

**Veermata Jijabai Technological Institute, Mumbai 400019**

**Experiment No.:** 01

**Aim:** Cyber Crime

**Group :** Kiran Patil - 211070904

Mayuresh Murudkar - 211070903

Pratiksha Sankhe – 201071049

**Branch:** Computer Engineering

**Batch:** D

**Case Study:** **Ransomware Attack on All-India Institute of Medical Sciences (AIIMS)**

November 2022, the premier medical institute in the country, All India Institute of Medical Sciences New Delhi (AIIMS) was crippled by a major cyberattack. Most of its servers stopped working as also the eHospital network. All functions including the emergency, out-patient, in-patient and laboratory wings had to be shifted to manual management.

**RANSOMWARE ATTACK ON AIIMS**

**DEVELOPMENTS SO FAR**

* On 23 November 2022, patients and doctors complained about the hospital’s services working slowly or not at all. As a result, the hospital was forced into working in a manual mode.
* The National Informatics Centre investigated the issue and found signs of a ransomware attack on the hospital’s servers.
* The attack corrupted all the files stored on the main and backup servers of the hospital.
* The cyber-attack derailed many day-to-day activities at AIIMS, with OPD registrations and blood sample reports being halted at the premier institute. While AIIMS was able to restart some of these services, records were being kept manually causing delays and inconvenience to medical personnel and patients alike.
* The breach in security has particularly affected the e-hospital application, which was provided and managed by NIC since 2011-12, stopping the online functioning of OPD, emergency, and other patient care services on the AIIMS premises.
* On 30 November 2022, AIIMS decided to get four new servers from the Defence Research and Development Organisation (DRDO) so it can resume its e-hospital facility for patients.
* On 16 December 2022, replying to another question in the Lok Sabha, Minister of State for Health and Family Welfare said
* All the data for e-Hospital had been retrieved from a backup server and restored on new servers. Most of the functions of e-Hospital application such as patient registration, appointment, admission, discharge etc. had been restored after two weeks of the attack.
* Probe agencies have still not located the person, organisation and exact physical location linked to the cyberattack. However, they have tracked a server address in China, which could be an indication towards state sponsored cyber warfare which was already flagged by various cyber threat intelligence firms.

**IMPACTS AND RAMIFICATIONS**

* The organisation’s critical data is encrypted so that they cannot access files, databases, or applications stored on the main and backup servers of the hospital.
* The cyberattack has frozen everyday work at AIIMS, including appointments and registration, billing, laboratory report generation, etc.
* The exploited databases also contained personally identifiable information of patients and healthcare workers — and administrative records on blood donors, ambulances, vaccination and caregivers, and employee log-in credentials.
* The data breach has reportedly compromised the data of nearly 3–4 crore patients, including sensitive data and medical records of several VIPs including former prime ministers, ministers, bureaucrats, and judges,

**RESPONSE OF SECURITY AGENCIES**

* **Multi-agency investigation**: The extent and threat of the attack was so much that multiple agencies like Delhi Police, the Centre’s Computer Emergency Response Team (CERT-In), the Ministry of Home Affairs, and even the National Investigation Agency have joined the probe.
* A case of extortion and cyber terrorism was registered by the Intelligence Fusion and Strategic Operations (IFSO) unit of the Delhi Police since the attackers made an undisclosed (allegedly Rs. 200 Crore) demand to be sought in cryptocurrency in exchange for a key that would decrypt the data.
* The Delhi Police’s use of the provisions of section 66 (F) of the Information Technology Amendment Act 2008 identifying this incident as a case of cyber terrorism is significant and indicates a much larger ambit than a typical ransomware case.
* The Computer Emergency Response Team (CERT-In) and National Informatics Centre worked on the hospital’s servers to restore functionality.

**FINDINGS**

* CERT-In, the country’s premier cybersecurity agency, has found that the hackers had two Protonmail addresses – “dog2398” and “mouse63209”.
* They also found that ‘dog2398’ and ‘mouse63209’ were generated in the first week of November 2022 in Hong Kong. They also found that another encrypted file was sent from China’s Henan.
* The targeted servers were infected with three ransomwares: Wammacry, Mimikatz and Trojan.
* The investigation also revealed that the main server and applications responsible for OPD services were down as all the system files in the home directory were encrypted by changing their extension to .bak9 – a new file that encrypted the extension files of the system.
* As per CERT-In’s preliminary diagnosis, the cyberattack was the result of an “unorganised ICT (information and communications technology) network without centralised monitoring or system administration”.
* This means the infected devices were connected to each other and the data on all of them could be accessed from every connected device — and no team was monitoring who was accessing these systems.

**CYBERATTACK ON CRITICAL INFORMATION (CI) INFRASTRUCTURE**

* In India, while health is not specified directly as a CI, an organisation like AIIMS New Delhi could be counted as a “strategic and public enterprise” as it treats crores of patients, including the top leadership of the country. It also handles and stores very sensitive medical research data. It is a natural target for cyber attackers and ransom seekers because the data available here is more precious than even oil.
* The ransomware attack on AIIMS is the first such attack on an Indian healthcare institution even as such institutions have been a favoured target of ransomware over the past few years.
* The Information Technology Act of 2000 defines “Critical Information Infrastructure” as a “computer resource, the incapacitation or destruction of which shall have debilitating impact on national security, economy, public health or safety”.
* The government, under the Act, has the power to declare any data, database, IT network or communications infrastructure as CII to protect that digital asset.

**SECURITY PARAMETERS**

The incident described in the news report appears to be a ransomware attack on the servers of the All-India Institute of Medical Sciences (AIIMS). Here's a breakdown of the attack and the potential violations of the CIA Triad (Confidentiality, Integrity, Availability):

1. **Confidentiality:**

Violation: The confidentiality of sensitive medical data was compromised as the attackers gained unauthorized access to AIIMS servers and encrypted approximately 1.3 terabytes of data. This data likely included patient records, which should remain confidential.

1. **Integrity:**

Violation: The integrity of the data was compromised as the ransomware encrypted the data on the servers. Ransomware attacks typically involve encryption, and the integrity of the data can be compromised if the decryption keys are not readily available.

1. **Availability:**

Violation: The availability of critical healthcare services and data was disrupted. The attack caused operational disruption due to non-functionality of critical applications, impacting patient care and hospital operations. It took two weeks to restore most of the functions, which is a significant availability issue.

