Cyber Security and Ethical Hacking Program

Information Gathering on Websites Using Linux

Introduction

Information gathering means collecting different kinds of information about the target. It is basically, the first step or the beginning stage of Ethical Hacking, where the penetration testers or hackers (both black hat and white hat) try to gather all the information about the target, in order to use it for Hacking.
Hacking is all about finding creative shortcuts, being limitless and you can apply it as a technique when approaching a target. In order to call yourself a hacker, you need to have the mindset of one and should be able to identify system weaknesses that require logical reasoning and the ability to think about all possible actions, alternatives, and potential conclusions.

Requirements

- **Recommended operating system Kali Linux**
- **Nmap, macchanger, and Wireshark must be installed**
- **Separate Windows machine**

Goal

- **To demonstrate the understanding of the tools.**
- **Candidate should be able to gather valuable information from targets to test.**

Scenario

You have been assigned as a network administrator in a company and have been given the task to inspect their network infrastructure. Find out what machines are running on the network and scan the individual devices to find out what services are running, open ports, operating systems, and if there is a firewall. Analyze the packets passing through the network and identify if there is a breach in the company network.

NAME : GAURAV UTTAM GHANDAT

Lab 1: Nmap
Description

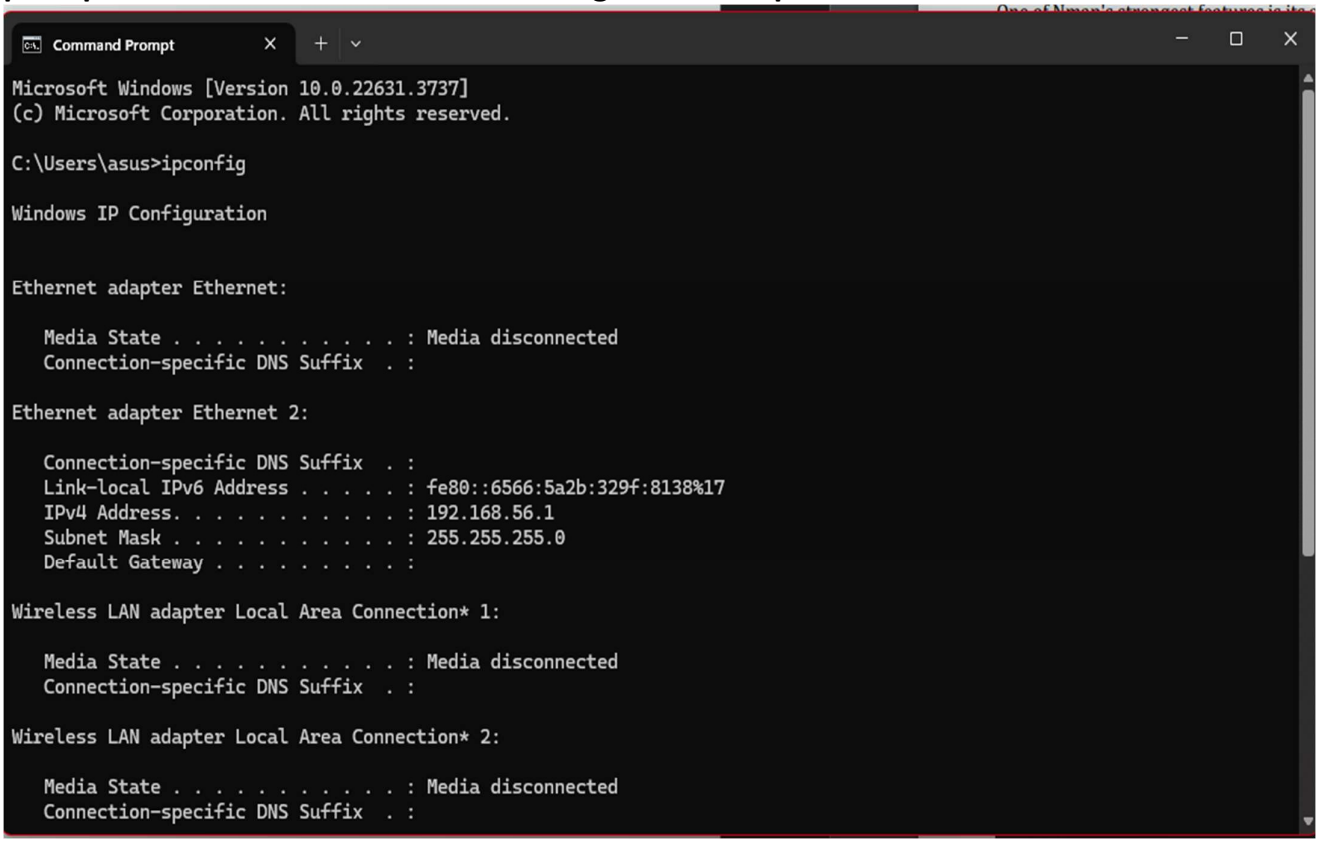
Network Mapper is referred to as Nmap. A network's IP addresses and ports can be scanned with
this free and open-source Linux command-line tool in order to find installed programs. Network administrators can use Nmap to identify the devices that are connected to their network,
find open ports and services, and find security holes. Nmap, for starters, makes it simple to quickly
map out a network without the need for complex commands or configurations. Additionally, it allows complex programming using the Nmap scripting engine as well as basic
commands (such checking is to see if a host is up).
One of Nmap's strongest features is its ability to swiftly identify every device on single or several
networks, including switches, routers, mobile devices, servers, and so on.

Task
Find the—
- **IP address of your Windows machine. (Target)**
- **OS Details of your target machine.**
- **port details of your target machine.**
- **service details of your target machine.**

SOLUTION :

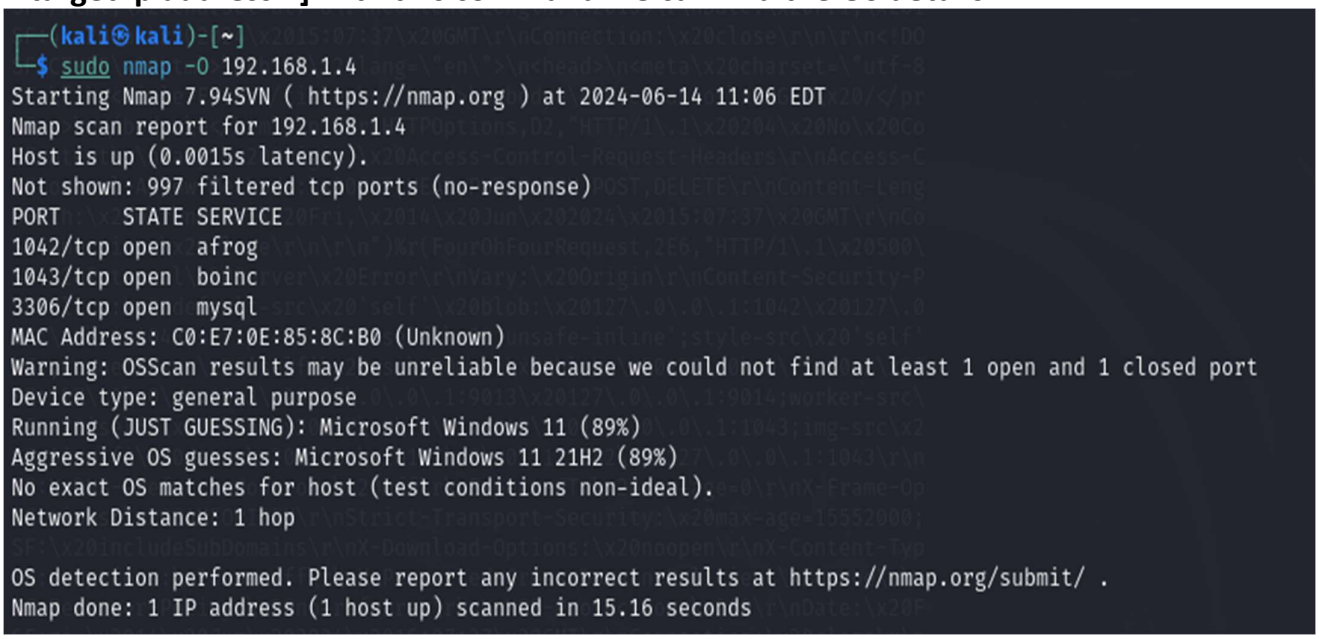
Task 1 :

In the first task we have to get ip address of windows machine using ipconfig in command prompt of windows machine for scanning in the nmap .



