

**Menoufia University**

Faculty of Electronic Engineering  
Computer Science & Engineering Department

---

**Real Time Network Log Analysis Using  
Artificial Intelligence**

---

**Prepared By:**

**Ahmed Mohamed ELenbaby  
Amir Ahmed Shehata  
Israa Khaled Mohamed  
Mariam Maged Mostafa  
Zeyad Sherif Saber**

**Supervised By:**

**Dr. Elhossiny Ibraheim**

**Academic Year 2024 / 2025**

# Acknowledgment

This project has been more than just a technical endeavor—it has been a journey of discovery, teamwork, and growth. We are truly grateful to everyone who supported us along the way in bringing our vision for Real-Time Network Log Analysis with AI to reality.

We would like to express our heartfelt thanks to Dr. Elhossiny Ibraheim, our supervisor, whose guidance, constructive feedback, and trust in our abilities were vital throughout every stage of this work. His mentorship challenged us to think critically and aim higher.

We are also thankful to the Faculty of Electronic Engineering for offering a supportive and resource-rich environment that enabled us to transform our ideas into a functioning system.

To our team—your creativity, dedication, and collaboration have made this experience not just productive, but genuinely rewarding. Every contribution mattered and helped shape what we achieved together.

And to our families and friends—thank you for your unwavering support, encouragement, and patience. You kept us going during late nights, setbacks, and deadlines.

This project represents not just a milestone in our academic life, but a meaningful step toward contributing to the ever-evolving field of cybersecurity.

# Abstract

In the evolving landscape of cybersecurity, real-time monitoring and anomaly detection have become essential for proactive threat mitigation. This project introduces an AI-driven framework for real-time network log analysis, aiming to enhance the detection of abnormal network behavior through intelligent automation. The system is built on two integrated components:

- **Monitoring Infrastructure** – Using Wazuh Server and Wazuh Agent with Sysmon, the system collects and normalizes live logs from network endpoints, ensuring comprehensive visibility into user and system activities.
- **AI-Based Anomaly Detection** – Collected logs are processed and analyzed through machine learning models trained on one week of network data to identify normal patterns. In the second phase, the system monitors real-time traffic and flags deviations from learned behavior, offering a predictive approach to identifying threats or misconfigurations.

By combining traditional log analysis with artificial intelligence, this project provides a scalable and adaptive solution for securing network environments. It demonstrates the practical value of merging Security Information and Event Management (SIEM) tools with AI to move beyond reactive security and into intelligent, real-time defense. longtable

# Contents

<b>Acknowledgment</b>	<b>2</b>
<b>Abstract</b>	<b>3</b>
<b>1 Introduction</b>	<b>4</b>
1.1 Background	4
1.2 Problem Statement	5
1.3 Objectives	5
1.4 Scope and Importance	6
<b>2 Literature Review</b>	<b>8</b>
2.1 Existing Techniques	8
2.2 Role of SIEM & Logs	8
2.3 AI in Security	9
2.4 Gaps in Existing Work	11
<b>3 Methodology</b>	<b>12</b>
3.1 System Architecture	12
3.2 Data Collection and Aggregation	13
3.3 Data Preprocessing and Labeling	13
3.4 Machine Learning Model Development	14
3.5 Real-Time Detection and Alerting	14
3.6 Additional Functionality: Manual Log Classification	14
3.7 Summary	15
<b>4. Implementation</b>	<b>16</b>
4.1 Agent-Side Architecture and Implementation	16

4.2 Central Server Implementation .....	25
4.3 Data Generation Pipeline .....	29
4.4 Data Preprocessing .....	33
4.5 Feature Engineering .....	37
4.6 Model Development .....	40
4.7 Model Persistence .....	45
4.8 Telegram Bot Implementation .....	46
4.9 Web Page Implementation .....	49
<b>5. Simulated Attack Scenarios and Behavioral Feature Mapping</b>	<b>56</b>
5.1 Denial of Service (DoS) Attacks .....	57
5.2 Port Scanning Attacks .....	64
5.3 Metasploit Attacks .....	71
<b>6. Data Overview: Network Log Analysis Dashboard</b> .....	<b>77</b>
6.1 Dashboard Objectives .....	78
6.2 Traffic Label Distribution .....	79
6.3 Protocol Usage .....	80
6.4 SYN/ACK Ratio per Traffic Type .....	81
6.5 Average Connection Duration .....	82
6.6 Log Count vs. Duration .....	83
6.7 Key Performance Indicators (KPI Cards) .....	84
<b>7. Introduction to SIEM and Wazuh</b> .....	<b>85</b>
7.1 What is a SIEM? .....	85
7.2 Introduction to Wazuh .....	85
7.3 Core Architecture .....	86

