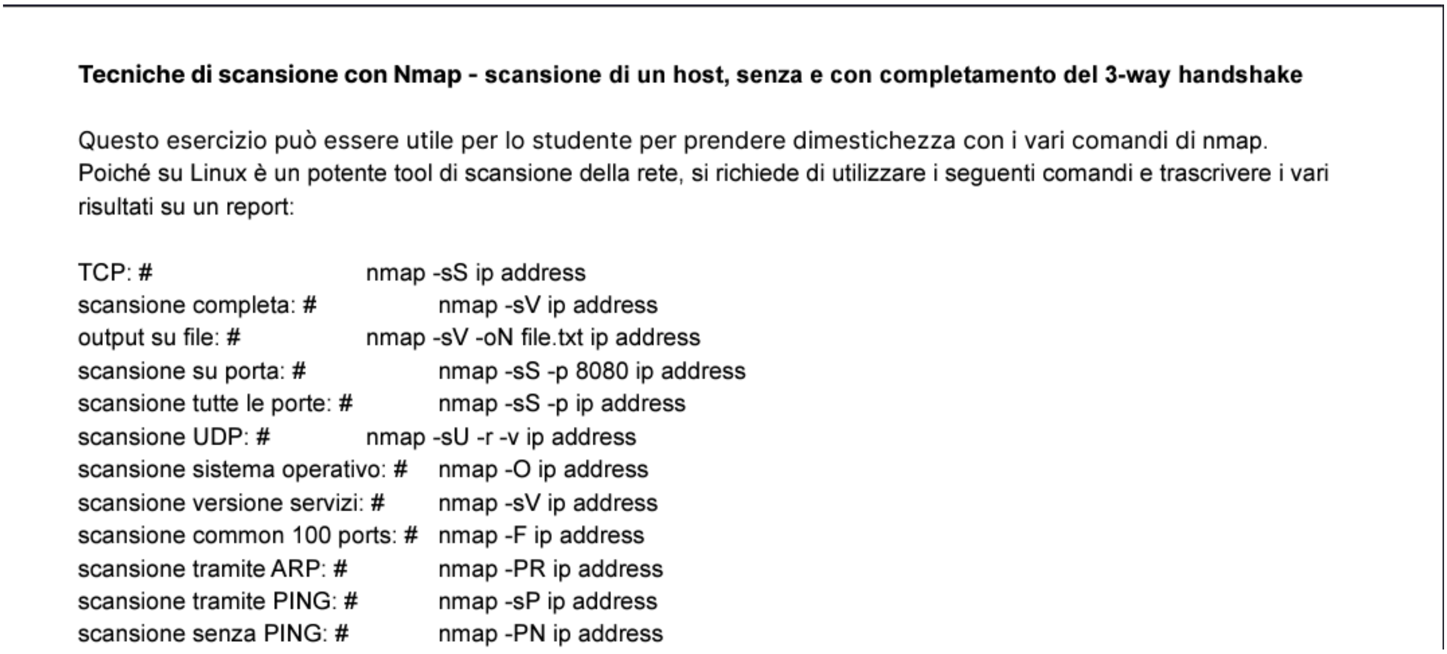
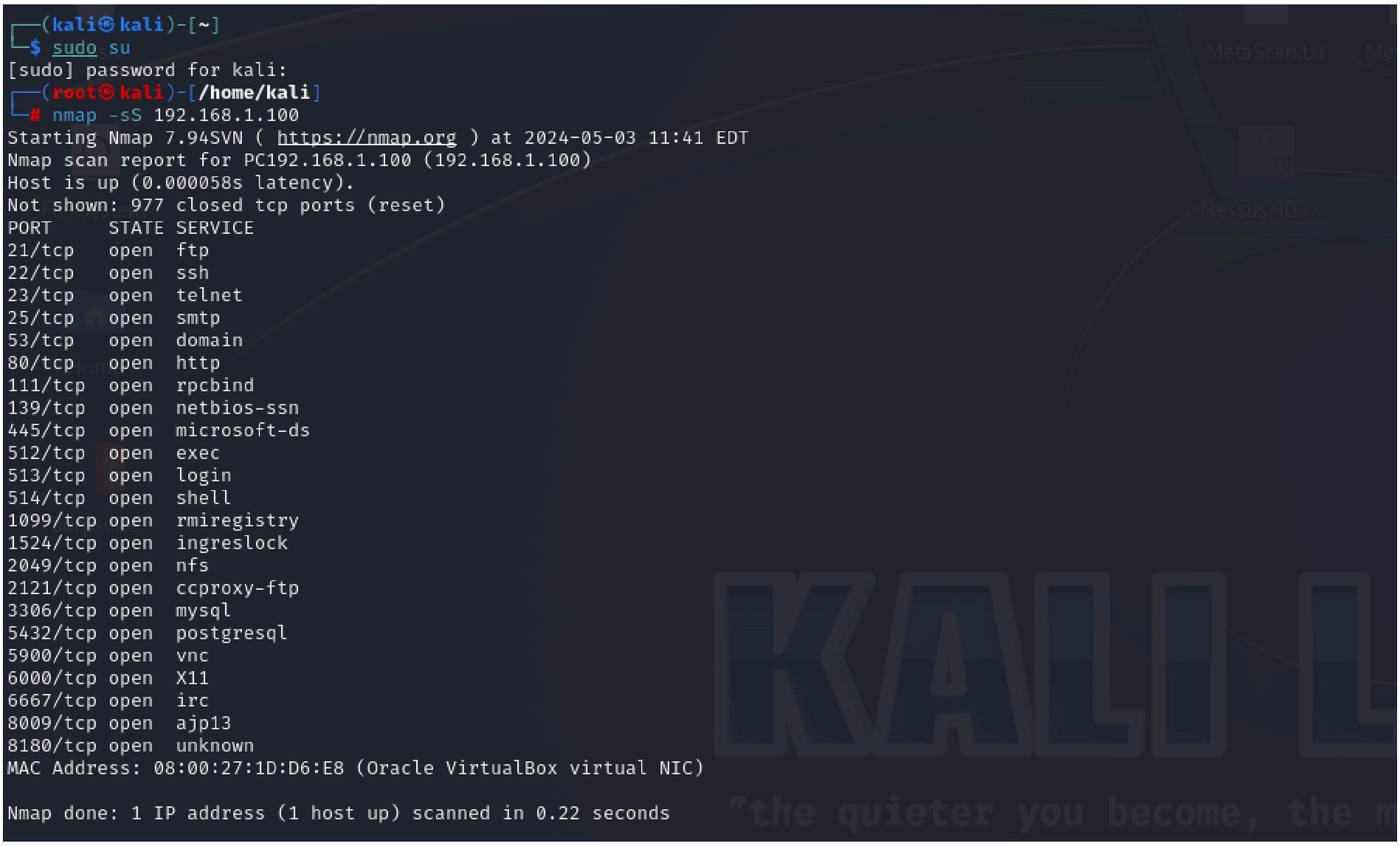


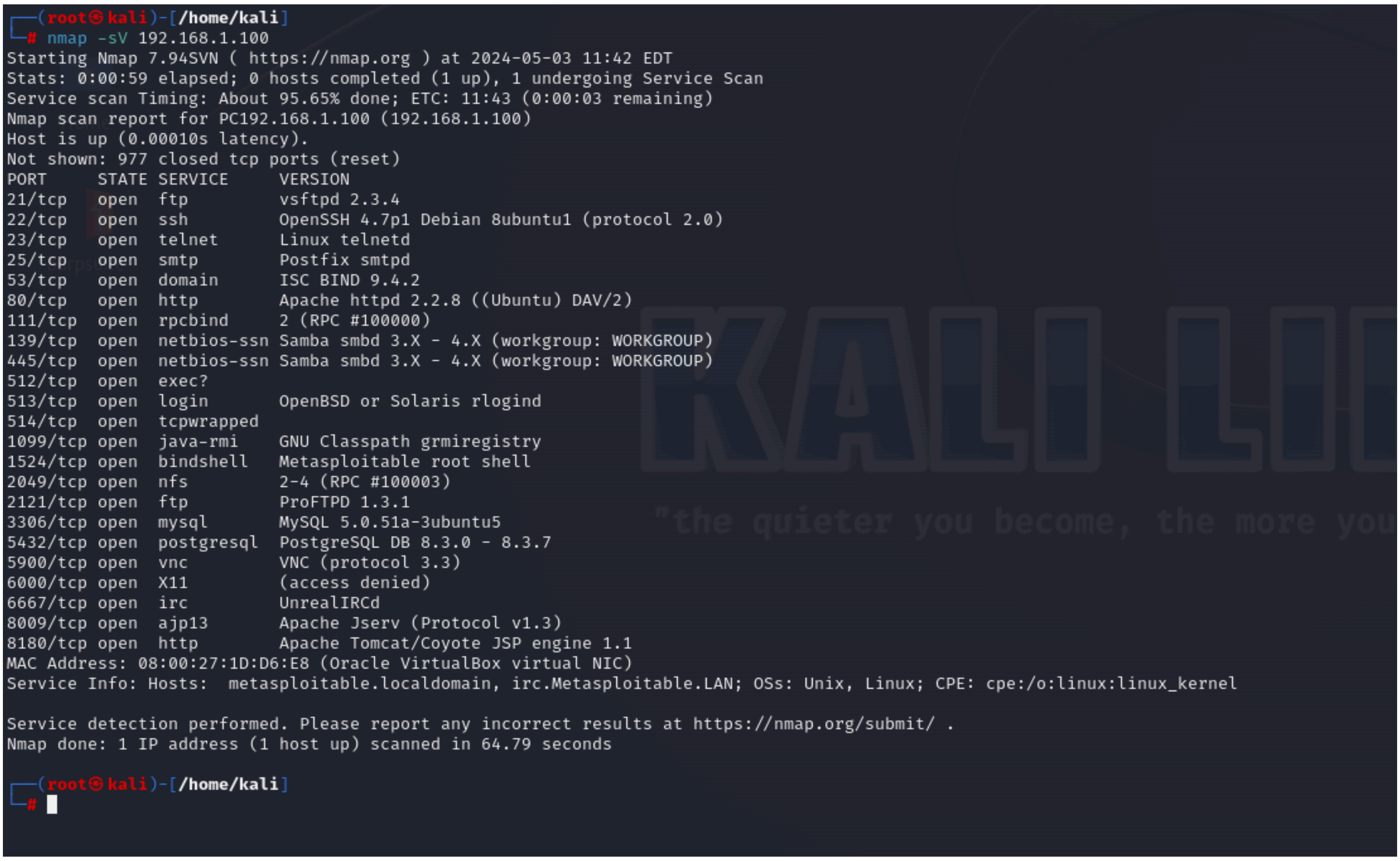
Tecniche di scansione con Nmap - scansione di un host, senza e con completamento del 3-way handshake

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:

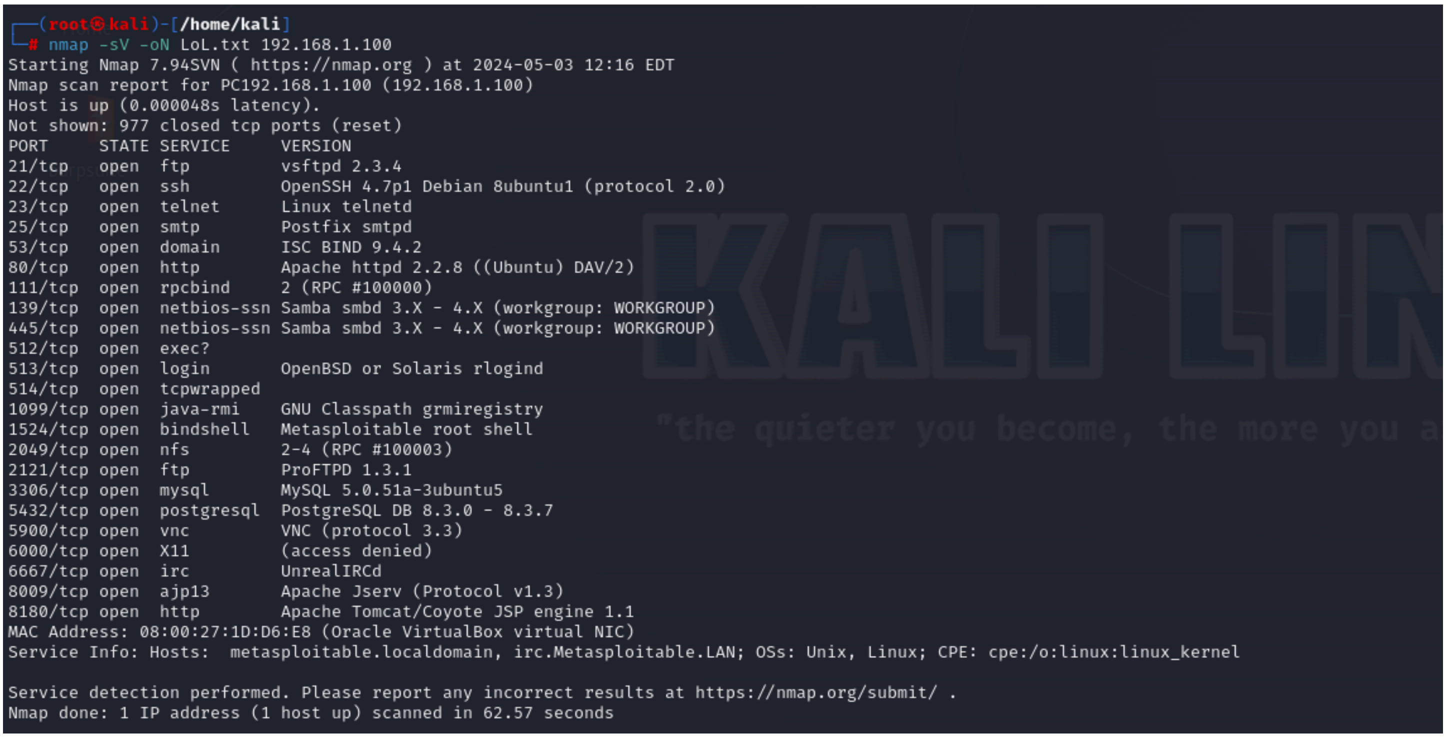
TCP: #	nmap -sS ip address
scansione completa: #	nmap -sV ip address
output su file: #	nmap -sV -oN file.txt ip address
