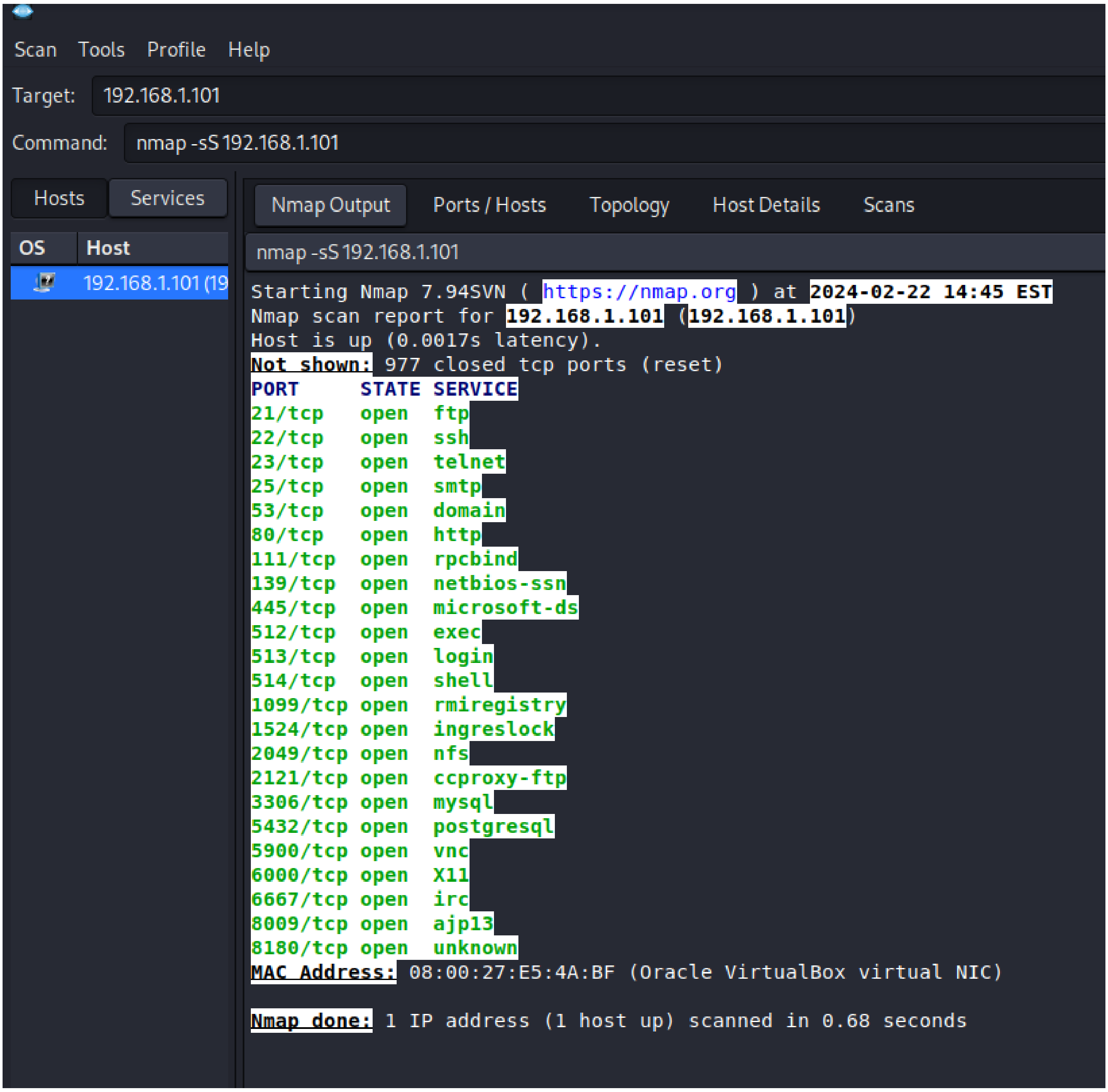
nmap -sS 192.168.1.101



Target: 192.168.1.101

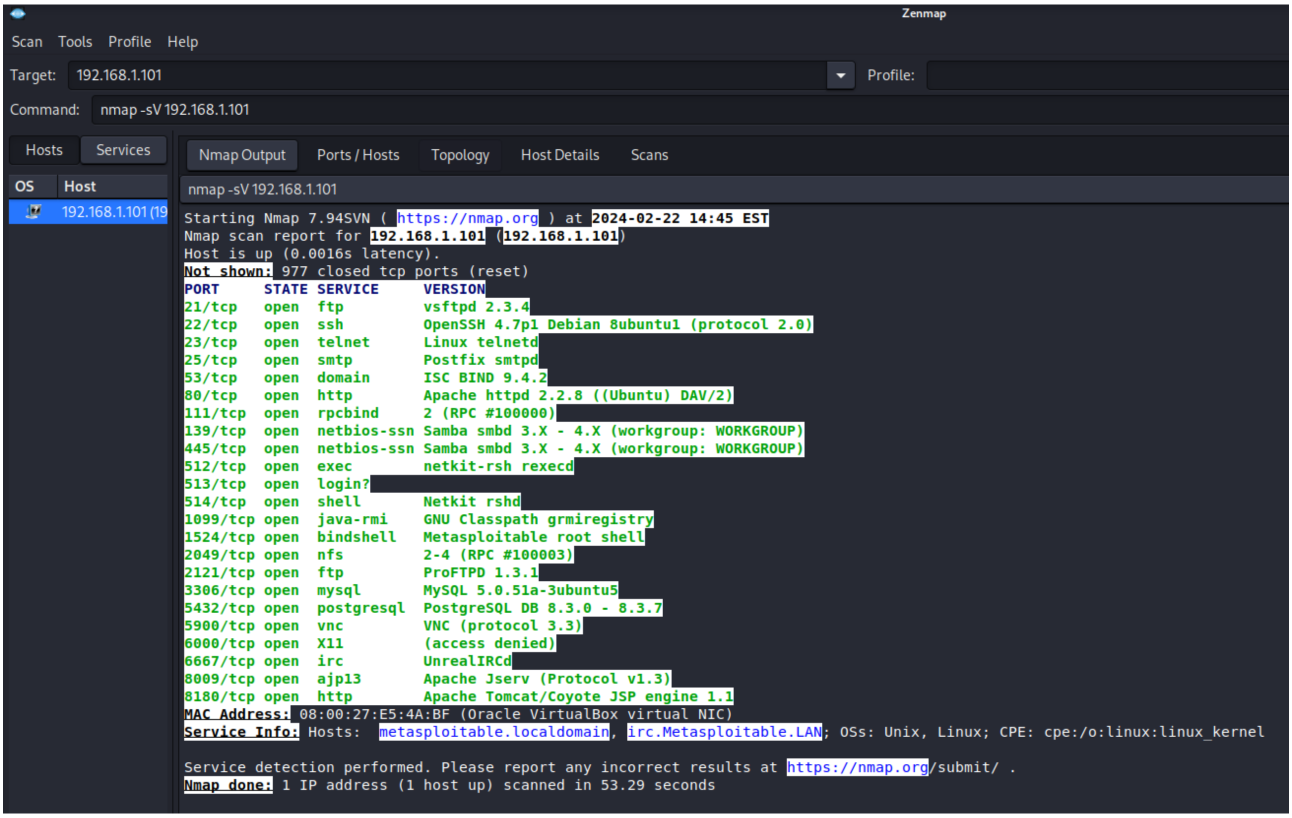
Command: nmap -sS 192.168.1.101

nmap -sS 192.168.1.101

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-22 14:45 EST
