Group No - 6
F. Y. B. Tech. C. S.
Cyber Security

Aditya Patkar - 181070045

Archeel Parekh - 181070044

Mohammed Mehdi - 181070036

Srushti Shah - 191071902

LAB ASSIGNMENT 1

***AIM*:** To install openssl and study its commands.

***THEORY*:**

CASE STUDY: Air India Data Breach

The attack:

Air India announced in May 2021 that its customer database had suffered a massive security breach. It informed its affected passengers that the "breach involved some personal data registered between August 2011 and February 2021" and that "no password data was affected."

Approximately 4.5 million records may have been leaked in this massive security breach. Leaked data included passengers':

- Name
- Contact information
- Date of birth
- Ticket information
- Passport information
- Credit card data
- Frequent flyer data

The breach involved personal data registered over a ten-year period, between 26 August 2011 and 3 February 2021.

How did they discover it?

Air India first received news of the incident from **SITA** on 25 February, but only found out the identity of the affected data subjects on 25 March and 5 April. Following the breach, a number of steps were taken including securing the compromised servers and notifying and liaising with credit card issuers.

A spokesperson from SITA told IT Pro that its passenger processing services were the target of a "highly sophisticated but limited cyber attack" which affected passenger data stored on servers in SITA PSS's data centre in Atlanta, Georgia.

"By global and industry standards, we identified this cyber-attack extremely quickly. The matter remains under active investigation by SITA," said the spokesperson.

The airline is encouraging its passengers to change passwords to ensure the safety of their personal data.

Security Parameter

SITA is a Switzerland-based technology company specializing in air transport communications and information technology. The company was started by 11 member airlines and now has over 2,500 customers in more than 200 countries.

SITA offers services such as passenger processing, reservation systems, etc.

Air India had entered into a deal with SITA in 2017 to upgrade its IT infrastructure to enable it to join Star Alliance.

At Air India, SITA also implemented an online booking engine, departure control system, check-in and automated boarding control, baggage reconciliation system and the frequent flyer programme.

What is known is that the breach occurred during a recent cybersecurity attack of the airline's ***third-party data processor, SITA PSS***, which handles the storage and processing of passengers' personal information in the cloud.

Air India Response to the Security Breach

In its response to its massive security breach, Air India announced it took the following steps to ensure passenger data safety by:

- Investigating the security breach
- Securing the servers that were compromised
- Working with external data security incident specialists
- Notifying and working with credit card issuers
- Resetting passwords for its Frequent Flyer program

The airline further stated:

"Further, our data processor has ensured that no abnormal activity was observed after securing the compromised servers. While we and our data processor continue to take remedial actions including but not limited to the above, we would also encourage passengers to change passwords wherever applicable to ensure safety of their personal data. The protection of our customers' personal data is of highest importance to us, and we deeply regret the inconvenience caused and appreciate continued support and trust of our passengers."

Steps to take to protect data:

The Air India security breach was India's second major airline data breach within six months. The number of security breaches grew exponentially during the COVID-19 pandemic and continues with no stop in sight post-pandemic. Let's also consider the recent high-profile attacks that have threatened critical infrastructures, such as the cyberattacks on the Colonial Pipeline in the United States and the world's largest meat supplier JBS. No company is immune from falling victim to a cyberattack.

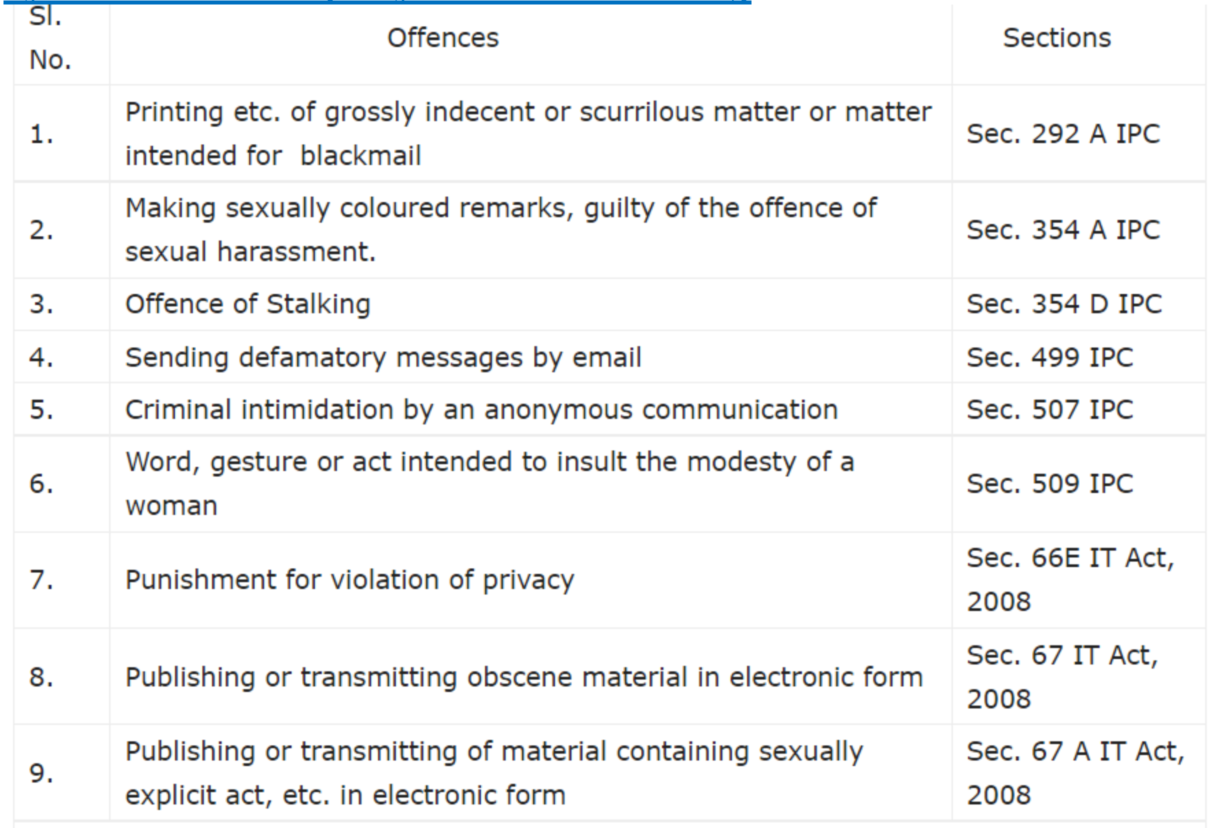
The question is whether companies like Air India and others are doing enough from a data security and data privacy point of view to protect themselves and their customers that put their trust in them. It is of the utmost importance that organizations take further steps to bulletproof their data from cyberattacks, especially if they are using external third-party services.

Compliance with best-practice data security guidelines and international standards is a significant step to prevent future breaches. Additionally, to mitigate the potential damage of breaches that may occur, it is of utmost importance that an organisation employs a strong encryption strategy and operational processes. To prevent unencrypted data being accessed by unauthorized parties, Air India must take steps to ensure that:

- Its data remains **encrypted while at rest in its databases.**
- Its data remains **encrypted while in transit** while it migrates between clients, applications, and Air India personnel.
- **The HSMs must not be accessible by the third-party data processor.**
- Only Air India performs all key management.
- Its encryption keys must never be with its third-party data processor and must remain stored in Air India's vaulted data center.
- Third parties will not have access to readable data.
- The mandatory multifactor authentication of clients is implemented to generally limit the access to data to only authorized persons like passengers who can only view their personal data.

These steps towards best practice emphasizes the need for strong cryptography (using HSMs) and lifecycle key management - to enable a business to be confident that its sensitive data is (at rest or in use) is protected against breaches - so confidential data remains encrypted regardless of whether attackers gain access to it.

Cyber Laws in India for cybercrime and stalking



Sl. No.	Offences	Sections
1.	Printing etc. of grossly indecent or scurrilous matter or matter intended for blackmail	Sec. 292 A IPC
2.	Making sexually coloured remarks, guilty of the offence of sexual harassment.	Sec. 354 A IPC
3.	Offence of Stalking	Sec. 354 D IPC
4.	Sending defamatory messages by email	Sec. 499 IPC
5.	Criminal intimidation by an anonymous communication	Sec. 507 IPC
6.	Word, gesture or act intended to insult the modesty of a woman	Sec. 509 IPC
7.	Punishment for violation of privacy	Sec. 66E IT Act, 2008
8.	Publishing or transmitting obscene material in electronic form	Sec. 67 IT Act, 2008
9.	Publishing or transmitting of material containing sexually explicit act, etc. in electronic form	Sec. 67 A IT Act, 2008

The cyber stalking cases are dealt in India by the:

1. Information Technology Act 2000

→ If any person is publishing or sending any salacious material in the form of electronic media is to be charged under section 67 of the Act. This dose not involves the determination of the extent of liability of ISP (internet service providers) and their directors.

→ For the preclusion of cyber stalking the protection of the data is very important, which gets leaked easily by the hackers. According to the amended IT act, section 43 A is added for the inclusion of a Body corporate", the allowing of the compensation in the case of a firm or a company which causes any wrongful losses or gain to any person by the way of transmitting any sensitive information and the maintenance of such type of security, then such body corporate shall be liable to pay damages by way of compensation.

→ The Information Technology Act, 2000 also comes into picture when the cyberstalker posts or sends any obscene content to the victim. Section 67 of the

Information Technology Act states that when any obscene material is published, transmitted or caused to be published in any electronic form, then it is a crime of obscenity, punishable with imprisonment for up to 5 years with fine of up to Rs. 1 lakh. A second or subsequent conviction is punishable by imprisonment for up to 10 years with a fine of up to Rs. 2 lakh.

→ Section 500 of the Indian Penal Code that deals with defamation, can be applied in case of cyber stalking in India if the stalker forges the victim’s personal information to post an obscene message or comment on any electronic media. Section 500 criminalises publishing any false statement against a person or harming the person's reputation and provides punishment for any such act with imprisonment up to 2 years, fine or both.

→ Section 43 - Applicable to people who damage the computer systems without permission from the owner. The owner can fully claim compensation for the entire damage in such cases.

→ Section 66 - Applicable in case a person is found to dishonestly or fraudulently committing any act referred to in section 43. The imprisonment term in such instances can mount up to three years or a fine of up to Rs. 5 lakh.

→ Section 66B - Incorporates the punishments for fraudulently receiving stolen communication devices or computers, which confirms a probable three years imprisonment. This term can also be topped by Rs. 1 lakh fine, depending upon the severity.

→ Section 66C - This section scrutinizes the identity thefts related to imposter digital signatures, hacking passwords, or other distinctive identification features. If proven guilty, imprisonment of three years might also be backed by Rs.1 lakh fine.

→ Section 66 D - This section was inserted on-demand, focusing on punishing cheaters doing impersonation using computer resources.

2. The criminal law (Amendment) Act, 2013

The act includes Stalking” as an offence under Section 35D of the IPC(Indian penal code).

This act states that, Any man who-

I. contacts and follows a woman or attempts to contacts such woman to proselytize personal communication repeatedly despite of being clear indication of disinterest by such woman or;

II. Observe the use of a woman over the internet, instant messages, e-mail or any other form of electronic communication is the offence of stalking”.

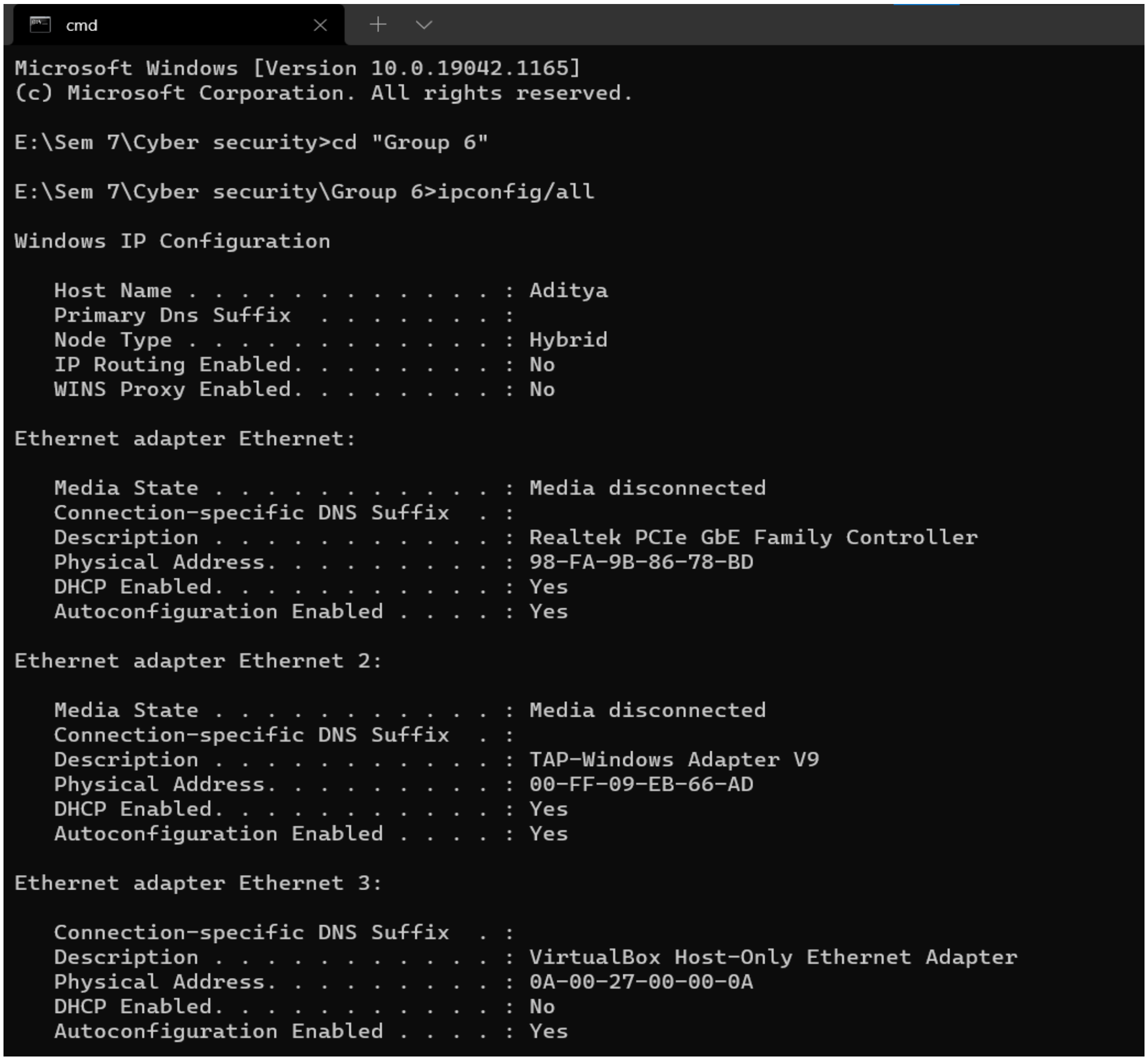
Racism is also a factor in cyber stalking.

IPCONFIG/ALL

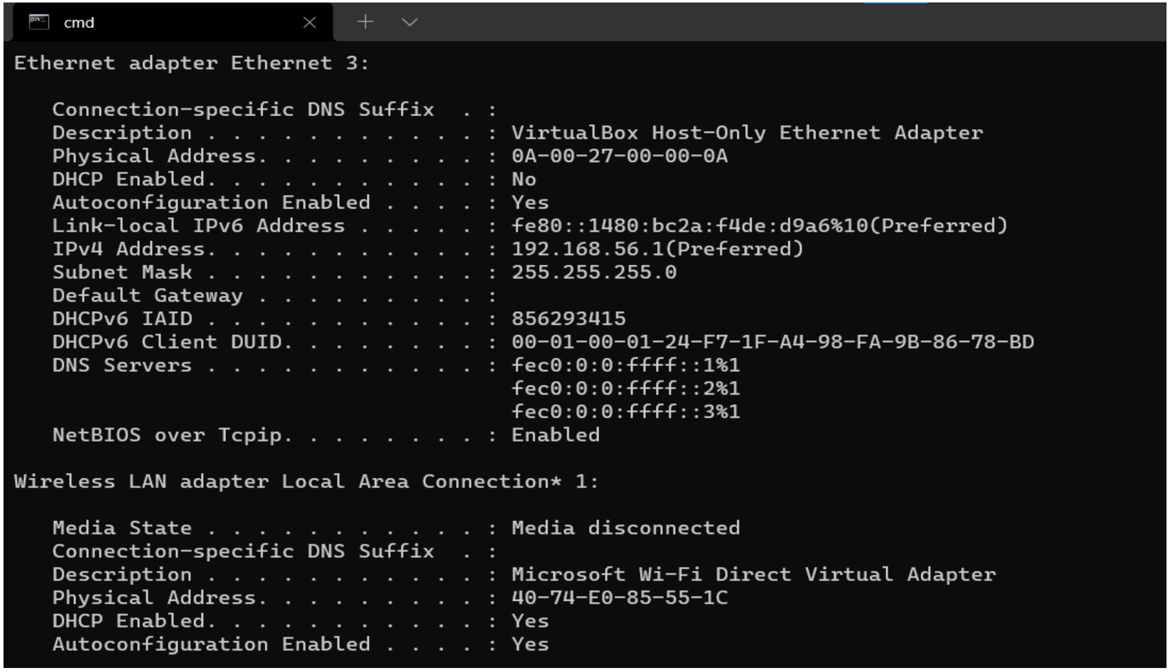
Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, ipconfig displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.

ipconfig /all displays all configuration information for each adapter bound to TCP/IP.

