



## **Veermata Jijabai Technological Institute, Mumbai 400019**

**Experiment No.:** 01

**Aim:** Cyber Crime

**Group :** Kiran Patil - 211070904  
Mayuresh Murudkar - 211070903  
Pratiksha Sankhe – 201070

**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.

### 2. 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.

### 3. 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

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 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

```
C:\Windows\System32\cmd.exe
C:\Users\ASUS\Desktop\Kiran>ipconfig/all

Windows IP Configuration

Host Name . . . . . : DESKTOP-I7IGORH
Primary Dns Suffix . . . . . :
Node Type . . . . . : Mixed
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Description . . . . . : VirtualBox Host-Only Ethernet Adapter
Physical Address. . . . . : 0A-00-27-00-00-10
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::2ebd:9b52:197e:5a21%16(Preferred)
IPv4 Address. . . . . : 192.168.56.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 621412391
DHCPv6 Client DUID. . . . . : 00-01-00-01-27-85-00-12-F4-D1-08-00-A3-9A
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. . . . . : F4-D1-08-00-A3-9B
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 10:

Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : F6-D1-08-00-A3-9A
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::ed27:f683:6e5e:12d5%8(Preferred)
IPv4 Address. . . . . : 192.168.137.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 150393896
```

**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.

```
C:\Windows\System32\cmd.exe
C:\Users\ASUS\Desktop\Kiran>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    Redisplay selected statistics, pausing interval seconds
           between each display. Press CTRL-C to stop redisplaying
           statistics. If omitted, netstat will print the current
           configuration information once.

C:\Users\ASUS\Desktop\Kiran>
```

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

```
C:\Windows\System32\cmd.exe - NETSTAT

C:\Users\ASUS\Desktop\Kiran>NETSTAT

Active Connections

   Proto Local Address           Foreign Address         State
   TCP    127.0.0.1:49671         DESKTOP-I7I6DRH:49672  ESTABLISHED
   TCP    127.0.0.1:49672         DESKTOP-I7I6DRH:49671  ESTABLISHED
   TCP    127.0.0.1:49673         DESKTOP-I7I6DRH:49674  ESTABLISHED
   TCP    127.0.0.1:49674         DESKTOP-I7I6DRH:49673  ESTABLISHED
   TCP    192.168.1.101:59625     whatsapp-cdn-shv-02-bom1:https ESTABLISHED
   TCP    192.168.1.101:59874     a23-54-82-203:https     CLOSE_WAIT
   TCP    192.168.1.101:59879     117.18.232.200:https     CLOSE_WAIT
   TCP    192.168.1.101:59885     13.107.246.48:https     CLOSE_WAIT
   TCP    192.168.1.101:59886     117.18.232.200:https     CLOSE_WAIT
   TCP    192.168.1.101:59889     152.199.43.62:https     CLOSE_WAIT
   TCP    192.168.1.101:59916     185.106.33.48:https     ESTABLISHED
   TCP    192.168.1.101:59917     sb-in-f188:5228         ESTABLISHED
   TCP    192.168.1.101:60122     bom07s18-in-f14:https   ESTABLISHED
   TCP    192.168.1.101:60125     static:https             ESTABLISHED
   TCP    192.168.1.101:60146     ec2-18-225-20-128:https ESTABLISHED
   TCP    192.168.1.101:60147     54.239.39.208:https     ESTABLISHED
   TCP    192.168.1.101:60151     ec2-18-225-20-128:https ESTABLISHED
   TCP    192.168.1.101:60154     a23-195-74-49:https     ESTABLISHED
```