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.0017s 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:E5:4A:BF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds
```

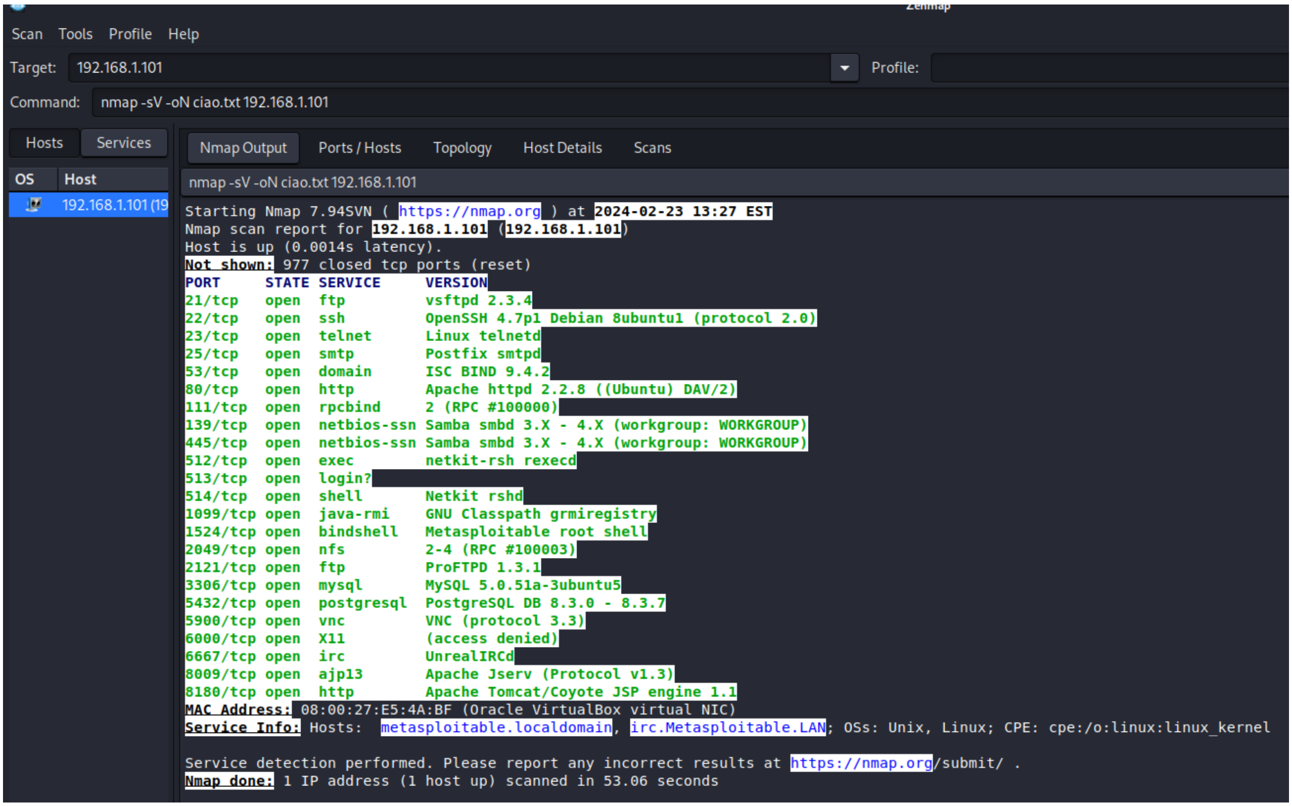
nmap -sV 192.168.1.101



