Smart Intrusion Detection System

By

DHRUVI SHAH (18BCE056)
PRANAV GAJJAR (18BCE064)

NIRMA UNIVERSITY
INSTITUTE OF TECHNOLOGY
NAAC ACCREDITED 'A' GRADE

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
Ahmedabad 382481

SMART INTRUSION DETECTION SYSTEM

Minor Project Report

Submitted in partial fulfillment of the requirements

For the degree of

Bachelor of Technology in Computer Science & Engineering

By

DHRUVI SHAH (18BCE056)
PRANAV GAJJAR (18BCE064)

Guided By
Prof. Pimal Khanpara
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

NIRMA UNIVERSITY
INSTITUTE OF TECHNOLOGY
NAAC ACCREDITED 'A' GRADE

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
Ahmedabad 382481

CONTENTS

CERTIFICATE

This is to certify that the minor project entitled “Smart Intrusion Detection System” submitted by DHRUVI SHAH (18BCE056) and PRANAV GAJJAR (18BCE064), towards the partial fulfillment of the requirements for the degree of Bachelor of Technology in Computer Science and Engineering of Nirma University is the record of work carried out by him/her under my supervision and guidance. In my opinion, the submitted work has reached a level required for being accepted for examination.

Prof. Pimal Khanpara
Assistant Professor
Computer Science and Engineering Dept.,
Institute of Technology,
Nirma University,
Ahmedabad

Dr. Madhuri Bhavsar,
Professor and HOD,
Computer Science and Engineering Dept.,
Institute of Technology,
Nirma University,
Ahmedabad

ACKNOWLEDGEMENT

Working on a project in the domain of Network Security, a field which both of us have interest in has been a wonderful experience. Through the six months of working on this project, we have learnt, researched and implemented various technologies. We would like to thank *Prof. Pimal Khanpara* for her valuable guidance and support throughout the development of this project. We would also like to thank the Computer Science and Engineering Department for the opportunity to work on such a great project. We would also like to thank our families and friends for their helpful attitude and support.

ABSTRACT/ Outline

An intrusion detection system (IDS) is a device or software programme that watches for hostile activity or policy breaches on a network. They are used to detect anomalies in order to catch hackers before they cause serious network or device harm. Snort is a network intrusion detection and prevention system that is free and open source. Snort is used to track traffic entering and exiting a network. When it detects potentially harmful packets or threats on Internet Protocol (IP) networks, it monitors traffic in real time and logs in alerts for users.The challenge faced by users while deploying Snort is that it is command line and confusing to configure and use. Our Intrusion Detection System focuses on developing a unique application, with the aid of Snort, which takes into consideration the user comfort, and makes the traffic and threats easier to detect, analyze and mitigate with the help of a dashboard.

1. Introduction

1.1 General

An intrusion is defined as illegal entry to someone's property or area in general, but in computer science, it is defined as an act that compromises the essential computer network security goals of confidentiality, integrity, and privacy. Intrusion detection is the process of continuously monitoring and analysing events in a computer system or network for signals of potential threats and violations of computer security practises, acceptable usage regulations, or standard security policies. The existence of infiltration in the network is detected by the Intrusion Detection System (IDS). It's made to keep track of what's going on in a computer system or network, and to respond to events that show symptoms of prospective security policy violations.

Malicious software (malware) is evolving at a rapid pace, posing a significant challenge to the design of intrusion detection systems (IDS). Malicious attacks have evolved, and the most difficult task is identifying unknown and obfuscated malware, since malware developers employ various evasion tactics for information concealment in order to avoid detection by an IDS. Furthermore, security concerns such as zero-day attacks meant to target internet users have increased.

Snort is a network-centric software. It studies movement both inline and offline as an intrusion detection system. Snort works on the basis of a "known bad" or "suspected evil" method, which involves watching movement for examples of harmful or suspicious behaviour. When snort identifies such behaviour, it is referred to as (passive mode) or square (active mode). The first could be an IDS, whereas the second could be an IPS.

Although, Snort does come in with its limitations. Some users find trying to manage the software overwhelming due to its complex interface. In addition, a lot of backend maintenance is also not provided. The logs are not in a format that could be easily understood either.