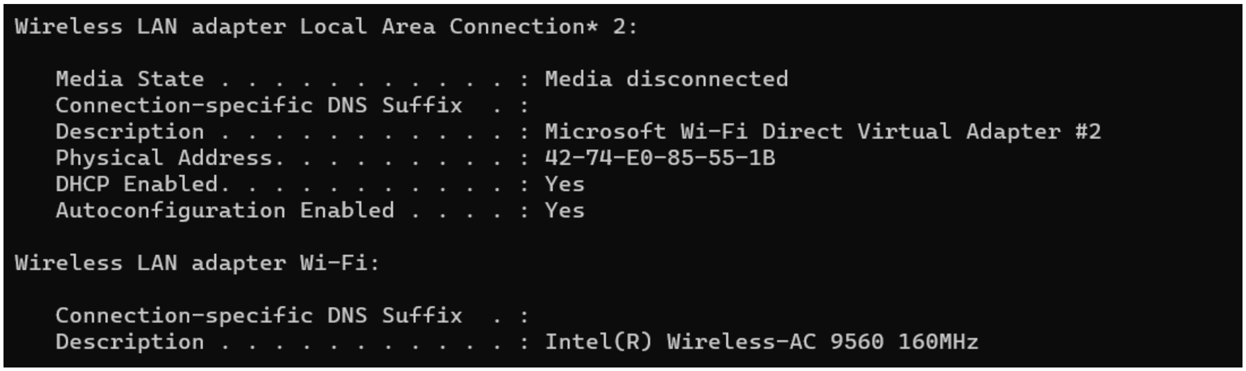
Ipconfig shows IP address, Subnet Mask, and Default gateway for all adapters. Ipconfig /all shows the description of each network connection along with additional information such as your physical (MAC) address, DHCP connections, Lease times, as well as in-depth IPv6 information.



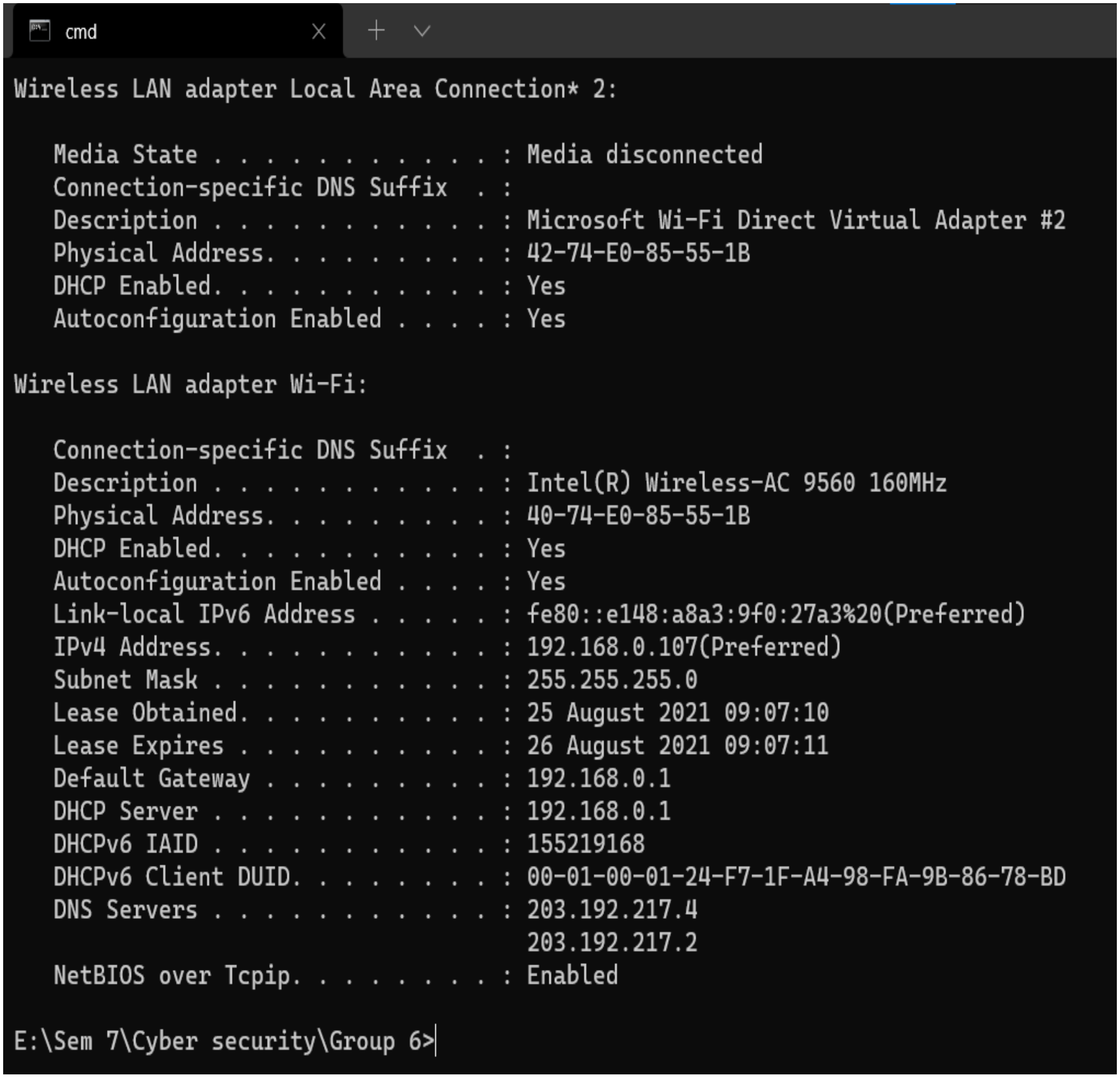
```
Microsoft Windows [Version 10.0.19042.1165]
(c) Microsoft Corporation. All rights reserved.

E:\Sem 7\Cyber security>cd "Group 6"

E:\Sem 7\Cyber security\Group 6>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Aditya
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : 98-FA-9B-86-78-BD
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : TAP-Windows Adapter V9
   Physical Address. . . . . . . . . : 00-FF-09-EB-66-AD
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-0A
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
```



```
Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-0A
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::1480:bc2a:f4de:d9a6%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.56.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 856293415
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-F7-1F-A4-98-FA-9B-86-78-BD
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 40-74-E0-85-55-1C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```



```
Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 42-74-E0-85-55-1B
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9560 160MHz
```



```
Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 42-74-E0-85-55-1B
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9560 160MHz
   Physical Address. . . . . . . . . : 40-74-E0-85-55-1B
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::e148:a8a3:9f0:27a3%20(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.107(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 25 August 2021 09:07:10
   Lease Expires . . . . . . . . . . : 26 August 2021 09:07:11
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 155219168
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-F7-1F-A4-98-FA-9B-86-78-BD
   DNS Servers . . . . . . . . . . . : 203.192.217.4
                                       203.192.217.2
   NetBIOS over Tcpip. . . . . . . . : Enabled

E:\Sem 7\Cyber security\Group 6>
```

NETSTAT

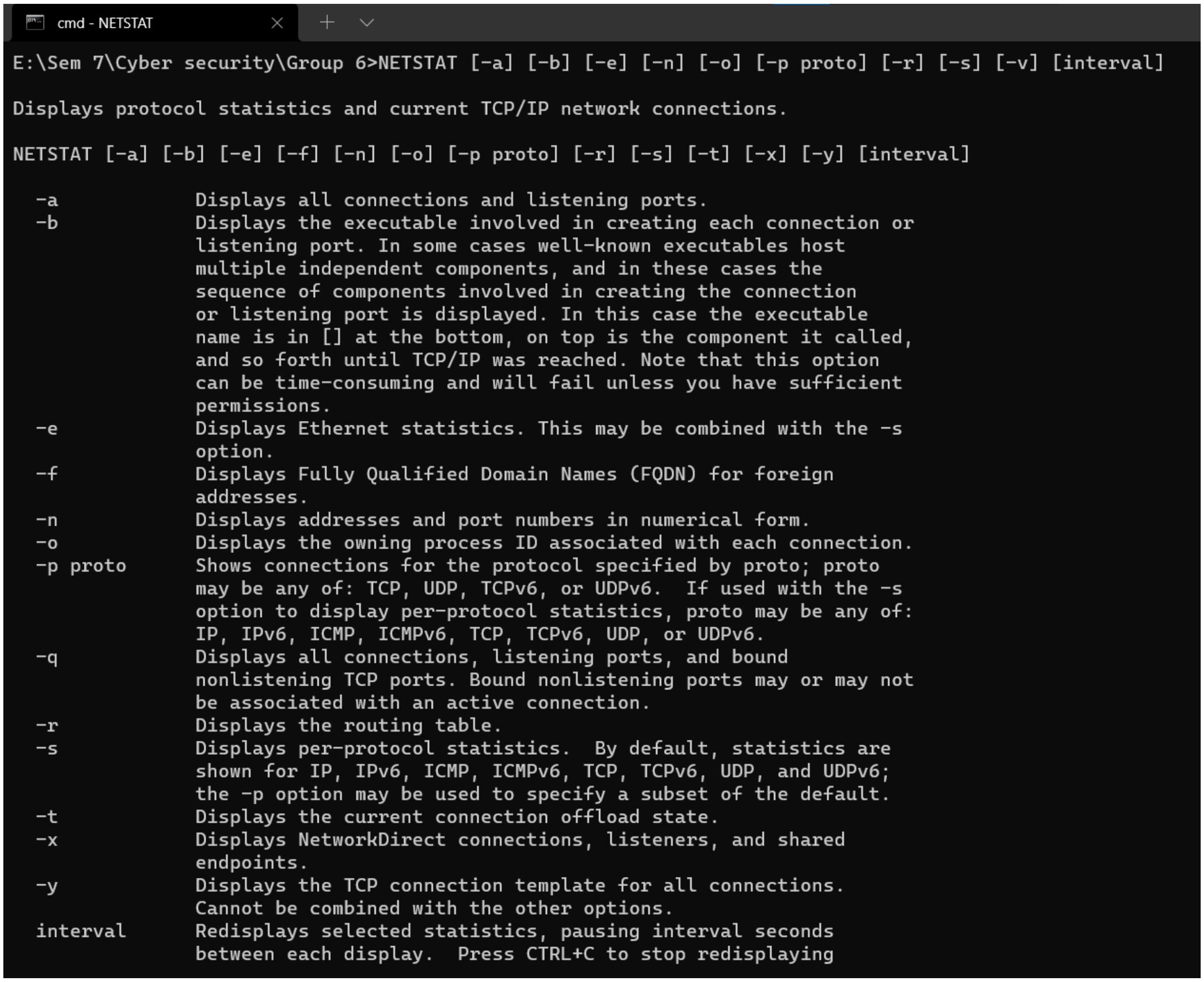
Stands for: Network statistics

Function: Print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships

Syntax: netstat [address_family_options] [--tcp|-t] [--udp|-u] [--raw|-w] [--listening|-l] [--all|-a] [--numeric|-n] [--numeric-hosts][--numeric-ports][--numeric-ports] [--symbolic|-N] [--extend|-e[--extend|-e]] [--timers|-o] [--program|-p] [--verbose|-v] [--continuous|-c] [delay]

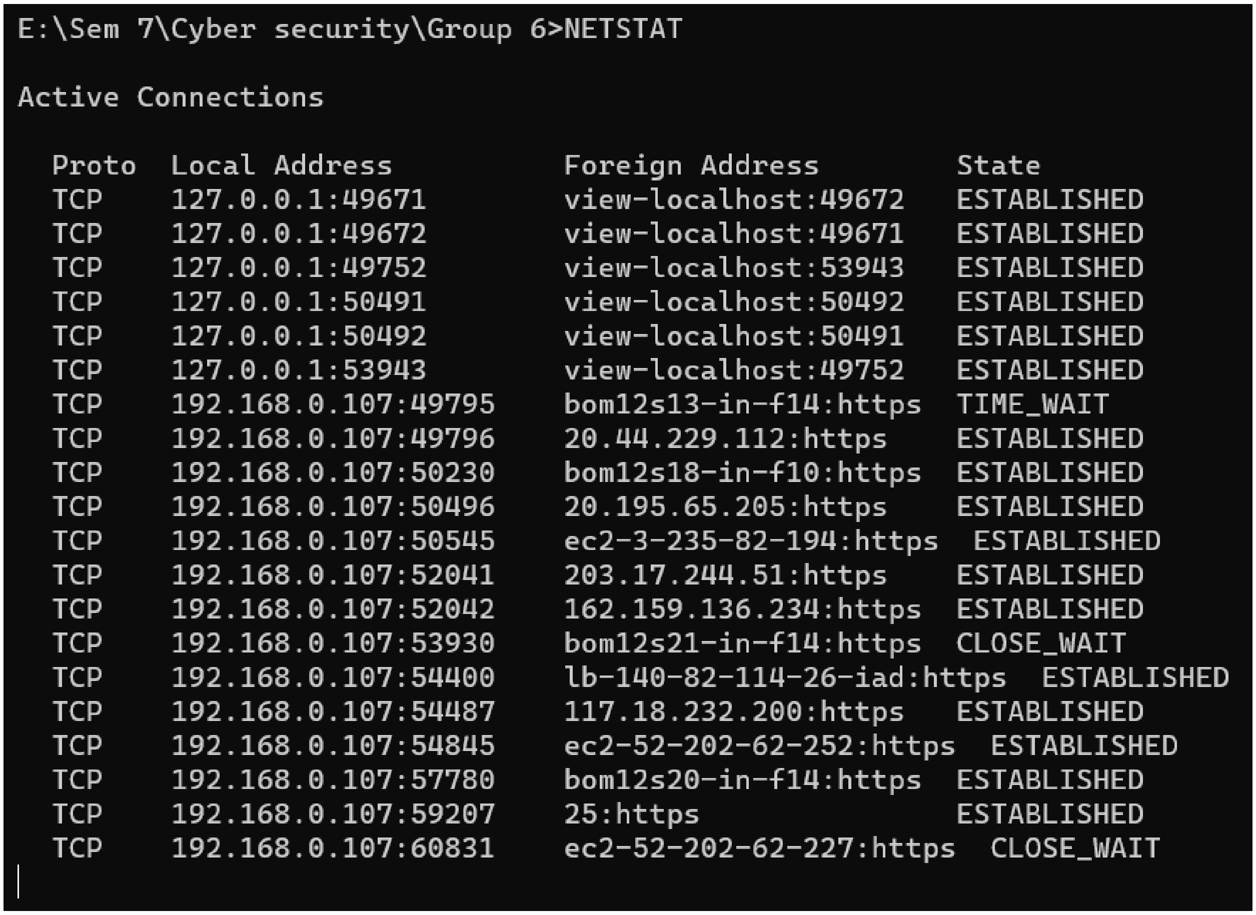
The network statistics (netstat) command is a networking tool used for troubleshooting and configuration, that can also serve as a monitoring tool for connections over the network. Both incoming and outgoing connections, routing tables, port listening, and usage statistics are common uses for this command.

Command -h



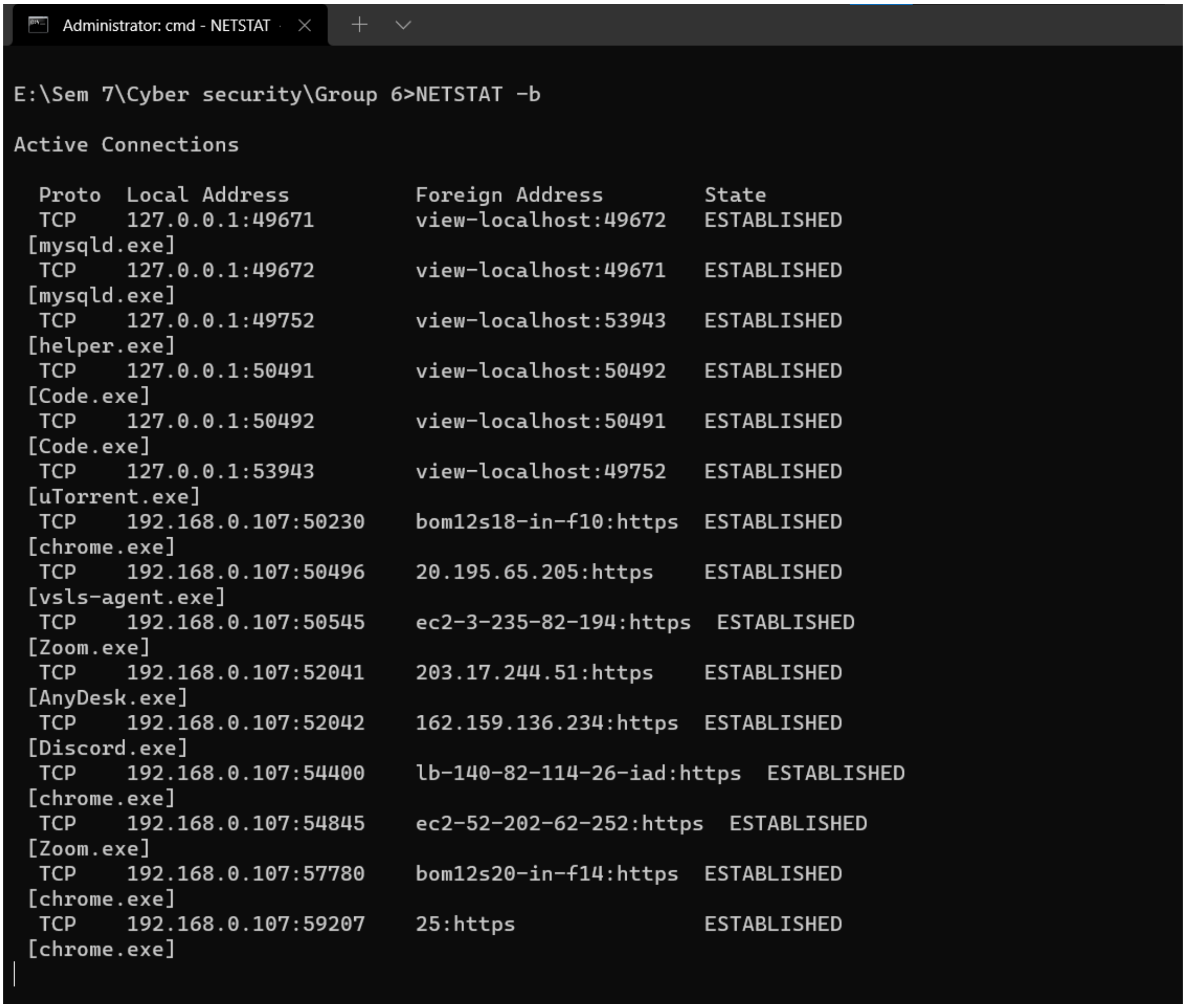
```
E:\Sem 7\Cyber security\Group 6>NETSTAT [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

