SCAN nmap -sV -oN

```
Nmap 7.94 scan initiated Sun Aug 20 20:18:02 2023 as: nmap -sV -oN
Nmap scan report for 192.168.60.101
Host is up (0.017s 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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs:
Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed.
```

SCAN Nmap -sS -oN

```
# Nmap done at Sun Aug 20 20:18:20 2023 -- 1 IP
# Nmap 7.94 scan initiated Sun Aug 20 20:20:18 2023 as: nmap -sS -oN
Nmap scan report for 192.168.60.101
Host is up (0.017s 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
# Nmap done at Sun Aug 20 20:20:25 2023 -- 1 IP address (1 host up) scanned in
7.00 seconds
address (1 host up) scanned in 18.26 seconds
```

```
SCAN nmap -sS -p 8080 -oN
# Nmap 7.94 scan initiated Sun Aug 20 20:21:18 2023 as: nmap -sS -p 8080 -oN
Nmap scan report for 192.168.60.101
Host is up (0.0025s latency).
PORT     STATE  SERVICE
8080/tcp closed http-proxy
# Nmap done at Sun Aug 20 20:21:25 2023 -- 1 IP address (1 host up) scanned in
6.72 seconds
```

```
SCAN  nmap -sS -p- -oN
# Nmap 7.94 scan initiated Sun Aug 20 20:22:20 2023 as: nmap -sS -p- -oN
Nmap scan report for 192.168.60.101
Host is up (0.0091s latency).
Not shown: 65464 closed tcp ports (reset), 41 filtered tcp ports (no-response)
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
41366/tcp open  unknown
41952/tcp open  unknown
43013/tcp open  unknown
47446/tcp open  unknown
# Nmap done at Sun Aug 20 20:23:09 2023 -- 1 IP address (1 host up) scanned in
49.58 seconds
```

```
SCAN nmap -sU -r -v -oN
# Nmap 7.94 scan initiated Sun Aug 20 20:23:53 2023 as: nmap -sU -r -v -oN
Nmap scan report for 192.168.60.101
Host is up (0.033s 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
# Nmap done at Sun Aug 20 20:41:55 2023 -- 1 IP address (1 host up) scanned in
1081.42 seconds
```

SCAN nmap -O -oN

```
# Nmap 7.94 scan initiated Sun Aug 20 20:42:40 2023 as: nmap -O -oN
Nmap scan report for 192.168.60.101
Host is up (0.0055s 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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops
OS detection performed.
# Nmap done at Sun Aug 20 20:42:48 2023 -- 1 IP address (1 host up) scanned in
8.47 seconds
```

SCAN nmap -sT -oN

```
# Nmap 7.94 scan initiated Sun Aug 20 20:43:27 2023 as: nmap -sT -oN
Nmap scan report for 192.168.60.101
Host is up (0.022s 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 at Sun Aug 20 20:43:34 2023 -- 1 IP address (1 host up) scanned in
6.86 seconds
```

SCAN nmap -F -oN

```
# Nmap 7.94 scan initiated Sun Aug 20 20:44:05 2023 as: nmap -F -oN
Nmap scan report for 192.168.60.101
Host is up (0.0084s 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
# Nmap done at Sun Aug 20 20:44:12 2023 -- 1 IP address (1 host up) scanned in
6.66 seconds
```

SCAN  nmap -PR -oN

```
# Nmap 7.94 scan initiated Sun Aug 20 20:44:41 2023 as: nmap -PR -oN
Nmap scan report for 192.168.60.101
Host is up (0.018s 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
# Nmap done at Sun Aug 20 20:44:48 2023 -- 1 IP address (1 host up) scanned in
6.91 seconds
```

SCAN  nmap -sP -oN

```
# Nmap 7.94 scan initiated Sun Aug 20 20:45:13 2023 as: nmap -sP -oN
Nmap scan report for 192.168.60.101
Host is up (0.0025s latency).
# Nmap done at Sun Aug 20 20:45:20 2023 -- 1 IP address (1 host up) scanned in
6.58 seconds
```

SCAN  nmap -Pn -oN

```
#Nmap 7.94 scan initiated Sun Aug 20 20:45:44 2023 as: nmap -Pn -oN
Nmap scan report for 192.168.60.101
Host is up (0.018s 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
# Nmap done at Sun Aug 20 20:45:51 2023 -- 1 IP address (1 host up) scanned in
6.87 seconds
```