Using Nmap in the lab

Start all your lab machines with Win10, Win11 and Kali Linux. Make sure the pings go between the machines and Win10 and W11 machines have Xampp installed and at least Apache and MySQL running on them.

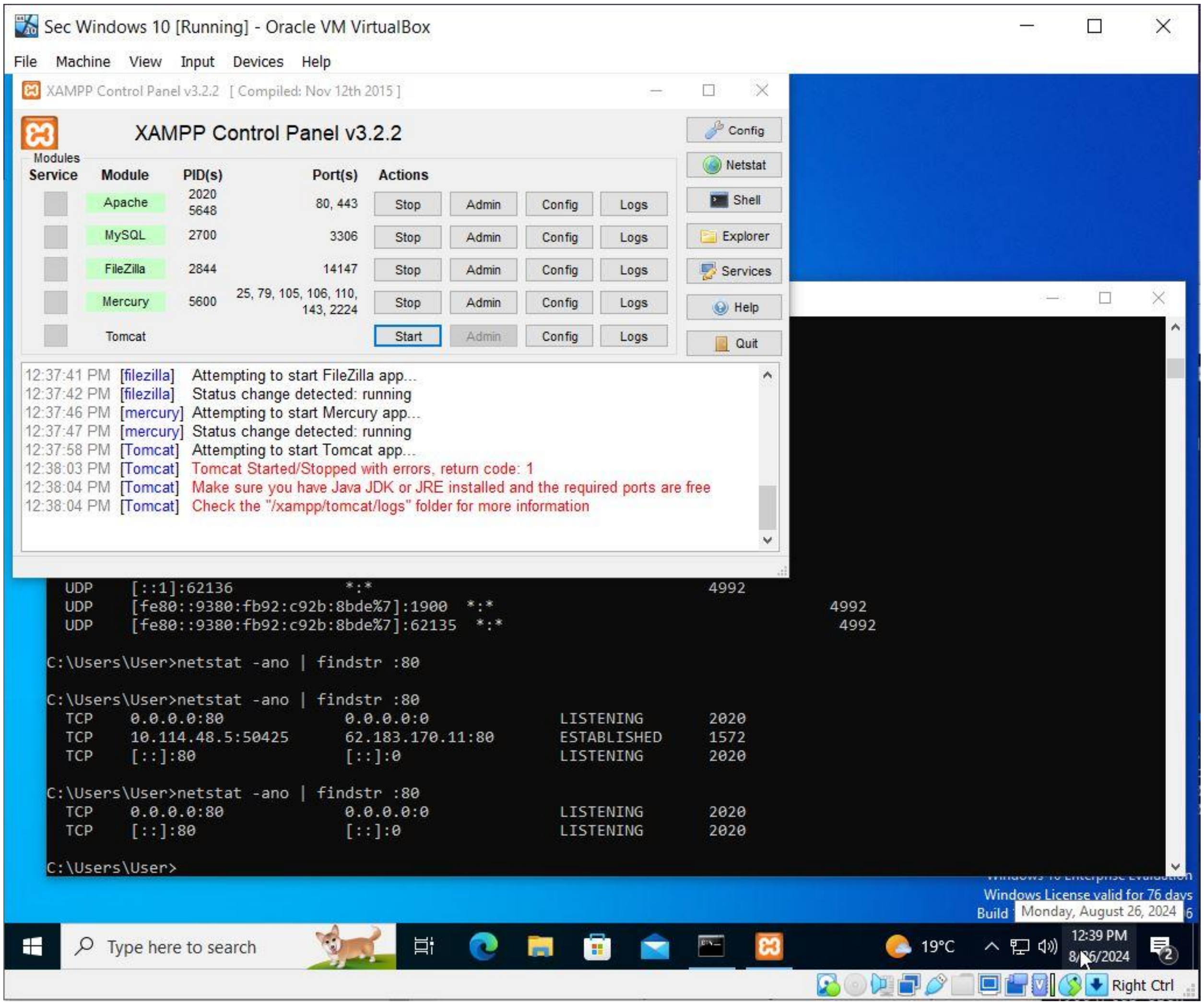
Produce a separate document in response. In your answer, write down what you are doing in that section, take a screenshot or screenshots of the results, and finally **analyze what you can conclude from the results**. On Win 10, port 80 = http port, which is used by Apache. The port must be open for the web service to work.

1. Use Nmap to scan your lab network so that the results show open ports for devices on the network.
2. Use Nmap to scan your lab network so that the results also show the operating system and the name and version of the programs.
3. Use Nmap to scan only the http and https ports of your devices from your lab network.
4. Use Nmap to scan only common UDP ports on devices in your lab network.
5. Use Nmap to scan your lab network to show the operating system, program name and version, and save the search results to a text file.

PART 2

Using Nmap in the lab

Started machines with Win10 and Kali Linux. Made sure the pings go between the machines and Win10 machine has Xampp installed and at least Apache and MySQL running on them.



