

IDS FOR ENHANCING NETWORK SECURITY AND NETWORK INFRASTRUCTURE

By

MR. ARKAN SHAH (2201830001)

MR. SHIVAM RAWAT(2201830003)

MR. RACHIT MEHNDIRATTA(2201830005)

MS. ADITI JHA(2201830007)

Under the guidance of

PROJECT MENTOR – DR. SURABHI SHANKER

INDUSTRY MENTOR – MR. HARSH GOYAL

Department of Computer Science and Engineering

School of Engineering and Technology

K. R. Mangalam University, Gurugram - 122003

October-December 2024

DECLARATION

We declare that this written submission represents our ideas in our own words and where other's ideas or words have been included, we have adequately cited and referenced the original sources. We also declare that we have adhered to all the principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will because for disciplinary action by the Institute and canal so evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed. We further declare that if any violation of the intellectual property right or copyright, my supervisor and university should not be held responsible for the same.

Student Name	(Roll No.)	(Signature)
Mr. ARKAN SHAH	(2201830001)	Arkan
Mr. SHIVAM RAWAT	(2201830003)	Shivam
Mr. RACHIT MEHNDIRATTA	(2201830005)	Rachit
Ms. ADITI JHA	(2201830007)	Aditi

Place : K.R.Mangalam University

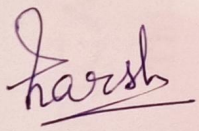
Date : 6th December 2024

CERTIFICATE

It is certified that the work contained in the project report titled **"IDS FOR ENHANCING NETWORK SECURITY AND NETWORK INFRASTRUCTURE"** by the following students:

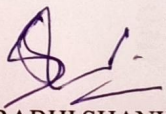
Name of the Student:	**ROLL NUMBER:**
Mr. ARKAN SHAH	(2201830001)
Mr. SHIVAM RAWAT	(2201830003)
Mr. RACHIT MEHNDIRATTA	(2201830005)
Ms. ADITI JHA	(2201830007)

has been carried out under our/my supervision and that this work has not been submitted elsewhere.



MR. HARSH GOYAL

Industry Mentor



DR. SURABHI SHANKER

Project Mentor

Date: - 6th December 2024

Place: - K.R. Mangalam University

SR. NO- SUVIKSAN/24-25/KRPC101

K.R. MANGALAM UNIVERSITY

SUVIKSAN
TECHNOLOGIES PRIVATE LIMITED

CERITIFICATE OF COMPLETION

This is to certify that

ARKAN SHAH

(Roll no -2201830001, B.Sc.(H) in Cyber Secuirty,5th Sem)

SCHOOL OF ENGINEERING AND TECHNOLOGY,
KR MANGALAM UNIVERSITY, GURUGRAM

has successfully completed the project on

IDS FOR ENHANCING NETWORK SECURITY AND NETWORK INFRASTRUCTURE

October 15, 2024 - December 05, 2024

10/12/2024
ISSUE DATE

INDUSTRY MENTOR

Suviksan Technologies Pvt. Ltd. New Delhi

VIKRANT KISHORE (DIRECTOR)
SUVIKSAN TECHNOLOGIES PVT. LTD.

SR. NO- SUVIKSAN/24-25/KRPC102

K R MANGALAM UNIVERSITY

SUVIKSAN
TECHNOLOGIES PRIVATE LIMITED

CERITIFICATE OF COMPLETION

This is to certify that

SHIVAM RAWAT

(Roll no -2201830003, B.Sc.(H) in Cyber Secuirty,5th Sem)

SCHOOL OF ENGINEERING AND TECHNOLOGY,
KR MANGALAM UNIVERSITY, GURUGRAM

SUVIKSAN

has successfully completed the project on

IDS FOR ENHANCING NETWORK SECURITY AND NETWORK INFRASTRUCTURE

October 15, 2024 - December 05, 2024

10/12/2024
ISSUE DATE

INDUSTRY MENTOR

Suviksan Technologies Pvt Ltd New Delhi

VIKRANT KISHORE (DIRECTOR)
SUVIKSAN TECHNOLOGIES PVT. LTD.

SR. NO- SUVIKSAN/24-25/KRPC103

K.R. MANGALAM UNIVERSITY

SUVIKSAN
TECHNOLOGIES PRIVATE LIMITED

CERITIFICATE OF COMPLETION

This is to certify that

RACHIT MEHNDIRATTA

(Roll no -2201830005, B.Sc.(H) in Cyber Secuirty,5th Sem)

SCHOOL OF ENGINEERING AND TECHNOLOGY,

KR MANGALAM UNIVERSITY, GURUGRAM

SUVIKSAN

has successfully completed the project on

IDS FOR ENHANCING NETWORK SECURITY AND NETWORK INFRASTRUCTURE

October 15, 2024 - December 05, 2024

10/12/2024
ISSUE DATE

INDUSTRY MENTOR

Suviksan Technologies Pvt. Ltd. New Delhi

VIKRANT KISHORE (DIRECTOR)
SUVIKSAN TECHNOLOGIES PVT. LTD.

