VISVESVARAYA TECHNOLOGICAL UNIVERSITY

"JNANA SANGAMA", BELAGAVI - 590 018

MINI PROJECT REPORT

on

"NETWORK BASED INTRUSION DETECTION SYSTEM"

Submitted by

VIJAYENDRA NAYAK	4SF21IS019
CHANDAN B	4SF21IS026
BALAMURALI M	4SF21IS021
DARSHITH PANDITH	4SF21IS028

In partial fulfillment of the requirements for the V semester

BACHELOR OF ENGINEERING

in

INFORMATION SCIENCE & ENGINEERING

Under the Guidance of

Mrs. Shwetha S Shetty

Assistant Professor, Department of ISE

at

SAHYADRI

College of Engineering & Management

An Autonomous Institution

MANGALURU

2023 - 24

SAHYADRI

College of Engineering & Management

Adyar, Mangaluru - 575 007

Department of Information Science & Engineering

CERTIFICATE

This is to certify that the **Mini Project** entitled **"Network Based Intrusion Detection System"** has been carried out by **Vijayendra Nayak (4SF21IS019), Chandan B(4SF21IS026), Balamurali M (4SF21IS021) and Darshith Pandith (4SF21IS028)**, the bonafide students of Sahyadri College of Engineering and Management in partial fulfillment of the requirements for the V semester of Bachelor of Engineering in Information Science and Engineering of Visvesvaraya Technological University, Belagavi during the year 2023 - 24. It is certified that all suggestions indicated for Internal Assessment have been incorporated in the Report deposited in the departmental library. The mini project report has been approved as it satisfies the academic requirements in respect of project work prescribed for the said degree.

Project Guide	**Project Coordinator**	**HOD**
Mrs. Shwetha S Shetty	**Dr. Navaneeth Bhaskar**	**Dr. Rithesh Pakkala P**
Assistant Professor	Associate Professor	Associate Professor & Head
Dept. of ISE	Dept. of ISE	Dept. of ISE

Evaluation:

Examiner's Name	Signature with Date
1.	.....
2.	.....

SAHYADRI

College of Engineering & Management

Adyar, Mangaluru - 575 007

Department of Information Science & Engineering

DECLARATION

We hereby declare that the entire work embodied in this Mini Project Report titled **"Network Based Intrusion Detection System"** has been carried out by us at Sahyadri College of Engineering and Management, Mangaluru under the supervision of **Dr. Navaneeth Bhaskar**, in partial fulfillment of the requirements for the V semester of **Bachelor of Engineering** in **Information Science and Engineering**. This report has not been submitted to this or any other University for the award of any other degree.

Vijayendra Nayak (4SF21IS019)

Chandan B (4SF21IS026)

Balamurali M (4SF21IS021)

Darshith Pandith (4SF21IS028)

Abstract

Intrusion-detection systems (IDS) aim at detecting attacks against computer systems and networks or, in general, against information systems. Its basic aim is to protect the system against malwares and unauthorized access of a network or a system. Intrusion Detection is of two types Network-IDS and Host Based- IDS. This paper covers the scope of both the types and their result analysis along with their comparison as stated. OSSEC (HIDS) is a free, open source host-base intrusion detection system. It performs log analysis, integrity checking, Windows registry monitoring, rootkit detection, time-based alerting and active response. While Snort (NIDS) is a lightweight intrusion detection system that can log packets coming across your network and can alert the user regarding any attack. Both are efficient in their own distinct fields

Acknowledgement

It is with great satisfaction we are submitting the Mini Project Report on **"Network Based Intrusion Detection System"**. We have completed it as a part of the curriculum of Visvesvaraya Technological University, Belagavi in partial fulfillment of the requirements for the V semester of Bachelor of Engineering in Information Science and Engineering.

We are profoundly indebted to our guide, **Mrs. Shwetha S Shetty**, Assistant Professor, Department of Information Science and Engineering for timely advice, encouragement and we sincerely express our gratitude.

We also thank **Dr. Navaneeth Bhaskar**, Associate Dean (R&D) and **Ms. Ashritha K P**, Project Coordinator, Department of Information Science and Engineering & CSE (Data Science) for their constant encouragement and support extended throughout.

We express our sincere gratitude to **Dr. Rithesh Pakkala P**, Head and Associate Professor, Department of Information Science and Engineering & CSE (Data Science) for his invaluable support and guidance.

We sincerely thank **Dr. S S Injaganeri**, Principal, Sahyadri College of Engineering and Management, who has always been a great source of inspiration.

Finally, we express our heartfelt thanks to our family and friends for their wishes and encouragement throughout the work.