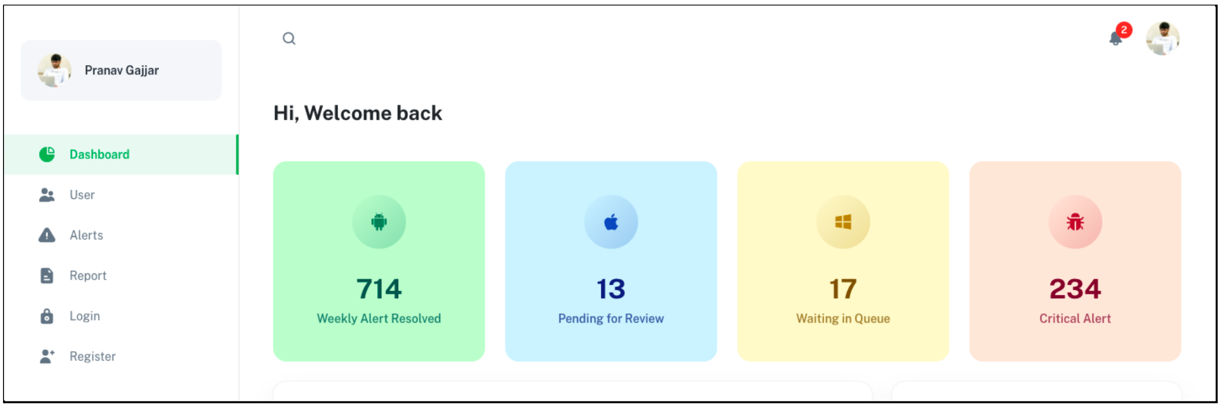
Our project aims at including the good features and overcoming the limitations of Snort and creating a unique product.

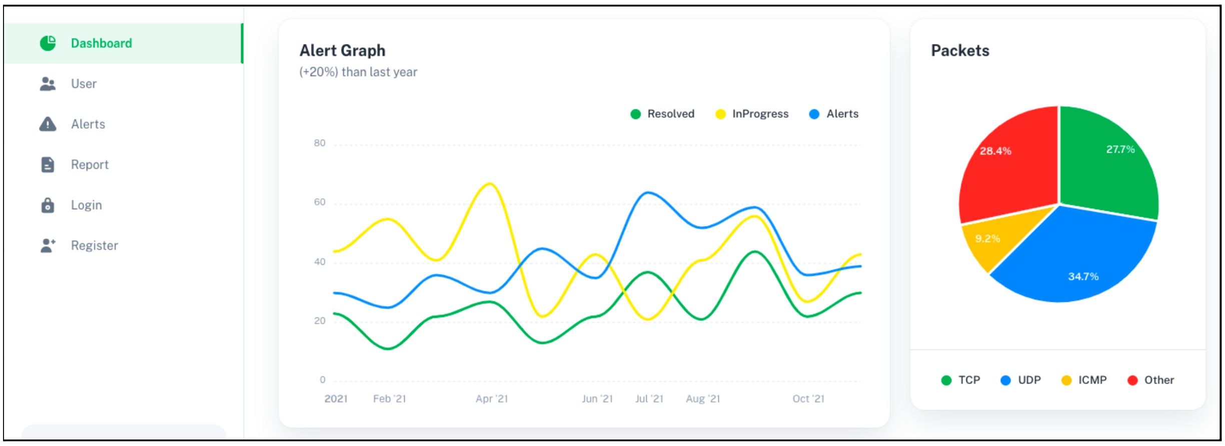
1.2 Smart Intrusion Detection System

Our aim was to build a Smart Intrusion Detection System that makes it easier for the end user to manage their security and take measures accordingly. The project has MongoDB as the database, along with Snort, and an Analytics Dashboard developed with React.

The dashboard contains various unique features:

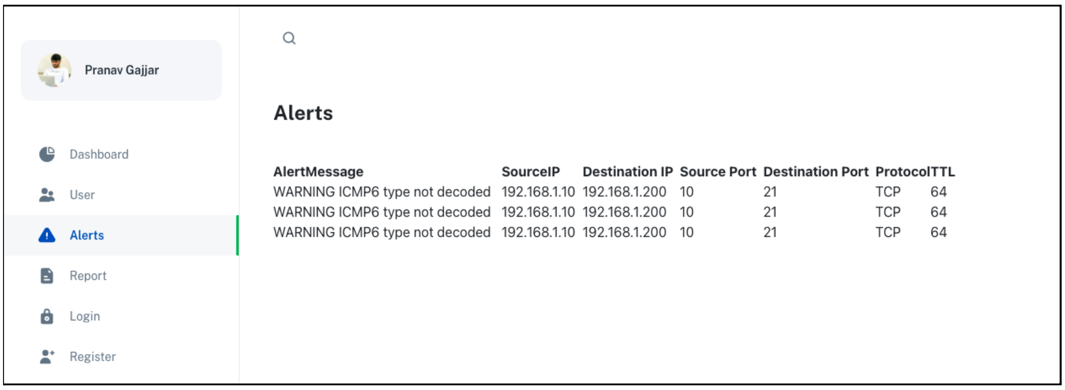
- Statistics about the weekly reports resolved, Alerts pending for review, and the critical alerts.
- A Pie Chart showcasing the different types of Packets received by the system.
- An Alert Graph showcasing the Resolved, In Progress and Pending Alerts.





From the Side Panel, the Admin can access the following:

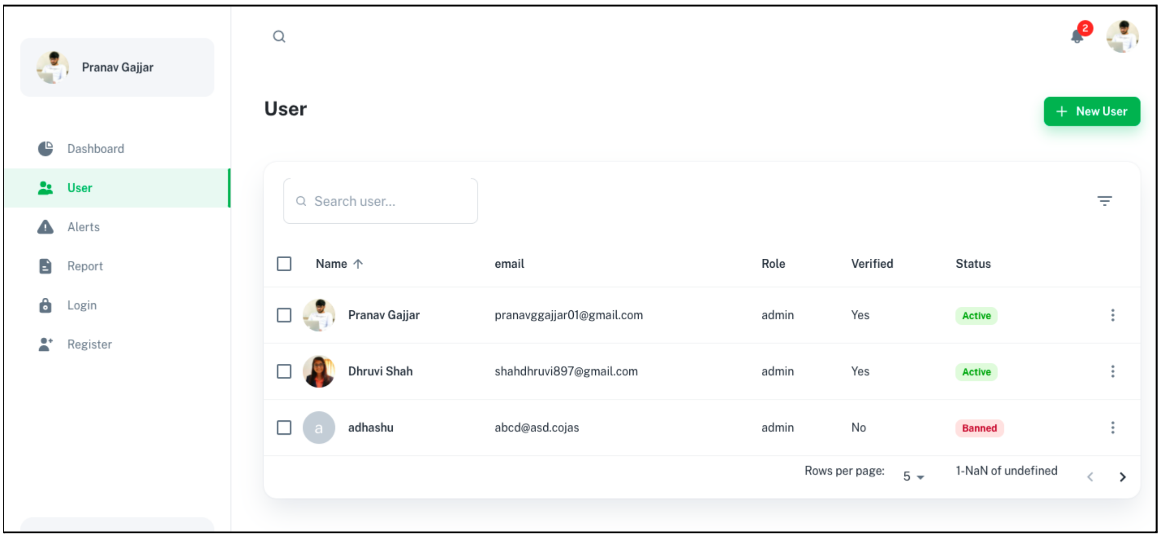
- All the Alerts in detail



Alerts

AlertMessage	SourceIP	Destination IP	Source Port	Destination Port	Protocol	TTL
WARNING ICMP6 type not decoded	192.168.1.10	192.168.1.200	10	21	TCP	64
WARNING ICMP6 type not decoded	192.168.1.10	192.168.1.200	10	21	TCP	64
WARNING ICMP6 type not decoded	192.168.1.10	192.168.1.200	10	21	TCP	64