## NETSTAT -b

```
C:\Windows\System32\cmd.exe - NETSTAT -a

C:\Users\ASUS\Desktop\Kiran>NETSTAT -b
The requested operation requires elevation.

C:\Users\ASUS\Desktop\Kiran>NETSTAT -a

Active Connections

   Proto Local Address           Foreign Address         State
   TCP    0.0.0.0:135             DESKTOP-I7I6DRH:0       LISTENING
   TCP    0.0.0.0:445             DESKTOP-I7I6DRH:0       LISTENING
   TCP    0.0.0.0:2869            DESKTOP-I7I6DRH:0       LISTENING
   TCP    0.0.0.0:3306            DESKTOP-I7I6DRH:0       LISTENING
   TCP    0.0.0.0:5040            DESKTOP-I7I6DRH:0       LISTENING
   TCP    0.0.0.0:5357            DESKTOP-I7I6DRH:0       LISTENING
   TCP    0.0.0.0:7250            DESKTOP-I7I6DRH:0       LISTENING
   TCP    0.0.0.0:33060           DESKTOP-I7I6DRH:0       LISTENING
   TCP    0.0.0.0:49664           DESKTOP-I7I6DRH:0       LISTENING
   TCP    0.0.0.0:49665           DESKTOP-I7I6DRH:0       LISTENING
   TCP    0.0.0.0:49666           DESKTOP-I7I6DRH:0       LISTENING
   TCP    0.0.0.0:49667           DESKTOP-I7I6DRH:0       LISTENING
   TCP    0.0.0.0:49668           DESKTOP-I7I6DRH:0       LISTENING
   TCP    0.0.0.0:49669           DESKTOP-I7I6DRH:0       LISTENING
   TCP    127.0.0.1:5354          DESKTOP-I7I6DRH:0       LISTENING
   TCP    127.0.0.1:49671         DESKTOP-I7I6DRH:49672  ESTABLISHED
   TCP    127.0.0.1:49672         DESKTOP-I7I6DRH:49671  ESTABLISHED
   TCP    127.0.0.1:49673         DESKTOP-I7I6DRH:49674  ESTABLISHED
   TCP    127.0.0.1:49674         DESKTOP-I7I6DRH:49673  ESTABLISHED
   TCP    192.168.1.101:139       DESKTOP-I7I6DRH:0       LISTENING
   TCP    192.168.1.101:59625     whatsapp-cdn-shv-02-bom1:https ESTABLISHED
   TCP    192.168.1.101:59874     a23-54-82-203:https     CLOSE_WAIT
   TCP    192.168.1.101:59879     117.18.232.200:https     CLOSE_WAIT
```

## NETSTAT -e

```
C:\Windows\System32\cmd.exe
C:\Users\ASUS\Desktop\Kiran>NETSTAT -e
Interface Statistics
```

	Received	Sent
Bytes	4031647214	328969735
Unicast packets	3558870	1238650
Non-unicast packets	91	25751
Discards	0	0
Errors	0	0
Unknown protocols	0	

## NETSTAT -n

```
C:\Windows\System32\cmd.exe
C:\Users\ASUS\Desktop\Kiran>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	127.0.0.1:49673	127.0.0.1:49674	ESTABLISHED
TCP	127.0.0.1:49674	127.0.0.1:49673	ESTABLISHED
TCP	192.168.1.101:59625	31.13.79.53:443	ESTABLISHED
TCP	192.168.1.101:59874	23.54.82.203:443	CLOSE_WAIT
TCP	192.168.1.101:59879	117.18.232.200:443	CLOSE_WAIT
TCP	192.168.1.101:59885	13.107.246.48:443	CLOSE_WAIT
TCP	192.168.1.101:59886	117.18.232.200:443	CLOSE_WAIT
TCP	192.168.1.101:59889	152.199.43.62:443	CLOSE_WAIT
TCP	192.168.1.101:59916	185.106.33.48:443	ESTABLISHED
TCP	192.168.1.101:59917	74.125.130.188:5228	ESTABLISHED
TCP	192.168.1.101:60125	157.90.91.75:443	ESTABLISHED
TCP	192.168.1.101:60146	18.225.20.128:443	ESTABLISHED
TCP	192.168.1.101:60151	18.225.20.128:443	ESTABLISHED
TCP	192.168.1.101:60154	23.195.74.49:443	ESTABLISHED
TCP	192.168.1.101:60165	18.225.20.128:443	ESTABLISHED
TCP	192.168.1.101:60166	18.225.20.128:443	ESTABLISHED
TCP	192.168.1.101:60167	18.225.20.128:443	ESTABLISHED
TCP	192.168.1.101:60177	18.225.20.128:443	ESTABLISHED
TCP	192.168.1.101:60204	67.220.224.104:443	CLOSE_WAIT

## NETSTAT -o