scansione su porta: #	nmap -sS -p 8080 ip address
scansione tutte le porte: #	nmap -sS -p ip address
scansione UDP: #	nmap -sU -r -v ip address
scansione sistema operativo: #	nmap -O 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



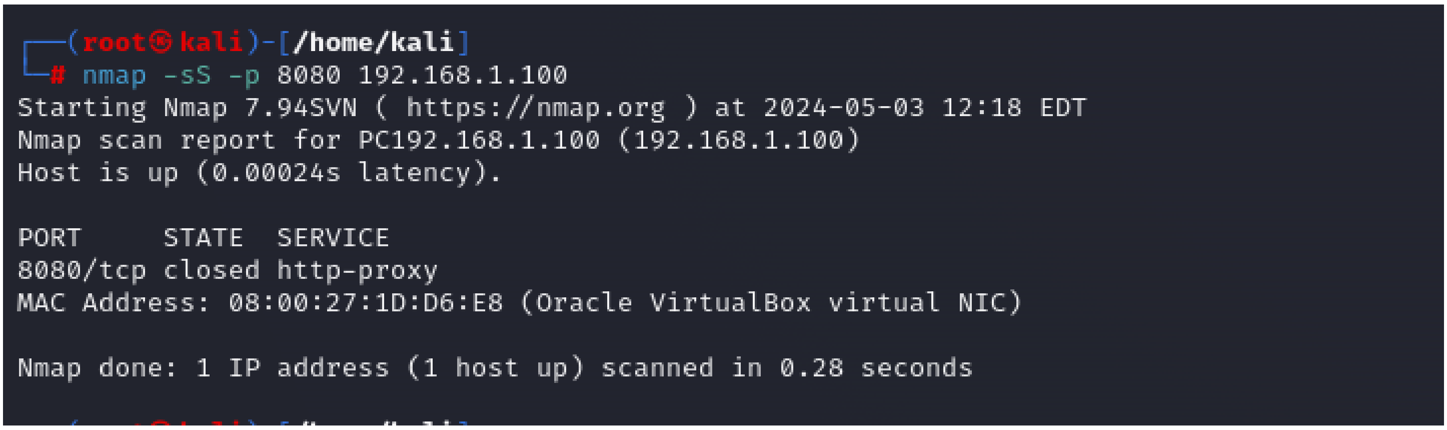
```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-03 11:41 EDT
Nmap scan report for PC192.168.1.100 (192.168.1.100)
Host is up (0.000058s latency).
