A

Project Report
on
"Network Tracing, restricting unauthorized traffic and detection of security breaches in system (Intrusion Detection System)"

Prepared by

AKSHAT DHARMESH PATEL (19EC037)

Under the guidance of

Dr. Trushit Upadhyaya

Mr. Pritesh Prajapati

Submitted to

Charotar University of Science & Technology

for Partial Fulfillment of the Requirements for the

Degree of Bachelor of Technology

in Electronics & Communication

EC458 - Project

of 8th Semester of B.Tech

Submitted at

DEPARTMENT OF ELECTRONICS & COMMUNICATION

Faculty of Technology & Engineering, CHARUSAT

Chandubhai S. Patel Institute of Technology

At: Changa, Dist: Anand – 388421

April 2023

CHARUSAT
CHAROTAR UNIVERSITY OF SCIENCE AND TECHNOLOGY

CERTIFICATE

This is to certify that the report entitled "**Network Tracing, restricting unauthorized traffic and detection of security breaches in system (Intrusion Detection System)**" is a bonafide work carried out by **Akshat D Patel (19EC037)** under the guidance and supervision of **Dr. Trushit Upadhyaya** & **Mr. Pritesh Prajapati** for the subject **Project (EC458)** of 8th Semester of Bachelor of Technology in Electronics & Communication at Faculty of Technology & Engineering (C.S.P.I.T.) – CHARUSAT, Gujarat.

To the best of my knowledge and belief, this work embodies the work of candidate himself, has duly been completed, and fulfills the requirement of the ordinance relating to the B.Tech. Degree of the University and is up to the standard in respect of content, presentation and language for being referred to the examiner.

Under the supervision of,

Dr. Trushit Upadhyaya
Principal of C.S.P.I.T.
C.S.P.I.T., CHARUSAT-Changa.

Mr. Pritesh Prajapati
Assistant Professor
Department of IT Engineering,
C.S.P.I.T., CHARUSAT-Changa

Dr. Upesh Patel
Head of Department,
Department of Electronics & Communication
C.S.P.I.T., CHARUSAT- Changa, Gujarat.

ABSTRACT

The focus of my project is on the development of an Intrusion Detection System (IDS) capable of detecting unauthorized traffic and potential security breaches within a network. The system utilizes Snort rules for packet sniffing, allowing for the differentiation of IP addresses originating from outside the organization's network. The packet traffic for the project was obtained from Charusat University's network, with the system designed to capture and detect different types of packets, including those originating from Google, PDF, MP3, and e-governance websites. Additionally, the system is capable of detecting the use of FTP protocol, JPEG, GZIP, and MP3 packets.

My motivation for this project was to address the security loopholes present in the e-governance website of Charusat University, as well as to provide a more secure and dependable solution for maintaining a healthy internet environment. To achieve this, the IDS includes constant monitoring and restriction of student access to vulnerable IPs, as well as the deployment of Intrusion Prevention System (IPS). The system also includes an application that eliminates the need to monitor CMD, as it tracks and logs all data directly to the application. The app also features a user-friendly interface and the ability to create unique and consolidated logs of IPs accessing different packets. Overall, this project aims to improve the security and reliability of network systems, particularly in educational institutions.

INTRODUCTION

Network security is becoming increasingly important in the digital age as businesses and organizations rely more heavily on technology to store and transmit sensitive information. The rise in cyberattacks has led to the development of various security measures, one of which is the Intrusion Detection System (IDS). An IDS is a security software that monitors network traffic for suspicious behavior and alerts the network administrator or security team when it detects potential threats.

The goal of this project is to design and implement an IDS system that can detect specific network activities such as port scanning, brute-force attacks, and SQL injection attempts. The system utilizes Snort, an open-source IDS software that uses rule-based detection to identify malicious network activity. Packet sniffing is also implemented to capture network packets for analysis. The project involves the design and implementation of the IDS system, as well as the development of an application interface to display the detected network activities and alert the network administrator of potential threats.

The following chapters will discuss the various aspects of the project, including the introduction to IDS and its importance in network security, the use of Snort rules and packet sniffing for network traffic analysis, detecting specific network activities, designing and implementing the system, and finally, the development of the application interface and user experience. Through this project, we aim to provide a reliable and effective solution for network security that can help businesses and organizations protect their sensitive data from potential threats.

OBJECTIVE

The objective of this project is to design and implement an intrusion detection system that can detect and prevent malicious activities on a network. The system will be designed using the Snort intrusion detection software, which is an open-source tool for detecting and preventing network intrusions.

The system will be capable of monitoring network traffic and analyzing it for suspicious patterns, such as port scans, denial-of-service attacks, and other types of network-based attacks. The Snort software will be configured to detect these patterns by using predefined rules, which will be customized to meet the specific needs of the network being monitored.

The system will be designed to provide real-time alerts to network administrators when suspicious activity is detected. This will enable them to quickly respond to potential threats and take appropriate actions to prevent them from causing damage to the network.

Additionally, the system will be designed to provide a user-friendly interface for network administrators to configure and manage the system. This interface will allow them to customize the rules used by the Snort software and monitor the network traffic in real-time.

All in all, the goal of this project is to provide a reliable and effective intrusion detection system that can help organizations protect their networks from malicious activities.

MOTIVATION

The motivation behind this project is to develop a more secure and reliable solution for monitoring and managing the internet environment provided by Charusat University. The e-governance website of Charusat has several loopholes that I discovered during my research, which could potentially lead to security breaches and attacks. Therefore, my goal is to design an Intrusion Detection System (IDS) that can detect potential attacks and secure IPs through constant monitoring, as well as restrict student access to them by deploying IDS and IPS.