```
C:\Windows\System32\cmd.exe - NETSTAT -o
C:\Users\ASUS\Desktop\Kiran>NETSTAT -o
Active Connections
```

Proto	Local Address	Foreign Address	State	PID
TCP	127.0.0.1:49671	DESKTOP-I7I6DRH:49672	ESTABLISHED	5316
TCP	127.0.0.1:49672	DESKTOP-I7I6DRH:49671	ESTABLISHED	5316
TCP	127.0.0.1:49673	DESKTOP-I7I6DRH:49674	ESTABLISHED	5316
TCP	127.0.0.1:49674	DESKTOP-I7I6DRH:49673	ESTABLISHED	5316
TCP	192.168.1.101:59625	whatsapp-cdn-shv-02-bom1:https	ESTABLISHED	15880
TCP	192.168.1.101:59874	a23-54-82-203:https	CLOSE_WAIT	11732
TCP	192.168.1.101:59879	117.18.232.200:https	CLOSE_WAIT	11732
TCP	192.168.1.101:59885	13.107.246.48:https	CLOSE_WAIT	11732
TCP	192.168.1.101:59886	117.18.232.200:https	CLOSE_WAIT	11732
TCP	192.168.1.101:59889	152.199.43.62:https	CLOSE_WAIT	11732

## NETSTAT -p

```
C:\Windows\System32\cmd.exe
C:\Users\ASUS\Desktop\Kiran>NETSTAT -p

Active Connections

Proto Local Address          Foreign Address         State
```

## NETSTAT -r

```
C:\Windows\System32\cmd.exe
C:\Users\ASUS\Desktop\Kiran>NETSTAT -r

=====
Interface List
16...0a 00 27 00 00 10 .....VirtualBox Host-Only Ethernet Adapter
12...f4 d1 08 d0 a3 9b .....Microsoft Wi-Fi Direct Virtual Adapter
8...f6 d1 08 d0 a3 9a .....Microsoft Wi-Fi Direct Virtual Adapter #2
6...f4 d1 08 d0 a3 9a .....Intel(R) Dual Band Wireless-AC 8265
1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination    Netmask          Gateway         Interface      Metric
0.0.0.0                0.0.0.0          192.168.1.1     192.168.1.101  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
192.168.1.0            255.255.255.0    On-link         192.168.1.101  306
192.168.1.101          255.255.255.255  On-link         192.168.1.101  306
192.168.1.255          255.255.255.255  On-link         192.168.1.101  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
192.168.137.0          255.255.255.0    On-link         192.168.137.1  281
192.168.137.1          255.255.255.255  On-link         192.168.137.1  281
192.168.137.255        255.255.255.255  On-link         192.168.137.1  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         192.168.1.101  306
```

**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.

```
C:\Windows\System32\cmd.exe
C:\Users\ASUS\Desktop\Kiran>ping www.google.com

Pinging www.google.com [142.251.42.36] with 32 bytes of data:
Reply from 142.251.42.36: bytes=32 time=4ms TTL=120
Reply from 142.251.42.36: bytes=32 time=5ms TTL=120
Reply from 142.251.42.36: bytes=32 time=5ms TTL=120
Reply from 142.251.42.36: bytes=32 time=6ms TTL=120

Ping statistics for 142.251.42.36:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 6ms, Average = 5ms
```

**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.

```
C:\Windows\System32\cmd.exe

C:\Users\ASUS\Desktop\Kiran>Tracert www.google.com

Tracing route to www.google.com [142.251.42.36]
over a maximum of 30 hops:

  1    1 ms    1 ms    <1 ms   192.168.1.1
  2    *        *        *       Request timed out.
  3    4 ms    5 ms    4 ms   113.193.240.161
  4    5 ms    6 ms    4 ms   74.125.48.53
  5    9 ms    5 ms    5 ms   172.253.69.227
  6    5 ms    7 ms    5 ms   142.251.69.43
  7    5 ms    6 ms    5 ms   bom12s20-in-f4.1e100.net [142.251.42.36]

Trace complete.