  -a            Displays all connections and listening ports.
  -b            Displays the executable involved in creating each connection or
                listening port. In some cases well-known executables host
                multiple independent components, and in these cases the
                sequence of components involved in creating the connection
                or listening port is displayed. In this case the executable
                name is in [] at the bottom, on top is the component it called,
                and so forth until TCP/IP was reached. Note that this option
                can be time-consuming and will fail unless you have sufficient
                permissions.
  -e            Displays Ethernet statistics. This may be combined with the -s
                option.
  -f            Displays Fully Qualified Domain Names (FQDN) for foreign
                addresses.
  -n            Displays addresses and port numbers in numerical form.
  -o            Displays the owning process ID associated with each connection.
  -p proto      Shows connections for the protocol specified by proto; proto
                may be any of: TCP, UDP, TCPv6, or UDPv6.  If used with the -s
                option to display per-protocol statistics, proto may be any of:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
  -q            Displays all connections, listening ports, and bound
                nonlistening TCP ports. Bound nonlistening ports may or may not
                be associated with an active connection.
  -r            Displays the routing table.
  -s            Displays per-protocol statistics.  By default, statistics are
                shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
                the -p option may be used to specify a subset of the default.
  -t            Displays the current connection offload state.
  -x            Displays NetworkDirect connections, listeners, and shared
                endpoints.
  -y            Displays the TCP connection template for all connections.
                Cannot be combined with the other options.
  interval      Redisplays selected statistics, pausing interval seconds
                between each display.  Press CTRL+C to stop redisplaying
```

NETSTAT



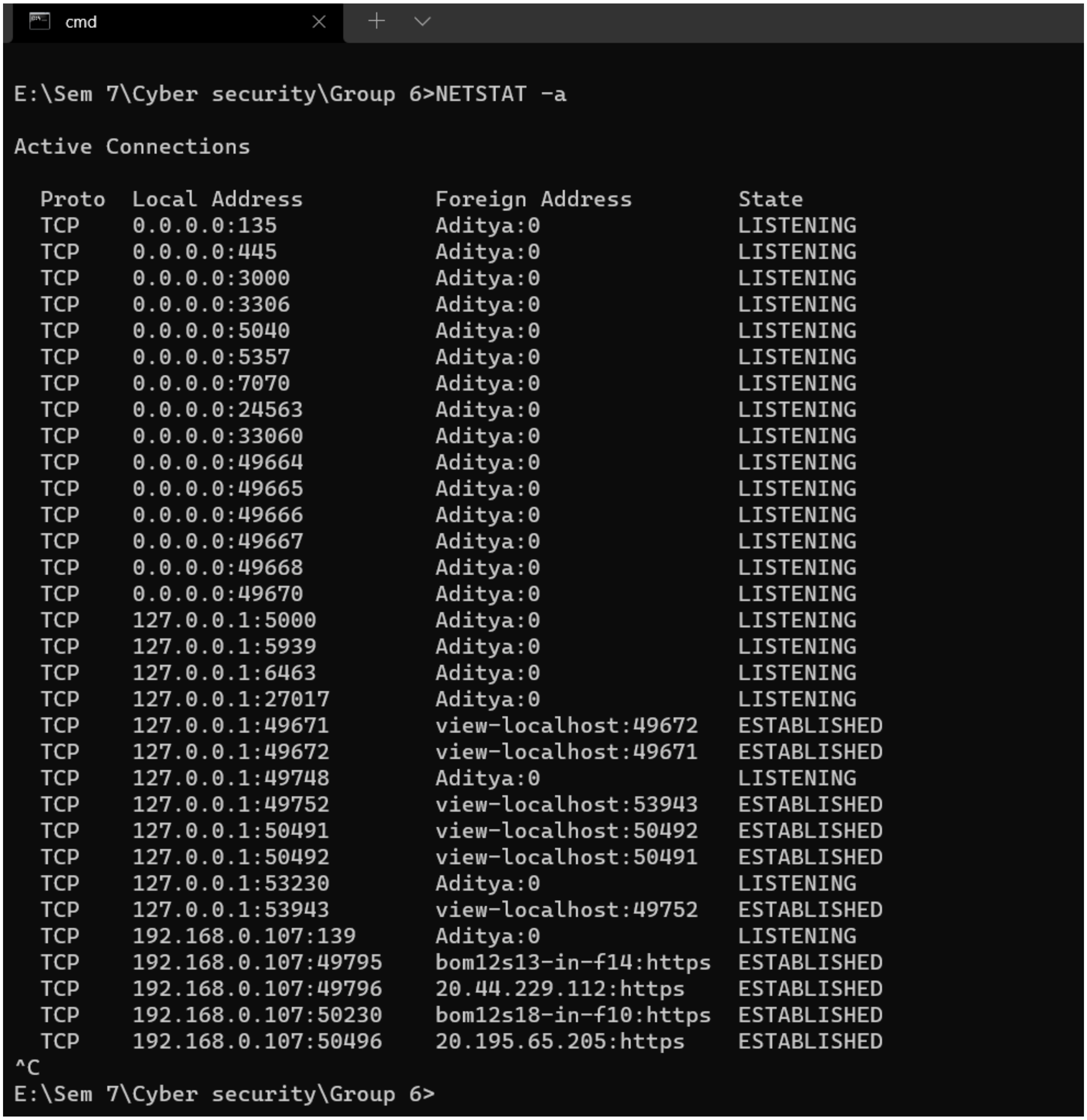
```
E:\Sem 7\Cyber security\Group 6>NETSTAT

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49671        view-localhost:49672   ESTABLISHED
  TCP    127.0.0.1:49672        view-localhost:49671   ESTABLISHED
  TCP    127.0.0.1:49752        view-localhost:53943   ESTABLISHED
  TCP    127.0.0.1:50491        view-localhost:50492   ESTABLISHED
  TCP    127.0.0.1:50492        view-localhost:50491   ESTABLISHED
  TCP    127.0.0.1:53943        view-localhost:49752   ESTABLISHED
  TCP    192.168.0.107:49795    bom12s13-in-f14:https  TIME_WAIT
  TCP    192.168.0.107:49796    20.44.229.112:https    ESTABLISHED
  TCP    192.168.0.107:50230    bom12s18-in-f10:https  ESTABLISHED
  TCP    192.168.0.107:50496    20.195.65.205:https    ESTABLISHED
  TCP    192.168.0.107:50545    ec2-3-235-82-194:https  ESTABLISHED
  TCP    192.168.0.107:52041    203.17.244.51:https    ESTABLISHED
  TCP    192.168.0.107:52042    162.159.136.234:https  ESTABLISHED
  TCP    192.168.0.107:53930    bom12s21-in-f14:https  CLOSE_WAIT
  TCP    192.168.0.107:54400    lb-140-82-114-26-iad:https  ESTABLISHED
  TCP    192.168.0.107:54487    117.18.232.200:https   ESTABLISHED
  TCP    192.168.0.107:54845    ec2-52-202-62-252:https  ESTABLISHED
  TCP    192.168.0.107:57780    bom12s20-in-f14:https  ESTABLISHED
  TCP    192.168.0.107:59207    25:https               ESTABLISHED
  TCP    192.168.0.107:60831    ec2-52-202-62-227:https  CLOSE_WAIT
```

NETSTAT -b



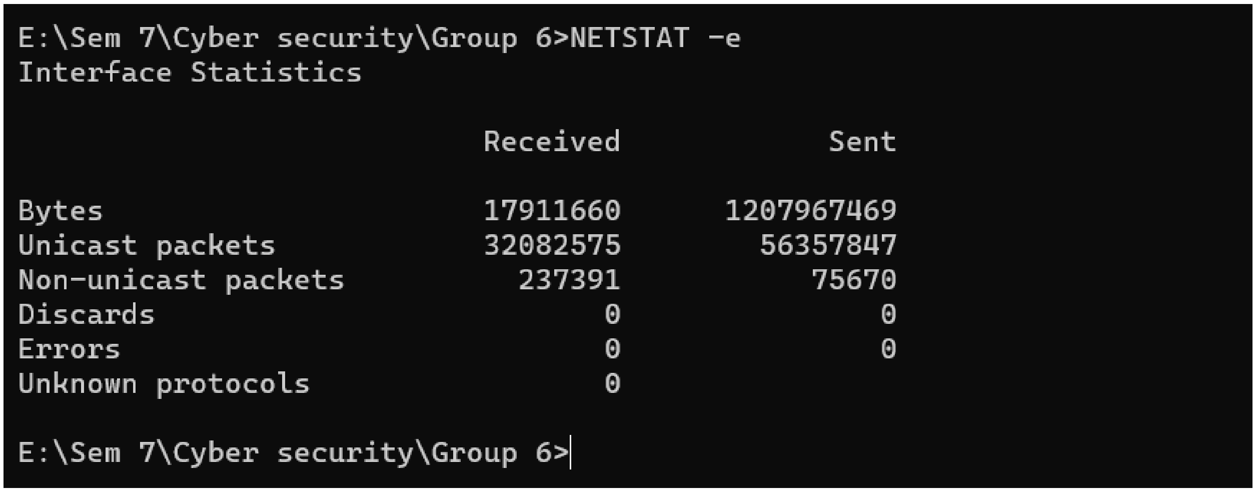
```
E:\Sem 7\Cyber security\Group 6>NETSTAT -b

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49671        view-localhost:49672   ESTABLISHED
 [mysqld.exe]
  TCP    127.0.0.1:49672        view-localhost:49671   ESTABLISHED
 [mysqld.exe]
  TCP    127.0.0.1:49752        view-localhost:53943   ESTABLISHED
 [helper.exe]
  TCP    127.0.0.1:50491        view-localhost:50492   ESTABLISHED
 [Code.exe]
  TCP    127.0.0.1:50492        view-localhost:50491   ESTABLISHED
 [Code.exe]
  TCP    127.0.0.1:53943        view-localhost:49752   ESTABLISHED
 [uTorrent.exe]
  TCP    192.168.0.107:50230    bom12s18-in-f10:https  ESTABLISHED
 [chrome.exe]
  TCP    192.168.0.107:50496    20.195.65.205:https    ESTABLISHED
 [vsls-agent.exe]
  TCP    192.168.0.107:50545    ec2-3-235-82-194:https  ESTABLISHED
 [Zoom.exe]
  TCP    192.168.0.107:52041    203.17.244.51:https    ESTABLISHED
 [AnyDesk.exe]
  TCP    192.168.0.107:52042    162.159.136.234:https  ESTABLISHED
 [Discord.exe]
  TCP    192.168.0.107:54400    lb-140-82-114-26-iad:https  ESTABLISHED
 [chrome.exe]
  TCP    192.168.0.107:54845    ec2-52-202-62-252:https  ESTABLISHED
 [Zoom.exe]
  TCP    192.168.0.107:57780    bom12s20-in-f14:https  ESTABLISHED
 [chrome.exe]
  TCP    192.168.0.107:59207    25:https               ESTABLISHED
 [chrome.exe]
```

NETSTAT -a



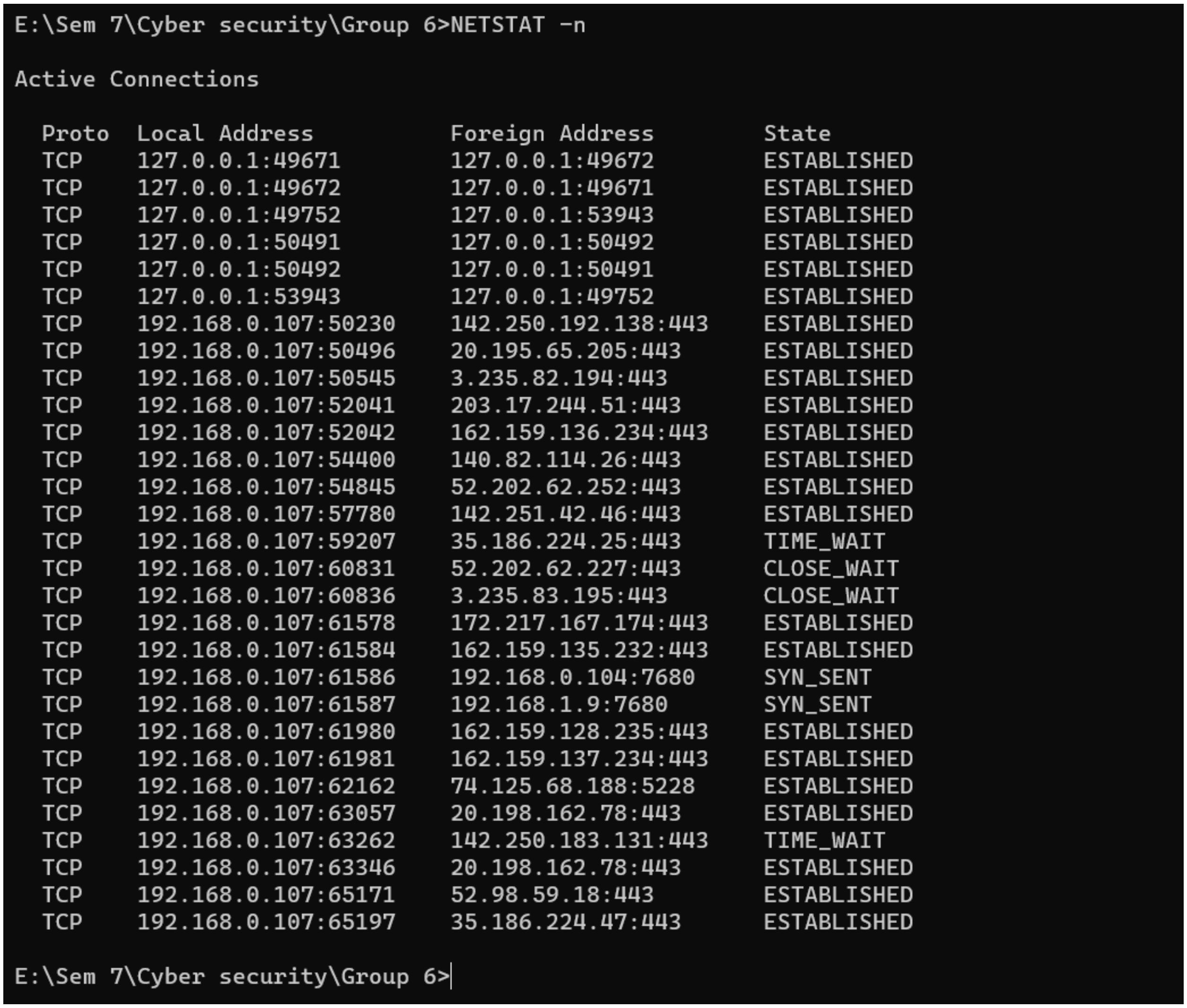
```
E:\Sem 7\Cyber security\Group 6>NETSTAT -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            Aditya:0               LISTENING
  TCP    0.0.0.0:445            Aditya:0               LISTENING
  TCP    0.0.0.0:3000           Aditya:0               LISTENING
  TCP    0.0.0.0:3306           Aditya:0               LISTENING
  TCP    0.0.0.0:5040           Aditya:0               LISTENING
  TCP    0.0.0.0:5357           Aditya:0               LISTENING
  TCP    0.0.0.0:7070           Aditya:0               LISTENING
  TCP    0.0.0.0:24563          Aditya:0               LISTENING
  TCP    0.0.0.0:33060          Aditya:0               LISTENING
  TCP    0.0.0.0:49664          Aditya:0               LISTENING
  TCP    0.0.0.0:49665          Aditya:0               LISTENING
  TCP    0.0.0.0:49666          Aditya:0               LISTENING
  TCP    0.0.0.0:49667          Aditya:0               LISTENING
  TCP    0.0.0.0:49668          Aditya:0               LISTENING
  TCP    0.0.0.0:49670          Aditya:0               LISTENING
  TCP    127.0.0.1:5000         Aditya:0               LISTENING
  TCP    127.0.0.1:5939         Aditya:0               LISTENING
  TCP    127.0.0.1:6463         Aditya:0               LISTENING
  TCP    127.0.0.1:27017        Aditya:0               LISTENING
  TCP    127.0.0.1:49671        view-localhost:49672   ESTABLISHED
  TCP    127.0.0.1:49672        view-localhost:49671   ESTABLISHED
  TCP    127.0.0.1:49748        Aditya:0               LISTENING
  TCP    127.0.0.1:49752        view-localhost:53943   ESTABLISHED
  TCP    127.0.0.1:50491        view-localhost:50492   ESTABLISHED
  TCP    127.0.0.1:50492        view-localhost:50491   ESTABLISHED
  TCP    127.0.0.1:53230        Aditya:0               LISTENING
  TCP    127.0.0.1:53943        view-localhost:49752   ESTABLISHED
  TCP    192.168.0.107:139      Aditya:0               LISTENING
  TCP    192.168.0.107:49795    bom12s13-in-f14:https  ESTABLISHED
  TCP    192.168.0.107:49796    20.44.229.112:https    ESTABLISHED
  TCP    192.168.0.107:50230    bom12s18-in-f10:https  ESTABLISHED
  TCP    192.168.0.107:50496    20.195.65.205:https    ESTABLISHED
^C
E:\Sem 7\Cyber security\Group 6>
```

NETSTAT -e



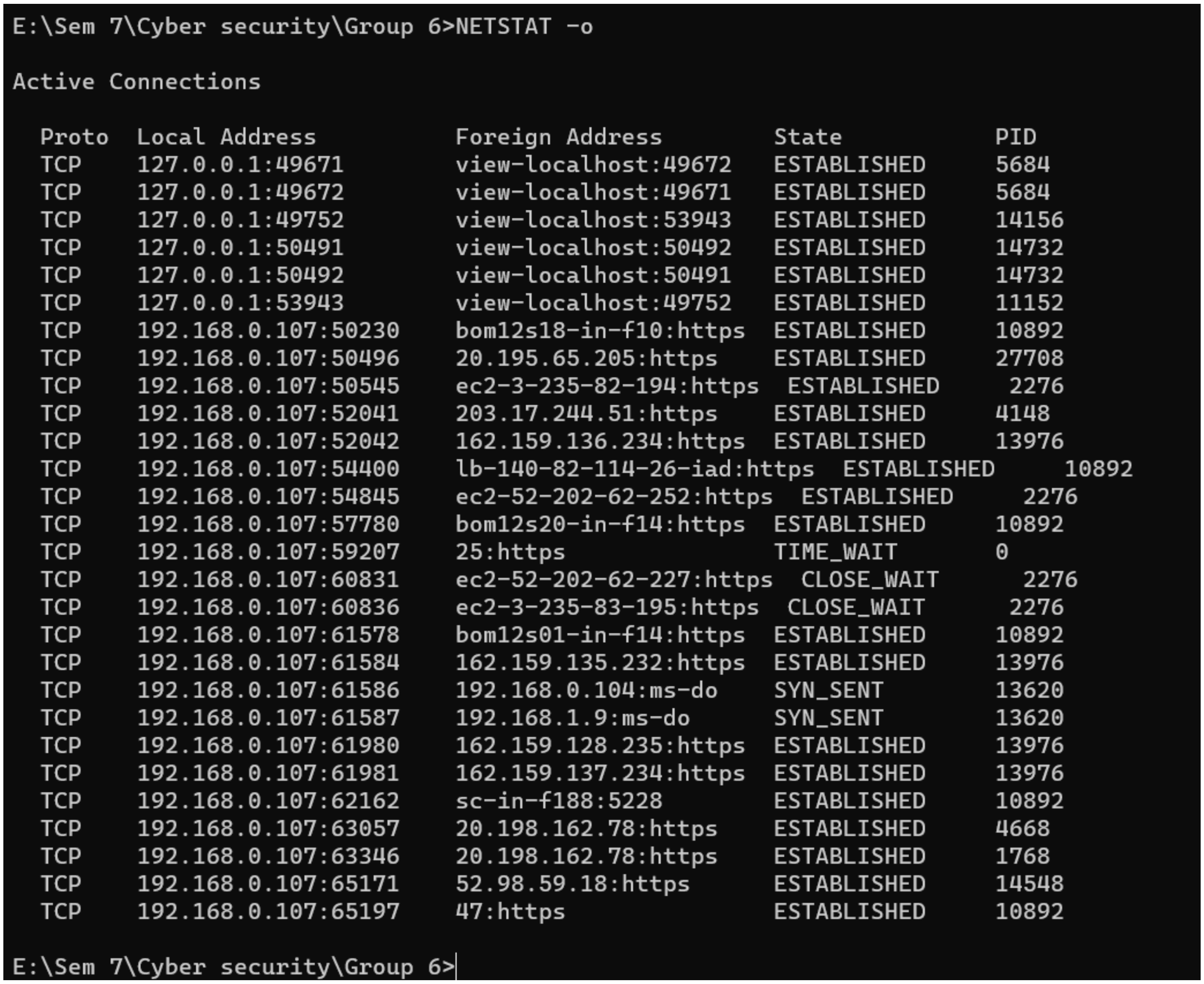
```
E:\Sem 7\Cyber security\Group 6>NETSTAT -e
Interface Statistics