```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-22 14:45 EST
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.0016s 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:E5:4A:BF (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 53.29 seconds
```

nmap -sV -oN file.txt 192.168.1.101



Target: 192.168.1.101

Profile:

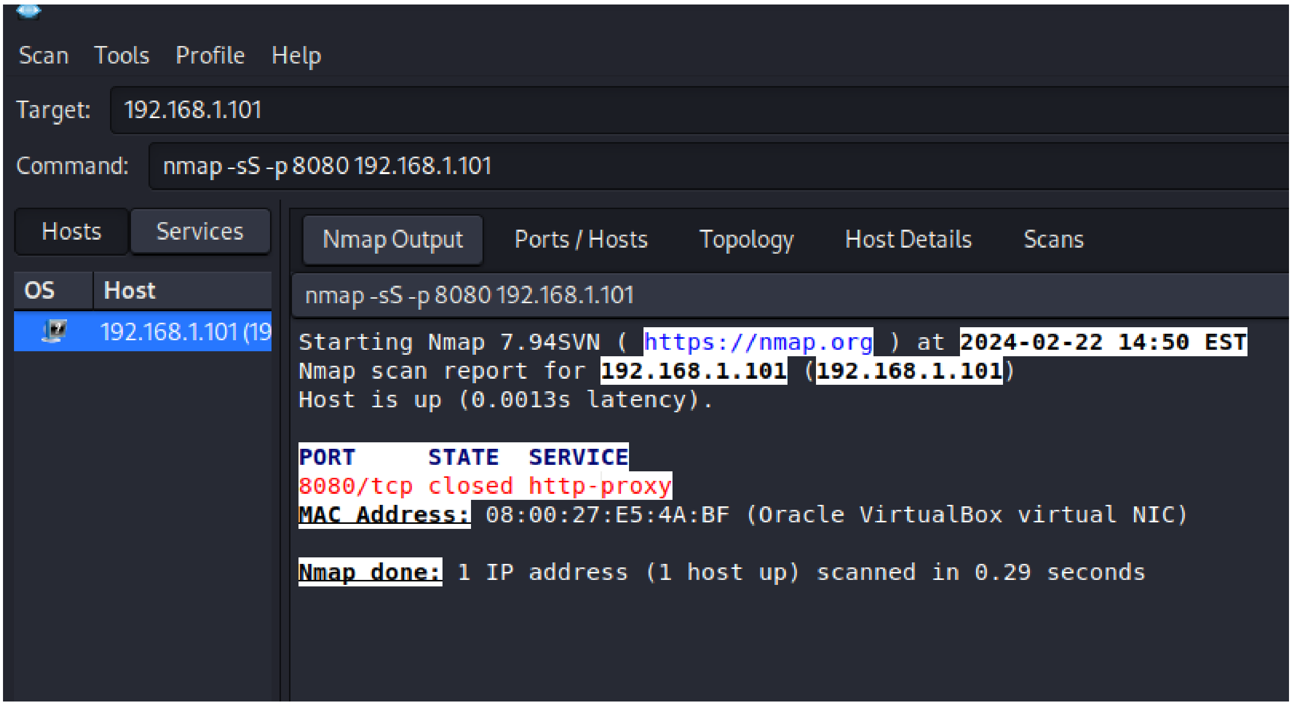
Command: nmap -sV -oN ciao.txt 192.168.1.101

nmap -sV -oN ciao.txt 192.168.1.101

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 13:27 EST
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.0014s 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:E5:4A:BF (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 53.06 seconds
```

nmap -sS -p 8080 192.168.1.101

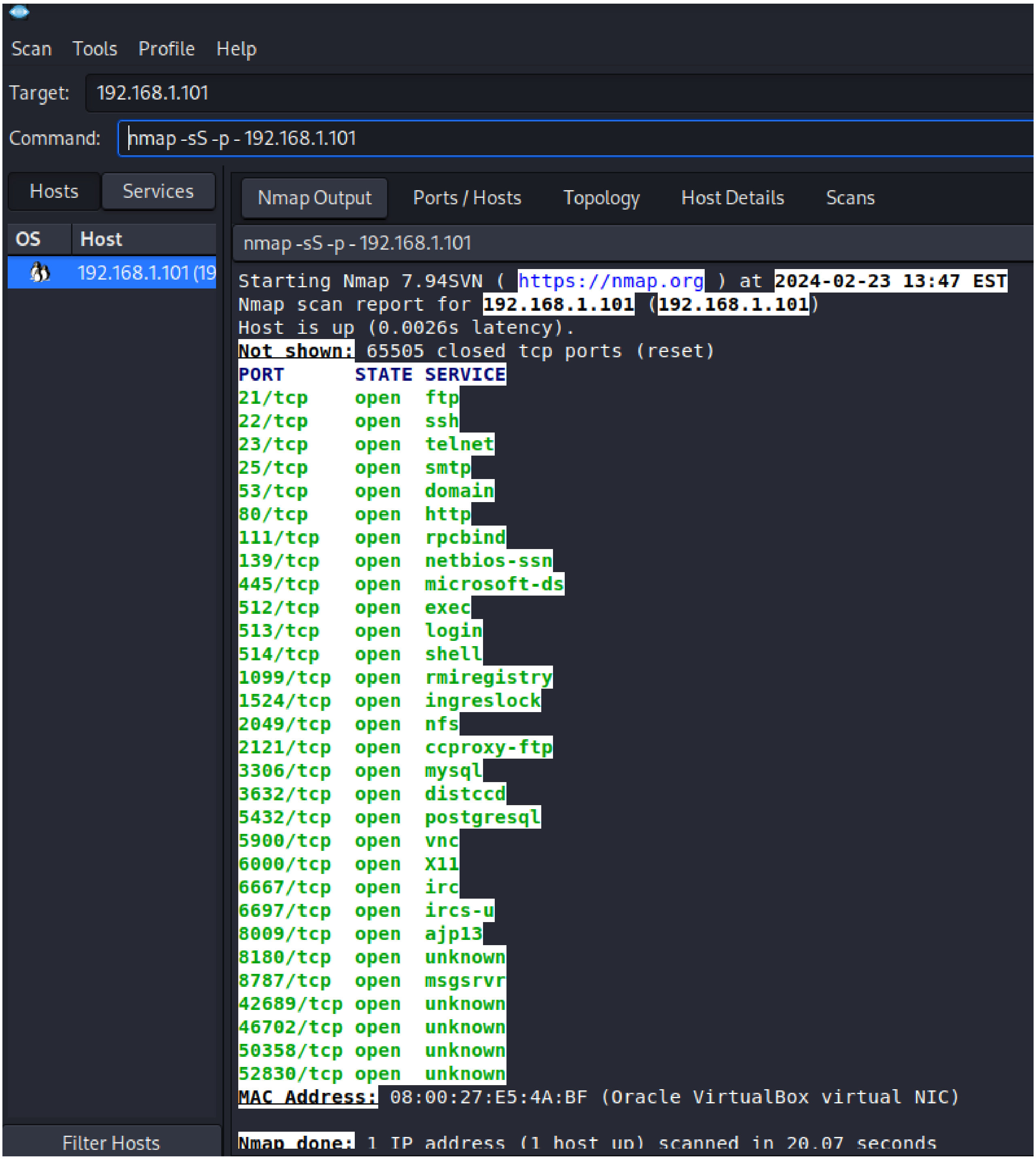


```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-22 14:50 EST
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.0013s latency).

PORT     STATE  SERVICE
8080/tcp closed http-proxy
MAC Address: 08:00:27:E5:4A:BF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
```

