*dGroup 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](https://timesofindia.indiatimes.com/business/india-business/air-india-hit-by-massive-data-breach-flyer-data-compromised/articleshow/82836734.cms) 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](https://www.itpro.co.uk/search/data%20breach), 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](https://www.itpro.co.uk/security/hacking/355773/hackers-take-on-unsuspecting-airliners-exposing-customer-data) 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](https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password) in the United States and the [world’s largest meat supplier JBS](https://www.nytimes.com/2021/06/01/business/meat-plant-cyberattack-jbs.html). 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**](https://www.cryptomathic.com/news-events/blog/cryptography-the-next-10-years-part-1) **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](https://www.cryptomathic.com/news-events/blog/digital-authentication-the-basics) 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



***The cyber stalking cases are dealt in India by the:***

##### 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.

##### 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-

1. 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;
2. 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”.

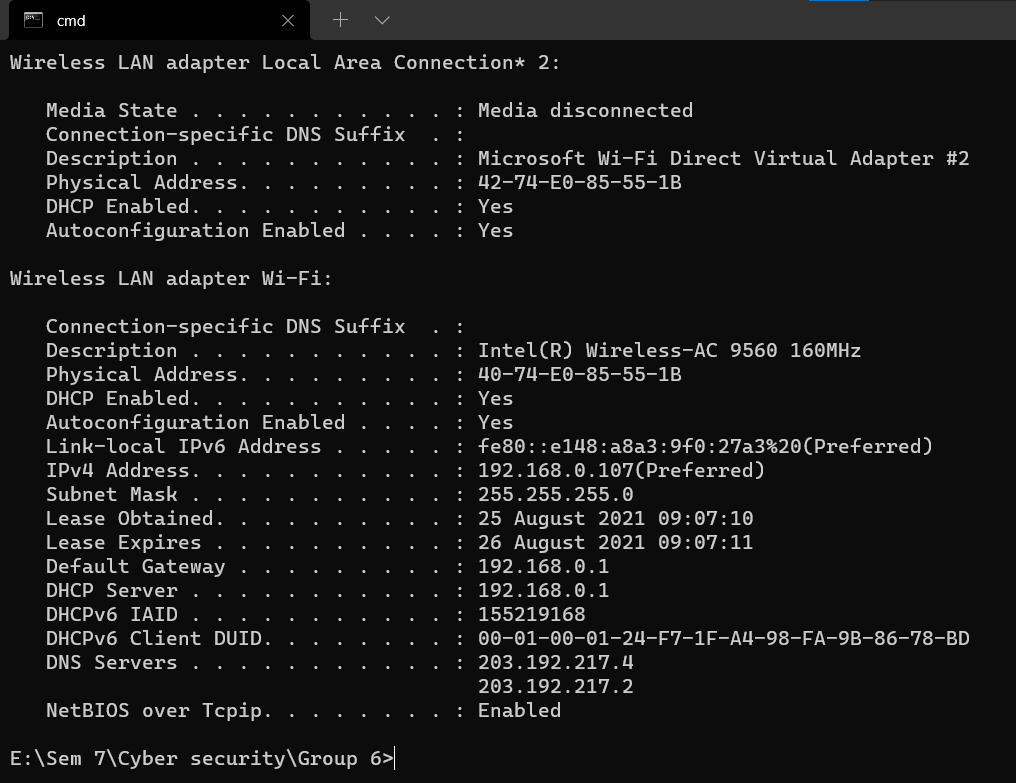
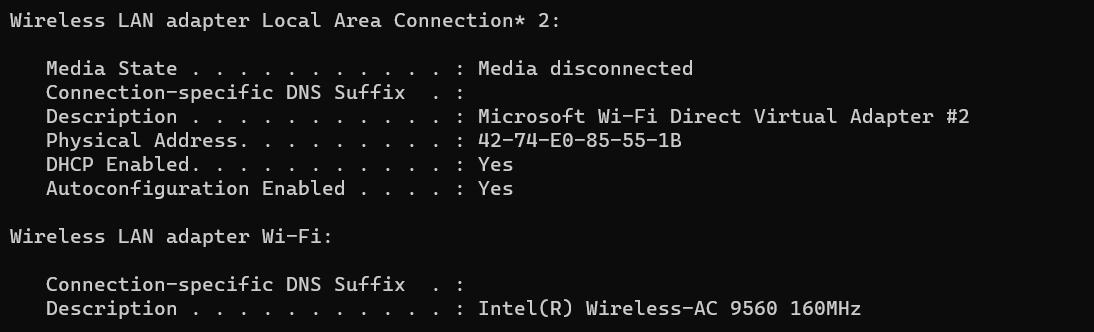
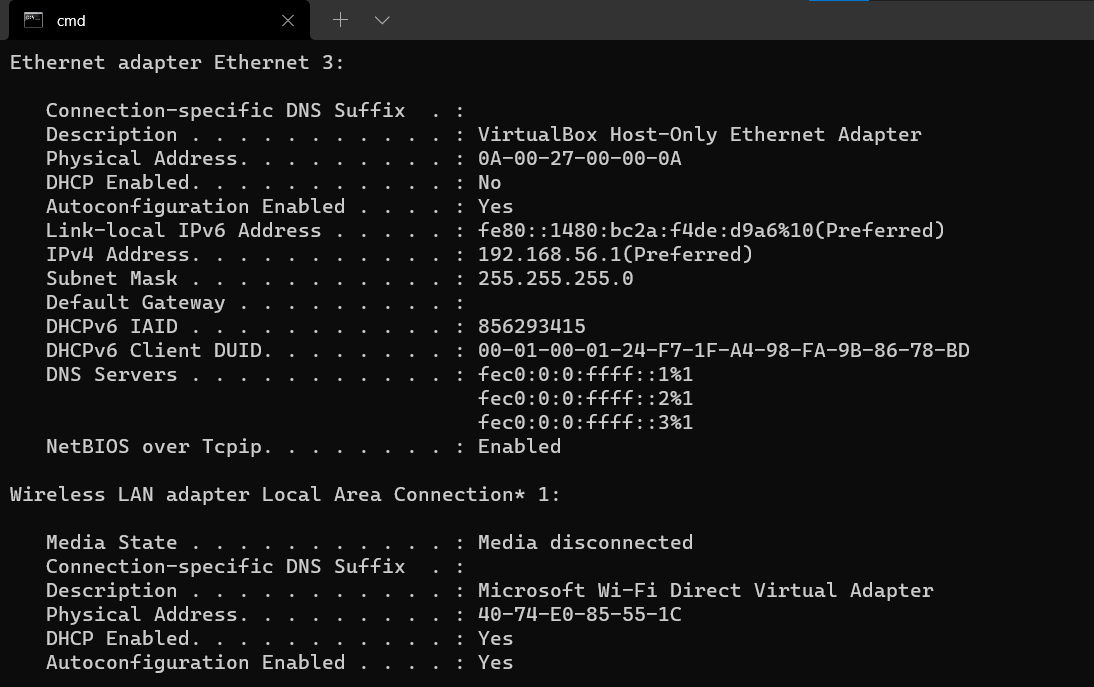
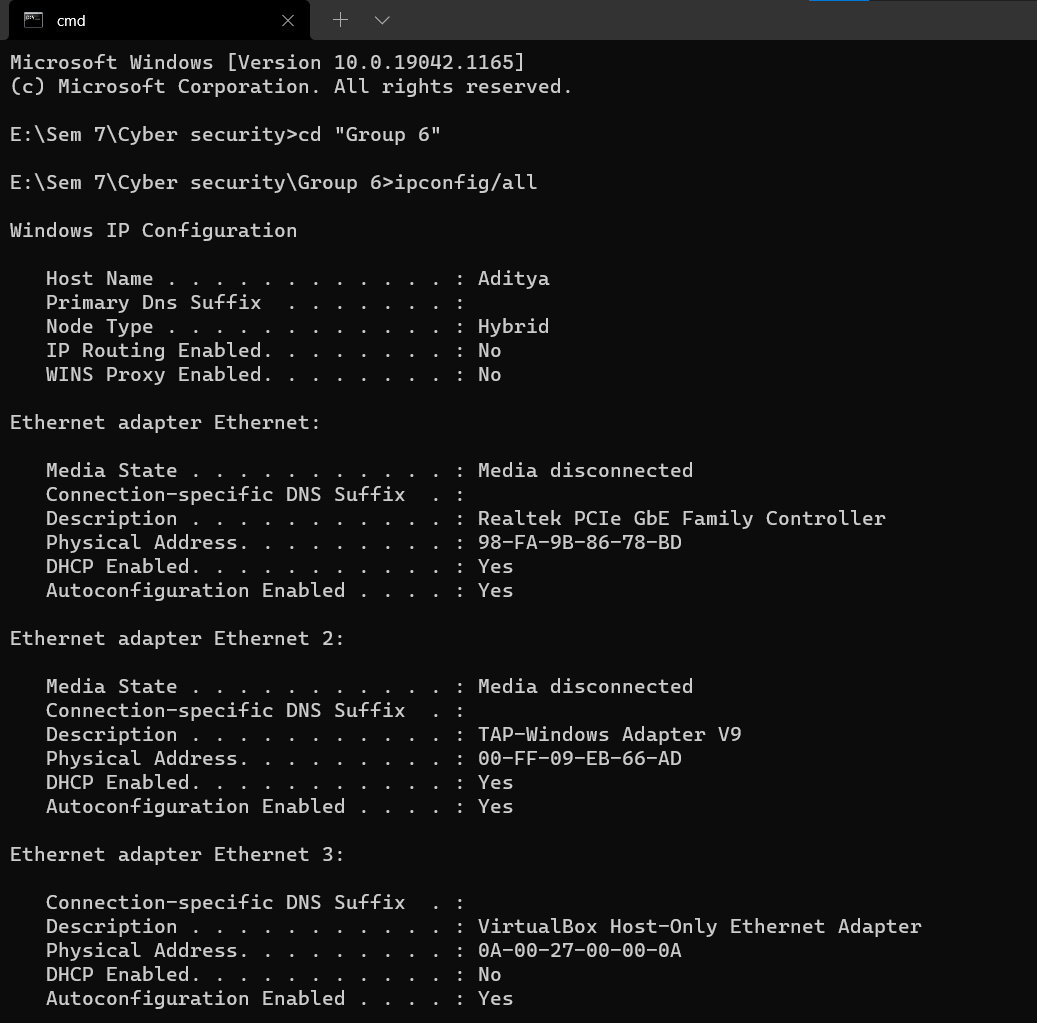
Racism is also a factor in cyber stalking.