Not shown: 977 closed tcp ports (reset)
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: 08:00:27:1D:D6:E8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```



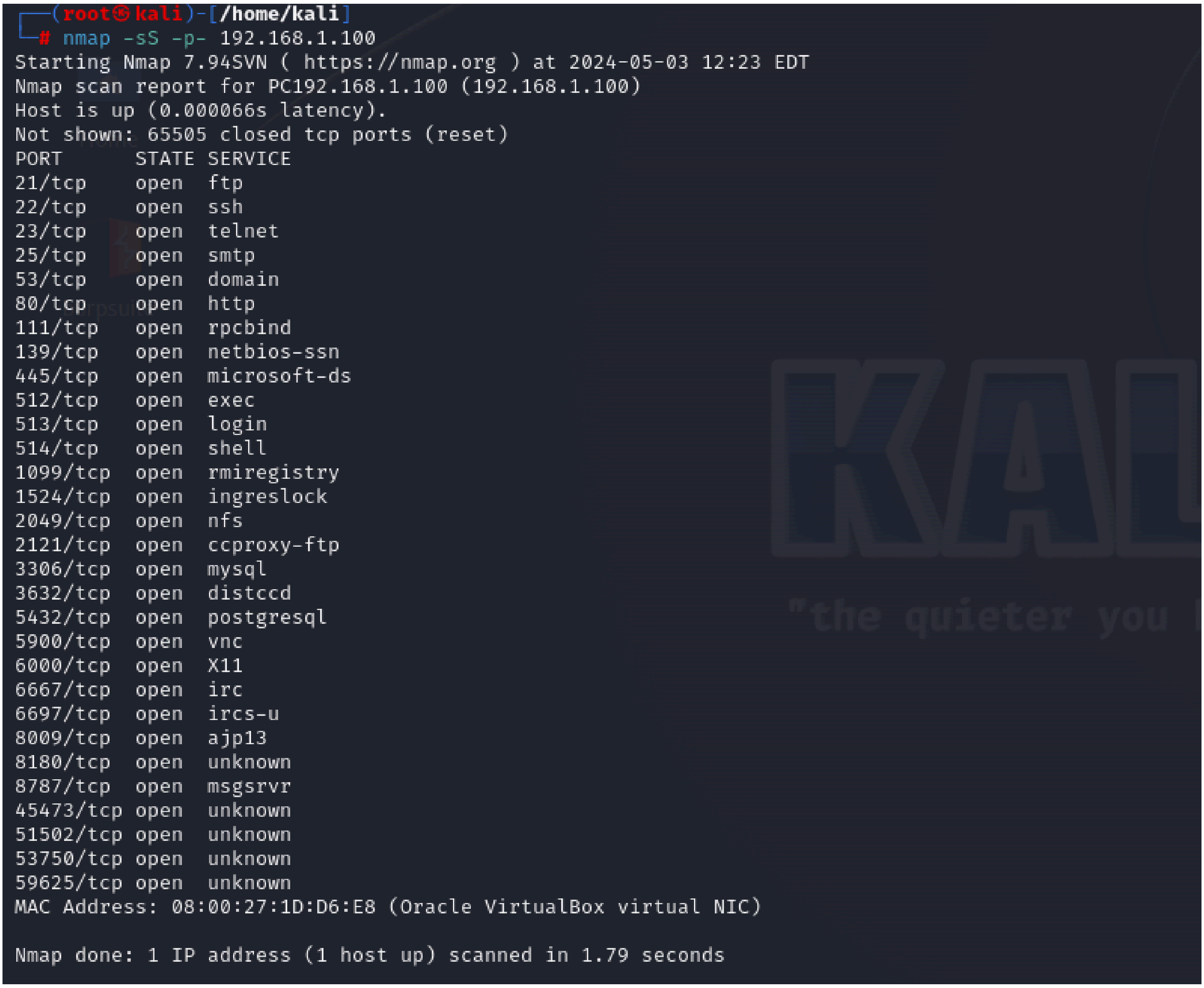
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-03 11:42 EDT
Stats: 0:00:59 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 11:43 (0:00:03 remaining)
Nmap scan report for PC192.168.1.100 (192.168.1.100)
Host is up (0.00010s 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?