SR. NO- SUVIKSAN/24-25/KRPC104

K.R MANGALAM UNIVERSITY

SUVIKSAN
TECHNOLOGIES PRIVATE LIMITED

CERITIFICATE OF COMPLETION

This is to certify that

ADITI JHA

(Roll no -2201830007, B.Sc.(H) in Cyber Secuirty,5th Sem)

SCHOOL OF ENGINEERING AND TECHNOLOGY,

KR MANGALAM UNIVERSITY, GURUGRAM

has successfully completed the project on

IDS FOR ENHANCING NETWORK SECURITY AND NETWORK INFRASTRUCTURE

October 15, 2024 - December 05, 2024

10/12/2024
ISSUE DATE

INDUSTRY MENTOR

Suviksan Technologies Pvt. Ltd. New Delhi

VIKRANT KISHORE (DIRECTOR)
SUVIKSAN TECHNOLOGIES PVT. LTD.

ACKNOWLEDGEMENT

I would like to extend my heartfelt gratitude to the faculty and industry mentors and team members for their invaluable support and contributions to the successful completion of this project. Your guidance, expertise, and unwavering support throughout the project were instrumental in its successful execution. I want to express my appreciation to my dedicated project team members who carryout the project to completion with their commitment were commendable. I want to acknowledge the valuable feedback and insights offered by our peer reviewers, which greatly improved the quality of this project. I am thankful for the mentorship and collaboration with **Suviksan Technologies Private Limited** which enriched my understanding of the subject matter. This project would not have been possible without the collective efforts and encouragement of these individuals and organizations. Your contributions have been deeply appreciated.

Mr. ARKAN SHAH
Mr. SHIVAM RAWAT
Mr. RACHIT MEHNDIRATTA
Ms. ADITI JHA

Place: - K.R. Mangalam University
Date: - 6th December 2024

ABSTRACT

This research presents a novel Intrusion Detection System (IDS) specifically designed to mitigate the growing threat of advanced persistent threats (APTs) and zero-day attacks. The IDS utilizes a hybrid approach combining signature-based detection and behaviour-based detection techniques. For behaviour detection, the system leverages a sophisticated analytics engine that analyses network traffic patterns, identifying deviations from established norms. The IDS is equipped with advanced correlation algorithms to detect complex attack sequences and real-time threats across network flows. The system is evaluated using a comprehensive dataset of real-world network traffic and demonstrates superior performance in detecting both known and unknown threats compared to traditional signature-based IDS. The proposed system holds significant potential for enhancing network security in critical infrastructure, financial institutions, and other industries vulnerable to sophisticated cyberattacks.

KEYWORDS: Intrusion Detection System (IDS) , Advanced Persistent Threats (APTs), Network traffic analysis , Network security

TABLE OF CONTENTS

	Page No
Declaration	i
Certificate	ii
Acknowledgement	iii
Abstract	iv
Chapter 1: INTRODUCTION	**7-8**
Chapter 2: LITERATURE REVIEW	**9-11**
Chapter 3: PROBLEM STATEMENT AND OBJECTIVES	**12**
Chapter 4: METHODOLOGY OF THE PROJECT	**13-17**
Chapter 5: IMPLEMENTATION	**18-19**
Chapter 6: RESULTS AND ANALYSIS	**20-24**
Chapter 7: CONCLUSION AND FUTURE SCOPE	**25**
REFERENCES	**26**

INTRODUCTION

BACKGROUND OF THE PROJECT

An Intrusion Detection System (IDS) is a software application that monitors network traffic for suspicious activity. It can detect potential security threats like unauthorized access, malware, and DoS attacks.

The proliferation of interconnected devices and the increasing reliance on digital infrastructure have made networks vulnerable to a wide range of security threats. Intrusion Detection Systems (IDS) have emerged as a critical component of network security, providing a proactive defense against unauthorized access, malware, and other malicious activities. Traditional IDS approaches often struggle to detect sophisticated attacks like Advanced Persistent Threats (APTs) and zero-day vulnerabilities.

This research presents a novel IDS that addresses the limitations of existing systems by employing advanced detection techniques and a hybrid detection approach. The proposed IDS combines signature-based detection with behavior-based detection, allowing it to effectively identify both known and unknown threats. By utilizing advanced traffic analysis methods, such as flow analysis, traffic profiling, and heuristic- based rule sets, the IDS can detect complex patterns and anomalies indicative of malicious activities.

The primary objective of this research is to develop an IDS capable of detecting a diverse range of threats, including APTs and zero-day attacks, with high accuracy and minimal false positives. The proposed IDS is designed to be adaptable to evolving threat landscapes and scalable to accommodate large-scale networks.

MOTIVATION

The increasing sophistication of cyberattacks, coupled with the growing reliance on digital infrastructure, has created an urgent need for robust and adaptive intrusion detection systems. Traditional signature-based IDS approaches often fall short in detecting advanced threats like Advanced Persistent Threats (APTs) and zero-day vulnerabilities. These attacks can have severe consequences, including data breaches, financial losses, and disruption of critical services.

