EXPERIMENT NUMBER 2

Name of Student: Sangeet Agrawal	PRN: 21070122140	Section: CS-B

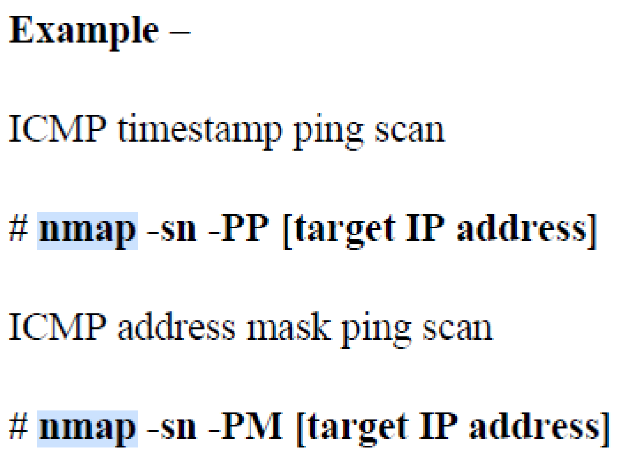
Title: Network forensic lab using Nmap tool

Aim: Study, understand and demonstrate network scanning tool

Objective: To make students understand and demonstrate various network scanning tools.

Theory:

Nmap is a utility used for network discovery, network administration, and security auditing. It is also used to perform tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.
Here, we will use Nmap to discover a list of live hosts in the target network. We can use Nmap to scan the active hosts in the target network using various host discovery techniques such as ARP ping scan, UDP ping scan, ICMP ECHO ping scan, ICMP ECHO ping sweep, etc.



Example –

ICMP timestamp ping scan

```
# nmap -sn -PP [target IP address]
```

ICMP address mask ping scan

```
# nmap -sn -PM [target IP address]
```

Nmap comes with various inbuilt scripts that can be employed during a scanning process in an attempt to find the open ports and services running on the ports. It sends specially crafted packets to the target host, and then analyzes the responses to accomplish its goal. Nmap includes many port scanning mechanisms (TCP and UDP), OS detection, version detection, ping sweeps, etc.

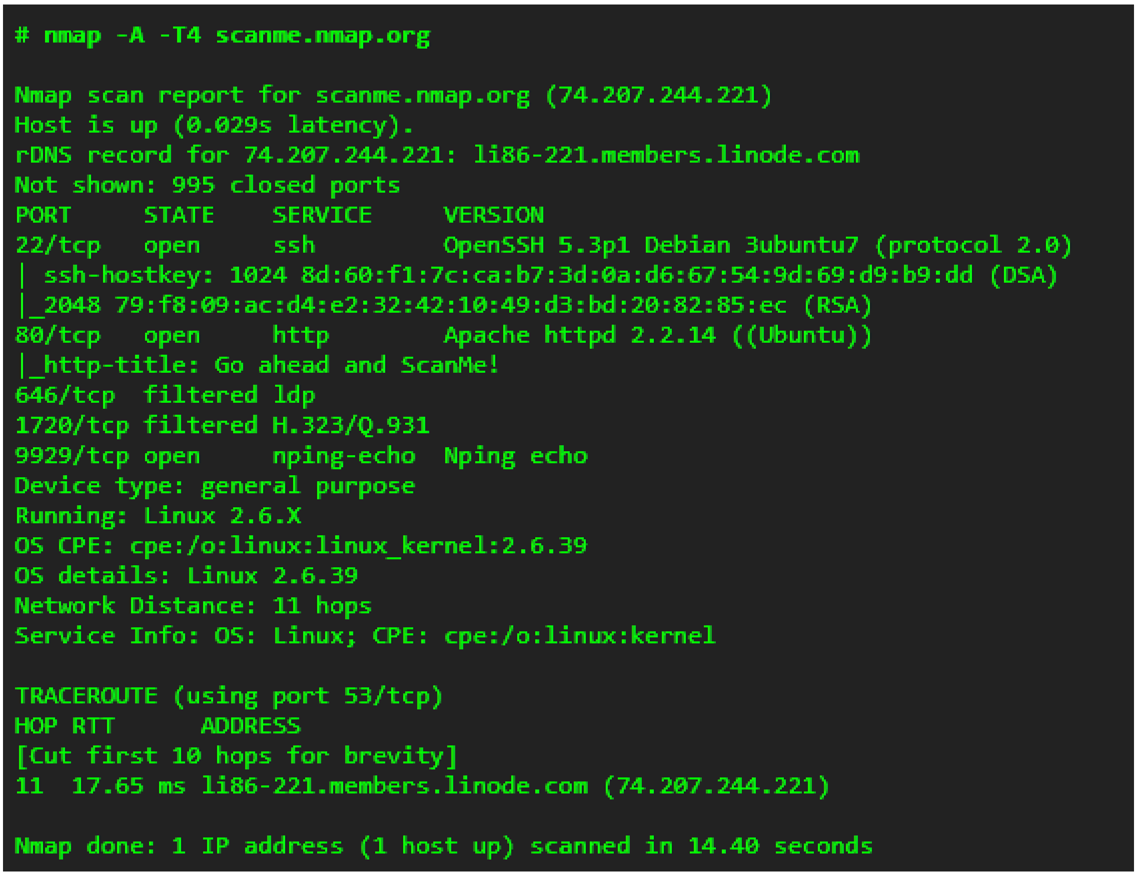
Port Scanning Basics – from nmap.org

Nmap began as an efficient port scanner, and that remains its core function. The simple command **nmap <*target*>** scans 1,000 TCP ports on the host <*target*>. While many port scanners have traditionally lumped all ports into the open or closed states, Nmap is much more granular. It divides ports into six states: open, closed, filtered, unfiltered, open|filtered, or closed|filtered.

These states are not intrinsic properties of the port itself, but describe how Nmap sees them.

The six port states recognized by Nmap

- Open: An application is actively accepting TCP connections, UDP datagrams or SCTP associations on this port. Finding these is often the primary goal of port scanning. Open ports are also interesting for non-security scans because they show services available for use on the network.



```
# nmap -A -T4 scanme.nmap.org

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT     STATE    SERVICE     VERSION
22/tcp   open     ssh         OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
| ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
|_2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp   open     http        Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
646/tcp  filtered ldp
1720/tcp filtered H.323/Q.931
9929/tcp open     nping-echo  Nping echo
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.39
OS details: Linux 2.6.39
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
[Cut first 10 hops for brevity]
11  17.65 ms li86-221.members.linode.com (74.207.244.221)

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
```

Soruce: https://nmap.org/book/man.html

- Closed: A closed port is accessible (it receives and responds to Nmap probe packets), but there is no application listening on it. They can be helpful in showing that a host is up on an IP address (host discovery, or ping scanning), and as part of OS detection.
- Filtered: Nmap cannot determine whether the port is open because packet filtering prevents its probes from reaching the port. The filtering could be from a dedicated firewall device, router rules, or host-based firewall software.
- Unfiltered: The unfiltered state means that a port is accessible, but Nmap is unable to determine whether it is open or closed. Only the ACK scan, which is used to map firewall rulesets, classifies ports into this state.

- open|filtered: Nmap places ports in this state when it is unable to determine whether a port is open or filtered. This occurs for scan types in which open ports give no response. The lack of response could also mean that a packet filter dropped the probe or any response it elicited
- closed|filtered: This state is used when Nmap is unable to determine whether a port is closed or filtered. It is only used for the IP ID idle scan.

Tools to be practiced:

1) Nmap
2) Angry IP Scanner
3) Advanced IP Scanner
4) Wireshark

Reference web links:

1) https://nmap.org/
2) https://www.stationx.net/nmap-cheat-sheet/
3) https://www.advanced-ip-scanner.com/
4) https://angryip.org/

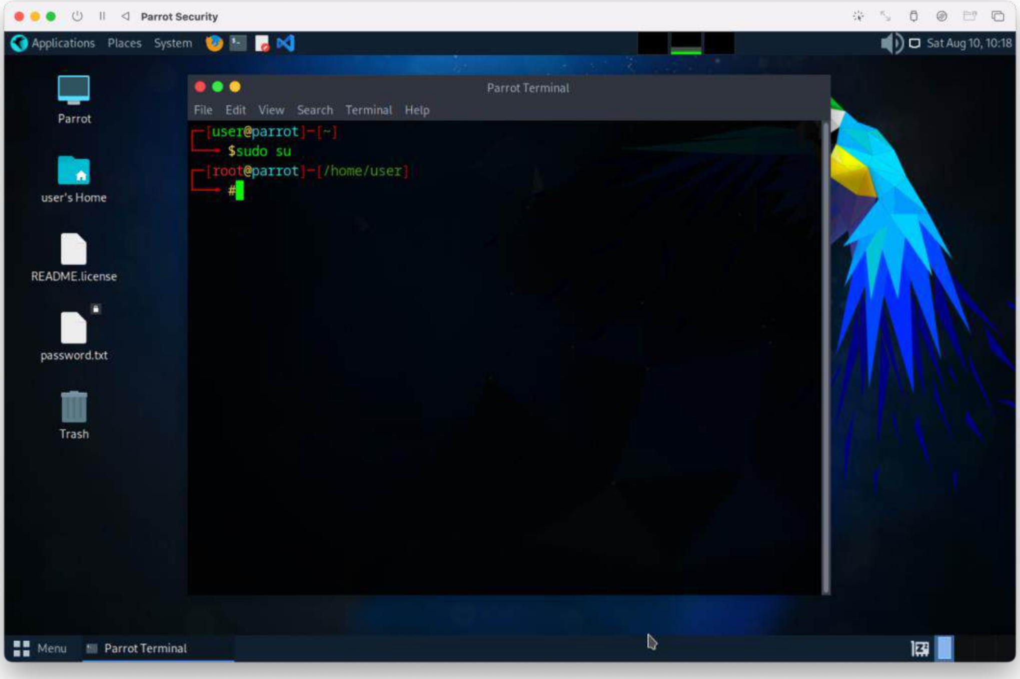
Conclusion:

In this experiment, we used Nmap for network scanning and forensics, identifying open, closed, and filtered ports. We also practiced with Angry IP Scanner, Advanced IP Scanner, and Wireshark, highlighting the importance of these tools for network security and resource management.

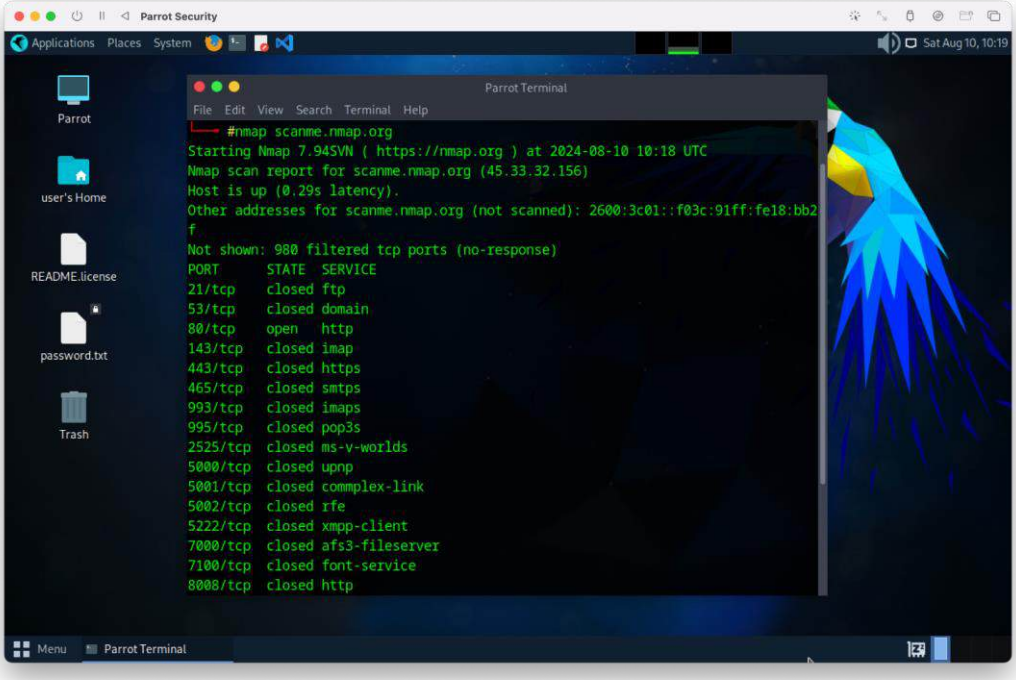
Implementation question:

1) Demonstrate various nmap options and submit screenshot - At least 12 different and important options, 3 Nmap Script Engine (NSE) scripts

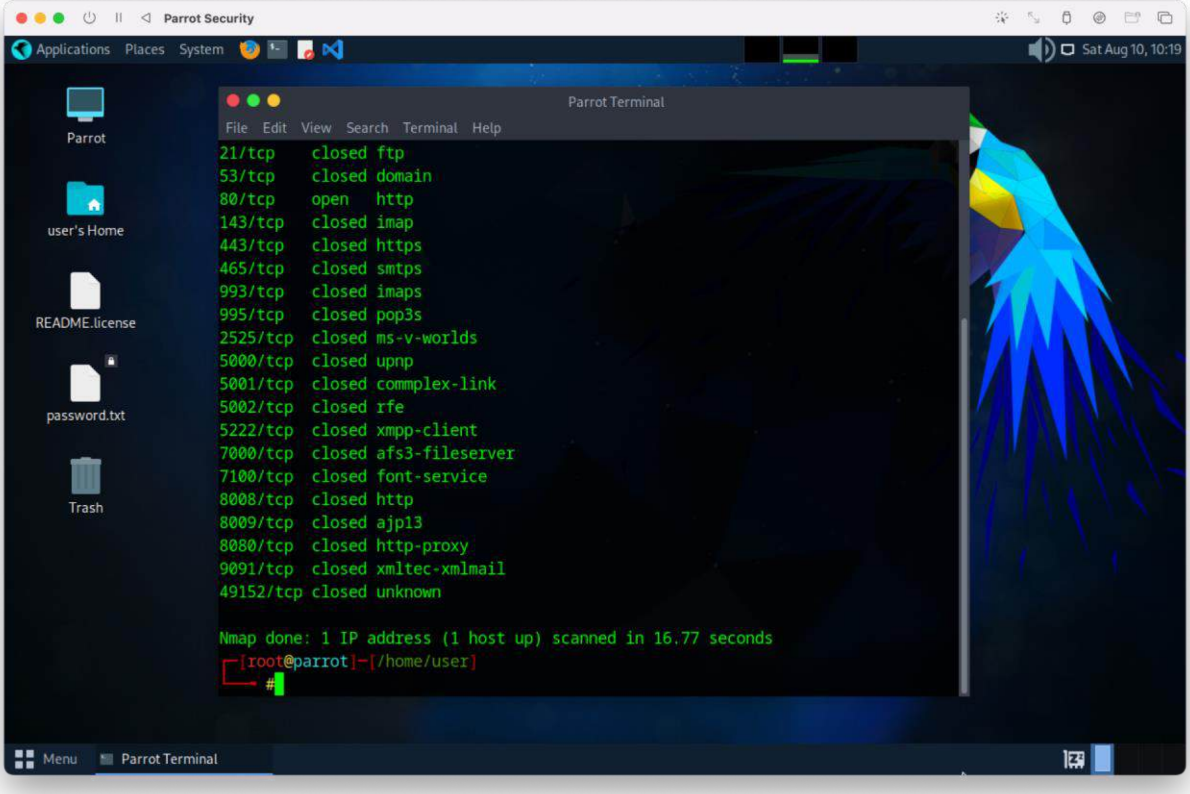
12 Nmap Commands:



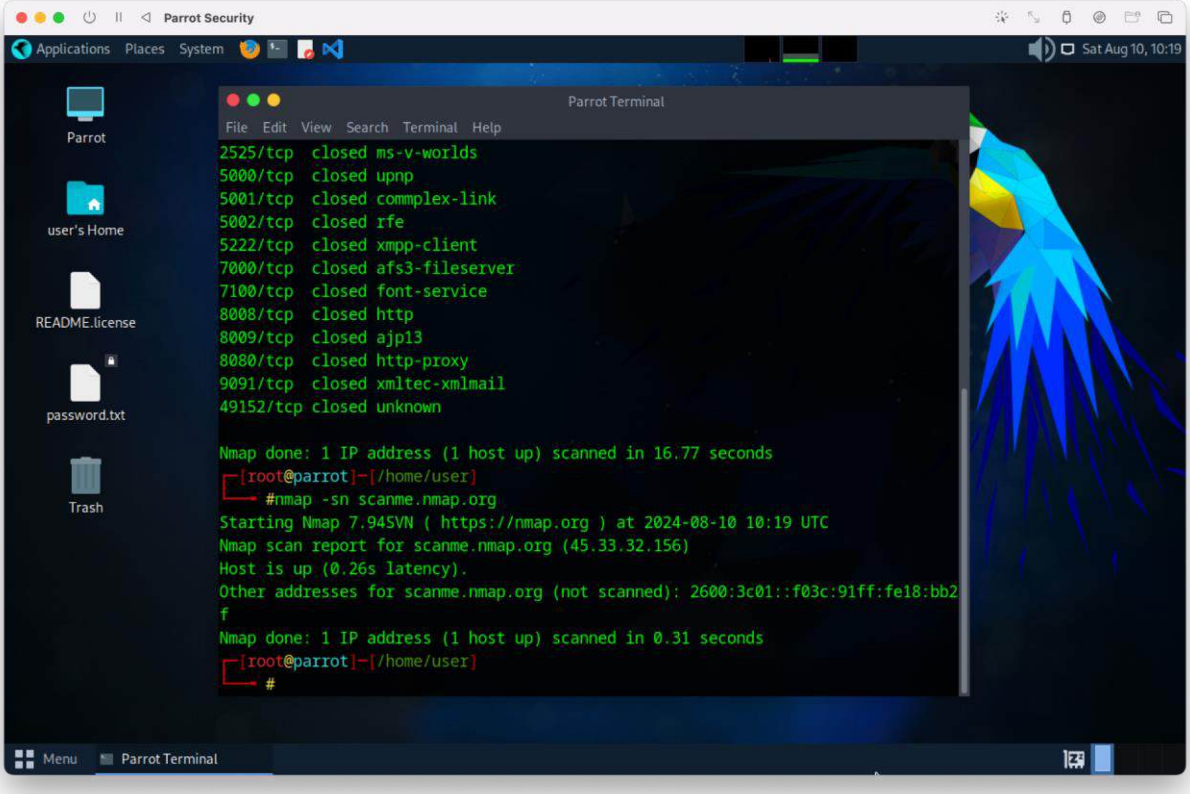
```
┌─[user@parrot]─[~]
└──╼ $sudo su
┌─[root@parrot]─[/home/user]
└──╼ #
```



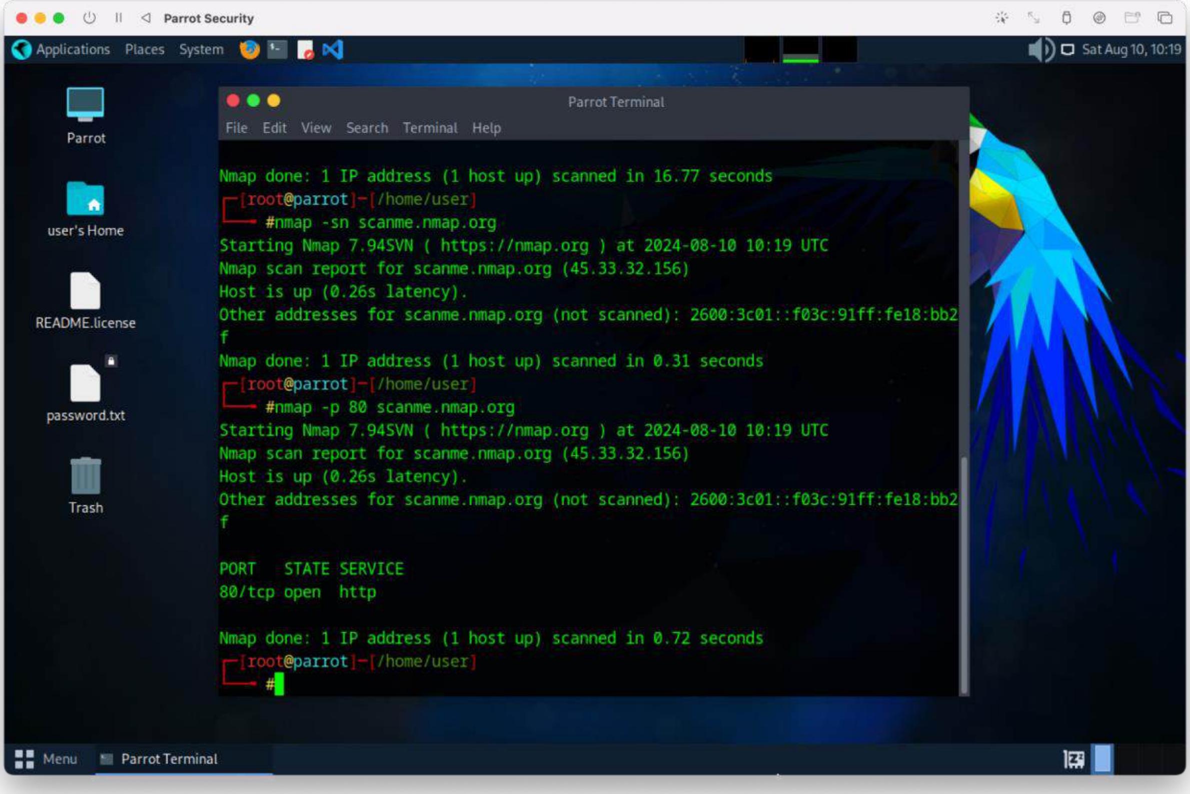
```
└──╼ #nmap scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 10:18 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.29s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f
Not shown: 980 filtered tcp ports (no-response)
PORT      STATE  SERVICE
21/tcp    closed ftp
53/tcp    closed domain
80/tcp    open   http
143/tcp   closed imap
443/tcp   closed https
465/tcp   closed smtps
993/tcp   closed imaps
995/tcp   closed pop3s
2525/tcp  closed ms-v-worlds
5000/tcp  closed upnp
5001/tcp  closed commplex-link
5002/tcp  closed rfe
5222/tcp  closed xmpp-client
7000/tcp  closed afs3-fileserver
7100/tcp  closed font-service
8008/tcp  closed http
```



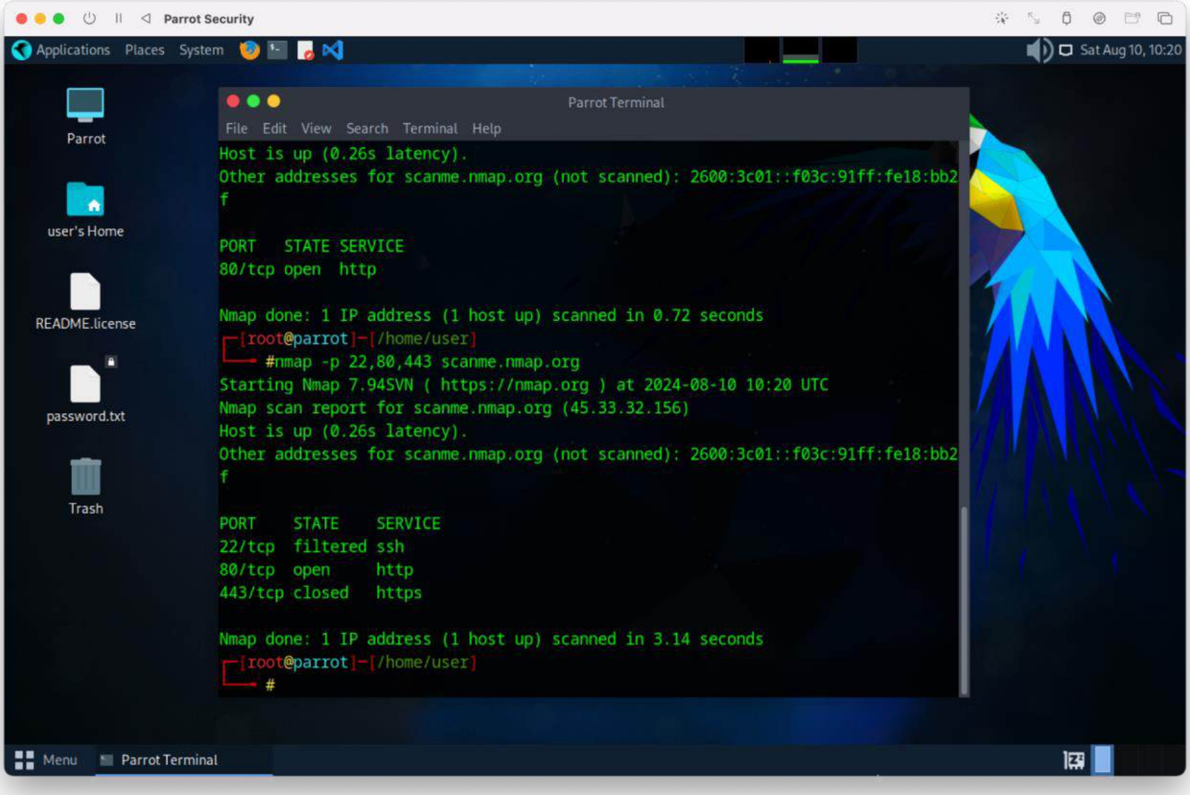
```
21/tcp    closed ftp
53/tcp    closed domain
80/tcp    open   http
143/tcp   closed imap
443/tcp   closed https
465/tcp   closed smtps
993/tcp   closed imaps
995/tcp   closed pop3s
2525/tcp  closed ms-v-worlds
5000/tcp  closed upnp
5001/tcp  closed commplex-link
5002/tcp  closed rfe
5222/tcp  closed xmpp-client
7000/tcp  closed afs3-fileserver
7100/tcp  closed font-service
8008/tcp  closed http
8009/tcp  closed ajp13
8080/tcp  closed http-proxy
9091/tcp  closed xmltec-xmlmail
49152/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 16.77 seconds
┌─[root@parrot]─[/home/user]
└──╼ #
```



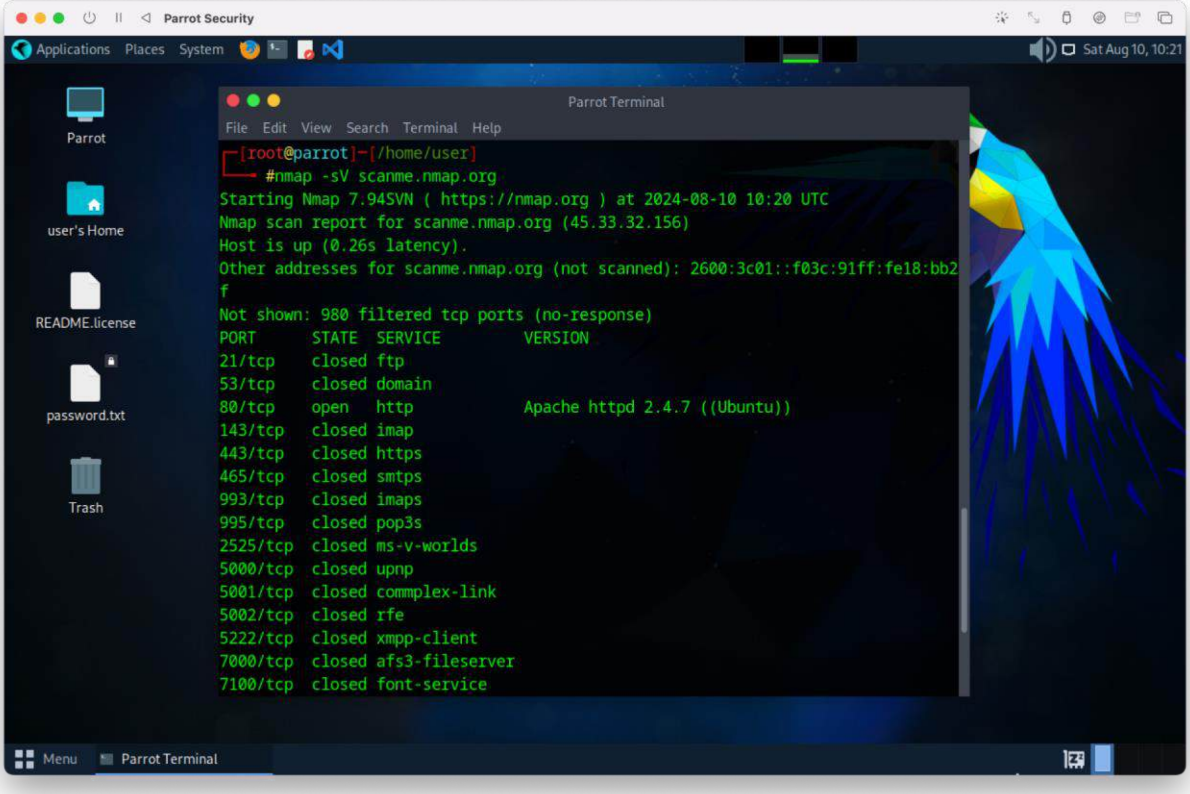
```
2525/tcp  closed ms-v-worlds
5000/tcp  closed upnp
5001/tcp  closed commplex-link
5002/tcp  closed rfe
5222/tcp  closed xmpp-client
7000/tcp  closed afs3-fileserver
7100/tcp  closed font-service
8008/tcp  closed http
8009/tcp  closed ajp13
8080/tcp  closed http-proxy
9091/tcp  closed xmltec-xmlmail
49152/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 16.77 seconds
┌─[root@parrot]─[/home/user]
└──╼ #nmap -sn scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 10:19 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f
Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
┌─[root@parrot]─[/home/user]
└──╼ #
```