                           Received            Sent

Bytes                      17911660      1207967469
Unicast packets            32082575        56357847
Non-unicast packets          237391           75670
Discards                          0               0
Errors                            0               0
Unknown protocols                 0

E:\Sem 7\Cyber security\Group 6>
```

NETSTAT -n



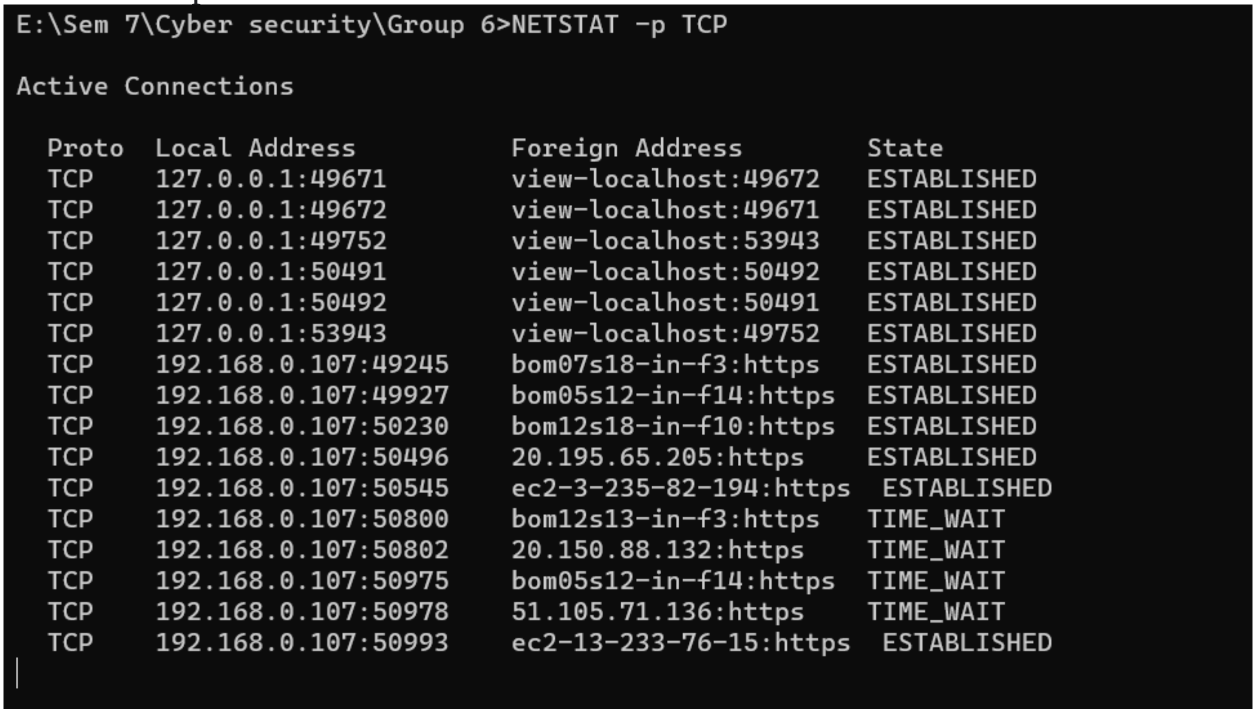
```
E:\Sem 7\Cyber security\Group 6>NETSTAT -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49671        127.0.0.1:49672        ESTABLISHED
  TCP    127.0.0.1:49672        127.0.0.1:49671        ESTABLISHED
  TCP    127.0.0.1:49752        127.0.0.1:53943        ESTABLISHED
  TCP    127.0.0.1:50491        127.0.0.1:50492        ESTABLISHED
  TCP    127.0.0.1:50492        127.0.0.1:50491        ESTABLISHED
  TCP    127.0.0.1:53943        127.0.0.1:49752        ESTABLISHED
  TCP    192.168.0.107:50230    142.250.192.138:443    ESTABLISHED
  TCP    192.168.0.107:50496    20.195.65.205:443      ESTABLISHED
  TCP    192.168.0.107:50545    3.235.82.194:443       ESTABLISHED
  TCP    192.168.0.107:52041    203.17.244.51:443      ESTABLISHED
  TCP    192.168.0.107:52042    162.159.136.234:443    ESTABLISHED
  TCP    192.168.0.107:54400    140.82.114.26:443      ESTABLISHED
  TCP    192.168.0.107:54845    52.202.62.252:443      ESTABLISHED
  TCP    192.168.0.107:57780    142.251.42.46:443      ESTABLISHED
  TCP    192.168.0.107:59207    35.186.224.25:443      TIME_WAIT
  TCP    192.168.0.107:60831    52.202.62.227:443      CLOSE_WAIT
  TCP    192.168.0.107:60836    3.235.83.195:443       CLOSE_WAIT
  TCP    192.168.0.107:61578    172.217.167.174:443    ESTABLISHED
  TCP    192.168.0.107:61584    162.159.135.232:443    ESTABLISHED
  TCP    192.168.0.107:61586    192.168.0.104:7680     SYN_SENT
  TCP    192.168.0.107:61587    192.168.1.9:7680       SYN_SENT
  TCP    192.168.0.107:61980    162.159.128.235:443    ESTABLISHED
  TCP    192.168.0.107:61981    162.159.137.234:443    ESTABLISHED
  TCP    192.168.0.107:62162    74.125.68.188:5228     ESTABLISHED
  TCP    192.168.0.107:63057    20.198.162.78:443      ESTABLISHED
  TCP    192.168.0.107:63262    142.250.183.131:443    TIME_WAIT
  TCP    192.168.0.107:63346    20.198.162.78:443      ESTABLISHED
  TCP    192.168.0.107:65171    52.98.59.18:443        ESTABLISHED
  TCP    192.168.0.107:65197    35.186.224.47:443      ESTABLISHED

E:\Sem 7\Cyber security\Group 6>
```

NETSTAT -o



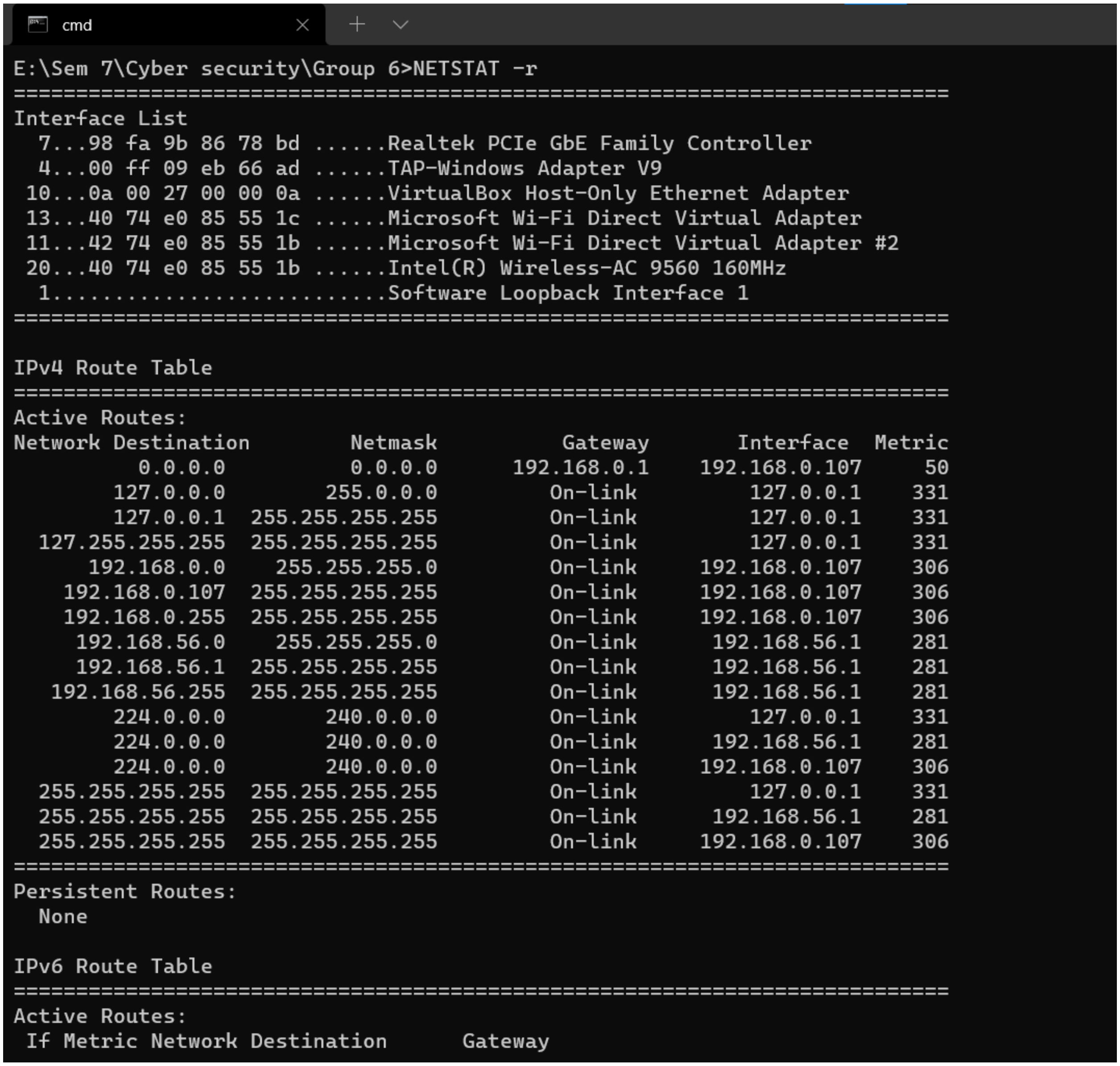
```
E:\Sem 7\Cyber security\Group 6>NETSTAT -o

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    127.0.0.1:49671        view-localhost:49672   ESTABLISHED     5684
  TCP    127.0.0.1:49672        view-localhost:49671   ESTABLISHED     5684
  TCP    127.0.0.1:49752        view-localhost:53943   ESTABLISHED     14156
  TCP    127.0.0.1:50491        view-localhost:50492   ESTABLISHED     14732
  TCP    127.0.0.1:50492        view-localhost:50491   ESTABLISHED     14732
  TCP    127.0.0.1:53943        view-localhost:49752   ESTABLISHED     11152
  TCP    192.168.0.107:50230    bom12s18-in-f10:https  ESTABLISHED     10892
  TCP    192.168.0.107:50496    20.195.65.205:https    ESTABLISHED     27708
  TCP    192.168.0.107:50545    ec2-3-235-82-194:https  ESTABLISHED     2276
  TCP    192.168.0.107:52041    203.17.244.51:https    ESTABLISHED     4148
  TCP    192.168.0.107:52042    162.159.136.234:https  ESTABLISHED     13976
  TCP    192.168.0.107:54400    lb-140-82-114-26-iad:https  ESTABLISHED     10892
  TCP    192.168.0.107:54845    ec2-52-202-62-252:https  ESTABLISHED     2276
  TCP    192.168.0.107:57780    bom12s20-in-f14:https  ESTABLISHED     10892
  TCP    192.168.0.107:59207    25:https               TIME_WAIT       0
  TCP    192.168.0.107:60831    ec2-52-202-62-227:https  CLOSE_WAIT      2276
  TCP    192.168.0.107:60836    ec2-3-235-83-195:https  CLOSE_WAIT      2276
  TCP    192.168.0.107:61578    bom12s01-in-f14:https  ESTABLISHED     10892
  TCP    192.168.0.107:61584    162.159.135.232:https  ESTABLISHED     13976
  TCP    192.168.0.107:61586    192.168.0.104:ms-do    SYN_SENT        13620
  TCP    192.168.0.107:61587    192.168.1.9:ms-do      SYN_SENT        13620
  TCP    192.168.0.107:61980    162.159.128.235:https  ESTABLISHED     13976
  TCP    192.168.0.107:61981    162.159.137.234:https  ESTABLISHED     13976
  TCP    192.168.0.107:62162    sc-in-f188:5228        ESTABLISHED     10892
  TCP    192.168.0.107:63057    20.198.162.78:https    ESTABLISHED     4668
  TCP    192.168.0.107:63346    20.198.162.78:https    ESTABLISHED     1768
  TCP    192.168.0.107:65171    52.98.59.18:https      ESTABLISHED     14548
  TCP    192.168.0.107:65197    47:https               ESTABLISHED     10892

