  open          rpcbind
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
2049/udp open          nfs
MAC Address: 08:00:27:18:5C:9A (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1066.46 seconds
           Raw packets sent: 1446 (66.532KB) | Rcvd: 1090 (79.483KB)

┌──(kali㉿kali)-[~]
```

7.

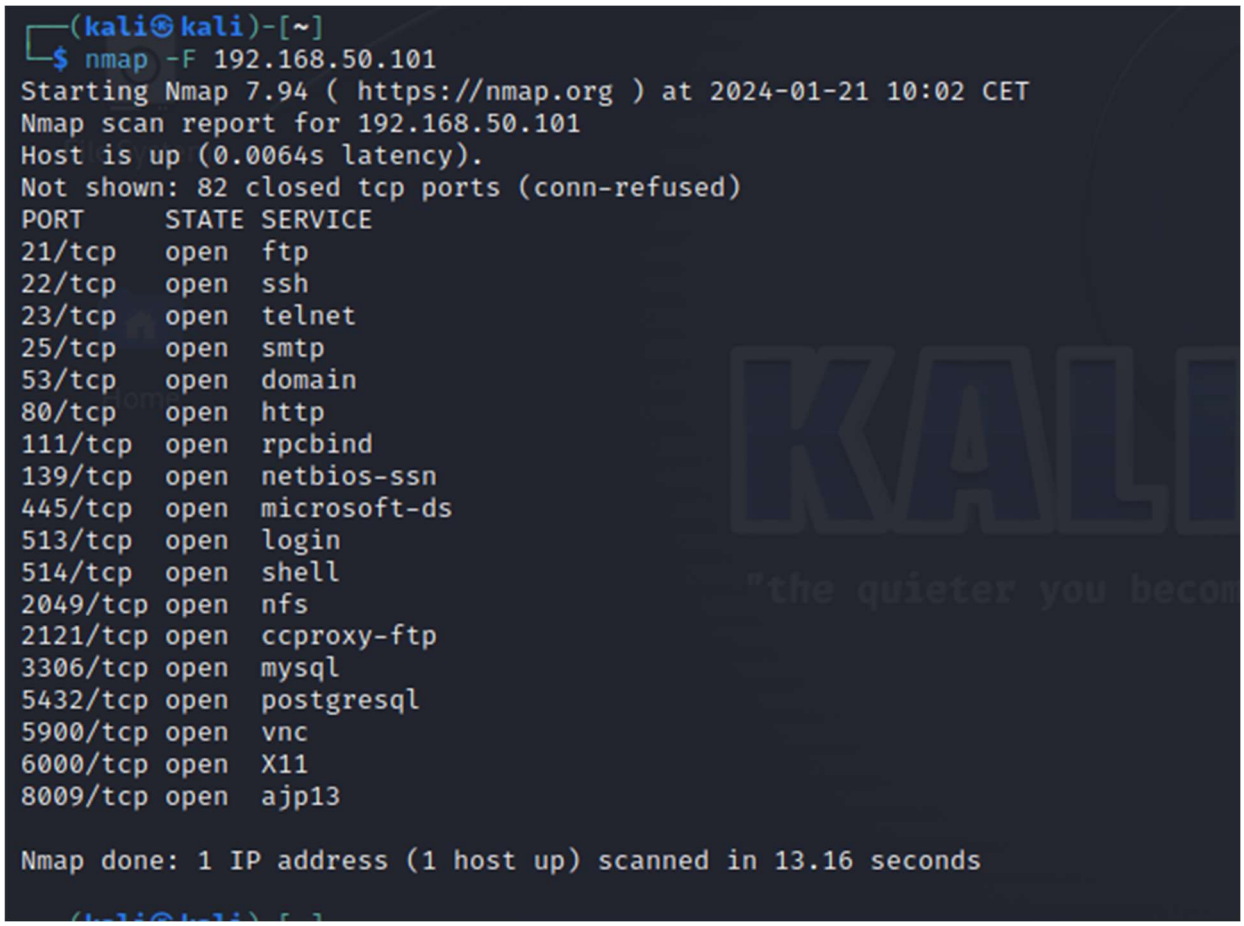
```
└─$ sudo nmap -O 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-20 19:45 CET
Nmap scan report for 192.168.50.101
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   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: 08:00:27:18:5C:9A (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
```

```
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: 08:00:27:18:5C:9A (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/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.03 seconds

┌──(kali㉿kali)-[~]
```

8.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-21 09:59 CET
Nmap scan report for 192.168.50.101
Host is up (0.0033s latency).
Not shown: 977 closed tcp ports (conn-refused)
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
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 66.94 seconds
```

9.


