E2-232-TCP/IP Networking

Write a script to look for vulnerable hosts

Patil Sarvjit Ajit

M.Tech. EPD DESE

SR. No.: 04-01-04-10-51-22-1-20862

1) Write a shell script to scan the given Subnet and look for vulnerable open ports. The script should also fingerprint the target hosts once vulnerable port is found to be open

The subnet and ports to be probed are provided as a command line options

Here following arguments are passed in command:

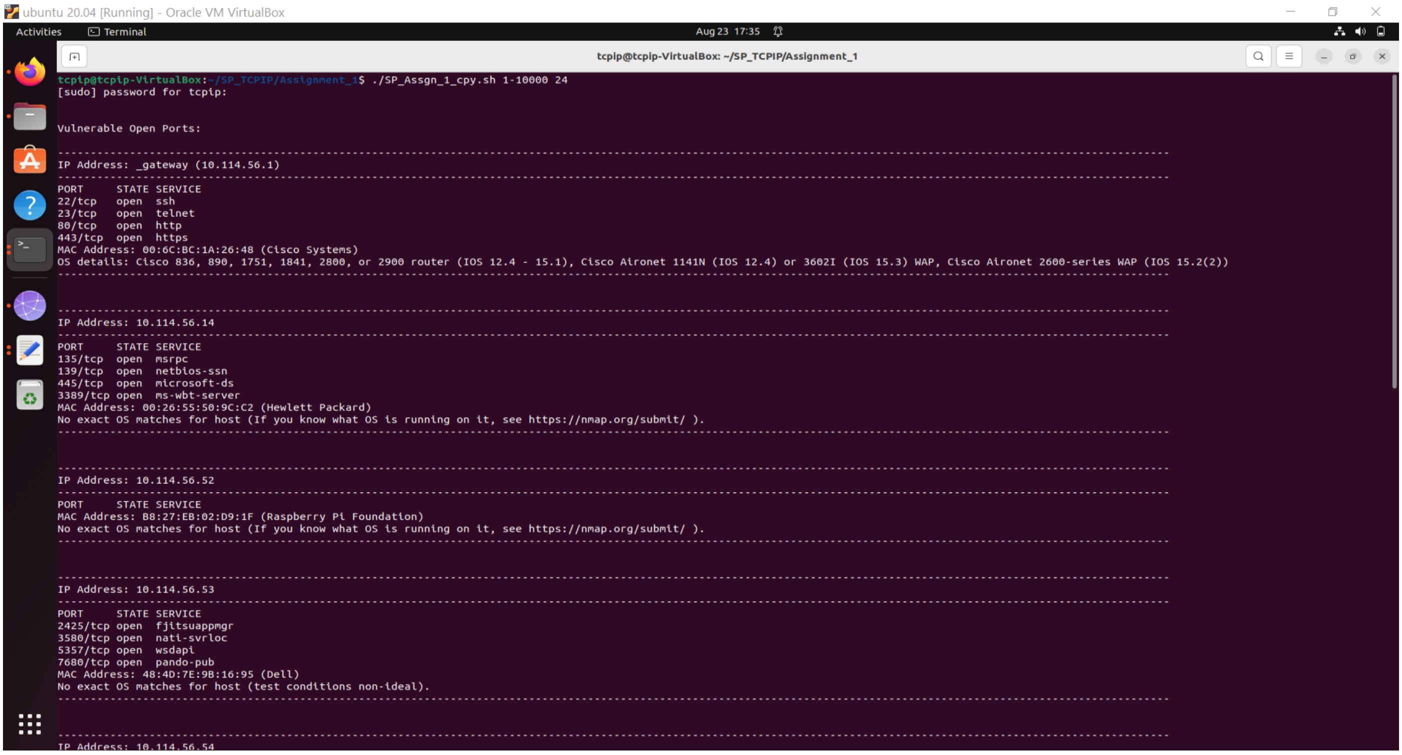
Argument 1: 1-10000 (Ports to be scanned)

Argument 2: 24 (Subnet Masks)