### 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.



***NETSTAT***

[**Stands for**](https://www.google.com/search?sxsrf=ALeKk01Zl-8k-v6gFPMyryO20zgcOowxvw%3A1628758337655&q=netstat%2Bstands%2Bfor&stick=H4sIAAAAAAAAAOPgE-LUz9U3MC5Iz7XQUsxOttLPLojPKdcvzcusiE_Oz81NzEuxKi4BksXxaflFi1iF8lJLgPwSBYigAlAQAE7YdnNFAAAA&sa=X&ved=2ahUKEwji1I_RjavyAhXLumMGHTfhCykQ6BMoADAgegQIPRAC)**:** Network statistics

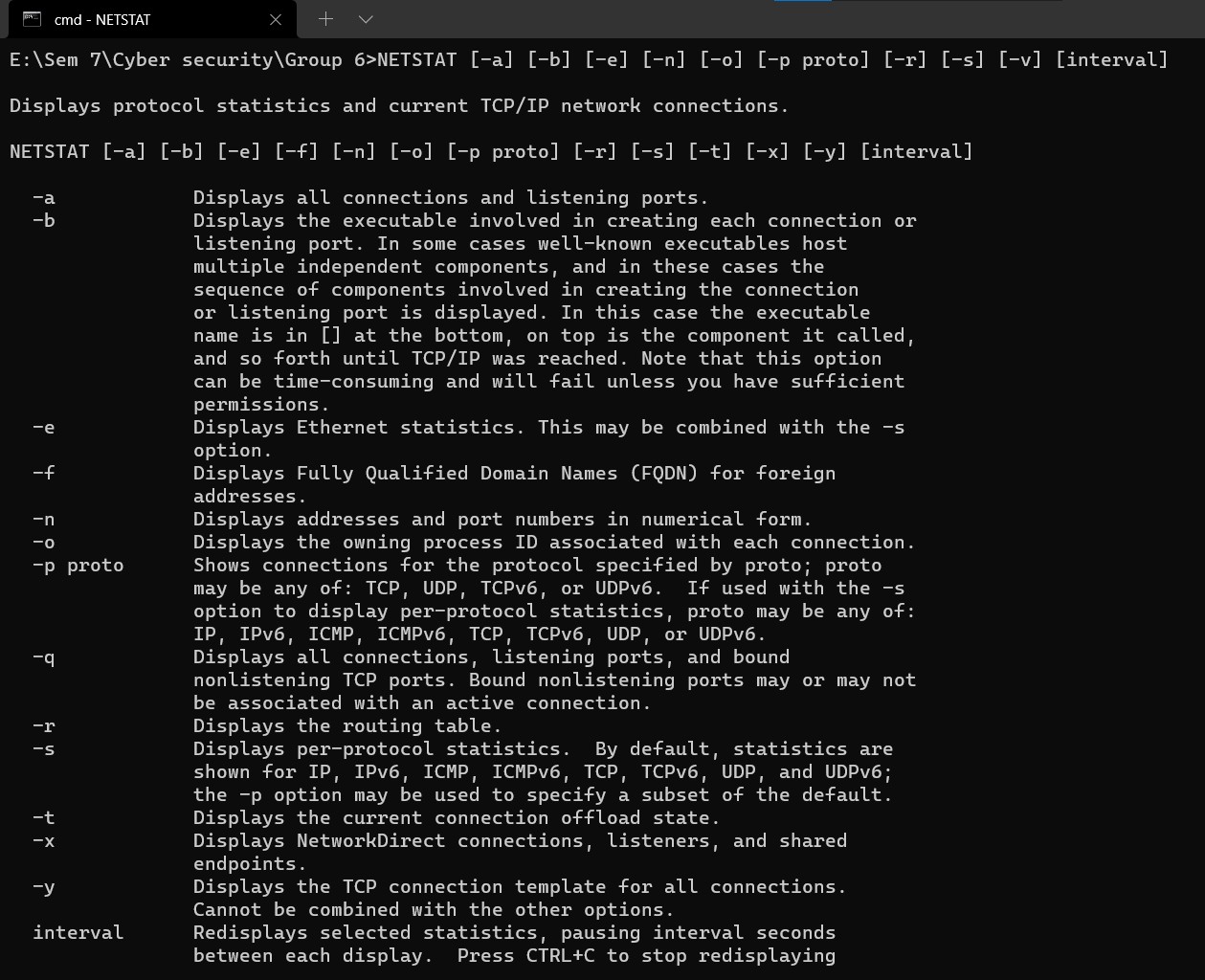
[**Function**](https://www.google.com/search?sxsrf=ALeKk01Zl-8k-v6gFPMyryO20zgcOowxvw%3A1628758337655&q=netstat%2Bfunction&stick=H4sIAAAAAAAAAOPgE-LUz9U3MC5Iz7XQks9OttLPLojPKdcvzcusiE_Oz81NzEuxSivNSy7JzM9bxCqQl1pSXJJYogATAgCA3BZ-QQAAAA&sa=X&ved=2ahUKEwji1I_RjavyAhXLumMGHTfhCykQ6BMoADAhegQIPhAC)**:** Print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships

[**Syntax**](https://www.google.com/search?sxsrf=ALeKk01Zl-8k-v6gFPMyryO20zgcOowxvw%3A1628758337655&q=netstat%2Bsyntax&stick=H4sIAAAAAAAAAOPgE-LUz9U3MC5Iz7XQks1OttLPLojPKdcvzcusiE_Oz81NzEuxKq7MK0msWMTKl5daUlySWKIAEQAAExCr2z0AAAA&sa=X&ved=2ahUKEwji1I_RjavyAhXLumMGHTfhCykQ6BMoADAiegQIQBAC)**:** netstat [address\_family\_options] [--tcp|-t] [--udp|-u] [--raw|-w] [-- listening|-l] [--all|-a] [--numeric|-n] [--numeric-hosts][--numeric-ports][--numeric-

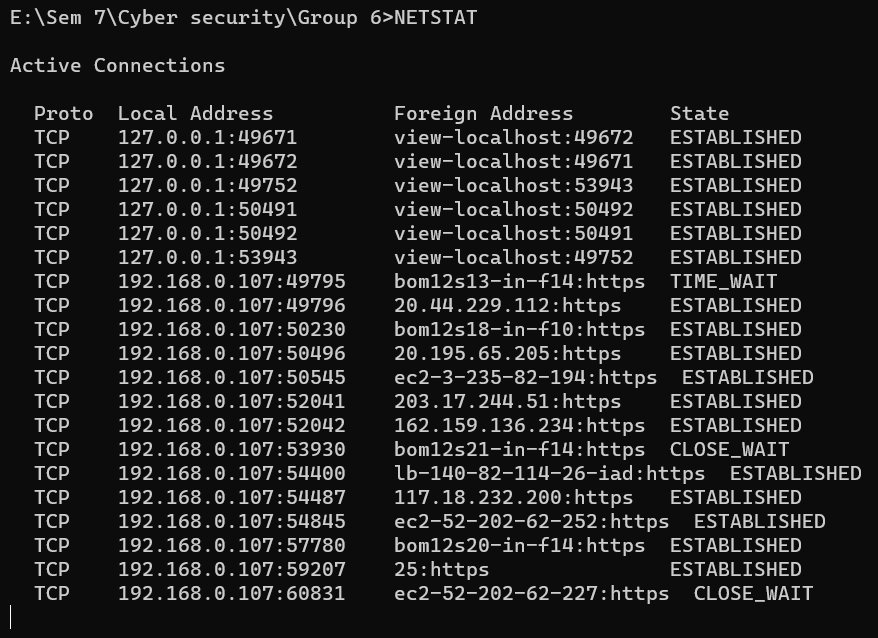
ports] [--symbolic|-N] [--extend|-e[--extend|-e]] [--timers|-o] [--program|-p] [-- verbose|-v] [--continuous|-c] [delay]

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.