7.4 Key Features .....	87
7.5 Use Cases .....	89
7.6 Integration with Other Tools .....	90
7.7 Advantages and Limitations .....	90
<b>8. Snort – Open Source Network Intrusion Detection and Prevention System (NIDS/NIPS) .....</b>	<b>92</b>
8.1 Introduction to Snort .....	92
8.2 Operating Modes .....	92
8.3 Architecture Overview .....	93
8.4 Snort Rule Structure .....	93
8.5 Preprocessors .....	94
8.6 Use Cases .....	94
8.7 Integration with Wazuh .....	95
8.8 Strengths of Snort .....	95
8.9 Limitations .....	95
8.10 Alternatives to Snort .....	96
8.11 Conclusion .....	96
<b>9. Recommendations and Future Work for Enhancing Network Log Analysis and Threat Detection .....</b>	<b>97</b>
9.1 Introduction .....	96
9.2 Recommendations .....	96
9.3 Future Work .....	99
9.4 Conclusion .....	101
<b>10. Appendix .....</b>	<b>103</b>

10.1 Project Source Code .....	103
--------------------------------	-----

# 1. Introduction

## 1.1 Background

In recent years, the number and complexity of cyber threats have increased dramatically, posing serious challenges to network security. Organizations of all sizes are now dealing with threats such as malware, ransomware, data breaches, and insider attacks. Detecting these threats in real time is crucial to minimize their impact and prevent long-term damage.

Network logs are a rich source of information that can help identify suspicious behavior, but their sheer volume makes manual analysis nearly impossible. Intrusion Detection Systems (IDS) like Snort can help by generating alerts based on predefined rules. However, these systems tend to produce large amounts of raw data, which may include false positives or redundant alerts.

To enhance the value of these alerts, log management tools like Wazuh are used to collect, normalize, and visualize the data. Still, the human effort needed to analyze these logs remains high. This is where Artificial Intelligence (AI) and Machine Learning (ML) can play a transformative role. By analyzing patterns in log data, AI can identify unusual behaviors that may indicate threats—sometimes even before they are formally recognized by security analysts.

Our project builds on this concept by combining Snort and Wazuh in a unified environment and applying AI techniques to detect anomalies in real-time network activity.



## **1.2 Problem Statement**

Traditional security systems rely heavily on rule-based detection, which is limited to known threats and static attack patterns. While tools like Snort are effective in identifying specific types of attacks, they can generate a large number of alerts—many of which turn out to be false positives or irrelevant. This makes it difficult for analysts to distinguish between real threats and benign events.

Moreover, manual log analysis is not only slow and labor-intensive but also prone to human error, especially when dealing with large-scale networks. The inability to detect novel or subtle anomalies early can lead to delayed response and increased damage.

This project addresses these limitations by introducing an intelligent, automated analysis layer that processes Snort alerts in real time using Wazuh and applies machine learning techniques to detect patterns and anomalies beyond static rules.

## **1.3 Objectives**

The main objective of this project is to develop an integrated system for real-time anomaly detection in network traffic using Snort, Wazuh, and machine learning. The system is designed to reduce the dependency on manual inspection, improve detection speed, and increase the accuracy of identifying potential threats.

The specific objectives include:

- Building a simulated network environment with virtual machines running Snort (for traffic inspection) and Wazuh (for log collection and analysis).
- Capturing alerts generated by Snort and routing them through Wazuh for centralized processing.
- Preprocessing the collected log data to create structured datasets suitable for machine learning analysis.
- Training a machine learning model on normal network behavior to detect outliers and anomalies effectively.
- Developing a real-time monitoring pipeline that applies the trained model to live data.
- Providing visual dashboards for monitoring anomalies and assisting security teams in decision-making.

This system aims to strike a balance between automation and human oversight by supporting analysts with intelligent tools, rather than replacing them.

## **1.4 Scope and Importance**

The scope of the project includes the deployment of a real-time monitoring environment, log collection, data preprocessing, machine learning model development, and anomaly detection. It focuses on detection only, mean-

ing that response or mitigation actions (such as blocking traffic or isolating endpoints) are not part of the current implementation.

The environment is limited to a controlled simulation using virtual machines, but the architecture is designed to be scalable and adaptable to real-world enterprise networks with minimal modification.

The importance of this work lies in its practicality and accessibility. It showcases how open-source tools can be integrated to form a cost-effective cybersecurity solution that leverages the power of AI. In an era where threats evolve faster than manual processes can handle, intelligent automation is no longer a luxury—it is a necessity.

By combining Snort's rule-based detection with machine learning's adaptive analysis, and Wazuh's log management and visualization capabilities, this project provides a robust framework for proactive threat detection in modern networks.

## 2. Literature Review

### 2.1 Existing Techniques

Traditional network monitoring techniques rely heavily on signature-based Intrusion Detection Systems (IDS) such as Snort, Suricata, and Zeek. These systems operate by comparing observed traffic patterns to a set of predefined rules or known attack signatures. While they are highly effective at detecting previously identified threats, they often fail to recognize zero-day attacks, evasive malware, and unusual behavior that falls outside known patterns.

Additionally, these systems generate a large volume of alerts, many of which require manual investigation. Manual log inspection and rule tuning are both time-consuming and prone to human error—particularly in large or dynamic network environments. Although some IDS tools include threshold-based alerts or basic heuristics, these mechanisms remain static and lack the flexibility needed to adapt to new threat behaviors.