(kali㉿kali)-[~]
$ nmap -F 192.168.50.101
Starting Nmap 7.94 (https://nmap.org) at 2024-01-21 10:02 CET
Nmap scan report for 192.168.50.101
Host is up (0.0064s latency).
Not shown: 82 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
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 13.16 seconds

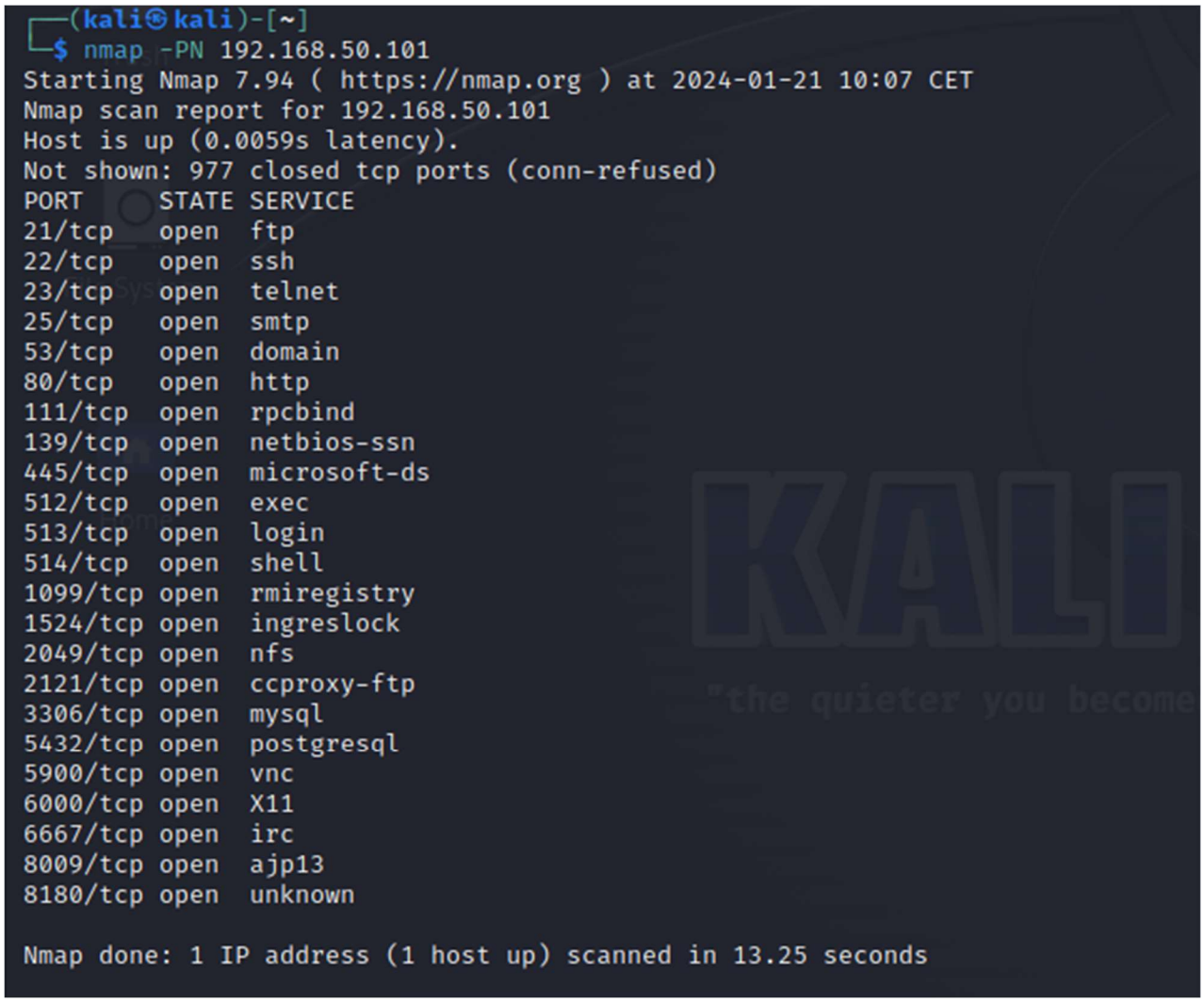
10.

```
┌──(kali㉿kali)-[~]
└─$ nmap -PR 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-21 10:04 CET
Nmap scan report for 192.168.50.101
Host is up (0.0012s 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 13.35 seconds
```

11.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-21 10:05 CET
Nmap scan report for 192.168.50.101
Host is up (0.0013s latency).
Nmap done: 1 IP address (1 host up) scanned in 13.00 seconds
```

12.


(kali㉿kali)-[~]
$ nmap -PN 192.168.50.101
Starting Nmap 7.94 (https://nmap.org) at 2024-01-21 10:07 CET
Nmap scan report for 192.168.50.101
Host is up (0.0059s 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 13.25 seconds