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: 08:00:27:1D:D6:E8 (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 64.79 seconds

┌──(root㉿kali)-[/home/kali]
└─# 
```



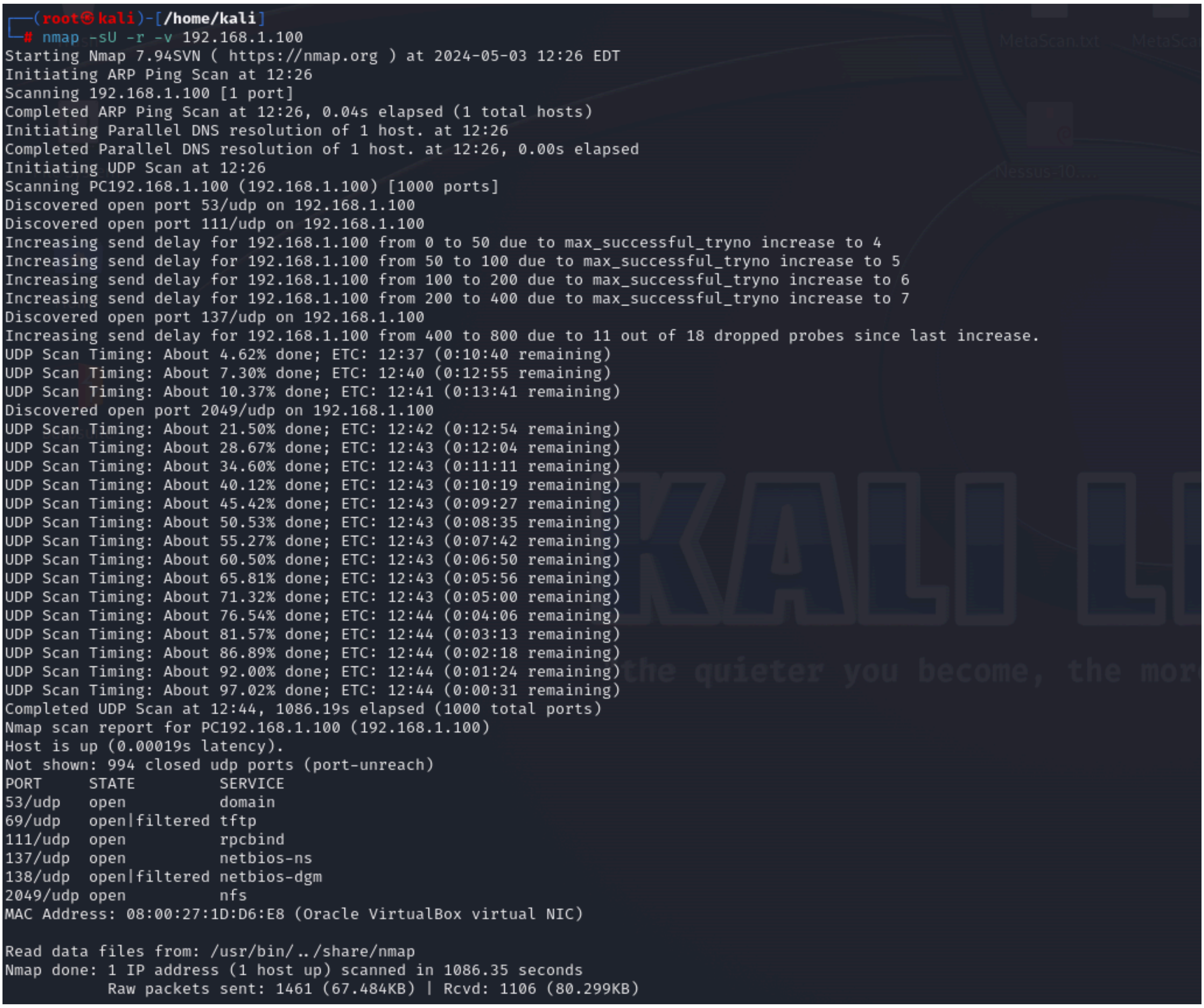
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -oN LoL.txt 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-03 12:16 EDT
Nmap scan report for PC192.168.1.100 (192.168.1.100)
Host is up (0.000048s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   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?
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: 08:00:27:1D:D6:E8 (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 62.57 seconds
```



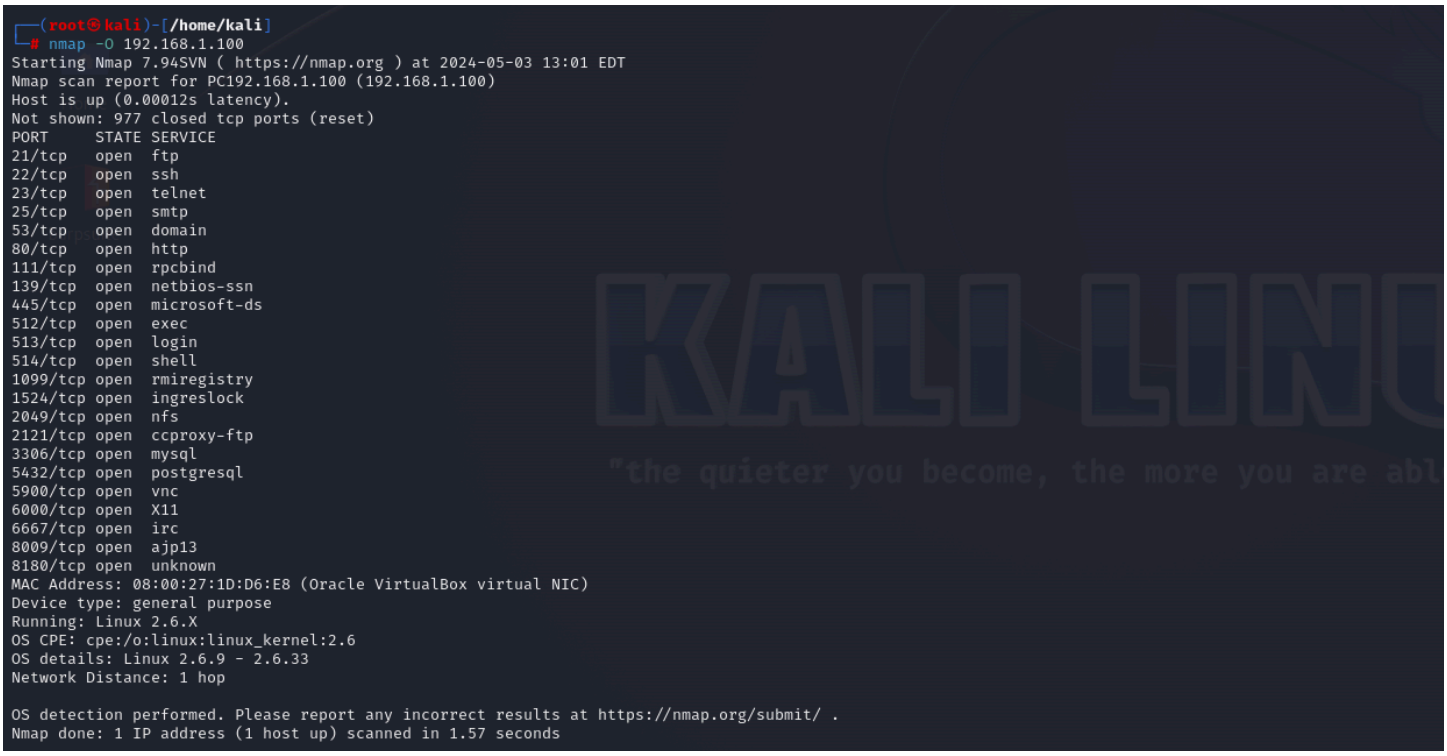
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -p 8080 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-03 12:18 EDT
Nmap scan report for PC192.168.1.100 (192.168.1.100)
Host is up (0.00024s latency).