Our research is motivated by the desire to address these challenges and develop an IDS capable of effectively mitigating emerging threats. By combining signature-based detection with advanced machine learning techniques, we aim to create a more comprehensive and resilient security solution. Our motivation stems from the following key factors:

- Addressing the limitations of traditional IDS: We seek to overcome the limitations of signature-based IDS, which often struggle to detect novel and evasive threats.
- Protecting critical infrastructure: Our research is driven by the imperative to safeguard critical infrastructure and prevent disruptions caused by cyberattacks.
- Contributing to cybersecurity advancements: We aim to contribute to the field of cybersecurity by developing innovative IDS solutions that can enhance network security and protect valuable assets.

LITERATURE REVIEW

- **Classification of intrusion detection system (IDS) based on computer network:**

Intrusion Detection Systems (IDS) have become essential for network security, but traditional signature-based approaches face limitations in detecting novel threats. Anomaly-based IDS, while promising, often suffer from high false positive rates. This study proposes a novel IDS approach that leverages machine learning to overcome these challenges. By employing the Naive Bayes algorithm with optimized feature selection and discretization using k-means clustering, our IDS achieves superior performance in classifying intrusion types. This research demonstrates the potential of machine
learning to significantly enhance IDS effectiveness and provide a more robust defense against emerging cyber threats.(1)

- **A Detailed Investigation and Analysis of Using Machine Learning Techniques for Intrusion Detection**

Intrusion detection remains a critical challenge in today's cyber landscape. While numerous machine learning techniques have been explored, their effectiveness in identifying all types of intrusions is limited. This paper delves into the underlying issues hindering machine learning-based intrusion detection, analyzing various techniques and their associated limitations. By examining attack classification, feature mapping, and the challenges of detecting low-frequency attacks, we provide insights and potential solutions for improvement. Additionally, we compare the detection capabilities of different machine learning techniques and discuss their respective limitations. The paper also highlights relevant data mining tools and outlines future research directions for enhancing intrusion detection using machine learning approaches.(2)

- **Survey of intrusion detection systems: techniques, datasets and challenges**

Cyber-attacks are becoming more sophisticated and thereby presenting increasing challenges in accurately detecting intrusions. Failure to prevent the intrusions could degrade the credibility of security services, e.g. data confidentiality, integrity, and

availability. Numerous intrusion detection methods have been proposed in the literature to tackle computer security threats, which can be broadly classified into Signature- based Intrusion Detection Systems (SIDS) and Anomaly-based Intrusion Detection Systems (AIDS). This survey paper presents a taxonomy of contemporary IDS, a comprehensive review of notable recent works, and an overview of the datasets commonly used for evaluation purposes. It also presents evasion techniques used by attackers to avoid detection and discusses future research challenges to counter such techniques so as to make computer systems more secure.(3)

- **Emerging Trends of Recently Published Datasets for Intrusion Detection Systems (IDS)**

Intrusion Detection Systems (IDS) have become indispensable for safeguarding modern networks against the escalating sophistication of cyberattacks. To effectively develop and evaluate IDS, researchers rely on comprehensive datasets that accurately represent contemporary threat landscapes. This analysis explores seven recent datasets published for IDS research, highlighting their contributions to advancing IDS development and their role in enabling novel research endeavors. The discussion emphasizes the need for more modern datasets, particularly for emerging technologies like IoT and smartphones, to ensure the security of evolving networks and communication channels. Additionally, a taxonomy is proposed to assist researchers in selecting suitable datasets for their specific research objectives.(4) [5] [6] [7] [8] [9]

PROJECT TITLE	OBJECTIVES	TECHNOLOGIES USED	KEY FINDINGS
Intrusion Detection System (IDS) Based on Machine Learning	Enhance IDS effectiveness using machine learning	Naive Bayes, kmeans clustering, feature selection	Machine learning can significantly improve IDS performance, especially when combined with optimized feature engineering.
A Detailed Investigation and Analysis of Using Machine Learning Techniques for Intrusion Detection	Analyze the limitations of machine learningbased IDS and identify potential solutions	Various machine learning techniques	Machine learning techniques have limitations in detecting all types of intrusions, and further research is needed to address these challenges.
Survey of Intrusion Detection Systems: Techniques, Datasets, and Challenges	Provide a comprehensive overview of IDS techniques, datasets, and challenges	Scapy	Presents a taxonomy of IDS, reviews recent works, and discusses datasets and challenges.
Emerging Trends of Recently Published Datasets for Intrusion Detection Systems (IDS)	Analyze recent datasets for IDS research and identify emerging trends	Suricata and Snort	Highlights the need for more modern datasets, particularly for emerging technologies like IoT and smartphones. Proposes a taxonomy for dataset selection.

Table 1: Literature Review Table

PROBLEM STATEMENT AND OBJECTIVES

Problem statement:

Intrusion Detection Systems (IDS) play a critical role in safeguarding networks from various threats, but traditional approaches often struggle to detect sophisticated attacks and may generate high false positive rates. This project aims to address these limitations by developing a novel IDS that effectively identifies and mitigates a wide range of threats while minimizing false alarms

Objective:

- Install and configure Snort and Suricata on an IDS machine.
- Set up network traffic monitoring using a dedicated interface (NIC) in Promiscuous Mode.
- Implement port mirroring on a router or switch to capture traffic.
- Configure Snort and Suricata to analyze traffic for various network protocols.
- Develop and apply custom IDS rules for detecting common attacks (e.g., SQL injection, XSS).
- Capture network traffic using WireShark and analyze it with Wireshark.
- Simulate common attack types (e.g., port scans, brute force, injection attacks).
- Analyze alerts generated by Snort and Suricata to verify detection capabilities.
- Integrate IDS alerts with a visualization tool (e.g., Snorby, BASE).
- Test IDS response times and performance under various network loads.
- Regularly update IDS rule sets to ensure detection of new threats.
- Optimize configurations to minimize false positives and maximize detection accuracy.