Vijayendra Nayak (4SF21IS019)
Chandan B (4SF21IS026)
Balamurali M (4SF21IS021)
Darshith Pandith (4SF21IS028)

Table of Contents

List of Figures

Chapter 1

Introduction

TIn the ever-evolving landscape of cybersecurity, the need for robust intrusion detection systems (IDS) is paramount to safeguarding sensitive information and networks from unauthorized access and malicious activities. Two main categories of IDS are hardware-based detection systems and network-based detection systems. Each approach has its unique strengths and weaknesses, catering to specific cybersecurity requirements. This introduction will provide an overview of these two types of intrusion detection systems.

Host-Based Intrusion Detection System (HIDS):

A Host-based intrusion detection system focuses on monitoring and analyzing activities on individual devices or hosts within a network. This approach involves installing security agents or sensors on endpoints, such as computers or servers, to gather data about the host's behavior and activities. Host-based detection systems rely on logs, file integrity checks, system calls, and various other host-level indicators to identify suspicious or malicious behavior. By examining the activities at the endpoint level, these systems can detect anomalies that might indicate a security threat, such as unauthorized access, malware infections, or abnormal system behavior.

Network-Based Intrusion Detection System (NIDS):

On the other hand, a network-based detection system operates at the network level, scrutinizing the traffic and communication patterns between devices within a network. Network-based detection systems use a variety of techniques, including signature-based detection, anomaly detection, and behavior analysis, to identify potential threats in real-time. These systems monitor network traffic, analyze packet payloads, and inspect communication patterns to detect malicious activities such as unauthorized access attempts, data exfiltration, and network intrusions.

Chapter 2

Literature Survey

Survey on Host and Network Based Intrusion Detection System.
According to " Survey on Host and Network Based Intrusion Detection System" done by Niva Das and Tanmoy Sarkar Network-based and host-based IDS prevent both insider as well as outsider attacks. There are ever evolving methods of intrusion detection but most systems utilize signatures to search for patterns of misuse and either automatically respond to the misuse or intimates system administrator to take appropriate action. Some intrusion detection systems even sense misappropriation by using behavioral data forensics. Due to inherent risk of some automated responses, there is still need for human intervention that can supervise and ensure the state of the system.

Comparison of the Host-Based Intrusion System and Network-Based Intrusion Systems.
Amrit Pal Singh and Manik Deep Singh suggested that by using IDS, is totally dependent on the requirements and results needed out of it. IDS is very flexible, and can be used for various purposes or can also be used in either HIDS or NIDS mode[2] Also after defining the type of results need to be obtained, its placement can be finalized in case of NIDS. It works totally on what are the priorities of a company or an individual is. We can use IDS to tackle with intruders in standalone or multi-network machines/systems. On the other hand Logs can help us compare or create new set of records/rules for future reference and measuring system efficiency.

Intrusion Detection and Prevention System (HIDPS) As we came across to this research paper we got to know that Kopelo Letou, Dhruwajita Devi and Y. Jayanta

Singh had surveyed the latest up-to-date technology trend on HIDPS and then selected the best intrusions detection techniques and algorithms for building the proposed model expecting high promising security, performance and accuracy. The field of HIDPS is intensive; recent research areas offer a hundred percent security on computer systems and Information Systems that can detect and prevent all types of intrusions and malicious activities in real time, creating no false alarms and without any human intervention. This HIDPS chooses the best algorithm individual for Misuse detection is C4.5 Decision tree algorithm and Anomaly detection techniques is Support vector machine algorithm respectively, and intrusions detection test data have to pass through two phases i.e., first misuse detection engine and then anomaly detection engine. Any malicious activities and abnormal Behaviours of internal or external intrusions and attacks can be detected and prevented from the computer systems by HIDPS.

Intrusion detection system: A comprehensive review

With the increasing amount of network throughput and security threat, the study of intrusion detection systems (IDSs) has received a lot of attention throughout the computer science field. Current IDSs pose challenges on not only capricious intrusion categories, but also huge computational power. Though there is a number of existing literatures to IDS issues, we attempt to give a more elaborate image for a comprehensive review. Through the extensive survey and sophisticated organization, we propose the taxonomy to outline modern IDSs. In addition, tables and figures we summarized in the content contribute to easily grasp the overall picture of IDSs.

Chapter 3

Problem Statement and Objectives

The rising threat of Advanced Persistent Threats (APTs) presents significant security challenges. Despite the global accessibility of information, citizens often prefer traditional methods due to security concerns, impacting reliance on server-hosted information services. This study addresses intricate security challenges, emphasizing APTs and dynamic cyber threats. It advocates for a comprehensive security approach, highlighting the vulnerability of information services.