PORT     STATE  SERVICE
8080/tcp closed http-proxy
MAC Address: 08:00:27:1D:D6:E8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```



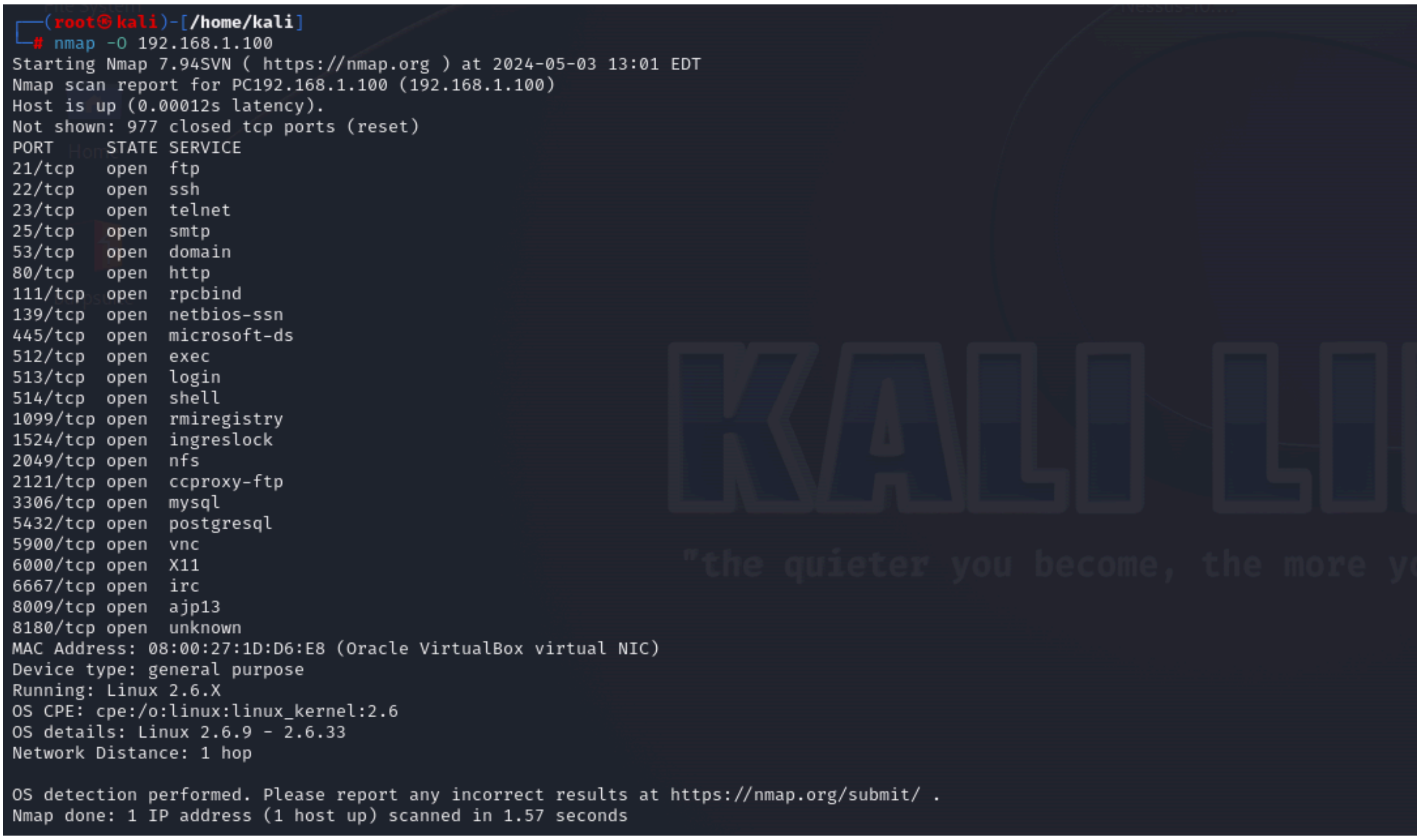
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -p- 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-03 12:23 EDT
Nmap scan report for PC192.168.1.100 (192.168.1.100)
Host is up (0.000066s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
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
45473/tcp open  unknown
51502/tcp open  unknown
53750/tcp open  unknown
59625/tcp open  unknown
MAC Address: 08:00:27:1D:D6:E8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.79 seconds
```



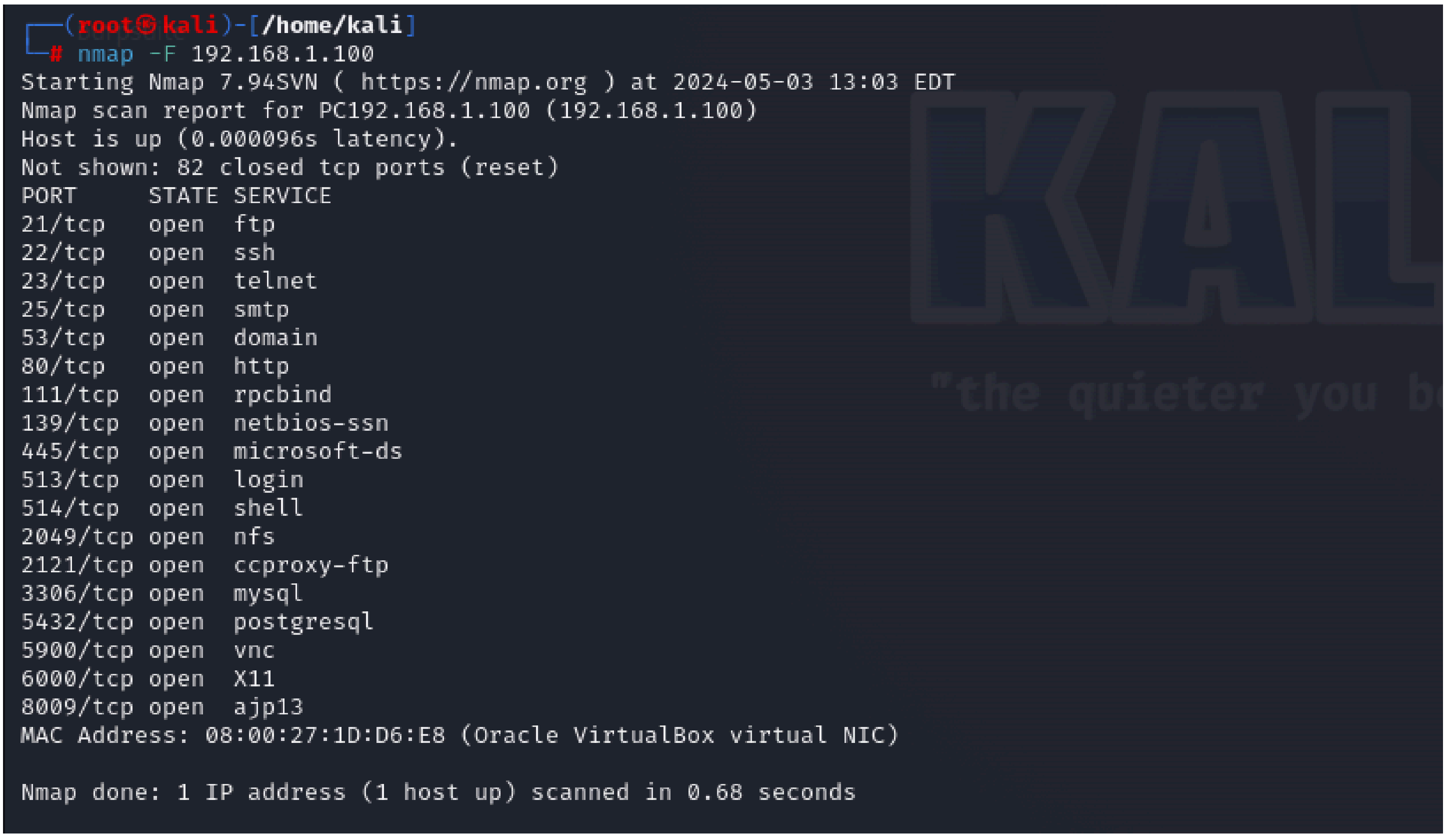
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sU -r -v 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-03 12:26 EDT
Initiating ARP Ping Scan at 12:26
Scanning 192.168.1.100 [1 port]
Completed ARP Ping Scan at 12:26, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:26
Completed Parallel DNS resolution of 1 host. at 12:26, 0.00s elapsed
Initiating UDP Scan at 12:26
Scanning PC192.168.1.100 (192.168.1.100) [1000 ports]
Discovered open port 53/udp on 192.168.1.100
Discovered open port 111/udp on 192.168.1.100
Increasing send delay for 192.168.1.100 from 0 to 50 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.1.100 from 50 to 100 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.1.100 from 100 to 200 due to max_successful_tryno increase to 6
Increasing send delay for 192.168.1.100 from 200 to 400 due to max_successful_tryno increase to 7
Discovered open port 137/udp on 192.168.1.100
Increasing send delay for 192.168.1.100 from 400 to 800 due to 11 out of 18 dropped probes since last increase.