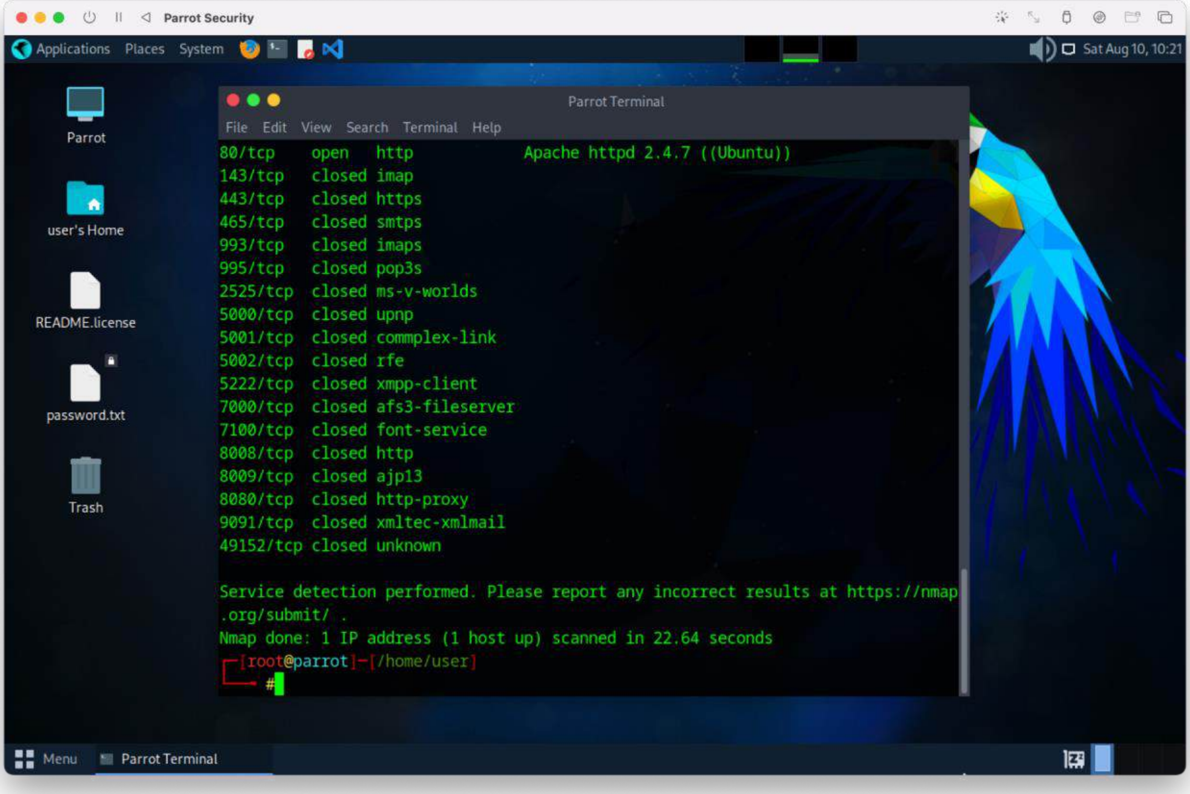
```
Nmap done: 1 IP address (1 host up) scanned in 16.77 seconds
┌─[root@parrot]─[/home/user]
└──╼ #nmap -sn scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 10:19 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f
Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
┌─[root@parrot]─[/home/user]
└──╼ #nmap -p 80 scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 10:19 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.72 seconds
┌─[root@parrot]─[/home/user]
└──╼ #
```



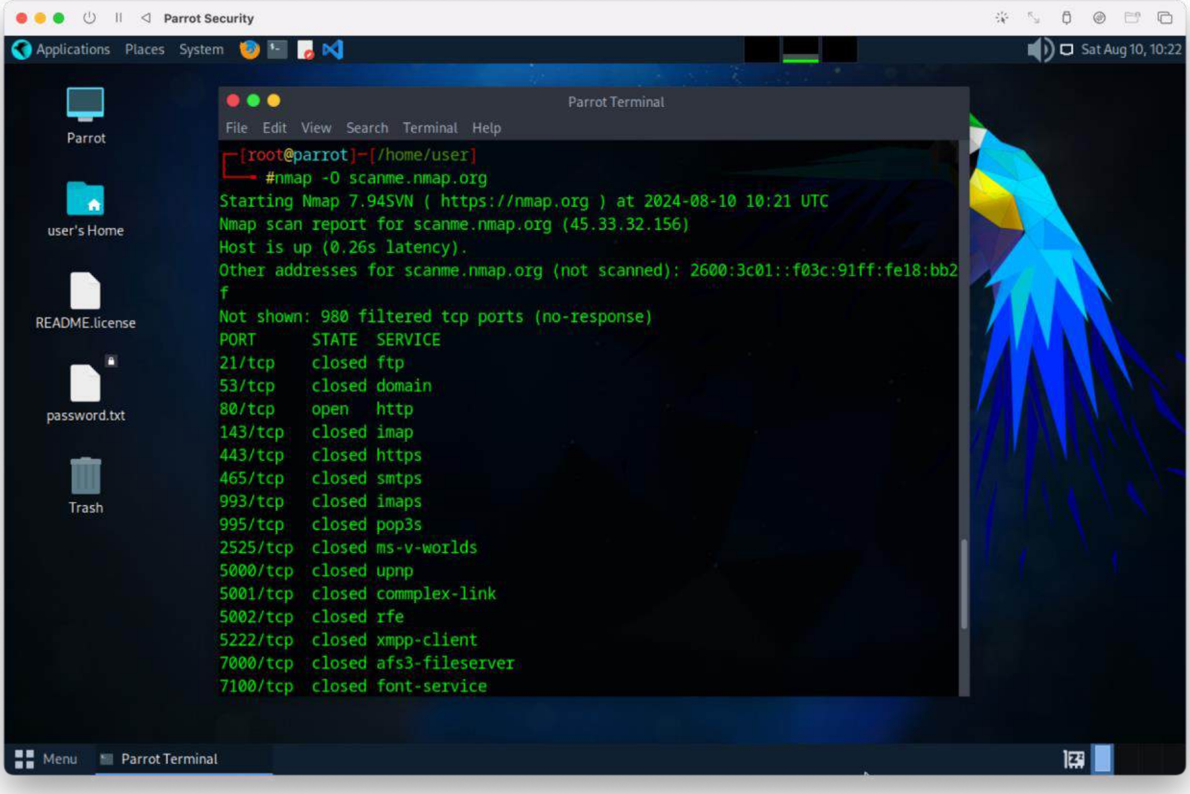
```
Host is up (0.26s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.72 seconds
┌─[root@parrot]─[/home/user]
└──╼ #nmap -p 22,80,443 scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 10:20 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  open     http
443/tcp closed   https

Nmap done: 1 IP address (1 host up) scanned in 3.14 seconds
┌─[root@parrot]─[/home/user]
└──╼ #
```



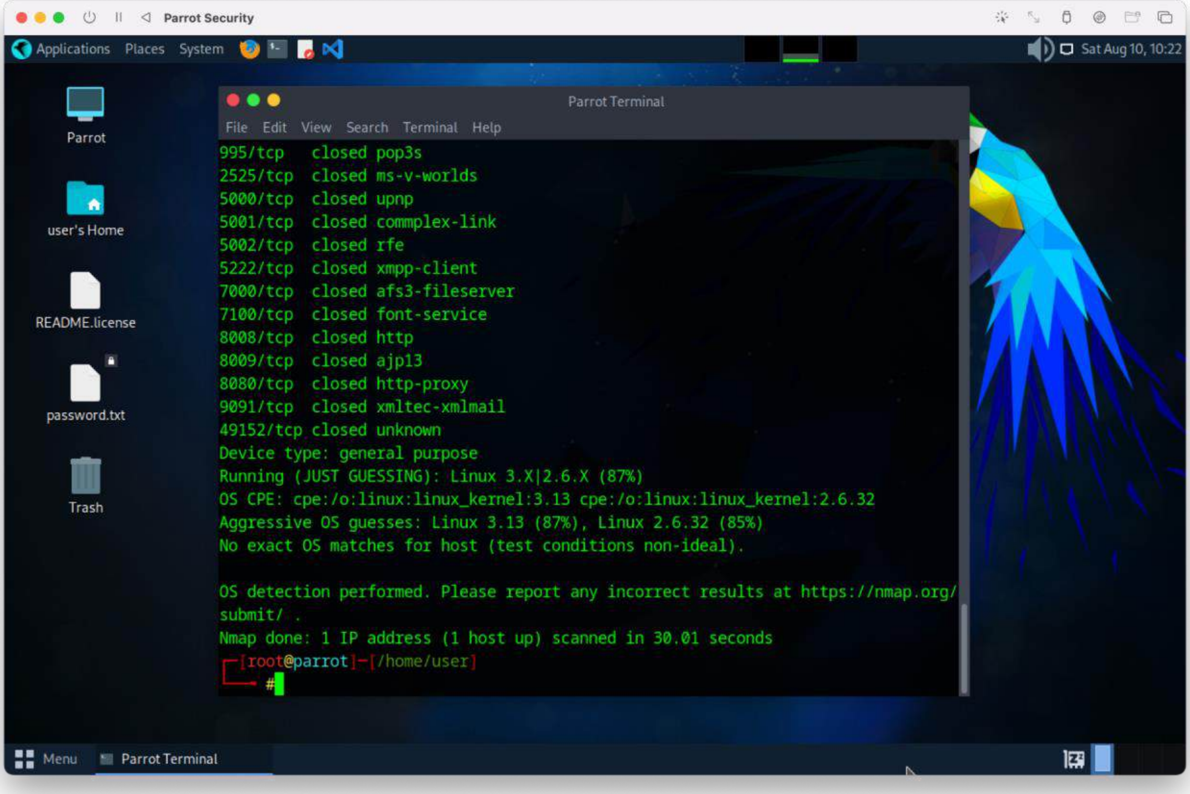
```
┌─[root@parrot]─[/home/user]
└──╼ #nmap -sV scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 10:20 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f
Not shown: 980 filtered tcp ports (no-response)
PORT      STATE  SERVICE          VERSION
21/tcp    closed ftp
53/tcp    closed domain
80/tcp    open   http             Apache httpd 2.4.7 ((Ubuntu))
143/tcp   closed imap
443/tcp   closed https
465/tcp   closed smtps
993/tcp   closed imaps
995/tcp   closed pop3s
2525/tcp  closed ms-v-worlds
5000/tcp  closed upnp
5001/tcp  closed commplex-link
5002/tcp  closed rfe
5222/tcp  closed xmpp-client
7000/tcp  closed afs3-fileserver
7100/tcp  closed font-service
```