nmap -sS -p- 192.168.1.101

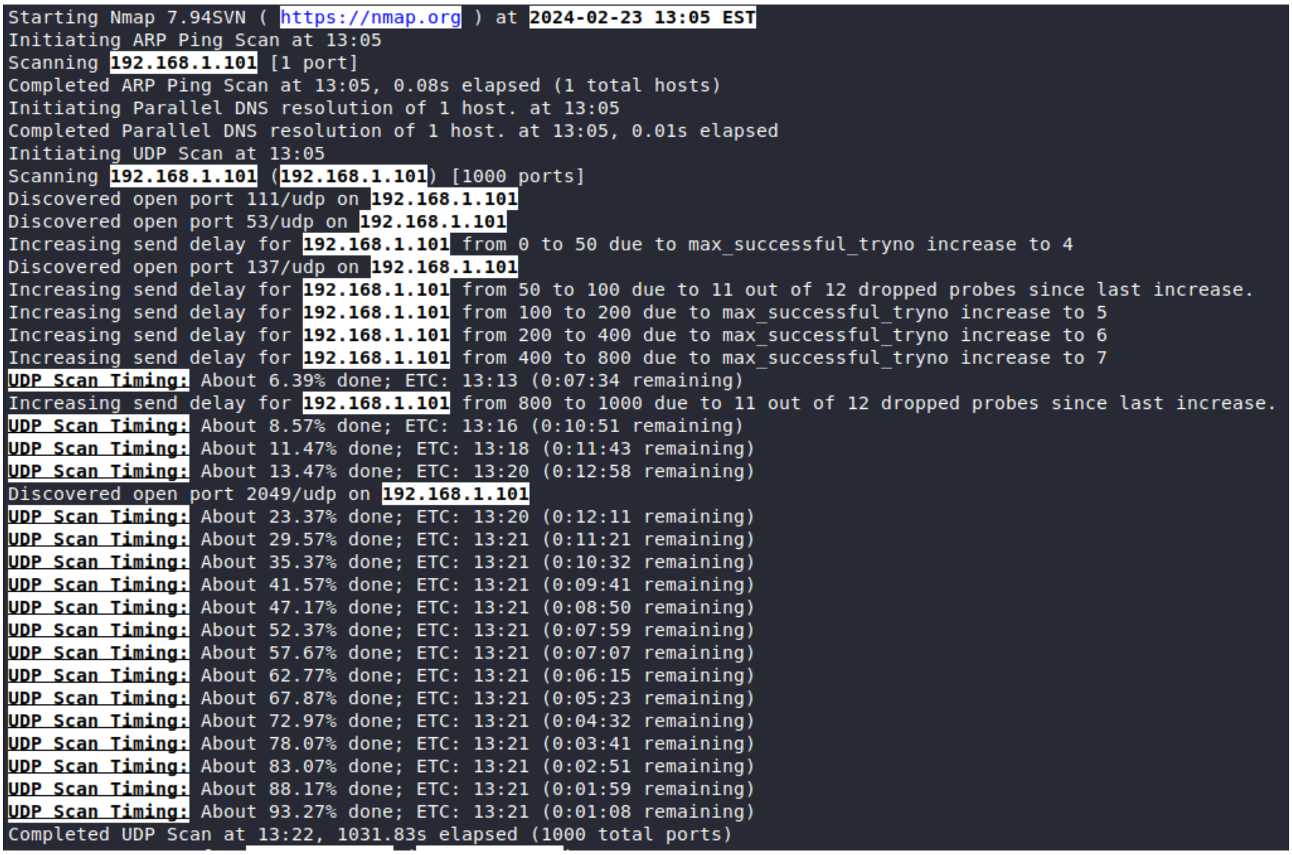


Command: nmap -sS -p - 192.168.1.101

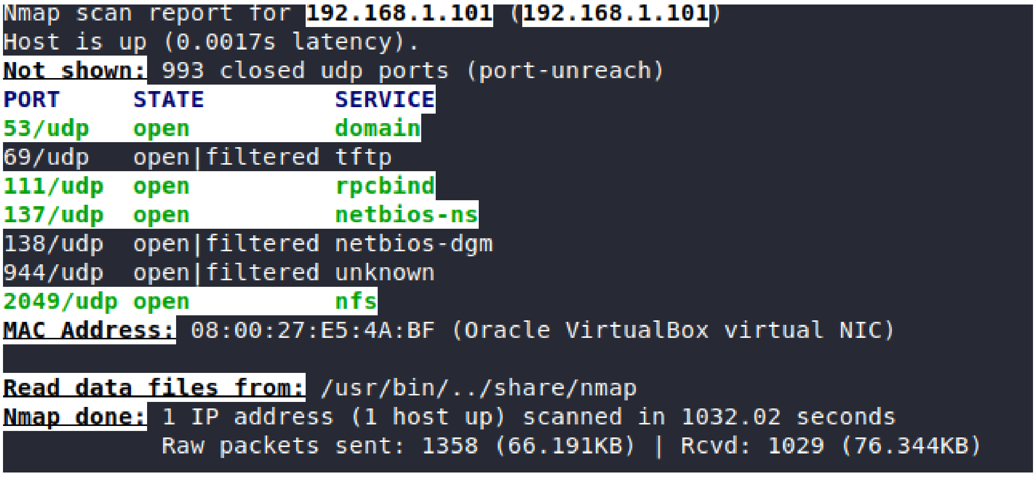
```
nmap -sS -p - 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 13:47 EST
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.0026s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  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
42689/tcp open  unknown
46702/tcp open  unknown
50358/tcp open  unknown
52830/tcp open  unknown
MAC Address: 08:00:27:E5:4A:BF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 20.07 seconds
```