METHODOLOGY OF THE PROJECT

. Data Collection and Preprocessing

- **Packet Capture:** Use tools like Scapy, Snort, or Suricata to capture network traffic on the specified interface. Ensure the IDS machine is connected in promiscuous mode to collect all traffic, including packets not destined for it.
- **Data Cleaning:** Filter and preprocess the collected traffic to remove any irrelevant data, normalize packet values, and eliminate noise. This ensures the dataset is clean and usable for further analysis.
- **Feature Engineering:** Extract meaningful features from the raw packet data, such as flow statistics (e.g., packet size, time intervals), protocol anomalies, frequency of certain requests, and time-based patterns to assist in detecting potential attacks.

2. **Model Development and Training**

- **Signature-Based Detection:** Build a database of known attack signatures by collecting patterns of previous attack traffic. Snort's rule-based system allows for detection by matching incoming traffic against predefined rules (e.g., SQL injection signatures or brute force attempts).

- **Anomaly-Based Detection:**
  - **Baseline Establishment:** Use statistical methods or machine learning algorithms to establish a baseline of normal network traffic behavior. This involves monitoring network traffic for a period to understand normal operations and any deviations.
  - **Model Training:** Train machine learning models like Support Vector Machines (SVM), Random Forest, or Neural Networks to recognize deviations from the baseline, which could indicate anomalies or potential attacks.

3. Intrusion Detection

- **Real-time Analysis:** Continuously analyze incoming packets against the predefined rules or trained anomaly detection models to detect real-time threats. Both Snort and Suricata will use these predefined rules for real-time traffic inspection.
- **Alert Generation:** When suspicious packets or patterns are detected, the system triggers alerts. Snort can generate alerts based on signatures and anomalies, which can

be viewed through the system's alert engine.

- **Alert Classification:** Categorize the detected threats based on their severity (e.g., low, medium, high) and type (e.g., DoS, SQL injection, brute force) to allow network administrators to prioritize and respond appropriately.

4. Evaluation and Refinement
   - **Performance Metrics:** Evaluate the IDS's effectiveness using metrics such as detection rate, false positive rate, and false negative rate. These metrics will determine how well the IDS can distinguish between legitimate and malicious traffic.
   - **Refinement:** Continuously improve the IDS by:
     - Updating and refining signature rules based on new threat intelligence.
     - Fine-tuning configurations to reduce false positives and false negatives.
5. **Integration and Deployment**
   - **Integration:** Ensure that the IDS is integrated with existing network security infrastructure like firewalls, intrusion prevention systems (IPS), and SIEM tools for enhanced security operations and threat monitoring.
   - **Deployment:** Deploy the IDS in the target network environment (e.g., LAN, DMZ) where it will monitor network traffic for malicious activity. Ensure the deployment is aligned with the network architecture (e.g., router or switch) and traffic flow.
   - **Testing:** Perform live traffic testing by simulating attack scenarios (e.g., SQL injection, brute force attacks) to ensure the IDS triggers accurate alerts and performs efficiently in real-time.
6. **Use of Router and Switch in IDS Setup**
   - **Router Setup**: Use routers for network segmentation and traffic filtering. For IDS monitoring, routers can be configured to mirror traffic using SPAN (Switched Port Analyzer) or port mirroring, which will direct traffic to the IDS machine for analysis.
   - **Switch Setup:** If using a switch, ensure that it supports port mirroring to allow all traffic to be analyzed by the IDS machine.
   - **Network Configuration:** Proper configuration of routers and switches allows the IDS system to monitor traffic efficiently without affecting the network's normal operations.