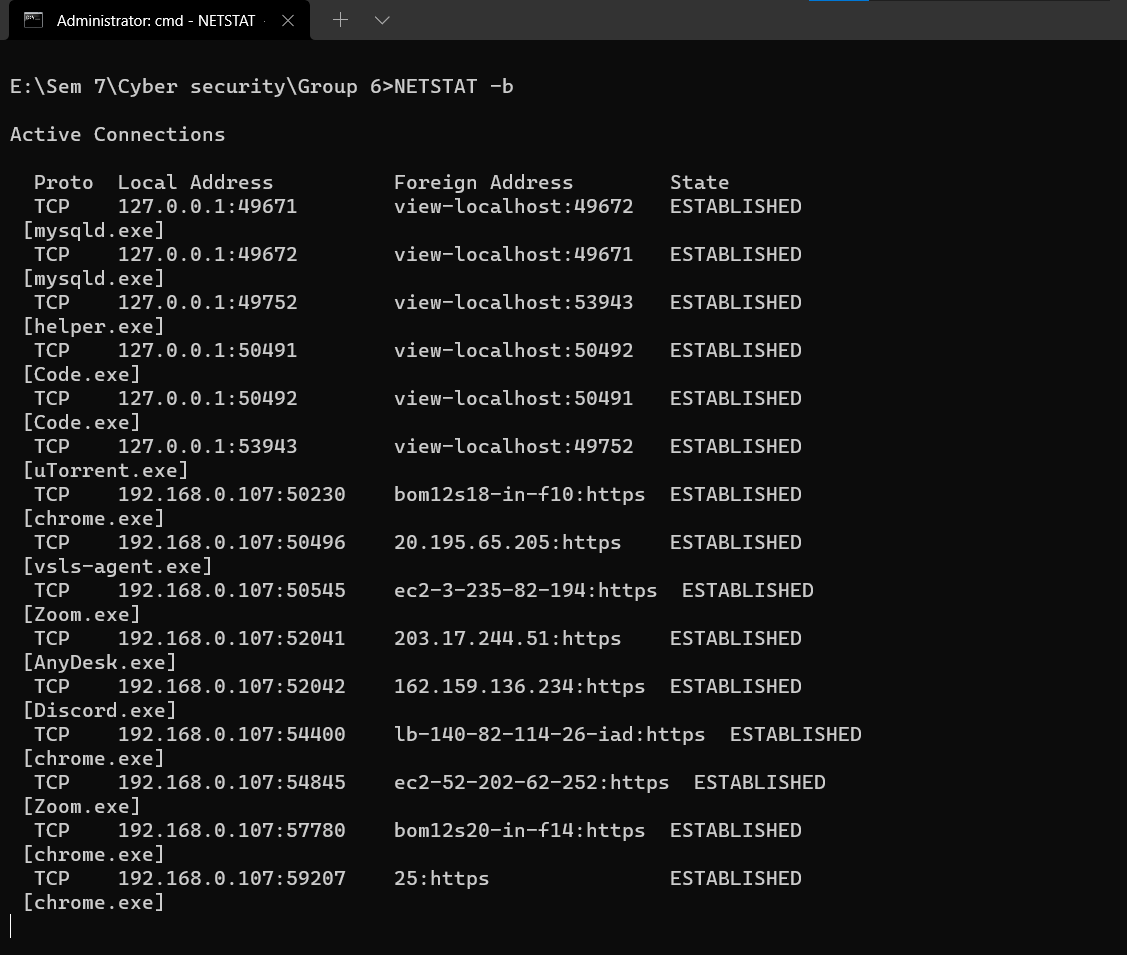
Command -h



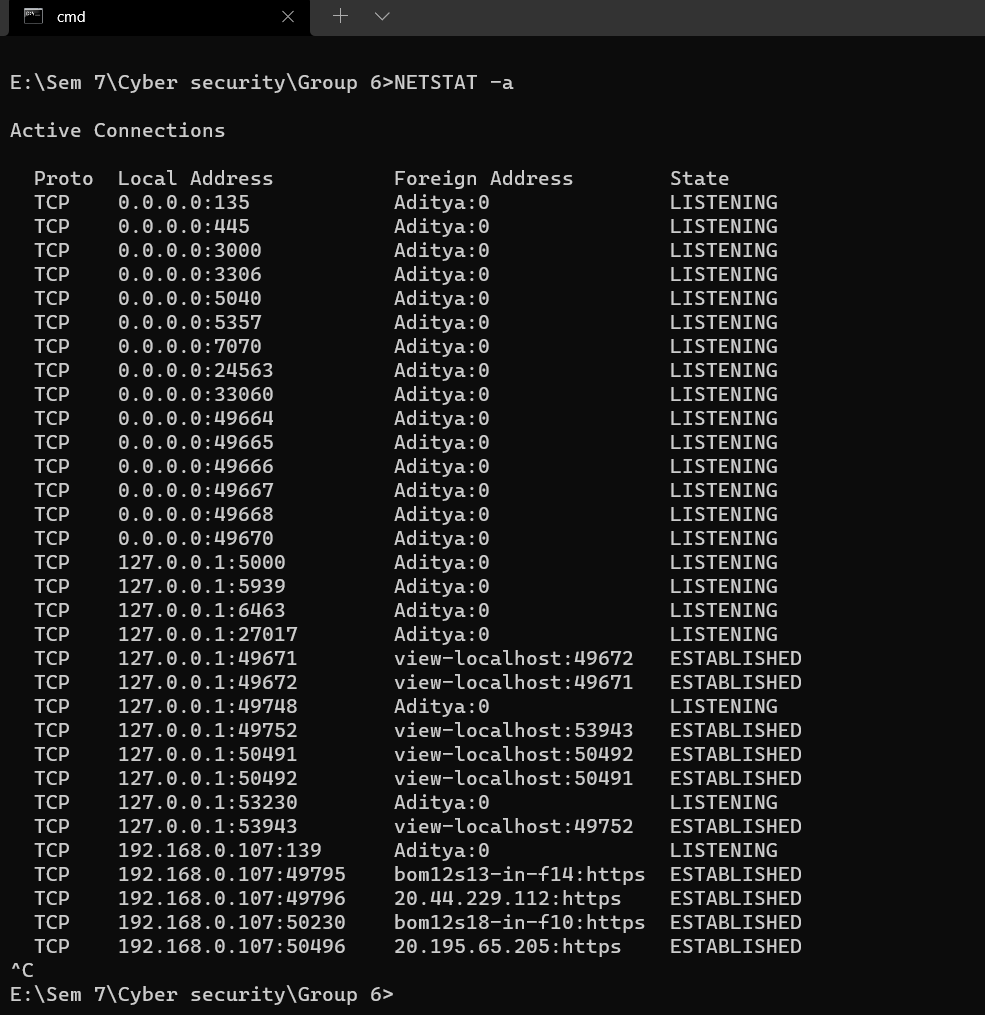
NETSTAT



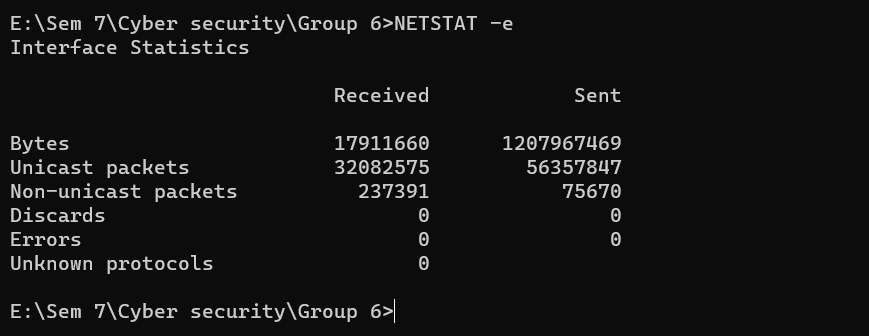
NETSTAT -b



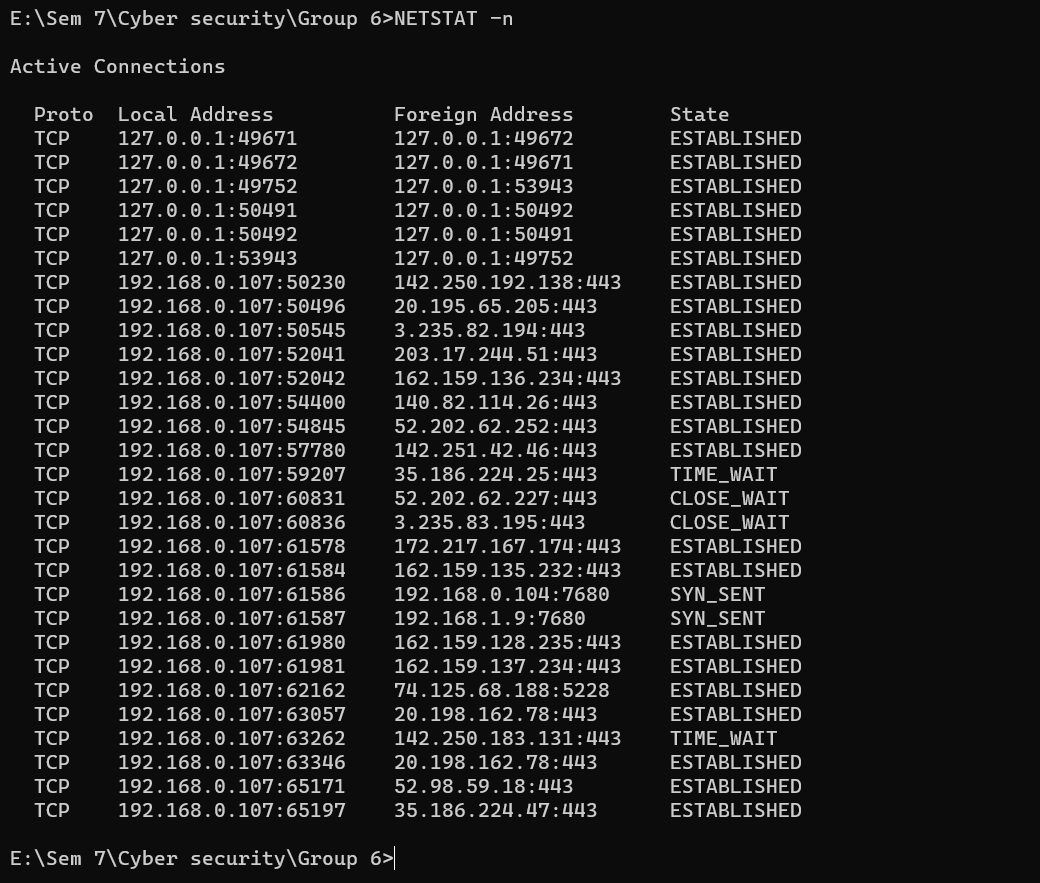
NETSTAT -a



NETSTAT -e



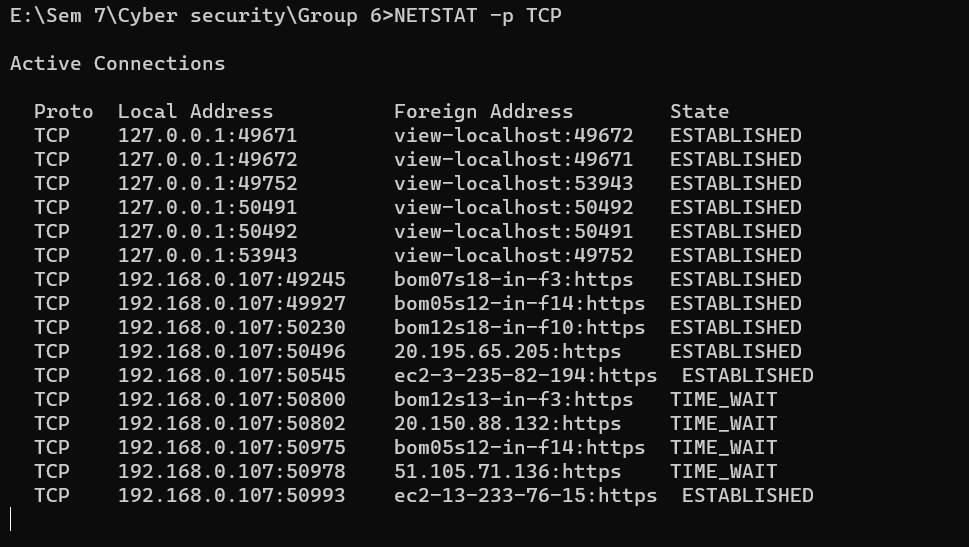
NETSTAT -n