nmap -sU -r -v 192.168.1.101



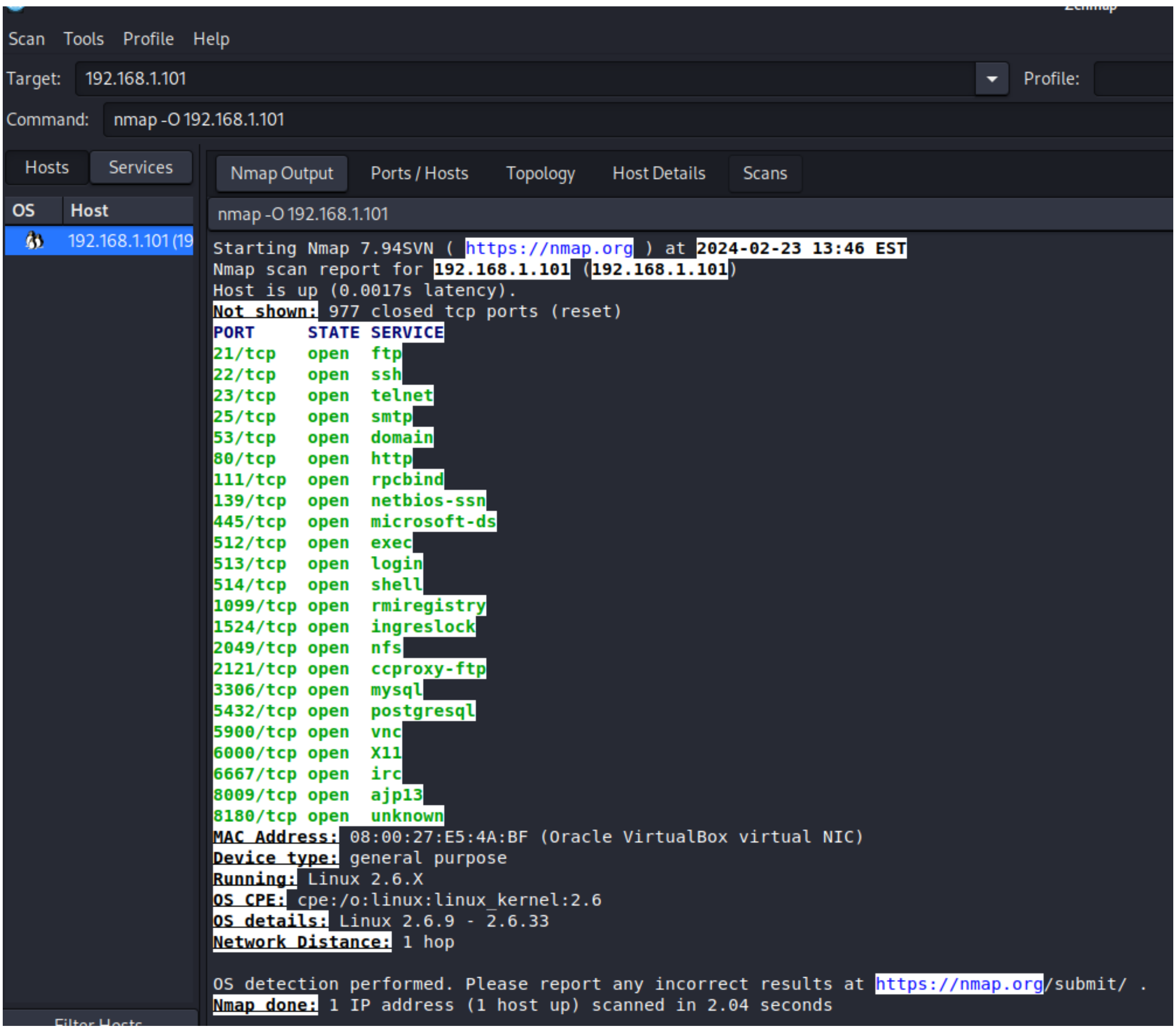
```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 13:05 EST
Initiating ARP Ping Scan at 13:05
Scanning 192.168.1.101 [1 port]
Completed ARP Ping Scan at 13:05, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:05
Completed Parallel DNS resolution of 1 host. at 13:05, 0.01s elapsed
Initiating UDP Scan at 13:05
Scanning 192.168.1.101 (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 increase to 4
Discovered open port 137/udp on 192.168.1.101
Increasing send delay for 192.168.1.101 from 50 to 100 due to 11 out of 12 dropped probes since last increase.
Increasing send delay for 192.168.1.101 from 100 to 200 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.1.101 from 200 to 400 due to max_successful_tryno increase to 6
Increasing send delay for 192.168.1.101 from 400 to 800 due to max_successful_tryno increase to 7
UDP Scan Timing: About 6.39% done; ETC: 13:13 (0:07:34 remaining)
Increasing send delay for 192.168.1.101 from 800 to 1000 due to 11 out of 12 dropped probes since last increase.
UDP Scan Timing: About 8.57% done; ETC: 13:16 (0:10:51 remaining)
UDP Scan Timing: About 11.47% done; ETC: 13:18 (0:11:43 remaining)
UDP Scan Timing: About 13.47% done; ETC: 13:20 (0:12:58 remaining)
Discovered open port 2049/udp on 192.168.1.101
UDP Scan Timing: About 23.37% done; ETC: 13:20 (0:12:11 remaining)
UDP Scan Timing: About 29.57% done; ETC: 13:21 (0:11:21 remaining)
UDP Scan Timing: About 35.37% done; ETC: 13:21 (0:10:32 remaining)
UDP Scan Timing: About 41.57% done; ETC: 13:21 (0:09:41 remaining)
UDP Scan Timing: About 47.17% done; ETC: 13:21 (0:08:50 remaining)
UDP Scan Timing: About 52.37% done; ETC: 13:21 (0:07:59 remaining)
UDP Scan Timing: About 57.67% done; ETC: 13:21 (0:07:07 remaining)
UDP Scan Timing: About 62.77% done; ETC: 13:21 (0:06:15 remaining)
UDP Scan Timing: About 67.87% done; ETC: 13:21 (0:05:23 remaining)
UDP Scan Timing: About 72.97% done; ETC: 13:21 (0:04:32 remaining)
UDP Scan Timing: About 78.07% done; ETC: 13:21 (0:03:41 remaining)
UDP Scan Timing: About 83.07% done; ETC: 13:21 (0:02:51 remaining)
UDP Scan Timing: About 88.17% done; ETC: 13:21 (0:01:59 remaining)
UDP Scan Timing: About 93.27% done; ETC: 13:21 (0:01:08 remaining)
Completed UDP Scan at 13:22, 1031.83s elapsed (1000 total ports)
```



```
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.0017s latency).
Not shown: 993 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
944/udp  open|filtered unknown
2049/udp open          nfs
MAC Address: 08:00:27:E5:4A:BF (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1032.02 seconds
           Raw packets sent: 1358 (66.191KB) | Rcvd: 1029 (76.344KB)
```