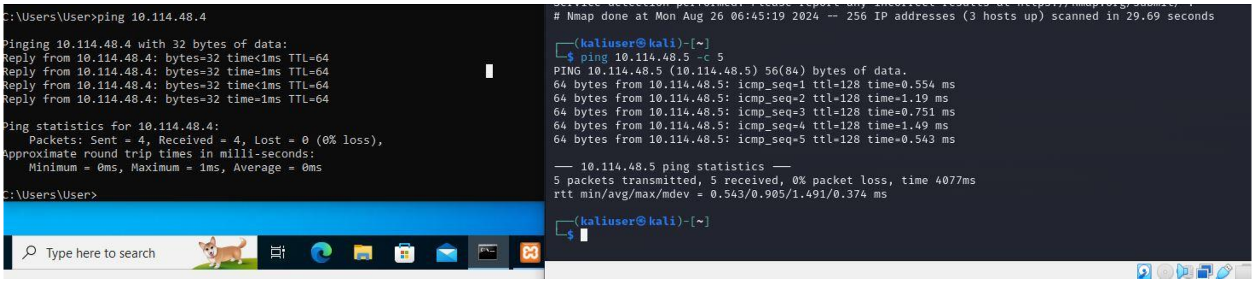
Sec Windows 10 [Running] - Oracle VM VirtualBox

XAMPP Control Panel v3.2.2 [Compiled: Nov 12th 2015]

Service	Module	PID(s)	Port(s)	Actions			
	Apache	2020 5648	80, 443	Stop	Admin	Config	Logs
	MySQL	2700	3306	Stop	Admin	Config	Logs
	FileZilla	2844	14147	Stop	Admin	Config	Logs
	Mercury	5600	25, 79, 105, 106, 110, 143, 2224	Stop	Admin	Config	Logs
	Tomcat			Start	Admin	Config	Logs

```
12:37:41 PM  [filezilla]  Attempting to start FileZilla app...
12:37:42 PM  [filezilla]  Status change detected: running
12:37:46 PM  [mercury]    Attempting to start Mercury app...
12:37:47 PM  [mercury]    Status change detected: running
12:37:58 PM  [Tomcat]     Attempting to start Tomcat app...
12:38:03 PM  [Tomcat]     Tomcat Started/Stopped with errors, return code: 1
12:38:04 PM  [Tomcat]     Make sure you have Java JDK or JRE installed and the required ports are free
12:38:04 PM  [Tomcat]     Check the "/xampp/tomcat/logs" folder for more information
```

```
  UDP    [::1]:62136            *:*                                    4992
  UDP    [fe80::9380:fb92:c2b:8bde%7]:1900  *:*                                    4992
  UDP    [fe80::9380:fb92:c2b:8bde%7]:62135  *:*                                    4992

C:\Users\User>netstat -ano | findstr :80

C:\Users\User>netstat -ano | findstr :80
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       2020
  TCP    10.114.48.5:50425      62.183.170.11:80       ESTABLISHED     1572
  TCP    [::]:80                [::]:0                 LISTENING       2020

C:\Users\User>netstat -ano | findstr :80
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       2020
  TCP    [::]:80                [::]:0                 LISTENING       2020

C:\Users\User>
```

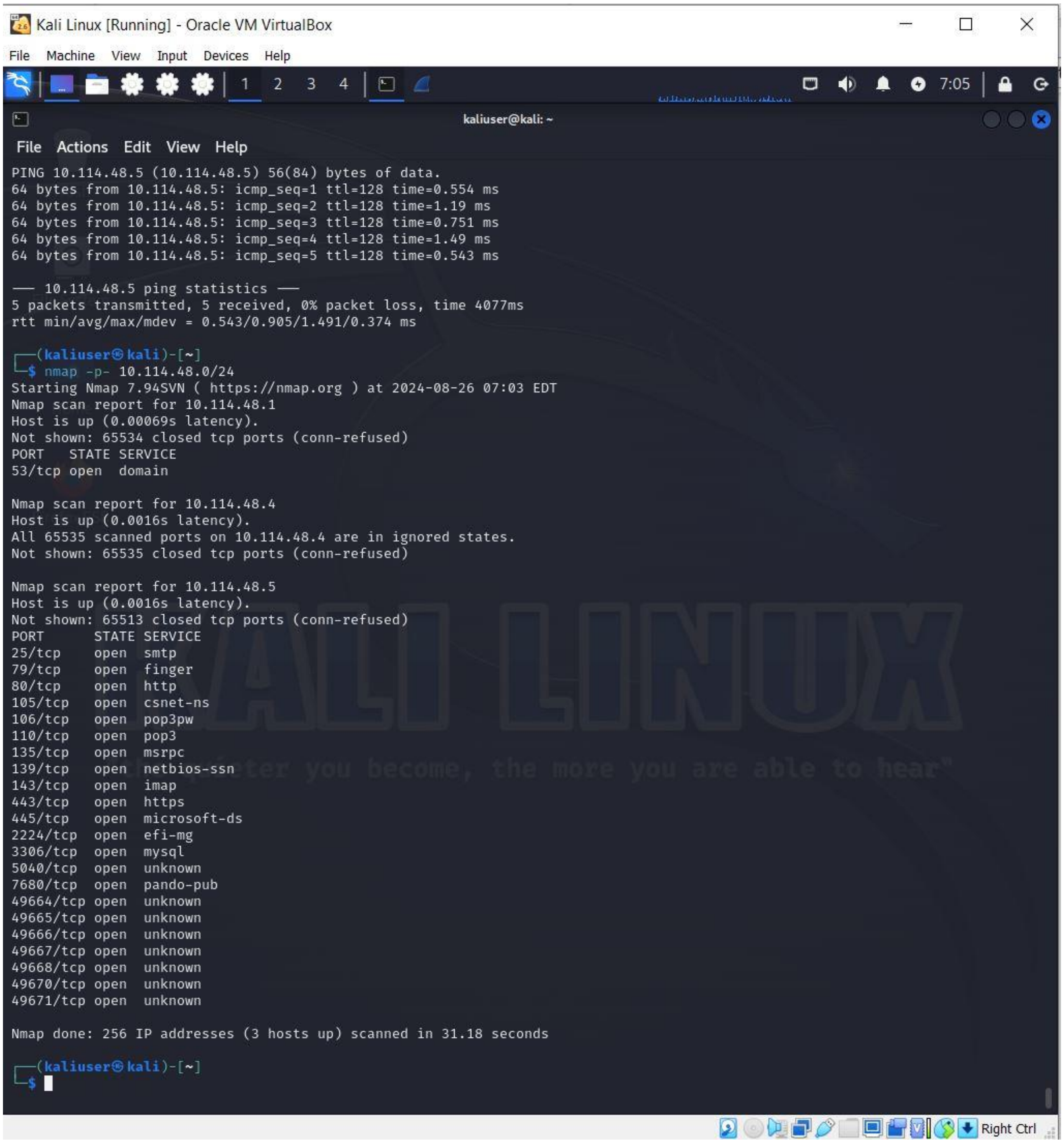


```
C:\Users\User>ping 10.114.48.4

Pinging 10.114.48.4 with 32 bytes of data:
Reply from 10.114.48.4: bytes=32 time<1ms TTL=64
Reply from 10.114.48.4: bytes=32 time=1ms TTL=64
Reply from 10.114.48.4: bytes=32 time<1ms TTL=64
Reply from 10.114.48.4: bytes=32 time=1ms TTL=64

Ping statistics for 10.114.48.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\User>
```

```
# Nmap done at Mon Aug 26 06:45:19 2024 -- 256 IP addresses (3 hosts up) scanned in 29.69 seconds

┌──(kaliuser㉿kali)-[~]
└─$ ping 10.114.48.5 -c 5
PING 10.114.48.5 (10.114.48.5) 56(84) bytes of data.
64 bytes from 10.114.48.5: icmp_seq=1 ttl=128 time=0.554 ms
64 bytes from 10.114.48.5: icmp_seq=2 ttl=128 time=1.19 ms
64 bytes from 10.114.48.5: icmp_seq=3 ttl=128 time=0.751 ms
64 bytes from 10.114.48.5: icmp_seq=4 ttl=128 time=1.49 ms
64 bytes from 10.114.48.5: icmp_seq=5 ttl=128 time=0.543 ms

--- 10.114.48.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4077ms
rtt min/avg/max/mdev = 0.543/0.905/1.491/0.374 ms

┌──(kaliuser㉿kali)-[~]
└─$ 
```