E:\Sem 7\Cyber security\Group 6>
```

NETSTAT -p TCP

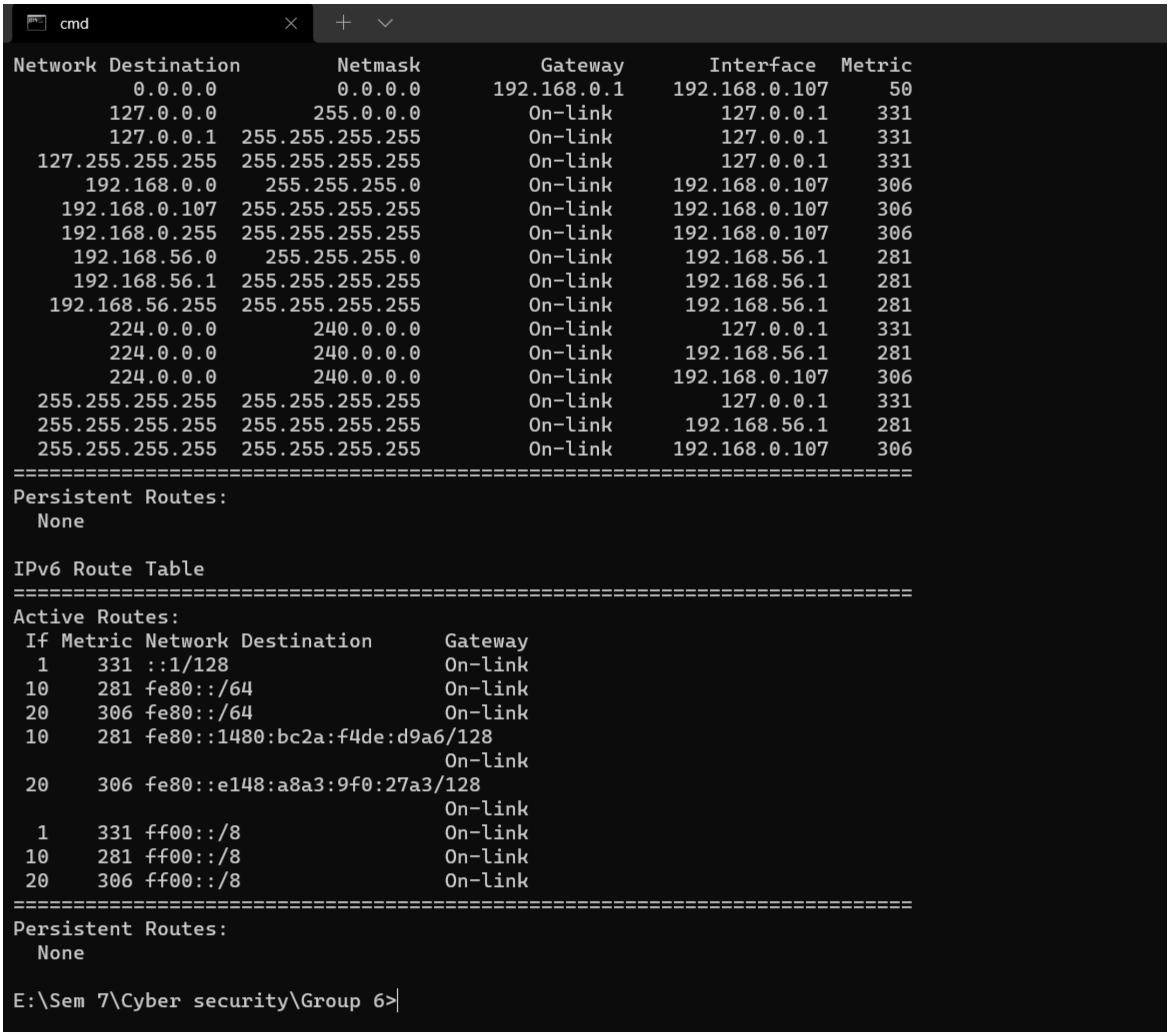


```
E:\Sem 7\Cyber security\Group 6>NETSTAT -p TCP

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49671        view-localhost:49672   ESTABLISHED
  TCP    127.0.0.1:49672        view-localhost:49671   ESTABLISHED
  TCP    127.0.0.1:49752        view-localhost:53943   ESTABLISHED
  TCP    127.0.0.1:50491        view-localhost:50492   ESTABLISHED
  TCP    127.0.0.1:50492        view-localhost:50491   ESTABLISHED
  TCP    127.0.0.1:53943        view-localhost:49752   ESTABLISHED
  TCP    192.168.0.107:49245    bom07s18-in-f3:https   ESTABLISHED
  TCP    192.168.0.107:49927    bom05s12-in-f14:https  ESTABLISHED
  TCP    192.168.0.107:50230    bom12s18-in-f10:https  ESTABLISHED
  TCP    192.168.0.107:50496    20.195.65.205:https    ESTABLISHED
  TCP    192.168.0.107:50545    ec2-3-235-82-194:https  ESTABLISHED
  TCP    192.168.0.107:50800    bom12s13-in-f3:https   TIME_WAIT
  TCP    192.168.0.107:50802    20.150.88.132:https    TIME_WAIT
  TCP    192.168.0.107:50975    bom05s12-in-f14:https  TIME_WAIT
  TCP    192.168.0.107:50978    51.105.71.136:https    TIME_WAIT
  TCP    192.168.0.107:50993    ec2-13-233-76-15:https  ESTABLISHED
```

NETSTAT -r

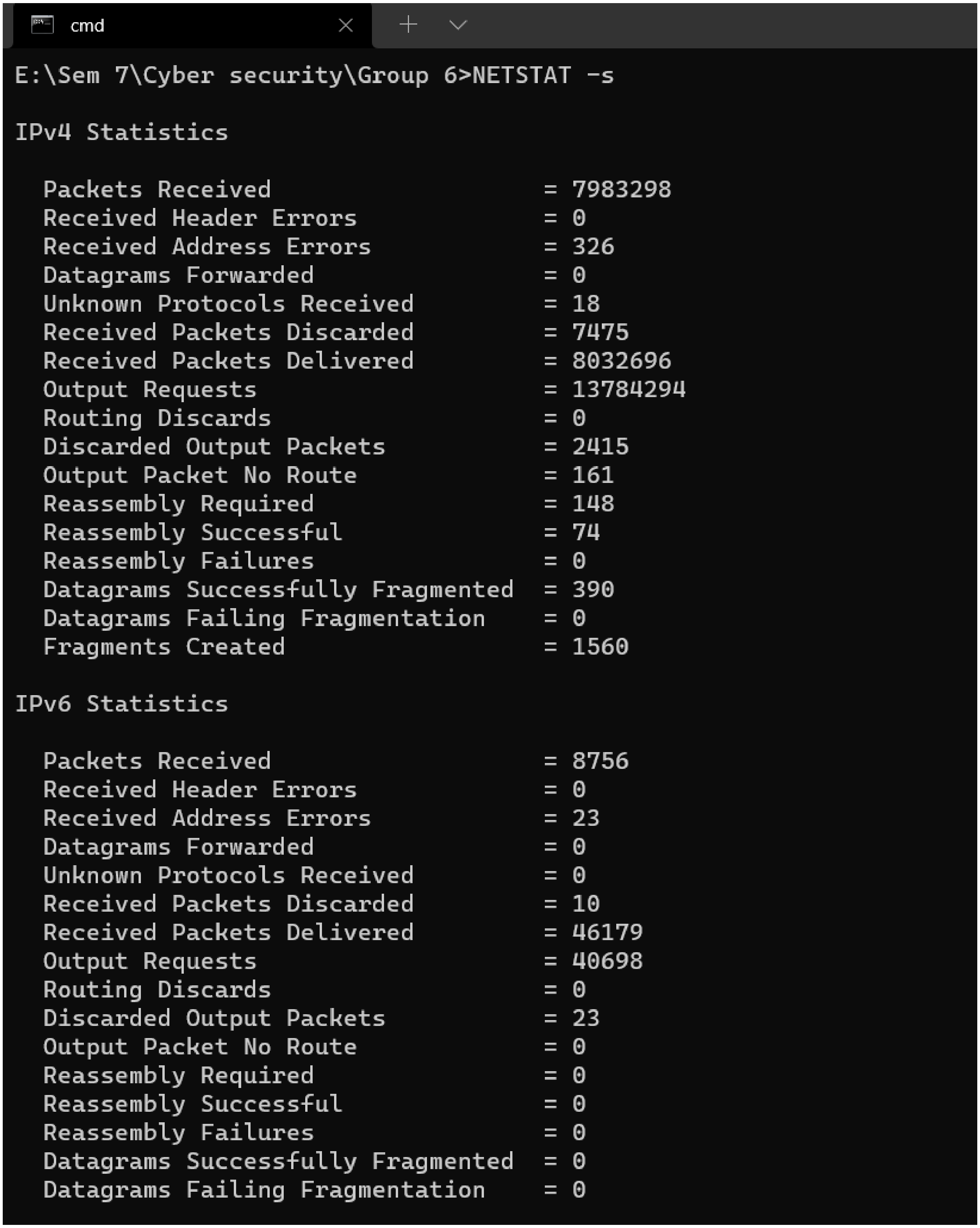


```
E:\Sem 7\Cyber security\Group 6>NETSTAT -r
===========================================================================
Interface List
  7...98 fa 9b 86 78 bd ......Realtek PCIe GbE Family Controller
  4...00 ff 09 eb 66 ad ......TAP-Windows Adapter V9
 10...0a 00 27 00 00 0a ......VirtualBox Host-Only Ethernet Adapter
 13...40 74 e0 85 55 1c ......Microsoft Wi-Fi Direct Virtual Adapter
 11...42 74 e0 85 55 1b ......Microsoft Wi-Fi Direct Virtual Adapter #2
 20...40 74 e0 85 55 1b ......Intel(R) Wireless-AC 9560 160MHz
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.0.1    192.168.0.107     50
        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
      192.168.0.0    255.255.255.0         On-link     192.168.0.107    306
    192.168.0.107  255.255.255.255         On-link     192.168.0.107    306
    192.168.0.255  255.255.255.255         On-link     192.168.0.107    306
     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     192.168.0.107    306
  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     192.168.0.107    306
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
```

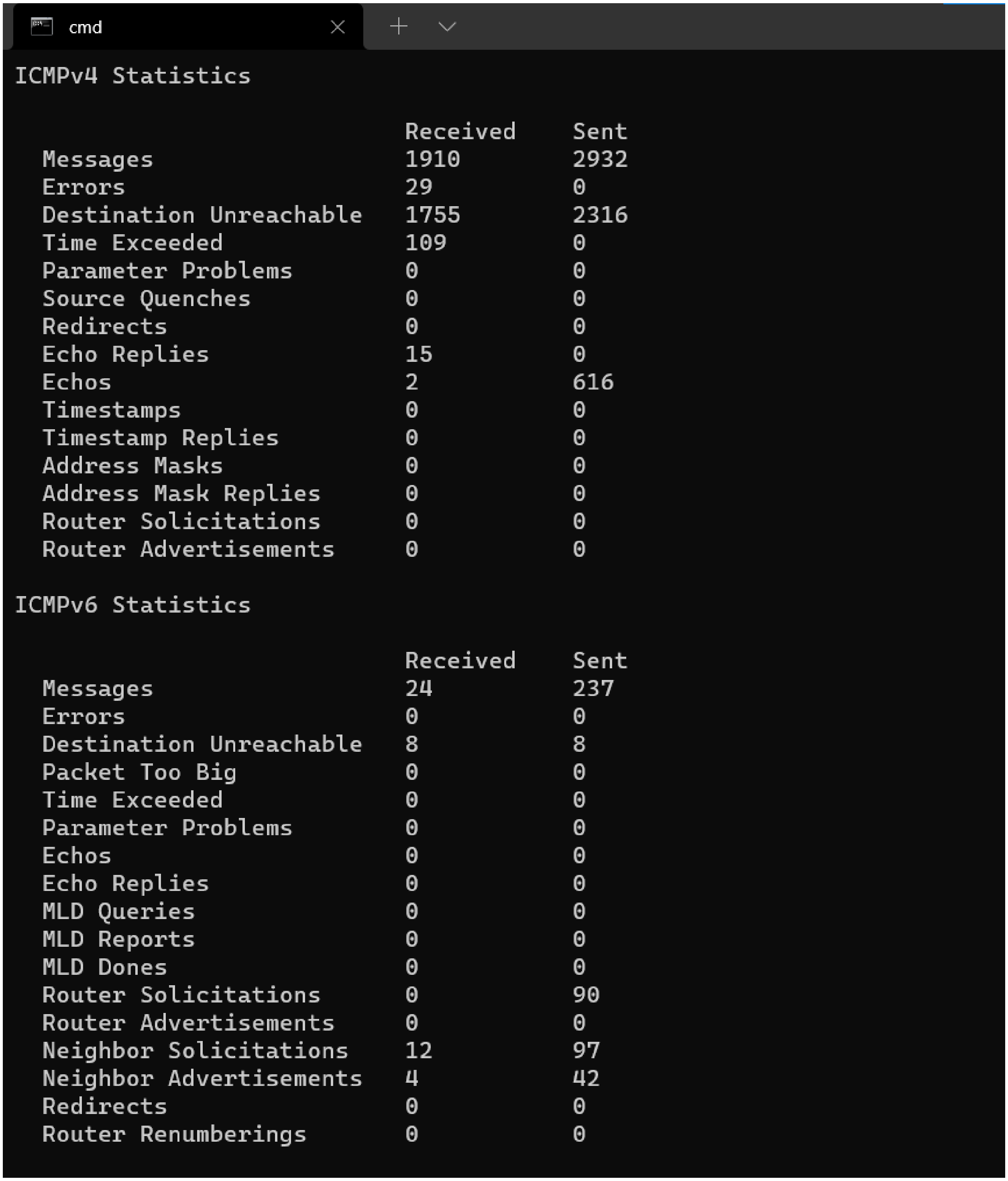


```
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.0.1    192.168.0.107     50
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.0.0    255.255.255.0         On-link     192.168.0.107    306
    192.168.0.107  255.255.255.255         On-link     192.168.0.107    306
    192.168.0.255  255.255.255.255         On-link     192.168.0.107    306
     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     192.168.0.107    306
  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     192.168.0.107    306
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
 10    281 fe80::/64                On-link
 20    306 fe80::/64                On-link
 10    281 fe80::1480:bc2a:f4de:d9a6/128
                                    On-link
 20    306 fe80::e148:a8a3:9f0:27a3/128
                                    On-link
  1    331 ff00::/8                 On-link
 10    281 ff00::/8                 On-link
 20    306 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None