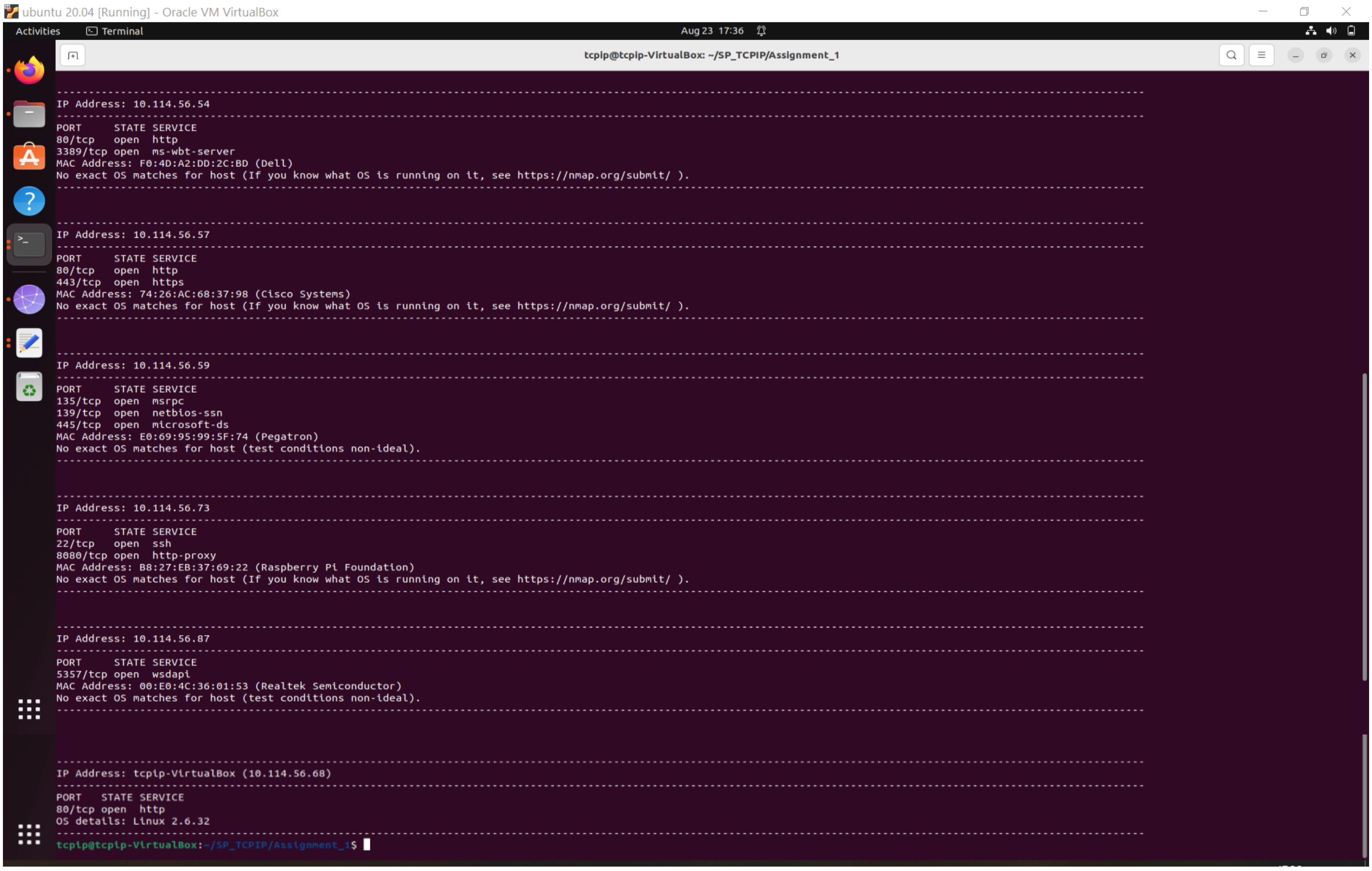
Code:

```
#! /bin/bash
#echo "Hello $USER"
#echo "TCP/IP Assignment 1"
#sudo nmap --open -O -p $1 10.114.56.0/$2 |tee output.txt > /dev/null
sudo nmap --open -O -p $1 10.114.56.0/$2 | grep 'Nmap scan report for\|PORT\|7/\|19/\|20/\|21/\|22/\|23/\|25/\|37/\|53/\|69/\|79/\|80/\|110/\|111/\|135/\|137/\|139/\|161/\|443/\|445/\|512/\|513/\|514/\|1433/\|1434/\|1723/\|3389/\|8080/\|8443/\|MAC Address\|OS details: \|No exact OS matches for host'| tee output1.txt > /dev/null
sed -i 's/Nmap scan report for/IP Address:/' output1.txt > /dev/null
sed -i '/^IP Address:.*/i \\n' output1.txt > /dev/null
sed -i '/^IP Address:.*/i \----------------------------------------------------------------------------------------------------------------------------------------------------------------------' output1.txt > /dev/null
sed -i '/^IP Address.*/a \----------------------------------------------------------------------------------------------------------------------------------------------------------------------' output1.txt > /dev/null
sed -i '/^OS details.*/a \----------------------------------------------------------------------------------------------------------------------------------------------------------------------' output1.txt > /dev/null
sed -i '/^No exact OS matches for host.*/a \----------------------------------------------------------------------------------------------------------------------------------------------------------------------' output1.txt > /dev/null
sed -i '1d' output1.txt
sed -i '1 i\Vulnerable Open Ports:' output1.txt
sed -i '/^Vulnerable Open Ports:.*/i \\n' output1.txt > /dev/null
cat output1.txt
```