- Details of the User

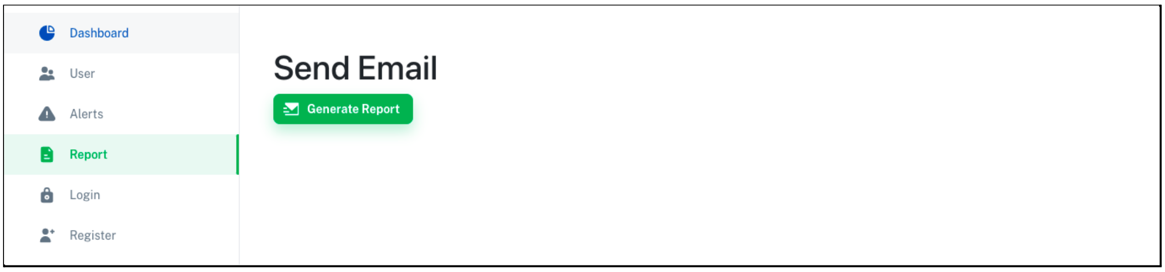


User

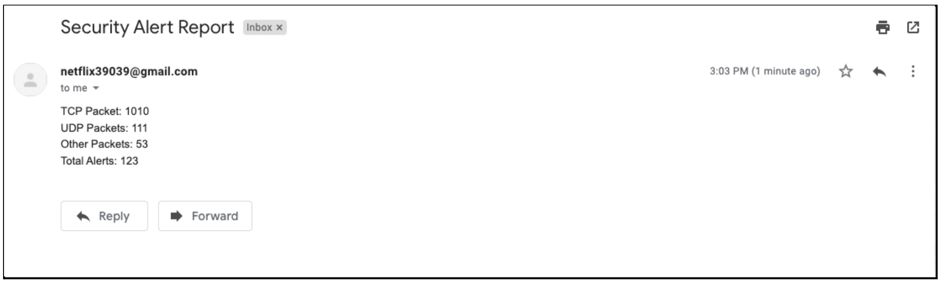
☐	Name ↑	email	Role	Verified	Status	
☐	Pranav Gajjar	pranavggajjar01@gmail.com	admin	Yes	Active	⋮
☐	Dhruvi Shah	shahdhruvi897@gmail.com	admin	Yes	Active	⋮
☐	a adhashu	abcd@asd.cojas	admin	No	Banned	⋮

Rows per page: 5 1-NaN of undefined

- Can add custom rules for monitoring traffic, or modify the existing rules
- Can Generate a detailed report which is then mailed to the admin



Send Email



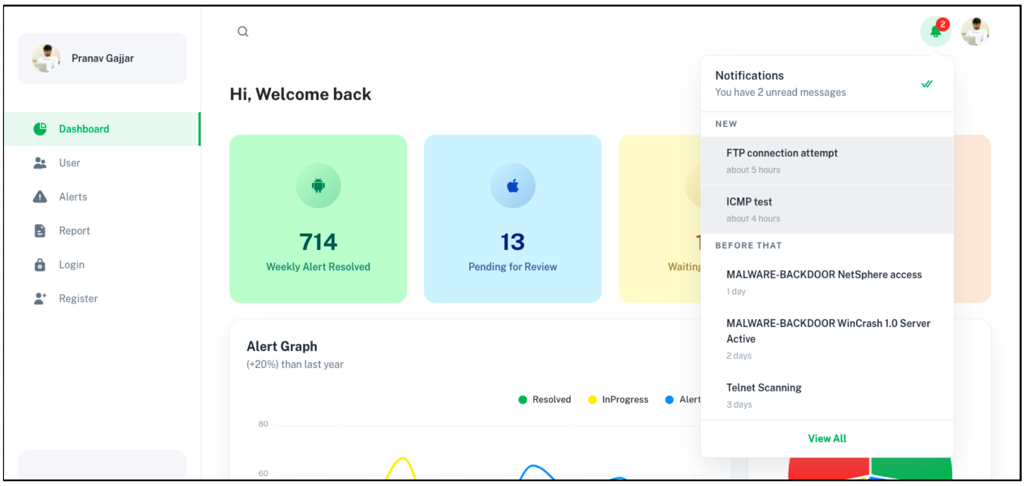
Security Alert Report

netflix39039@gmail.com
to me

3:03 PM (1 minute ago)

TCP Packet: 1010
UDP Packets: 111
Other Packets: 53
Total Alerts: 123

As soon as any malicious activity is detected, an alert is logged and an email is sent to the user, warning them of that particular activity with the required details.



Hi, Welcome back

714
Weekly Alert Resolved

13
Pending for Review

1
Waiting

Notifications
You have 2 unread messages

NEW

FTP connection attempt
about 5 hours

ICMP test
about 4 hours

BEFORE THAT

MALWARE-BACKDOOR NetSphere access
1 day

MALWARE-BACKDOOR WinCrash 1.0 Server Active
2 days

Telnet Scanning
3 days

View All

Alert Graph
(+20%) than last year

1.3 Objectives

The project aims to build a Smart Intrusion Detection System that makes it easier for the end user to detect anomalies and manage their security accordingly. The objectives can be divided as:

1. Training and testing the system to detect Malicious Behaviour in the network using datasets, Capturing the packets,
2. Notifying the user if any suspicious activity is detected.
3. Making a dashboard that helps the end-user to analyse the network graphically, keeps track of the past activities through an efficient database, and,
4. Suggesting preventive and security measures against the attacks on the dashboard

1.4 Problem Statement

Intrusion Detection Systems have become a needful component for computers and network security, but no matter how efficient, human intervention is needed in most cases before taking action as there is a high ratio of false positives. Another issue that arises is sometimes, IDS are too complex to understand or run on a system for users. Our system aims at increasing the usability and understandability of the working of an IDS by developing a dashboard for analysing the data easily and notifying the user periodically for malicious activities.