Task 2 :

In the second task we have to find OS details of your target machine using the nmap and ip address of the windows. We use nmap command to get the OS details using [nmap -0 < target ip address>] with this command we can find the OS details.



Task 3 :

In the third task we have to find the port details of your target machine using the nmap and ip address of the windows. We use the nmap command to get the port details using [nmap -p- <target ip address>] with this command we can find the port details.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- 192.168.1.4
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 11:03 EDT
Nmap scan report for 192.168.1.4
Host is up (0.0013s latency).
Not shown: 65520 filtered tcp ports (no-response)
PORT      STATE SERVICE
1042/tcp  open  afrog
1043/tcp  open  boinc
3306/tcp  open  mysql
7250/tcp  open  unknown
7680/tcp  open  pando-pub
9012/tcp  open  unknown
9013/tcp  open  unknown
9014/tcp  open  unknown
33060/tcp open  mysqlx
49696/tcp open  unknown
49697/tcp open  unknown
49700/tcp open  unknown
49704/tcp open  unknown
49707/tcp open  unknown
49714/tcp open  unknown
MAC Address: C0:E7:0E:85:8C:B0 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 119.70 seconds
```

Task 4 :

In the fourth task we have to find the service details of your target machine using the nmap and ip address of the windows. We use the nmap command to get the service details using [nmap -sV <target ip address>] with this command we can find the service details.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.1.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 11:09 EDT
Nmap scan report for 192.168.1.4
Host is up (0.0020s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
1042/tcp open  afrog?
1043/tcp open  ssl/boinc?
3306/tcp open  mysql      MySQL (unauthorized)
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port1042-TCP:V=7.94SVN%I=7%D=6/14%Time=666C5D24%P=x86_64-pc-linux-gnu%r
SF:(GetRequest,27E,"HTTP/1\.1\x20404\x20Not\x20Found\r\nVary:\x20Origin\r\
SF:nContent-Security-Policy:\x20default-src\x20'self'\r\nX-DNS-Prefetch-Co
SF:ntrol:\x20off\r\nExpect-CT:\x20max-age=0\r\nX-Frame-Options:\x20SAMEORI
SF:GIN\r\nStrict-Transport-Security:\x20max-age=15552000;\x20includeSubDom
SF:ains\r\nX-Download-Options:\x20noopen\r\nX-Content-Type-Options:\x20nos
SF:niff\r\nX-Permitted-Cross-Domain-Policies:\x20none\r\nReferrer-Policy:\
SF:x20no-referrer\r\nX-XSS-Protection:\x200\r\nContent-Type:\x20text/html;
SF:\x20charset=utf-8\r\nContent-Length:\x20139\r\nDate:\x20Fri,\x2014\x20J
SF:un\x202024\x2015:09:25\x20GMT\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\
SF:x20html>\n<html\x20lang=\"en\">\n<head>\n<meta\x20charset=\"utf-8\">\n<
SF:title>Error</title>\n</head>\n<body>\n<pre>Cannot\x20GET\x20/</pre>\n</
SF:body>\n</html>\n")%r(HTTPOptions,D2,"HTTP/1\.1\x20204\x20No\x20Content\
SF:r\nVary:\x20Origin,\x20Access-Control-Request-Headers\r\nAccess-Control
SF:-Allow-Methods:\x20GET,HEAD,PUT,PATCH,POST,DELETE\r\nContent-Length:\x2
SF:00\r\nDate:\x20Fri,\x2014\x20Jun\x202024\x2015:09:25\x20GMT\r\nConnecti
SF:on:\x20close\r\n\r\n")%r(RTSPRequest,2F,"HTTP/1\.1\x20400\x20Bad\x20Req
SF:uest\r\nConnection:\x20close\r\n\r\n")%r(RPCCheck,2F,"HTTP/1\.1\x20400\
SF:x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(DNSVersionBindReq
SF:TCP,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\
SF:r\n")%r(DNSStatusRequestTCP,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nC
SF:onnection:\x20close\r\n\r\n")%r(Help,2F,"HTTP/1\.1\x20400\x20Bad\x20Req
SF:uest\r\nConnection:\x20close\r\n\r\n")%r(SSLSessionReq,2F,"HTTP/1\.1\x2
SF:0400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(TerminalServ
SF:erCookie,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close
SF:\r\n\r\n")%r(TLSSessionReq,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nCo
SF:nnection:\x20close\r\n\r\n")%r(Kerberos,2F,"HTTP/1\.1\x20400\x20Bad\x20
SF:Request\r\nConnection:\x20close\r\n\r\n")%r(SMBProgNeg,2F,"HTTP/1\.1\x2
SF:0400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(X11Probe,2F,
SF:"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n");
```