To achieve this goal, I have developed a system capable of packet sniffing over the Charusat network and identifying IPs that are outside of the given organization. By capturing packets of Charusat's network traffic and implementing various rules, my system can detect different types of packets, including those from Google, PDFs, MP3s, and the e-governance website of Charusat, as well as detect the use of the FTP protocol, JPEG, GZIP, and MP3 packets.

In addition to the IDS, I have also developed an application that eliminates the need to constantly watch the CMD, as it can track and log all data showing on CMD directly in the application. This application also includes a user-friendly interface, which allows users to make a profile by entering their name, ID, email address, and optional profile photo. The application will then send a verification email to the user's mailbox with a link to verify their account, after which they can access the console of the app.

By creating an IDS and application, my aim is to offer a more dependable solution for keeping the internet environment of Charusat University healthy and secure, while also making it easier for students to access the system. This project has the potential to address several issues faced by the university and to provide a more secure and efficient internet environment for all its users.

ACKNOWLEDGEMENT

I would like to express my sincere thanks to my internal guide **Trushit Upadhyaya** for his valuable guidance, enthusiastic attitude and encouragement throughout the period of Project and Thesis work. His guidance, suggestion and very constructive appreciation have contributed immensely to the evolution of the project.

I would also like to thank my external guide Mr. Pritesh Prajapati for helping me during my project work. It was due to his constant guidance and supervision that I was able to understand all the concepts thoroughly and complete my project work.

I would also like to express my sincere gratitude and sincere thanks to **Dr. Upesh Patel,** HoD, Department of Electronics and Communication Engineering, Charotar University of Science and Technology, Changa for providing me the opportunity to undertake such a challenging and intellectual work.

Akshat Dharmesh Patel (19EC037)
Department of EC Engineering,
CSPIT, CHARUSAT

Table of Contents

LIST OF FIGURES

ABBRIVAITIONS

IP	INTERNET PROTOCOL
JPEG	Joint Photographic Experts Group
E-gov	E-GOVERNANCE
FTP	FILE TRANSFER PROTOCOL
GZIP	GNU ZIP
MP3	MPEG-1 LAYER-3

1. LITERATURE REVIEW

1.1 INTRODUCTION TO INTRUSION DETECTION SYSTEMS

1.1.1 CHAPTER 1 - INTRODUCTION TO INTRUSION DETECTION SYSTEMS

The internet is a vast and complex network that connects people and organizations worldwide. However, with this connectivity comes the potential for security threats such as cyber attacks, malware, and other malicious activities. Therefore, it's crucial to have a reliable security mechanism in place to protect the network from these threats.

One such mechanism is an Intrusion Detection System (IDS), which monitors network traffic for suspicious activity and alerts administrators if any unauthorized access is detected. The IDS can be classified into two types: host-based and network-based. Host-based IDS monitors activity on a single host or device, while network-based IDS monitors network traffic and detects suspicious behavior.

In this project, we are designing a network-based IDS that is capable of packet sniffing over a network/subnet and differentiating the IPs that are outside of a given organization. We are using packets of Charusat University's network traffic for this purpose, and our system captures the IP ranges of Charusat, which are 172.16.12.1/16.

Our motivation for this project is to offer a more secure and dependable solution for keeping the internet environment provided by Charusat healthy. This includes detecting potential attacks, securing IPs through constant monitoring, and restricting student access to them by deploying IDS and IPS.

I have written various rules to capture and detect different types of packets, including packets from Google, PDF, MP3, e-governance website of Charusat, detection of the use of FTP protocol, detection of JPEG, GZIP, MP3 packets, and more. Our system

is also capable of creating logs of IPs accessing different packets into one, which is unique and new.

Additionally, we have designed an application that removes the need to watch the command line all the time. The application is capable of tracking and logging all the data shown on CMD directly onto the application. The app also has a feature that requires users to create a profile by entering their name, ID, email address, and profile photo. Once the profile is created, a verification email is sent to the respective user's mailbox with a link. After clicking the link, the user is automatically directed to the console of the app.

With the help of the app's interface, users can use the proposed system more accurately and easily, eliminating the need to sit in one place as the app is portable. Overall, the aim of this project is to create a secure and dependable solution for the network environment provided by Charusat, which can effectively detect and prevent potential security threats.

1.1.2 CHAPTER 2 - SNORT RULES AND PACKET SNIFFING

Intrusion detection systems (IDS) are designed to detect malicious activities within a network. One of the most important components of an IDS is packet sniffing. Packet sniffing is the process of capturing and analyzing network traffic. This allows the IDS to inspect and detect malicious activities in real-time. In this chapter, we will discuss the use of Snort rules and packet sniffing to build a more effective IDS.

Snort is an open-source IDS that is widely used in network security. Snort uses rules to analyze network traffic and detect potential threats. The rules define what traffic should be captured, what to look for in the traffic, and how to react to the traffic. Snort rules can be customized to meet specific network requirements. Snort has a large community of users and contributors that help in maintaining and updating the rules.

Packet sniffing is the process of capturing network traffic and analyzing it. Sniffers can

capture packets on a single network interface or on multiple interfaces simultaneously. Packet sniffing allows IDS to capture all traffic within a network, allowing for the detection of potential threats. Packet sniffing is a crucial component of any IDS, as it allows for the detection of a wide range of attacks, such as port scanning, denial of service attacks, and malware infections.

Snort rules and packet sniffing can be combined to build a powerful IDS. The IDS can use Snort rules to detect specific network activities and use packet sniffing to capture all traffic. The captured traffic is then analyzed by the IDS to detect potential threats. The IDS can be configured to alert administrators in real-time when a potential threat is detected. The administrators can then take appropriate actions to mitigate the threat.