E:\Sem 7\Cyber security\Group 6>
```

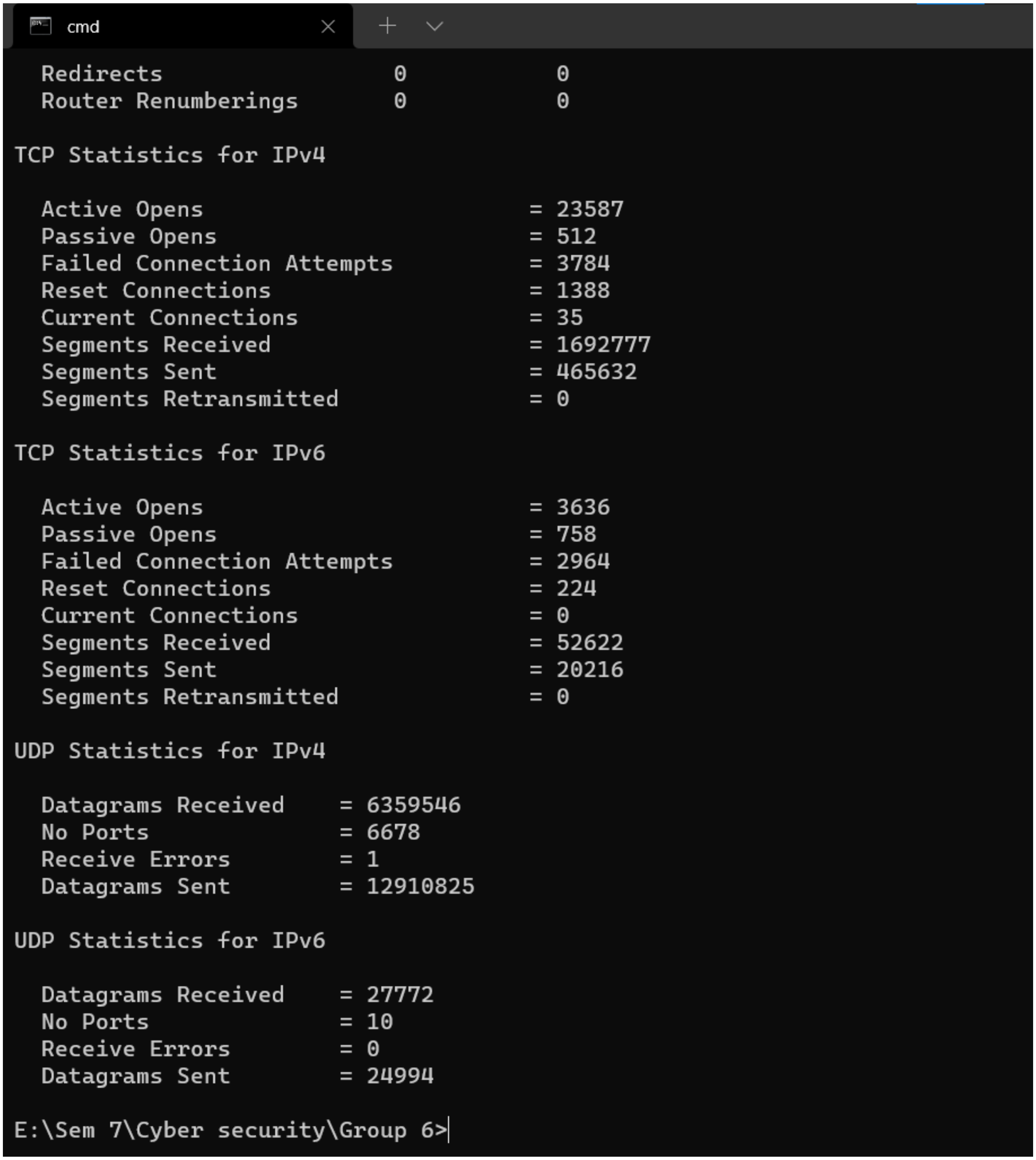
NETSTAT -s



```
E:\Sem 7\Cyber security\Group 6>NETSTAT -s

IPv4 Statistics

  Packets Received                   = 7983298
  Received Header Errors             = 0
  Received Address Errors            = 326
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 18
  Received Packets Discarded         = 7475
  Received Packets Delivered         = 8032696
  Output Requests                    = 13784294
  Routing Discards                   = 0
  Discarded Output Packets           = 2415
  Output Packet No Route             = 161
  Reassembly Required                = 148
  Reassembly Successful              = 74
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 390
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 1560

IPv6 Statistics

  Packets Received                   = 8756
  Received Header Errors             = 0
  Received Address Errors            = 23
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 10
  Received Packets Delivered         = 46179
  Output Requests                    = 40698
  Routing Discards                   = 0
  Discarded Output Packets           = 23
  Output Packet No Route             = 0
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
```

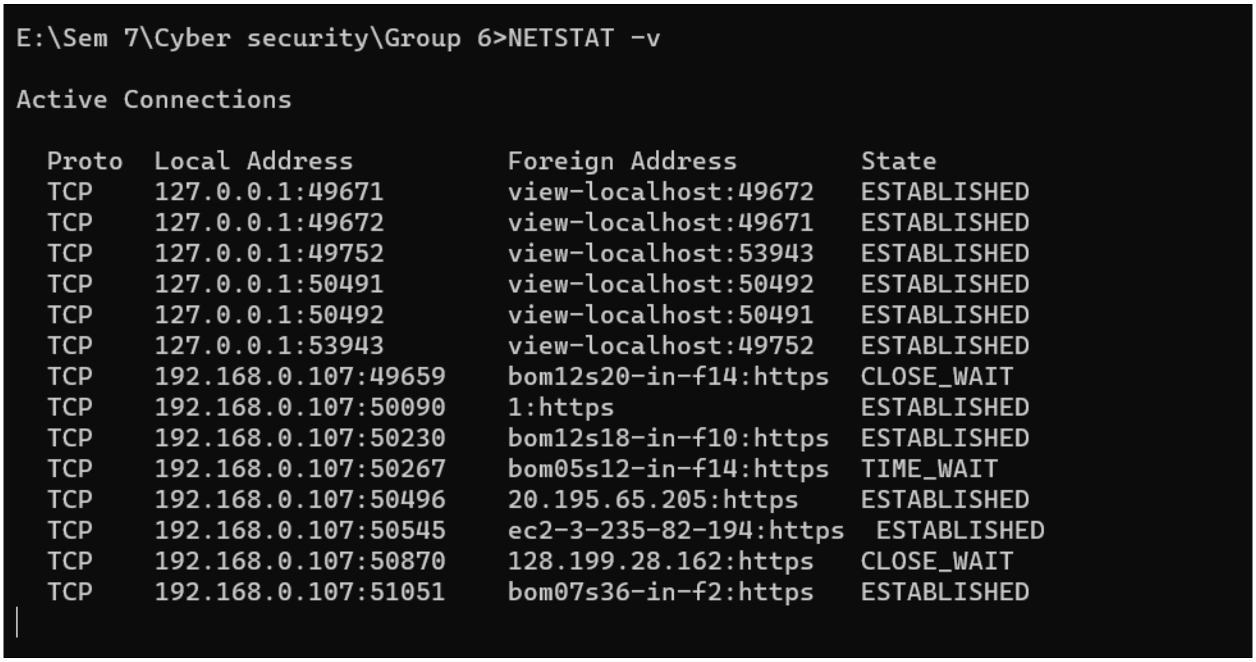


```
ICMPv4 Statistics

                            Received    Sent
  Messages                  1910        2932
  Errors                    29          0
  Destination Unreachable   1755        2316
  Time Exceeded             109         0
  Parameter Problems        0           0
  Source Quenches           0           0
  Redirects                 0           0
  Echo Replies              15          0
  Echos                     2           616
  Timestamps                0           0
  Timestamp Replies         0           0
  Address Masks             0           0
  Address Mask Replies      0           0
  Router Solicitations      0           0
  Router Advertisements     0           0

ICMPv6 Statistics

                            Received    Sent
  Messages                  24          237
  Errors                    0           0
  Destination Unreachable   8           8
  Packet Too Big            0           0
  Time Exceeded             0           0
  Parameter Problems        0           0
  Echos                     0           0
  Echo Replies              0           0
  MLD Queries               0           0
  MLD Reports               0           0
  MLD Dones                 0           0
  Router Solicitations      0           90
  Router Advertisements     0           0
  Neighbor Solicitations    12          97
  Neighbor Advertisements   4           42
  Redirects                 0           0
  Router Renumberings       0           0
```



```
  Redirects                 0           0
  Router Renumberings       0           0

TCP Statistics for IPv4

  Active Opens                        = 23587
  Passive Opens                       = 512
  Failed Connection Attempts          = 3784
  Reset Connections                   = 1388
  Current Connections                 = 35
  Segments Received                   = 1692777
  Segments Sent                       = 465632
  Segments Retransmitted              = 0

TCP Statistics for IPv6

  Active Opens                        = 3636
  Passive Opens                       = 758
  Failed Connection Attempts          = 2964
  Reset Connections                   = 224
  Current Connections                 = 0
  Segments Received                   = 52622
  Segments Sent                       = 20216
  Segments Retransmitted              = 0

UDP Statistics for IPv4

  Datagrams Received    = 6359546
  No Ports              = 6678
  Receive Errors        = 1
  Datagrams Sent        = 12910825

UDP Statistics for IPv6

  Datagrams Received    = 27772
  No Ports              = 10
  Receive Errors        = 0
  Datagrams Sent        = 24994

E:\Sem 7\Cyber security\Group 6>
```

NETSTAT -v

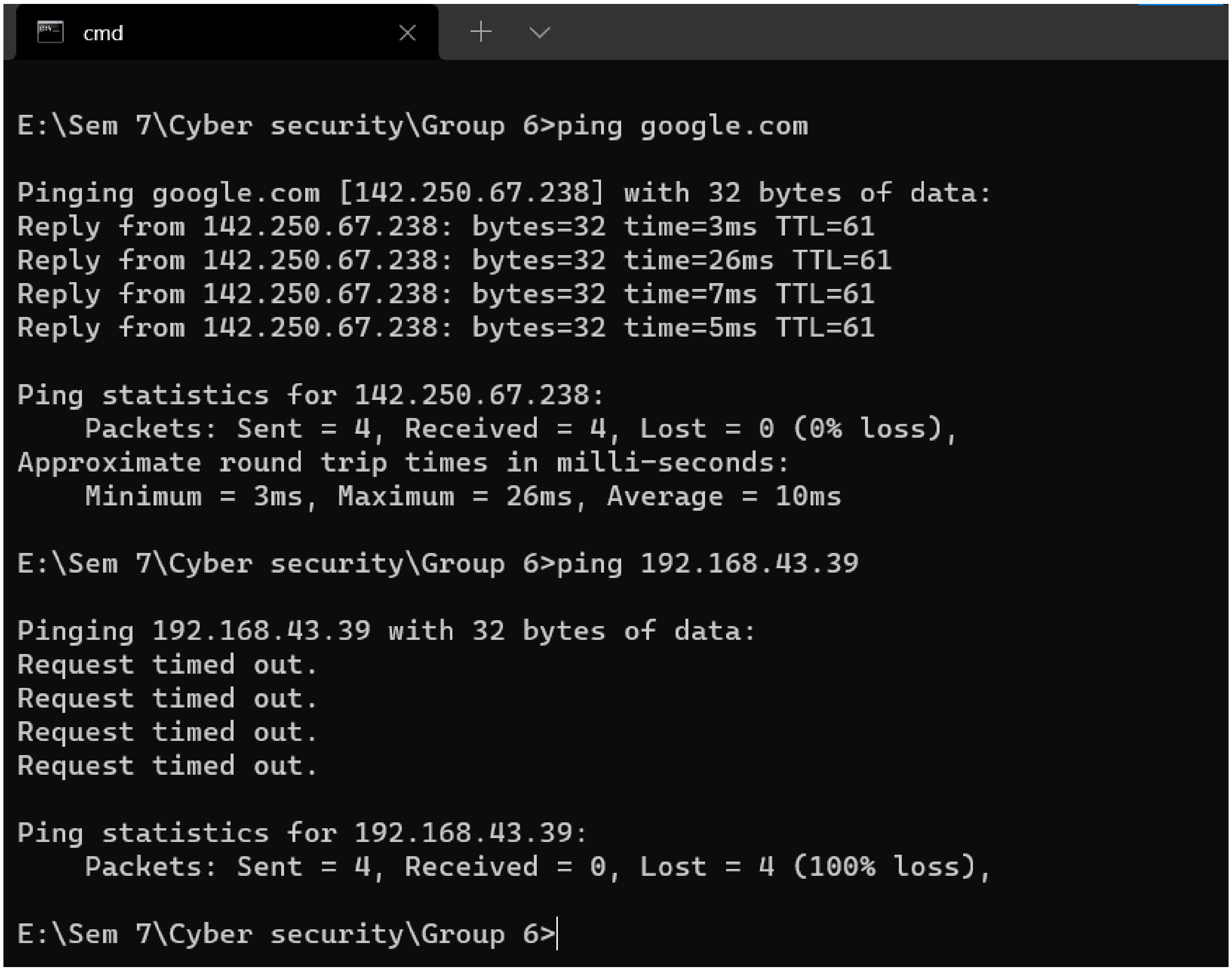


```
E:\Sem 7\Cyber security\Group 6>NETSTAT -v

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49671        view-localhost:49672   ESTABLISHED
  TCP    127.0.0.1:49672        view-localhost:49671   ESTABLISHED
  TCP    127.0.0.1:49752        view-localhost:53943   ESTABLISHED
  TCP    127.0.0.1:50491        view-localhost:50492   ESTABLISHED
  TCP    127.0.0.1:50492        view-localhost:50491   ESTABLISHED
  TCP    127.0.0.1:53943        view-localhost:49752   ESTABLISHED
  TCP    192.168.0.107:49659    bom12s20-in-f14:https  CLOSE_WAIT
  TCP    192.168.0.107:50090    1:https                ESTABLISHED
  TCP    192.168.0.107:50230    bom12s18-in-f10:https  ESTABLISHED
  TCP    192.168.0.107:50267    bom05s12-in-f14:https  TIME_WAIT
  TCP    192.168.0.107:50496    20.195.65.205:https    ESTABLISHED
  TCP    192.168.0.107:50545    ec2-3-235-82-194:https  ESTABLISHED
  TCP    192.168.0.107:50870    128.199.28.162:https   CLOSE_WAIT
  TCP    192.168.0.107:51051    bom07s36-in-f2:https   ESTABLISHED
```

Ping

The Ping tool is used to test whether a particular host is reachable across an IP network. A Ping measures the time it takes for packets to be sent from the local host to a destination computer and back. The Ping tool measures and records the round-trip time of the packet and any losses along the way.

The full form of PING is the Packet InterNet Groper. It is a computer network management system software or utility software used to test the network communication between the two devices.

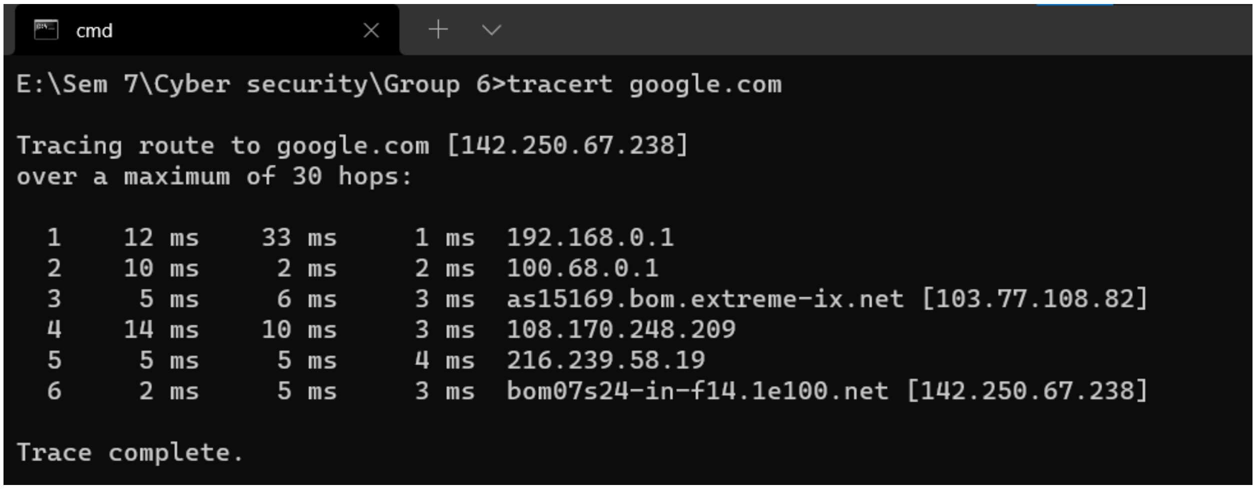


```
E:\Sem 7\Cyber security\Group 6>ping google.com

Pinging google.com [142.250.67.238] with 32 bytes of data:
Reply from 142.250.67.238: bytes=32 time=3ms TTL=61
Reply from 142.250.67.238: bytes=32 time=26ms TTL=61
Reply from 142.250.67.238: bytes=32 time=7ms TTL=61
Reply from 142.250.67.238: bytes=32 time=5ms TTL=61

Ping statistics for 142.250.67.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 26ms, Average = 10ms

E:\Sem 7\Cyber security\Group 6>ping 192.168.43.39

Pinging 192.168.43.39 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.43.39:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

E:\Sem 7\Cyber security\Group 6>
```

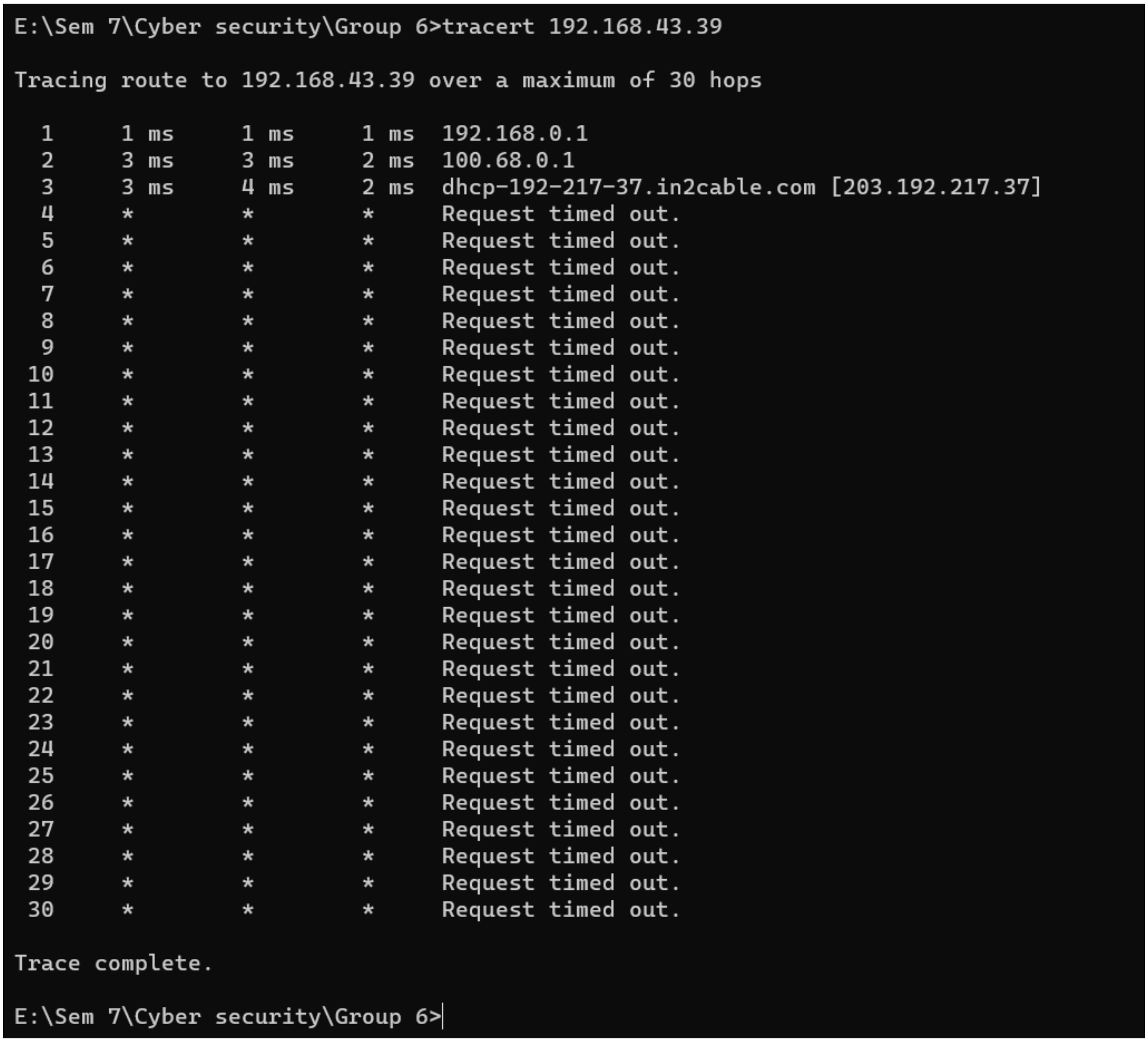
Tracert

The tracert command is one of the key diagnostic tools for TCP/IP. It displays a list of all the routers that a packet must go through to get from the computer where tracert is run to any other computer on the Internet.

The tracert command is a Command Prompt command that's used to show several details about the path that a packet takes from the computer or device you're on to whatever destination you specify. You might also sometimes see the tracert command referred to as the trace route command or traceroute command.