Output:


ubuntu 20.04 [Running] - Oracle VM VirtualBox
Activities
Terminal
Aug 23 17:35
tcpip@tcpip-VirtualBox: ~/SP_TCPIP/Assignment_1

```
tcpip@tcpip-VirtualBox:~/SP_TCPIP/Assignment_1$ ./SP_Assgn_1_cpy.sh 1-10000 24
[sudo] password for tcpip:


Vulnerable Open Ports:

------------------------------------------------------------------------------------------------------------------------------------------------------------------------
IP Address: _gateway (10.114.56.1)
------------------------------------------------------------------------------------------------------------------------------------------------------------------------
PORT     STATE SERVICE
22/tcp   open  ssh
23/tcp   open  telnet
80/tcp   open  http
443/tcp  open  https
MAC Address: 00:6C:BC:1A:26:48 (Cisco Systems)
OS details: Cisco 836, 890, 1751, 1841, 2800, or 2900 router (IOS 12.4 - 15.1), Cisco Aironet 1141N (IOS 12.4) or 3602I (IOS 15.3) WAP, Cisco Aironet 2600-series WAP (IOS 15.2(2))
------------------------------------------------------------------------------------------------------------------------------------------------------------------------


------------------------------------------------------------------------------------------------------------------------------------------------------------------------
IP Address: 10.114.56.14
------------------------------------------------------------------------------------------------------------------------------------------------------------------------
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:26:55:50:9C:C2 (Hewlett Packard)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
------------------------------------------------------------------------------------------------------------------------------------------------------------------------


------------------------------------------------------------------------------------------------------------------------------------------------------------------------
IP Address: 10.114.56.52
------------------------------------------------------------------------------------------------------------------------------------------------------------------------
PORT     STATE SERVICE
MAC Address: B8:27:EB:02:D9:1F (Raspberry Pi Foundation)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
------------------------------------------------------------------------------------------------------------------------------------------------------------------------


------------------------------------------------------------------------------------------------------------------------------------------------------------------------
IP Address: 10.114.56.53
------------------------------------------------------------------------------------------------------------------------------------------------------------------------
PORT     STATE SERVICE
2425/tcp open  fjitsuappmgr
3580/tcp open  nati-svrloc
5357/tcp open  wsdapi
7680/tcp open  pando-pub
MAC Address: 48:4D:7E:9B:16:95 (Dell)
No exact OS matches for host (test conditions non-ideal).
------------------------------------------------------------------------------------------------------------------------------------------------------------------------


------------------------------------------------------------------------------------------------------------------------------------------------------------------------
IP Address: 10.114.56.54
```