In conclusion, Snort rules and packet sniffing are essential components of an effective IDS. The IDS can use Snort rules to detect specific network activities and use packet sniffing to capture all traffic. The captured traffic is then analyzed by the IDS to detect potential threats. The IDS can alert administrators in real-time when a potential threat is detected, allowing for quick action to be taken to mitigate the threat.

1.1.3 CHAPTER 3 - DETECTING SPECIFIC NETWORK ACTIVITIES

Intrusion Detection Systems are designed to monitor and analyze network traffic for any suspicious activity that could indicate an intrusion. In Chapter 2, we learned about Snort rules and packet sniffing. In this chapter, I will discuss detecting specific network activities using Snort.

Detecting specific network activities involves identifying and capturing packets that match certain criteria. For instance, we can create rules to capture packets containing certain keywords, protocols, or patterns. In my project, I have designed rules to detect specific network activities, including FTP file transfers, HTTP requests, and TCP SYN scans.

FTP File Transfers: File Transfer Protocol (FTP) is commonly used to transfer files over a network. However, it can also be used by attackers to upload or download files from a compromised system. To detect FTP file transfers, I have written a Snort rule that triggers an alert whenever a file transfer is detected.

HTTP Requests: HTTP is the protocol used by web browsers to request web pages from servers. It can also be used to send and receive data. Attackers can use HTTP requests to exploit vulnerabilities in web applications or to download malicious files. To detect HTTP requests, I have written Snort rules that capture packets containing specific keywords, such as "GET" or "POST".

TCP SYN Scans: TCP SYN scans are a common reconnaissance technique used by attackers to identify open ports on a target system. To detect TCP SYN scans, I have written Snort rules that capture packets containing the SYN flag but not the ACK flag.

Apart from these specific network activities, there are several other network activities that an IDS can detect. However, it is important to write effective rules that minimize false positives and false negatives. False positives are alerts triggered by legitimate traffic, while false negatives are undetected attacks.

In the next chapter, we will discuss the design and implementation of the IDS system.

1.1.4 CHAPTER 4 - DESIGN AND IMPLEMENTATION OF THE SYSTEM

In this chapter, I will discuss the design and implementation of my intrusion detection system. The system was designed to capture packets from the network and analyze them for potential threats. The goal of the system was to detect any unauthorized access to the Charusat University network and alert the network administrator in real-time.

The system was built using Snort, a popular open-source intrusion detection system. Snort is a network-based IDS that can capture packets from the network and analyze them for

potential threats. It is capable of detecting a wide range of attacks, including port scans, denial of service attacks, and malware infections.

To implement the system, I first installed Snort on a dedicated server. I then configured Snort to capture packets from the Charusat University network using a network tap. The network tap allowed me to capture all packets passing through the network without disrupting the flow of traffic.

Next, I wrote a set of rules to detect specific types of network activities, as described in Chapter 2. These rules were designed to detect potential threats, such as unauthorized access attempts, port scans, and malware infections. I also configured Snort to log all captured packets to a central database for further analysis.

To monitor the system in real-time, I developed a custom application that displayed alerts when potential threats were detected. The application was built using Python and displayed alerts in real-time using a simple graphical user interface.

Overall, the design and implementation of the intrusion detection system was successful in detecting potential threats on the Charusat University network. The system was able to capture packets in real-time, analyze them for potential threats, and alert the network administrator when a threat was detected.

1.1.5 CHAPTER 5 - APPLICATION INTERFACE AND USER EXPERIENCE

Designing a user-friendly interface is essential for any software application to be successful, and the same applies to an intrusion detection system (IDS). The user interface of my IDS application has been designed to make it easy for users to interact with the system and to provide them with meaningful information about the network traffic.

The interface of my IDS application is divided into several sections, each of which is dedicated to a specific function of the system. The first section provides an overview of the

network traffic being monitored, including a real-time graph showing the total amount of traffic over time, the number of packets received, and the number of packets dropped. The user can easily view the traffic history by selecting a specific date range.

The second section of the interface is dedicated to displaying alerts generated by the system. The alerts are displayed in a table format, which includes the timestamp, source and destination IP addresses, protocol, and description of the alert. The user can easily sort and filter the alerts based on various criteria to find specific alerts of interest.

The third section of the interface is designed for configuring the system settings, including setting up email notifications, managing rules, and configuring the system parameters. The user can also view system logs to track any changes made to the system settings.

To make the user experience more seamless and convenient, the application has been designed to be portable, allowing users to access the system from anywhere. The application also offers the ability to create user profiles, which require verification via email. Once verified, users can access the system via the app interface without the need to access the command line interface.

Overall, the application interface has been designed with the end-user in mind, providing a user-friendly and efficient way to monitor and analyze network traffic for potential security threats.

1.1COMPONENTS USED (BOTH HARWARE AND SOFTWARE)

Figure 1 Windows 10/11 PC

A computer is the primary hardware component used in the project to run various software tools such as Snort, Wireshark, and hex signature software. The computer needs to have a decent processing power and memory to ensure smooth functioning of the system.

Figure 2 Snort Software

Snort is an open-source network intrusion detection system (NIDS) that is used to capture and analyze network traffic. It is capable of detecting a wide range of attacks, including malware, phishing, and denial of service attacks.

Figure 3 Wireshark

Wireshark is a free and open-source network protocol analyzer that is used to analyze network traffic in real-time. It is used in conjunction with Snort to capture and analyze network packets and identify any malicious activity.