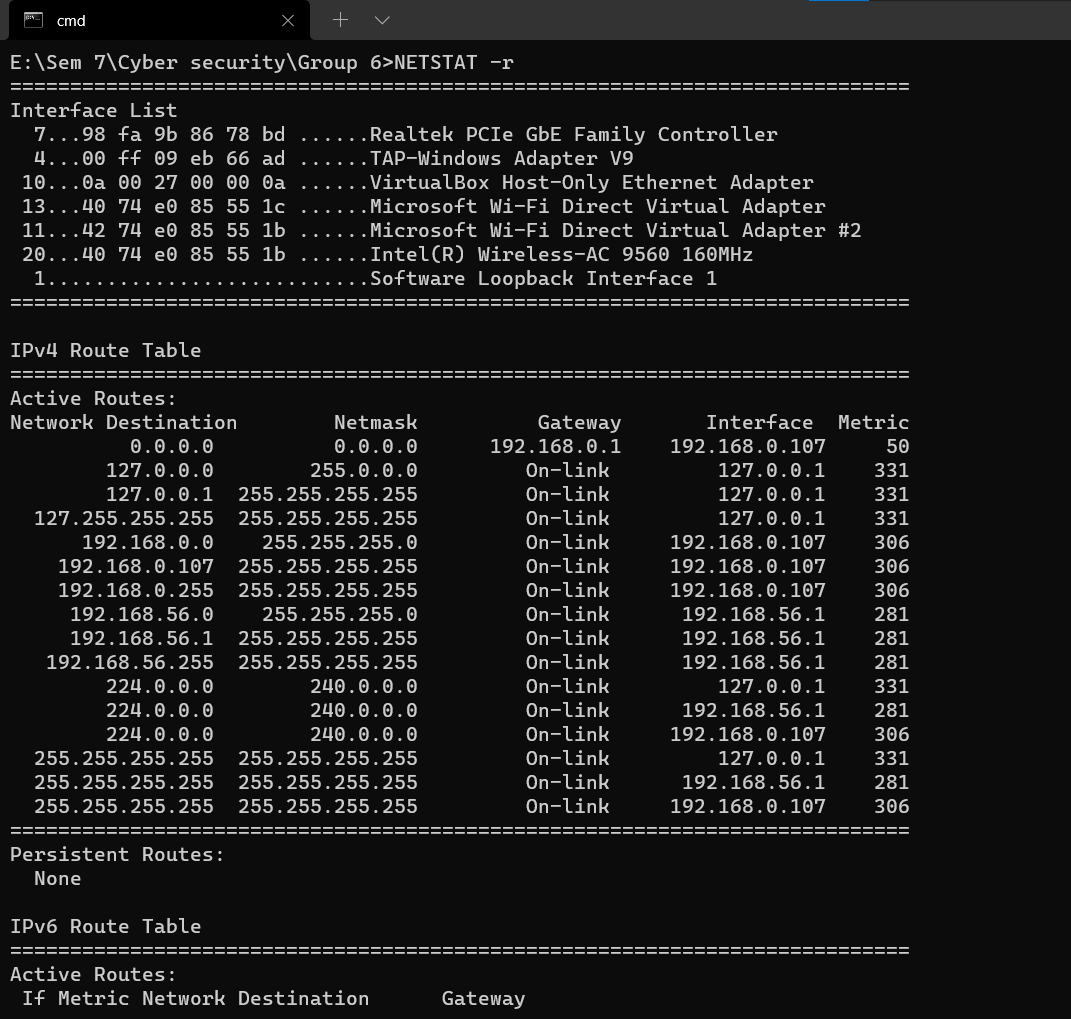
NETSTAT -o

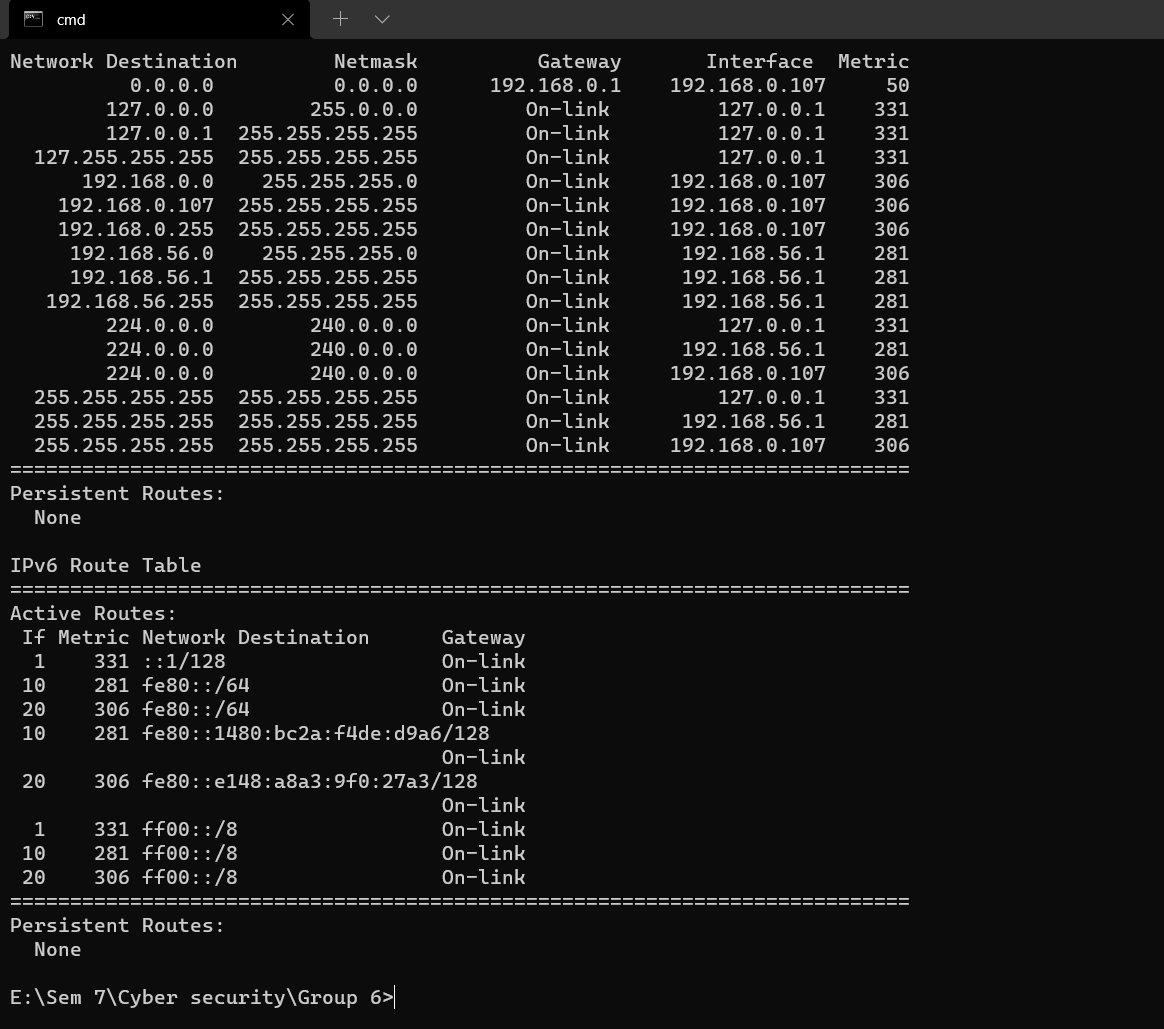


NETSTAT -p TCP

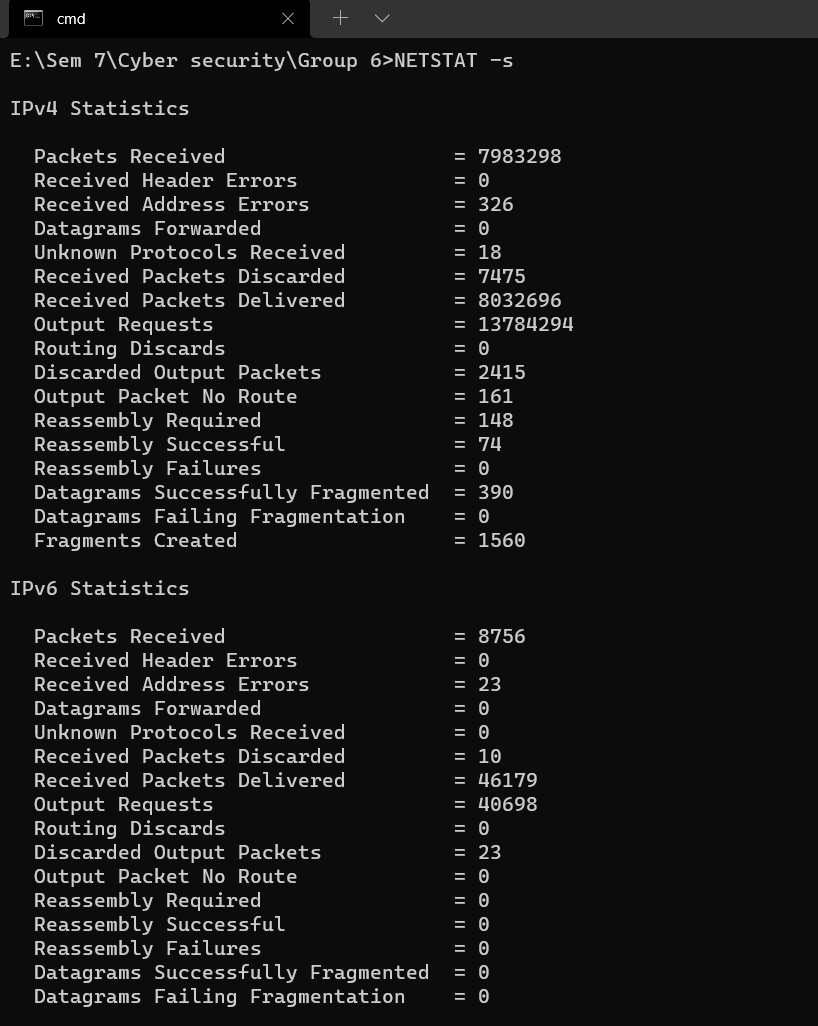


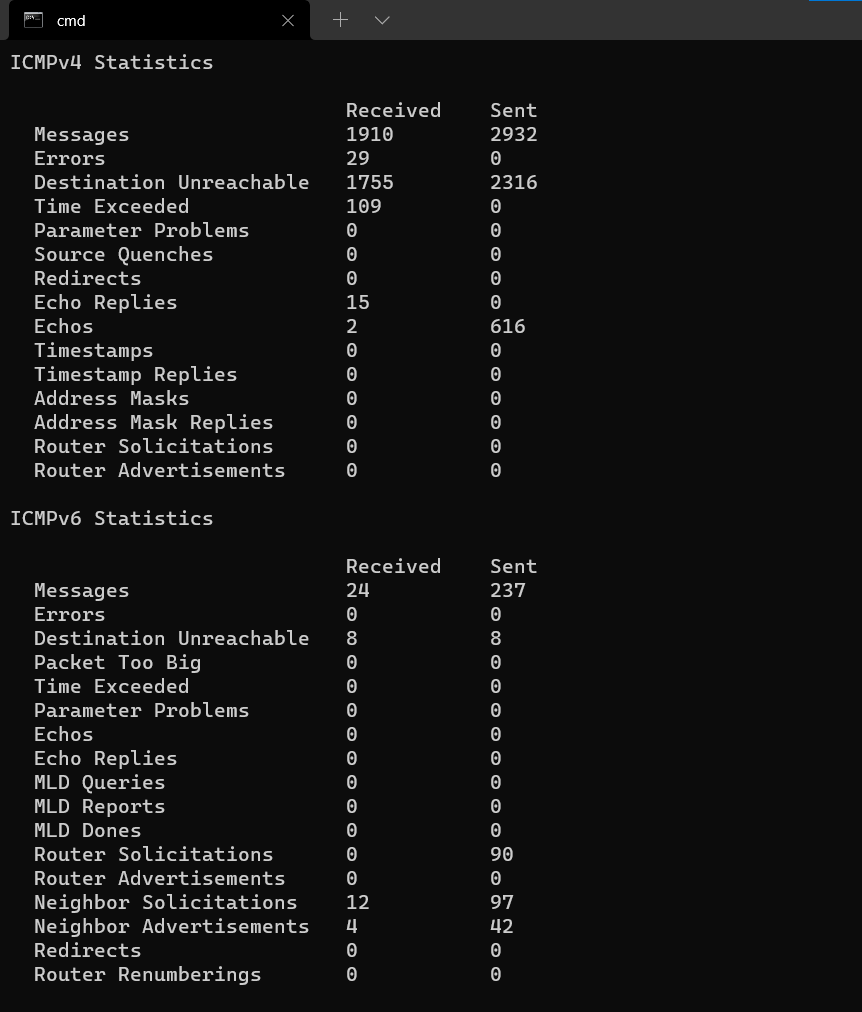
NETSTAT -r





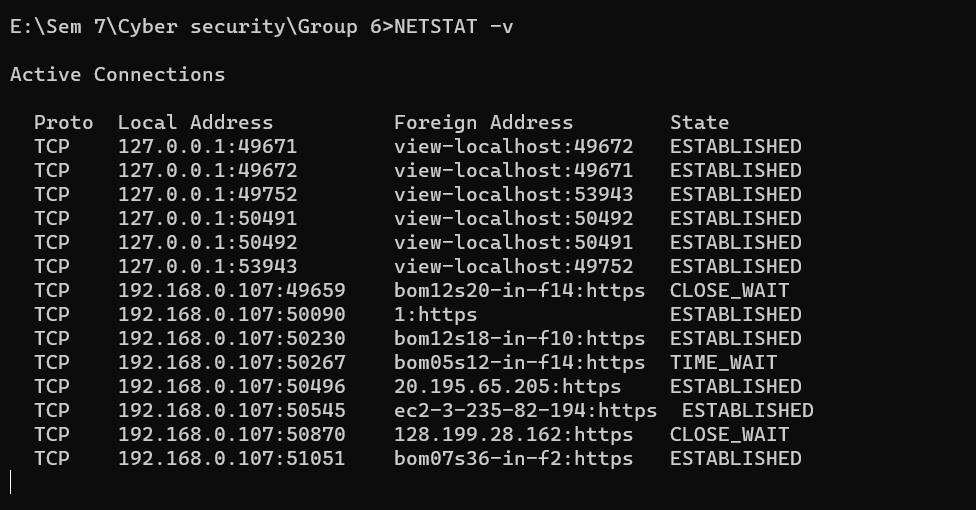
NETSTAT -s







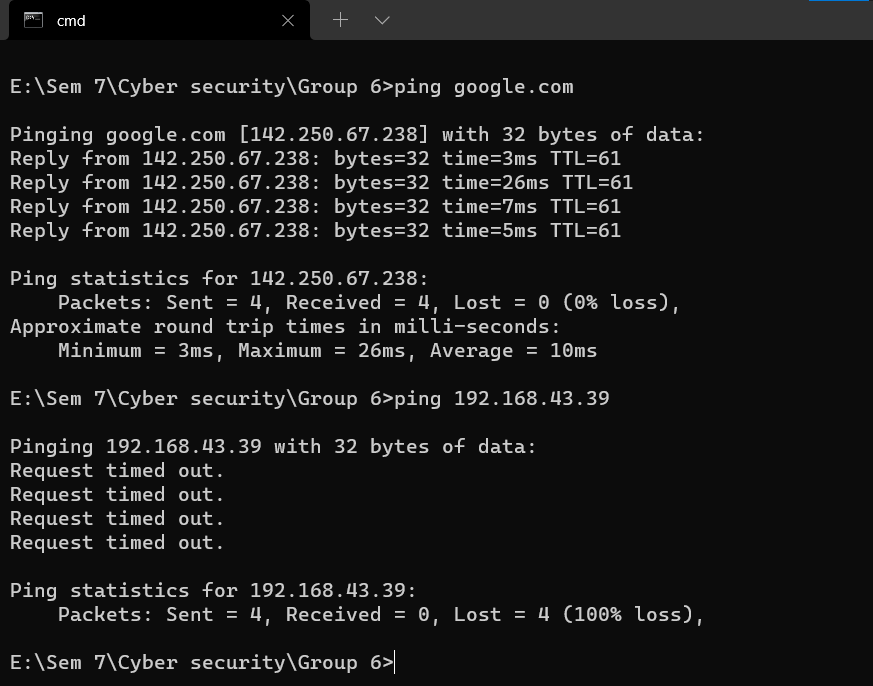