Regarding measures to prevent such attacks in the future, several steps can be taken:

* **Making threat analysis a norm**: Vulnerability report should be generated followed by an audit which will highlight the loopholes in the cyber-attack preparedness of the organisation. An annual review of the software should also be conducted, as and when the software is changed/updated.
* **Capacity building**: The capacity enhancement for the NCIIPC and CERT-In needs to be undertaken in areas like AI/ML, Blockchain, IoT, Cloud, Automation to address the emerging sophisticated nature of threats and attacks. Sectoral CERTs also have to be set up for many areas including health.
* **‘3-2-1 backup’ approach:** Healthcare entities must save 3 copies of each type of data in 2 different formats, including 1 offline. This is an industry best practice to make healthcare institutes cyber secure.
* **Enhanced budgetary allocation**: A minimum allocation of 0.25% of the annual budget, which can be raised up to 1% to be set aside for cyber security as recommended by the National Cyber Security Strategy. An organisation like AIIMS New Delhi could be counted as a “strategic and public enterprise” as it deals with crores of patients, including the top leadership of the country.
* **Crisis Management**: For adequate preparation to handle a crisis, cyber security drills can be undertaken which include real-life scenarios with their ramifications. A National Gold Standard should be created, which ensures that Indian hardware and software companies adhere to the highest safety protocols.
* **Cyber Diplomacy**: On countering cyber-attacks, the cyber security preparedness of key regional blocks like BIMSTEC and Shanghai Cooperation Organisation (SCO) must be ensured via programs, exchanges and industrial support.
* **Awareness generation**: The general public needs to be made aware of what value their personal data holds or what vulnerabilities it could generate if accessed illegally.
* **Network Segmentation**: Properly segment the network to limit lateral movement for attackers. In this case, improper network segmentation was cited as a reason for the compromise.
* **Security Patching**: Keep all systems and software up-to-date with the latest security patches to protect against known vulnerabilities.
* **Implement Multi-Factor Authentication (MFA):** MFA can add an extra layer of security to prevent unauthorized access even if credentials are compromised.
* **Incident Response Plan:** Develop and regularly update an incident response plan to guide actions in the event of a cyberattack. This should include communication protocols and steps for data recovery.
* **Cybersecurity Audits:** Regularly conduct cybersecurity audits and vulnerability assessments to identify and address weaknesses in the infrastructure.
* **Collaboration with CERT-In and Law Enforcement:** Cooperate with cybersecurity agencies like CERT-In and law enforcement agencies to investigate and respond to cyberattacks effectively.
* **Implement Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):** These can help detect and block malicious activities in real-time.

## ****CYBER SECURITY ARCHITECTURE IN INDIA LEGAL FRAMEWORK****

**INFORMATION TECHNOLOGY ACT,2000**

* The provisions of the IT Act deal with evidentiary value of electronic transactions, digital signatures, cyber-crimes, cyber security and data protection.
* It intends to give legal recognition to e-commerce and e-governance and facilitate its development as an alternate to paper based traditional methods.

**OTHER LAWS**

Several other laws complement the IT Act in governing cyberspace in India:

* Indian Contracts Act: Defines the legality of online contracts.
* Sale of Goods Act, 1930: Addresses the sale of goods in online transactions.
* Competition Act, 2002: Addresses competition-related issues in cyberspace.
* Consumer Protection Act, 1986: Protects consumer rights in online transactions.
* Indian Copyright Act: Protects intellectual property rights in the digital domain.
* Trade Marks Act: Provides protection for trademarks in cyberspace.

**National Cyber Security Policy, 2013:**

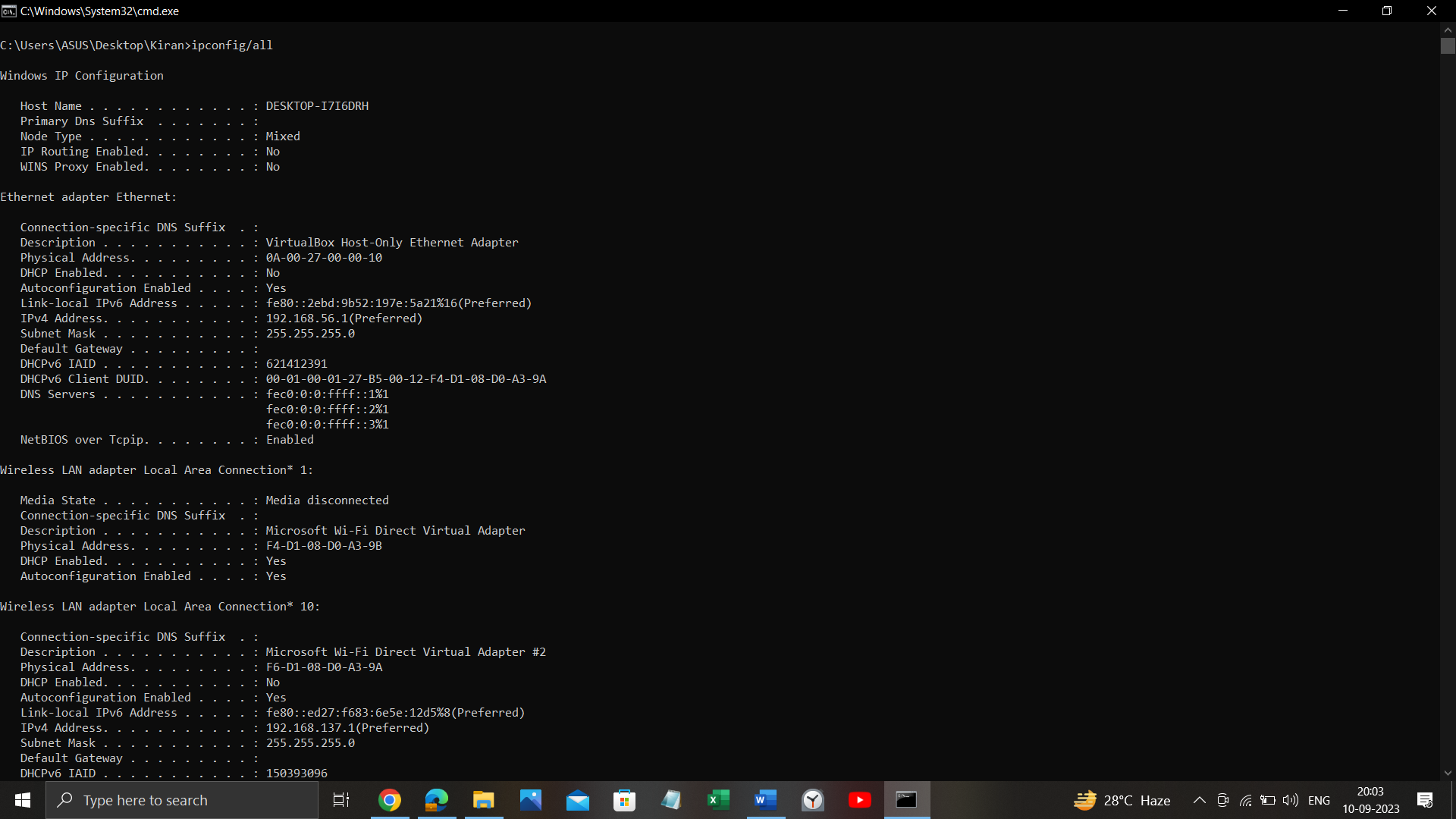
* **Purpose**: The National Cyber Security Policy outlines a comprehensive framework to address cybersecurity issues in India.
* **Vision**: To establish a secure and resilient cyberspace for citizens, businesses, and the government.
* **Mission**: To protect information and information infrastructure, build cybersecurity capacities, reduce vulnerabilities, and minimize damage from cyber incidents.
* **Important Features:**
* Creation of a secure cyber ecosystem to generate trust in IT transactions.
* Establishment of the National Critical Information Infrastructure Protection Center (NCIIPC) to monitor and protect critical infrastructure.
* Promotion of indigenous technological solutions to reduce reliance on foreign software.
* Testing and certification of ICT products to ensure security.
* Focus on building a skilled cybersecurity workforce.
* Fiscal incentives for businesses adopting standard IT practices.
* Following are some cyber laws cybercrime and stalking