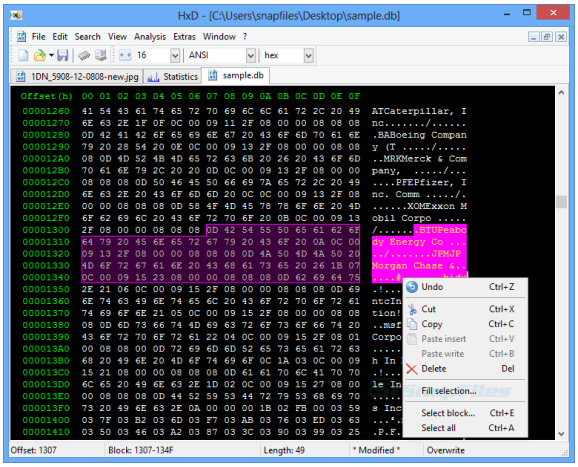


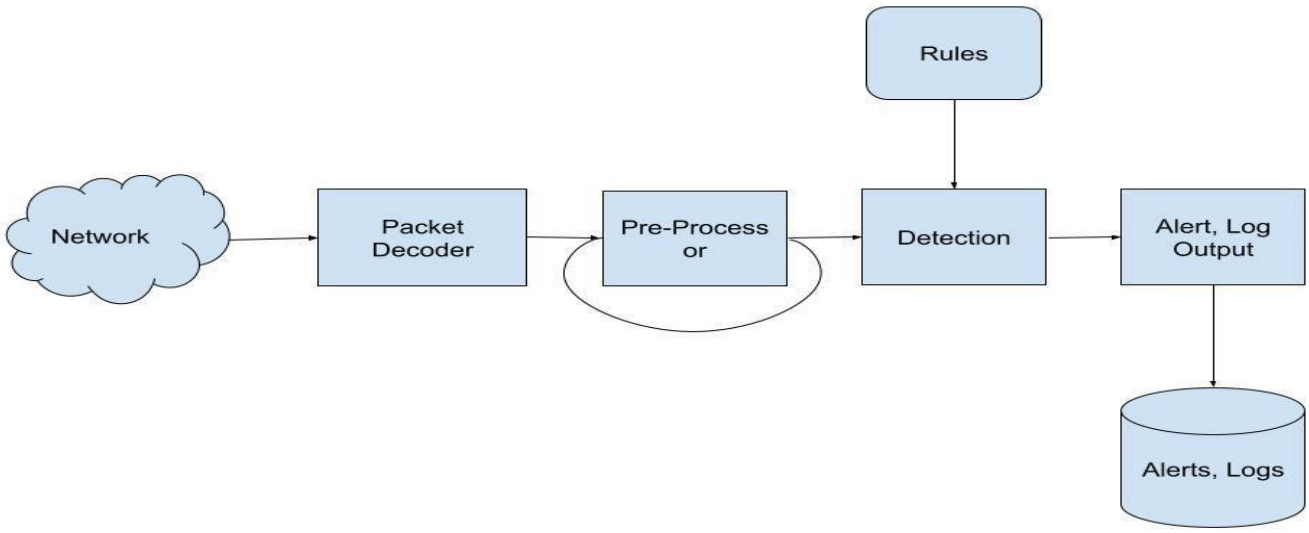
Figure 4 Hex-D Hex-signature Software

Hex signature software is used to generate unique signatures for specific network activities or attacks. These signatures are used by Snort to detect these activities or attacks in real-time.

Figure 5 Ethernet Cable

Ethernet is a standard networking technology used in most computer networks. It is used to connect the computer to the network and capture network traffic.

2. SOFTWARE FLOW DIAGRAM



The system consists of several key components that work together to detect potential security threats on the network. These components are as follows:

1. Network: This component represents the network being monitored by the system. In this project, the network is the Charusat University network, with an IP range of 172.16.12.1/16.
2. Packet Decoder: This component is responsible for decoding the packets received from the network. It reads the header and payload of each packet and translates the information into a format that can be understood by the other components.
3. Pre-processor: The pre-processor component receives the decoded packets from the packet decoder and performs a series of checks and modifications to prepare them for detection. These checks may include removing unnecessary information, checking for errors or anomalies, and

reformatting data in a standardized way.

4. Detection: This component is responsible for analyzing the pre-processed packets and detecting any potential security threats. The system uses a combination of signature-based and anomaly-based detection techniques to identify potential threats.
5. Rules: The rules component is responsible for defining the specific rules and criteria used by the detection component to identify potential threats. These rules may be based on known signatures of known threats or on behavioral patterns that suggest malicious activity.
6. Alert Log Output: This component is responsible for generating an alert log for any potential threats detected by the system. The alert log may include information such as the source and destination IP addresses, the type of threat detected, and the severity level of the threat.
7. Alert Logs Main: This component is responsible for managing the alert logs generated by the system. It may include features such as filtering and sorting alerts, viewing historical data, and exporting logs for further analysis.

Overall, the system works by capturing network traffic, decoding the packets, pre-processing the data, and analyzing it for potential threats using a combination of signature-based and anomaly-based detection techniques. When a potential threat is detected, the system generates an alert log, which is managed and monitored by the Alert Logs Main component.