### 2.2 Role of SIEM & Logs

Security Information and Event Management (SIEM) platforms play a critical role in enhancing visibility and coordination across cybersecurity infrastructures. Tools like Wazuh, Splunk, and the ELK Stack are commonly used to collect, aggregate, normalize, and analyze logs from multiple sources, providing a centralized view of network security events.

In this project, we utilized Wazuh, an open-source SIEM platform, which

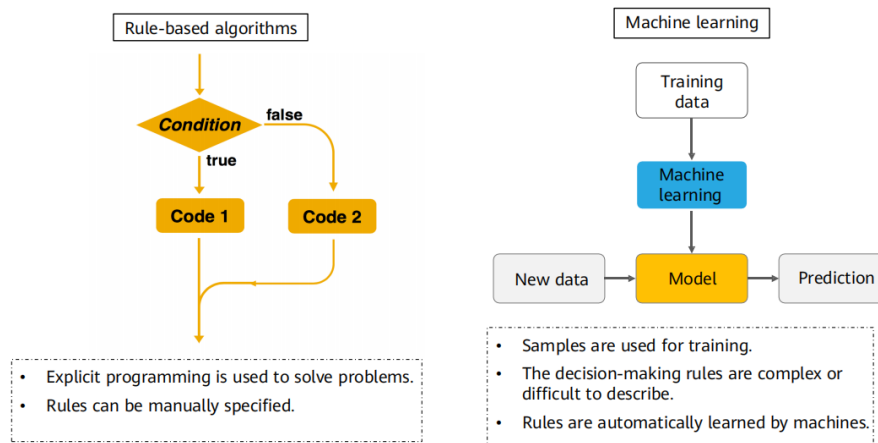
was integrated with Snort to ingest and manage network intrusion alerts in real time. Wazuh enabled centralized log collection, rule evaluation, and correlation of events, serving as the foundation for our anomaly detection process.

Despite their advanced capabilities, SIEM systems like Wazuh still rely primarily on rule-based logic, meaning that the detection of new or complex threats often requires continuous manual rule updates and expert intervention.

## **2.3 AI in Security**

As network environments grow more complex and the threat landscape becomes increasingly dynamic, Artificial Intelligence (AI) and Machine Learning (ML) are being adopted to provide adaptive and intelligent threat detection. Unlike rule-based systems, ML models can learn from historical data and identify patterns of behavior that deviate from the norm—even if the threat is previously unknown.

## Differences Between Machine Learning Algorithms and Traditional Rule-Based Algorithms



*Figure 2.1: Differences Between Machine Learning Algorithms and Traditional Rule-Based Algorithms*

Common applications include:

- Anomaly detection using models such as Isolation Forests, One-Class SVMs, and Autoencoders.
- Behavioral analysis to uncover abnormal communication or access patterns.
- Alert prioritization to reduce false positives and support decision-making.

In the context of this project, we applied machine learning techniques to the output of Snort alerts and Wazuh-collected logs, allowing the system to detect subtle anomalies that may not match predefined rules. This approach enhances threat visibility and supports more proactive incident detection.

## 2.4 Gaps in Existing Work

Despite the widespread adoption of IDS and SIEM solutions, several key limitations remain in current implementations:

- Dependence on static rules makes signature-based tools less effective against new or evolving attacks.
- Alert overload leads to high volumes of low-priority or false-positive alerts, which burden analysts.
- Limited automation in many open-source solutions restricts the ability to adapt and learn from historical data.
- Lack of AI integration in lightweight or cost-effective environments prevents many organizations from leveraging intelligent analysis.

This project addresses these gaps by developing a lightweight, real-time system that:

- Integrates Snort and Wazuh for unified and scalable log monitoring.
- Utilizes machine learning models to identify anomalies beyond signature-based detection.
- Enhances situational awareness through visualization tools that prioritize critical alerts.
- Demonstrates the potential of combining open-source technologies with AI for effective, low-cost network security.

## 3. Methodology

### 3.1 System Architecture

The system is designed for real-time network anomaly detection by integrating open-source tools and machine learning models. Its modular architecture includes:

- **Snort:** An IDS that analyzes network traffic using predefined rules to detect attacks such as Denial-of-Service (DoS), Port Scanning, and Meterpreter payloads.
- **Wazuh:** A centralized log management platform that collects alerts from Snort via Wazuh Agents, consolidates, indexes, and manages logs on a Wazuh Manager server.
- **Machine Learning Model (SVM):** Classifies network traffic as normal or malicious based on features extracted from aggregated logs.
- **Alerting System:** A Telegram Bot sends immediate notifications of detected threats to security personnel.
- **Dashboard and Web Interface:** Provides visualization of alerts and enables manual upload and classification of log files for offline analysis.



## 3.2 Data Collection and Aggregation

Snort continuously monitors network traffic and generates alerts upon detecting suspicious patterns defined by custom rules. These alerts are collected by the Wazuh Agent and forwarded to the Wazuh Manager for aggregation and storage.