The focus is on intrusion detection systems (NIDS) and their effectiveness in enhancing security by addressing configurability, and robustness, and minimizing false positives and negatives. The rising prevalence of Advanced Persistent Threats (APTs) has resulted in considerable security challenges, prompting individuals to show a preference for conventional methods over online services. In addressing these intricacies, this study concentrates on APTs and the ever-changing landscape of cyber threats. The research underscores the vulnerability of information services 4 hosted on servers and advocates for a comprehensive security approach. At the heart of the investigation is an examination of the efficacy of intrusion detection systems (NIDS) in reducing false positives and negatives, with an emphasis on improving configurability and robustness.

3.1 Objectives

- To Detect and identify various types of cybersecurity threats, including malware, intrusion attempts, and other malicious activities within the network.
- To Provide early warning signals to security teams by detecting abnormal patterns or behaviors, enabling timely response to potential security incidents

Chapter 4

Methodology

This study extensively reviews security risks and the role of Intrusion Detection Systems (IDS) in risk mitigation. It identifies specific threats such as information intercepting, tampering, service denial, system resource stealing, and information faking. The analysis underscores how IDS systems can effectively address these security challenges, emphasizing the preservation of information confidentiality, integrity, and availability. The overview traces the evolution of IDS from its inception in 1987 to its current significance in network security. The classification of IDS into Network-Based (NIDS) categories is explained, alongside an exploration of intrusion detection methods. The study introduces the ISP model for categorizing IDS as active/passive and host-based/network-based systems. The evolving role of IDS in Intrusion Prevention Systems is discussed, detailing the functionalities of NIDS in analyzing incoming packets, abnormality detection, and real-time response for network security. The study concludes by summarizing key findings and proposing potential future trends in IDS technology.

4.1 Architecture Diagram

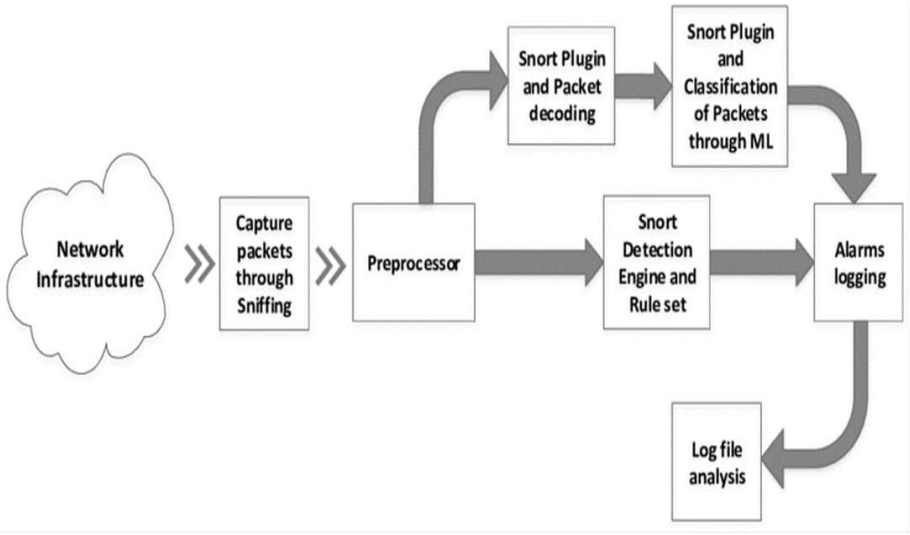

Figure 4.1: Block Diagram for illustration of Network Security System

The above diagram illustrates a network security system built around Snort, a free and widely used tool for detecting and preventing intrusions. It captures data packets flowing through the network, analyzes them against a set of pre-defined rules, and raises alarms if any suspicious activity is identified. Similar to a security guard checking IDs, Snort safeguards your network by constantly monitoring for potential threats and alerting you of any concerning patterns.

4.2 Components Requirements

4.2.1 Software Requirements

- UBUNTU : It can be used to detect various attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and much more. Configuring Snort on an Ubuntu 20.04 server can significantly enhance your network's security posture.

Figure 4.2: Ubuntu Software

This diagram illustrates a network security system built around Snort, a free and widely used tool for detecting and preventing intrusions. It captures data packets flowing through the network, analyzes them against a set of pre-defined rules, and raises alarms if any suspicious activity is identified. Similar to a security guard checking IDs, Snort safeguards your network by constantly monitoring for potential threats and alerting you of any concerning patterns.