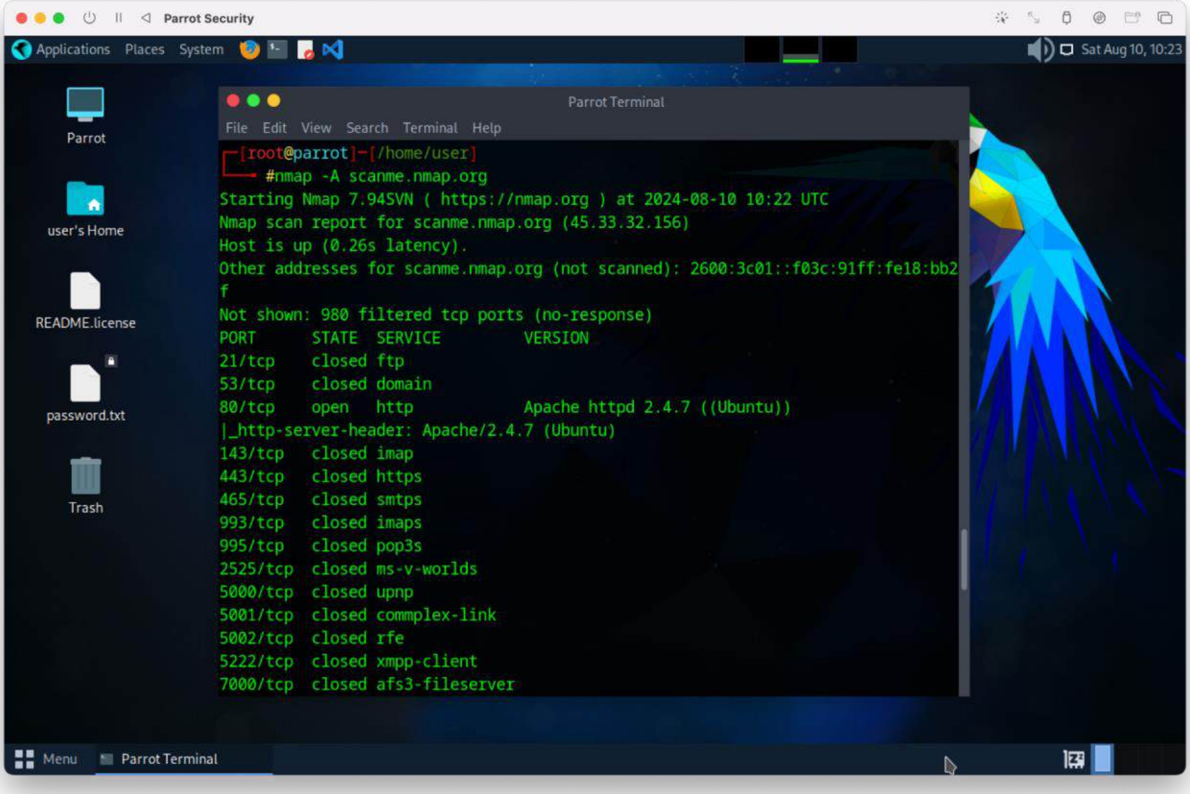
```
80/tcp    open   http             Apache httpd 2.4.7 ((Ubuntu))
143/tcp   closed imap
443/tcp   closed https
465/tcp   closed smtps
993/tcp   closed imaps
995/tcp   closed pop3s
2525/tcp  closed ms-v-worlds
5000/tcp  closed upnp
5001/tcp  closed commplex-link
5002/tcp  closed rfe
5222/tcp  closed xmpp-client
7000/tcp  closed afs3-fileserver
7100/tcp  closed font-service
8008/tcp  closed http
8009/tcp  closed ajp13
8080/tcp  closed http-proxy
9091/tcp  closed xmltec-xmlmail
49152/tcp closed unknown

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.64 seconds
┌─[root@parrot]─[/home/user]
└──╼ #
```



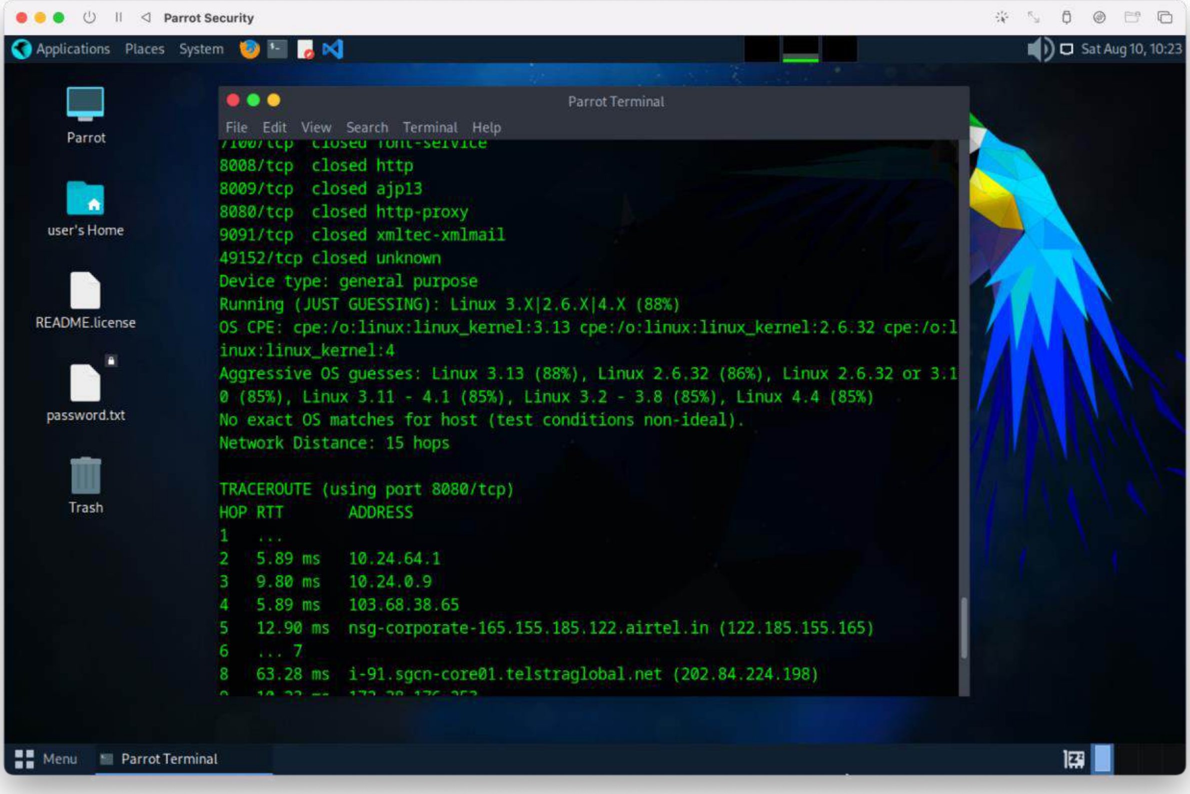
```
┌─[root@parrot]─[/home/user]
└──╼ #nmap -O scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 10:21 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f
Not shown: 980 filtered tcp ports (no-response)
PORT      STATE  SERVICE
21/tcp    closed ftp
53/tcp    closed domain
80/tcp    open   http
143/tcp   closed imap
443/tcp   closed https
465/tcp   closed smtps
993/tcp   closed imaps
995/tcp   closed pop3s
2525/tcp  closed ms-v-worlds
5000/tcp  closed upnp
5001/tcp  closed commplex-link
5002/tcp  closed rfe
5222/tcp  closed xmpp-client
7000/tcp  closed afs3-fileserver
7100/tcp  closed font-service
```



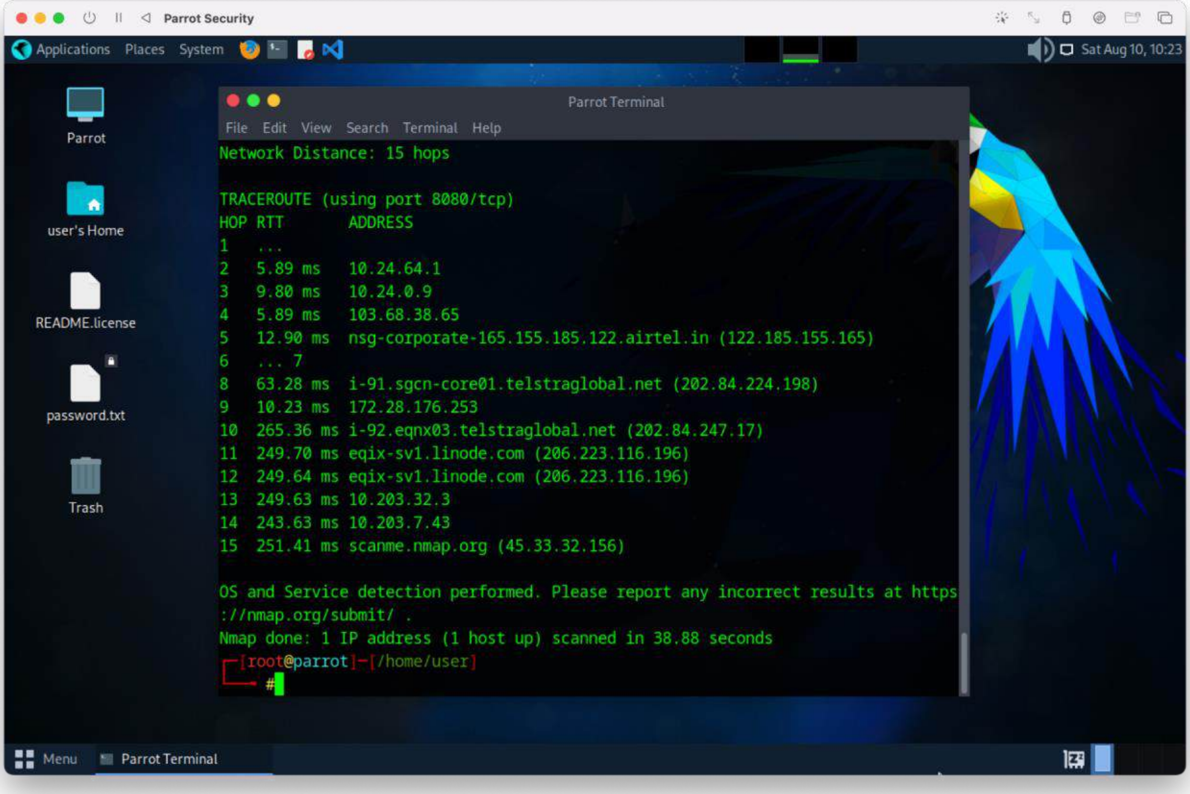
```
995/tcp   closed pop3s
2525/tcp  closed ms-v-worlds
5000/tcp  closed upnp
5001/tcp  closed commplex-link
5002/tcp  closed rfe
5222/tcp  closed xmpp-client
7000/tcp  closed afs3-fileserver
7100/tcp  closed font-service
8008/tcp  closed http
8009/tcp  closed ajp13
8080/tcp  closed http-proxy
9091/tcp  closed xmltec-xmlmail
49152/tcp closed unknown
Device type: general purpose
Running (JUST GUESSING): Linux 3.X|2.6.X (87%)
OS CPE: cpe:/o:linux:linux_kernel:3.13 cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: Linux 3.13 (87%), Linux 2.6.32 (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.01 seconds
┌─[root@parrot]─[/home/user]
└──╼ #
```



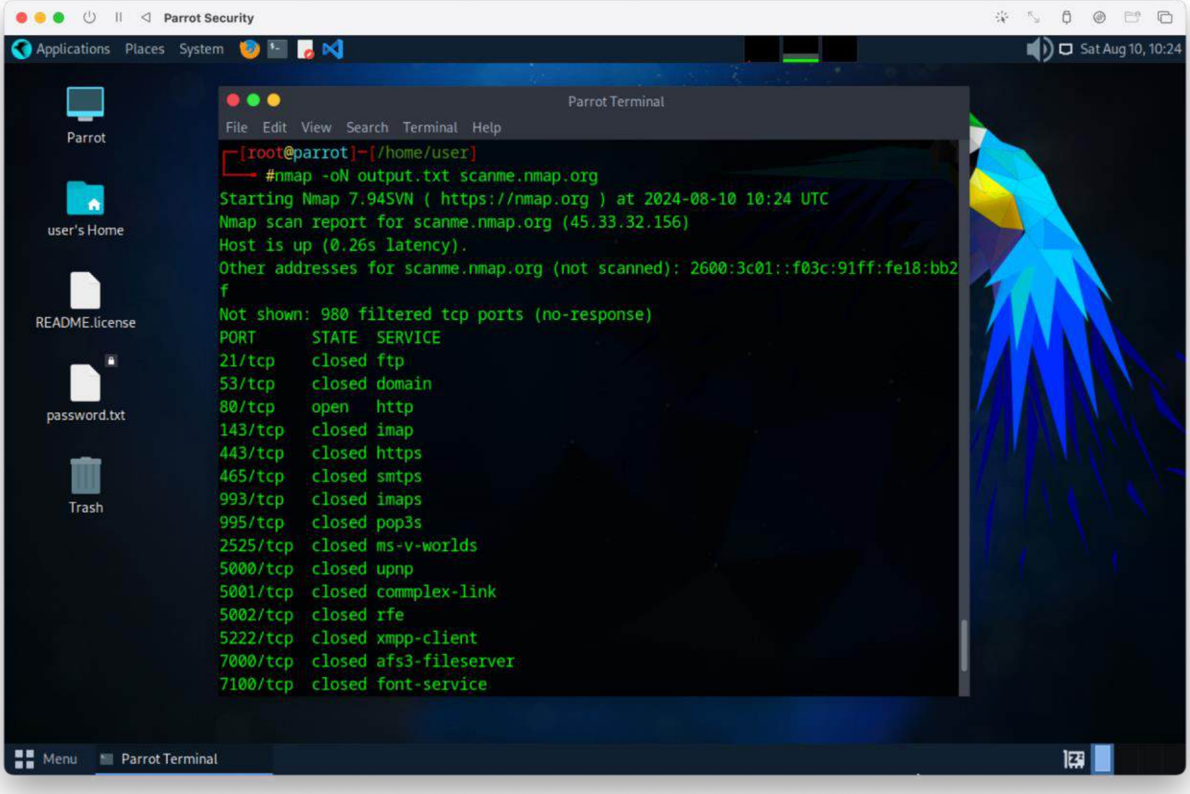
```
┌─[root@parrot]─[/home/user]
└──╼ #nmap -A scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 10:22 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f
Not shown: 980 filtered tcp ports (no-response)
PORT      STATE  SERVICE         VERSION
21/tcp    closed ftp
53/tcp    closed domain
80/tcp    open   http            Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
143/tcp   closed imap
443/tcp   closed https
465/tcp   closed smtps
993/tcp   closed imaps
995/tcp   closed pop3s
2525/tcp  closed ms-v-worlds
5000/tcp  closed upnp
5001/tcp  closed commplex-link
5002/tcp  closed rfe
5222/tcp  closed xmpp-client
7000/tcp  closed afs3-fileserver
```