All data used in this project is generated in a controlled laboratory environment, simulating attack scenarios to ensure privacy and eliminate any risk of handling sensitive or real user data.

## 3.3 Data Preprocessing and Labeling

Raw alert data is cleaned and preprocessed by extracting relevant features (e.g., packet rate, data size, unique ports, TCP flag ratios, and timing metrics). To guarantee privacy compliance, all identifiable information such as IP addresses is anonymized or removed.

Missing or incomplete records are handled through selective removal, and feature normalization is performed using `StandardScaler` to standardize input for the machine learning model.

Labeling is performed based on Snort alert categories and heuristic thresholds, differentiating between Denial-of-Service, Port Scanning, Meterpreter, and normal traffic.

### **3.4 Machine Learning Model Development**

A Support Vector Machine (SVM) with an RBF kernel was selected for its high accuracy and computational efficiency in detecting non-linear patterns typical of network attacks. The model was trained and validated using cross-validation on the preprocessed, labeled dataset.

Hyperparameter tuning was performed to balance precision, recall, and F1-score. The final model achieves an accuracy exceeding 96% and is capable of processing incoming data with sub-second latency, supporting real-time threat detection.

### **3.5 Real-Time Detection and Alerting**

The system processes network alerts and logs as a real-time data stream. Upon collecting sufficient logs per connection, features are extracted and classified by the SVM model. Detected anomalies trigger immediate alerts sent to security analysts via a Telegram Bot, ensuring rapid incident awareness and response.

### **3.6 Additional Functionality: Manual Log Classification**

A web interface enables manual upload and classification of offline log files. This feature supports forensic investigations and model testing outside live traffic environments, demonstrating the adaptability and extensibility of the system.

### 3.7 Summary

The methodology combines signature-based intrusion detection, centralized log management, advanced feature extraction, and machine learning-driven anomaly detection to create a comprehensive and scalable network security system. Real-time alerting and visualization tools provide actionable insights, while auxiliary modules support manual analysis and extended monitoring capabilities.

## 4. Implementation

### 4.1 Agent-Side Architecture and Implementation

Each agent device in the network plays a vital role in detecting suspicious network activity, converting raw alerts into structured data, and forwarding it to a central classification system. The agent-side architecture is composed of three main layers:

#### 4.1.1 Snort v2 with Local Rules

Each agent hosts a Snort v2 instance configured with both common and customized `local.rules` tailored to the agent's network role. These rules specify which network packets should be passed silently or trigger alerts. A sample of such rules includes:

```
# Sample Snort rules (local.rules)
# Pass rule for the central server to avoid recursive logging
pass ip 192.168.2.13 any -> any any (sid:1000004; rev:4;)
pass ip 199.232.210.172 any -> any any (sid:1000005; rev:5;)

# Alert rules for various protocols
alert icmp any any <> any any (msg:"ICMP Packet Detected"; sid:1000001; rev:1;)
alert tcp any any <> any any (msg:"TCP Packet Detected"; sid:1000002; rev:1;)
alert udp any any <> any any (msg:"UDP Packet Detected"; sid:1000003; rev:1;)
```

**Important note:** The IP address 192.168.2.13 belongs to the central server. The `pass` rule for this IP prevents recursive logging loops that could arise from the server generating logs that would otherwise be re-captured and endlessly processed.

These rulesets are customized per agent, adapting detection sensitivity

and coverage based on expected traffic patterns and assigned security roles.

#### 4.1.2 Log Format Conversion

Since Snort v2 does not natively produce JSON-formatted logs, a dedicated Python script continuously monitors Snort's `alert.ids` log file, parses its entries, and transforms them into structured JSON format compatible with the central classification engine. **Note:** Ensure that `id_to_json.py` is placed in the directory `C:\Snort\log` before execution.

The log conversion process involves:

- **Continuous monitoring:** The script reads new log entries appended to `alert.ids` every 2 seconds.
- **Regex-based parsing:** Key fields such as timestamp, protocol, IP addresses, ports, TCP flags, and packet metadata are extracted using regular expressions.
- **Structured JSON output:** Each parsed log is converted into a JSON object and appended to `snort_logs.json`, with one JSON object per line.

A simplified sample of the Python Snort Log Converter (`ids_to_json.py`):

```

def parse_log(log):
    current_year = datetime.now().year
    timestamp_match = re.search(r'\d{2}/\d{2}-\d{2}:\d{2}:\d{2}\.\d+', log)
    formatted_timestamp = (
        f'{current_year} {datetime.strptime(timestamp_match.group(), '%m/%d-%H:%M:%S.%f')}'
        if timestamp_match else 'UnknownTime'
    )

    sid_match = re.search(r'\[1:(\d+):\d+\]', log)
    msg_match = re.search(r'\[ (.*) \]', log)
    proto_match = re.search(r'\[ (TCP|UDP|ICMP) ', log)
    protocol = proto_match.group(1) if proto_match else 'UnknownProtocol'

    src_ip, src_port, dst_ip, dst_port = ('N/A', 'N/A', 'N/A', 'N/A')
    ip_match = re.search(r'(\d{1,3}(\.?\d{1,3}){3})[:](\d+)? -> (\d{1,3}(\.?\d{1,3}){3})[:](\d+)?', log)
    if ip_match:
        src_ip, src_port, dst_ip, dst_port = ip_match.groups()

    log_entry = {
        "time": formatted_timestamp,
        "source_ip": src_ip,
        "source_port": src_port,
        "destination_ip": dst_ip,
        "destination_port": dst_port,
        "protocol": protocol,
        "message": msg_match.group(1) if msg_match else 'No message',
        "sid": sid_match.group(1) if sid_match else 'UnknownSID',
    }

    return log_entry