2. Literature Survey

The study [1] looked at Snort's architecture and how it works. They created a system based on Snort Intrusion behaviour that can be detected using the PF RING data packet capture module in IDS. This technique is effective and has been thoroughly tested. According to the authors, this system could serve as a viable model for the implementation of an intrusion detection system. This paper [2] describes the structure of snort and NTOP, as well as a novel design proposal for integrating the two, which is supported by an experiment. The findings of the experiment show that this system can detect incursion activity. This technique is effective and has been thoroughly tested.

The authors of paper [3] built a system based on the Software Engineering Framework that provides a solution for combining logging and a network-based intrusion detection and prevention system. For intrusion prevention, they set up the snort in inline mode. The logging of dropped packets was done using Splunk technology. This paper's future potential include writing signatures for additional protocols and infections.

The authors of study [4] examine several ways provided by security researchers, focusing on Snort as their IDS tool. This study presents a level-based architecture that can identify and prevent both known and new assaults to overcome numerous problems in the intrusion detection process. The suggested architecture's efficiency may be demonstrated by combining it with the Snort Tool via Code Refactoring. It also provided a configuration for evaluating the updated Snort Tool's performance in the future. By building a distributed intrusion detection system architecture in networks based on Snort, this research [5] provides an effective answer to network security concerns. It uses a centralised network intrusion detection system based on Snort to explicate the principles and methodology of a Snort-based architecture in networks. The major goal of this study article is to use a hierarchical distribution structure to unite dispersed detection and centralised administration, and therefore to handle the security concerns that the campus network faces more effectively.

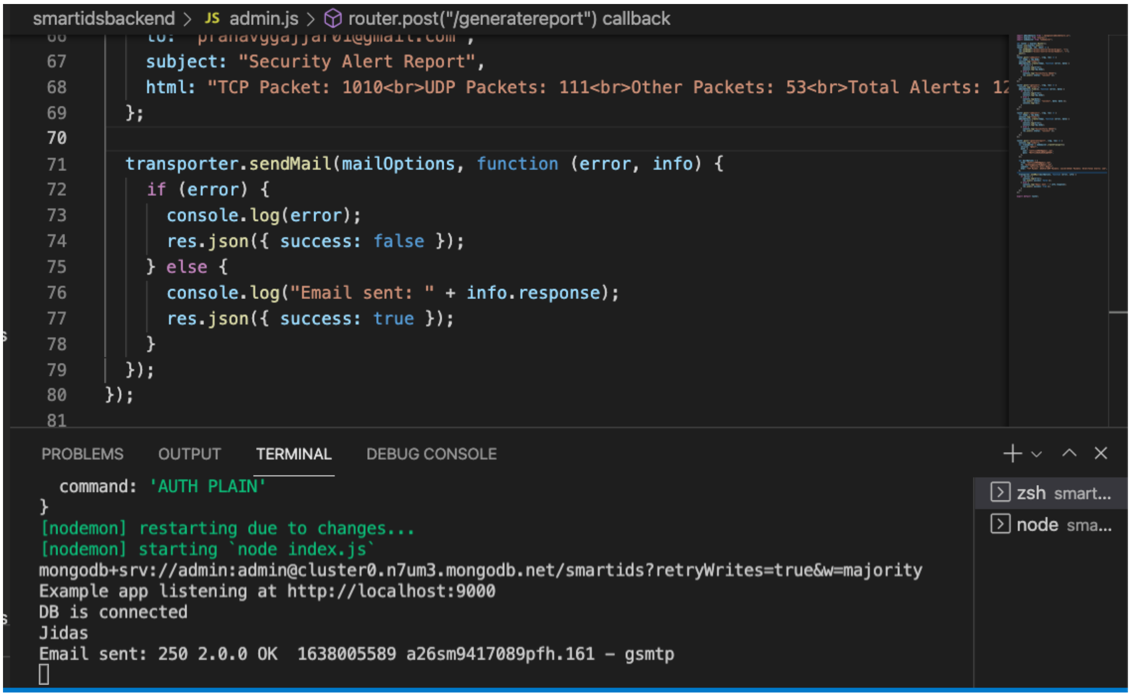
The authors present a critical analysis of IDS technology, issues that arise during installation, and challenges and limitations in the Intrusion Detection System in their work [6]. It contained potential future work while examining all of the IDS issues, as well as the in-depth discussion and contribution of each research in its specific sector.