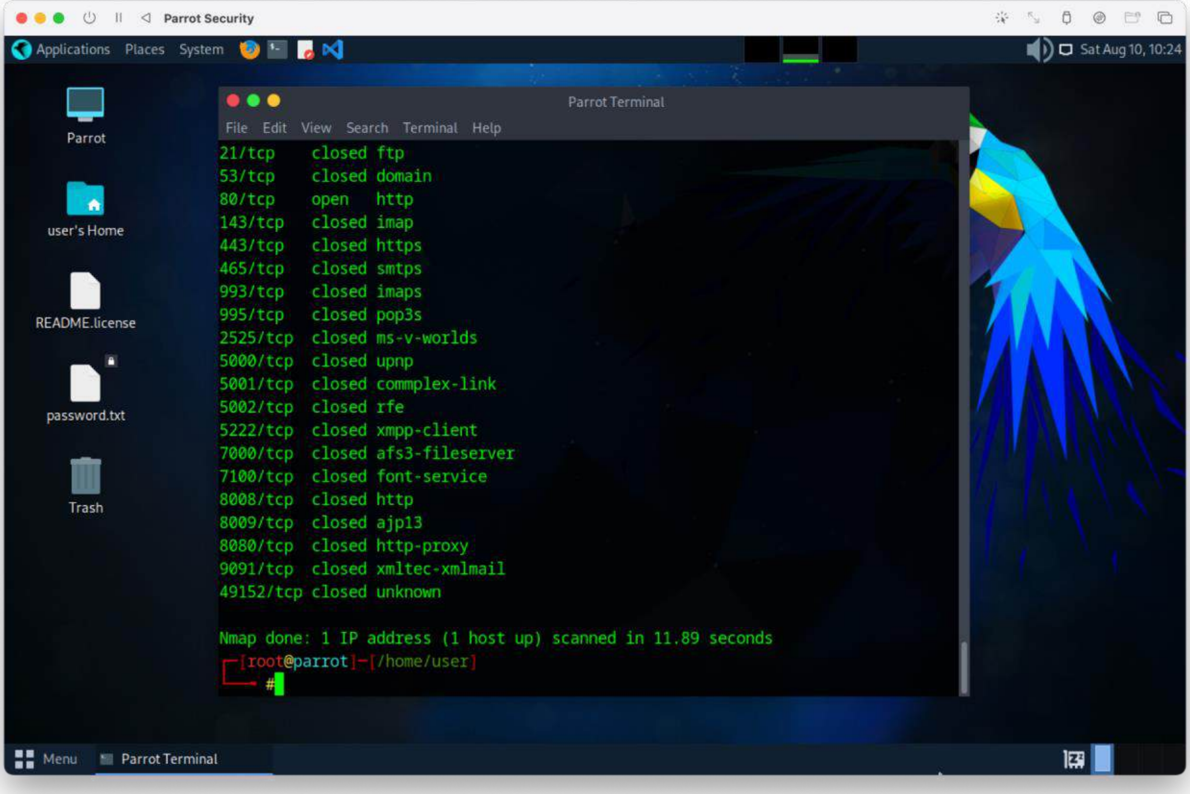
```
7100/tcp  closed font-service
8008/tcp  closed http
8009/tcp  closed ajp13
8080/tcp  closed http-proxy
9091/tcp  closed xmltec-xmlmail
49152/tcp closed unknown
Device type: general purpose
Running (JUST GUESSING): Linux 3.X|2.6.X|4.X (88%)
OS CPE: cpe:/o:linux:linux_kernel:3.13 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:l
inux:linux_kernel:4
Aggressive OS guesses: Linux 3.13 (88%), Linux 2.6.32 (86%), Linux 2.6.32 or 3.1
0 (85%), Linux 3.11 - 4.1 (85%), Linux 3.2 - 3.8 (85%), Linux 4.4 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 15 hops

TRACEROUTE (using port 8080/tcp)
HOP RTT       ADDRESS
1   ...
2   5.89 ms   10.24.64.1
3   9.80 ms   10.24.0.9
4   5.89 ms   103.68.38.65
5   12.90 ms  nsg-corporate-165.155.185.122.airtel.in (122.185.155.165)
6   ... 7
8   63.28 ms  i-91.sgcn-core01.telstraglobal.net (202.84.224.198)
9   10.23 ms  172.28.176.253
```



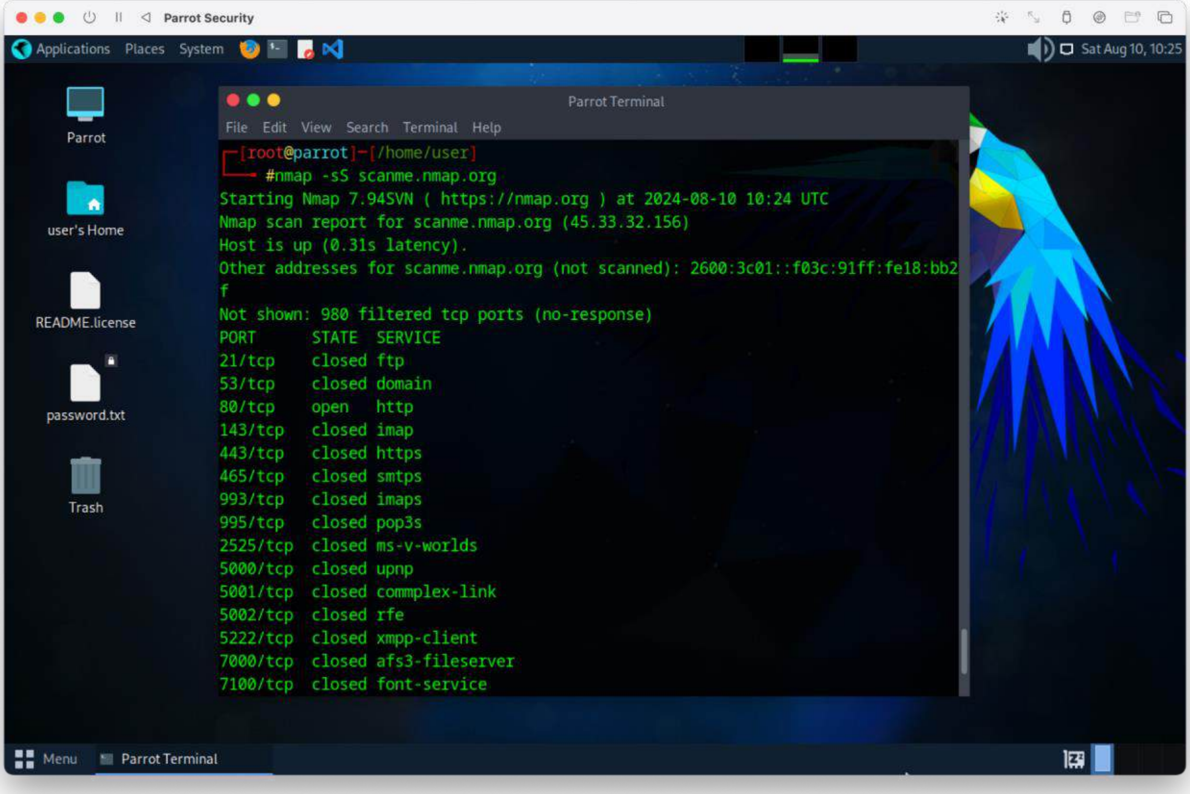
```
Network Distance: 15 hops

TRACEROUTE (using port 8080/tcp)
HOP RTT       ADDRESS
1   ...
2   5.89 ms   10.24.64.1
3   9.80 ms   10.24.0.9
4   5.89 ms   103.68.38.65
5   12.90 ms  nsg-corporate-165.155.185.122.airtel.in (122.185.155.165)
6   ... 7
8   63.28 ms  i-91.sgcn-core01.telstraglobal.net (202.84.224.198)
9   10.23 ms  172.28.176.253
10  265.36 ms i-92.eqnx03.telstraglobal.net (202.84.247.17)
11  249.70 ms eqix-sv1.linode.com (206.223.116.196)
12  249.64 ms eqix-sv1.linode.com (206.223.116.196)
13  249.63 ms 10.203.32.3
14  243.63 ms 10.203.7.43
15  251.41 ms scanme.nmap.org (45.33.32.156)

OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.88 seconds
┌─[root@parrot]─[/home/user]
└──╼ #
```



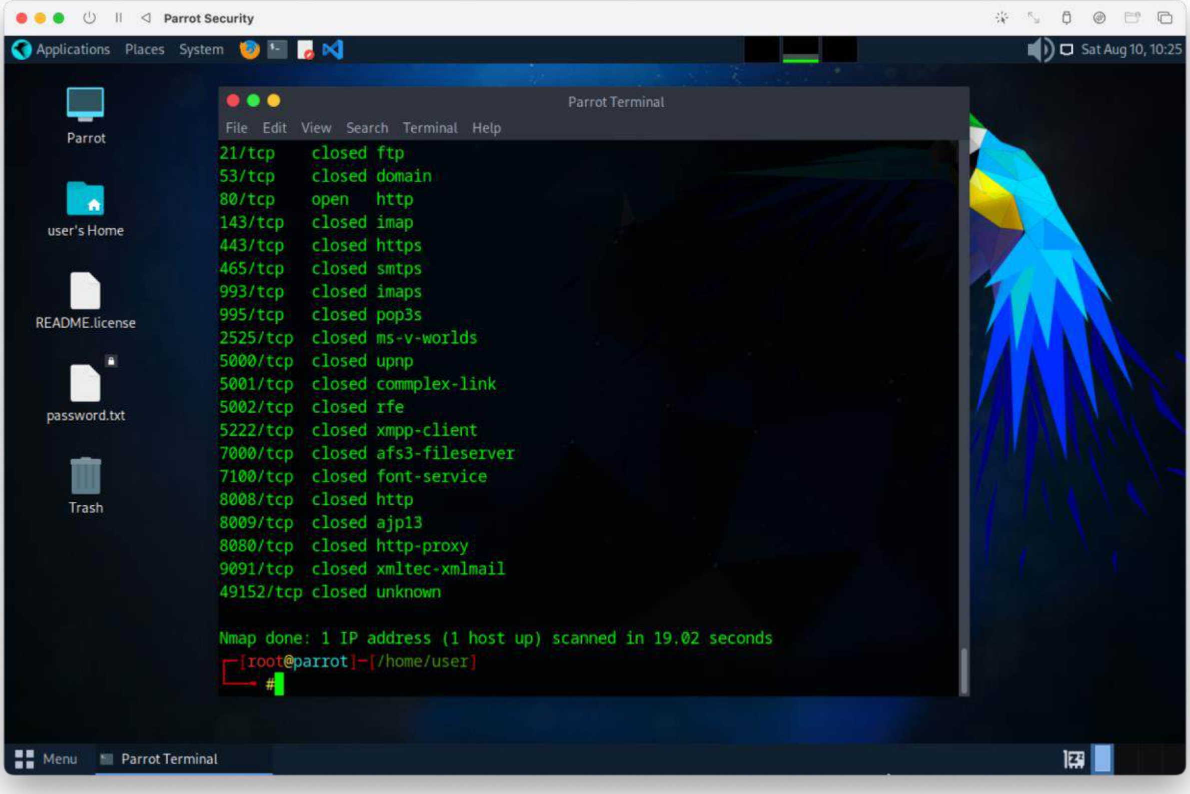
```
┌─[root@parrot]─[/home/user]
└──╼ #nmap -oN output.txt scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 10:24 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f
Not shown: 980 filtered tcp ports (no-response)
PORT      STATE  SERVICE
21/tcp    closed ftp
53/tcp    closed domain
80/tcp    open   http
143/tcp   closed imap
443/tcp   closed https
465/tcp   closed smtps
993/tcp   closed imaps
995/tcp   closed pop3s
2525/tcp  closed ms-v-worlds
5000/tcp  closed upnp
5001/tcp  closed commplex-link
5002/tcp  closed rfe
5222/tcp  closed xmpp-client
7000/tcp  closed afs3-fileserver
7100/tcp  closed font-service
```



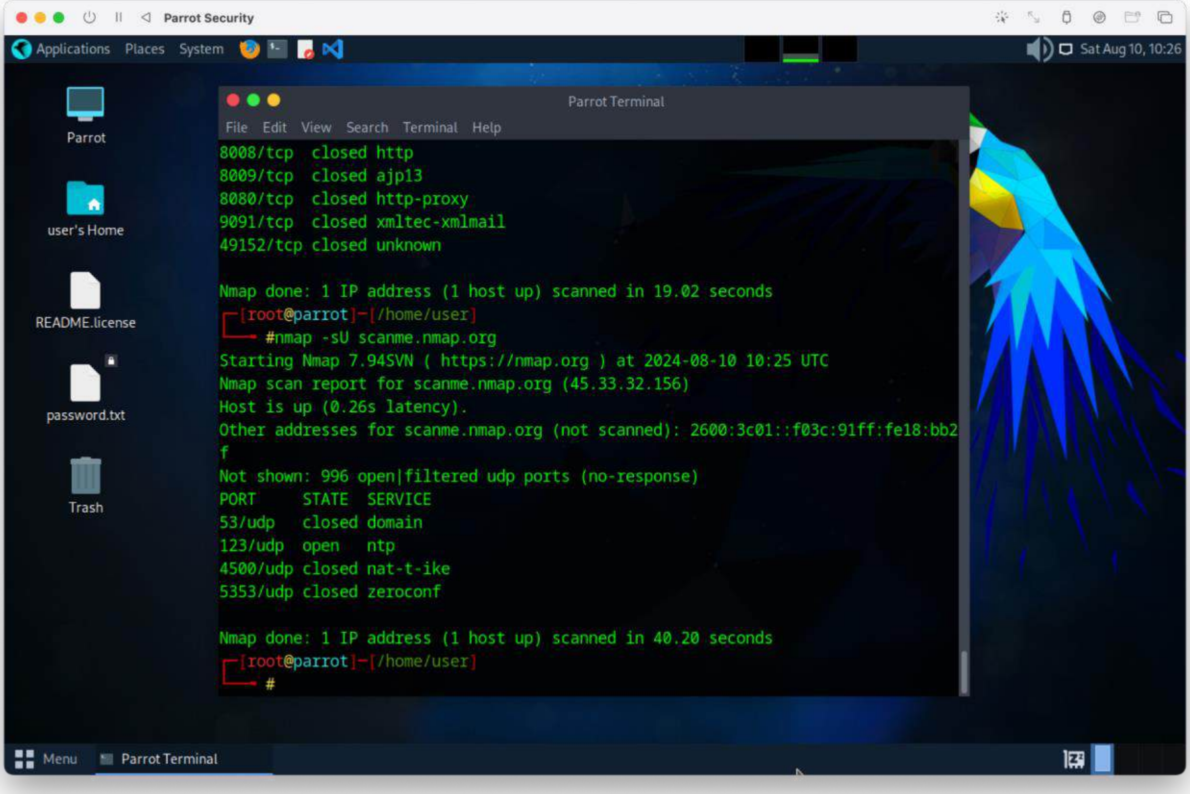
```
21/tcp    closed ftp
53/tcp    closed domain
80/tcp    open   http
143/tcp   closed imap
443/tcp   closed https
465/tcp   closed smtps
993/tcp   closed imaps
995/tcp   closed pop3s
2525/tcp  closed ms-v-worlds
5000/tcp  closed upnp
5001/tcp  closed commplex-link
5002/tcp  closed rfe
5222/tcp  closed xmpp-client
7000/tcp  closed afs3-fileserver
7100/tcp  closed font-service
8008/tcp  closed http
8009/tcp  closed ajp13
8080/tcp  closed http-proxy
9091/tcp  closed xmltec-xmlmail
49152/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 11.89 seconds
┌─[root@parrot]─[/home/user]
└──╼ #
```