ubuntu 20.04 [Running] - Oracle VM VirtualBox
Activities
Terminal
Aug 23 17:36
tcpip@tcpip-VirtualBox: ~/SP_TCPIP/Assignment_1

```
------------------------------------------------------------------------------------------------------------------------------------------------------------------------
IP Address: 10.114.56.54
------------------------------------------------------------------------------------------------------------------------------------------------------------------------
PORT     STATE SERVICE
80/tcp   open  http
3389/tcp open  ms-wbt-server
MAC Address: F0:4D:A2:DD:2C:BD (Dell)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
------------------------------------------------------------------------------------------------------------------------------------------------------------------------


------------------------------------------------------------------------------------------------------------------------------------------------------------------------
IP Address: 10.114.56.57
------------------------------------------------------------------------------------------------------------------------------------------------------------------------
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
MAC Address: 74:26:AC:68:37:98 (Cisco Systems)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
------------------------------------------------------------------------------------------------------------------------------------------------------------------------


------------------------------------------------------------------------------------------------------------------------------------------------------------------------
IP Address: 10.114.56.59
------------------------------------------------------------------------------------------------------------------------------------------------------------------------
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
MAC Address: E0:69:95:99:5F:74 (Pegatron)
No exact OS matches for host (test conditions non-ideal).
------------------------------------------------------------------------------------------------------------------------------------------------------------------------


------------------------------------------------------------------------------------------------------------------------------------------------------------------------
IP Address: 10.114.56.73
------------------------------------------------------------------------------------------------------------------------------------------------------------------------
PORT     STATE SERVICE
22/tcp   open  ssh
8080/tcp open  http-proxy
MAC Address: B8:27:EB:37:69:22 (Raspberry Pi Foundation)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
------------------------------------------------------------------------------------------------------------------------------------------------------------------------


------------------------------------------------------------------------------------------------------------------------------------------------------------------------
IP Address: 10.114.56.87
------------------------------------------------------------------------------------------------------------------------------------------------------------------------
PORT     STATE SERVICE
5357/tcp open  wsdapi
MAC Address: 00:E0:4C:36:01:53 (Realtek Semiconductor)
No exact OS matches for host (test conditions non-ideal).
------------------------------------------------------------------------------------------------------------------------------------------------------------------------




------------------------------------------------------------------------------------------------------------------------------------------------------------------------
IP Address: tcpip-VirtualBox (10.114.56.68)
------------------------------------------------------------------------------------------------------------------------------------------------------------------------
PORT   STATE SERVICE
80/tcp open  http
OS details: Linux 2.6.32
------------------------------------------------------------------------------------------------------------------------------------------------------------------------
tcpip@tcpip-VirtualBox:~/SP_TCPIP/Assignment_1$ 
```

2)

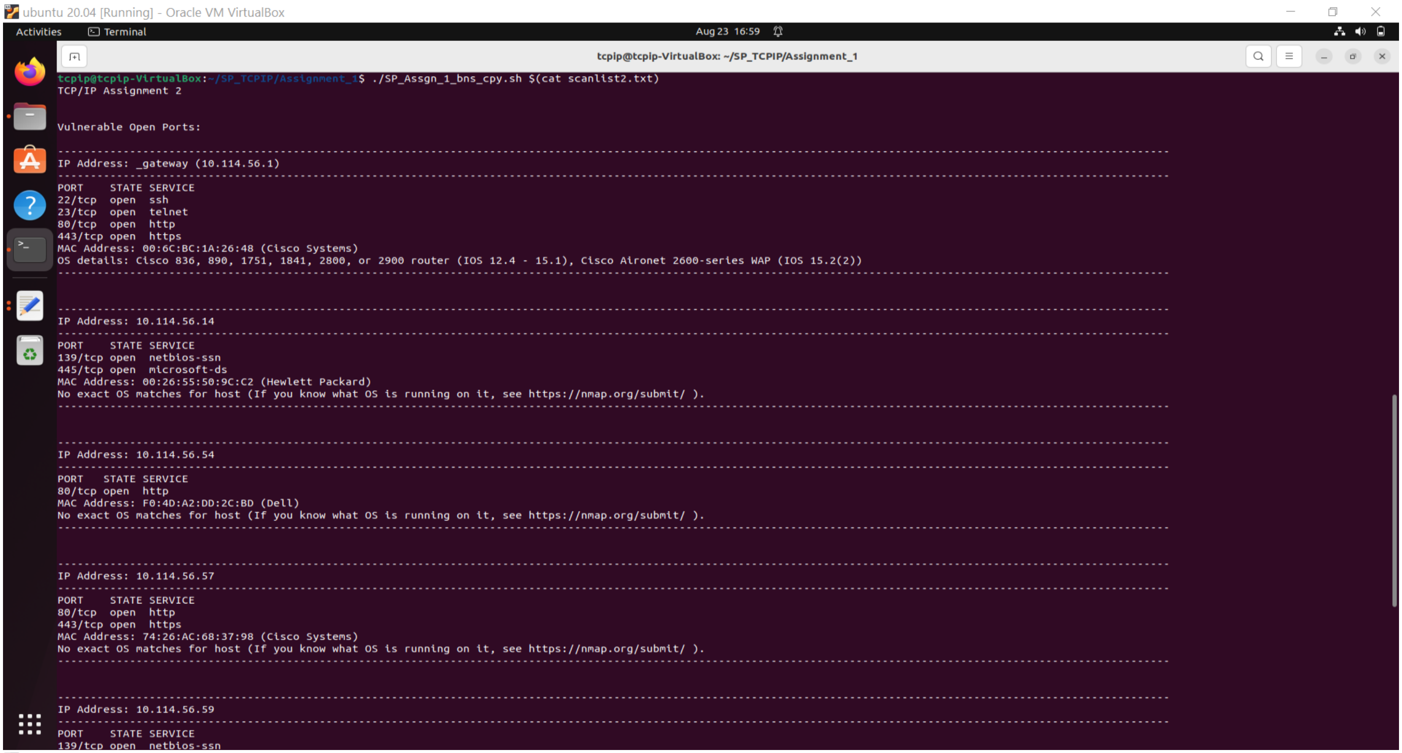
a. List of Subnets and ports to be scanned can be read from the input file scanlist.txt
b. Ports can be specified either using comma separated list or as a range using a dash. For example --ports 21,22,80, 1024-5000