nmap -O 192.168.1.101



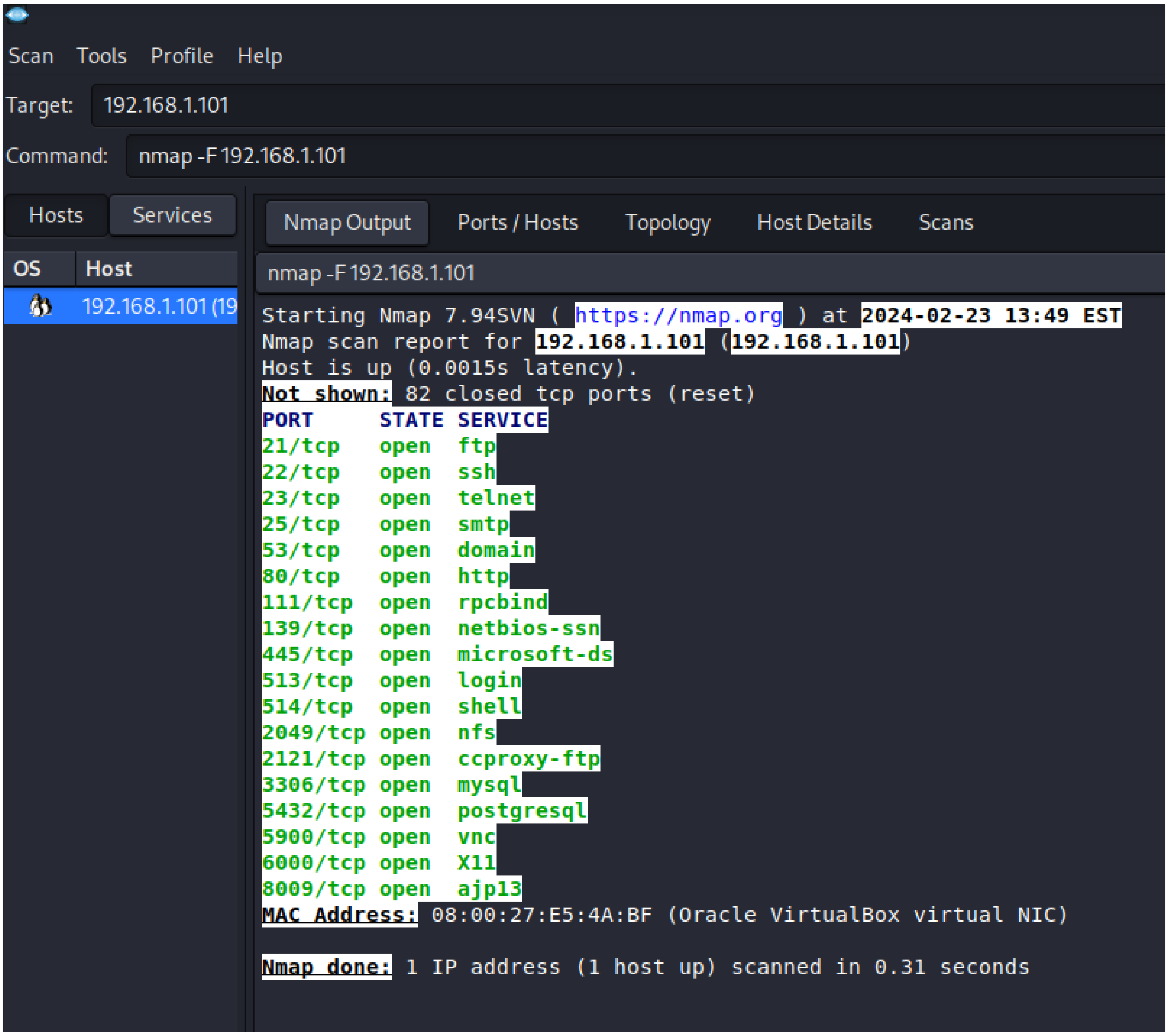
Target: 192.168.1.101

Command: nmap -O 192.168.1.101

```
nmap -O 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 13:46 EST
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.0017s 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:E5:4A:BF (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 2.04 seconds
```