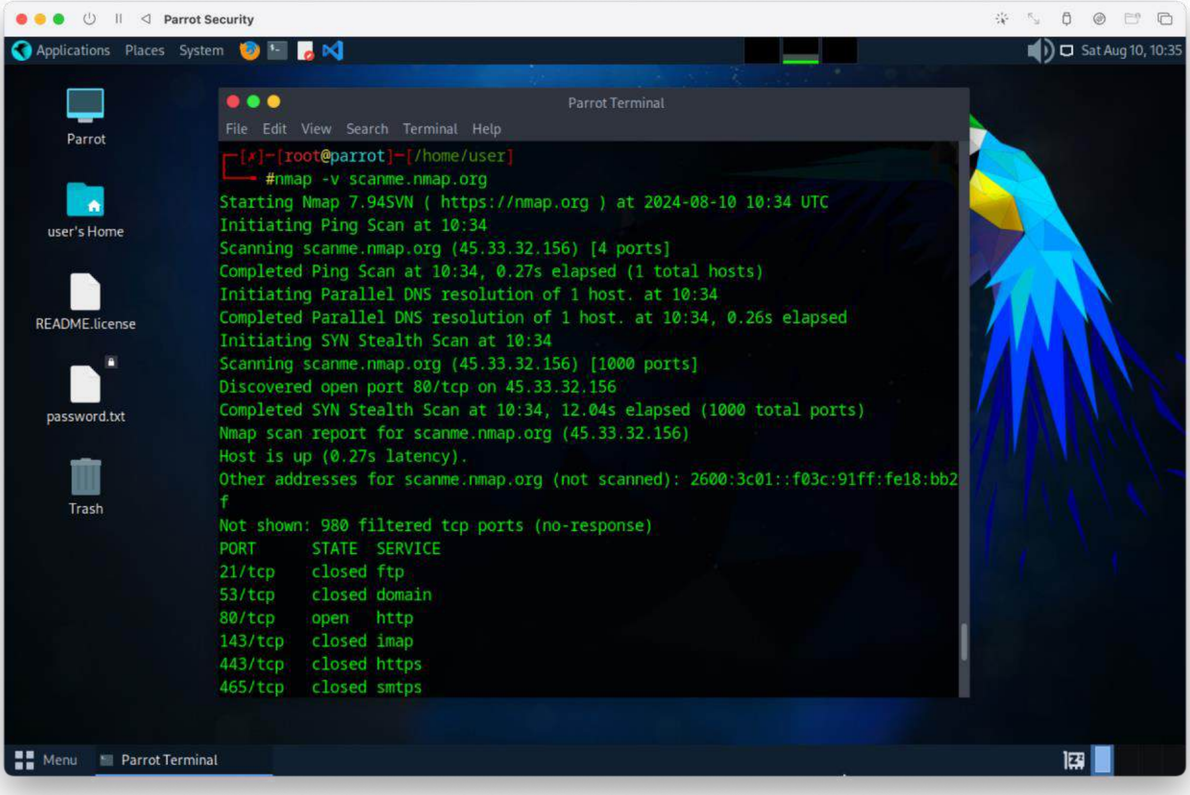
```
┌─[root@parrot]─[/home/user]
└──╼ #nmap -sS scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 10:24 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.31s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f
Not shown: 980 filtered tcp ports (no-response)
PORT      STATE  SERVICE
21/tcp    closed ftp
53/tcp    closed domain
80/tcp    open   http
143/tcp   closed imap
443/tcp   closed https
465/tcp   closed smtps
993/tcp   closed imaps
995/tcp   closed pop3s
2525/tcp  closed ms-v-worlds
5000/tcp  closed upnp
5001/tcp  closed commplex-link
5002/tcp  closed rfe
5222/tcp  closed xmpp-client
7000/tcp  closed afs3-fileserver
7100/tcp  closed font-service
```



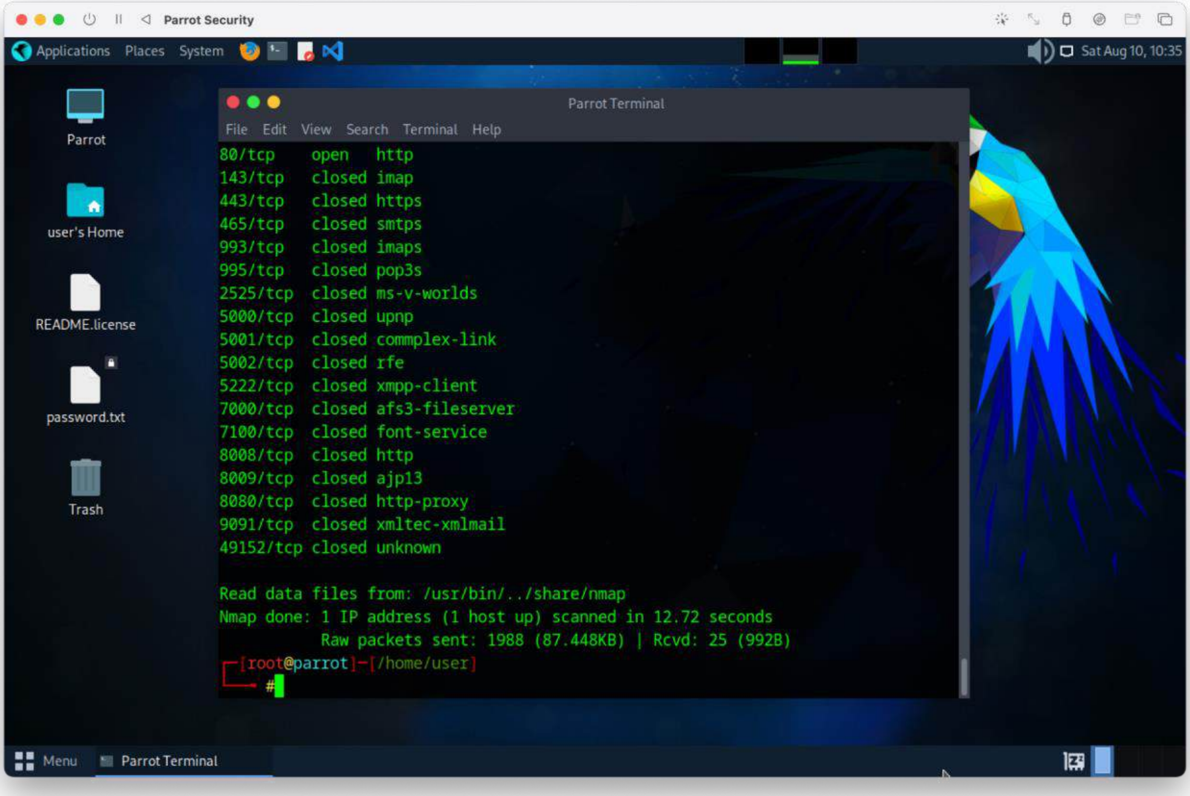
```
21/tcp    closed ftp
53/tcp    closed domain
80/tcp    open   http
143/tcp   closed imap
443/tcp   closed https
465/tcp   closed smtps
993/tcp   closed imaps
995/tcp   closed pop3s
2525/tcp  closed ms-v-worlds
5000/tcp  closed upnp
5001/tcp  closed commplex-link
5002/tcp  closed rfe
5222/tcp  closed xmpp-client
7000/tcp  closed afs3-fileserver
7100/tcp  closed font-service
8008/tcp  closed http
8009/tcp  closed ajp13
8080/tcp  closed http-proxy
9091/tcp  closed xmltec-xmlmail
49152/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 19.02 seconds
┌─[root@parrot]─[/home/user]
└──╼ #
```



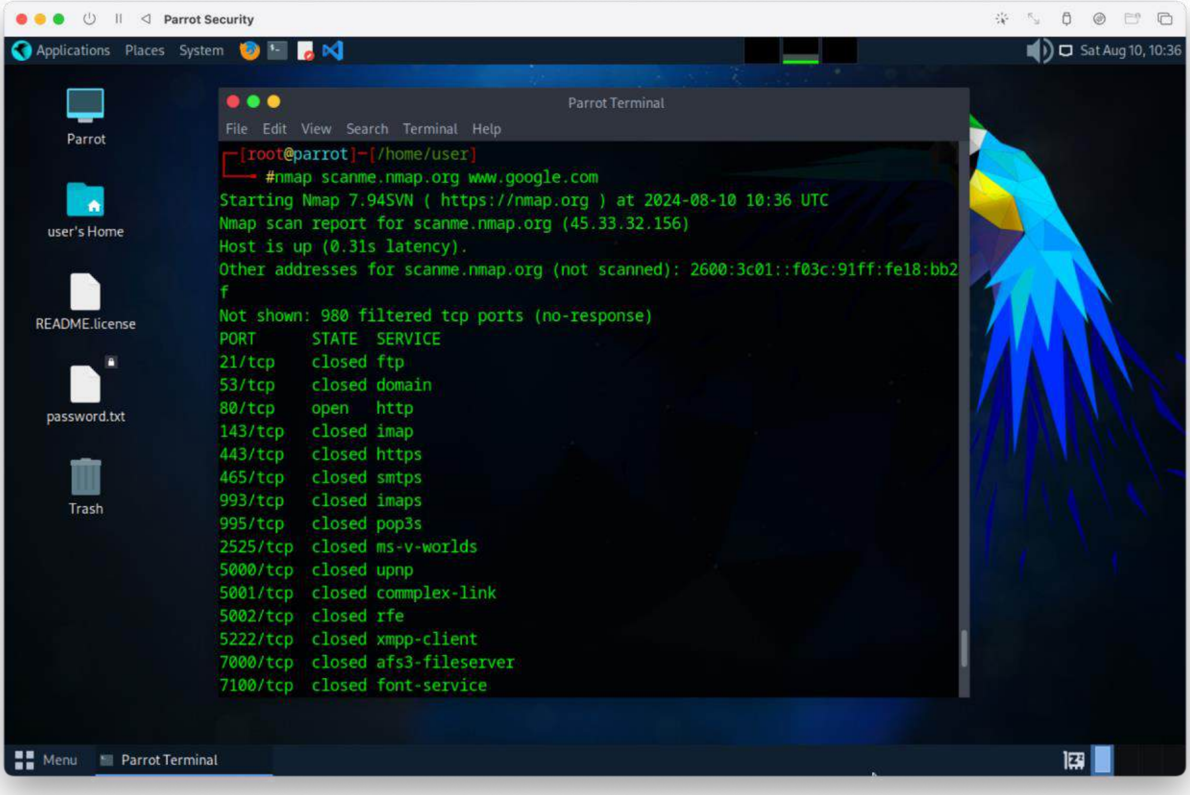
```
8008/tcp  closed http
8009/tcp  closed ajp13
8080/tcp  closed http-proxy
9091/tcp  closed xmltec-xmlmail
49152/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 19.02 seconds
┌─[root@parrot]─[/home/user]
└──╼ #nmap -sU scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 10:25 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f
Not shown: 996 open|filtered udp ports (no-response)
PORT     STATE  SERVICE
53/udp   closed domain
123/udp  open   ntp
4500/udp closed nat-t-ike
5353/udp closed zeroconf

Nmap done: 1 IP address (1 host up) scanned in 40.20 seconds
┌─[root@parrot]─[/home/user]
└──╼ #
```