UDP Scan Timing: About 4.62% done; ETC: 12:37 (0:10:40 remaining)
UDP Scan Timing: About 7.30% done; ETC: 12:40 (0:12:55 remaining)
UDP Scan Timing: About 10.37% done; ETC: 12:41 (0:13:41 remaining)
Discovered open port 2049/udp on 192.168.1.100
UDP Scan Timing: About 21.50% done; ETC: 12:42 (0:12:54 remaining)
UDP Scan Timing: About 28.67% done; ETC: 12:43 (0:12:04 remaining)
UDP Scan Timing: About 34.60% done; ETC: 12:43 (0:11:11 remaining)
UDP Scan Timing: About 40.12% done; ETC: 12:43 (0:10:19 remaining)
UDP Scan Timing: About 45.42% done; ETC: 12:43 (0:09:27 remaining)
UDP Scan Timing: About 50.53% done; ETC: 12:43 (0:08:35 remaining)
UDP Scan Timing: About 55.27% done; ETC: 12:43 (0:07:42 remaining)
UDP Scan Timing: About 60.50% done; ETC: 12:43 (0:06:50 remaining)
UDP Scan Timing: About 65.81% done; ETC: 12:43 (0:05:56 remaining)
UDP Scan Timing: About 71.32% done; ETC: 12:43 (0:05:00 remaining)
UDP Scan Timing: About 76.54% done; ETC: 12:44 (0:04:06 remaining)
UDP Scan Timing: About 81.57% done; ETC: 12:44 (0:03:13 remaining)
UDP Scan Timing: About 86.89% done; ETC: 12:44 (0:02:18 remaining)
UDP Scan Timing: About 92.00% done; ETC: 12:44 (0:01:24 remaining)
UDP Scan Timing: About 97.02% done; ETC: 12:44 (0:00:31 remaining)
Completed UDP Scan at 12:44, 1086.19s elapsed (1000 total ports)
Nmap scan report for PC192.168.1.100 (192.168.1.100)
Host is up (0.00019s 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: 08:00:27:1D:D6:E8 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1086.35 seconds
           Raw packets sent: 1461 (67.484KB) | Rcvd: 1106 (80.299KB)
```



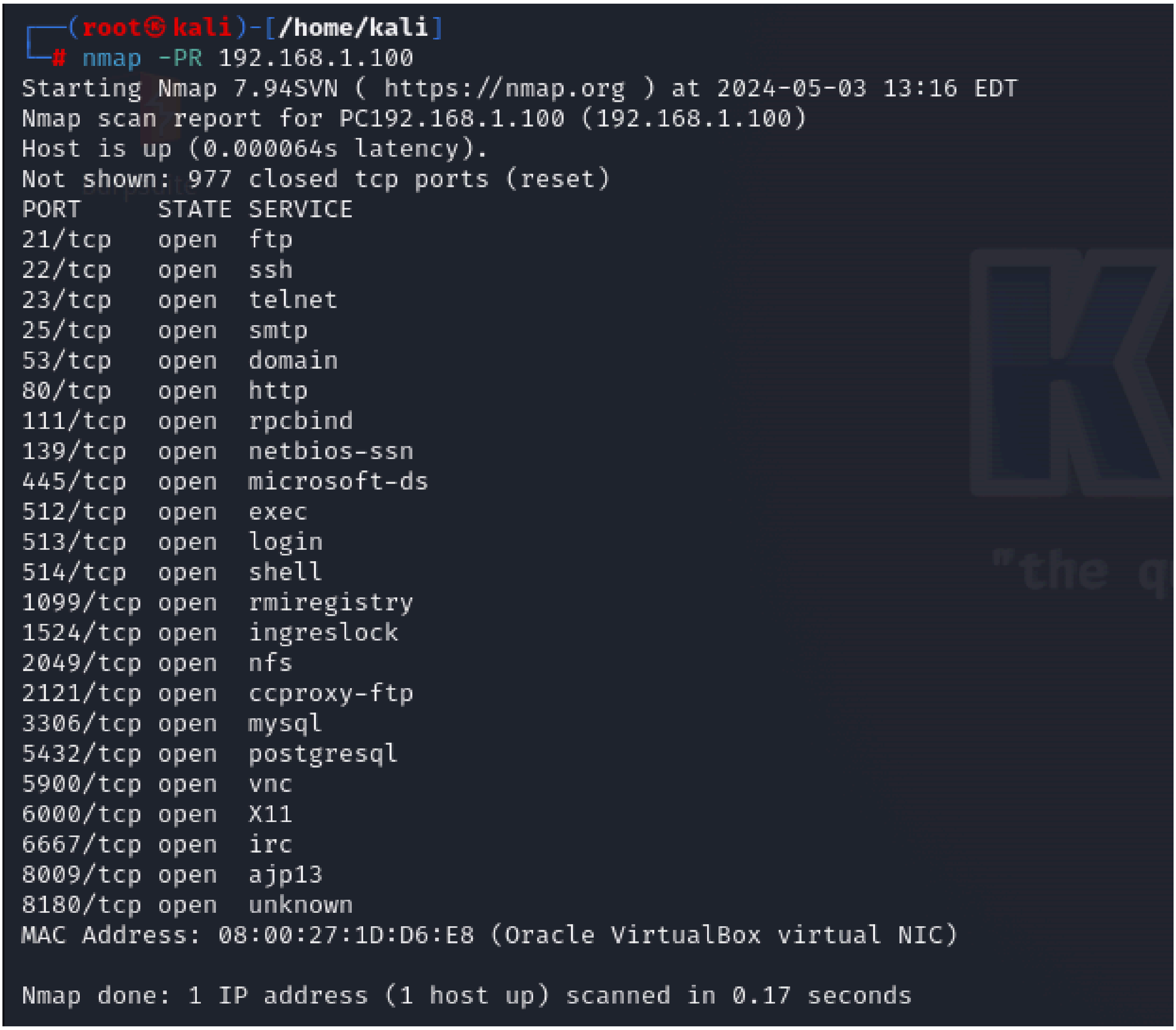
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-03 13:01 EDT