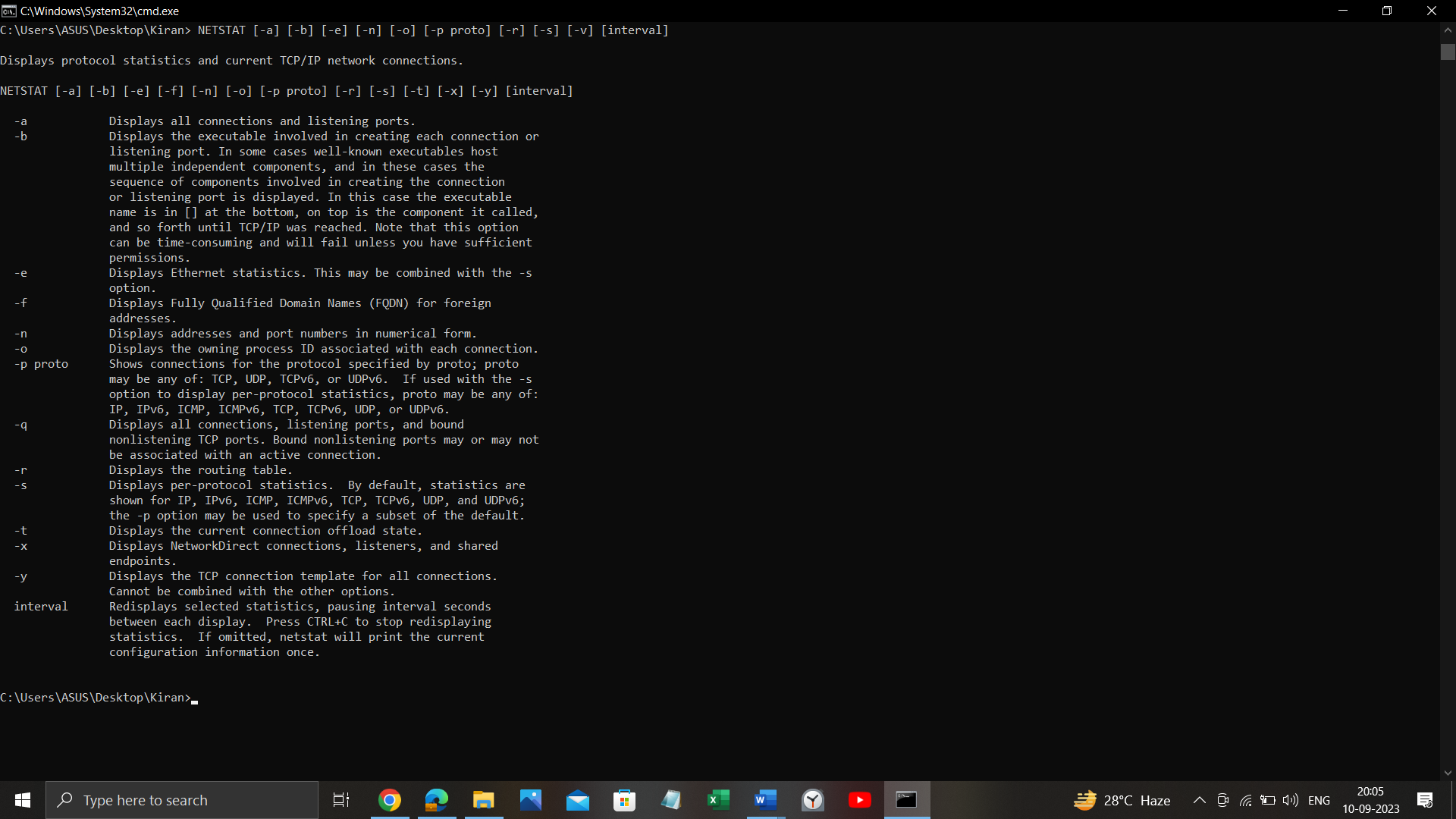
The Conclusion : Cyber-attacks and Ransomware-attacks reflect the still-inadequate protection measures afforded to critical information infrastructure in India. The government needs to step up its data protection efforts through additional measures if it is to prevent such frequent cyberattacks. The absence of awareness of cyber risks among the users and the use of old, legacy technologies are among the factors that add to the vulnerabilities. India also needs to study the evolving tactics, techniques, and procedures (TTPs) of hackers and criminals to be able to prevent these attacks

**Ipconfig** : This command is used in Windows operating systems to display information about the computer's network configuration. It provides details such as the computer's IP address, subnet mask, default gateway, and other network-related information. This command is valuable for troubleshooting network connectivity issues and verifying network settings.