nmap -F 192.168.1.101



Target: 192.168.1.101

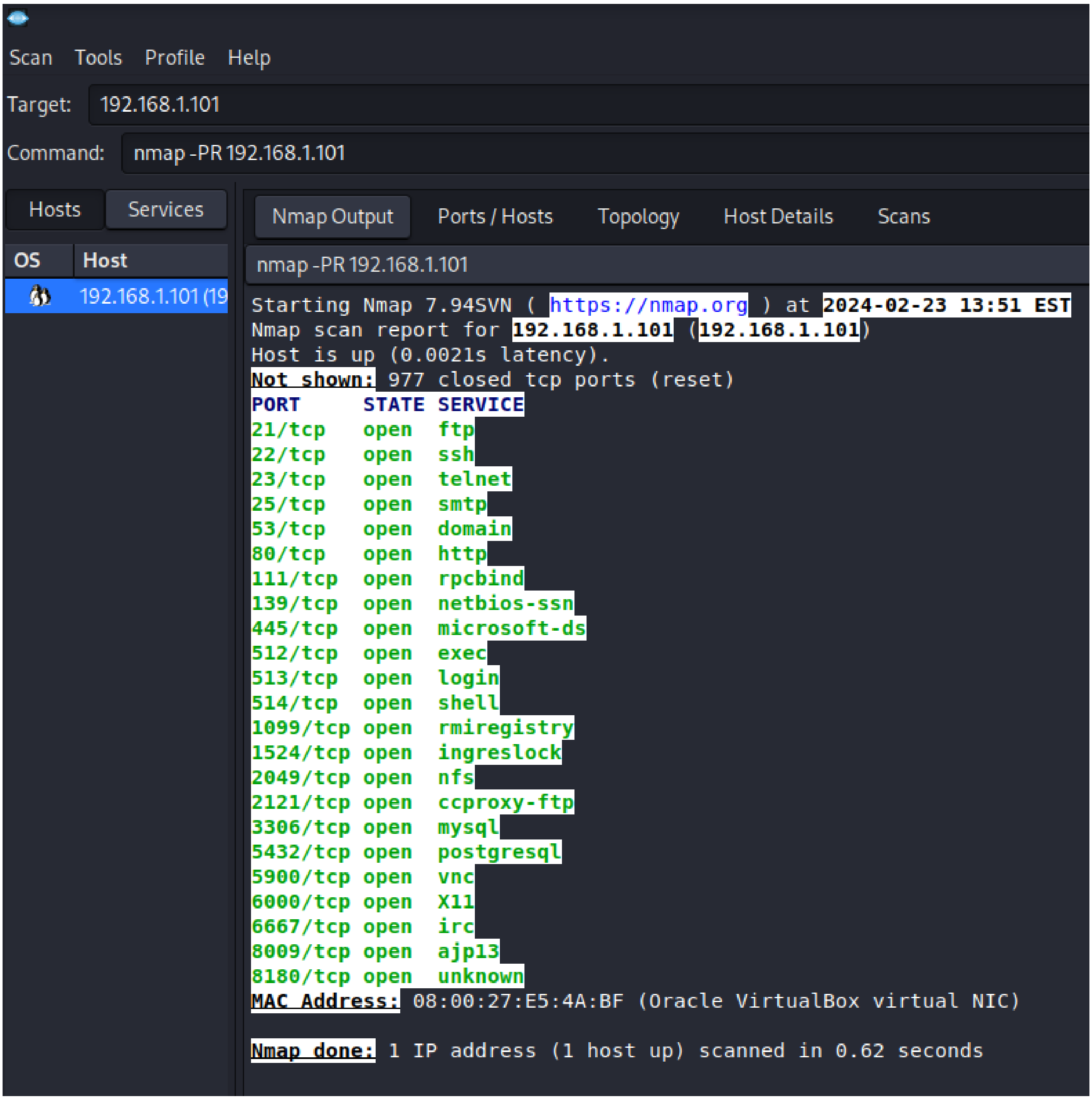
Command: nmap -F 192.168.1.101

nmap -F 192.168.1.101

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 13:49 EST
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.0015s 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:E5:4A:BF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

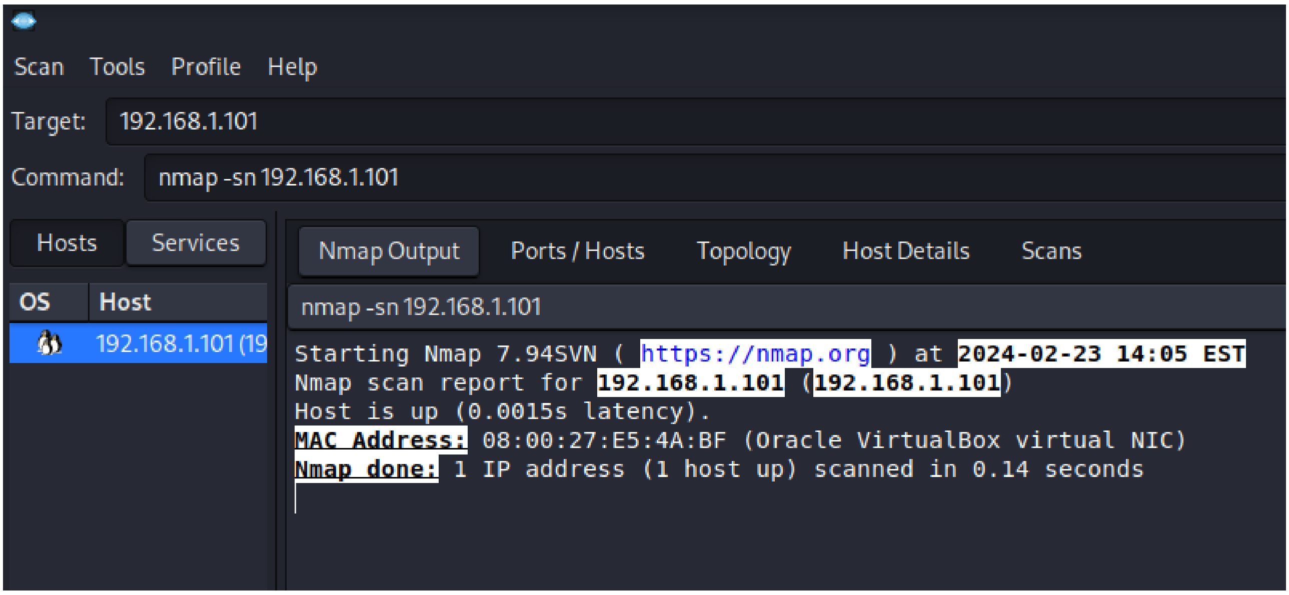
nmap -PR 192.168.1.101



```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 13:51 EST
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.0021s 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:E5:4A:BF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds
```