Paper [7] gives in-depth information on current intrusion detection methodologies and tactics. It outlines the general architecture of IDS, as well as its limitations and current issues. The authors have conducted a survey on the overall advancement of intrusion detection systems based on their knowledge of existing kinds, methodologies, and architectures in the literature and highlighted current research problems and IDS loopholes in the study. The authors of paper [8] present a review of how AI-based techniques play a key role in the IDS. They talked about the benefits and drawbacks of AI-based techniques. The article aids in a better understanding of concepts and ideas in relation to various research directions in the subject of IDS. This paper provides important information on how AI-based techniques might be applied to IDS and related disciplines.

3. Methodology

This project works on top of the Snort system. After the initial configuration, the Snort is run in monitoring and logging mode. The log file generated is changed into a suitable JSON format, and that data is displayed on the dashboard in real-time. The user can then analyse through the graph charts.

In case of a malicious activity, an alert file is generated and the user is notified through the system and through the email.



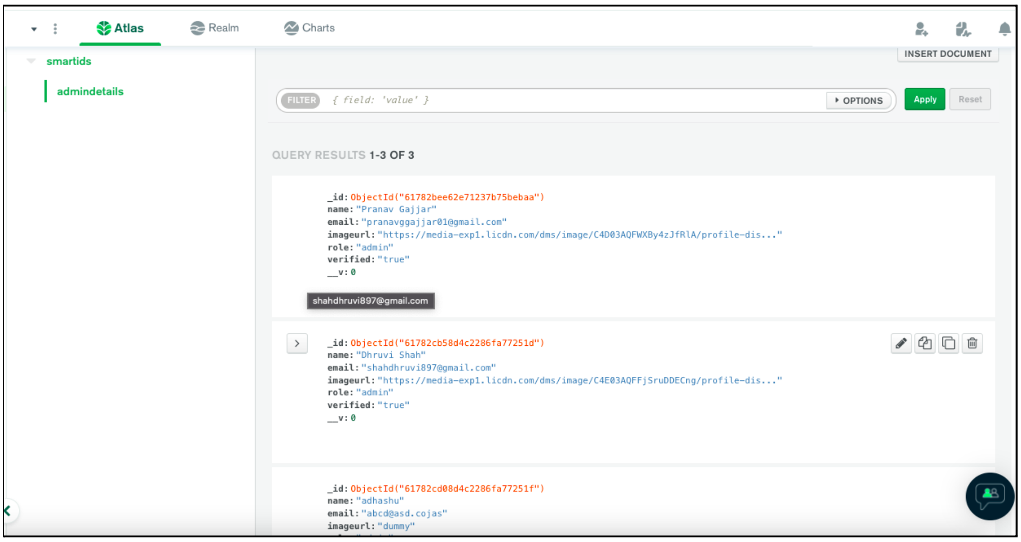
smartidsbackend > JS admin.js > router.post("/generatereport") callback
PROBLEMS
OUTPUT
TERMINAL
DEBUG CONSOLE
zsh smart...
node sma...

```
      to: "pranavggajjar01@gmail.com",
      subject: "Security Alert Report",
      html: "TCP Packet: 1010<br>UDP Packets: 111<br>Other Packets: 53<br>Total Alerts: 12
    };

    transporter.sendMail(mailOptions, function (error, info) {
      if (error) {
        console.log(error);
        res.json({ success: false });
      } else {
        console.log("Email sent: " + info.response);
        res.json({ success: true });
      }
    });
  });
```

```
  command: 'AUTH PLAIN'
}
[nodemon] restarting due to changes...
[nodemon] starting `node index.js`
mongodb+srv://admin:admin@cluster0.n7um3.mongodb.net/smartids?retryWrites=true&w=majority
Example app listening at http://localhost:9000
DB is connected
Jidas
Email sent: 250 2.0.0 OK  1638005589 a26sm9417089pfh.161 - gsmtp
```

All the user details are stored in a MongoDB database.