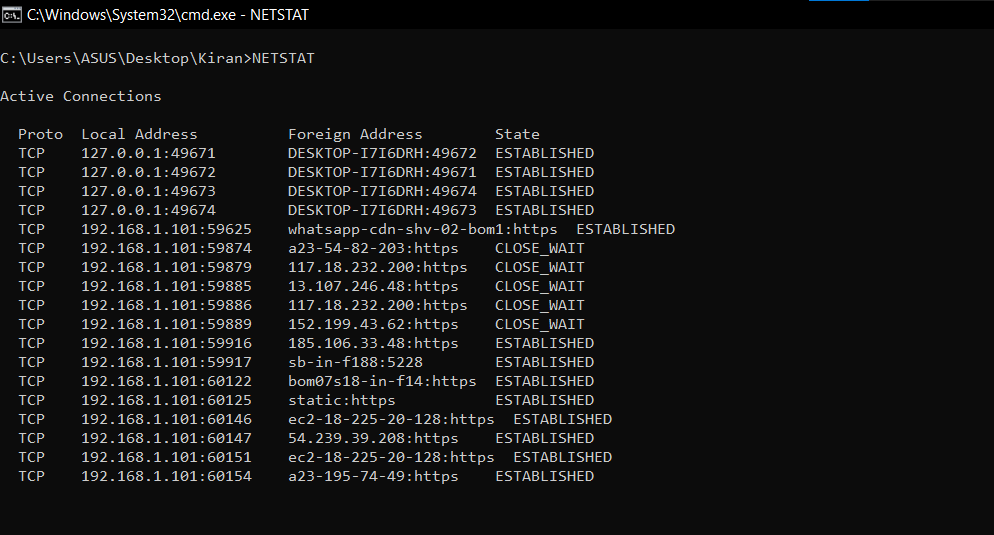
1. ipconfig



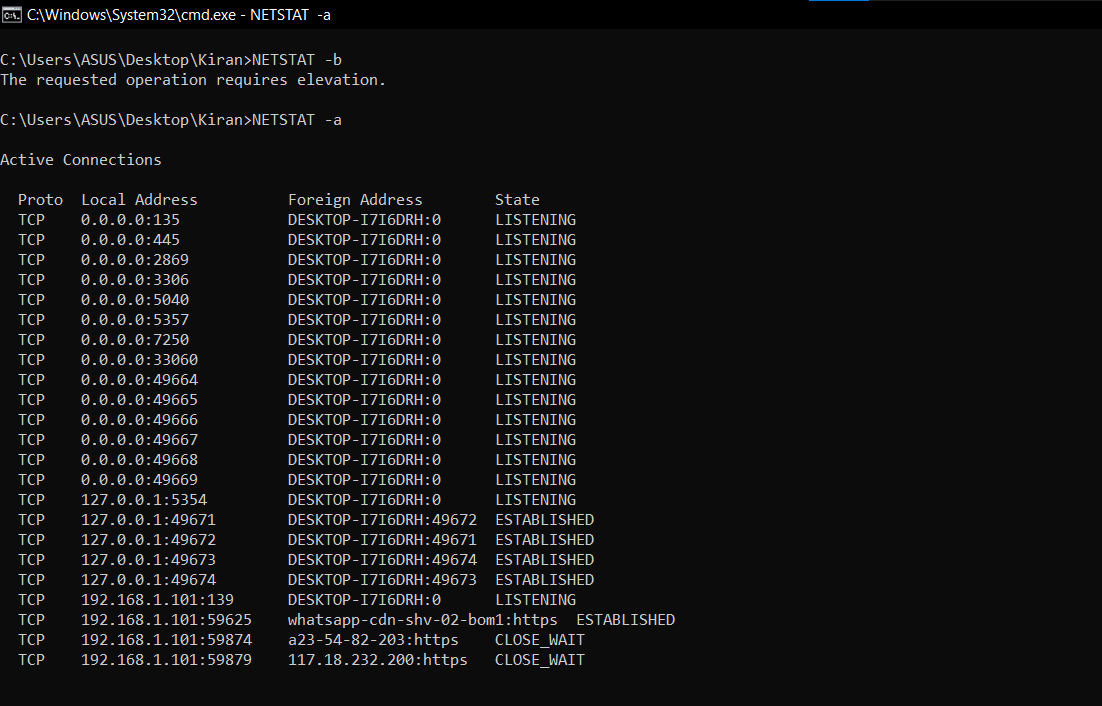
2. **NETSTAT** : The NETSTAT command, short for "Network Statistics," is a command-line utility available in various operating systems, including Windows and Unix-like systems (e.g., Linux). It is used to display network-related information and statistics about network connections, routing tables, and network interfaces on a computer.



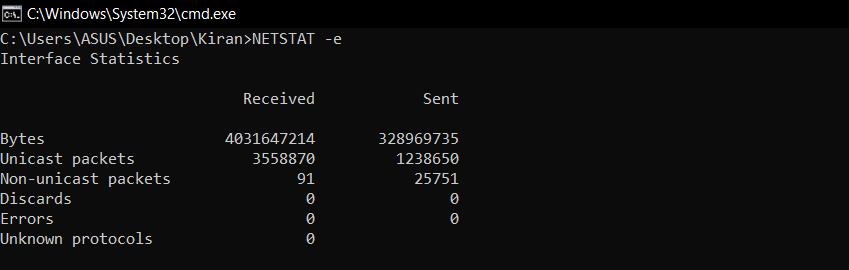
**NETSTAT [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]**