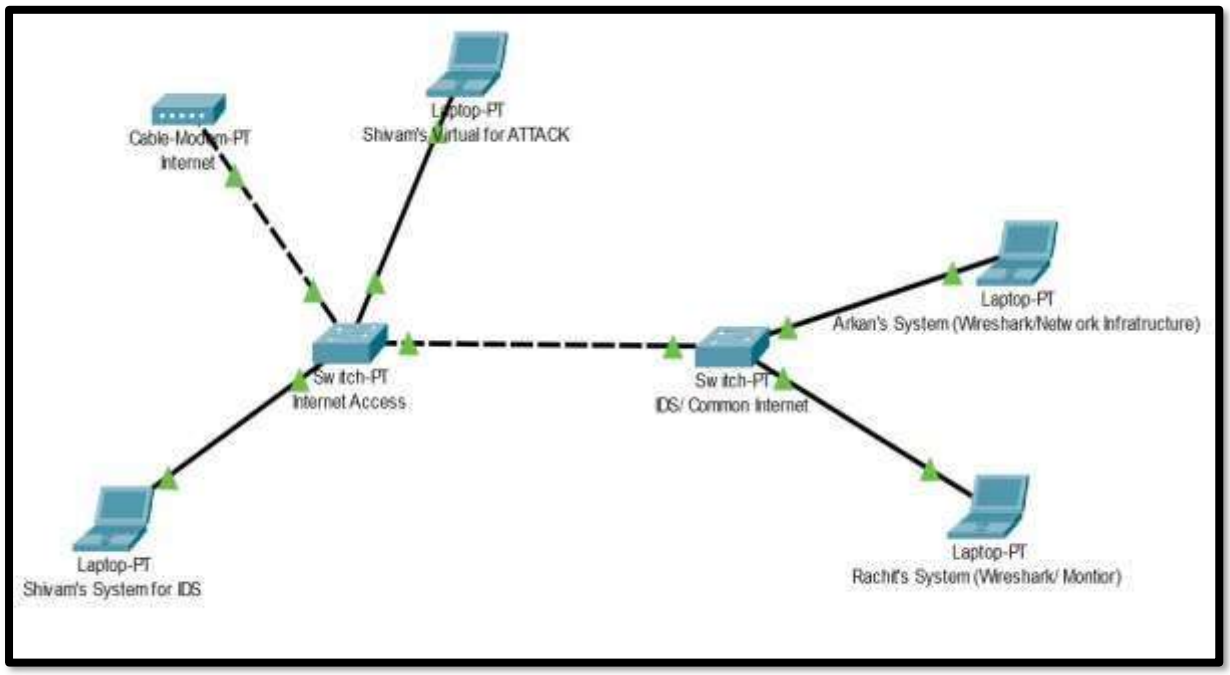


Fig.1: Network Configuration

7. Visualization and Analysis

- **Alert Monitoring:** Use tools like **Snorby** or **BASE** for real-time visualization of IDS alerts. This helps in monitoring detected threats, categorizing them, and enabling quick responses.
- **Traffic Analysis:** Leverage **Wireshark** or **Tcpdump** for in-depth analysis of network traffic. These tools will assist in verifying detected threats and ensure that the IDS is functioning as expected.

1. Details of tools, software, and equipment utilized. PLATFORM USED

For this project, we have used various technologies that are essential for building and testing an Intrusion Detection System (IDS), with a detailed evaluation of their purpose and usage.

PROGRAMMING LANGUAGE: PYTHON

- Python is used due to its versatility, ease of integration with network libraries, and widespread use in network security tools.

Network Libraries:

- **Scapy**: A powerful Python library for packet manipulation and analysis, ideal for network- based IDS.
- **Libpcap:** A C library for packet capture, used in many network tools and libraries.
- **Npcap:** A Windows port of libpcap for packet capture on Windows systems.

Operating Systems:

- **Linux (Ubuntu):** The primary OS used for IDS deployment due to its flexibility, security features, and open-source nature. Ubuntu is chosen for installing and configuring tools like Snort, Suricata, and other security-related packages.
- **Windows:** Can be used for IDS development but is limited compared to Linux, particularly for network traffic capture and analysis.

Other Tools:

- **Snort:** A popular open-source IDS that can be integrated with Python using the libpcap library.
- **Suricata:** Another high-performance IDS engine that can be integrated with Python.
- **Bro:** A network security monitoring framework that can be used for IDS development.
- **Elasticsearch:** A distributed search engine that can be used for storing and analyzing large amounts of IDS data.

2. Environmental Setup SOFTWARE REQUIREMENTS

The software setup for this project includes:

- **Ubuntu (Linux):** Used for the IDS system setup and configuration.
- **Snort and Suricata:** Installed on the Ubuntu system to detect and analyze network traffic.
- **Wireshark:** Used to monitor and capture network traffic for traffic analysis and to verify IDS alerts.
- **Kali Linux:** Used as the attacker system to simulate various network attacks (e.g., SQL Injection, Brute Force, DoS).
- **Routers:** Two routers are utilized in this project to simulate a segmented network environment. One router acts as the gateway to the internet (WAN), while the other router segments the internal network (LAN), providing additional layers of security and ensuring efficient traffic monitoring.
  - o **Router Configuration:** Traffic mirroring (SPAN or Port Mirroring) is configured on the routers to forward network traffic to the IDS machine (Ubuntu).
  - o **Router Setup:** The routers are configured to filter and forward traffic, enabling the IDS to monitor both external and internal traffic efficiently.
- **Cisco Packet Tracer:** Used to simulate the network environment and visualize the IDS

setup with Snort, helping in the simulation and testing of different attack scenarios and network configurations. Cisco Packet Tracer aids in simulating traffic patterns and IDS responses in a controlled virtual environment before real-world deployment.

The IDS system runs on Ubuntu with Snort or Suricata, while Kali Linux is used to generate traffic for attack simulations. The routers ensure proper network segmentation, and Wireshark allows for real -time network traffic analysis to monitor IDS alerts and traffic patterns

Implementation

The implementation of the Intrusion Detection System (IDS) project involves setting up and configuring multiple tools and technologies to detect, analyze, and respond to network intrusions. Below is a detailed step-by-step implementation guide:

1. **Network Setup**

Network Segmentation with Routers:

- Router Configuration: Two routers are used to create a segmented network environment:
  - **Router 1** (WAN side) connects to the internet. o **Router 2** (LAN side) handles traffic within the internal network.
  - **Traffic Mirroring**: Router 1 is configured to mirror network traffic to the IDS machine. This is done using Port Mirroring or SPAN (Switched Port Analyzer) to capture all traffic passing through the network.