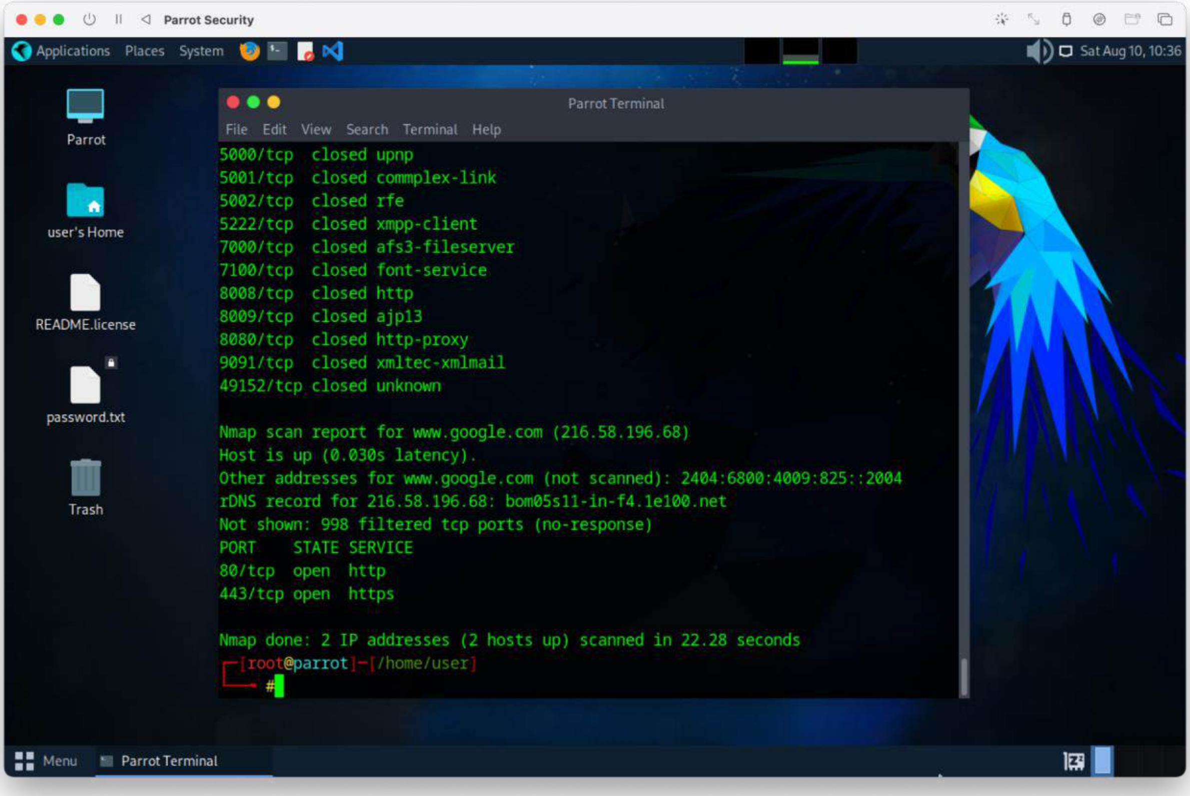
```
┌─[✗]─[root@parrot]─[/home/user]
└──╼ #nmap -v scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 10:34 UTC
Initiating Ping Scan at 10:34
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 10:34, 0.27s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:34
Completed Parallel DNS resolution of 1 host. at 10:34, 0.26s elapsed
Initiating SYN Stealth Scan at 10:34
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 80/tcp on 45.33.32.156
Completed SYN Stealth Scan at 10:34, 12.04s elapsed (1000 total ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.27s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f
Not shown: 980 filtered tcp ports (no-response)
PORT      STATE  SERVICE
21/tcp    closed ftp
53/tcp    closed domain
80/tcp    open   http
143/tcp   closed imap
443/tcp   closed https
465/tcp   closed smtps
```



```
80/tcp    open   http
143/tcp   closed imap
443/tcp   closed https
465/tcp   closed smtps
993/tcp   closed imaps
995/tcp   closed pop3s
2525/tcp  closed ms-v-worlds
5000/tcp  closed upnp
5001/tcp  closed commplex-link
5002/tcp  closed rfe
5222/tcp  closed xmpp-client
7000/tcp  closed afs3-fileserver
7100/tcp  closed font-service
8008/tcp  closed http
8009/tcp  closed ajp13
8080/tcp  closed http-proxy
9091/tcp  closed xmltec-xmlmail
49152/tcp closed unknown

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 12.72 seconds
           Raw packets sent: 1988 (87.448KB) | Rcvd: 25 (992B)
┌─[root@parrot]─[/home/user]
└──╼ #
```

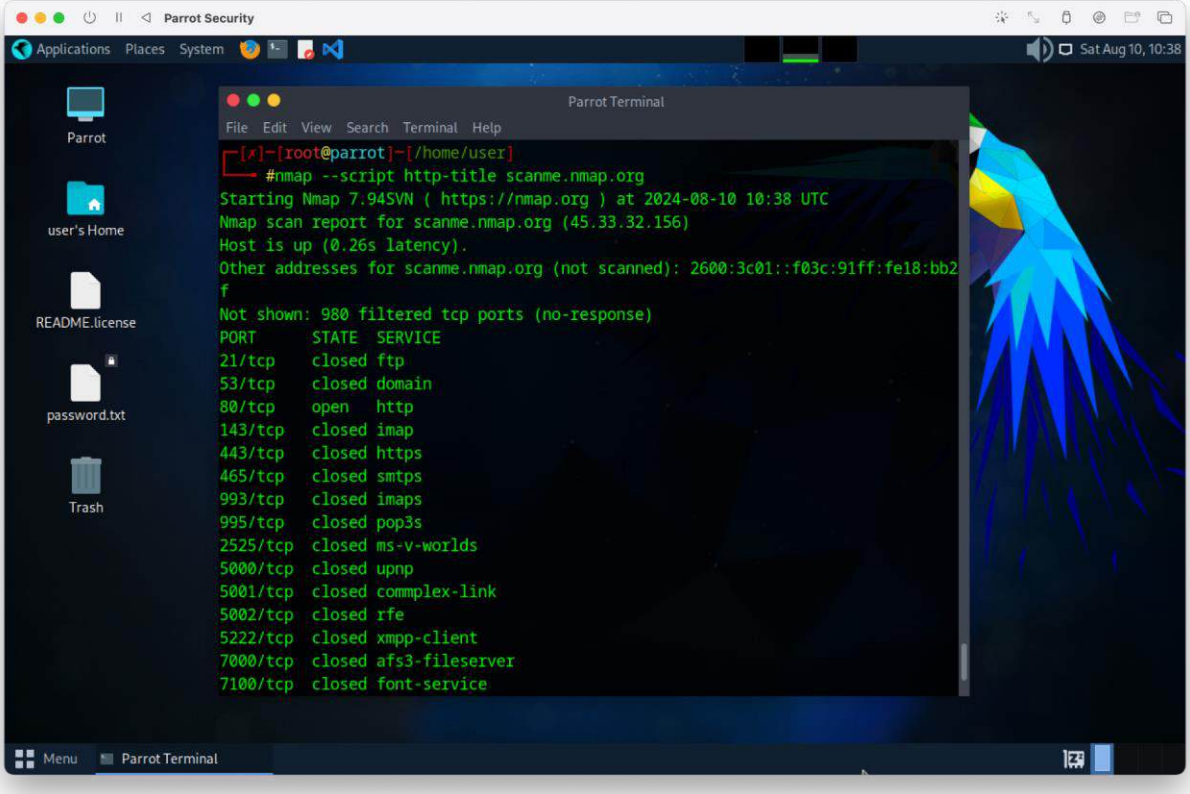


```
┌─[root@parrot]─[/home/user]
└──╼ #nmap scanme.nmap.org www.google.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 10:36 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.31s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f
Not shown: 980 filtered tcp ports (no-response)
PORT      STATE  SERVICE
21/tcp    closed ftp
53/tcp    closed domain
80/tcp    open   http
143/tcp   closed imap
443/tcp   closed https
465/tcp   closed smtps
993/tcp   closed imaps
995/tcp   closed pop3s
2525/tcp  closed ms-v-worlds
5000/tcp  closed upnp
5001/tcp  closed commplex-link
5002/tcp  closed rfe
5222/tcp  closed xmpp-client
7000/tcp  closed afs3-fileserver
7100/tcp  closed font-service
```

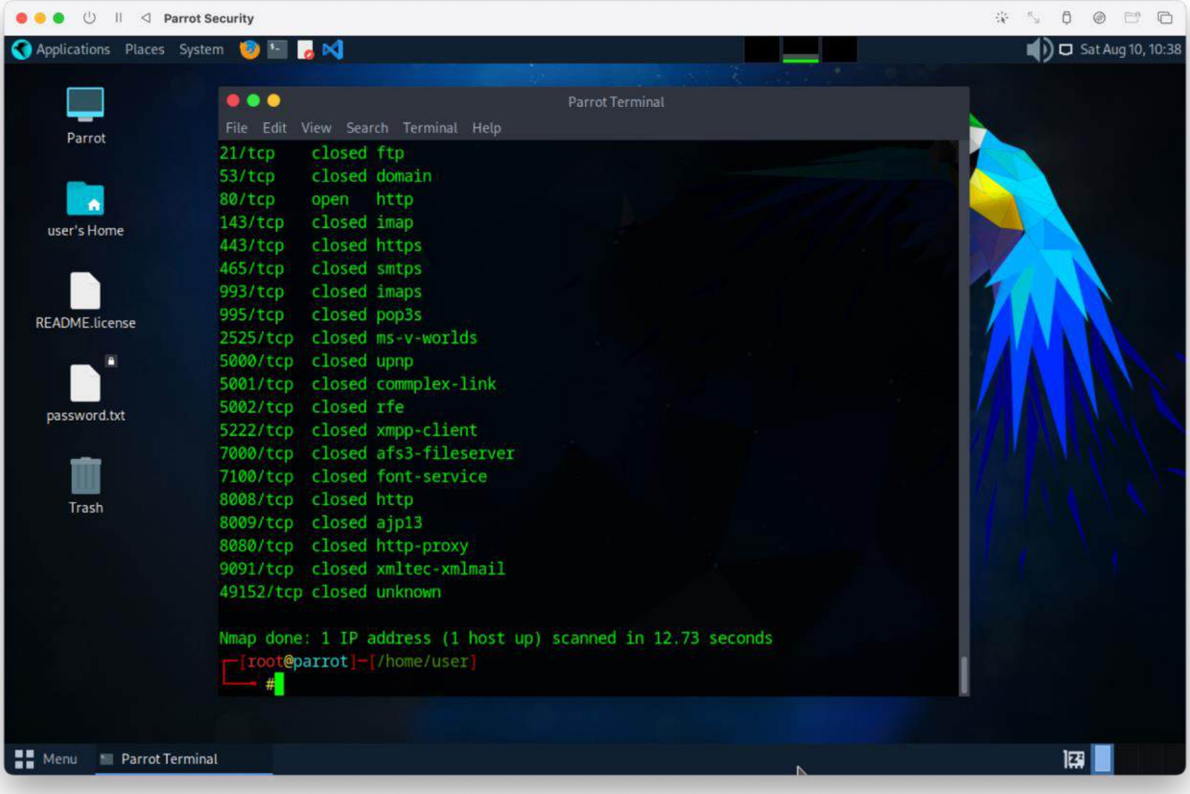


```
5000/tcp  closed upnp
5001/tcp  closed commplex-link
5002/tcp  closed rfe
5222/tcp  closed xmpp-client
7000/tcp  closed afs3-fileserver
7100/tcp  closed font-service
8008/tcp  closed http
8009/tcp  closed ajp13
8080/tcp  closed http-proxy
9091/tcp  closed xmltec-xmlmail
49152/tcp closed unknown

Nmap scan report for www.google.com (216.58.196.68)
Host is up (0.030s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:825::2004
rDNS record for 216.58.196.68: bom05s11-in-f4.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 2 IP addresses (2 hosts up) scanned in 22.28 seconds
┌─[root@parrot]─[/home/user]
└──╼ #
```

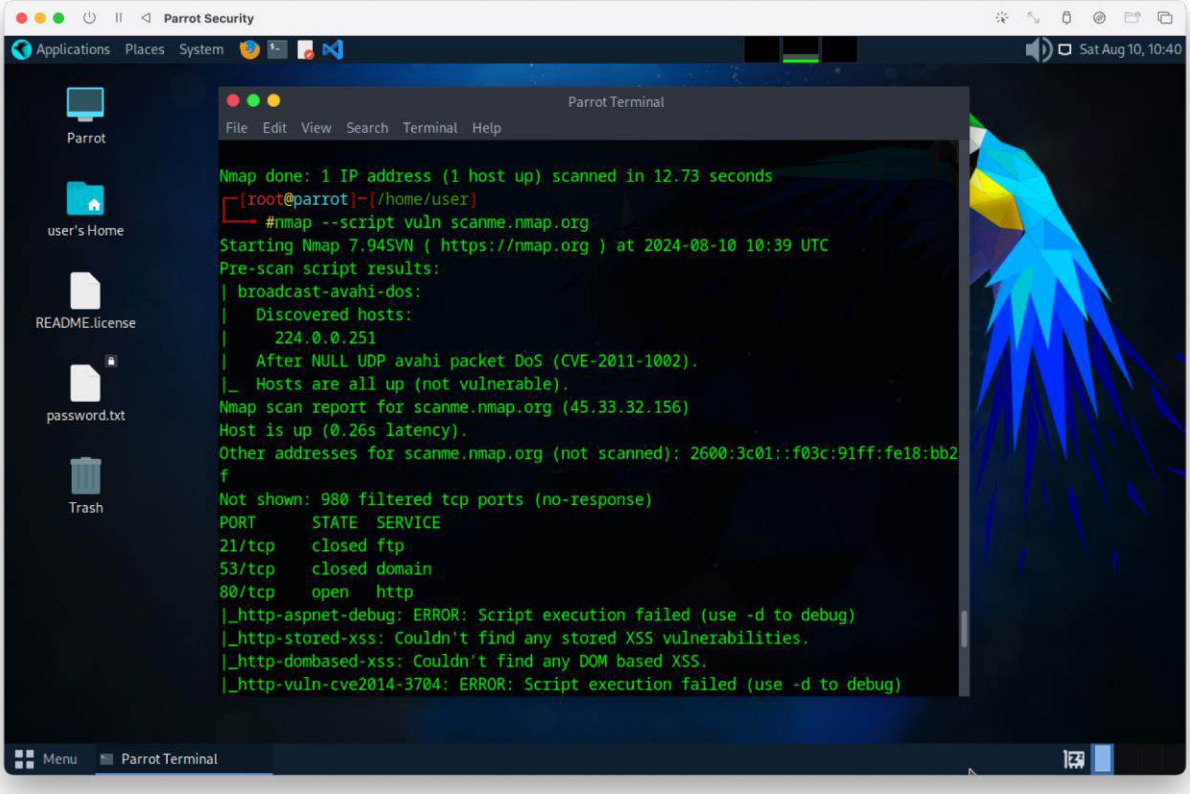
3 Nmap Script Engine (NSE) Script Commands:



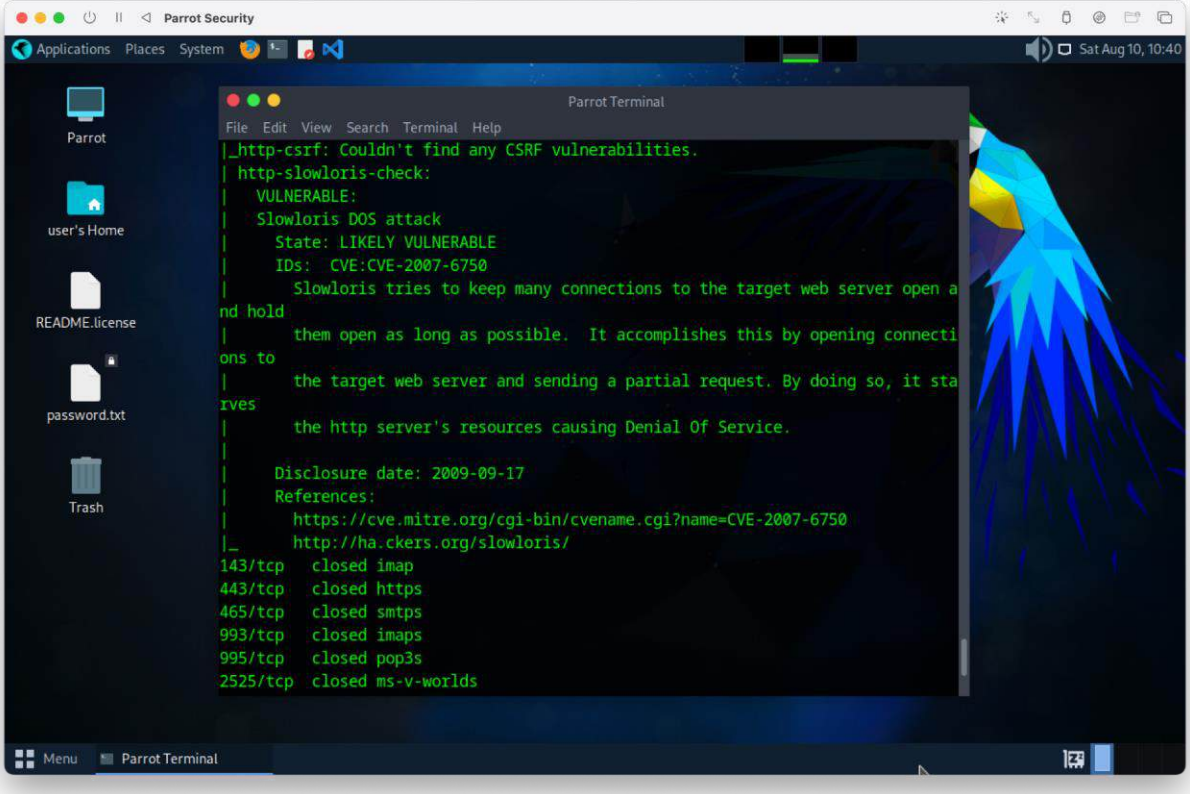
```
┌─[✗]─[root@parrot]─[/home/user]
└──╼ #nmap --script http-title scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 10:38 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f
Not shown: 980 filtered tcp ports (no-response)
PORT      STATE  SERVICE
21/tcp    closed ftp
53/tcp    closed domain
80/tcp    open   http
143/tcp   closed imap
443/tcp   closed https
465/tcp   closed smtps
993/tcp   closed imaps
995/tcp   closed pop3s
2525/tcp  closed ms-v-worlds
5000/tcp  closed upnp
5001/tcp  closed commplex-link
5002/tcp  closed rfe
5222/tcp  closed xmpp-client
7000/tcp  closed afs3-fileserver
7100/tcp  closed font-service
```



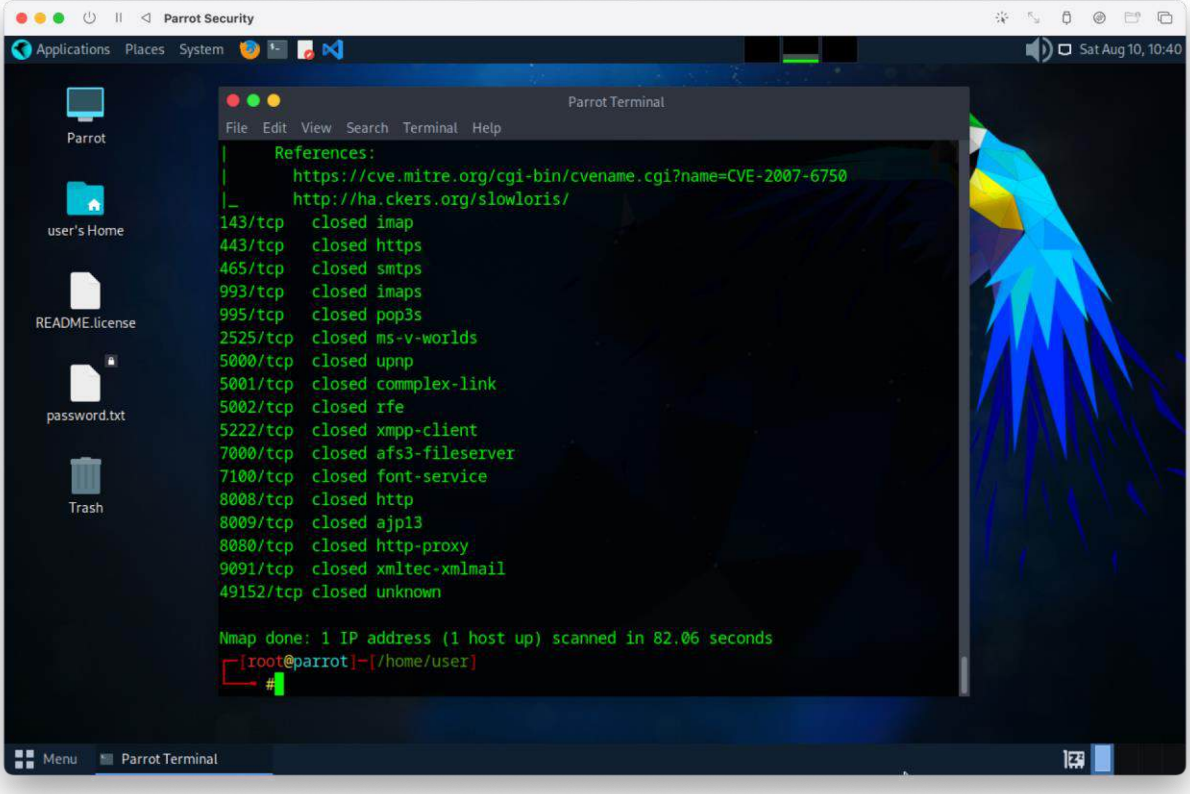
```
21/tcp    closed ftp
53/tcp    closed domain
80/tcp    open   http
143/tcp   closed imap
443/tcp   closed https
465/tcp   closed smtps
993/tcp   closed imaps
995/tcp   closed pop3s
2525/tcp  closed ms-v-worlds
5000/tcp  closed upnp
5001/tcp  closed commplex-link
5002/tcp  closed rfe
5222/tcp  closed xmpp-client
7000/tcp  closed afs3-fileserver
7100/tcp  closed font-service
8008/tcp  closed http
8009/tcp  closed ajp13
8080/tcp  closed http-proxy
9091/tcp  closed xmltec-xmlmail
49152/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 12.73 seconds
┌─[root@parrot]─[/home/user]
└──╼ #
```



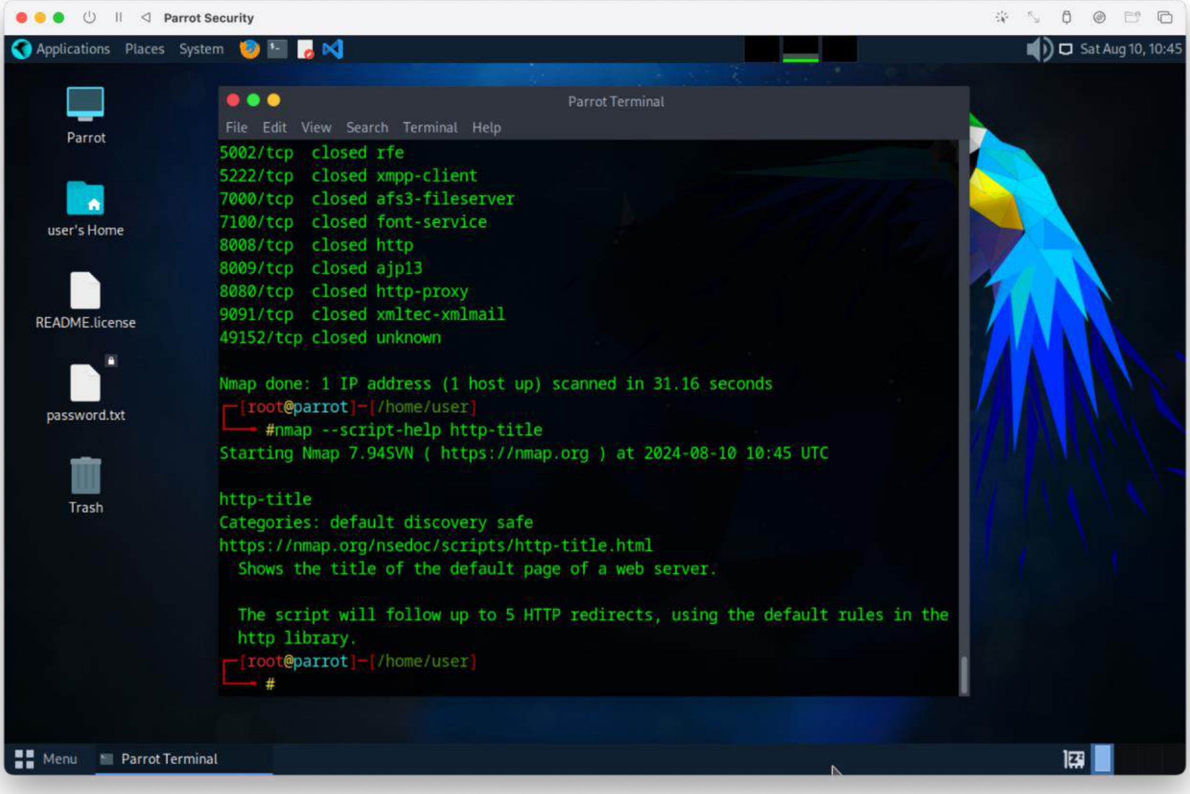
```
Nmap done: 1 IP address (1 host up) scanned in 12.73 seconds
┌─[root@parrot]─[/home/user]
└──╼ #nmap --script vuln scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 10:39 UTC
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f
Not shown: 980 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   closed ftp
53/tcp   closed domain
80/tcp   open   http
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
```



```
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open a
nd hold
|       them open as long as possible.  It accomplishes this by opening connecti
ons to
|       the target web server and sending a partial request. By doing so, it sta
rves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
143/tcp  closed imap
443/tcp  closed https
465/tcp  closed smtps
993/tcp  closed imaps
995/tcp  closed pop3s
2525/tcp closed ms-v-worlds
```

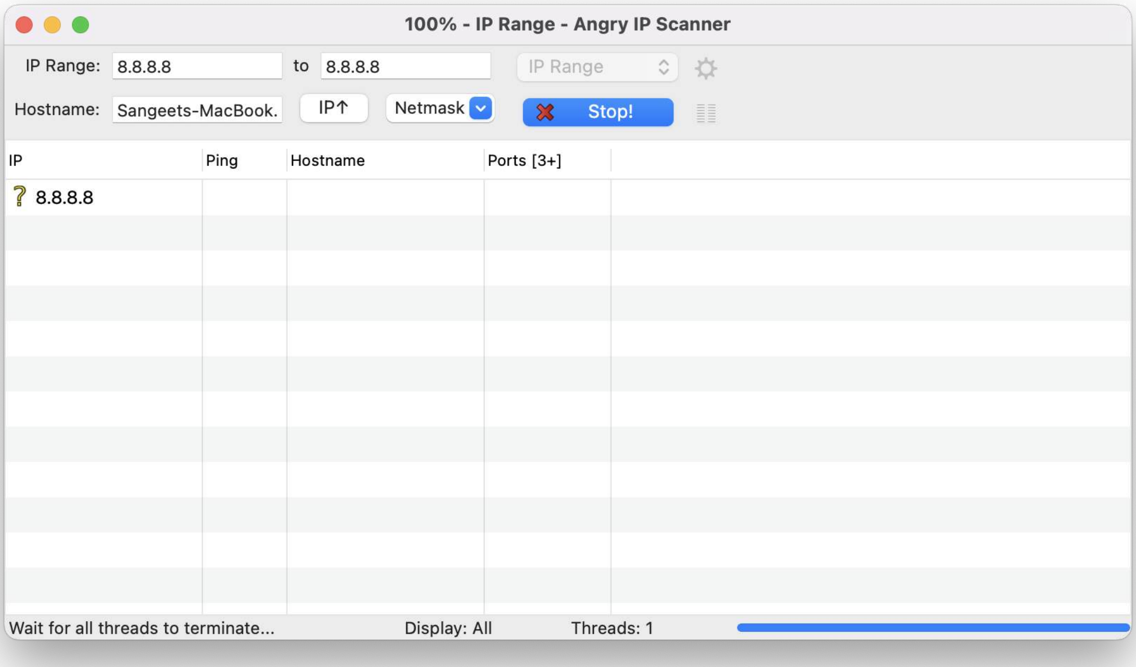


```
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
143/tcp   closed imap
443/tcp   closed https
465/tcp   closed smtps
993/tcp   closed imaps
995/tcp   closed pop3s
2525/tcp  closed ms-v-worlds
5000/tcp  closed upnp
5001/tcp  closed commplex-link
5002/tcp  closed rfe
5222/tcp  closed xmpp-client
7000/tcp  closed afs3-fileserver
7100/tcp  closed font-service
8008/tcp  closed http
8009/tcp  closed ajp13
8080/tcp  closed http-proxy
9091/tcp  closed xmltec-xmlmail
49152/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 82.06 seconds
┌─[root@parrot]─[/home/user]
└──╼ #
```



```
5002/tcp  closed rfe
5222/tcp  closed xmpp-client
7000/tcp  closed afs3-fileserver
7100/tcp  closed font-service
8008/tcp  closed http
8009/tcp  closed ajp13
8080/tcp  closed http-proxy
9091/tcp  closed xmltec-xmlmail
49152/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 31.16 seconds
┌─[root@parrot]─[/home/user]
└──╼ #nmap --script-help http-title
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 10:45 UTC

http-title
Categories: default discovery safe
https://nmap.org/nsedoc/scripts/http-title.html
  Shows the title of the default page of a web server.

  The script will follow up to 5 HTTP redirects, using the default rules in the
  http library.
┌─[root@parrot]─[/home/user]
└──╼ #
```

2) Demonstrate any network scanning free tools other than nmap



100% - IP Range - Angry IP Scanner

IP Range: 8.8.8.8 to 8.8.8.8

Hostname: Sangeets-MacBook.

IP	Ping	Hostname	Ports [3+]
? 8.8.8.8			

Wait for all threads to terminate... Display: All Threads: 1

Note: Students are suggested to use Linux OS based tools or free Windows OS based tools.