Analysis

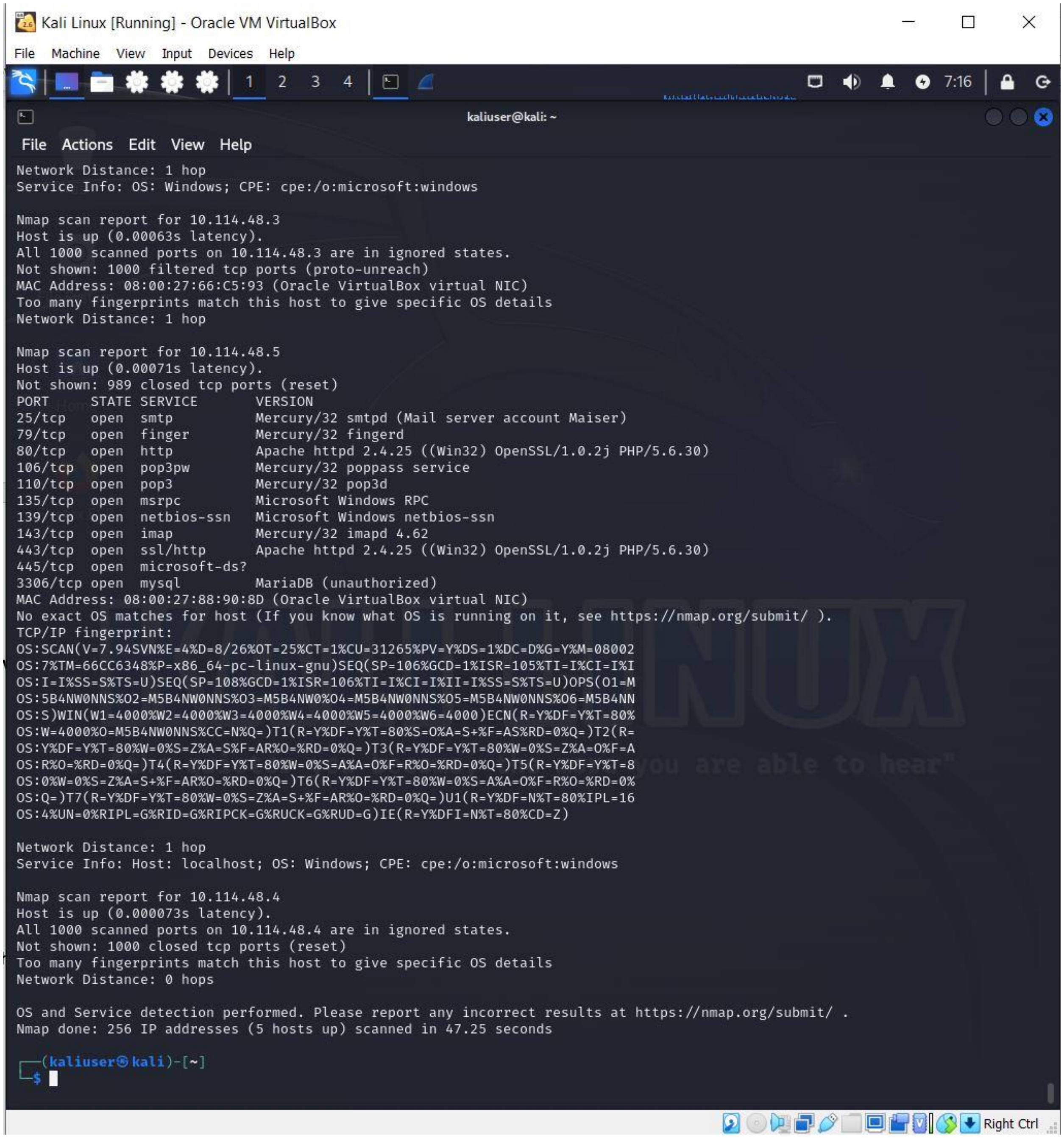
Use Nmap to scan your lab network so that the results show open ports for devices on the network.