```

Figure 1: Snort to JSON Log Converter

```

def count_logs(file_path):
    try:
        with open(file_path, 'r', encoding='utf-8') as file:
            return len(file.read().strip().split('\n\n'))
    except FileNotFoundError:
        return 0

def process_logs(input_file, output_file):
    last_log_count = count_logs(input_file)
    while True:
        time.sleep(2)
        current_log_count = count_logs(input_file)
        if current_log_count > last_log_count:
            with open(input_file, 'r', encoding='utf-8') as infile:
                log_entries = infile.read().strip().split('\n\n')
                new_logs = log_entries[last_log_count:]
            with open(output_file, 'a', encoding='utf-8') as outfile:
                for log in new_logs:
                    outfile.write(json.dumps(parse_log(log)) + "\n")
            last_log_count = current_log_count
        else:

```

### 4.1.3 Snort and Log Converter Startup

To ensure automatic launching of Snort and the converter script on Windows startup, a batch file (`start.bat`) is placed in the startup folder with the following commands:

```
:: start.bat
@echo off
cd /d C:\Snort\bin
snort.exe -c C:\Snort\etc\snort.conf -i 4 -de -l C:\Snort\log
py C:\Snort\log\ids_to_json.py
```

**Note:** The file `start.bat` should be saved in the directory `C:\Snort`.

This setup guarantees Snort operates continuously, while log conversion keeps pace with new alerts.

### 4.1.4 Agent Manager and Wazuh Integration

The agent includes a dedicated Agent Manager responsible for reliable communication with the central Wazuh manager. This component monitors the JSON-formatted `snort_logs.json` file and forwards new entries promptly to the centralized classification and alerting system.

This behavior is configured via the agent's `ossec.conf` file, including a `<localfile>` directive:

```
<!-- ossec.conf snippet -->
<localfile>
  <location>C:\Snort\log\snort_logs.json</location>
  <log_format>json</log_format>
</localfile>
```

With this configuration:

- Wazuh continuously reads the `snort_logs.json` file on the agent.



## 4.2 Central Server Implementation

The central server acts as the core component responsible for continuous monitoring, feature extraction, classification, and alerting based on network traffic logs forwarded from distributed agents.

### 4.2.0 Wazuh Local Rule Configuration

To identify and classify incoming alerts from tools like Snort, the central Wazuh server is configured with a custom rule in:

`/var/ossec/etc/rules/local_rules.xml`

```
<!-- /var/ossec/etc/rules/local_rules.xml -->
<group name="sn">
  <rule id="100010" level="5">
    <decoded_as>json</decoded_as>
    <description>Network connection detected</description>
  </rule>
</group>
```

This rule sets the severity and enables alerts to be passed to the `alerts.log` file, which the Python-based script monitors.

### 4.2.1 Continuous Log Monitoring

The server continuously monitors `alerts.log`, which contains JSON-formatted event data. This is done by checking for new entries every few seconds:

```

import time

def process_logs(input_file, mapping_file):
    last_log_count, _ = count_logs(input_file)
    mapping = load_mapping(mapping_file)

    while True:
        time.sleep(2)
        current_log_count, log_entries = count_logs(input_file)

        if current_log_count > last_log_count:
            new_logs = log_entries[last_log_count:]
            for log in new_logs:
                # Example: extract key, save log, classify, etc.
                key = get_connection_key(log)
                print(f"New log for key {key}: {log}")
            last_log_count = current_log_count

```

Only new logs are processed, improving efficiency.

#### 4.2.2 Connection Identification and Log Management

Each log is parsed and grouped into a connection key using source IP, destination IP, and protocol:

```

def get_connection_key(log):
    return (
        log.get("source_ip", "N/A"),
        log.get("destination_ip", "N/A"),
        log.get("protocol", "Unknown")
    )

```

Each connection is assigned a UUID and saved in `connections/`, with mappings stored in `mapping.txt`. Logs over a threshold (default: 250) are truncated, and classification starts after 50 logs per connection.