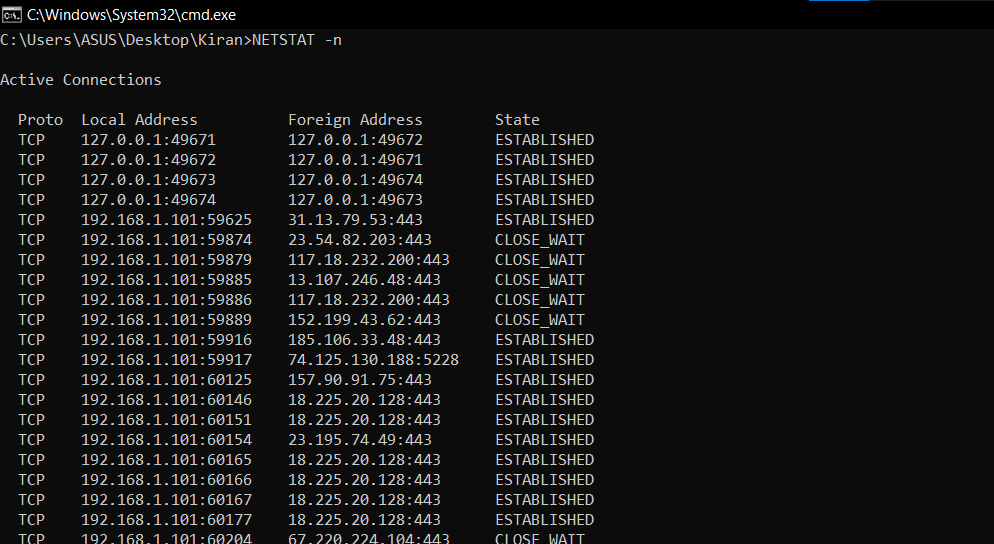
NETSTAT -b



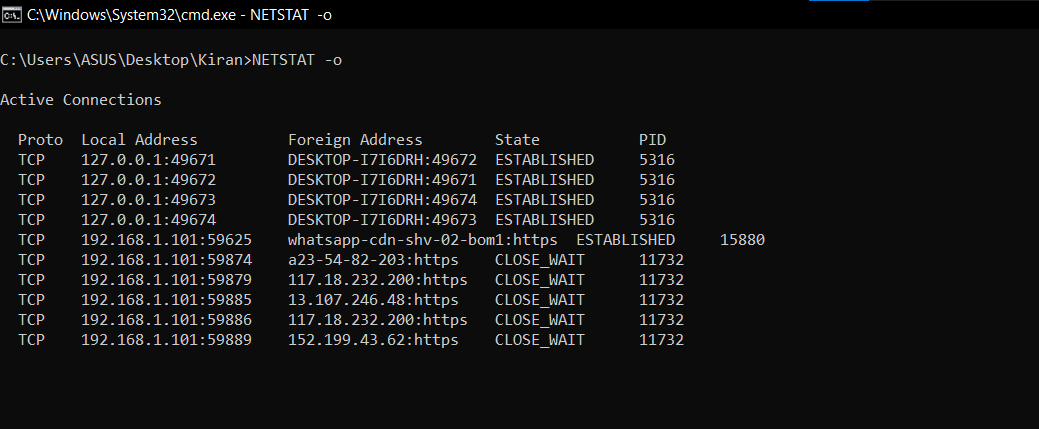
NETSTAT -e



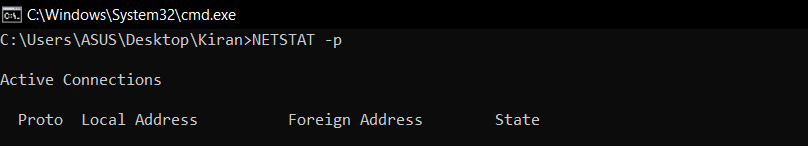
NETSTAT -n



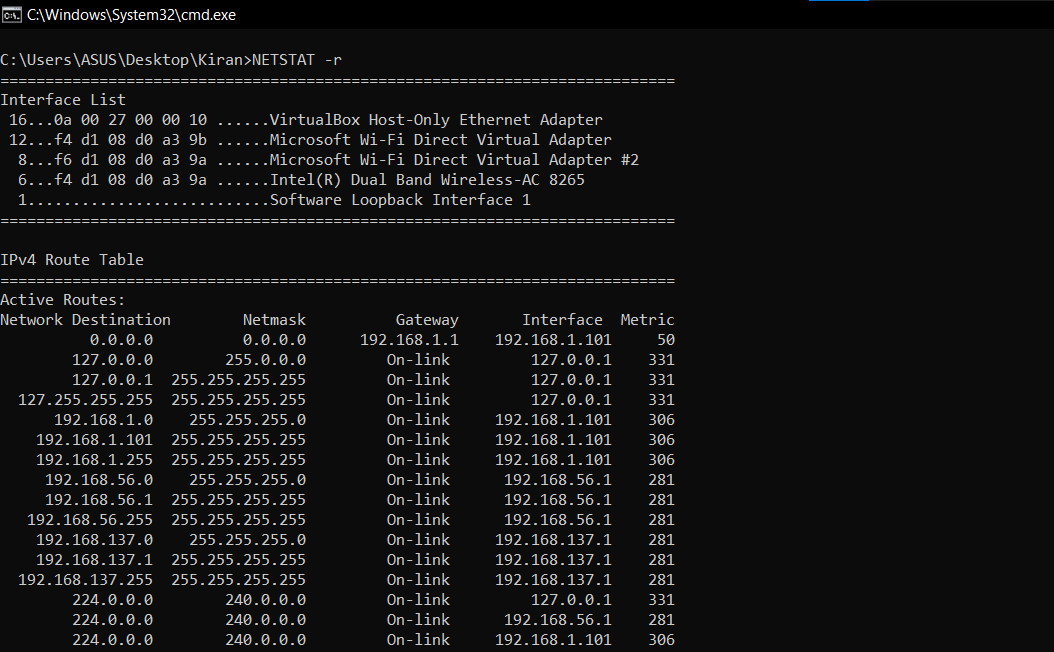
NETSTAT -o



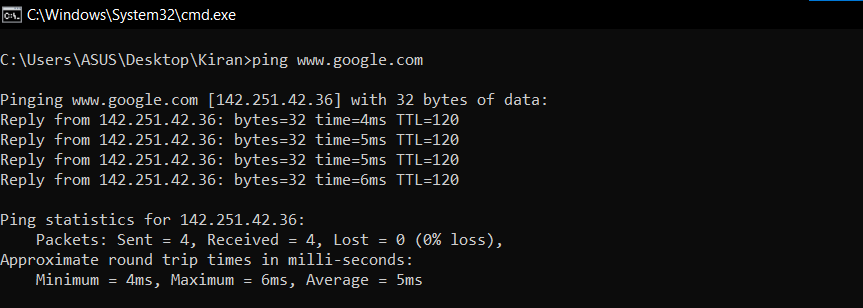
NETSTAT -p



NETSTAT -r

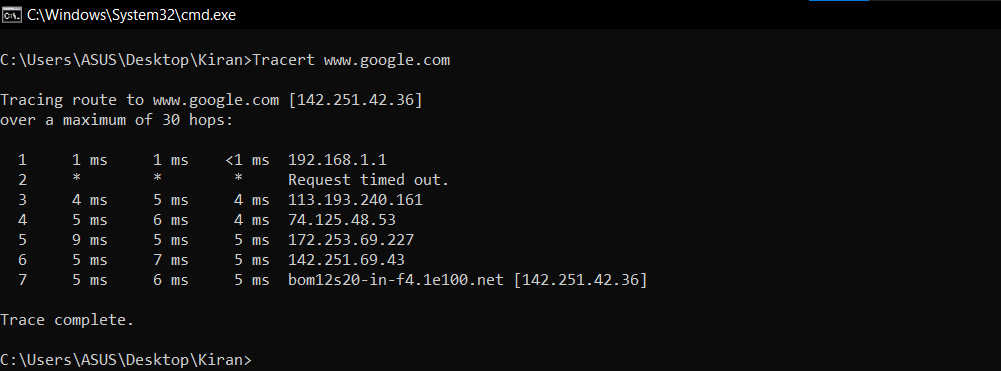


**Ping** : Ping is A command-line utility that assesses network connectivity by sending packets to a remote host and measuring the time it takes for responses to return. It's a fundamental tool for diagnosing network issues, determining if a server or website is online, and gauging network performance by providing real-time feedback on response times and potential packet loss.

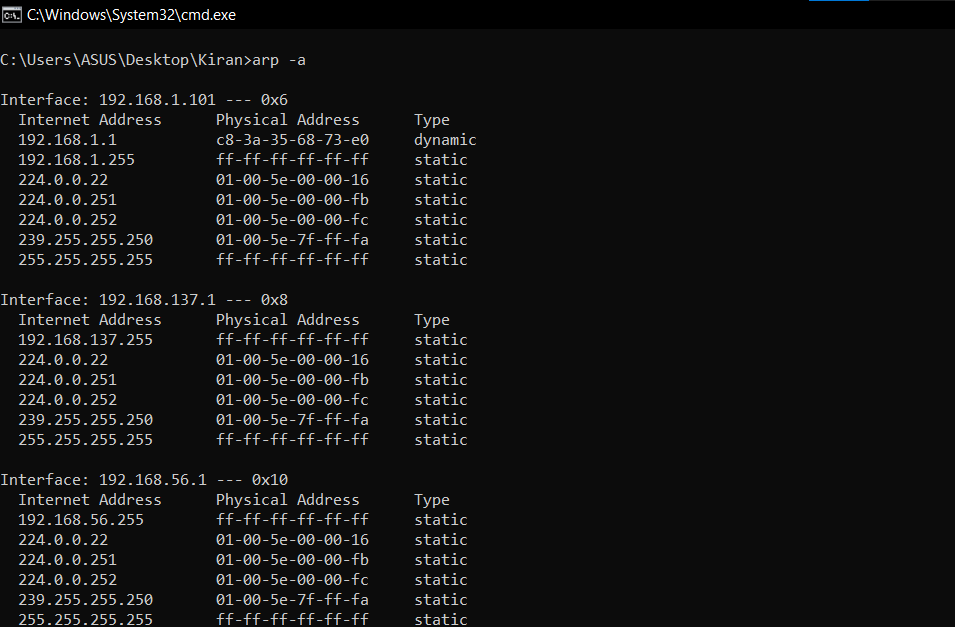