NETSTAT -v



# 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.

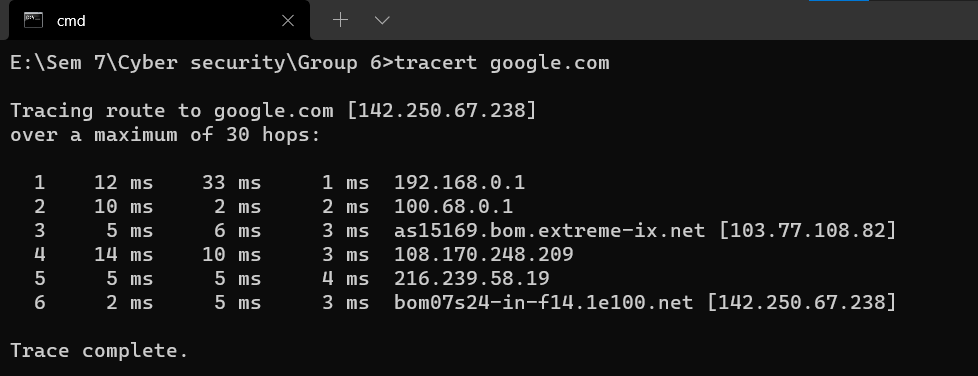
The full form of PING is the Packet InterNet Groper. It is a computer network management system software or utility software used to test the network communication between the two devices.