nmap -sP 192.168.1.101



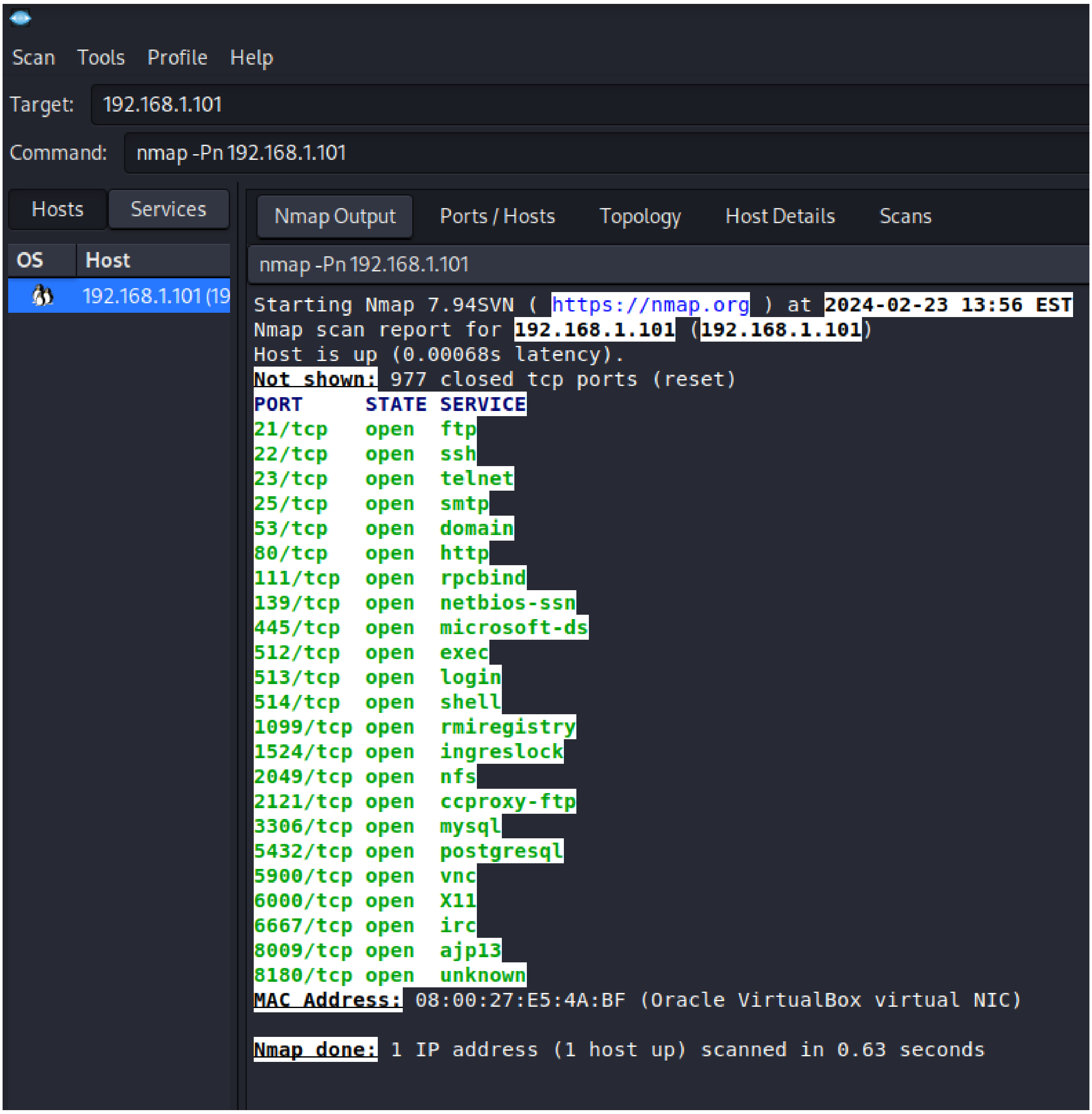
Target: 192.168.1.101

Command: nmap -sn 192.168.1.101

nmap -sn 192.168.1.101

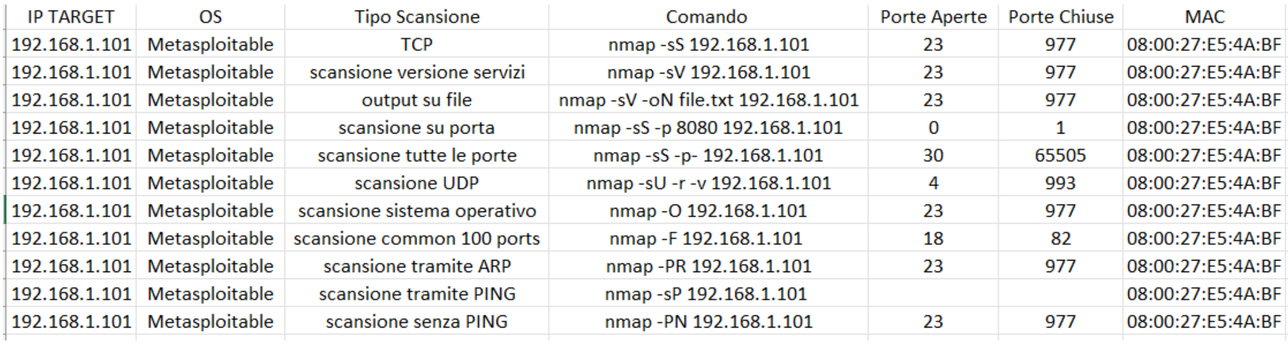
```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 14:05 EST
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.0015s latency).
MAC Address: 08:00:27:E5:4A:BF (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

nmap -PN 192.168.1.101



```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 13:56 EST
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.00068s 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:E5:4A:BF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.63 seconds
```



IP TARGET	OS	Tipo Scansione	Comando	Porte Aperte	Porte Chiuse	MAC
192.168.1.101	Metasploitable	TCP	nmap -sS 192.168.1.101	23	977	08:00:27:E5:4A:BF
192.168.1.101	Metasploitable	scansione versione servizi	nmap -sV 192.168.1.101	23	977	08:00:27:E5:4A:BF
192.168.1.101	Metasploitable	output su file	nmap -sV -oN file.txt 192.168.1.101	23	977	08:00:27:E5:4A:BF
192.168.1.101	Metasploitable	scansione su porta	nmap -sS -p 8080 192.168.1.101	0	1	08:00:27:E5:4A:BF
192.168.1.101	Metasploitable	scansione tutte le porte	nmap -sS -p- 192.168.1.101	30	65505	08:00:27:E5:4A:BF
192.168.1.101	Metasploitable	scansione UDP	nmap -sU -r -v 192.168.1.101	4	993	08:00:27:E5:4A:BF
192.168.1.101	Metasploitable	scansione sistema operativo	nmap -O 192.168.1.101	23	977	08:00:27:E5:4A:BF
192.168.1.101	Metasploitable	scansione common 100 ports	nmap -F 192.168.1.101	18	82	08:00:27:E5:4A:BF
192.168.1.101	Metasploitable	scansione tramite ARP	nmap -PR 192.168.1.101	23	977	08:00:27:E5:4A:BF
192.168.1.101	Metasploitable	scansione tramite PING	nmap -sP 192.168.1.101			08:00:27:E5:4A:BF
192.168.1.101	Metasploitable	scansione senza PING	nmap -PN 192.168.1.101	23	977	08:00:27:E5:4A:BF