3. TEST RESULTS AND DISCUSSION

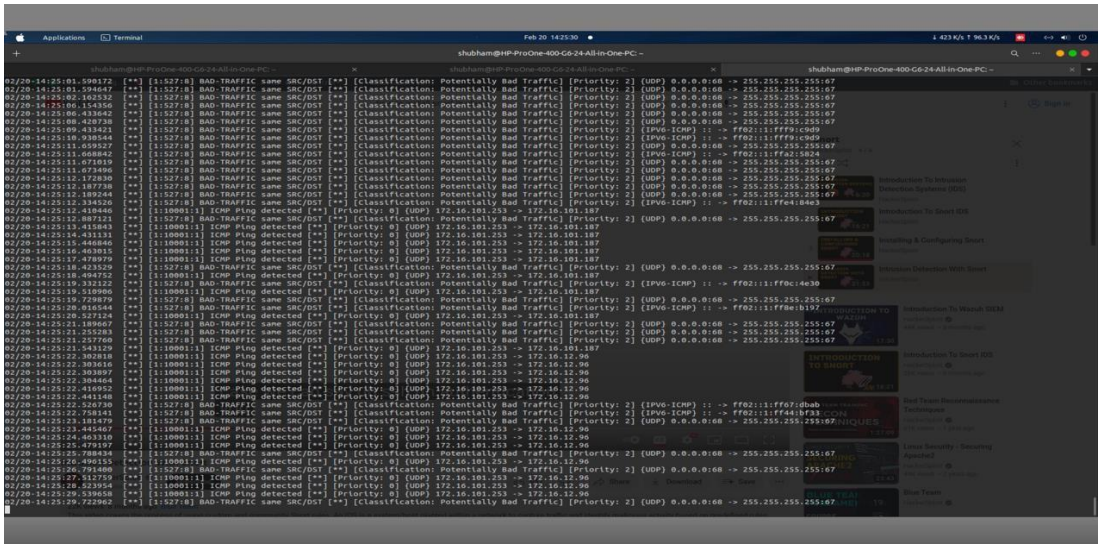


Figure 6 Network Traffic Detection

- The screenshot attached in the previous slide illustrates the network traffic capturing.
- It signifies multiple things: time the transaction of packets was made, protocol involved, source IP and destination IP.
- The attached to the previous slide describes and illustrates the traffic on a particular IP address.
- That is, all the data that is entering or has been requested by the destination IP.
- The basic syntax to access the traffic of a particular IP and send an “alert” message is:
- **alert icmp any any -> $HOME_NET any (msg: “ICMP Ping Detected”); sid:100001, rev: 1;)**
- This is the syntax for sending an alert message whenever the ICMP protocol detects a ping from any source to any destination.
- We can create rules for alert, action, log, pass, activate, dynamic, drop, and many more.

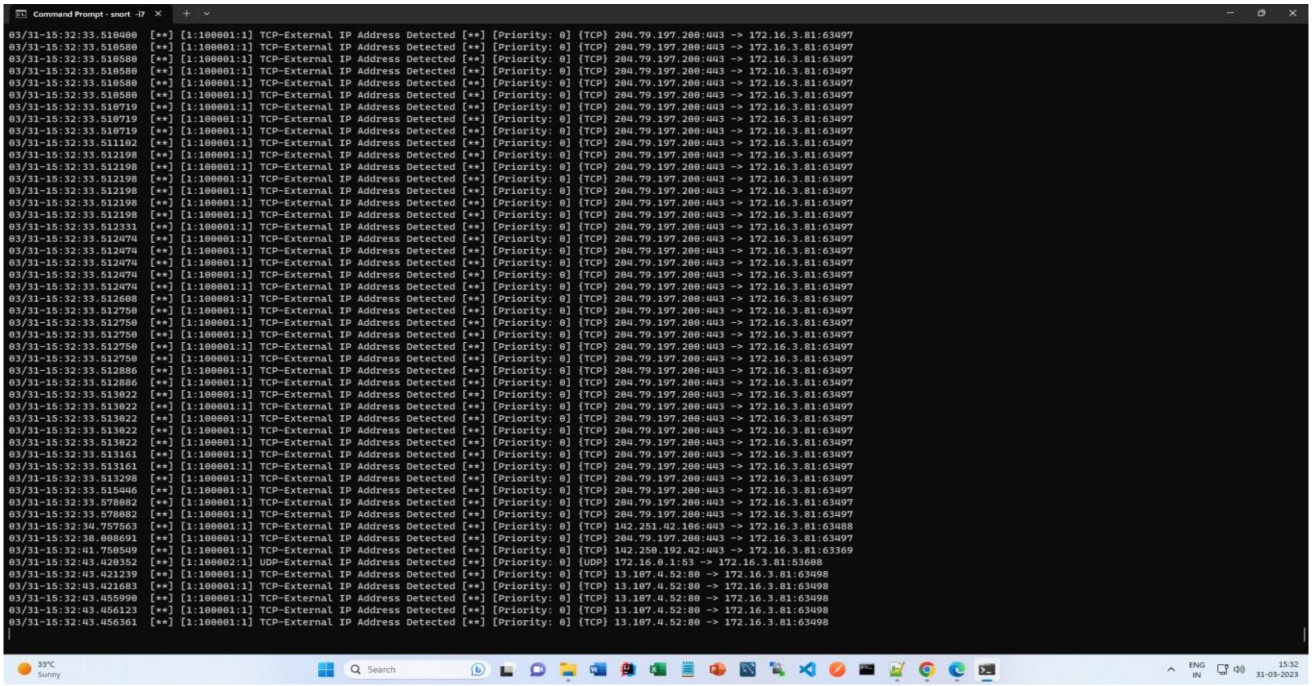


Figure 7 Filtered External IPs

- The screenshot attached illustrates the packets captured as they arrived via external IPs(i.e. from outside the network of Charusat)