Nmap scan report for PC192.168.1.100 (192.168.1.100)
Host is up (0.00012s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  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: 08:00:27:1D:D6:E8 (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 1.57 seconds
```



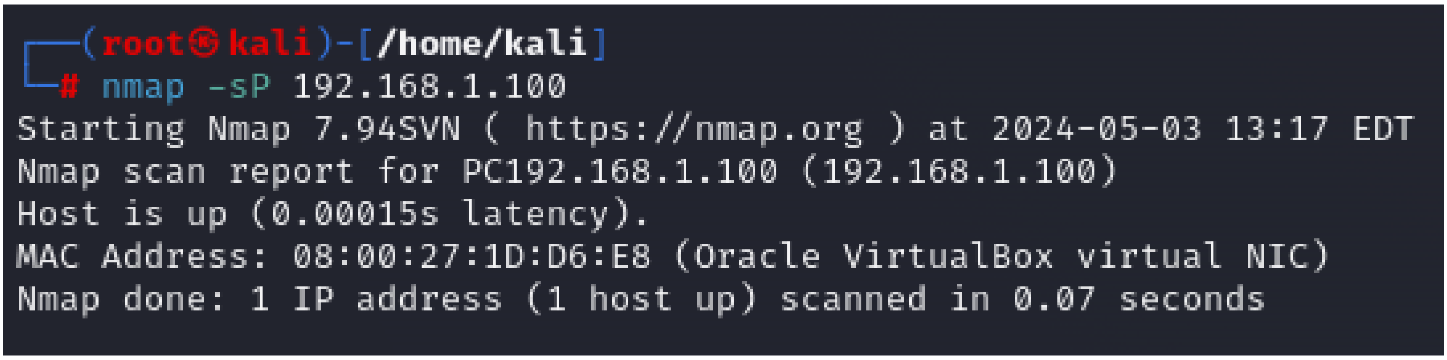
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-03 13:01 EDT
Nmap scan report for PC192.168.1.100 (192.168.1.100)
Host is up (0.00012s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  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: 08:00:27:1D:D6:E8 (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 1.57 seconds
```



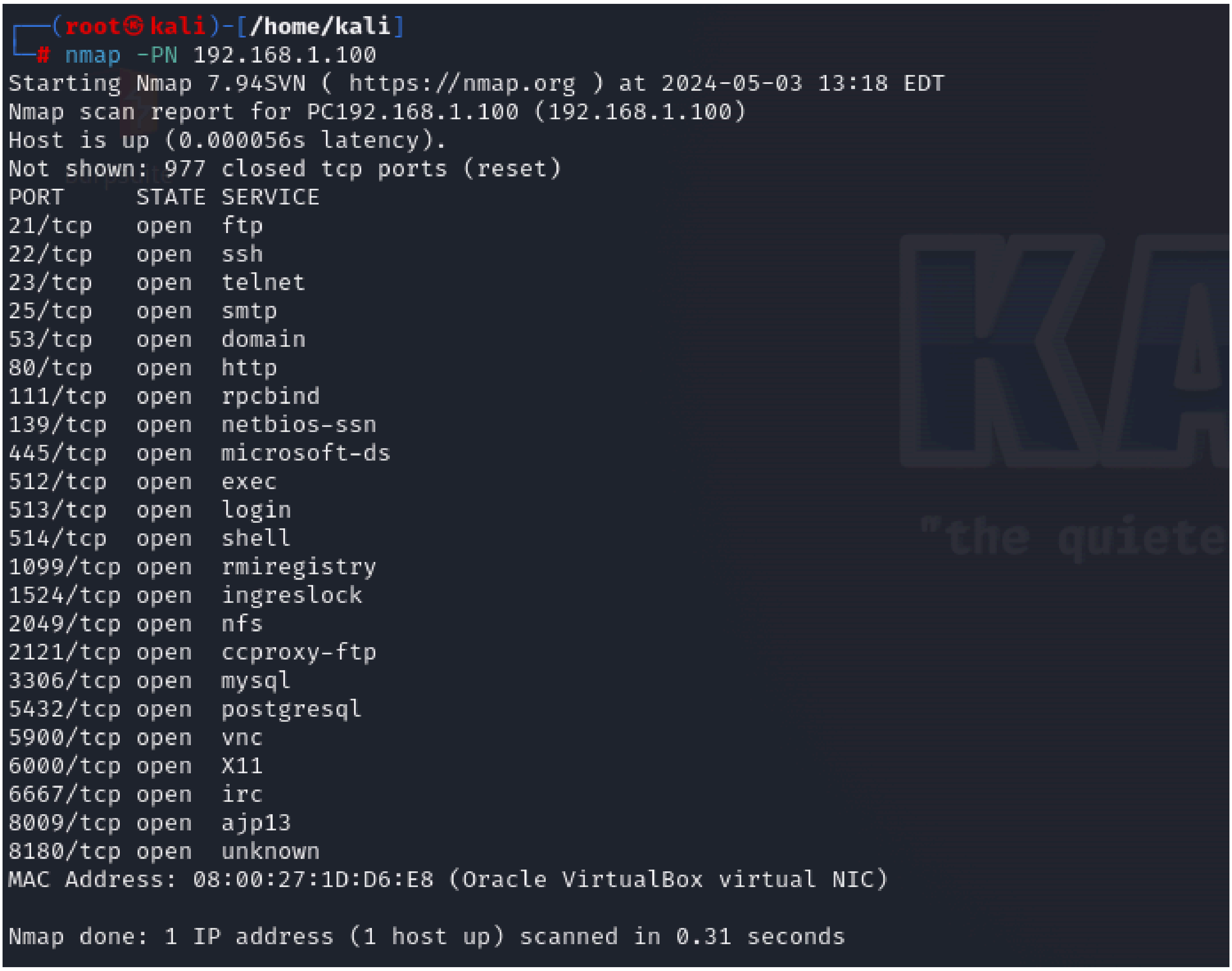
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -F 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-03 13:03 EDT
Nmap scan report for PC192.168.1.100 (192.168.1.100)
Host is up (0.000096s latency).
Not shown: 82 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  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: 08:00:27:1D:D6:E8 (Oracle VirtualBox virtual NIC)

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



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -PR 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-03 13:16 EDT
Nmap scan report for PC192.168.1.100 (192.168.1.100)
Host is up (0.000064s 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: 08:00:27:1D:D6:E8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```



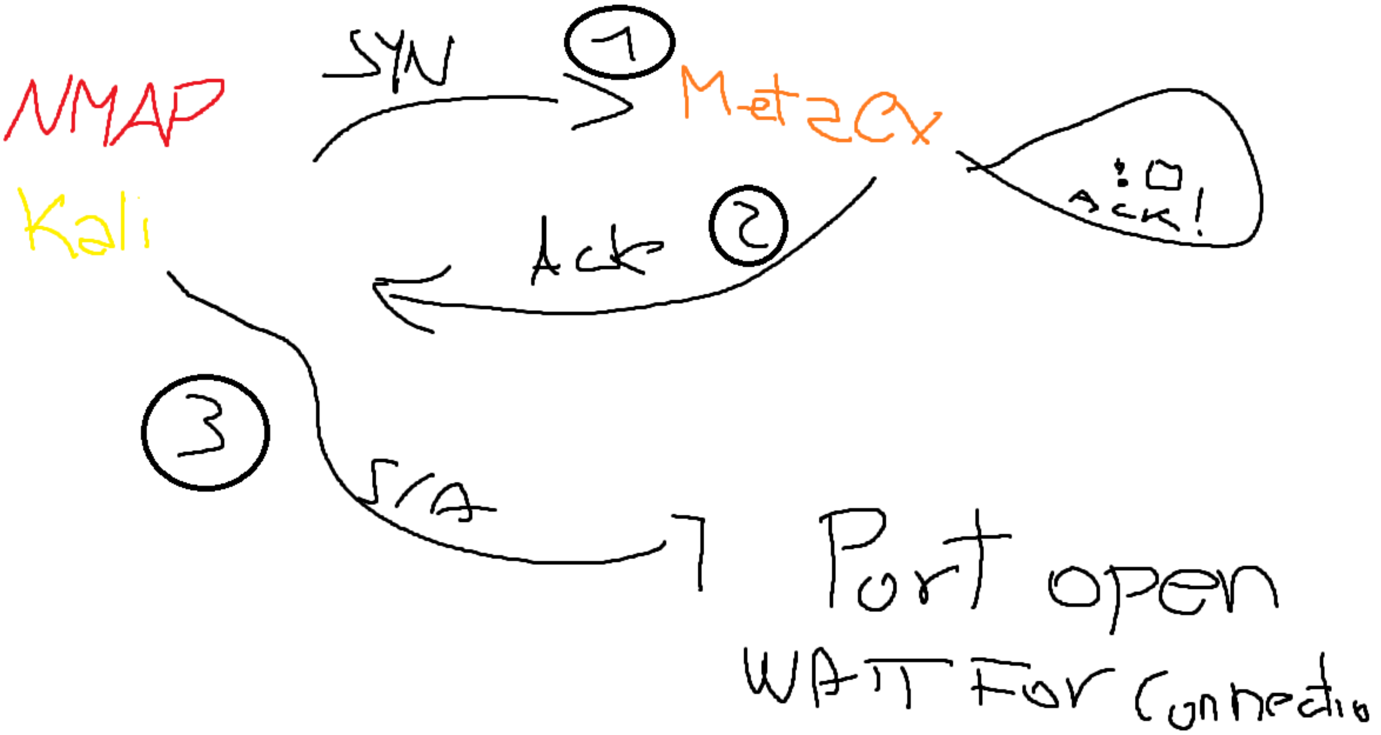
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sP 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-03 13:17 EDT
Nmap scan report for PC192.168.1.100 (192.168.1.100)
Host is up (0.00015s latency).