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
7:05
kaliuser@kali: ~
File Actions Edit View Help
Right Ctrl

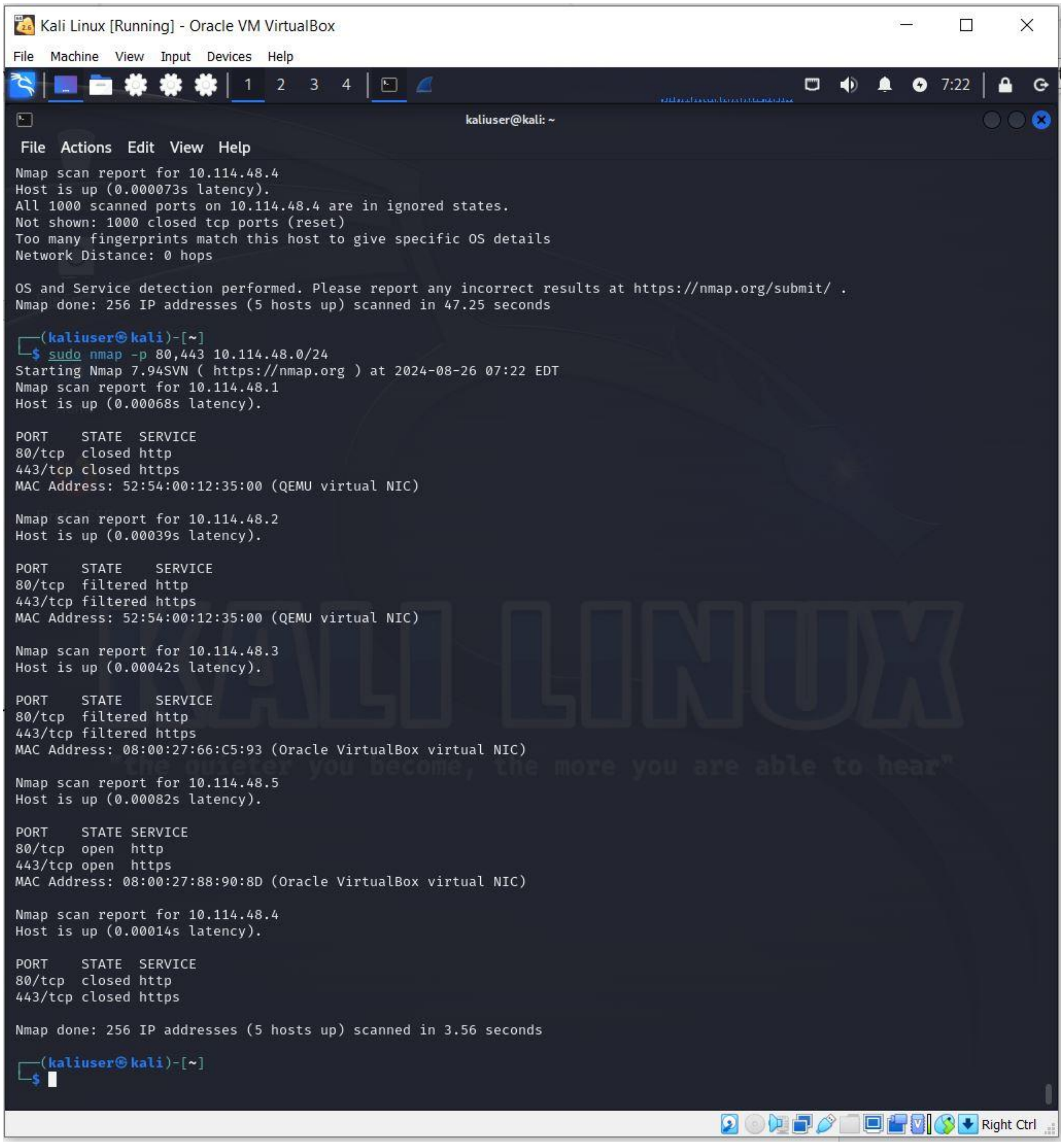
```
PING 10.114.48.5 (10.114.48.5) 56(84) bytes of data.
64 bytes from 10.114.48.5: icmp_seq=1 ttl=128 time=0.554 ms
64 bytes from 10.114.48.5: icmp_seq=2 ttl=128 time=1.19 ms
64 bytes from 10.114.48.5: icmp_seq=3 ttl=128 time=0.751 ms
64 bytes from 10.114.48.5: icmp_seq=4 ttl=128 time=1.49 ms
64 bytes from 10.114.48.5: icmp_seq=5 ttl=128 time=0.543 ms

—— 10.114.48.5 ping statistics ——
5 packets transmitted, 5 received, 0% packet loss, time 4077ms
rtt min/avg/max/mdev = 0.543/0.905/1.491/0.374 ms

┌──(kaliuser㉿kali)-[~]
└─$ nmap -p- 10.114.48.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 07:03 EDT
Nmap scan report for 10.114.48.1
Host is up (0.00069s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for 10.114.48.4
Host is up (0.0016s latency).
All 65535 scanned ports on 10.114.48.4 are in ignored states.
Not shown: 65535 closed tcp ports (conn-refused)

Nmap scan report for 10.114.48.5
Host is up (0.0016s latency).
Not shown: 65513 closed tcp ports (conn-refused)
PORT      STATE SERVICE
25/tcp    open  smtp
79/tcp    open  finger
80/tcp    open  http
105/tcp   open  csnet-ns
106/tcp   open  pop3pw
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   open  microsoft-ds
2224/tcp  open  efi-mg
3306/tcp  open  mysql
5040/tcp  open  unknown
7680/tcp  open  pando-pub
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49670/tcp open  unknown
49671/tcp open  unknown

Nmap done: 256 IP addresses (3 hosts up) scanned in 31.18 seconds

┌──(kaliuser㉿kali)-[~]
└─$ 
```

Use Nmap to scan your lab network so that the results also show the operating system and the name and version of the programs.