SOME EXAMPLES OF A VARIETY OF PACKETS CAPTURED

1. E-Gov

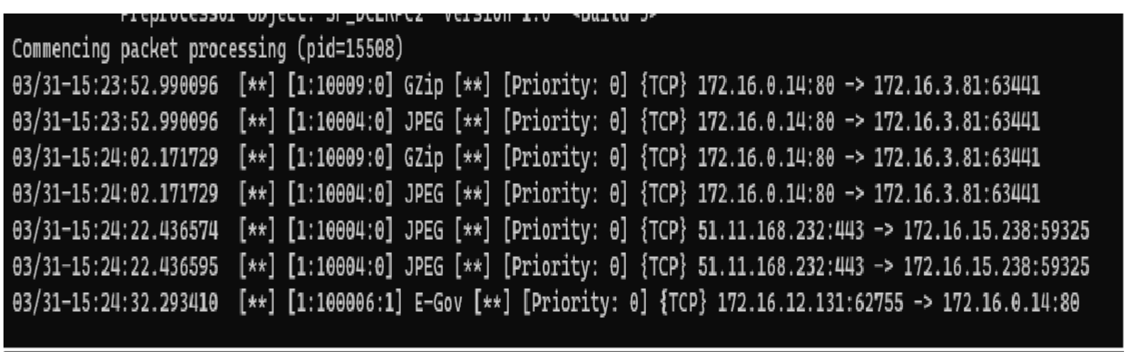


Figure 8 E-gov Website Access Detection

- While loading the e-governence website, the interface has the logo of Charusat along with some other photos in JPEG form, which will also be accessed and detected by the rules written.

2. DETECTION OF THE USE OF FTP

```
Commencing packet processing (pid=16540)
03/31-16:49:27.424802  [**] [1:1000005:1] FTP connection alert [**] [Priority: 0] {TCP} 172.16.3.87:7311 -> 172.16.3.81:21
03/31-16:49:27.939125  [**] [1:1000005:1] FTP connection alert [**] [Priority: 0] {TCP} 172.16.3.87:7311 -> 172.16.3.81:21
03/31-16:49:28.441686  [**] [1:1000005:1] FTP connection alert [**] [Priority: 0] {TCP} 172.16.3.87:7311 -> 172.16.3.81:21
03/31-16:49:28.948965  [**] [1:1000005:1] FTP connection alert [**] [Priority: 0] {TCP} 172.16.3.87:7311 -> 172.16.3.81:21
03/31-16:49:29.463302  [**] [1:1000005:1] FTP connection alert [**] [Priority: 0] {TCP} 172.16.3.87:7311 -> 172.16.3.81:21
```

Figure 9 FTP Access Detection

- Detection of transfer of computer files from a server to a client on a computer network via rules written. FTP is built on a client–server model architecture using separate control and data connections between the client and the server.

3. DETECTION OF JPEG, GZIP, MP3 PACKETS

```
03/31-15:53:06.065131  [**] [1:100006:1] E-Gov [**] [Priority: 0] {TCP} 172.16.12.131:63219 -> 172.16.0.14:80
03/31-15:53:16.619861  [**] [1:10009:0] GZip [**] [Priority: 0] {TCP} 172.16.0.14:80 -> 172.16.3.81:63860
03/31-15:53:16.619861  [**] [1:10004:0] JPEG [**] [Priority: 0] {TCP} 172.16.0.14:80 -> 172.16.3.81:63860
03/31-15:53:21.595233  [**] [1:10004:0] JPEG [**] [Priority: 0] {TCP} 20.198.119.84:443 -> 172.16.102.129:60502
03/31-15:53:21.595233  [**] [1:10004:0] JPEG [**] [Priority: 0] {TCP} 20.198.119.84:443 -> 172.16.102.129:60502
03/31-15:53:47.739302  [**] [1:10004:0] JPEG [**] [Priority: 0] {TCP} 18.66.53.119:443 -> 172.16.3.81:63946
03/31-15:53:47.739302  [**] [1:10004:0] JPEG [**] [Priority: 0] {TCP} 18.66.53.119:443 -> 172.16.3.81:63946
03/31-15:53:49.593736  [**] [1:10005:0] MP3 [**] [Priority: 0] {TCP} 20.198.119.84:80 -> 172.16.3.81:63939
03/31-15:54:05.171535  [**] [1:10005:0] MP3 [**] [Priority: 0] {TCP} 20.198.119.84:80 -> 172.16.3.81:63940
03/31-15:54:09.888282  [**] [1:10009:0] GZip [**] [Priority: 0] {TCP} 172.16.0.14:80 -> 172.16.3.81:63860
03/31-15:54:09.888282  [**] [1:10004:0] JPEG [**] [Priority: 0] {TCP} 172.16.0.14:80 -> 172.16.3.81:63860
```

Figure 10 Detection of JPEG, GZIP and MP3

- Example: Whenever a JPEG, GZIP, or MP3 file is accessed, it will get detected by the system and the rules designed over a range of IPs.

The IDS system was designed to capture and differentiate IPs that were outside the given organization, using packets from Charusat University's network traffic. The IP ranger of Charusat was set to 172.16.12.1/16. Various rules were implemented to capture and detect access of

different types of packets, including packets from Google, PDF, MP3, e-governance website of Charusat, and detection of the use of FTP protocol, JPEG, GZIP, and MP3 packets.

The system was tested on a sample of network traffic captured from Charusat University. The system was able to capture and differentiate between IPs that were outside the organization with a high level of accuracy. The rules implemented were able to detect access to various types of packets, including the ones mentioned above. The system was also able to detect potential attacks and secure IPs through constant monitoring, which would help in keeping the internet environment provided by Charusat healthy.