Here we used a scanlist2.txt test file to get ports to be scanned and IP address with subnet masks. We read that file in bash script and took the IP addresses and ports to be scanned as arguments using while loop.

Code:

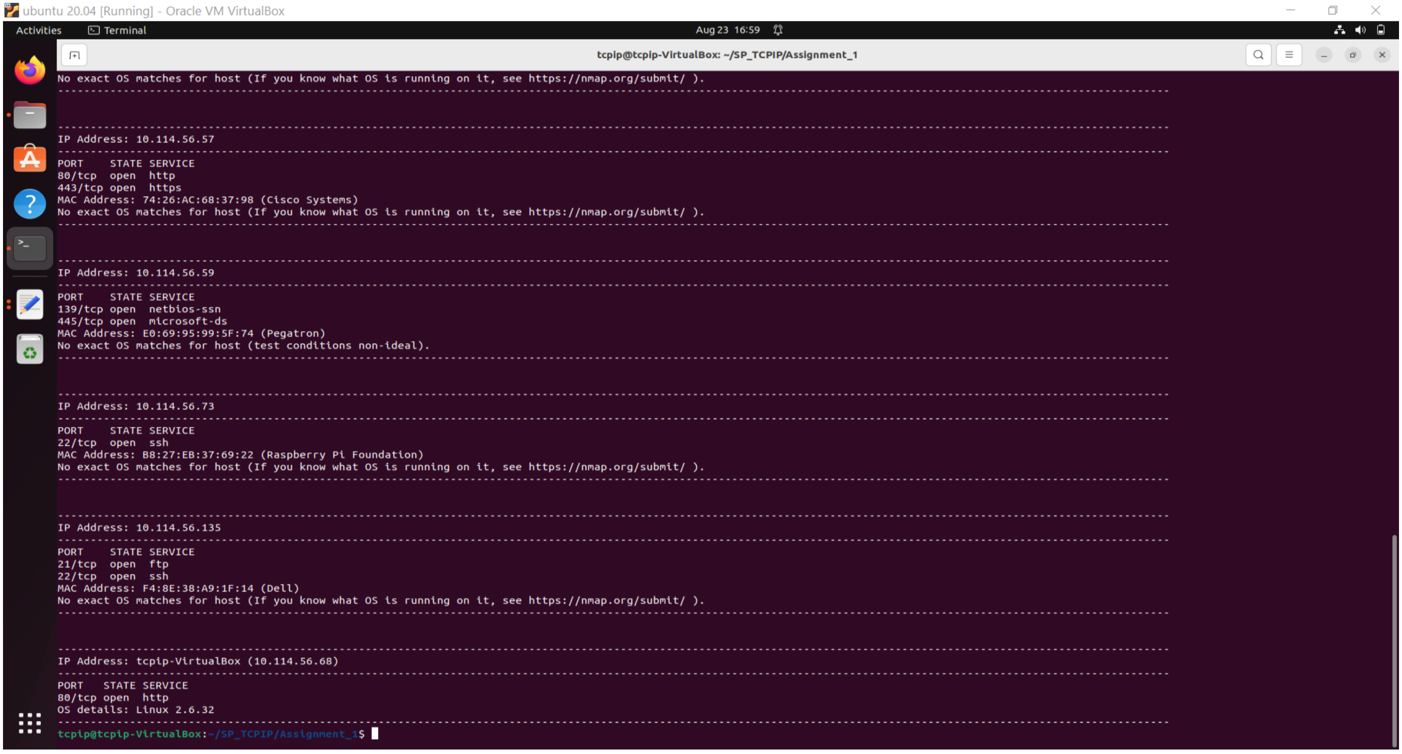
```
#! /bin/bash
#echo "Hello $USER"
echo "TCP/IP Assignment 2"
while read line; do
echo "Scanning with Ports and IP with subnet mask: $line"
echo  "--------------------------------------------------------------------------------------------------------------------------------------------------------------------------"
sudo nmap --open -O -p $line | grep 'Nmap scan report for\|PORT\|20/\|21/\|22/\|23/\|25/\|53/\|69/\|80/\|137/\|139/\|443/\|445/\|8080/\|8443/\|MAC Address\|OS details: \|No exact OS matches for host'| tee output3.txt > /dev/null
done <scanlist.txt > output3.txt
sed -i 's/Nmap scan report for/IP Address:/' output3.txt > /dev/null
sed -i '/^IP Address:.*/i \\n' output3.txt > /dev/null
sed -i '/^IP Address:.*/i \--------------------------------------------------------------------------------------------------------------------------------------------------------------------------' output3.txt > /dev/null
sed -i '/^IP Address.*/a \--------------------------------------------------------------------------------------------------------------------------------------------------------------------------' output3.txt > /dev/null
sed -i '/^OS details.*/a \--------------------------------------------------------------------------------------------------------------------------------------------------------------------------' output3.txt > /dev/null
sed -i '/^No exact OS matches for host.*/a \--------------------------------------------------------------------------------------------------------------------------------------------------------------------------' output3.txt > /dev/null
sed -i '1d' output3.txt
sed -i '1 i\Vulnerable Open Ports:' output3.txt
sed -i '/^Vulnerable Open Ports:.*/i \\n' output3.txt > /dev/null
cat output3.txt
```