```
E:\Sem 7\Cyber security\Group 6>tracert google.com

Tracing route to google.com [142.250.67.238]
over a maximum of 30 hops:

  1    12 ms    33 ms     1 ms  192.168.0.1
  2    10 ms     2 ms     2 ms  100.68.0.1
  3     5 ms     6 ms     3 ms  as15169.bom.extreme-ix.net [103.77.108.82]
  4    14 ms    10 ms     3 ms  108.170.248.209
  5     5 ms     5 ms     4 ms  216.239.58.19
  6     2 ms     5 ms     3 ms  bom07s24-in-f14.1e100.net [142.250.67.238]

Trace complete.
```



```
E:\Sem 7\Cyber security\Group 6>tracert 192.168.43.39

Tracing route to 192.168.43.39 over a maximum of 30 hops

  1     1 ms     1 ms     1 ms  192.168.0.1
  2     3 ms     3 ms     2 ms  100.68.0.1
  3     3 ms     4 ms     2 ms  dhcp-192-217-37.in2cable.com [203.192.217.37]
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.

E:\Sem 7\Cyber security\Group 6>
```

Arp-a

The ARP commands to view, display, or modify the details/information in an ARP table/cache.

The ARP cache or table has the dynamic list of IP and MAC addresses of those devices to which your computer has communicated recently in a local network. The purpose of maintaining an ARP table is that when you want to communicate with another device, your device does not need to send the ARP request for the MAC address of that device.

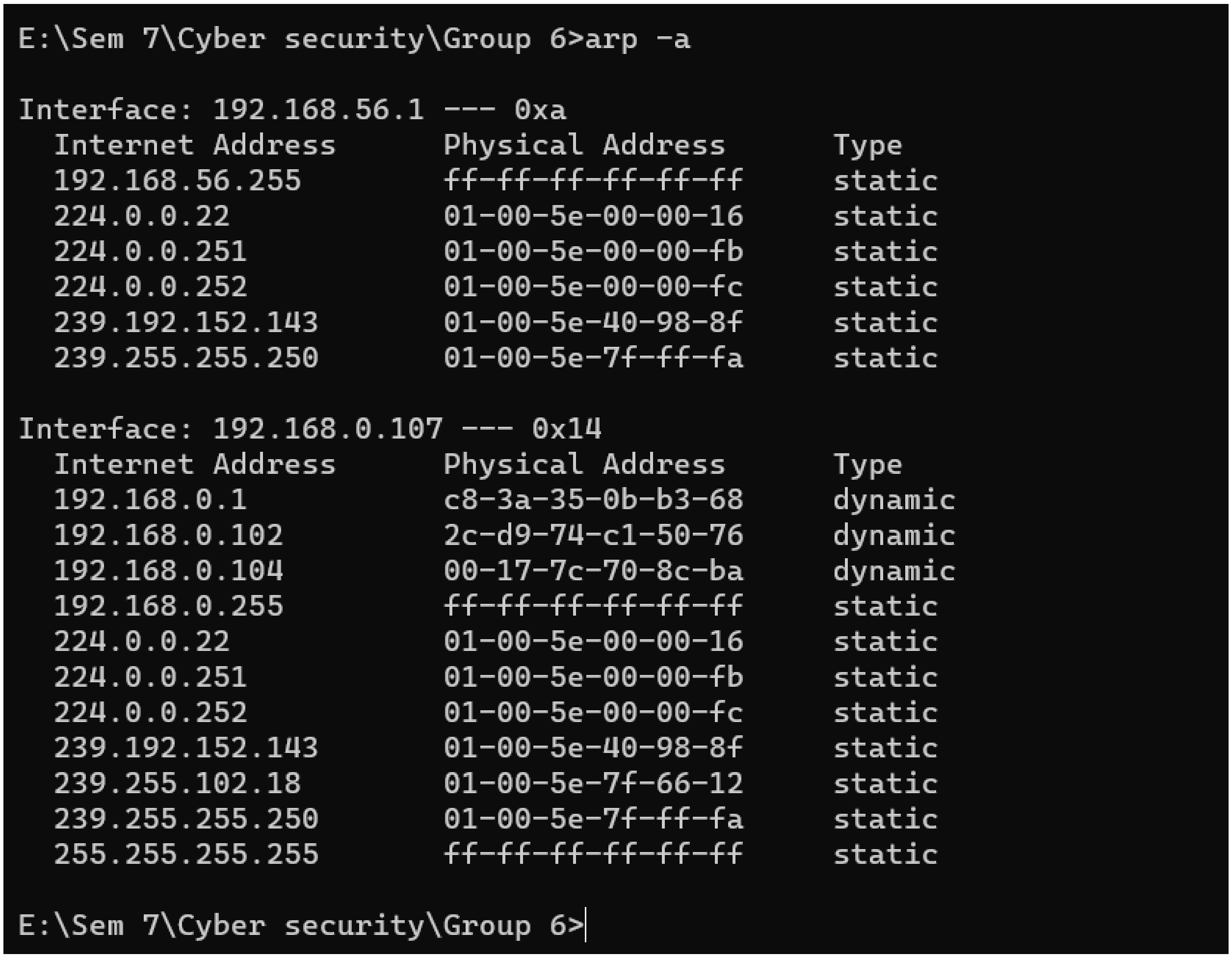
The ARP commands also helps to find out the duplicate IP address and invalid entries in an ARP table/cache.

Some ARP commands are given below:

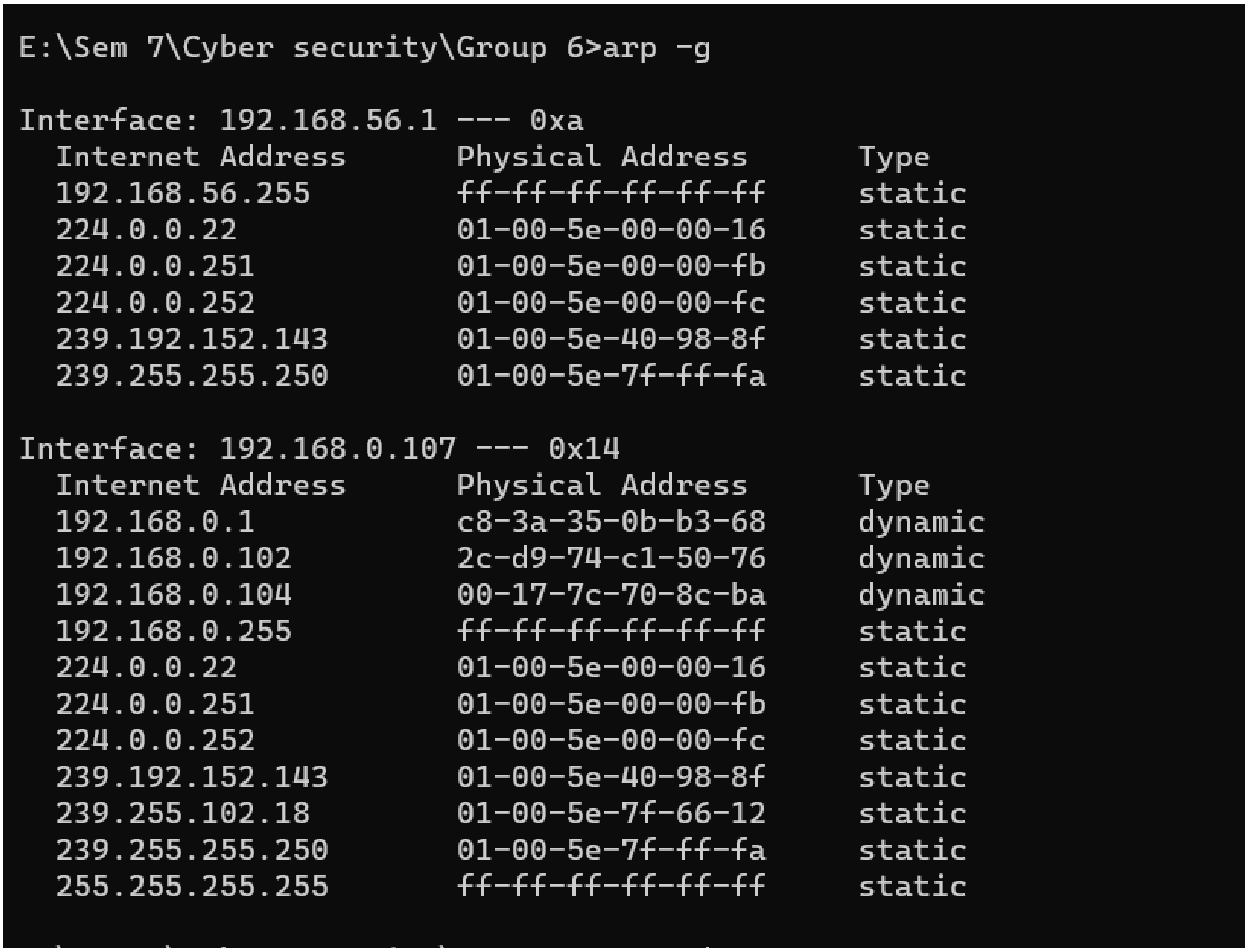
○ **arp -a:** This command is used to display the ARP table for a particular IP address. It also shows all the entries of the ARP cache or table.

○ **arp -g:** This command works the same as the **arp -a** command.

○ **arp -d:** This command is used when you want to delete an entry from the ARP table for a particular interface. To delete an entry, write **arp -d** command along with the **IP address** in a command prompt you want to delete.



```
E:\Sem 7\Cyber security\Group 6>arp -a

Interface: 192.168.56.1 --- 0xa
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.192.152.143       01-00-5e-40-98-8f     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.0.107 --- 0x14
  Internet Address      Physical Address      Type
  192.168.0.1           c8-3a-35-0b-b3-68     dynamic
  192.168.0.102         2c-d9-74-c1-50-76     dynamic
  192.168.0.104         00-17-7c-70-8c-ba     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.192.152.143       01-00-5e-40-98-8f     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

E:\Sem 7\Cyber security\Group 6>
```



```
E:\Sem 7\Cyber security\Group 6>arp -g

Interface: 192.168.56.1 --- 0xa
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.192.152.143       01-00-5e-40-98-8f     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.0.107 --- 0x14
  Internet Address      Physical Address      Type
  192.168.0.1           c8-3a-35-0b-b3-68     dynamic
  192.168.0.102         2c-d9-74-c1-50-76     dynamic
  192.168.0.104         00-17-7c-70-8c-ba     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.192.152.143       01-00-5e-40-98-8f     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

NETWOX tools 67

This tool checks if several TCP ports are open on host.This tool sends a TCP SYN to a computer. If host permits TCP, it will send back a TCP SYN-ACK (if port is open), or a TCP RST (if port is closed).

Parameter
--spoofip indicates how to generate link layer for spoofing. Values 'best', 'link' or 'raw' are common choices for --spoofip. Here is the list of accepted values:
- 'raw' means to spoof at IP4/IP6 level (it uses system IP stack). If a firewall is installed, or on some systems, this might not work.
- 'linkf' means to spoof at link level (currently, only Ethernet is supported). The 'f' means to Fill source Ethernet address. However, if source IP address is spoofed, it might be impossible to Fill it. So, linkf will not work: use linkb or linkfb instead.
- 'linkb' means to spoof at link level. The 'b' means to left a Blank source Ethernet address (0:0:0:0:0:0, do not try to Fill it).

- 'linkfb' means to spoof at link level. The 'f' means to try to Fill source Ethernet address, but if it is not possible, it is left Blank.
- 'rawlinkf' means to try 'raw', then try 'linkf'
- 'rawlinkb' means to try 'raw', then try 'linkb'
- 'rawlinkfb' means to try 'raw', then try 'linkfb'
- 'linkfraw' means to try 'linkf', then try 'raw'
- 'linkbraw' means to try 'linkb', then try 'raw'
- 'linkfbraw' means to try 'linkfb', then try 'raw'
- 'link' is an alias for 'linkfb'
- 'rawlink' is an alias for 'rawlinkfb'
- 'linkraw' is an alias for 'linkfbraw'
- 'best' is an alias for 'linkraw'. It should work in all cases.

Parameters:

parameter	*description*	*example*
-i|--ips ips	list/range of IP addresses	1.2.3.4,5.6.7.8
-p|--ports ports	list/range of port number	123,456
-s|--spoofip spoofip	IP spoof initialization type	best
-m|--min-ms uint32	min millisecond delay between packets	0
-M|--max-ms uint32	max millisecond wait for answers	0
-u|--disp-useful|+u|--no-disp-useful	only display useful info	
-n|--numtargets uint32	number of simultaneous targets	20

Internet Address tools

Every computer is connected to some other computer through a network whether internally or externally to exchange some information. This network can be small as some computers connected in your home or office, or can be large or complicated as in large University or the entire Internet.

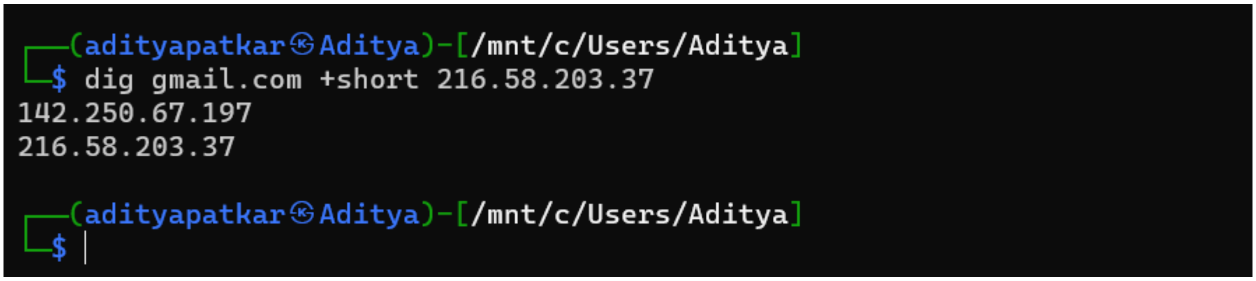
Maintaining a system's network is a task of System/Network administrator. Their task includes network configuration and troubleshooting.

a) dig :

Dig stands for (Domain Information Groper) is a network administration command-line tool for querying Domain Name System (DNS) name servers. It is useful for verifying and troubleshooting DNS problems and also to perform DNS lookups and displays the answers that are returned from the name server that were queried.
"Dig" is a robust command-line tool developed by BIND for querying DNS nameservers. It can identify IP address records, record the query route as it obtains answers from an authoritative nameserver, diagnose other DNS problems.