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
7:16
kaliuser@kali: ~
File Actions Edit View Help
Right Ctrl

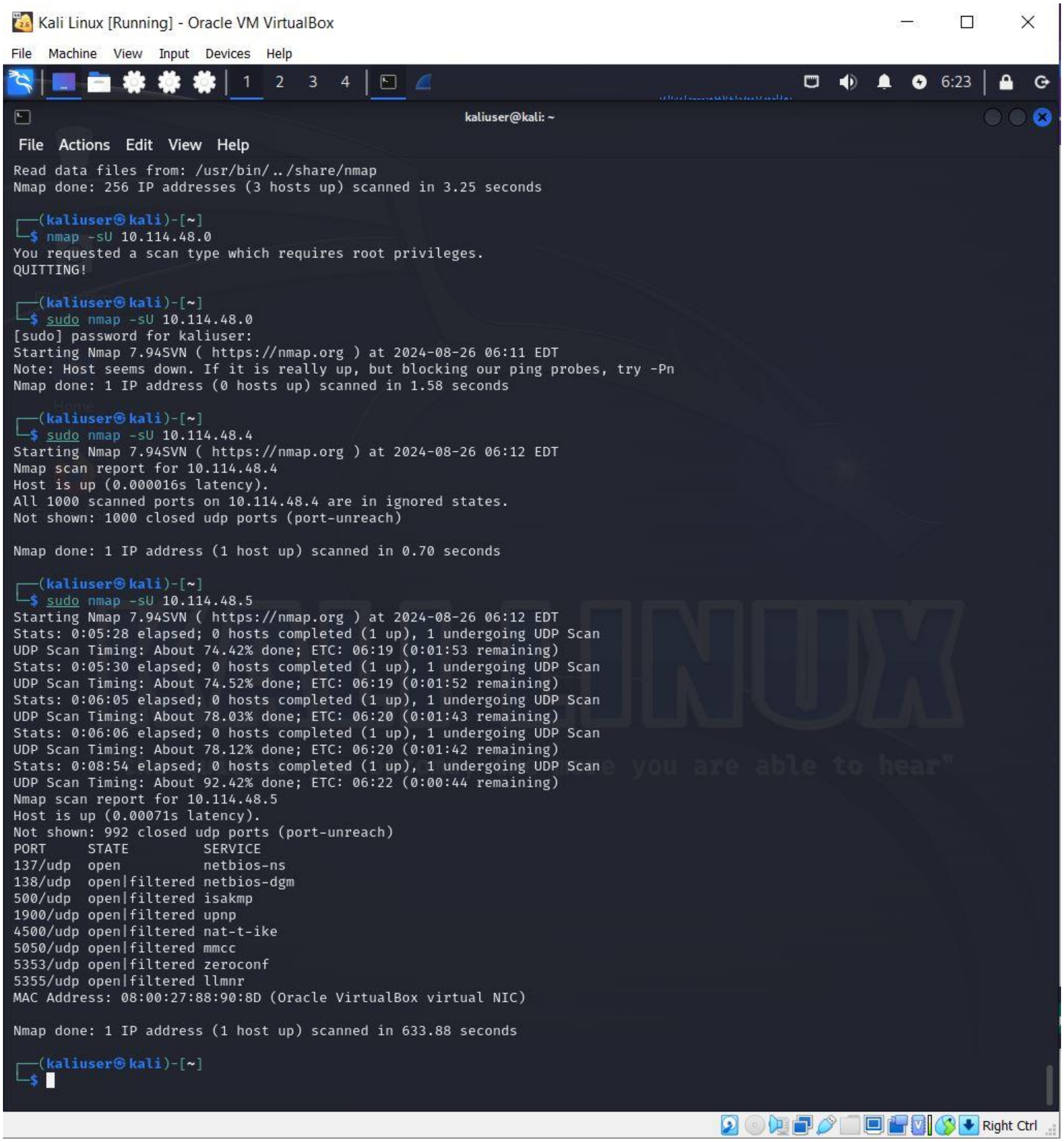
```
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.114.48.3
Host is up (0.00063s latency).
All 1000 scanned ports on 10.114.48.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:66:C5:93 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 10.114.48.5
Host is up (0.00071s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
25/tcp   open  smtp          Mercury/32 smtpd (Mail server account Maiser)
79/tcp   open  finger        Mercury/32 fingerd
80/tcp   open  http          Apache httpd 2.4.25 ((Win32) OpenSSL/1.0.2j PHP/5.6.30)
106/tcp  open  pop3pw        Mercury/32 poppass service
110/tcp  open  pop3          Mercury/32 pop3d
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
143/tcp  open  imap          Mercury/32 imapd 4.62
443/tcp  open  ssl/http      Apache httpd 2.4.25 ((Win32) OpenSSL/1.0.2j PHP/5.6.30)
445/tcp  open  microsoft-ds?
3306/tcp open  mysql         MariaDB (unauthorized)
MAC Address: 08:00:27:88:90:8D (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=8/26%OT=25%CT=1%CU=31265%PV=Y%DS=1%DC=D%G=Y%M=08002
OS:7%TM=66CC6348%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=105%TI=I%CI=I%I
OS:I=I%SS=S%TS=U)SEQ(SP=108%GCD=1%ISR=106%TI=I%CI=I%II=I%SS=S%TS=U)OPS(O1=M
OS:5B4NW0NNS%O2=M5B4NW0NNS%O3=M5B4NW0%O4=M5B4NW0NNS%O5=M5B4NW0NNS%O6=M5B4NN
OS:S)WIN(W1=4000%W2=4000%W3=4000%W4=4000%W5=4000%W6=4000)ECN(R=Y%DF=Y%T=80%
OS:W=4000%O=M5B4NW0NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=
OS:Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=A
OS:R%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=8
OS:0%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%
OS:Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=16
OS:4%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 1 hop
Service Info: Host: localhost; OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.114.48.4
Host is up (0.000073s latency).
All 1000 scanned ports on 10.114.48.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 47.25 seconds

┌──(kaliuser㉿kali)-[~]
└─$ 
```

