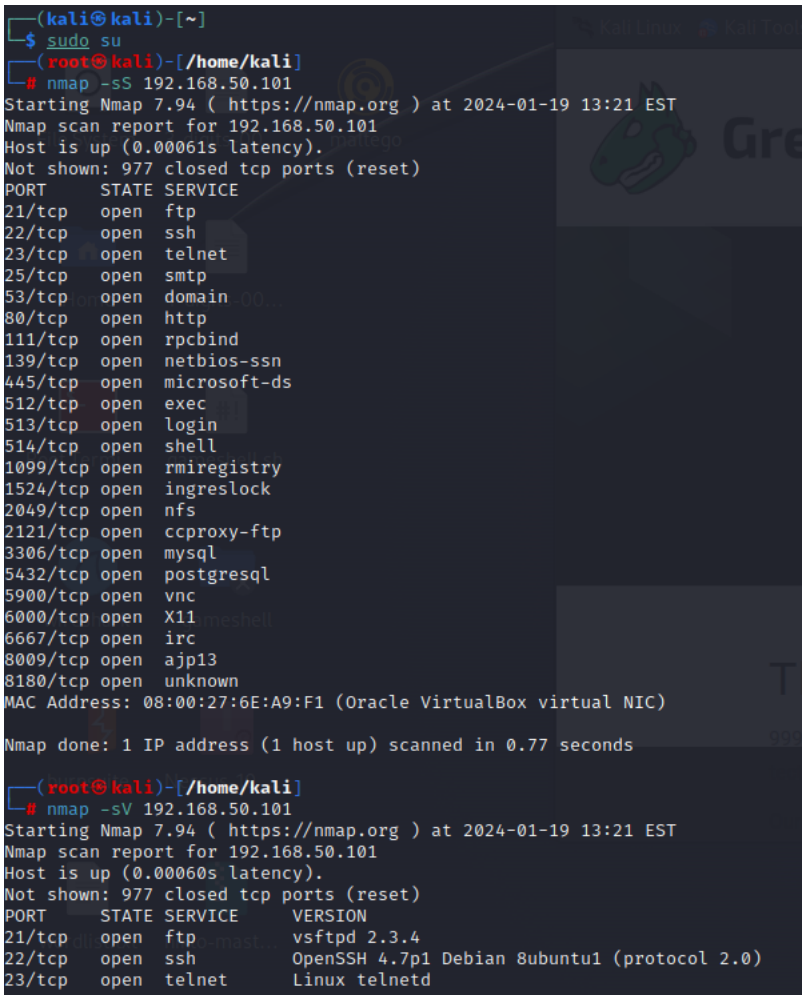
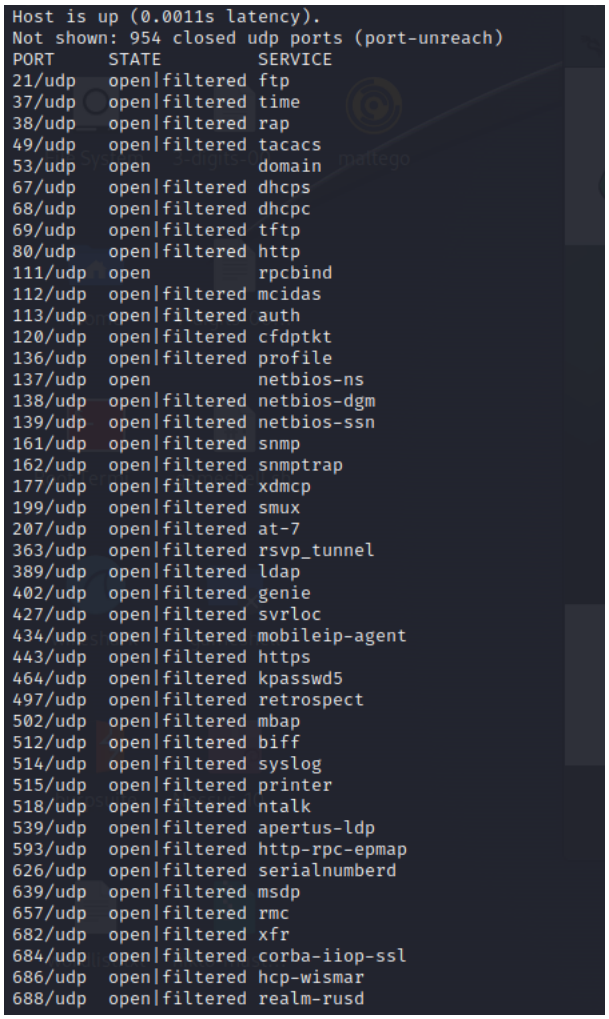


```
┌──(kali㉿kali)-[~]
└─$ sudo su
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 13:21 EST
Nmap scan report for 192.168.50.101
Host is up (0.00061s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
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: 08:00:27:6E:A9:F1 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 13:21 EST
Nmap scan report for 192.168.50.101
Host is up (0.00060s 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
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 13:21 EST
Nmap scan report for 192.168.50.101
Host is up (0.00060s 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       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: 08:00:27:6E:A9:F1 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OS
s: 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 12.54 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -oN file.txt 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 13:23 EST
Nmap scan report for 192.168.50.101
Host is up (0.00055s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
```



```
Host is up (0.0011s latency).