Virtual Machines (VMs):

- Victim Machine: Ubuntu or Kali Linux configured as the target machine for testing.
- Attacker Machine: Kali Linux used for simulating attacks, such as SQL Injection or Brute Force.
- IDS Machine: Ubuntu or another Linux distribution running Snort and Suricata for monitoring network traffic.

2. **IDS Tool Setup**

Installing and Configuring Snort on IDS Machine:

- Step 1: Install Snort on Ubuntu: sudo apt-get install snort

- Step 2: Configure the network interface for Snort:
  - Edit the snort.conf configuration file to specify the network interface and set up rules.
  - sudo nano /etc/snort/snort.co
  - Set the HOME_NET variable to the local network's IP range (e.g., 192.168.1.0/24).
  - Set the EXTERNAL_NET variable to !HOME_NET to define external network traffic.

3. **Final Testing**

Test the IDS System:

- After configuration, test the IDS by running attack simulations from Kali Linux.
- Ensure that Snort and Suricata detect these attacks and generate appropriate alerts.

Visualize Alerts:

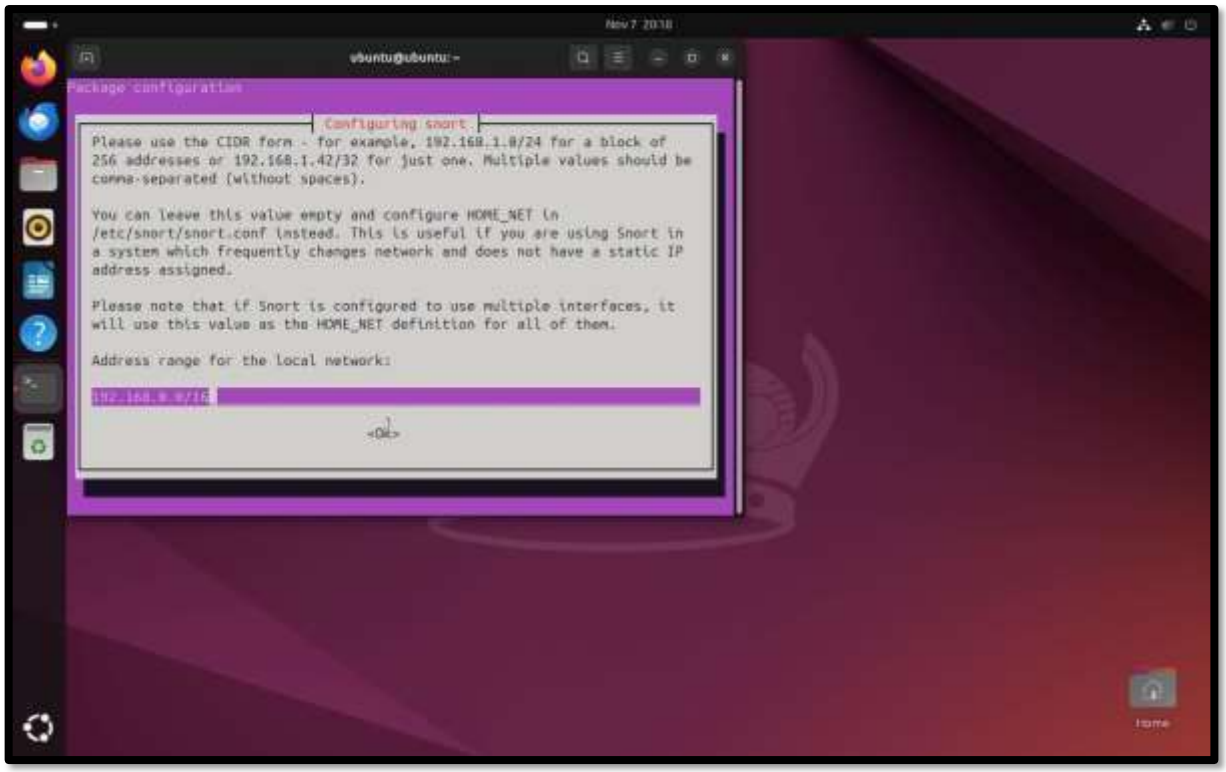
- Use tools like Snorby or BASE to visualize and manage Snort alerts in a more user-friendly interface.
- Analyze the patterns of detected attacks and improve detection rules as needed.