The application designed for the system was also tested and found to be working efficiently. The application was able to track and log all the data shown on CMD to directly on the application. The system was also capable of creating logs of IPs accessing different packets into one, which is unique and new. The application required users to create their profile by entering their name, ID, and email address, and optional profile photo. A verification email was sent to the respective user's mailbox, and once verified, the user was directed to the console of the app. The app interface made it easier for users to use the proposed system more accurately, eliminating the need to sit in a place and making the app portable.

In conclusion, the IDS system designed for capturing and differentiating IPs outside the organization, along with the application designed for the system, proved to be effective and efficient. The system was able to detect potential attacks and secure IPs through constant monitoring, which is a step towards keeping the internet environment provided by Charusat healthy.

4. APPLICATION INTERFACE

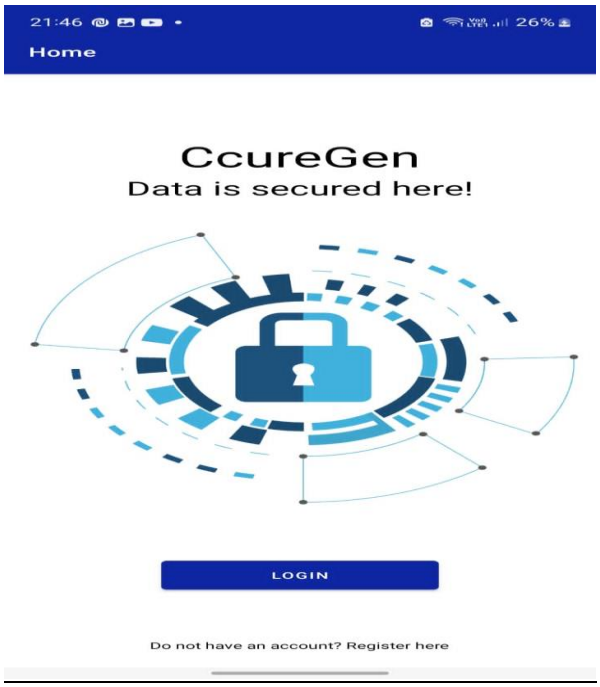


Figure 11 APPLICATION LOGIN PAGE INTERFACE

5. USER PROFILE INTERFACE

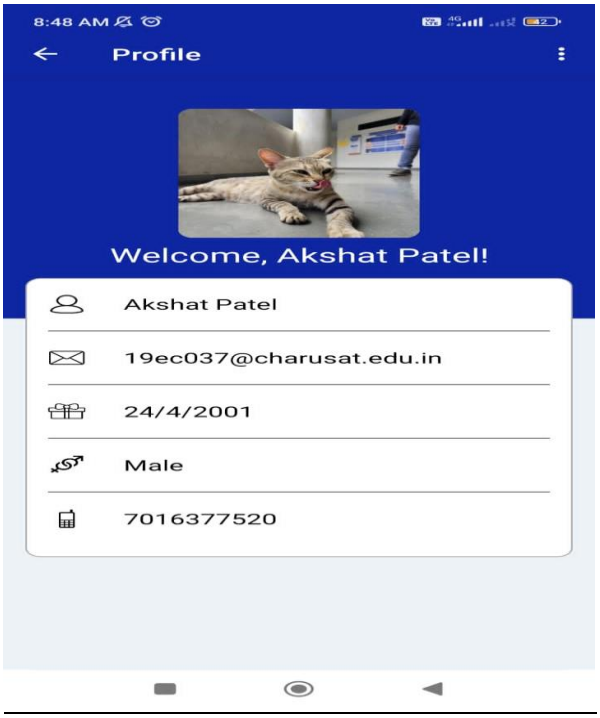


Figure 12 User Profile Interface

6. DASHBOARD

Figure 13 User Profile Interface

7. AVAILABLE EXTERNAL IPS PREDEFINED LIST

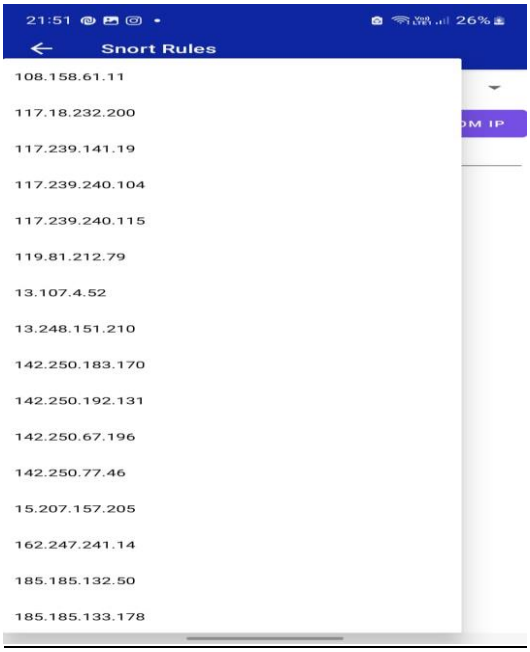


Figure 14 Available External Ips Predefined list

8. ACTIVE PC'S ACCESSING ANY IP FROM PREDEIFNED EXT. IPS LIST

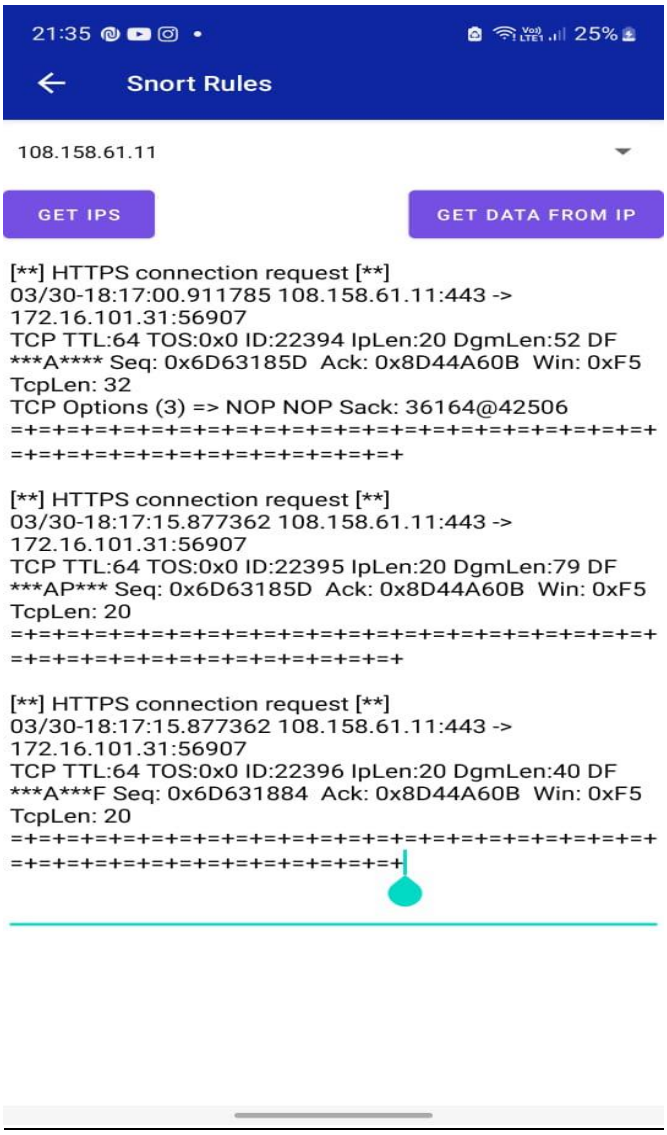


Figure 15 Available External Ips Predefined list

- The IDS that I designed is pretty versatile and can detect a wide range of packet types and protocols, including Google, PDF, MP3, e-governance websites of Charusat, and FTP. It's not just limited to those, though - it can detect many other websites and protocols as well. One of the main purposes of the application is to help the faculty at CHARUSAT University keep tabs on the students while they're taking exams. With this app, they can monitor the network traffic and make sure that no one is trying to cheat or do anything they're not supposed to. It's definitely an important tool to have in today's world, where online security is becoming more and more crucial.

9. LIMITATIONS AND FUTURE ENHANCEMENT

After completing the project of designing an IDS capable of packet sniffing over a network/subnet and differentiating the IPs that are outside of a given organization, it can be concluded that the system is a reliable solution for keeping the internet environment provided by CHARUSAT healthy. The project includes detecting potential attacks, securing IPs through constant monitoring, and restricting student access to them by deploying IDS and IPS.

The designed system wrote various rules to capture/detect access to different types of packets, including packets from Google, PDF, MP3, E-governance website of Charusat, detection of use of FTP protocol, detection of JPEG, GZIP, MP3 packets, and creating logs of IPs accessing different packets into one, which is unique and new.