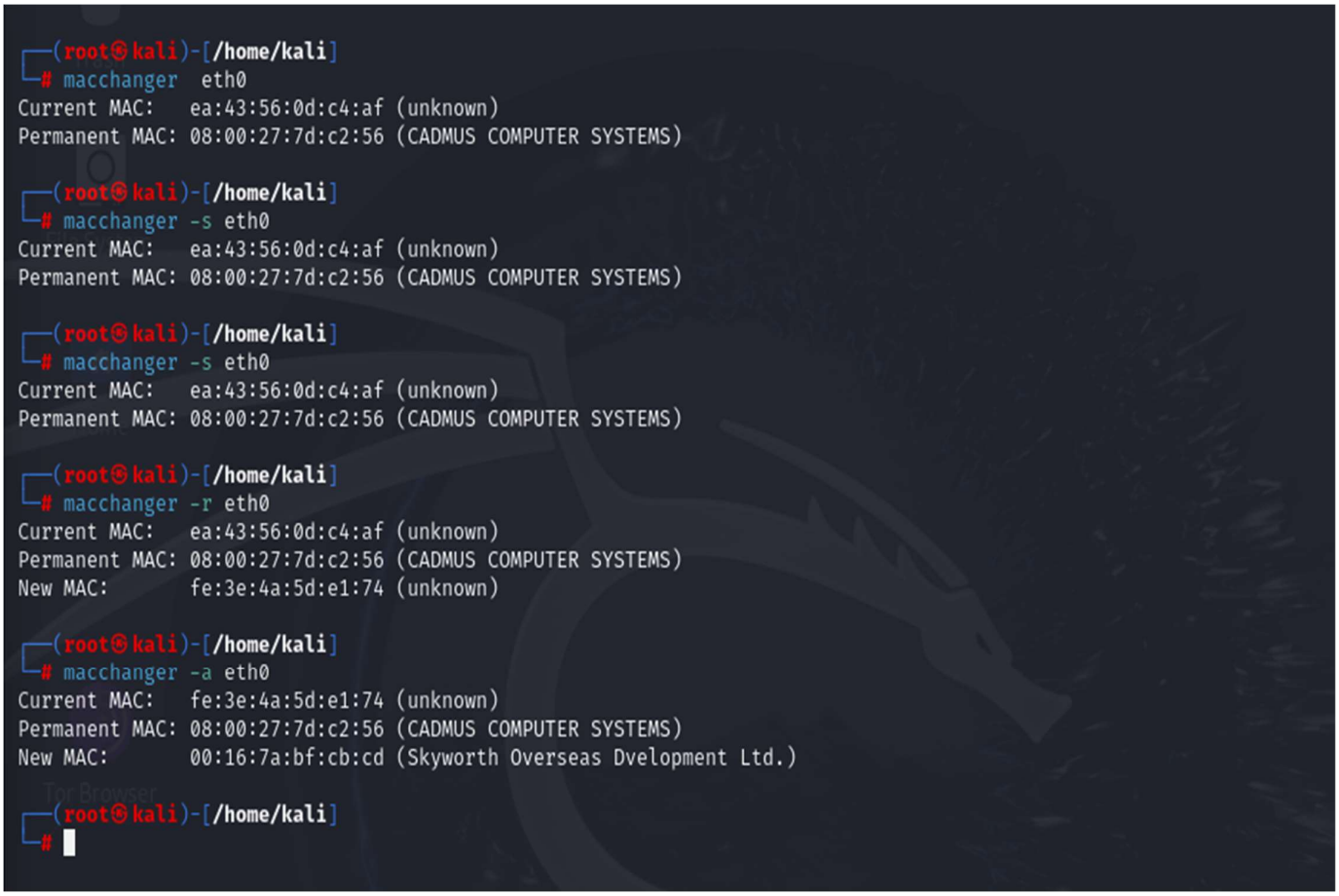
```
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port1043-TCP:V=7.94SVN%T=SSL%I=7%D=6/14%Time=666C5D2F%P=x86_64-pc-linux
SF:-gnu%r(GetRequest,27E,"HTTP/1\.1\x20404\x20Not\x20Found\r\nVary:\x20Ori
SF:gin\r\nContent-Security-Policy:\x20default-src\x20'self'\r\nX-DNS-Prefe
SF:tch-Control:\x20off\r\nExpect-CT:\x20max-age=0\r\nX-Frame-Options:\x20S
SF:AMEORIGIN\r\nStrict-Transport-Security:\x20max-age=15552000;\x20include
SF:SubDomains\r\nX-Download-Options:\x20noopen\r\nX-Content-Type-Options:\
SF:x20nosniff\r\nX-Permitted-Cross-Domain-Policies:\x20none\r\nReferrer-Po
SF:licy:\x20no-referrer\r\nX-XSS-Protection:\x200\r\nContent-Type:\x20text
SF:/html;\x20charset=utf-8\r\nContent-Length:\x20139\r\nDate:\x20Fri,\x201
SF:4\x20Jun\x202024\x2015:09:36\x20GMT\r\nConnection:\x20close\r\n\r\n<!DO
SF:CTYPE\x20html>\n<html\x20lang=\"en\">\n<head>\n<meta\x20charset=\"utf-8
SF:\">\n<title>Error</title>\n</head>\n<body>\n<pre>Cannot\x20GET\x20/</pr
SF:e>\n</body>\n</html>\n")%r(HTTPOptions,D2,"HTTP/1\.1\x20204\x20No\x20Co
SF:ntent\r\nVary:\x20Origin,\x20Access-Control-Request-Headers\r\nAccess-C
SF:ontrol-Allow-Methods:\x20GET,HEAD,PUT,PATCH,POST,DELETE\r\nContent-Leng
SF:th:\x200\r\nDate:\x20Fri,\x2014\x20Jun\x202024\x2015:09:36\x20GMT\r\nCo
SF:nnection:\x20close\r\n\r\n")%r(TerminalServerCookie,2F,"HTTP/1\.1\x2040
SF:0\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(FourOhFourReque
SF:st,2E6,"HTTP/1\.1\x20500\x20Internal\x20Server\x20Error\r\nVary:\x20Ori
SF:gin\r\nContent-Security-Policy:\x20default-src\x20'self'\x20blob:\x2012
SF:7\.0\.0\.1:1042\x20127\.0\.0\.1:1043;script-src\x20'self'\x20'unsafe-in
SF:line';style-src\x20'self';connect-src\x20'self'\x20ws:\x20wss:\x20blob:
SF:\x20127\.0\.0\.1:1042\x20127\.0\.0\.1:1043\x20127\.0\.0\.1:9013\x20127\
SF:.0\.0\.1:9014;worker-src\x20'self'\x20blob:\x20127\.0\.0\.1:1042\x20127
SF:\.0\.0\.1:1043;img-src\x20'self'\x20data:\x20blob:\x20127\.0\.0\.1:1042
SF:\x20127\.0\.0\.1:1043\r\nX-DNS-Prefetch-Control:\x20off\r\nExpect-CT:\x
SF:20max-age=0\r\nX-Frame-Options:\x20SAMEORIGIN\r\nStrict-Transport-Secur
SF:ity:\x20max-age=15552000;\x20includeSubDomains\r\nX-Download-Options:\x
SF:20noopen\r\nX-Content-Type-Options:\x20nosniff\r\nX-Permitted-Cross-Dom
SF:ain-Policies:\x20none\r\nReferrer-Policy:\x20no-referrer\r\nX-XSS-Prote
SF:ction:\x200\r\nDate:\x20Fri,\x2014\x20Jun\x202024\x2015:09:37\x20GMT\r\
SF:nConnection:\x20close\r\n\r\n");
MAC Address: C0:E7:0E:85:8C:B0 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.15 seconds
```

Lab 2 :Macchanger :
Task
□ Change your mac address to any random Mac address

SOULTION :

We use the various macchanger command in kali linux terminal to change the mac address. We use [macchanger eth0] OR [macchanger -s eth0] with this command we can get the current and permanent mac address of the Machine . If we want to generate any random Mac address. We use [macchanger -r eth0] OR [macchanger -a eth0]with this command we can generate the random mac address.