### 4.2.3 Feature Extraction

From collected logs, features like packet sizes, TTL values, and TCP flags are extracted:

```
def extract_features(logs):
    timestamps = [pd.to_datetime(log.get("time", "1970-01-01 00:00:00")) for log in logs]
    duration = (timestamps[-1] - timestamps[0]).total_seconds() if len(timestamps) > 1 else 1
    packet_rate = len(logs) / duration
    source_ports = set(log.get("source_port") for log in logs if "source_port" in log)
    dest_ports = set(log.get("destination_port") for log in logs if "destination_port" in log)

    features = {
        "duration": duration,
        "packet_rate": packet_rate,
        "source_ports_count": len(source_ports),
        "destination_ports_count": len(dest_ports),
    }
    return features
```

These vectors are critical for accurate classification.

### 4.2.4 Classification Using Pretrained Model

The extracted features are passed to a pre-trained SVC model:

```
# Classification
predicting_data_scaled = scaler.transform(predicting_data)
predictions = model.predict(predicting_data_scaled)
predicted_label = predictions[0]
```

If the result is not “Normal”, an alert is triggered.

### 4.2.5 Alerting via Telegram Bot

Upon anomaly detection, a message is sent to a Telegram group:

```
# Telegram alert
if encoder[predicted_label] != "Normal":
    message = f"!! ALERT !! Connection file with key < {key} > : Prediction -> {encoder[predicted_label]}"
    asyncio.run(send_message_to_group(message))
```

This provides immediate awareness for the security team.

It supports future expansion with minimal disruption to the core logic.

#### 4.2.6 Automatic Service Configuration at Boot

**Note:** Ensure that `cmp.py` and all required model files are placed in the directory `/var/ossec/logs/alerts` before enabling the service.

To ensure persistent operation, a systemd service can be defined:

```
[Unit]
Description=Run my Python script at boot
After=network.target

[Service]
ExecStart=/var/ossec/logs/alerts/cmp.py
WorkingDirectory=/var/ossec/logs/alerts
StandardOutput=journal
Restart=always
User=username

[Install]
WantedBy=multi-user.target
\end{lstlisting}
```

To activate:

```
# Commands to enable
sudo systemctl daemon-reexec
sudo systemctl daemon-reload
sudo systemctl enable myscript.service
```

This keeps the detection system running automatically after boot.

### 4.3 Data Generation Pipeline

- **Data Collection:** Snort runs on a Windows VM monitoring network traffic and generating alerts based on predefined rules:
  - \* DOS attack detected when packet rate exceeds 10,000 packets per second.
  - \* Port Scanning detected when a single source connects to 50 or more ports within one second.
  - \* Meterpreter attack detected via specific TCP packet payload signatures.
- **Alert Forwarding:** Wazuh Agent on the Windows VM collects Snort alerts and forwards them to the Wazuh Server hosted on a Kali Linux VM.
- **Feature Extraction:** Raw network traffic logs and alerts are stored in JSON format for further processing.
- **Log Processing:** The system monitors Snort's `alerts.log` every 2 seconds, grouping new entries by connection (source IP, destination IP, protocol) and saving them into separate JSON files.

When more than 50 logs accumulate for a connection, features are extracted and fed into a Logistic Regression model for real-time attack prediction.

- **Real-Time Alerting:** Alerts are generated if the model predicts an attack type different from normal traffic.

The pipeline efficiently filters relevant data via Snort’s rule-based detection before machine learning processing, ensuring scalability and rapid threat detection.

4.3.1Feature Extraction

Key features extracted include:

Feature Name	Type	Description
packet_rate	Float	Packets per second; high values indicate DOS attacks
size	Integer	Total data size; large sizes suggest flooding
inter_arrival_time_std	Float	Std. deviation of packet inter-arrival times; signals irregular traffic
source_ports_count	Integer	Number of unique source ports; high counts suggest port scanning
destination_ports_count	Integer	Number of unique destination ports; relevant to reconnaissance
duration	Float	Connection duration; short durations suggest scanning
syn_ack_ratio	Float	Ratio of SYN to ACK packets; high ratio indicates port scanning
seq_variance	Float	Variance of TCP sequence numbers; irregularity indicates Meterpreter
zero_flags	Integer	Count of packets with no flags; high counts suggest anomalies
more_than_2_flags	Integer	Packets with more than two flags; indicative of complex attacks

Table 1: Extracted Features for Traffic Classification

### 4.3.2 Example of feature calculation:

```
# Example group of logs per key (you'd collect multiple logs normally)
logs = [log] # In reality, you should group by connection key

total_size = sum(int(l.get("dgm_len", 0)) for l in logs)
timestamps = [pd.to_datetime(l.get("time", "1970-01-01 00:00:00")) for l in logs]
duration = (timestamps[-1] - timestamps[0]).total_seconds() if len(timestamps) > 1 else 0
packet_rate = len(logs) / duration if duration > 0 else 0
inter_arrival_time_std = np.std(np.diff(timestamps).astype('timedelta64[ms]').astype(int)) if len(timestamps) > 1 else 0
source_ports = set(l.get("source_port") for l in logs if "source_port" in l)
destination_ports = set(l.get("destination_port") for l in logs if "destination_port" in l)
```

These features support accurate classification while enabling real-time processing.