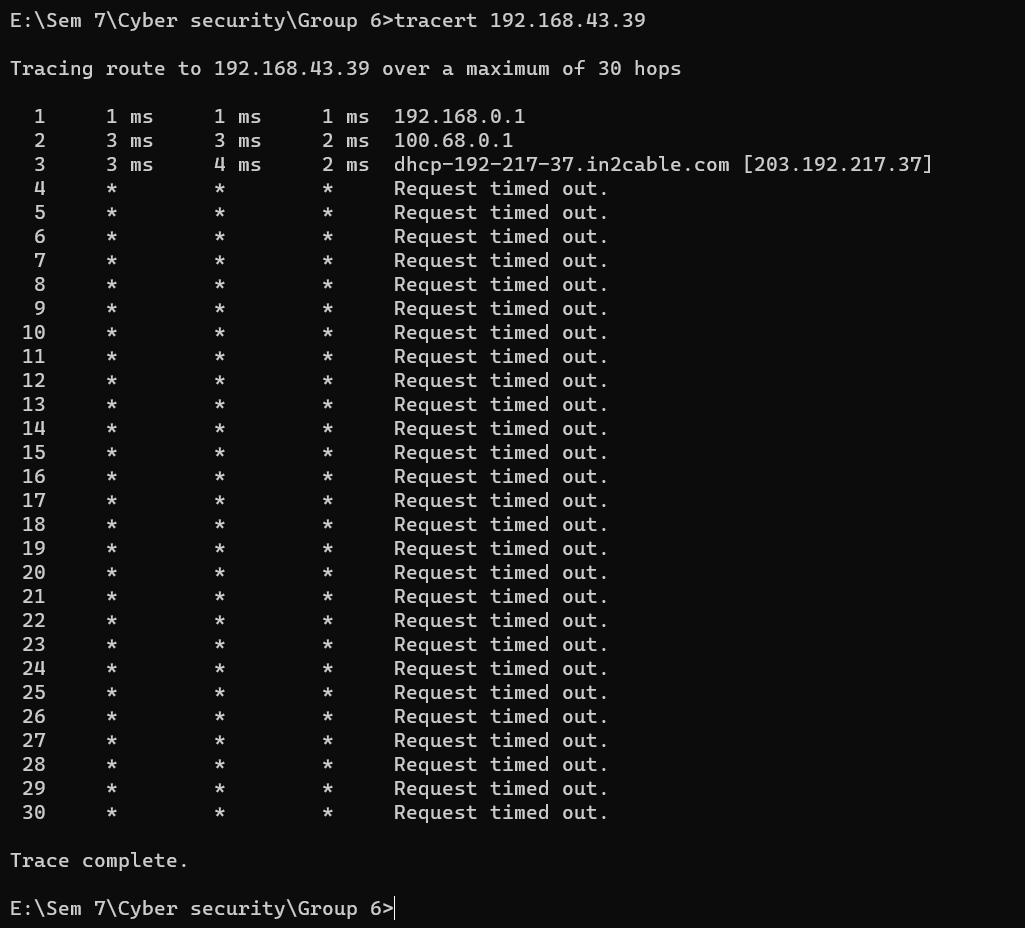


## Tracert

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.





## Arp-a

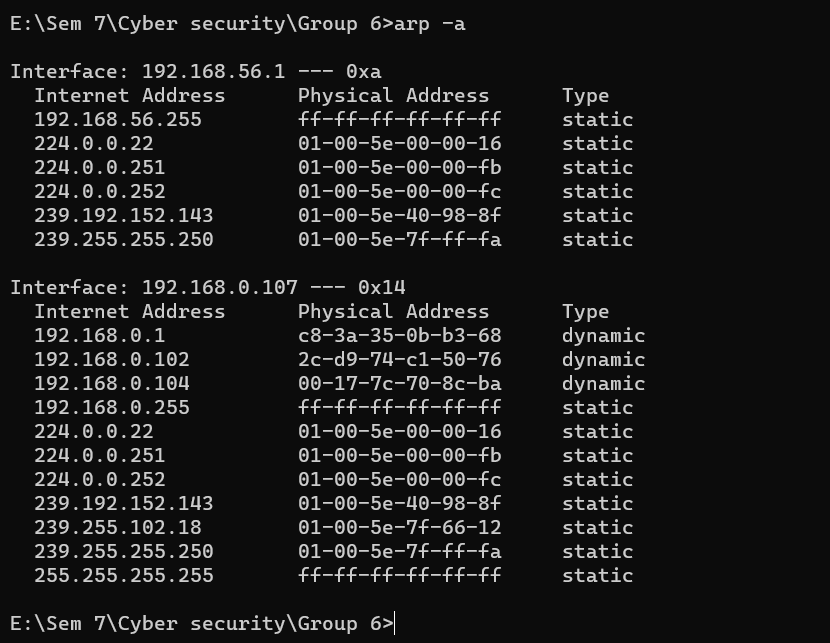
The ARP commands to view, display, or modify the details/information in an ARP table/cache.

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](https://www.javatpoint.com/arp-table) [table](https://www.javatpoint.com/arp-table) is that when you want to communicate with another device, your device does not need to send the [ARP request](https://www.javatpoint.com/arp-request) for the MAC address of that device.

The [ARP](https://www.javatpoint.com/address-resolution-protocol) commands also helps to find out the duplicate [IP](https://www.javatpoint.com/ip-full-form) 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.





## 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.

##### dig :

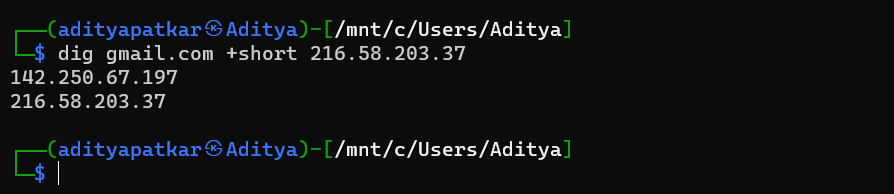
Dig stands for (Domain Information Groper) is a network

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]

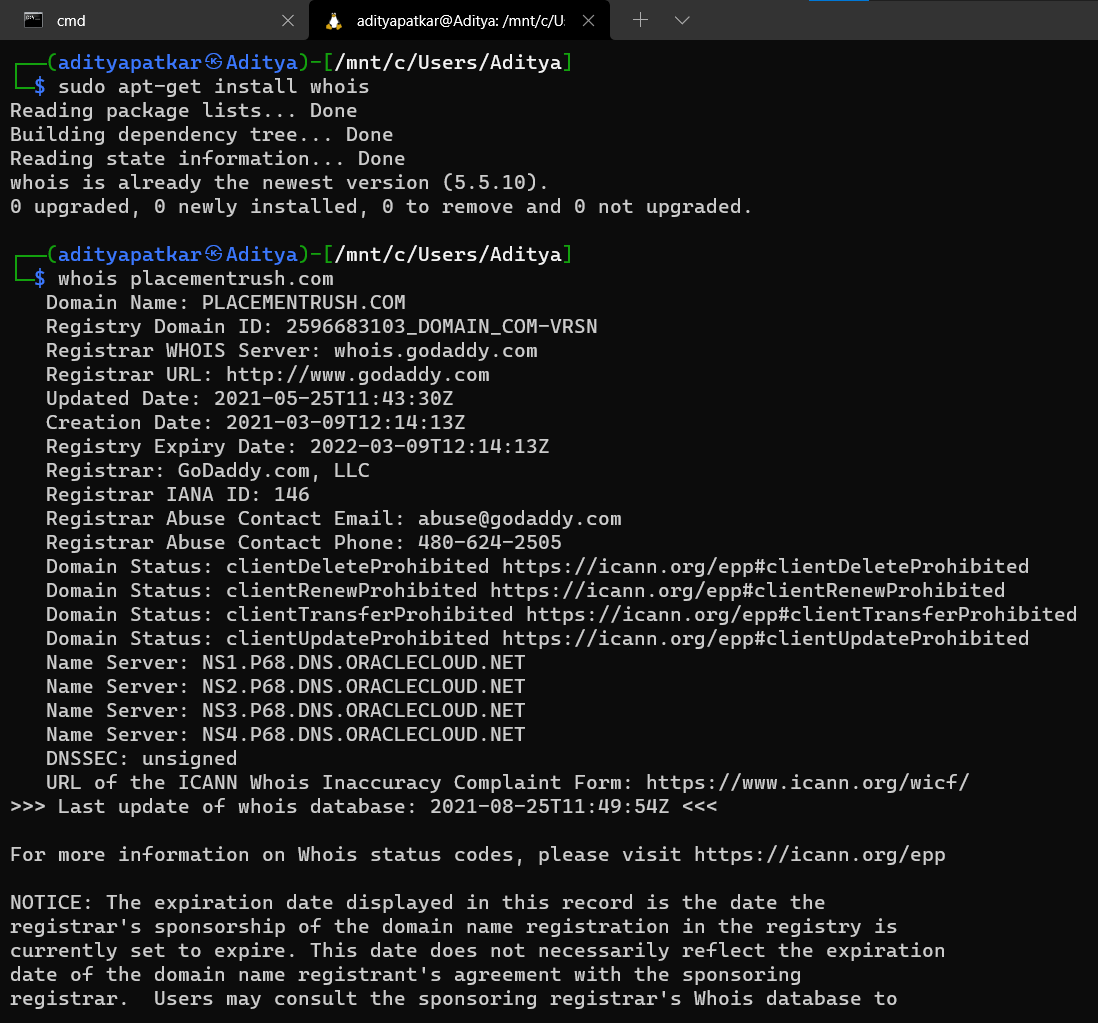


##### whois :

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.