**tracert** : The tracert command is one of the key diagnostic tools for TCP/IP. It displays a list of all the routers that a packet must go through to get from the computer where tracert is run to any other computer on the Internet.

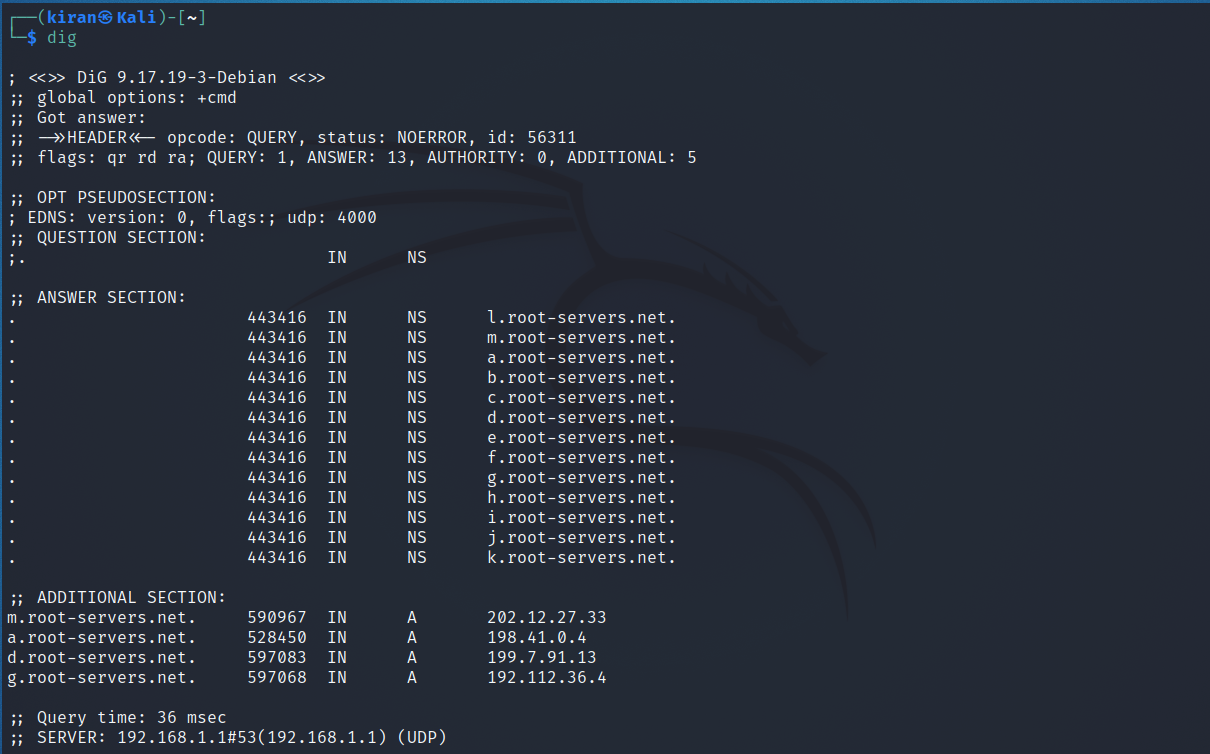
The tracert command is a Command Prompt command that's used to show several details about the path that a packet takes from the computer or device you're on to whatever destination you specify. You might also sometimes see the tracert command referred to as the trace route command or traceroute command.