Output:



ubuntu 20.04 [Running] - Oracle VM VirtualBox
Activities
Terminal
Aug 23 16:59
tcpip@tcpip-VirtualBox: ~/SP_TCPIP/Assignment_1

```
tcpip@tcpip-VirtualBox:~/SP_TCPIP/Assignment_1$ ./SP_Assgn_1_bns_cpy.sh $(cat scanlist2.txt)
TCP/IP Assignment 2


Vulnerable Open Ports:

--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
IP Address: _gateway (10.114.56.1)
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
80/tcp  open  http
443/tcp open  https
MAC Address: 00:6C:BC:1A:26:48 (Cisco Systems)
OS details: Cisco 836, 890, 1751, 1841, 2800, or 2900 router (IOS 12.4 - 15.1), Cisco Aironet 2600-series WAP (IOS 15.2(2))
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------


--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
IP Address: 10.114.56.14
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:26:55:50:9C:C2 (Hewlett Packard)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------


--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
IP Address: 10.114.56.54
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
PORT   STATE SERVICE
80/tcp open  http
MAC Address: F0:4D:A2:DD:2C:BD (Dell)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------


--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
IP Address: 10.114.56.57
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
MAC Address: 74:26:AC:68:37:98 (Cisco Systems)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------


--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
IP Address: 10.114.56.59
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
PORT    STATE SERVICE
139/tcp open  netbios-ssn
```



ubuntu 20.04 [Running] - Oracle VM VirtualBox
Activities
Terminal
Aug 23 16:59
tcpip@tcpip-VirtualBox: ~/SP_TCPIP/Assignment_1

```
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------


--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
IP Address: 10.114.56.57
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
MAC Address: 74:26:AC:68:37:98 (Cisco Systems)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------


--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
IP Address: 10.114.56.59
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: E0:69:95:99:5F:74 (Pegatron)
No exact OS matches for host (test conditions non-ideal).
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------


--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
IP Address: 10.114.56.73
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
PORT    STATE SERVICE
22/tcp  open  ssh
MAC Address: B8:27:EB:37:69:22 (Raspberry Pi Foundation)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------


--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
IP Address: 10.114.56.135
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
MAC Address: F4:8E:38:A9:1F:14 (Dell)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------


--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
IP Address: tcpip-VirtualBox (10.114.56.68)
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
PORT   STATE SERVICE
80/tcp open  http
OS details: Linux 2.6.32
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------
tcpip@tcpip-VirtualBox:~/SP_TCPIP/Assignment_1$ 
```