MAC Address: 08:00:27:1D:D6:E8 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

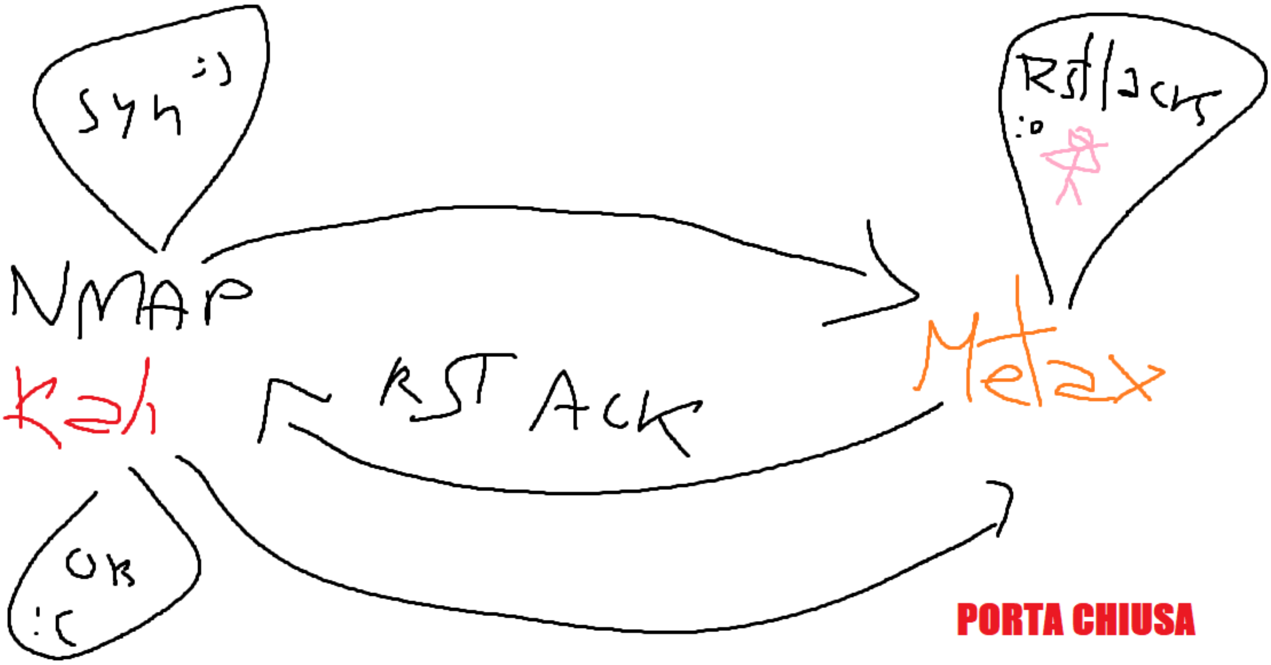


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -PN 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-03 13:18 EDT
Nmap scan report for PC192.168.1.100 (192.168.1.100)
Host is up (0.000056s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   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: 08:00:27:1D:D6:E8 (Oracle VirtualBox virtual NIC)

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

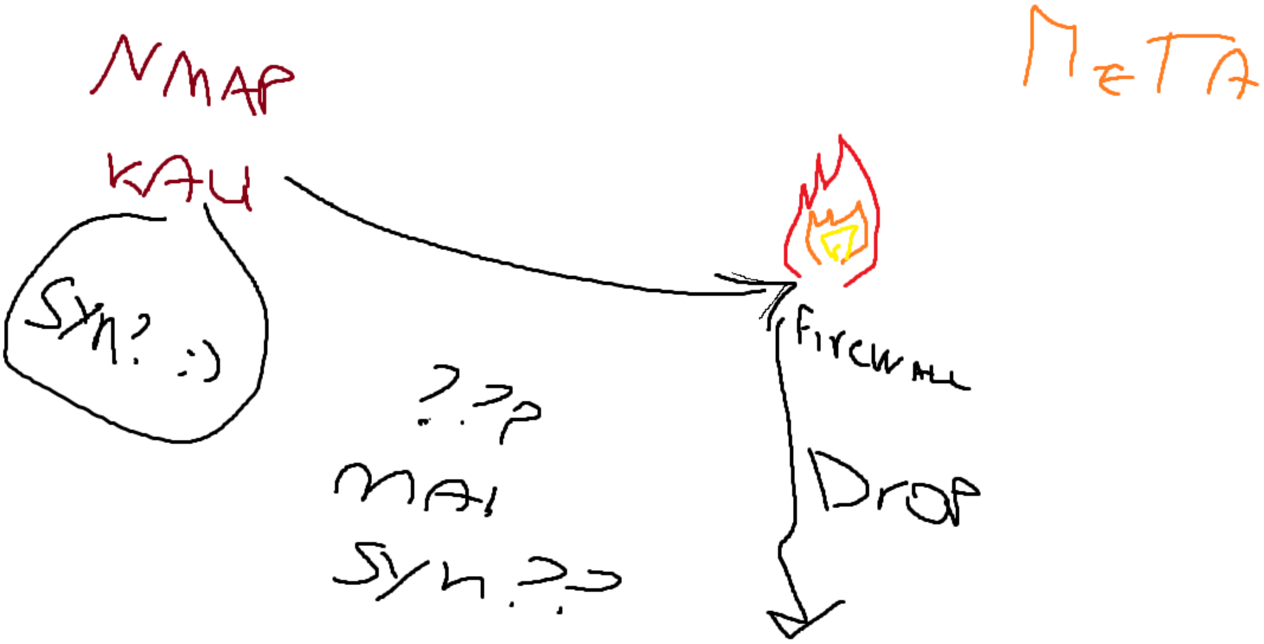
Tecniche di scansione con Nmap - scansione di un host, senza e con completamento del 3-way handshake

Infine, disegnare 3-4 grafici delle scansioni effettuate, esplicitando le varie fasi di syn, syn/ack ecc.





PORTA CHIUSA


NMAP
KALI
Syn? :)
???
mai
Syn??
META
firewall
Drop