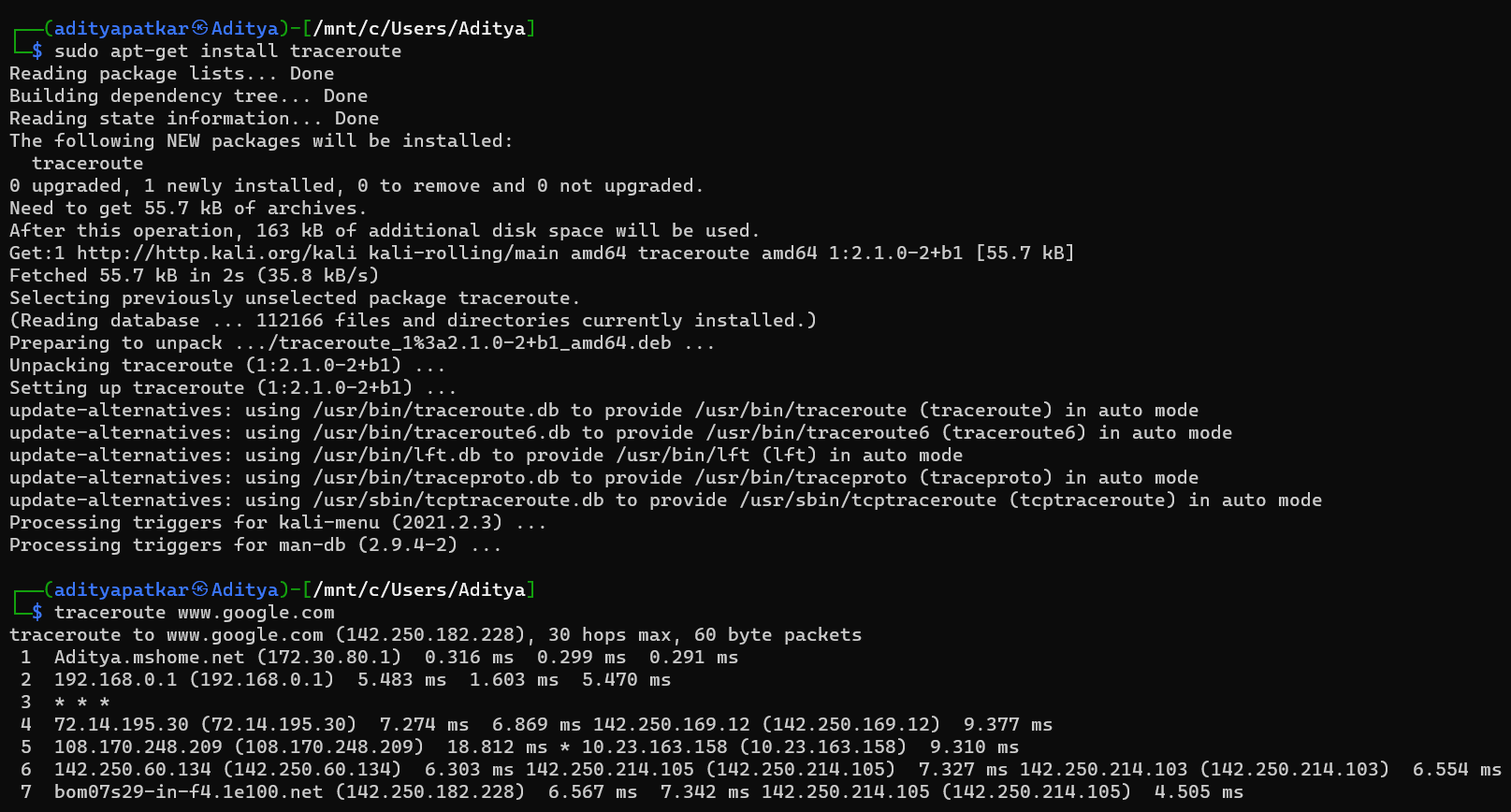
##### Syntax :

whois [target]

##### 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](https://www.javatpoint.com/ip-full-form) addresses, and hostnames of routers over a network. It can be useful for diagnosing network issues.

##### Syntax :

traceroute [OPTION...] HOST

# 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](https://attack.mitre.org/software/S0097) or net view using [Net](https://attack.mitre.org/software/S0039). 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](https://attack.mitre.org/techniques/T1047) and [PowerShell](https://attack.mitre.org/techniques/T1059/001).

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](https://attack.mitre.org/software/S0552) | [AdFind](https://attack.mitre.org/software/S0552) | [AdFind](https://attack.mitre.org/software/S0552) has the ability to query Active Directory for  computers. |
| [G0016](https://attack.mitre.org/groups/G0016) | [APT29](https://attack.mitre.org/groups/G0016) | [APT29](https://attack.mitre.org/groups/G0016) has used [AdFind](https://attack.mitre.org/software/S0552) to enumerate remote systems. |
| [G0022](https://attack.mitre.org/groups/G0022) | [APT3](https://attack.mitre.org/groups/G0022) | [APT3](https://attack.mitre.org/groups/G0022) has a tool that can detect the existence of remote  systems. |
| [G0050](https://attack.mitre.org/groups/G0050) | [APT32](https://attack.mitre.org/groups/G0050) | [APT32](https://attack.mitre.org/groups/G0050) has enumerated DC servers using the command net group "Domain Controllers" /domain. The group has also used  the ping command |
| [G0087](https://attack.mitre.org/groups/G0087) | [APT39](https://attack.mitre.org/groups/G0087) | [APT39](https://attack.mitre.org/groups/G0087) has used [NBTscan](https://attack.mitre.org/software/S0590) and custom tools to discover  remote systems. |
| [S0534](https://attack.mitre.org/software/S0534) | [Bazar](https://attack.mitre.org/software/S0534) | [Bazar](https://attack.mitre.org/software/S0534) can enumerate remote systems using Net View. |
| [S0570](https://attack.mitre.org/software/S0570) | [BitPaymer](https://attack.mitre.org/software/S0570) | [BitPaymer](https://attack.mitre.org/software/S0570) can use net view to discover remote systems. |