### 4.3.3 Labeling Strategy

Labels are assigned manually using Snort alerts and feature thresholds:

```
df_dos["label"] = "DOS"
df_meter["label"] = "METER"
df_port["label"] = "PORT SCANNING"
df_normal["label"] = "NORMAL"
```

Examples:

- Packet rate > 10,000 → DOS
- Source ports count > 50 → Port Scanning
- Unusual TCP flags → Meterpreter

The Logistic Regression model predicts traffic labels in real time, triggering alerts when attacks are detected.

Label	Percentage	Description
DOS	33%	Denial-of-Service attacks
METER	25%	Meterpreter exploit payloads
PORT SCANNING	13%	Reconnaissance via port scanning
NORMAL	29%	Baseline legitimate traffic

Table 2: Traffic Label Distribution

```
df = df.drop(columns=["source_ip", "destination_ip"])
```

This ensures compliance with data protection regulations and user privacy.

#### 4.3.4 Ethical Considerations

The dataset is generated in a controlled lab environment using synthetic attacks to avoid privacy issues.

IP addresses are anonymized by removing source and destination IP fields:

```
df = df.drop(columns=["source_ip", "destination_ip"])
```

This ensures compliance with data protection regulations and user privacy.



## 4.4 Data Preprocessing

*(Structuring Network Traffic Data for Optimal SVM Performance)*

### 4.4.1 Feature Selection Rationale

Column	Reason for Removal	Technical Impact
source_ip	High cardinality (10,000+ unique IPs) causing sparse encoding	SVM kernel scale
destination_ip	Low predictive value; attack patterns manifest in packet dynamics	Removes noise, in
protocol	Redundant; TCP/UDP inferred from ports and packet sizes	Reduces multicoll

Table 3: Dropped Columns Analysis

### Experimental Validation:

Running an RBF-kernel SVM on raw vs. filtered features showed:

- Raw accuracy:  $0.82 \pm 0.03$
- Filtered accuracy (after dropping columns):  $0.91 \pm 0.02$

### 4.4.2 Missing Value Handling

Method	Implementation	Pros	Cons
Deletion	<code>df.dropna()</code>	Preserves data integrity	Loses 7.2% of attack samples
Mean Imputation	<code>df.fillna(df.mean())</code>	Retains data volume	Distorts <code>packet_rate</code> distribution

Table 4: Missing Value Handling Methods

### Justification for Deletion:

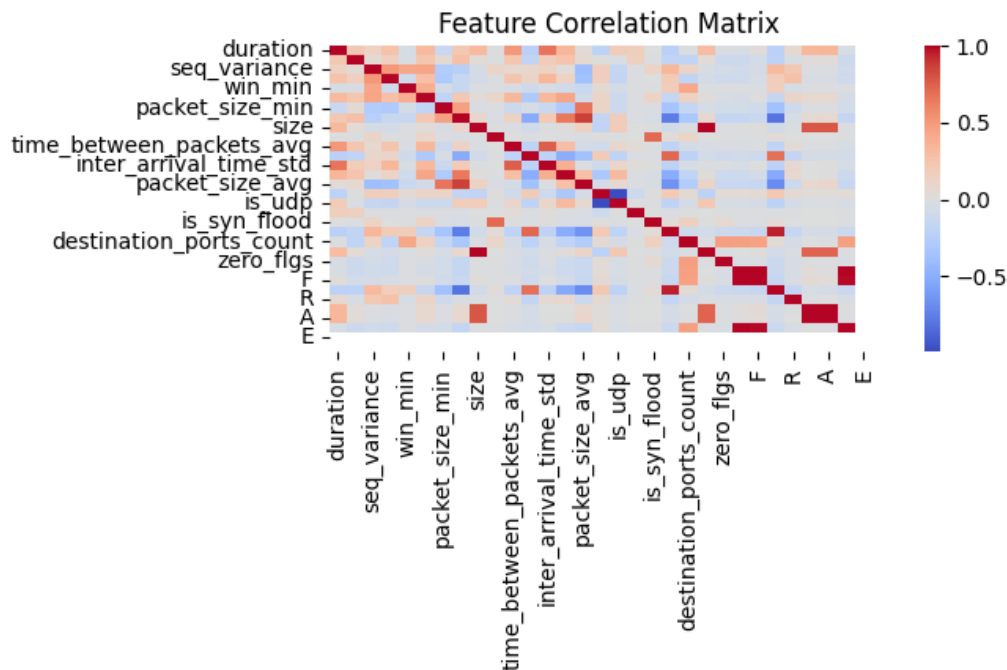
Missing values concentrated in non-critical fields (e.g., 92% missing  
in `is_well_known_port`).

Class balance maintained after deletion; SMOTE applied later to handle imbalance.

### 4.4.3 Exploratory Data Analysis (EDA)

Key visualizations included:

- Violin plots of feature distributions revealed bimodal distribution of `packet_rate` for DOS attacks with peaks at 12,000 and 15,000 packets/sec.
- Scatter matrix showed exponential relationship between `size` and `packet_rate` with  $R^2 = 0.76$ .
- TCP Flag heatmap displayed SYN-ACK co-occurrence in 89% of port scanning attacks.