Use Nmap to scan only the http and https ports of your devices from your lab network.


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
7:22
kaliuser@kali: ~
File Actions Edit View Help
Right Ctrl

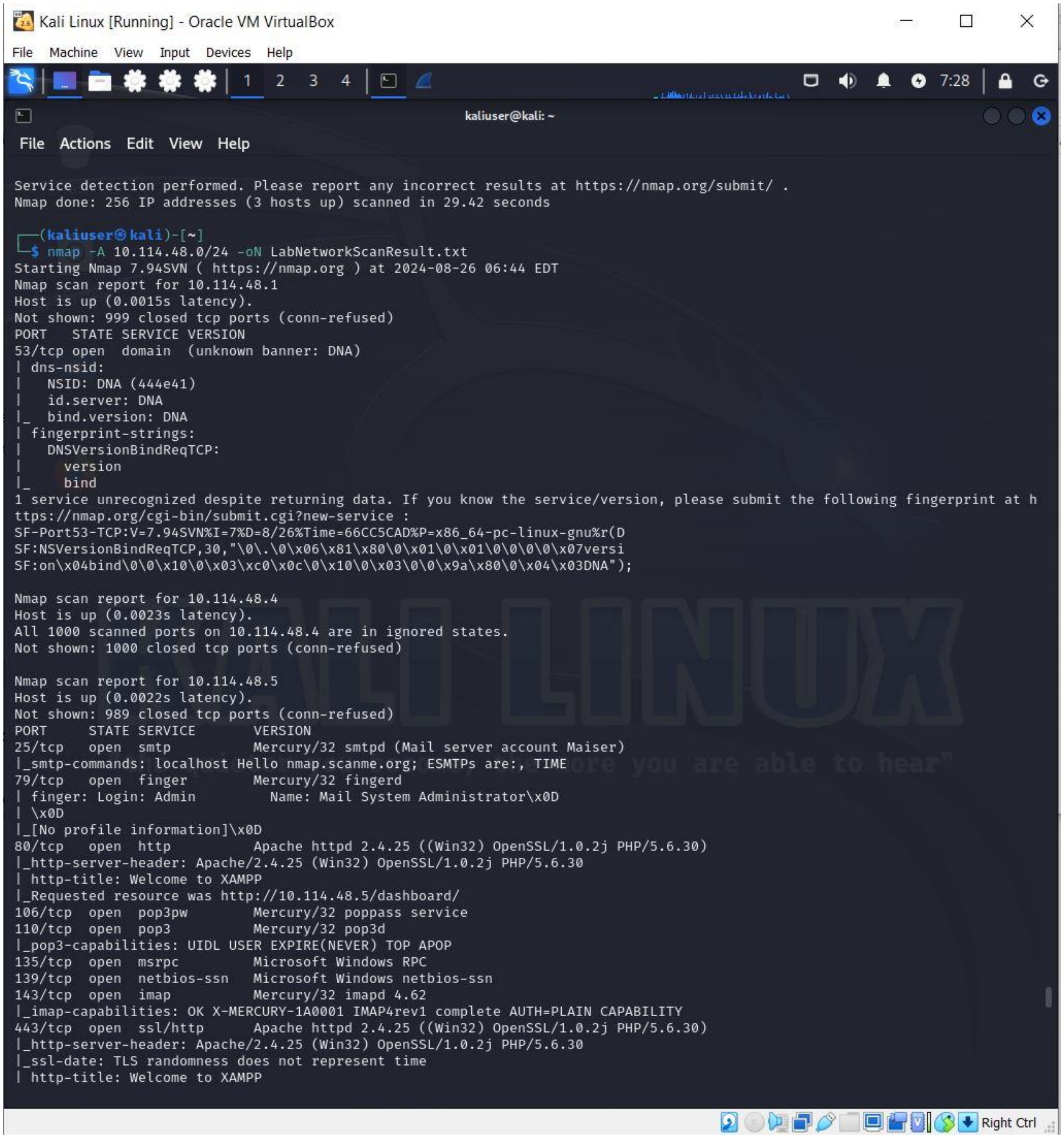
```
Nmap scan report for 10.114.48.4
Host is up (0.000073s latency).
All 1000 scanned ports on 10.114.48.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 47.25 seconds

┌──(kaliuser㉿kali)-[~]
└─$ sudo nmap -p 80,443 10.114.48.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 07:22 EDT
Nmap scan report for 10.114.48.1
Host is up (0.00068s latency).

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.114.48.2
Host is up (0.00039s latency).

PORT    STATE    SERVICE
80/tcp  filtered http
443/tcp filtered https
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.114.48.3
Host is up (0.00042s latency).

PORT    STATE    SERVICE
80/tcp  filtered http
443/tcp filtered https
MAC Address: 08:00:27:66:C5:93 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.114.48.5
Host is up (0.00082s latency).

PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
MAC Address: 08:00:27:88:90:8D (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.114.48.4
Host is up (0.00014s latency).

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https

Nmap done: 256 IP addresses (5 hosts up) scanned in 3.56 seconds

┌──(kaliuser㉿kali)-[~]
└─$ 
```

Use Nmap to scan only common UDP ports on devices in your lab network.