Lab 3: Netstat

Task

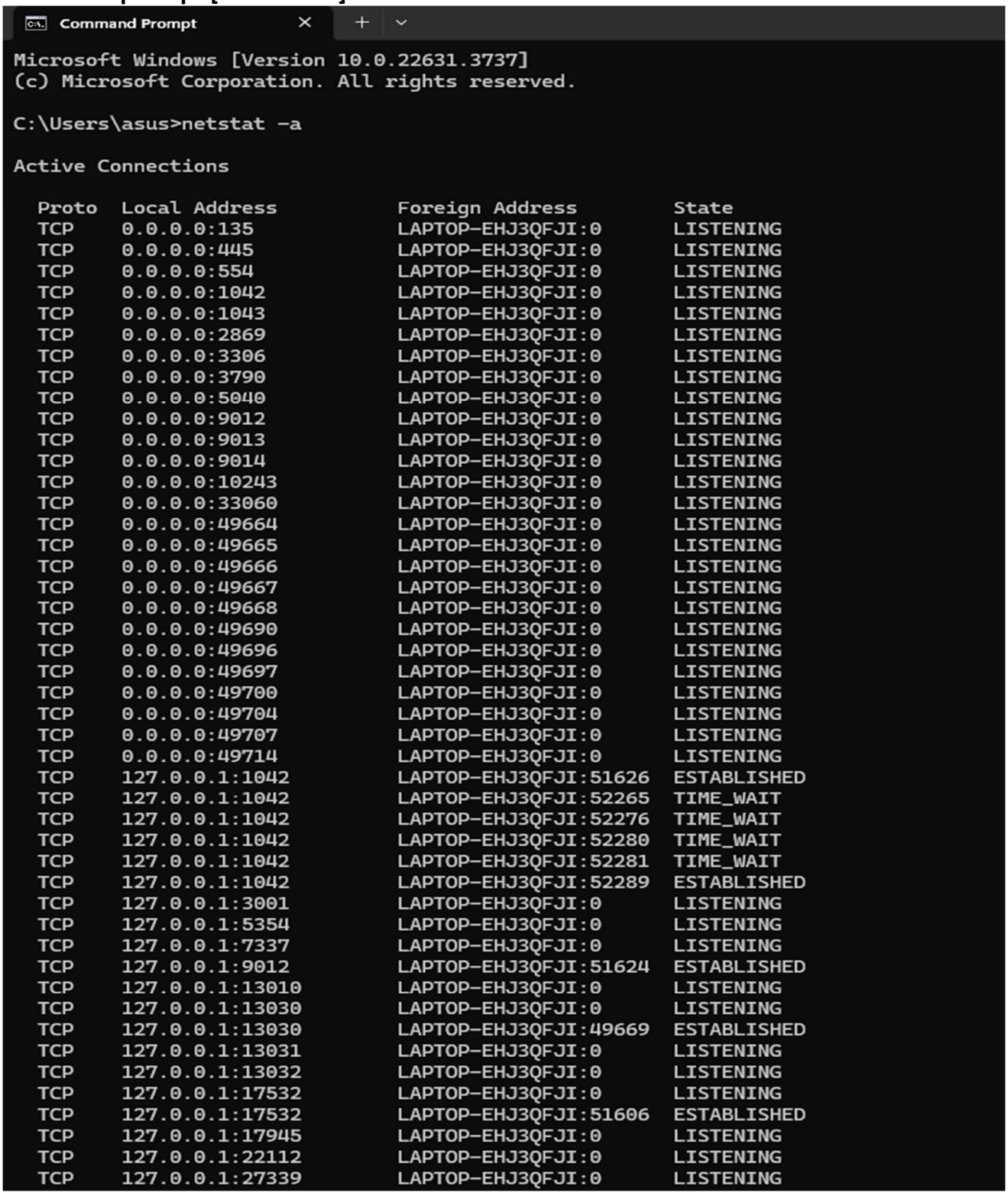
□ Enumerate all the ports in the Windows machine.

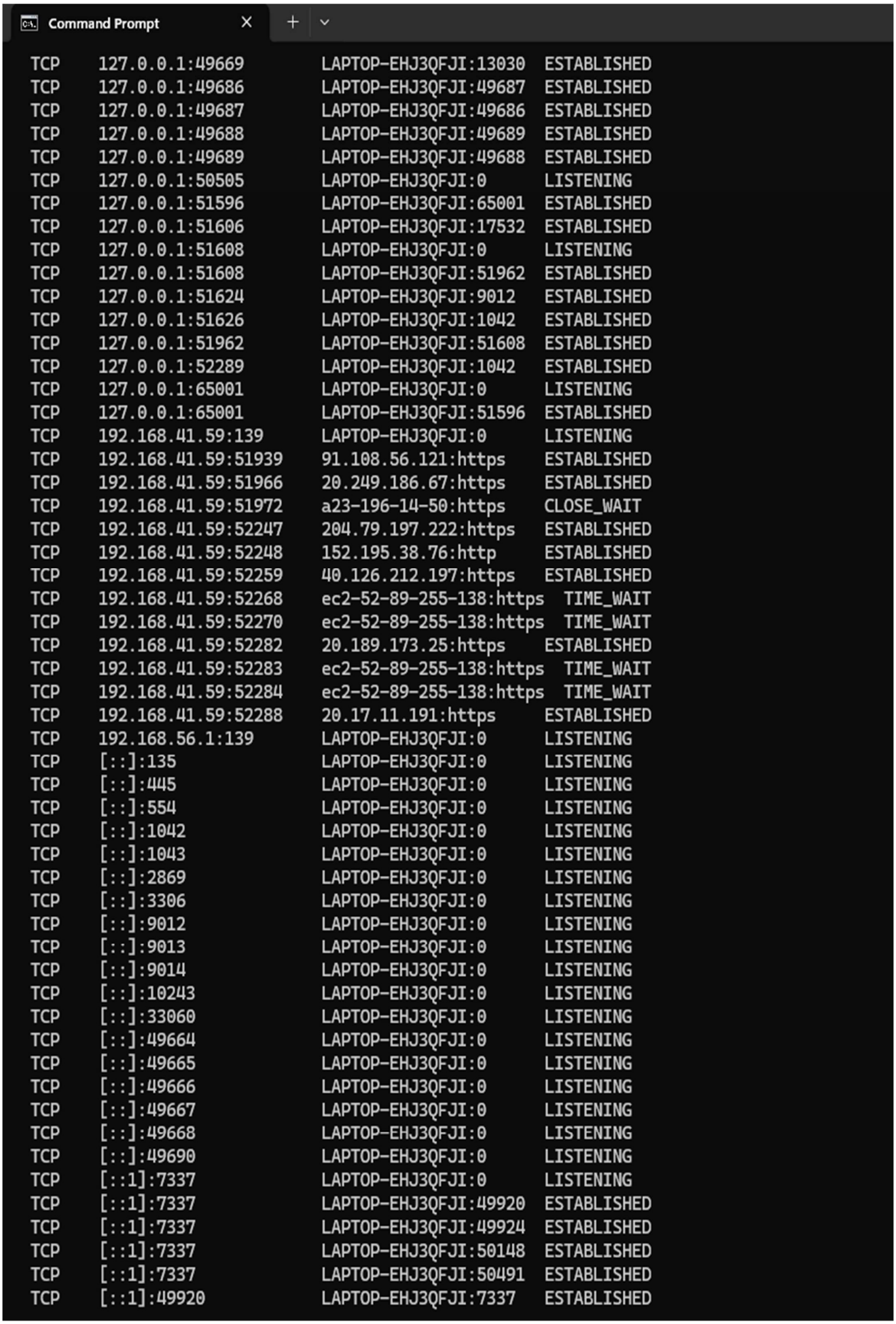
□ Display routing table of Windows machine.

SOULTION :

TASK 1 :