RESULTS AND ANALYSIS

1. INSTALL URBUNTU (LINUX OS) SYSTEM



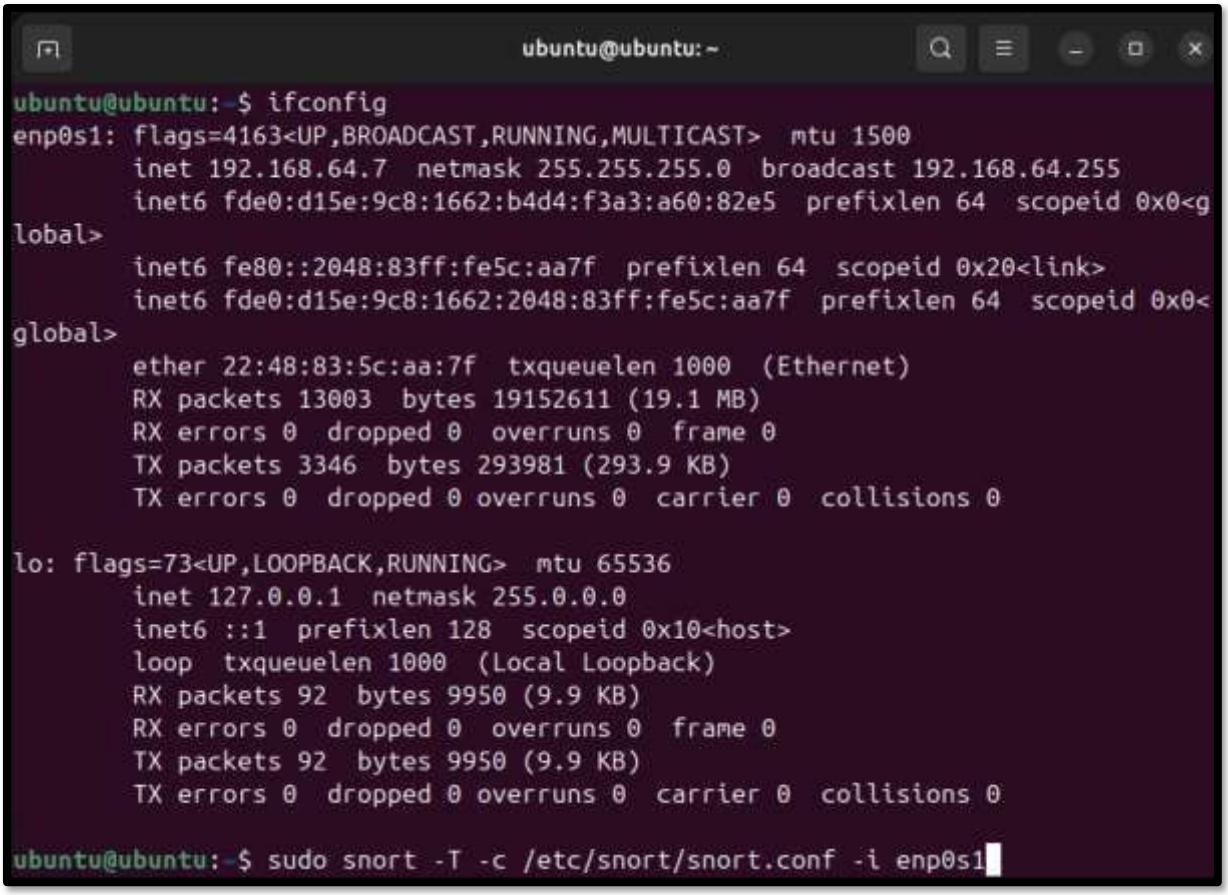
2. Install Snort Tool :