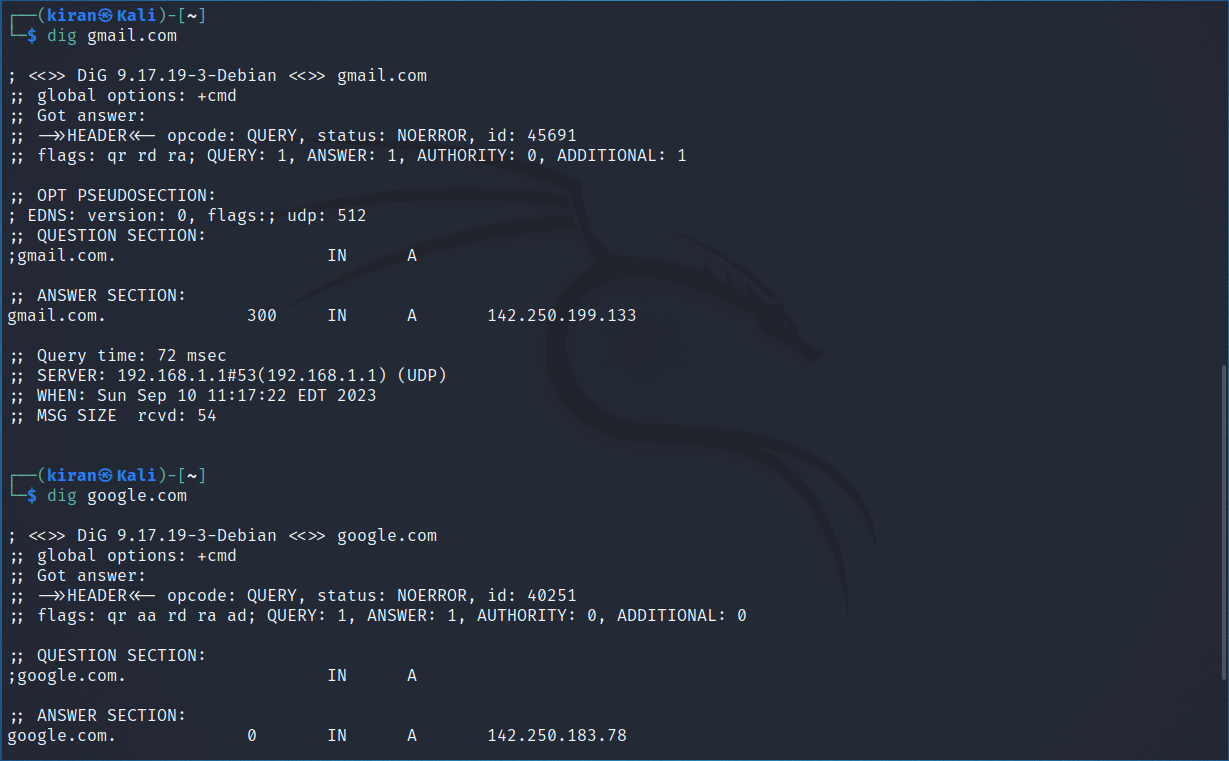


**Arp -a :** The arp -a command is used in Windows command prompt or PowerShell to display the ARP (Address Resolution Protocol) cache table for the local computer. The ARP cache contains a list of IP addresses and their corresponding physical MAC (Media Access Control) addresses that the computer has recently communicated with on the local network.

Executing arp -a will provide a list of these cached entries, showing the IP addresses and their associated MAC addresses. This information is helpful for troubleshooting network issues, verifying network connections, and checking the hardware addresses of devices on the local network.

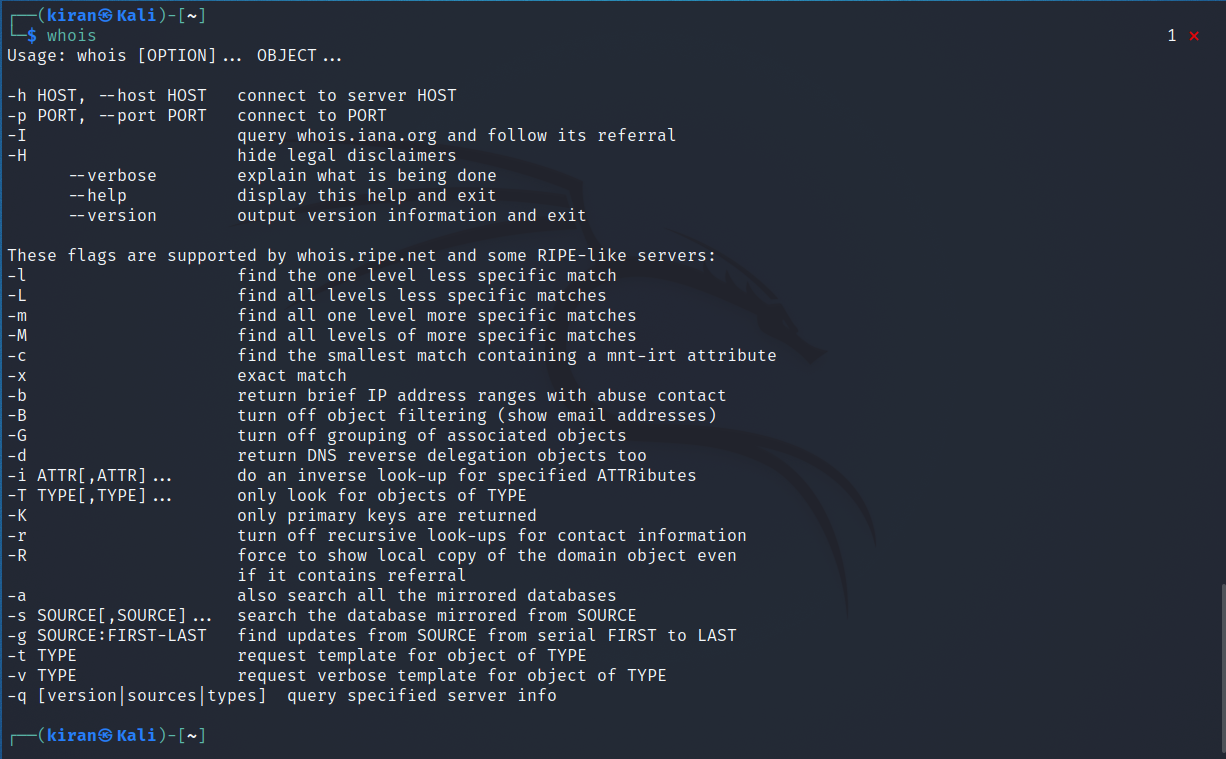
**Dig :** dig command stands for Domain Information Groper. It is used for retrieving information about DNS name servers. It is basically used by network administrators. It is used for verifying and troubleshooting DNS problems and to perform DNS lookups. Dig command replaces older tools such as nslookup and the host.