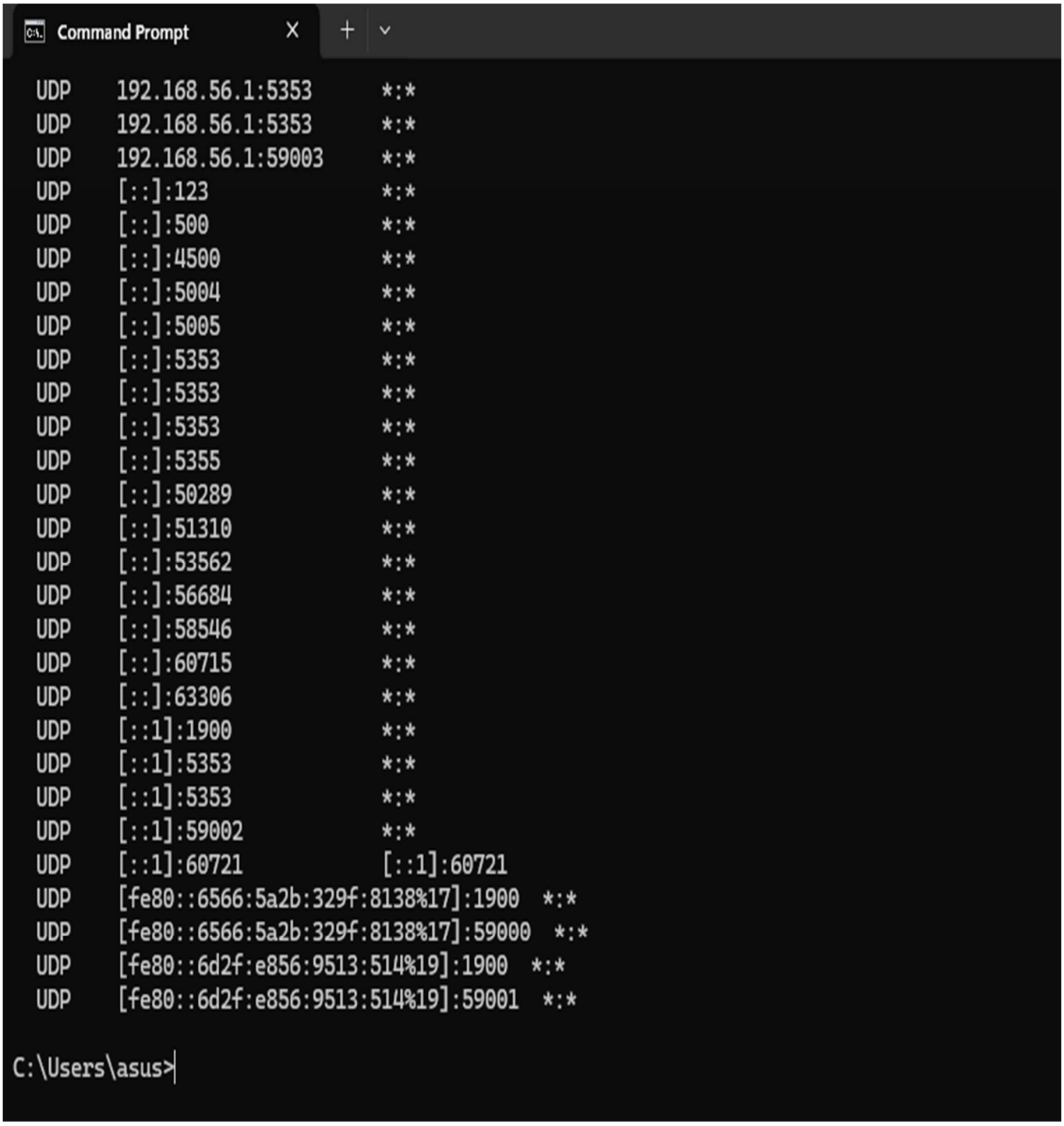
Enumerate all the ports in the Windows machine. Using netstat command in the windows command prompt [netstat -a].




Command Prompt
TCP 127.0.0.1:49669 LAPTOP-EHJ3QFJI:13030 ESTABLISHED
TCP 127.0.0.1:49686 LAPTOP-EHJ3QFJI:49687 ESTABLISHED
TCP 127.0.0.1:49687 LAPTOP-EHJ3QFJI:49686 ESTABLISHED
TCP 127.0.0.1:49688 LAPTOP-EHJ3QFJI:49689 ESTABLISHED
TCP 127.0.0.1:49689 LAPTOP-EHJ3QFJI:49688 ESTABLISHED
TCP 127.0.0.1:50505 LAPTOP-EHJ3QFJI:0 LISTENING
TCP 127.0.0.1:51596 LAPTOP-EHJ3QFJI:65001 ESTABLISHED
TCP 127.0.0.1:51606 LAPTOP-EHJ3QFJI:17532 ESTABLISHED
TCP 127.0.0.1:51608 LAPTOP-EHJ3QFJI:0 LISTENING
TCP 127.0.0.1:51608 LAPTOP-EHJ3QFJI:51962 ESTABLISHED
TCP 127.0.0.1:51624 LAPTOP-EHJ3QFJI:9012 ESTABLISHED
TCP 127.0.0.1:51626 LAPTOP-EHJ3QFJI:1042 ESTABLISHED
TCP 127.0.0.1:51962 LAPTOP-EHJ3QFJI:51608 ESTABLISHED
TCP 127.0.0.1:52289 LAPTOP-EHJ3QFJI:1042 ESTABLISHED
TCP 127.0.0.1:65001 LAPTOP-EHJ3QFJI:0 LISTENING
TCP 127.0.0.1:65001 LAPTOP-EHJ3QFJI:51596 ESTABLISHED
TCP 192.168.41.59:139 LAPTOP-EHJ3QFJI:0 LISTENING
TCP 192.168.41.59:51939 91.108.56.121:https ESTABLISHED
TCP 192.168.41.59:51966 20.249.186.67:https ESTABLISHED
TCP 192.168.41.59:51972 a23-196-14-50:https CLOSE_WAIT
TCP 192.168.41.59:52247 204.79.197.222:https ESTABLISHED
TCP 192.168.41.59:52248 152.195.38.76:http ESTABLISHED
TCP 192.168.41.59:52259 40.126.212.197:https ESTABLISHED
TCP 192.168.41.59:52268 ec2-52-89-255-138:https TIME_WAIT
TCP 192.168.41.59:52270 ec2-52-89-255-138:https TIME_WAIT
TCP 192.168.41.59:52282 20.189.173.25:https ESTABLISHED
TCP 192.168.41.59:52283 ec2-52-89-255-138:https TIME_WAIT
TCP 192.168.41.59:52284 ec2-52-89-255-138:https TIME_WAIT
TCP 192.168.41.59:52288 20.17.11.191:https ESTABLISHED
TCP 192.168.56.1:139 LAPTOP-EHJ3QFJI:0 LISTENING
TCP [::]:135 LAPTOP-EHJ3QFJI:0 LISTENING
TCP [::]:445 LAPTOP-EHJ3QFJI:0 LISTENING
TCP [::]:554 LAPTOP-EHJ3QFJI:0 LISTENING
TCP [::]:1042 LAPTOP-EHJ3QFJI:0 LISTENING
TCP [::]:1043 LAPTOP-EHJ3QFJI:0 LISTENING
TCP [::]:2869 LAPTOP-EHJ3QFJI:0 LISTENING
TCP [::]:3306 LAPTOP-EHJ3QFJI:0 LISTENING
TCP [::]:9012 LAPTOP-EHJ3QFJI:0 LISTENING
TCP [::]:9013 LAPTOP-EHJ3QFJI:0 LISTENING
TCP [::]:9014 LAPTOP-EHJ3QFJI:0 LISTENING
TCP [::]:10243 LAPTOP-EHJ3QFJI:0 LISTENING
TCP [::]:33060 LAPTOP-EHJ3QFJI:0 LISTENING
TCP [::]:49664 LAPTOP-EHJ3QFJI:0 LISTENING
TCP [::]:49665 LAPTOP-EHJ3QFJI:0 LISTENING
TCP [::]:49666 LAPTOP-EHJ3QFJI:0 LISTENING
TCP [::]:49667 LAPTOP-EHJ3QFJI:0 LISTENING
TCP [::]:49668 LAPTOP-EHJ3QFJI:0 LISTENING
TCP [::]:49690 LAPTOP-EHJ3QFJI:0 LISTENING
TCP [::1]:7337 LAPTOP-EHJ3QFJI:0 LISTENING
TCP [::1]:7337 LAPTOP-EHJ3QFJI:49920 ESTABLISHED
TCP [::1]:7337 LAPTOP-EHJ3QFJI:49924 ESTABLISHED
TCP [::1]:7337 LAPTOP-EHJ3QFJI:50148 ESTABLISHED
TCP [::1]:7337 LAPTOP-EHJ3QFJI:50491 ESTABLISHED
TCP [::1]:49920 LAPTOP-EHJ3QFJI:7337 ESTABLISHED