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
6:23
kaliuser@kali: ~
File Actions Edit View Help
Right Ctrl

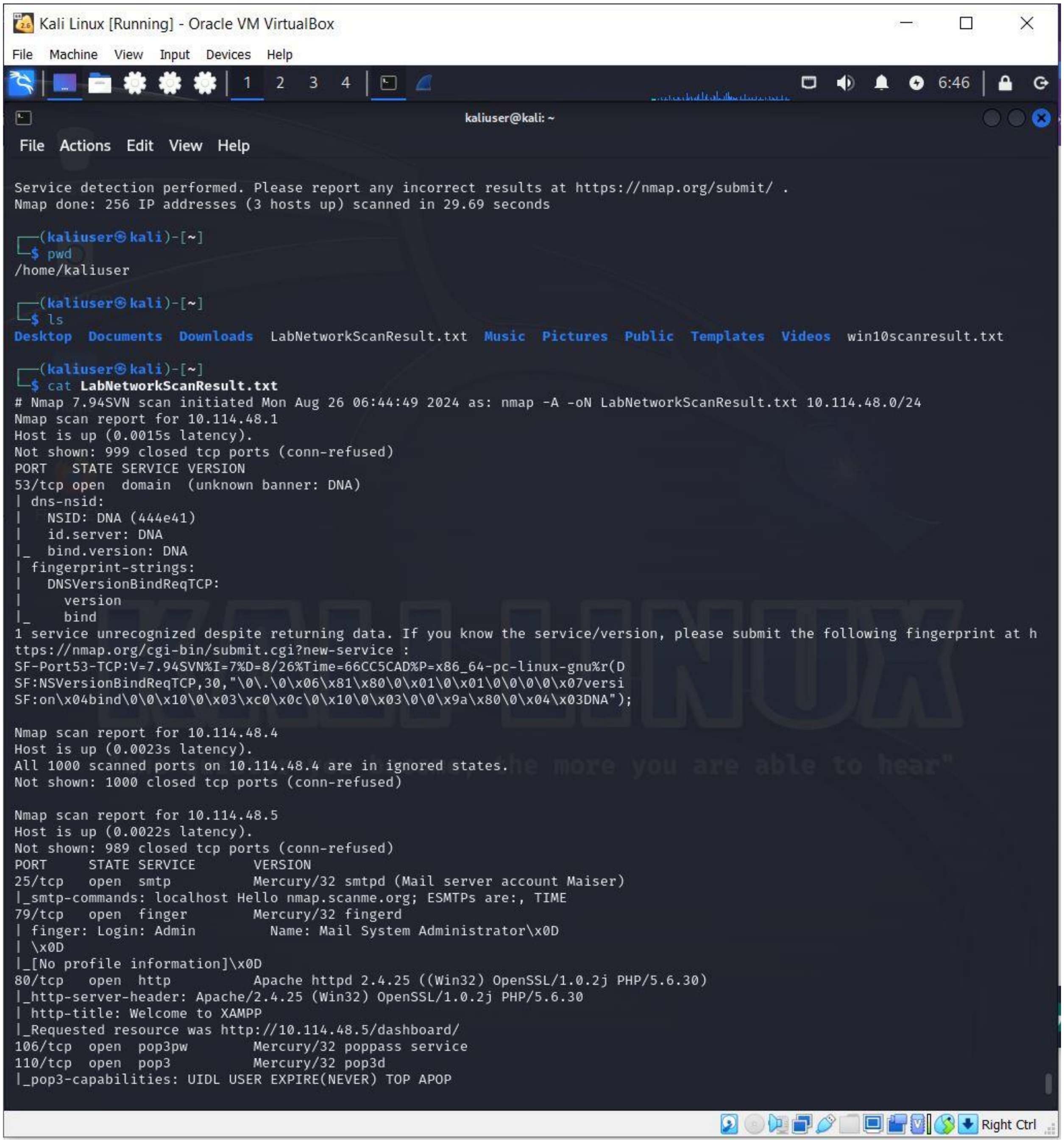
```
Read data files from: /usr/bin/../share/nmap
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.25 seconds

┌──(kaliuser㉿kali)-[~]
└─$ nmap -sU 10.114.48.0
You requested a scan type which requires root privileges.
QUITTING!

┌──(kaliuser㉿kali)-[~]
└─$ sudo nmap -sU 10.114.48.0
[sudo] password for kaliuser:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 06:11 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.58 seconds

┌──(kaliuser㉿kali)-[~]
└─$ sudo nmap -sU 10.114.48.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 06:12 EDT
Nmap scan report for 10.114.48.4
Host is up (0.000016s latency).
All 1000 scanned ports on 10.114.48.4 are in ignored states.
Not shown: 1000 closed udp ports (port-unreach)

Nmap done: 1 IP address (1 host up) scanned in 0.70 seconds

┌──(kaliuser㉿kali)-[~]
└─$ sudo nmap -sU 10.114.48.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 06:12 EDT
Stats: 0:05:28 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 74.42% done; ETC: 06:19 (0:01:53 remaining)
Stats: 0:05:30 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 74.52% done; ETC: 06:19 (0:01:52 remaining)
Stats: 0:06:05 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 78.03% done; ETC: 06:20 (0:01:43 remaining)
Stats: 0:06:06 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 78.12% done; ETC: 06:20 (0:01:42 remaining)
Stats: 0:08:54 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 92.42% done; ETC: 06:22 (0:00:44 remaining)
Nmap scan report for 10.114.48.5
Host is up (0.00071s latency).
Not shown: 992 closed udp ports (port-unreach)
PORT     STATE         SERVICE
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
500/udp  open|filtered isakmp
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
5050/udp open|filtered mmcc
5353/udp open|filtered zeroconf
5355/udp open|filtered llmnr
MAC Address: 08:00:27:88:90:8D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 633.88 seconds

┌──(kaliuser㉿kali)-[~]
└─$ █
```