QUERY RESULTS 1-3 OF 3

```
_id: ObjectId("61782bee62e71237b75bebaa")
name: "Pranav Gajjar"
email: "pranavggajjar01@gmail.com"
imageurl: "https://media-exp1.licdn.com/dms/image/C4D03AQFWXBy4zJfRlA/profile-dis..."
role: "admin"
verified: "true"
__v: 0
```

shahdhruvi897@gmail.com

```
_id: ObjectId("61782cb58d4c2286fa77251d")
name: "Dhruvi Shah"
email: "shahdhruvi897@gmail.com"
imageurl: "https://media-exp1.licdn.com/dms/image/C4E03AQFFjSruDDECng/profile-dis..."
role: "admin"
verified: "true"
__v: 0
```

```
_id: ObjectId("61782cd08d4c2286fa77251f")
name: "adhashu"
email: "abcd@asd.cojas"
imageurl: "dummy"
```

4. Conclusion

An Intrusion Detection System protects our device and network from hackers and keeps it secure. An ID system gathers data from a variety of sources and analyses data from multiple regions within a computer or network to identify potential security breaches, such as intrusions (attacks from outside the business) and misuse (attacks from within the organization). Snort, as an IDS has many advantages like scalability, flexibility, delivering real-time network traffic event information and more. Our system has enhanced the working of Snort with an Analytical dashboard and overcome the limitations with varied functionalities. The future work that can be researched upon and implemented has also been provided.

5. Future Work

With this system, we have successfully developed a user-understandable Smart Intrusion Detection System with multiple functionalities. This system can be further improved by reducing the number of false positives. There are certain rules according to which the system works, by analysing them and the false positives together, we can further work on developing a new rule or algorithm which can prevent the anomalies in the software. Another area which can be developed is a Prevention System which can automatically take actions against a potential threat, after getting the respective permission from the Admin.

6. References

1. Chi, R. (2014, January). Intrusion detection system based on snort. In Proceedings of the 9th International Symposium on Linear Drives for Industry Applications, Volume 3 (pp. 657-664). Springer Berlin Heidelberg.
2. Peng, Y. (2012, May). Research of network intrusion detection system based on snort and NTOP. In Fuzzy Systems and Knowledge Discovery (FSKD), 2012 9th International Conference on (pp. 2764-2768). IEEE.
3. Kenkre, P. S., Pai, A., & Colaco, L. (2015). Real time intrusion detection and prevention system. In Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014 (pp. 405-411). Springer, Cham.
4. Gaddam, R., & Nandhini, M. (2017, March). An analysis of various snort based techniques to detect and prevent intrusions in networks proposal with code refactoring snort tool in Kali Linux environment. In Inventive Communication and Computational Technologies (ICICCT), 2017 International Conference on (pp. 10-15). IEEE.

5. Kai, Z. (2012, March). Research and design of the distributed intrusion detection system based on Snort. In 2012 International Conference on Computer Science and Electronics Engineering (pp. 525-527). IEEE.
6. Mohamed, A. B., Idris, N. B., & Shanmugum, B. (2012). A brief introduction to intrusion detection system. In Trends in Intelligent Robotics, Automation, and Manufacturing (pp. 263-271). Springer, Berlin, Heidelberg
7. Bashir, U., & Chachoo, M. (2014, March). Intrusion detection and prevention system: Challenges & opportunities. In Computing for Sustainable Global Development (INDIACom), 2014 International Conference on (pp. 806-809). IEEE.
8. Kumar, G., Kumar, K., & Sachdeva, M. (2010). The use of artificial intelligence based techniques for intrusion detection: a review. Artificial Intelligence Review, 34(4), 369-387.
9. Tasneem, Aaliya & Kumar, Abhishek & Sharma, Shabnam. (2018). Intrusion Detection Prevention System using SNORT. International Journal of Computer Applications. 181. 21-24. 10.5120/ijca2018918280.
10. Khraisat, A., Gondal, I., Vamplew, P. et al. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecur 2, 20 (2019). https://doi.org/10.1186/s42400-019-0038-7
11. TrustRadius. 2021. Snort Reviews. [online] Available at: <https://www.trustradius.com/products/cisco-snort/reviews?qs=pros-and-cons> [Accessed 27 November 2021].