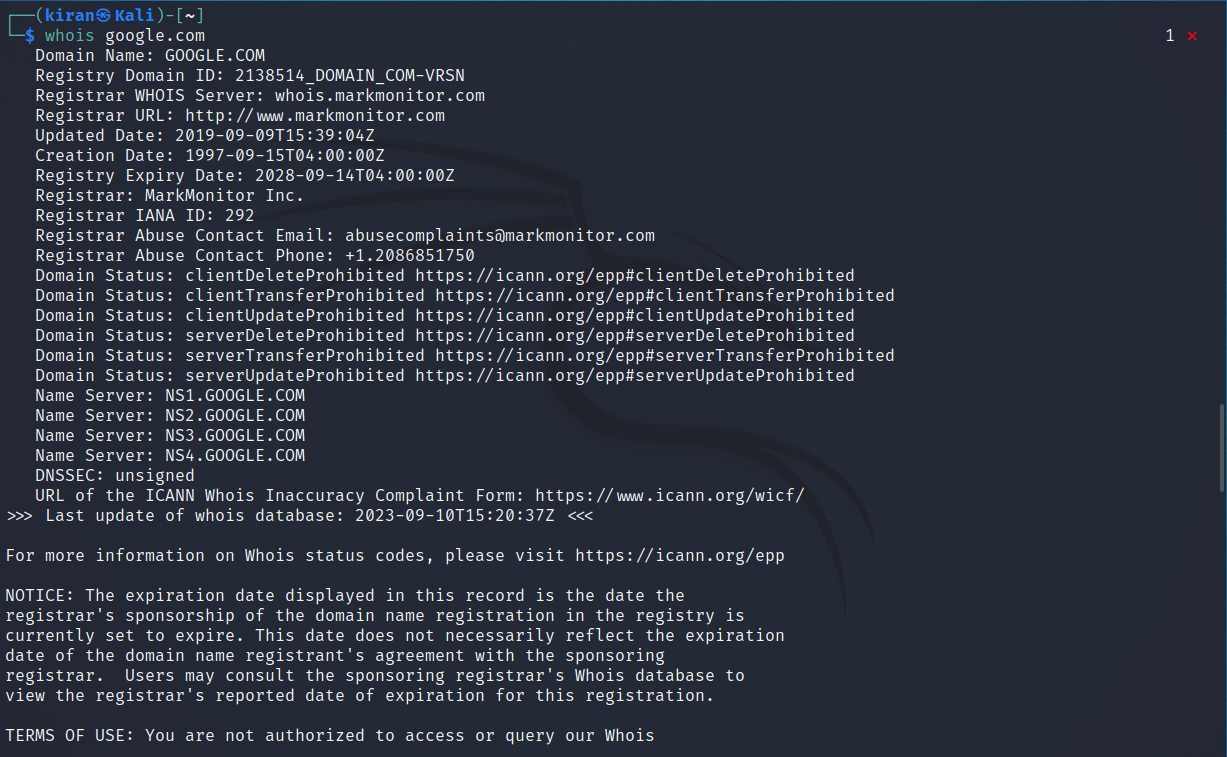




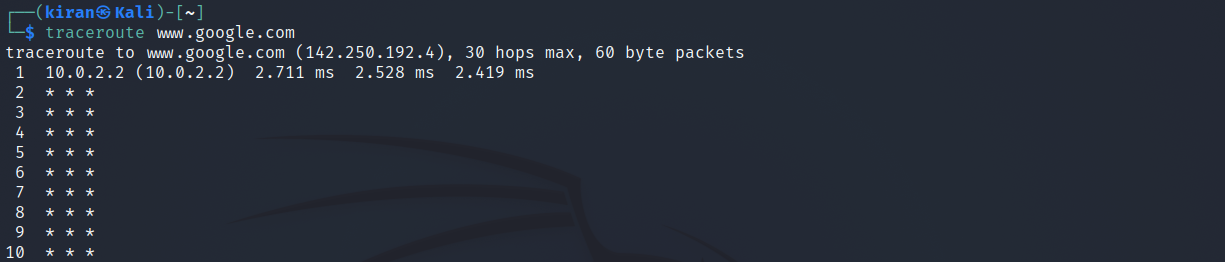
The **whois** command is a network utility used to retrieve detailed information about domain names, IP addresses, and network resources from a WHOIS database. When you execute the **whois** command followed by a domain name or IP address, it queries a WHOIS server to provide information such as:

1. **Domain Ownership**: For domain names, it reveals details about the domain registrar, domain owner's contact information, and registration and expiration dates.
2. **IP Address Information**: For IP addresses, it can display information about the allocation of the IP range, the organization that owns the IP address, and the contact information of the network administrator.
3. **Name Servers**: It shows the authoritative name servers associated with a domain





**traceroute** : In Linux, the **traceroute** command is used to trace the route that packets take from your computer to a specified destination host or IP address on a network. It helps you identify the path that network traffic follows, including the IP addresses of intermediate routers or hops and the round-trip time for each hop. This command is often used for diagnosing network connectivity issues and identifying network bottlenecks.



# **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 cyber attack on AIIMS 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.