Use Nmap to scan your lab network to show the operating system, program name and version, and save the search results to a text file.



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
7:28
kaliuser@kali: ~
File Actions Edit View Help
Right Ctrl

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 29.42 seconds

┌──(kaliuser㉿kali)-[~]
└─$ nmap -A 10.114.48.0/24 -oN LabNetworkScanResult.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 06:44 EDT
Nmap scan report for 10.114.48.1
Host is up (0.0015s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
53/tcp open  domain  (unknown banner: DNA)
| dns-nsid:
|   NSID: DNA (444e41)
|   id.server: DNA
|_  bind.version: DNA
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at h
ttps://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.94SVN%I=7%D=8/26%Time=66CC5CAD%P=x86_64-pc-linux-gnu%r(D
SF:NSVersionBindReqTCP,30,"\0\.\0\x06\x81\x80\0\x01\0\x01\0\0\0\0\x07versi
SF:on\x04bind\0\0\x10\0\x03\xc0\x0c\0\x10\0\x03\0\0\x9a\x80\0\x04\x03DNA");

Nmap scan report for 10.114.48.4
Host is up (0.0023s latency).
All 1000 scanned ports on 10.114.48.4 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 10.114.48.5
Host is up (0.0022s latency).
Not shown: 989 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
25/tcp   open  smtp          Mercury/32 smtpd (Mail server account Maiser)
|_smtp-commands: localhost Hello nmap.scanme.org; ESMTPs are:, TIME
79/tcp   open  finger        Mercury/32 fingerd
| finger: Login: Admin         Name: Mail System Administrator\x0D
| \x0D
|_[No profile information]\x0D
80/tcp   open  http          Apache httpd 2.4.25 ((Win32) OpenSSL/1.0.2j PHP/5.6.30)
|_http-server-header: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
| http-title: Welcome to XAMPP
|_Requested resource was http://10.114.48.5/dashboard/
106/tcp  open  pop3pw        Mercury/32 poppass service
110/tcp  open  pop3          Mercury/32 pop3d
|_pop3-capabilities: UIDL USER EXPIRE(NEVER) TOP APOP
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
143/tcp  open  imap          Mercury/32 imapd 4.62
|_imap-capabilities: OK X-MERCURY-1A0001 IMAP4rev1 complete AUTH=PLAIN CAPABILITY
443/tcp  open  ssl/http      Apache httpd 2.4.25 ((Win32) OpenSSL/1.0.2j PHP/5.6.30)
|_http-server-header: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
|_ssl-date: TLS randomness does not represent time
| http-title: Welcome to XAMPP
```


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
6:46
kaliuser@kali: ~
File Actions Edit View Help
Right Ctrl

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 29.69 seconds

┌──(kaliuser㉿kali)-[~]
└─$ pwd
/home/kaliuser

┌──(kaliuser㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  LabNetworkScanResult.txt  Music  Pictures  Public  Templates  Videos  win10scanresult.txt

┌──(kaliuser㉿kali)-[~]
└─$ cat LabNetworkScanResult.txt
# Nmap 7.94SVN scan initiated Mon Aug 26 06:44:49 2024 as: nmap -A -oN LabNetworkScanResult.txt 10.114.48.0/24
Nmap scan report for 10.114.48.1
Host is up (0.0015s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
53/tcp open  domain  (unknown banner: DNA)
| dns-nsid:
|   NSID: DNA (444e41)
|   id.server: DNA
|_  bind.version: DNA
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at h
ttps://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.94SVN%I=7%D=8/26%Time=66CC5CAD%P=x86_64-pc-linux-gnu%r(D
SF:NSVersionBindReqTCP,30,"\0\.\0\x06\x81\x80\0\x01\0\x01\0\0\0\0\x07versi
SF:on\x04bind\0\0\x10\0\x03\xc0\x0c\0\x10\0\x03\0\0\x9a\x80\0\x04\x03DNA");

Nmap scan report for 10.114.48.4
Host is up (0.0023s latency).
All 1000 scanned ports on 10.114.48.4 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 10.114.48.5
Host is up (0.0022s latency).
Not shown: 989 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
25/tcp   open  smtp          Mercury/32 smtpd (Mail server account Maiser)
|_smtp-commands: localhost Hello nmap.scanme.org; ESMTPs are:, TIME
79/tcp   open  finger        Mercury/32 fingerd
| finger: Login: Admin         Name: Mail System Administrator\x0D
| \x0D
|_[No profile information]\x0D
80/tcp   open  http          Apache httpd 2.4.25 ((Win32) OpenSSL/1.0.2j PHP/5.6.30)
|_http-server-header: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
| http-title: Welcome to XAMPP
|_Requested resource was http://10.114.48.5/dashboard/
106/tcp  open  pop3pw        Mercury/32 poppass service
110/tcp  open  pop3          Mercury/32 pop3d
|_pop3-capabilities: UIDL USER EXPIRE(NEVER) TOP APOP
```