- Kali LINUX : It can be said as an basic essential component of network security which can help us to detect and respond to attacks in real time.And it comes with several other components that can be used for the purpose of intrusion detection.

Figure 4.3: Kali Linux

- Snort : It is used to monitor the traffic that goes in and out of a network. It will monitor traffic in real time and issue alerts to users when it discovers potentially malicious packets or threats on Internet Protocol (IP) networks.

Figure 4.4: Snort

- Virtual Box : It is cross-platform virtualization software. It allows users to extend their existing computer to run multiple operating systems including Microsoft Windows, Mac OS X, Linux, and Oracle Solaris, at the same time.

4.2.2 Hardware Requirements

- System used with these configuarations

  64-bit x86/AMD64 CPU launched in 2011 or later. A core speed of 1.3GHz or faster 2GB RAM minimum, 4GB RAM recommended. General Host OS Requirements

4.3 System Design

- **Network Infrastructure:** This is the network that the system is monitoring for suspicious activity.
- **Snort IDS:** This is the core of the system. It takes the captured packets from the sniffers and analyzes them for malicious activity. Snort uses a rule-based approach to identify suspicious activity. It compares the packets to a set of predefined rules, and if a match is found, Snort generates an alert.
- **Snort Plugin and Packet Decoding:** This component helps Snort to decode and understand the different protocols used in network traffic. This is important because Snort needs to be able to understand the structure of a packet in order to determine whether it is malicious or not.
- **Preprocessor:** This component prepares the captured packets for analysis by Snort. It may perform tasks such as removing irrelevant information from the packets and converting them into a format that Snort can understand.
- **Snort Detection Engine and Rule Set:** This component is the heart of Snort's detection capabilities. It compares the captured packets to the Snort rule set, which is a collection of rules that define what constitutes malicious activity. If a packet matches a rule, Snort generates an alert.
- **Alarms and Logging:** When Snort detects suspicious activity, it generates an alert. This alert can be logged to a file, sent to a security information and event management (SIEM) system, or displayed on a console.

Procedure:

- Packets are captured from the network by sniffers.
- The captured packets are sent to the Snort IDS.
- The Snort IDS preprocesses the packets and then decodes them using the Snort Plugin and Packet Decoding component.
- The Snort IDS then classifies the packets as malicious or benign using the Snort Plugin and Classification of Packets through ML component.
- The Snort IDS compares the packets to the Snort rule set using the Snort Detection Engine and Rule Set component.
- If a packet matches a rule, Snort generates an alert and logs the event.

This is a simplified overview of the system design. The actual implementation may vary depending on the specific needs of the organization.

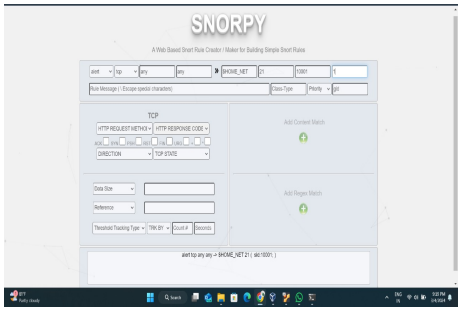

Figure 4.5: Snorpy Tool

Snorpy is Web-Application to easily build snort rules in a graphical way.

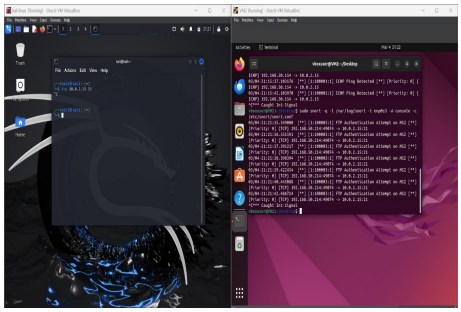

Figure 4.6: FTP Authentication Attempt

FTP a process that verifies the identity of a user or system trying to access an FTP server.

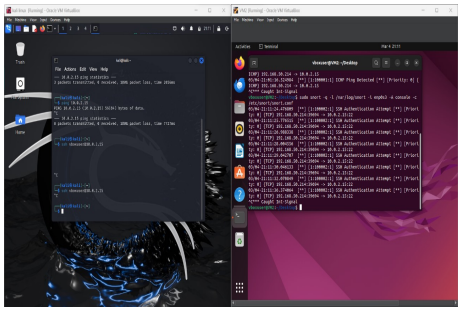

Figure 4.7: SSH Authentication Attempt

SSH is set of rules that devices use to communicate data transmission errors in a network.