3. IP ADDRESS of KALI IPCONFIG



4. **UBUNTU IP ADDRESS**

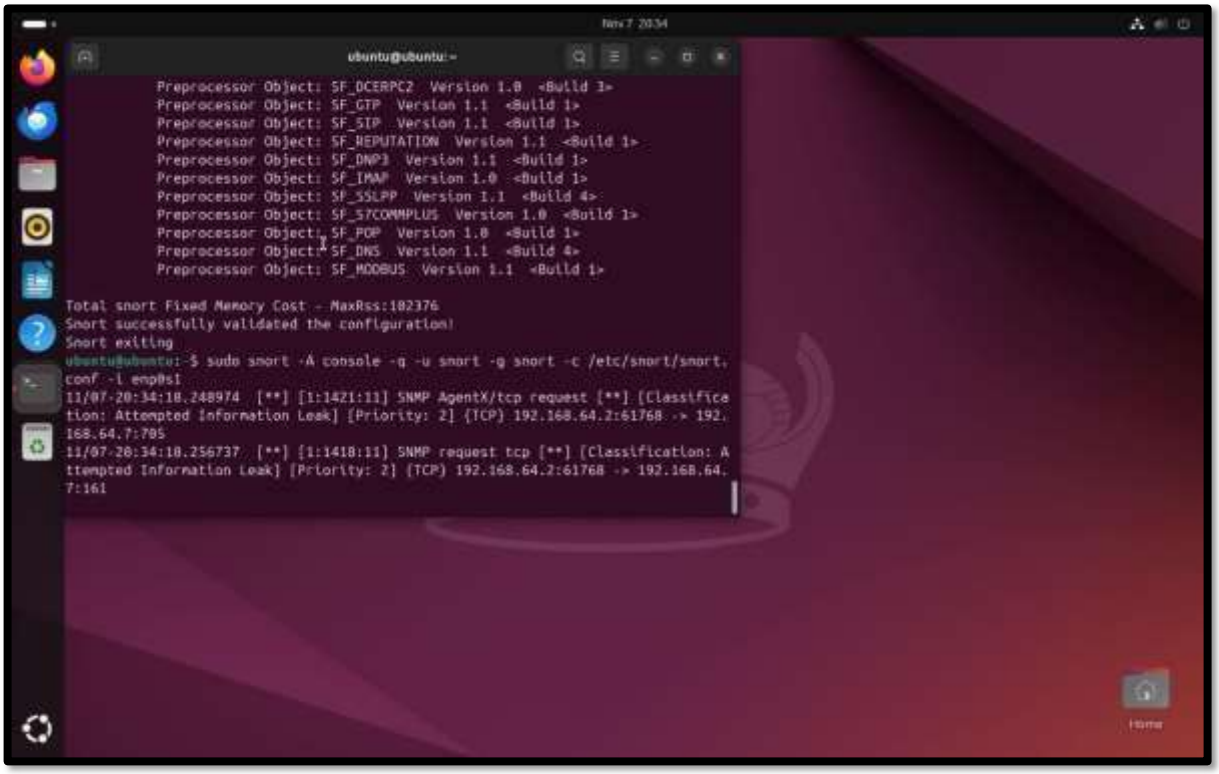


5. **Nmap ATTACK FROM KALI LINUX TO UBUNTU SYSTEM**



6. **AN IDS IDENTIFIES THE TYPE OF ATTACK AND PROVIDES THE IP ADDRESS OF THE ATTACKER.**

```
ubuntu@ubuntu:~$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.
conf -i enp0s1
11/07-20:34:18.248974  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classifica
tion: Attempted Information Leak] [Priority: 2] {TCP} 192.168.64.2:61768 -> 192.
168.64.7:705
11/07-20:34:18.256737  [**] [1:1418:11] SNMP request tcp [**] [Classification: A
ttempted Information Leak] [Priority: 2] {TCP} 192.168.64.2:61768 -> 192.168.64.
7:161
```



7. ROUTERS AND GROUP PHOTOS







CONCLUSION

To build an IDS with Snort or Suricata, set up a dedicated machine, configure network interfaces for promiscuous mode, and install the chosen IDS software. Create rules to detect attacks like SQL injection, port scanning, and brute force. Capture network traffic using Wireshark, analyze it with Wireshark, and use tools like Snorby or BASE to manage alerts. Regularly update rules and refine configurations for optimal protection.

Hardware:

- Powerful machine with sufficient CPU and RAM
- Network interface cards configured for promiscuous mode **Software:**
- Install Snort or Suricata
- Configure rules to detect attacks (SQL injection, port scanning, etc.) **Traffic Analysis:**
- Capture traffic using WireShark
- Analyze captured packets with Wireshark

Testing:

- Simulate attacks with tools like SQLmap and Nmap
- Verify IDS detection capabilities **Alert Management:**
- Use Snorby, BASE, or SIEM tools for alert visualization and analysis
- **Optimization:** Regularly update rules
- Fine-tune rules for specific threats
- Review logs and alerts

FUTURE SCOPE

Future directions for IDS research include integrating advanced machine learning techniques like deep learning and anomaly detection to enhance threat detection accuracy. Real-time threat intelligence integration and improved correlation analysis are crucial for timely and effective response. Reducing false positives and automating incident response through SOAR integration are key priorities. Cloud-based IDS solutions and IoT security considerations will also be essential in the evolving threat landscape.

REFERENCES

1. Effendy, D. A., Kusrini, K., & Sudarmawan, S. (2017, November). Classification of intrusion detection system (IDS) based on computer network. In *2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE)* (pp. 90-94). IEEE.

2. Mishra, P., Varadharajan, V., Tupakula, U., & Pilli, E. S. (2018). A detailed investigation and analysis of using machine learning techniques for intrusion detection. *IEEE communications surveys & tutorials*, *21*(1), 686-728.

3. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, *2*(1), 1-22.

4. Jindal, R., & Anwar, A. (2021). Emerging trends of recently published datasets for intrusion detection systems (IDS): A survey. *arXiv preprint arXiv:2110.00773*.

5. A. Borkar, A. Donode and A. Kumari, "A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS)," *2017 International Conference on Inventive Computing and Informatics (ICICI)*, Coimbatore, India, 2017, pp. 949-953, doi: 10.1109/ICICI.2017.8365277.

6. Mayank Agarwal, Sanketh Purwar, Santosh Biswas, Sukumar Nandi, "Internal Detection System for PS- Poll DOS attack in 802.11 networks using real-time discrete event system",IEEE,vol.4,issue4,2017.

7. Kim, J., & Lee, Y. (2020). A study on the performance evaluation of Snort and Suricata IDS. Proceedings of the 2020 International Conference on Information and Communication Technology Convergence (ICTC), 1051-1055. DOI: 10.1109/ICTC49870.2020.9289423

8. Patel, A., & Rathod, V. (2019). Comparative analysis of Snort and Suricata intrusion detection systems. Proceedings of the 2019 International Conference on Intelligent Computing and Communication (ICICC), 1-5. DOI: 10.1109/ICICC.2019.8713132

9. Al-Janabi, S., & Al-Shoura, M. (2019). Enhancing Snort IDS using machine learning algorithms. Proceedings of the 2019 International Conference on Computer and Information Sciences (ICCIS), 1-5. DOI: 10.1109/ICCIS.2019.8715380