C:\Users\ASUS\Desktop\Kiran>
```

**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.

```
C:\Windows\System32\cmd.exe

C:\Users\ASUS\Desktop\Kiran>arp -a

Interface: 192.168.1.101 --- 0x6
    Internet Address      Physical Address         Type
    192.168.1.1           c8-3a-35-68-73-e0       dynamic
    192.168.1.255         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
    239.255.255.250       01-00-5e-7f-ff-fa       static
    255.255.255.255       ff-ff-ff-ff-ff-ff       static

Interface: 192.168.137.1 --- 0x8
    Internet Address      Physical Address         Type
    192.168.137.255       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
    239.255.255.250       01-00-5e-7f-ff-fa       static
    255.255.255.255       ff-ff-ff-ff-ff-ff       static

Interface: 192.168.56.1 --- 0x10
    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
    239.255.255.250       01-00-5e-7f-ff-fa       static
    255.255.255.255       ff-ff-ff-ff-ff-ff       static
```

**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.

```
(kiran@Kali)-[~]
$ dig

; <<>> DiG 9.17.19-3-Debian <<>>
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 56311
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
; .                IN      NS

;; ANSWER SECTION:
.                443416 IN      NS      l.root-servers.net.
.                443416 IN      NS      m.root-servers.net.
.                443416 IN      NS      a.root-servers.net.
.                443416 IN      NS      b.root-servers.net.
.                443416 IN      NS      c.root-servers.net.
.                443416 IN      NS      d.root-servers.net.
.                443416 IN      NS      e.root-servers.net.
.                443416 IN      NS      f.root-servers.net.
.                443416 IN      NS      g.root-servers.net.
.                443416 IN      NS      h.root-servers.net.
.                443416 IN      NS      i.root-servers.net.
.                443416 IN      NS      j.root-servers.net.
.                443416 IN      NS      k.root-servers.net.

;; ADDITIONAL SECTION:
m.root-servers.net. 590967 IN      A      202.12.27.33
a.root-servers.net. 528450 IN      A      198.41.0.4
d.root-servers.net. 597083 IN      A      199.7.91.13
g.root-servers.net. 597068 IN      A      192.112.36.4

;; Query time: 36 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
```

```
(kiran@Kali)-[~]
$ dig gmail.com

; <<>> DiG 9.17.19-3-Debian <<>> gmail.com
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 45691
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
; gmail.com.       IN      A

;; ANSWER SECTION:
gmail.com.         300     IN      A      142.250.199.133

;; Query time: 72 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Sun Sep 10 11:17:22 EDT 2023
;; MSG SIZE rcvd: 54
```

```
(kiran@Kali)-[~]
$ dig google.com

; <<>> DiG 9.17.19-3-Debian <<>> google.com
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 40251
;; flags: qr aa rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
; google.com.      IN      A

;; ANSWER SECTION:
google.com.        0       IN      A      142.250.183.78
```



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

```
(kiran@Kali)-[~]
$ whois
Usage: whois [OPTION]... OBJECT...

-h HOST, --host HOST    connect to server HOST
-p PORT, --port PORT    connect to PORT
-I                      query whois.iana.org and follow its referral
-H                      hide legal disclaimers
    --verbose           explain what is being done
    --help              display this help and exit
    --version           output version information and exit

These flags are supported by whois.ripe.net and some RIPE-like servers:
-l                      find the one level less specific match
-L                      find all levels less specific matches
-m                      find all one level more specific matches
-M                      find all levels of more specific matches
-c                      find the smallest match containing a mnt-irt attribute
-x                      exact match
-b                      return brief IP address ranges with abuse contact
-B                      turn off object filtering (show email addresses)
-G                      turn off grouping of associated objects
-d                      return DNS reverse delegation objects too
-i ATTR[,ATTR]...      do an inverse look-up for specified ATTRibutes
-T TYPE[,TYPE]...      only look for objects of TYPE
-K                      only primary keys are returned
-r                      turn off recursive look-ups for contact information
-R                      force to show local copy of the domain object even
                        if it contains referral
-a                      also search all the mirrored databases
-s SOURCE[,SOURCE]...  search the database mirrored from SOURCE
-g SOURCE:FIRST-LAST   find updates from SOURCE from serial FIRST to LAST
-t TYPE                request template for object of TYPE
-v TYPE                request verbose template for object of TYPE
-q [version|sources|types] query specified server info