***Syntax* :**

dig [target][-options]



```
┌──(adityapatkar㉿Aditya)-[/mnt/c/Users/Aditya]
└─$ dig gmail.com +short 216.58.203.37
142.250.67.197
216.58.203.37

┌──(adityapatkar㉿Aditya)-[/mnt/c/Users/Aditya]
└─$ 
```

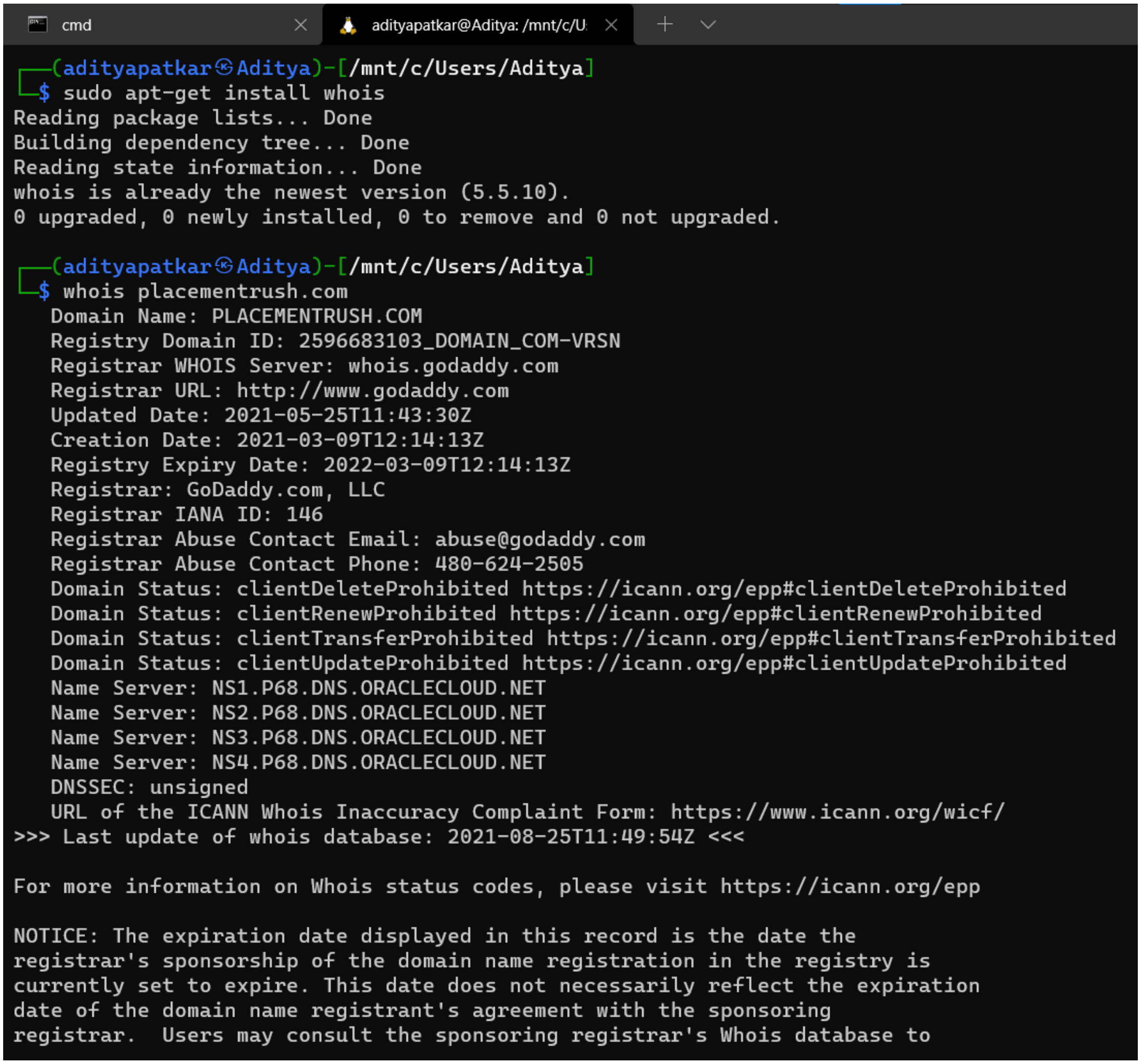
b) whois :

In Linux, the whois command line utility is a WHOIS client for communicating with the WHOIS server (or database host) which listen to requests on the well-known port number 43, which stores and delivers database content in a human-readable format.

When a domain is registered, or the contact details listed in Whois for a domain are modified, the updated information must be verified. This process is referred to as Whois Verification.

***Syntax* :**

whois [target]



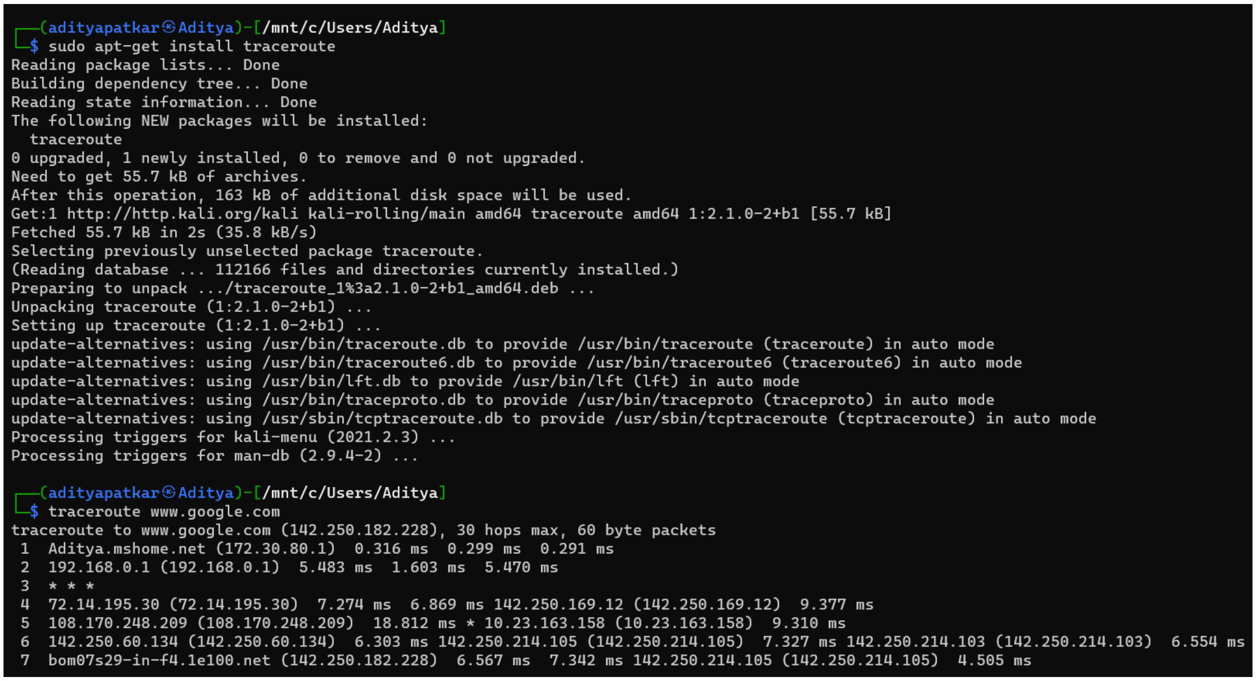
```
┌──(adityapatkar㉿Aditya)-[/mnt/c/Users/Aditya]
└─$ sudo apt-get install whois
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
whois is already the newest version (5.5.10).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

┌──(adityapatkar㉿Aditya)-[/mnt/c/Users/Aditya]
└─$ whois placementrush.com
   Domain Name: PLACEMENTRUSH.COM
   Registry Domain ID: 2596683103_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.godaddy.com
   Registrar URL: http://www.godaddy.com
   Updated Date: 2021-05-25T11:43:30Z
   Creation Date: 2021-03-09T12:14:13Z
   Registry Expiry Date: 2022-03-09T12:14:13Z
   Registrar: GoDaddy.com, LLC
   Registrar IANA ID: 146
   Registrar Abuse Contact Email: abuse@godaddy.com
   Registrar Abuse Contact Phone: 480-624-2505
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: NS1.P68.DNS.ORACLECLOUD.NET
   Name Server: NS2.P68.DNS.ORACLECLOUD.NET
   Name Server: NS3.P68.DNS.ORACLECLOUD.NET
   Name Server: NS4.P68.DNS.ORACLECLOUD.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2021-08-25T11:49:54Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
```

c) *traceroute :*

Linux traceroute command is a network troubleshooting utility that helps us determine the number of hops and packets traveling path required to reach a destination. It is used to display how the data transmitted from a local machine to a remote machine. Loading a web page is one of the common examples of the traceroute. A web page loading transfers data through a network and routers. The traceroute can display the routes, IP addresses, and hostnames of routers over a network. It can be useful for diagnosing network issues.

***Syntax* :**

traceroute [OPTION...] HOST



```
┌──(adityapatkar㉿Aditya)-[/mnt/c/Users/Aditya]
└─$ sudo apt-get install traceroute
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  traceroute
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 55.7 kB of archives.
After this operation, 163 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 traceroute amd64 1:2.1.0-2+b1 [55.7 kB]
Fetched 55.7 kB in 2s (35.8 kB/s)
Selecting previously unselected package traceroute.
(Reading database ... 112166 files and directories currently installed.)
Preparing to unpack .../traceroute_1%3a2.1.0-2+b1_amd64.deb ...
Unpacking traceroute (1:2.1.0-2+b1) ...
Setting up traceroute (1:2.1.0-2+b1) ...
update-alternatives: using /usr/bin/traceroute.db to provide /usr/bin/traceroute (traceroute) in auto mode
update-alternatives: using /usr/bin/traceroute6.db to provide /usr/bin/traceroute6 (traceroute6) in auto mode
update-alternatives: using /usr/bin/lft.db to provide /usr/bin/lft (lft) in auto mode
update-alternatives: using /usr/bin/traceproto.db to provide /usr/bin/traceproto (traceproto) in auto mode
update-alternatives: using /usr/sbin/tcptraceroute.db to provide /usr/sbin/tcptraceroute (tcptraceroute) in auto mode
Processing triggers for kali-menu (2021.2.3) ...
Processing triggers for man-db (2.9.4-2) ...

┌──(adityapatkar㉿Aditya)-[/mnt/c/Users/Aditya]
└─$ traceroute www.google.com
traceroute to www.google.com (142.250.182.228), 30 hops max, 60 byte packets
 1  Aditya.mshome.net (172.30.80.1)  0.316 ms  0.299 ms  0.291 ms
 2  192.168.0.1 (192.168.0.1)  5.483 ms  1.603 ms  5.470 ms
 3  * * *
 4  72.14.195.30 (72.14.195.30)  7.274 ms  6.869 ms 142.250.169.12 (142.250.169.12)  9.377 ms
 5  108.170.248.209 (108.170.248.209)  18.812 ms * 10.23.163.158 (10.23.163.158)  9.310 ms
 6  142.250.60.134 (142.250.60.134)  6.303 ms 142.250.214.105 (142.250.214.105)  7.327 ms 142.250.214.103 (142.250.214.103)  6.554 ms
 7  bom07s29-in-f4.1e100.net (142.250.182.228)  6.567 ms  7.342 ms 142.250.214.105 (142.250.214.105)  4.505 ms
```

Enumerate Remote Systems

Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system. Functionality could exist within remote access tools to enable this, but utilities available on the operating system could also be used such as Ping or net view using Net. Adversaries may also use local host files (ex: C:\Windows\System32\Drivers\etc\hosts or /etc/hosts) in order to discover the hostname to IP address mappings of remote systems.

Mitigations

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

Detection

System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

Normal, benign system and network events related to legitimate remote system discovery may be uncommon, depending on the environment and how they are used. Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Monitor for processes that can be used to discover remote systems, such as ping.exe and tracert.exe, especially when executed in quick succession

ID	Name	Description
S0552	AdFind	AdFind has the ability to query Active Directory for computers.
G0016	APT29	APT29 has used AdFind to enumerate remote systems.
G0022	APT3	APT3 has a tool that can detect the existence of remote systems.
G0050	APT32	APT32 has enumerated DC servers using the command net group "Domain Controllers" /domain. The group has also used the ping command
G0087	APT39	APT39 has used NBTscan and custom tools to discover remote systems.
S0534	Bazar	Bazar can enumerate remote systems using Net View.
S0570	BitPaymer	BitPaymer can use net view to discover remote systems.

S0521	BloodHound	BloodHound can enumerate and collect the properties of domain computers, including domain controllers.
G0060	BRONZE BUTLER	BRONZE BUTLER typically use ping and Net to enumerate systems.
S0335	Carbon	Carbon uses the net view command.
G0114	Chimera	Chimera has utilized various scans and queries to find domain controllers and remote services in the target environment.
S0154	Cobalt Strike	Cobalt Strike uses the native Windows Network Enumeration APIs to interrogate and discover targets in a Windows Active Directory network.
S0244	Comnie	Comnie runs the net view command
S0488	CrackMapExec	CrackMapExec can discover active IP addresses, along with the machine name, within a targeted network.
G0009	Deep Panda	Deep Panda has used ping to identify other machines of interest.
G0074	Dragonfly 2.0	Dragonfly 2.0 likely obtained a list of hosts in the victim environment.
S0091	Epic	Epic uses the net view command on the victim’s machine.
G0053	FIN5	FIN5 has used the open source tool Essential NetTools to map the network and build a list of targets.
G0037	FIN6	FIN6 used publicly available tools (including Microsoft's built-in SQL querying tool, osql.exe) to map the internal network and conduct reconnaissance against Active Directory, Structured Query Language (SQL) servers, and NetBIOS.
G0061	FIN8	FIN8 uses dsquery and other Active Directory utilities to enumerate hosts.
G0117	Fox Kitten	Fox Kitten has used Angry IP Scanner to detect remote systems.
G0093	GALLIUM	GALLIUM used a modified version of NBTscan to identify available NetBIOS name servers over the network as well as ping to identify remote systems.
G0004	Ke3chang	Ke3chang has used network scanning and enumeration tools, including Ping.
S0599	Kinsing	Kinsing has used a script to parse files like /etc/hosts and SSH known_hosts to discover remote systems.
S0236	Kwampirs	Kwampirs collects a list of available servers with the command net view
G0077	Leafminer	Leafminer used Microsoft’s Sysinternals tools to gather detailed information about remote systems.
G0045	menuPass	menuPass uses scripts to enumerate IP ranges on the victim network. menuPass has also issued the

		command net view /domain to a PlugX implant to gather information about remote systems on the network.
S0233	MURKYTOP	MURKYTOP has the capability to identify remote hosts on connected networks.
S0590	NBTscan	NBTscan can list NetBIOS computer names.
S0039	Net	Commands such as net view can be used in Net to gather information about available remote systems.
S0385	njRAT	njRAT can identify remote hosts on connected networks.
S0359	Nltest	Nltest may be used to enumerate remote domain controllers using options such as /dclist and /dsgetdc.
S0365	Olympic Destroyer	Olympic Destroyer uses Windows Management Instrumentation to enumerate all systems in the network.
G0116	Operation Wocao	Operation Wocao can use the ping command to discover remote systems.
S0165	OSInfo	OSInfo performs a connection test to discover remote systems in the network
S0097	Ping	Ping can be used to identify remote systems within a network.
S0428	PoetRAT	PoetRAT used Nmap for remote system discovery.
S0241	RATANKBA	RATANKBA runs the net view /domain and net view commands.
S0125	Remsec	Remsec can ping or traceroute a remote host.
G0106	Rocke	Rocke has looked for IP addresses in the known_hosts file on the infected system and attempted to SSH into them.[46]
G0034	Sandworm Team	Sandworm Team has used a tool to query Active Directory using LDAP, discovering information about computers listed in AD.
S0140	Shamoon	Shamoon scans the C-class subnet of the IPs on the victim's interfaces.[48]
S0063	SHOTPUT	SHOTPUT has a command to list all servers in the domain, as well as one to locate domain controllers on a domain.

G0091	Silence	Silence has used Nmap to scan the corporate network, build a network topology, and identify vulnerable hosts.
S0018	Sykipot	Sykipot may use net view /domain to display hostnames of available systems on a network.
S0586	TAINTEDSCRIBE	The TAINTEDSCRIBE command and execution module can perform target system enumeration.
G0027	Threat Group-3390	Threat Group-3390 has used the net view command.
S0266	TrickBot	TrickBot can enumerate computers and network devices.
G0010	Turla	Turla surveys a system upon check-in to discover remote systems on a local network using the net view and net view /DOMAIN commands. Turla has also used net group "Domain Computers" /domain, net group "Domain Controllers" /domain, and net group "Exchange Servers" /domain to enumerate domain computers, including the organization's DC and Exchange Server.
S0452	USBferry	USBferry can use net view to gather information about remote systems.
S0366	WannaCry	WannaCry scans its local network segment for remote systems to try to exploit and copy itself to.
G0102	Wizard Spider	Wizard Spider has used networkdll for network discovery and psfin specifically for financial and point of sale indicators. Wizard Spider has also used AdFind and nltest/dclist to enumerate domain computers, including the domain controller.
S0248	yty	yty uses the net view command for discovery.

CONCLUSION: Thus, from this experiement, we did a case study on Air India Data Breach and understood the its reason and way to prevent it, studied the Cyber Laws. We implemented commands for network discovery and information like ipconfig, ping, tracroute etc. Lastly, we studied the Enumerate Remote System.