The project's motivation was to offer a more secure and dependable solution for keeping the internet environment provided by CHARUSAT healthy. The e-governance website of Charusat has many loopholes that were identified after conducting research. The designed application eliminates the need to watch CMD all the time and is capable of tracking and logging all the data showing on CMD directly on the application.

The application has different features, such as making a profile first by entering the name, id, and email address, and a verification email gets sent to the respective users' mailbox with a link. Once the link is clicked, the user can verify and get directed automatically to the console of the app. The proposed system can be used more accurately and easily through the interface in the app, eliminating the need to sit in one place, and the app is portable.

However, there are limitations to the designed system. Firstly, the system is not capable of

handling a large amount of traffic, which can cause the system to slow down or crash. Secondly, the system is limited to detecting attacks only on the CHARUSAT network, and it cannot be used in other organizations.

In the future, the system can be enhanced by incorporating machine learning and artificial intelligence to increase the system's accuracy and efficiency. Also, the system can be designed to handle a large amount of traffic, and it can be made scalable to accommodate other organizations. Additionally, the application can be enhanced to provide real-time alerts for potential attacks, making it more effective in preventing cyber-attacks.

10. CONCLUSION

In conclusion, the IDS developed in this project offers a reliable and secure solution for keeping the internet environment of Charusat University healthy. By detecting potential attacks and securing IPs through constant monitoring, the system restricts student access to potentially harmful sites and helps to mitigate the risk of cyber attacks. Additionally, the application developed alongside the IDS streamlines the monitoring process and offers a more user-friendly experience for the system administrator.

However, there are some limitations to the system. For instance, the system is only capable of detecting attacks and suspicious activity within the university's own network, meaning that external threats may go undetected. Also, the system currently only supports a limited range of file types and protocols, which could potentially miss some malicious activities.

To enhance the system's capabilities, future work could involve expanding the system's monitoring capabilities to include external threats and supporting a wider range of file types and protocols. Furthermore, implementing machine learning algorithms could improve the system's ability to detect suspicious activity and potentially reduce the number of false positives. Overall, this project provides a solid foundation for building a more robust and effective IDS for Charusat University.

11. REFERENCES

- Google Diagram – Website to make block diagram.
- https://ieeexplore.ieee.org/abstract/document/8537852- Research Paper on Early Detection of Ransomware Exploits Using Snort.