Chapter 5

Results and Discussion

This assessment of Network Intrusion Detection Systems (NIDS) showcased commendable detection rates within the monitored network, effectively identifying a range of malicious activities. While NIDS demonstrated high accuracy, occasional false positives were noted, necessitating fine-tuning of parameters and rule sets to optimize performance. Although resource utilization was generally acceptable, it highlighted the need for a delicate balance between security measures and system performance. The combined deployment of NIDS emerged as a potent strategy, offering a comprehensive defense against both network-wide and host-specific threats.

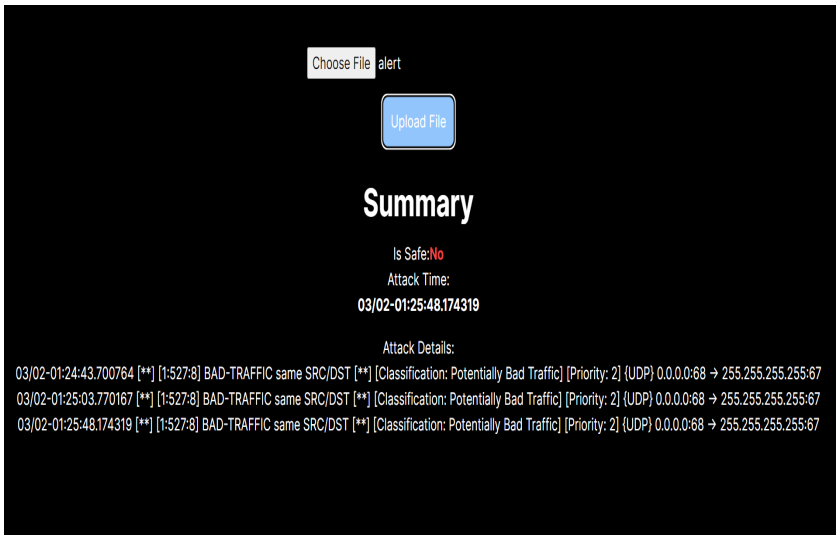

Figure 5.1: User Interface for Threat Detection

The integration of NIDS is crucial for a holistic intrusion detection approach. NIDS excels in network-wide monitoring. Our findings emphasize the importance of adaptive security policies, with continuous updates and customization based on evolving threats. Regular monitoring and evaluation are pivotal, ensuring alignment with the dynamic threat landscape. Furthermore, user awareness and training emerged as critical factors, as educated users contribute significantly to the effectiveness of intrusion detection systems. In conclusion, a well-balancing NIDS, adaptive security policies, continuous monitoring, and user education forms a robust strategy for intrusion detection and prevention in contemporary cybersecurity landscapes.

Chapter 6

Outcome and Future Scope of Work

- Provide insights into specific security risks faced by systems, including information intercepting, tampering, service denial, system resource stealing, and information faking.
- Assess how Intrusion Detection Systems (IDS) effectively mitigate identified security risks, focusing on their role in maintaining information confidentiality, integrity, and availability.
- Offer a historical overview of IDS development, tracing its evolution from inception in 1987 to its current importance in addressing network security challenges.
- Offer a historical overview of IDS development, tracing its evolution from inception in 1987 to its current importance in addressing network security challenges.
- Clarify the classification and categorization of IDS based on their environment, by Network-Based IDS (NIDS) and categorizing them as active/passive and network-based.

Chapter 7

Conclusion

In summary, this study provides valuable insights into the specific security risks faced by systems, emphasizing information intercepting, tampering, denying services, system resource stealing, and information faking. The evaluation of Intrusion Detection Systems (IDS) reveals their effectiveness in mitigating these risks, with a focus on maintaining information confidentiality, integrity, and availability. The historical development, classification, and categorization of IDS, along with the exploration of intrusion detection methods, contribute to a 7 holistic understanding. Despite limitations, IDS advancements, including the shift towards Intrusion Prevention Systems, showcase their adaptability. The study concludes that IDS plays a crucial role in security, paving the way for potential future trends in IDS technology.

References

[1] Niva Das and Tanmoy Sarkar. Survey on host and network based intrusion detection system. *International Journal of Advanced Networking and Applications*, 6(2):2266, 2014.

[2] Kopelo Letou, Dhruwajita Devi, and Y Jayanta Singh. Host-based intrusion detection and prevention system (hidps). *International Journal of Computer Applications*, 69(26):28–33, 2013.

[3] Hung-Jen Liao, Chun-Hung Richard Lin, Ying-Chih Lin, and Kuang-Yuan Tung. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36(1):16–24, 2013.

[4] Amrit Pal Singh and Manik Deep Singh. Analysis of host-based and network-based intrusion detection system. *International Journal of Computer Network and Information Security*, 6(8):41–47, 2014.