(kiran@Kali)-[~]
```

```
(kiran@Kali)-[~]
$ whois google.com
Domain Name: GOOGLE.COM
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T15:39:04Z
Creation Date: 1997-09-15T04:00:00Z
Registry Expiry Date: 2028-09-14T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-09-10T15:20:37Z <<<
```



**tracert** : In Linux, the **tracert** 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.

```
(kiran@kali)-[~]
$ tracert www.google.com
tracert to www.google.com (142.250.192.4), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  2.711 ms  2.528 ms  2.419 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
```

## 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 accesstools 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
<u>S0552</u>	<u>AdFind</u>	<u>AdFind</u> has the ability to query Active Directory for computers.
<u>G0016</u>	<u>APT29</u>	<u>APT29</u> has used <u>AdFind</u> to enumerate remote systems.
<u>G0022</u>	<u>APT3</u>	<u>APT3</u> has a tool that can detect the existence of remote systems.
<u>G0050</u>	<u>APT32</u>	<u>APT32</u> has enumerated DC servers using the command netgroup "Domain Controllers" /domain. The group has also used the ping command
<u>G0087</u>	<u>APT39</u>	<u>APT39</u> has used <u>NBTscan</u> and custom tools to discover remote systems.
<u>S0534</u>	<u>Bazar</u>	<u>Bazar</u> can enumerate remote systems using Net View.
<u>S0570</u>	<u>BitPaymer</u>	<u>BitPaymer</u> can use net view to discover remote systems.
<u>S0521</u>	<u>BloodHound</u>	<u>BloodHound</u> can enumerate and collect the properties of domain computers, including domain controllers.
<u>G0060</u>	<u>BRONZE BUTLER</u>	<u>BRONZE BUTLER</u> typically use ping and Net to enumerate systems.
<u>S0335</u>	<u>Carbon</u>	<u>Carbon</u> uses the net view command.
<u>G0114</u>	<u>Chimera</u>	<u>Chimera</u> has utilized various scans and queries to find domain controllers and remote services in the target environment.
<u>S0154</u>	<u>Cobalt Strike</u>	<u>Cobalt Strike</u> uses the native Windows Network Enumeration APIs to interrogate and discover targets in a Windows Active Directory network.
<u>S0244</u>	<u>Comnie</u>	<u>Comnie</u> runs the net view command
<u>S0488</u>	<u>CrackMapExec</u>	<u>CrackMapExec</u> can discover active IP addresses, along with the machine name, within a targeted network.
<u>G0009</u>	<u>Deep Panda</u>	<u>Deep Panda</u> has used ping to identify other machines of interest.
<u>G0074</u>	<u>Dragonfly 2.0</u>	<u>Dragonfly 2.0</u> likely obtained a list of hosts in the victim environment.
<u>S0091</u>	<u>Epic</u>	<u>Epic</u> uses the net view command on the victim's machine.
<u>G0053</u>	<u>FIN5</u>	<u>FIN5</u> has used the open source tool Essential NetTools to map the network and build a list of targets.
<u>G0037</u>	<u>FIN6</u>	<u>FIN6</u> 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.
<u>G0061</u>	<u>FIN8</u>	<u>FIN8</u> uses dsquery and other Active Directory utilities to enumerate hosts.
<u>G0117</u>	<u>Fox Kitten</u>	<u>Fox Kitten</u> 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 netview 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. <sup>[46]</sup>
G0034	Sandworm Team	Sandworm Team has used a tool to query ActiveDirectory 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. <sup>[48]</sup>
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 netview 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 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.