|  |  |  |
| --- | --- | --- |
| [S0521](https://attack.mitre.org/software/S0521) | [BloodHound](https://attack.mitre.org/software/S0521) | [BloodHound](https://attack.mitre.org/software/S0521) can enumerate and collect the properties of domain computers, including domain controllers. |
| [G0060](https://attack.mitre.org/groups/G0060) | [BRONZE BUTLER](https://attack.mitre.org/groups/G0060) | [BRONZE BUTLER](https://attack.mitre.org/groups/G0060) typically use ping and [Net](https://attack.mitre.org/software/S0039) to enumerate systems. |
| [S0335](https://attack.mitre.org/software/S0335) | [Carbon](https://attack.mitre.org/software/S0335) | [Carbon](https://attack.mitre.org/software/S0335) uses the net view command. |
| [G0114](https://attack.mitre.org/groups/G0114) | [Chimera](https://attack.mitre.org/groups/G0114) | [Chimera](https://attack.mitre.org/groups/G0114) has utilized various scans and queries to find domain controllers and remote services in the target environment. |
| [S0154](https://attack.mitre.org/software/S0154) | [Cobalt Strike](https://attack.mitre.org/software/S0154) | [Cobalt Strike](https://attack.mitre.org/software/S0154) uses the native Windows Network Enumeration APIs to interrogate and discover targets in a Windows Active Directory network. |
| [S0244](https://attack.mitre.org/software/S0244) | [Comnie](https://attack.mitre.org/software/S0244) | [Comnie](https://attack.mitre.org/software/S0244) runs the net view command |
| [S0488](https://attack.mitre.org/software/S0488) | [CrackMapExec](https://attack.mitre.org/software/S0488) | [CrackMapExec](https://attack.mitre.org/software/S0488) can discover active IP addresses, along with the machine name, within a targeted network. |
| [G0009](https://attack.mitre.org/groups/G0009) | [Deep Panda](https://attack.mitre.org/groups/G0009) | [Deep Panda](https://attack.mitre.org/groups/G0009) has used ping to identify other machines of interest. |
| [G0074](https://attack.mitre.org/groups/G0074) | [Dragonfly 2.0](https://attack.mitre.org/groups/G0074) | [Dragonfly 2.0](https://attack.mitre.org/groups/G0074) likely obtained a list of hosts in the victim environment. |
| [S0091](https://attack.mitre.org/software/S0091) | [Epic](https://attack.mitre.org/software/S0091) | [Epic](https://attack.mitre.org/software/S0091) uses the net view command on the victim’s machine. |
| [G0053](https://attack.mitre.org/groups/G0053) | [FIN5](https://attack.mitre.org/groups/G0053) | [FIN5](https://attack.mitre.org/groups/G0053) has used the open source tool Essential NetTools to map the network and build a list of targets. |
| [G0037](https://attack.mitre.org/groups/G0037) | [FIN6](https://attack.mitre.org/groups/G0037) | [FIN6](https://attack.mitre.org/groups/G0037) 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](https://attack.mitre.org/groups/G0061) | [FIN8](https://attack.mitre.org/groups/G0061) | [FIN8](https://attack.mitre.org/groups/G0061) uses [dsquery](https://attack.mitre.org/software/S0105) and other Active Directory utilities to enumerate hosts. |
| [G0117](https://attack.mitre.org/groups/G0117) | [Fox Kitten](https://attack.mitre.org/groups/G0117) | [Fox Kitten](https://attack.mitre.org/groups/G0117) has used Angry IP Scanner to detect remote systems. |
| [G0093](https://attack.mitre.org/groups/G0093) | [GALLIUM](https://attack.mitre.org/groups/G0093) | [GALLIUM](https://attack.mitre.org/groups/G0093) used a modified version of [NBTscan](https://attack.mitre.org/software/S0590) to identify available NetBIOS name servers over the network as well as ping to identify remote systems. |
| [G0004](https://attack.mitre.org/groups/G0004) | [Ke3chang](https://attack.mitre.org/groups/G0004) | [Ke3chang](https://attack.mitre.org/groups/G0004) has used network scanning and enumeration tools, including [Ping](https://attack.mitre.org/software/S0097). |
| [S0599](https://attack.mitre.org/software/S0599) | [Kinsing](https://attack.mitre.org/software/S0599) | [Kinsing](https://attack.mitre.org/software/S0599) has used a script to parse files  like /etc/hosts and SSH known\_hosts to discover remote systems. |
| [S0236](https://attack.mitre.org/software/S0236) | [Kwampirs](https://attack.mitre.org/software/S0236) | [Kwampirs](https://attack.mitre.org/software/S0236) collects a list of available servers with the command net view |
| [G0077](https://attack.mitre.org/groups/G0077) | [Leafminer](https://attack.mitre.org/groups/G0077) | [Leafminer](https://attack.mitre.org/groups/G0077) used Microsoft’s Sysinternals tools to gather detailed information about remote systems. |
| [G0045](https://attack.mitre.org/groups/G0045) | [menuPass](https://attack.mitre.org/groups/G0045) | [menuPass](https://attack.mitre.org/groups/G0045) uses scripts to enumerate IP ranges on the victim network. [menuPass](https://attack.mitre.org/groups/G0045) has also issued the |

|  |  |  |
| --- | --- | --- |
|  |  | command net view /domain to a [PlugX](https://attack.mitre.org/software/S0013) implant to gather information about remote systems on the network. |
| [S0233](https://attack.mitre.org/software/S0233) | [MURKYTOP](https://attack.mitre.org/software/S0233) | [MURKYTOP](https://attack.mitre.org/software/S0233) has the capability to identify remote hosts on connected networks. |
| [S0590](https://attack.mitre.org/software/S0590) | [NBTscan](https://attack.mitre.org/software/S0590) | [NBTscan](https://attack.mitre.org/software/S0590) can list NetBIOS computer names. |
| [S0039](https://attack.mitre.org/software/S0039) | [Net](https://attack.mitre.org/software/S0039) | Commands such as net view can be used in [Net](https://attack.mitre.org/software/S0039) to gather information about available remote systems. |
| [S0385](https://attack.mitre.org/software/S0385) | [njRAT](https://attack.mitre.org/software/S0385) | [njRAT](https://attack.mitre.org/software/S0385) can identify remote hosts on connected networks. |
| [S0359](https://attack.mitre.org/software/S0359) | [Nltest](https://attack.mitre.org/software/S0359) | [Nltest](https://attack.mitre.org/software/S0359) may be used to enumerate remote domain controllers using options such  as /dclist and /dsgetdc. |
| [S0365](https://attack.mitre.org/software/S0365) | [Olympic Destroyer](https://attack.mitre.org/software/S0365) | [Olympic Destroyer](https://attack.mitre.org/software/S0365) uses [Windows Management](https://attack.mitre.org/techniques/T1047) [Instrumentation](https://attack.mitre.org/techniques/T1047) to enumerate all systems in the  network. |
| [G0116](https://attack.mitre.org/groups/G0116) | [Operation Wocao](https://attack.mitre.org/groups/G0116) | [Operation Wocao](https://attack.mitre.org/groups/G0116) can use the ping command to discover remote systems. |
| [S0165](https://attack.mitre.org/software/S0165) | [OSInfo](https://attack.mitre.org/software/S0165) | [OSInfo](https://attack.mitre.org/software/S0165) performs a connection test to discover remote systems in the network |
| [S0097](https://attack.mitre.org/software/S0097) | [Ping](https://attack.mitre.org/software/S0097) | [Ping](https://attack.mitre.org/software/S0097) can be used to identify remote systems within a network. |
| [S0428](https://attack.mitre.org/software/S0428) | [PoetRAT](https://attack.mitre.org/software/S0428) | [PoetRAT](https://attack.mitre.org/software/S0428) used Nmap for remote system  discovery. |
| [S0241](https://attack.mitre.org/software/S0241) | [RATANKBA](https://attack.mitre.org/software/S0241) | [RATANKBA](https://attack.mitre.org/software/S0241) runs the net view /domain and net view commands. |
| [S0125](https://attack.mitre.org/software/S0125) | [Remsec](https://attack.mitre.org/software/S0125) | [Remsec](https://attack.mitre.org/software/S0125) can ping or traceroute a remote host. |
| [G0106](https://attack.mitre.org/groups/G0106) | [Rocke](https://attack.mitre.org/groups/G0106) | [Rocke](https://attack.mitre.org/groups/G0106) has looked for IP addresses in the known\_hosts file on the infected system and attempted to SSH into them.[[46]](https://blog.talosintelligence.com/2018/08/rocke-champion-of-monero-miners.html) |
| [G0034](https://attack.mitre.org/groups/G0034) | [Sandworm Team](https://attack.mitre.org/groups/G0034) | [Sandworm Team](https://attack.mitre.org/groups/G0034) has used a tool to query Active Directory using LDAP, discovering information  about computers listed in AD. |
| [S0140](https://attack.mitre.org/software/S0140) | [Shamoon](https://attack.mitre.org/software/S0140) | [Shamoon](https://attack.mitre.org/software/S0140) scans the C-class subnet of the IPs on the victim's interfaces.[[48]](https://www.fireeye.com/blog/threat-research/2016/11/fireeye_respondsto.html) |
| [S0063](https://attack.mitre.org/software/S0063) | [SHOTPUT](https://attack.mitre.org/software/S0063) | [SHOTPUT](https://attack.mitre.org/software/S0063) has a command to list all servers in the  domain, as well as one to locate domain controllers on a domain. |

|  |  |  |
| --- | --- | --- |
| [G0091](https://attack.mitre.org/groups/G0091) | [Silence](https://attack.mitre.org/groups/G0091) | [Silence](https://attack.mitre.org/groups/G0091) has used Nmap to scan the corporate network, build a network topology, and identify vulnerable hosts. |
| [S0018](https://attack.mitre.org/software/S0018) | [Sykipot](https://attack.mitre.org/software/S0018) | [Sykipot](https://attack.mitre.org/software/S0018) may use net view /domain to display hostnames of available systems on a network. |
| [S0586](https://attack.mitre.org/software/S0586) | [TAINTEDSCRIBE](https://attack.mitre.org/software/S0586) | The [TAINTEDSCRIBE](https://attack.mitre.org/software/S0586) command and execution module can perform target system enumeration. |
| [G0027](https://attack.mitre.org/groups/G0027) | [Threat Group-3390](https://attack.mitre.org/groups/G0027) | [Threat Group-3390](https://attack.mitre.org/groups/G0027) has used the net view command. |
| [S0266](https://attack.mitre.org/software/S0266) | [TrickBot](https://attack.mitre.org/software/S0266) | [TrickBot](https://attack.mitre.org/software/S0266) can enumerate computers and network devices. |
| [G0010](https://attack.mitre.org/groups/G0010) | [Turla](https://attack.mitre.org/groups/G0010) | [Turla](https://attack.mitre.org/groups/G0010) surveys a system upon check-in to discover remote systems on a local network using the net view and net view  /DOMAIN commands. [Turla](https://attack.mitre.org/groups/G0010) 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](https://attack.mitre.org/software/S0452) | [USBferry](https://attack.mitre.org/software/S0452) | [USBferry](https://attack.mitre.org/software/S0452) can use net view to gather information about remote systems. |
| [S0366](https://attack.mitre.org/software/S0366) | [WannaCry](https://attack.mitre.org/software/S0366) | [WannaCry](https://attack.mitre.org/software/S0366) scans its local network segment for remote systems to try to exploit and copy itself to. |
| [G0102](https://attack.mitre.org/groups/G0102) | [Wizard Spider](https://attack.mitre.org/groups/G0102) | [Wizard Spider](https://attack.mitre.org/groups/G0102) has used networkdll for network discovery and psfin specifically for financial and point of sale indicators. [Wizard Spider](https://attack.mitre.org/groups/G0102) has also used [AdFind](https://attack.mitre.org/software/S0552) and nltest/dclist to enumerate  domain computers, including the domain controller. |
| [S0248](https://attack.mitre.org/software/S0248) | [yty](https://attack.mitre.org/software/S0248) | [yty](https://attack.mitre.org/software/S0248) 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.