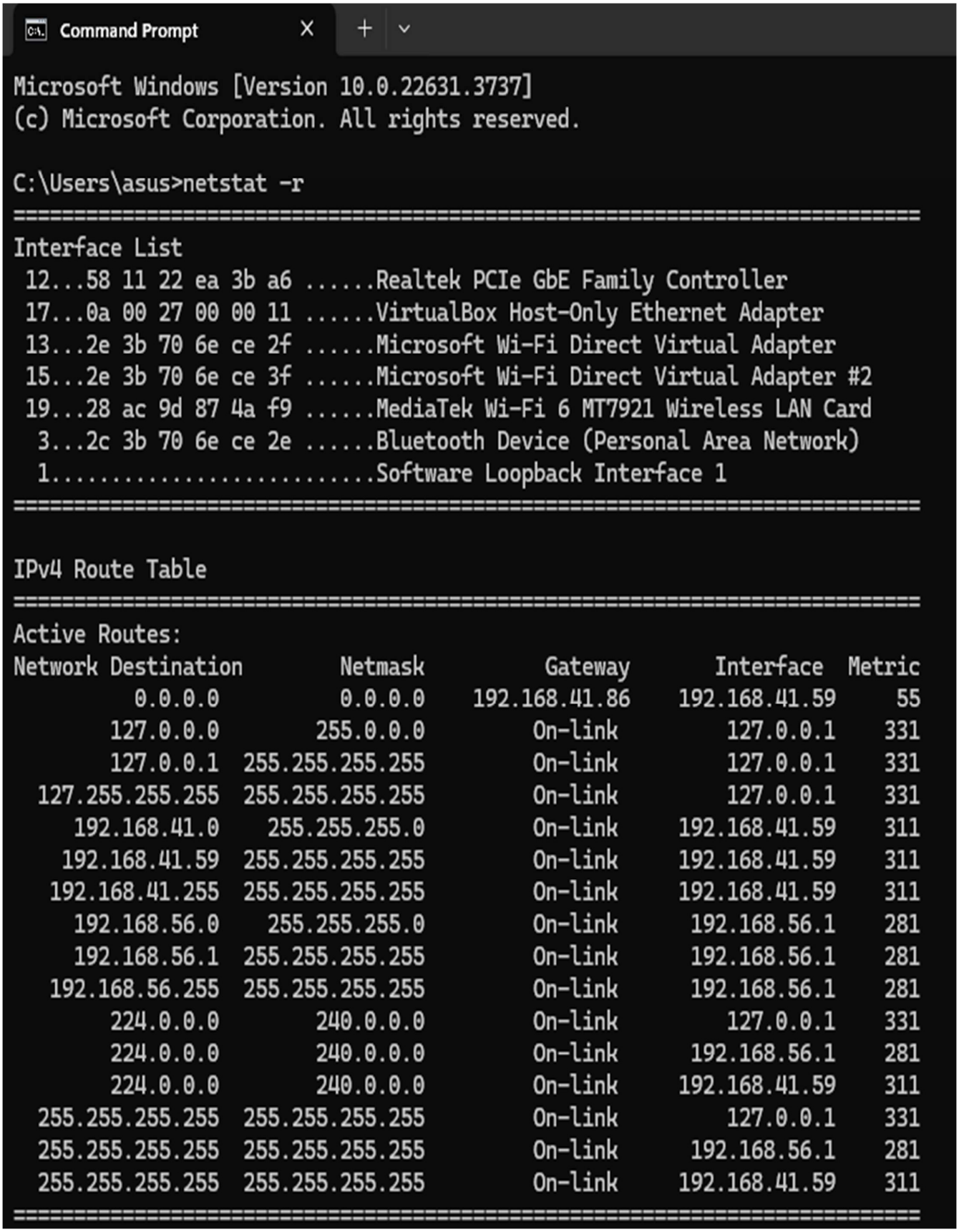
Command Prompt

```
TCP    [::1]:49924            LAPTOP-EHJ3QFJI:7337   ESTABLISHED
TCP    [::1]:50148            LAPTOP-EHJ3QFJI:7337   ESTABLISHED
TCP    [::1]:50491            LAPTOP-EHJ3QFJI:7337   ESTABLISHED
TCP    [2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:49414  [2603:1040:a06:6::2]:https  ESTABLISHED
TCP    [2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:51934  [2603:1040:a06:6::2]:https  ESTABLISHED
TCP    [2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:51948  g2600-140f-0004-0d9b-0000-0000-0000-1011:https  CLOSE_WAIT
TCP    [2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:52246  g2600-140f-1e00-0000-0000-0000-17c4-0e80:https  ESTABLISHED
TCP    [2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:52253  [2620:1ec:bdf::68]:https  ESTABLISHED
TCP    [2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:52256  [2603:1063:2000::254]:https  ESTABLISHED
TCP    [2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:52262  g2600-140f-1e00-0000-0000-0000-17c4-0ec9:https  ESTABLISHED
TCP    [2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:52263  [2603:1046:900:2c::2]:https  ESTABLISHED
TCP    [2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:52279  [2600:9000:2600:1800:5:c033:1800:93a1]:https  ESTABLISHED
TCP    [2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:52285  [2620:1ec:bdf::254]:https  ESTABLISHED
TCP    [2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:52286  [2603:1063:27:2::254]:https  ESTABLISHED
TCP    [2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:52293  [2803:f800:53::3]:https  TIME_WAIT
TCP    [2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:52294  [2803:f800:53::3]:https  TIME_WAIT
TCP    [2405:204:922d:3cad:c8cd:6e4d:fa57:b575]:52295  [2803:f800:53::3]:https  TIME_WAIT
UDP    0.0.0.0:123            *:*
UDP    0.0.0.0:500            *:*
UDP    0.0.0.0:4500           *:*
UDP    0.0.0.0:5004           *:*
UDP    0.0.0.0:5004           *:*
UDP    0.0.0.0:5005           *:*
UDP    0.0.0.0:5005           *:*
UDP    0.0.0.0:5050           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5355           *:*
UDP    0.0.0.0:50289          *:*
UDP    0.0.0.0:51310          *:*
UDP    0.0.0.0:53561          *:*
UDP    0.0.0.0:56684          *:*
UDP    0.0.0.0:58546          *:*
UDP    0.0.0.0:60714          *:*
UDP    0.0.0.0:63306          *:*
UDP    127.0.0.1:1900         *:*
UDP    127.0.0.1:10020        *:*
UDP    127.0.0.1:28363        *:*
UDP    127.0.0.1:57252        *:*
UDP    127.0.0.1:59005        *:*
UDP    127.0.0.1:60716        127.0.0.1:60716
UDP    192.168.41.59:137      *:*
UDP    192.168.41.59:138      *:*
UDP    192.168.41.59:1900     *:*
UDP    192.168.41.59:5353     *:*
UDP    192.168.41.59:5353     *:*
UDP    192.168.41.59:59004    *:*
UDP    192.168.56.1:137       *:*
UDP    192.168.56.1:138       *:*
UDP    192.168.56.1:1900      *:*
UDP    192.168.56.1:5353      *:*
```