Not shown: 954 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
177/udp  open|filtered xdmcp
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
514/udp  open|filtered syslog
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
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -oN file.txt 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 13:23 EST
Nmap scan report for 192.168.50.101
Host is up (0.00055s 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  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: 08:00:27:6E:A9:F1 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OS
s: 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 12.24 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -p 8080 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 13:25 EST
Nmap scan report for 192.168.50.101
Host is up (0.00097s latency).

PORT     STATE  SERVICE    VERSION
8080/tcp closed http-proxy
MAC Address: 08:00:27:6E:A9:F1 (Oracle VirtualBox virtual NIC)
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -p 8080 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 13:26 EST
Nmap scan report for 192.168.50.101
Host is up (0.00087s latency).

PORT     STATE  SERVICE
8080/tcp closed http-proxy
MAC Address: 08:00:27:6E:A9:F1 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -p 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 13:26 EST
Error #487: Your port specifications are illegal.  Example of proper form: "
-100,200-1024,T:3000-4000,U:60000-"
QUITTING!

┌──(root㉿kali)-[/home/kali]
└─# nmap -sU -r -v 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 13:26 EST
Initiating ARP Ping Scan at 13:26
Scanning 192.168.50.101 [1 port]
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sU -r -v 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 13:26 EST
Initiating ARP Ping Scan at 13:26
Scanning 192.168.50.101 [1 port]
Completed ARP Ping Scan at 13:26, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:26
Completed Parallel DNS resolution of 1 host. at 13:26, 0.01s elapsed
Initiating UDP Scan at 13:26
Scanning 192.168.50.101 [1000 ports]
Discovered open port 111/udp on 192.168.50.101
Discovered open port 53/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
Discovered open port 137/udp on 192.168.50.101
Increasing send delay for 192.168.50.101 from 50 to 100 due to 11 out of 12
dropped probes since last increase.
Increasing send delay for 192.168.50.101 from 100 to 200 due to 11 out of 12
 dropped probes since last increase.
UDP Scan Timing: About 9.55% done; ETC: 13:32 (0:04:54 remaining)
Increasing send delay for 192.168.50.101 from 200 to 400 due to 11 out of 11
 dropped probes since last increase.
Increasing send delay for 192.168.50.101 from 400 to 800 due to 11 out of 11
 dropped probes since last increase.
UDP Scan Timing: About 13.28% done; ETC: 13:34 (0:06:38 remaining)
UDP Scan Timing: About 16.10% done; ETC: 13:36 (0:07:54 remaining)
UDP Scan Timing: About 18.92% done; ETC: 13:37 (0:08:39 remaining)
Discovered open port 2049/udp on 192.168.50.101
UDP Scan Timing: About 25.90% done; ETC: 13:39 (0:09:12 remaining)
UDP Scan Timing: About 39.18% done; ETC: 13:40 (0:08:34 remaining)
UDP Scan Timing: About 46.28% done; ETC: 13:41 (0:07:51 remaining)
UDP Scan Timing: About 52.58% done; ETC: 13:41 (0:07:06 remaining)
UDP Scan Timing: About 58.00% done; ETC: 13:41 (0:06:19 remaining)
UDP Scan Timing: About 63.75% done; ETC: 13:42 (0:05:32 remaining)
UDP Scan Timing: About 69.18% done; ETC: 13:42 (0:04:45 remaining)
UDP Scan Timing: About 74.62% done; ETC: 13:42 (0:03:57 remaining)
UDP Scan Timing: About 80.05% done; ETC: 13:42 (0:03:08 remaining)
UDP Scan Timing: About 85.18% done; ETC: 13:42 (0:02:21 remaining)
UDP Scan Timing: About 90.40% done; ETC: 13:42 (0:01:32 remaining)
UDP Scan Timing: About 95.53% done; ETC: 13:42 (0:00:43 remaining)
Completed UDP Scan at 13:43, 1026.92s elapsed (1000 total ports)
Nmap scan report for 192.168.50.101
Host is up (0.0011s latency).
Not shown: 954 closed udp ports (port-unreach)
PORT      STATE         SERVICE
21/udp    open|filtered ftp
37/udp    open|filtered time
```

```
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
177/udp  open|filtered xdmcp
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
514/udp  open|filtered syslog
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
764/udp  open|filtered omserv
2049/udp open          nfs
MAC Address: 08:00:27:6E:A9:F1 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1027.12 seconds
           Raw packets sent: 1750 (79.523KB) | Rcvd: 1049 (76.892KB)
```

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 13:34 EST
Nmap scan report for 192.168.50.101
Host is up (0.00070s 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: 08:00:27:6E:A9:F1 (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 1.80 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 13:36 EST
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 47.83% done; ETC: 13:36 (0:00:07 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.00080s 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       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: 08:00:27:6E:A9:F1 (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 11.55 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -F 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 13:37 EST
Nmap scan report for 192.168.50.101
Host is up (0.00036s 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: 08:00:27:6E:A9:F1 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap - PR 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 13:38 EST
Failed to resolve "-".
Bare '-': did you put a space between '--'?
Failed to resolve "PR".
Nmap scan report for 192.168.50.101
Host is up (0.00029s 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
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -PN 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 13:40 EST
Nmap scan report for 192.168.50.101
Host is up (0.00036s 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: 08:00:27:6E:A9:F1 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -PR 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 13:39 EST
Nmap scan report for 192.168.50.101
Host is up (0.00035s 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: 08:00:27:6E:A9:F1 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sP 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 13:39 EST
Nmap scan report for 192.168.50.101
Host is up (0.00066s latency).
MAC Address: 08:00:27:6E:A9:F1 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```