Command Prompt
UDP 192.168.56.1:5353 *:*
UDP 192.168.56.1:5353 *:*
UDP 192.168.56.1:59003 *:*
UDP [::]:123 *:*
UDP [::]:500 *:*
UDP [::]:4500 *:*
UDP [::]:5004 *:*
UDP [::]:5005 *:*
UDP [::]:5353 *:*
UDP [::]:5353 *:*
UDP [::]:5353 *:*
UDP [::]:5355 *:*
UDP [::]:50289 *:*
UDP [::]:51310 *:*
UDP [::]:53562 *:*
UDP [::]:56684 *:*
UDP [::]:58546 *:*
UDP [::]:60715 *:*
UDP [::]:63306 *:*
UDP [::1]:1900 *:*
UDP [::1]:5353 *:*
UDP [::1]:5353 *:*
UDP [::1]:59002 *:*
UDP [::1]:60721 [::1]:60721
UDP [fe80::6566:5a2b:329f:8138%17]:1900 *:*
UDP [fe80::6566:5a2b:329f:8138%17]:59000 *:*
UDP [fe80::6d2f:e856:9513:514%19]:1900 *:*
UDP [fe80::6d2f:e856:9513:514%19]:59001 *:*
C:\Users\asus>

TASK 2 :

Display routing table of Windows machine. Using the netstat command in windows command prompt [netstat -r].



```
Command Prompt

Microsoft Windows [Version 10.0.22631.3737]
(c) Microsoft Corporation. All rights reserved.

C:\Users\asus>netstat -r
===========================================================================
Interface List
 12...58 11 22 ea 3b a6 ......Realtek PCIe GbE Family Controller
 17...0a 00 27 00 00 11 ......VirtualBox Host-Only Ethernet Adapter
 13...2e 3b 70 6e ce 2f ......Microsoft Wi-Fi Direct Virtual Adapter
 15...2e 3b 70 6e ce 3f ......Microsoft Wi-Fi Direct Virtual Adapter #2
 19...28 ac 9d 87 4a f9 ......MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
  3...2c 3b 70 6e ce 2e ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.41.86    192.168.41.59     55
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
     192.168.41.0    255.255.255.0         On-link     192.168.41.59    311
    192.168.41.59  255.255.255.255         On-link     192.168.41.59    311
   192.168.41.255  255.255.255.255         On-link     192.168.41.59    311
     192.168.56.0    255.255.255.0         On-link      192.168.56.1    281
     192.168.56.1  255.255.255.255         On-link      192.168.56.1    281
   192.168.56.255  255.255.255.255         On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link     192.168.41.59    311
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      192.168.56.1    281
  255.255.255.255  255.255.255.255         On-link     192.168.41.59    311
===========================================================================
```

```
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 19     71 ::/0                     fe80::28c1:bfff:fec9:fd70
  1    331 ::1/128                  On-link
 19     71 2405:204:922d:3cad::/64  On-link
 19    311 2405:204:922d:3cad:53aa:ffbf:5857:8e9/128
                                    On-link
 19    311 2405:204:922d:3cad:c8cd:6e4d:fa57:b575/128
                                    On-link
 17    281 fe80::/64                On-link
 19    311 fe80::/64                On-link
 17    281 fe80::6566:5a2b:329f:8138/128
                                    On-link
 19    311 fe80::6d2f:e856:9513:514/128
                                    On-link
  1    331 ff00::/8                 On-link
 17    281 ff00::/8                 On-link
 19    311 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None

C:\Users\asus>
```

Lab 4: WireShark
Description

Wireshark is an open-source packet analyzer used for monitoring networks by network or security administrators. This tool lets you see traffic passing through the network and helps you to inspect the traffic, troubleshoot the network, and even understand how communication between network devices takes place. Wireshark is built into Linux distributions like Kali Linux and is also available on OS X and Windows. Before opening Kali make sure you have the network settings on the bridged network. Select your Kali VM to go to settings and change the following settings. This will put your windows machine and Kali VM in the same network.

Things to know before performing the lab

Protocols

An established set of guidelines that govern how data is exchanged across various devices connected to the same network is known as a network protocol.

TCP stream

You can monitor a specific TCP discussion between two or more hosts using this capability. It locates all the TCP packets between a specific source and destination and puts the data sent during that exchange back together in a parseable form.

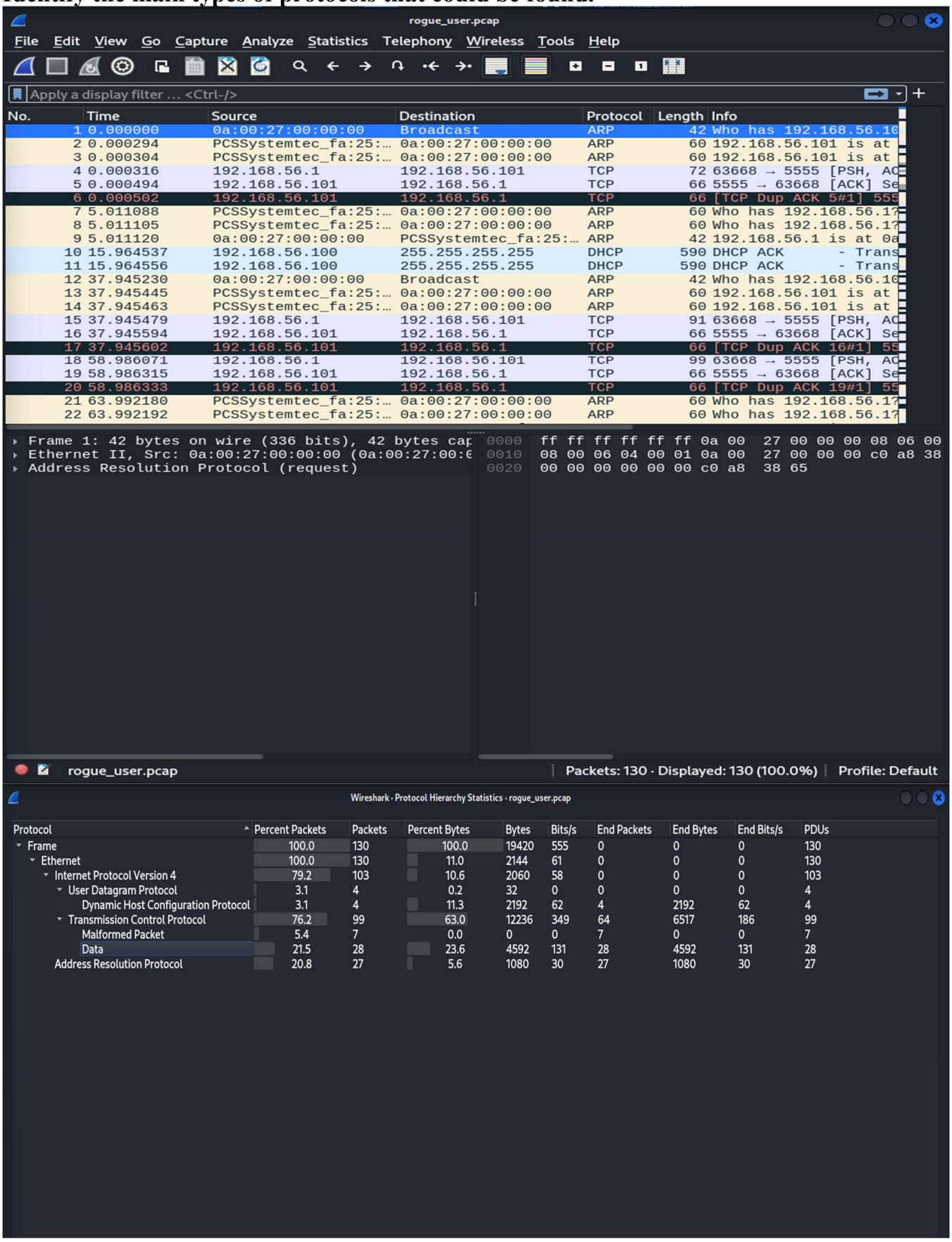
Task

- **Identify the main types of protocols that could be found.**
- **Find the protocol through which data is passed.**
- **Create a column to identify TCP Streams.**
- **Find the actual data that's passed in the TCP Streams.**

SOLUTION :

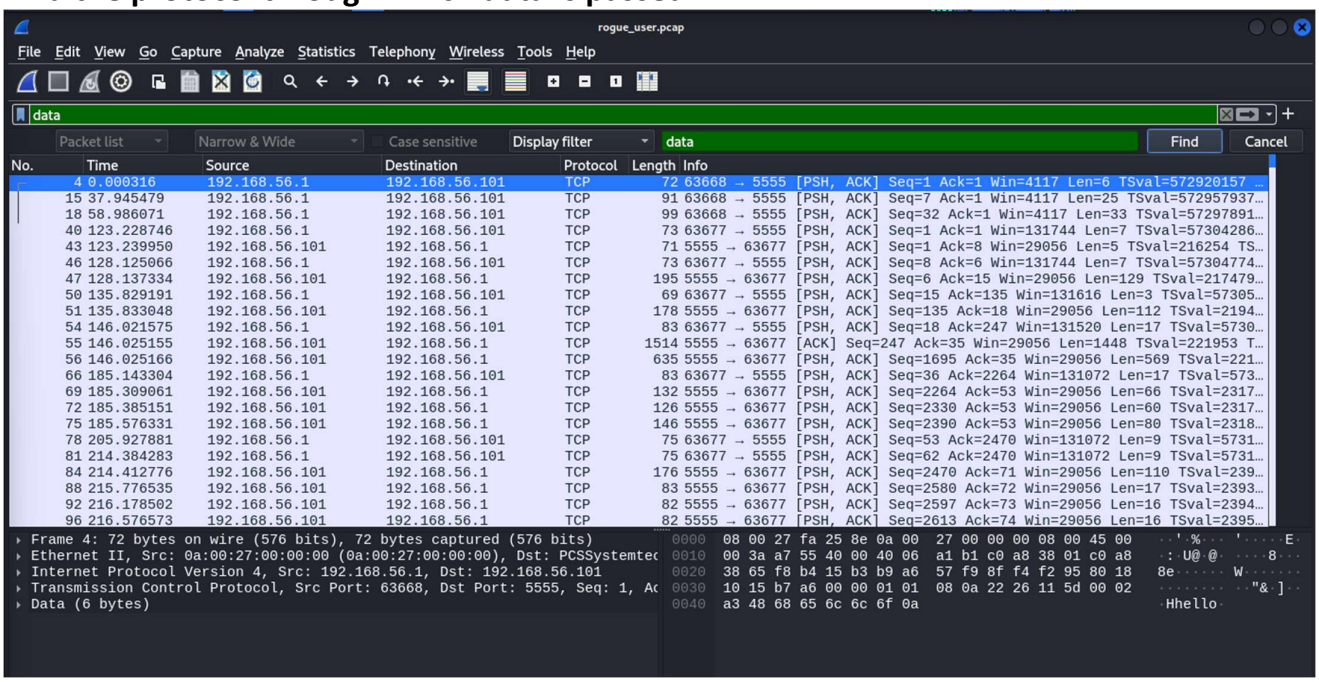
TASK 1 :

Identify the main types of protocols that could be found.



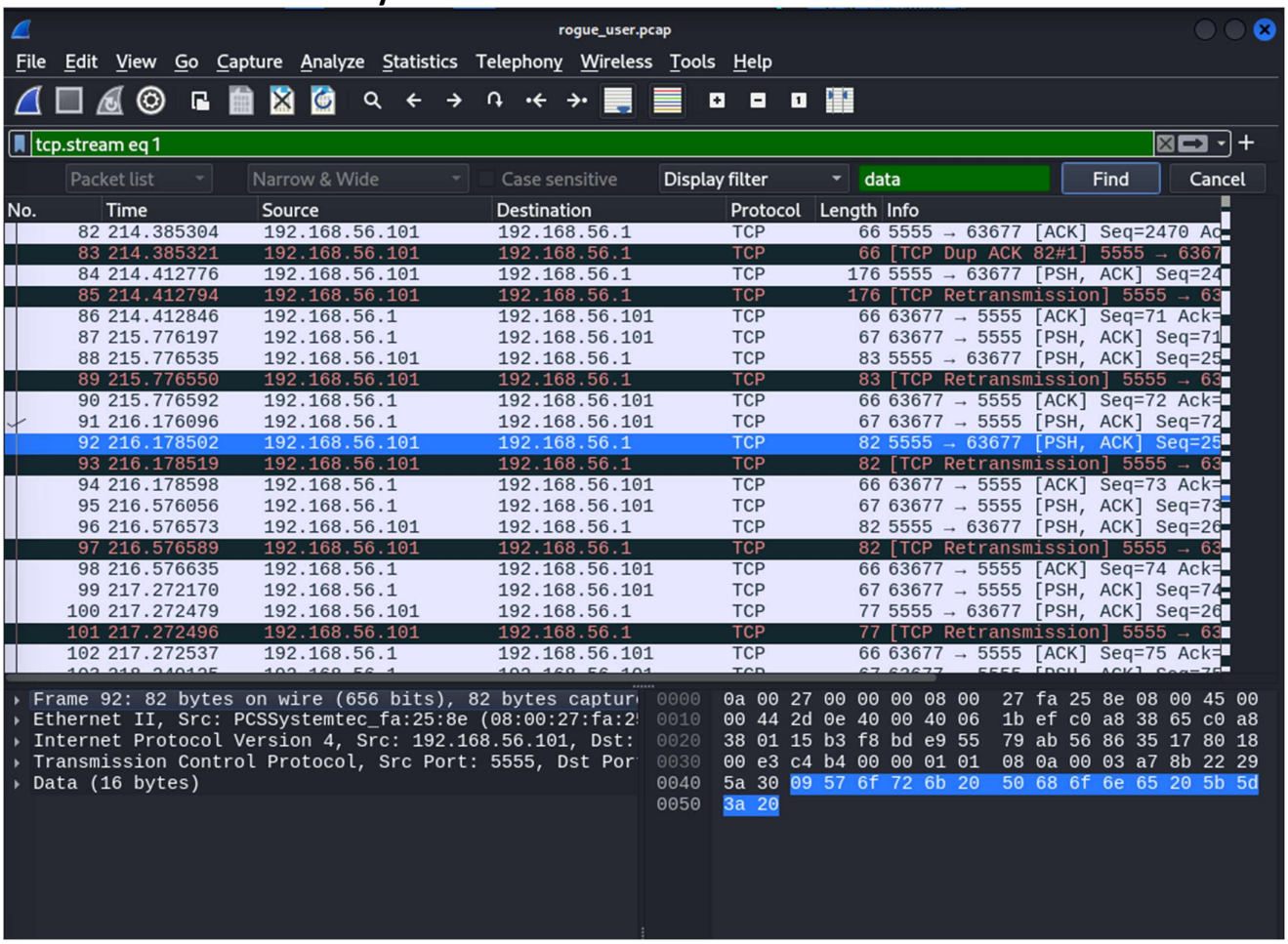
TASK 2 :

Find the protocol through which data is passed.



TASK 3:

Create a column to identify TCP Streams.



TASK 4 :

Find the actual data that's passed in the TCP Streams.