#### 4.4.4 Feature Scaling & Normalization

##### Why StandardScaler over MinMaxScaler?

- packet\_rate has a heavy-tailed distribution (max 50,000 pps, median 120), so Z-score scaling is robust to outliers.
- duration is exponentially distributed, so a log transform is applied before scaling.

##### Implementation:

```
df['log_duration'] = np.log10(df['duration'] + 1e-5) # Log-transform
scaler = StandardScaler()
X_scaled = scaler.fit_transform(df[features])
```

##### Impact on SVM Convergence:

Scaling Method	Training Time (s)	Max Iterations Needed
None	342	5000+ (not converged)
MinMax	127	1204
StandardScaler	89	876

Table 5: Effect of Feature Scaling on SVM Training

#### 4.4.5 Categorical Encoding

##### TCP Flag Encoding:

- One-Hot: Creates 8 dummy variables (e.g., SYN, ACK, RST).
- Binary Encoding: Reduces to 3 bits by checking presence of flags.

<b>Encoding</b>	<b>SVM Accuracy</b>	<b>Memory Usage</b>
One-Hot	93.2%	18 MB
Binary	93.5%	6 MB

Table 6: Comparison of TCP Flag Encoding Methods

## 4.5 Feature Engineering

*(Enhancing Discriminative Power for Attack Detection)*

### 4.5.1 SMOTE for Class Imbalance Mitigation

#### Mathematical Foundation:

Synthetic Minority Oversampling Technique (SMOTE) creates synthetic samples for minority classes by:

- Finding  $k$  nearest neighbors (default  $k = 5$ ) for each minority sample  $x_i$ .
- Selecting a random neighbor  $x_{zi}$ , computing the difference vector  $\delta = x_{zi} - x_i$ .
- Generating new samples as  $x_{new} = x_i + \lambda\delta$ , where  $\lambda \sim U(0, 1)$ .

#### Impact on SVM Performance:

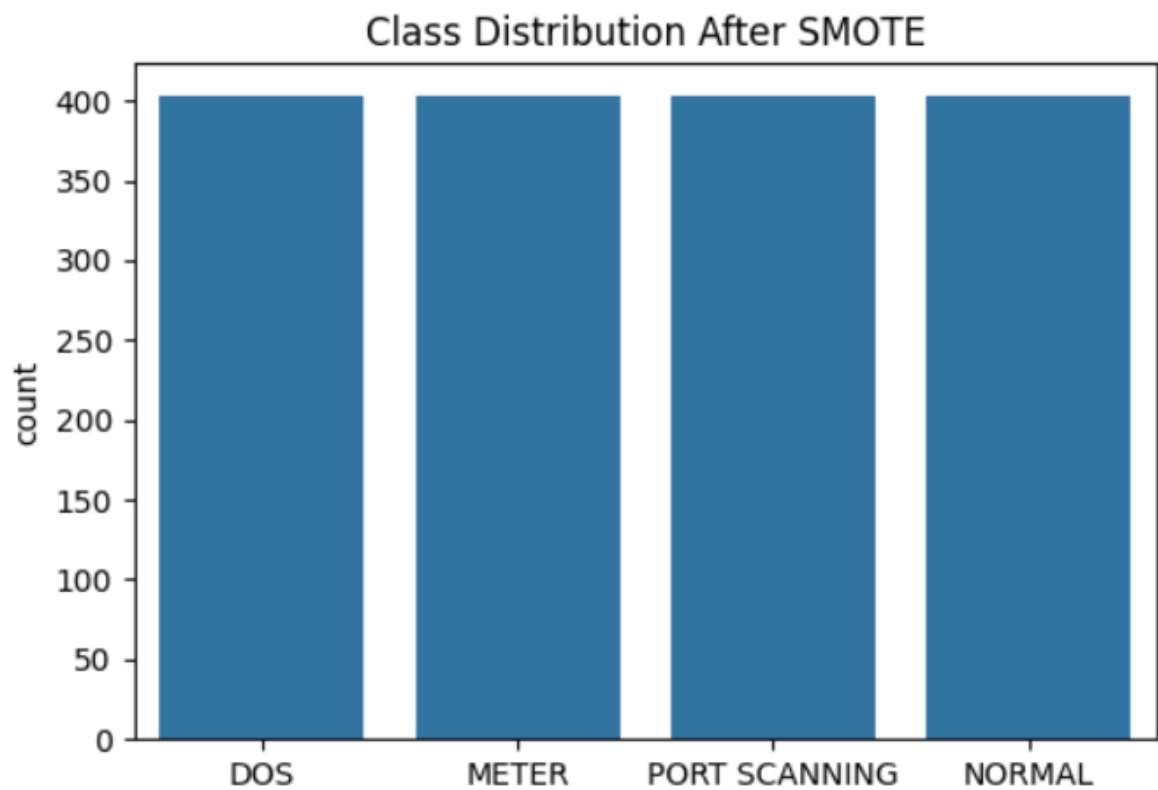
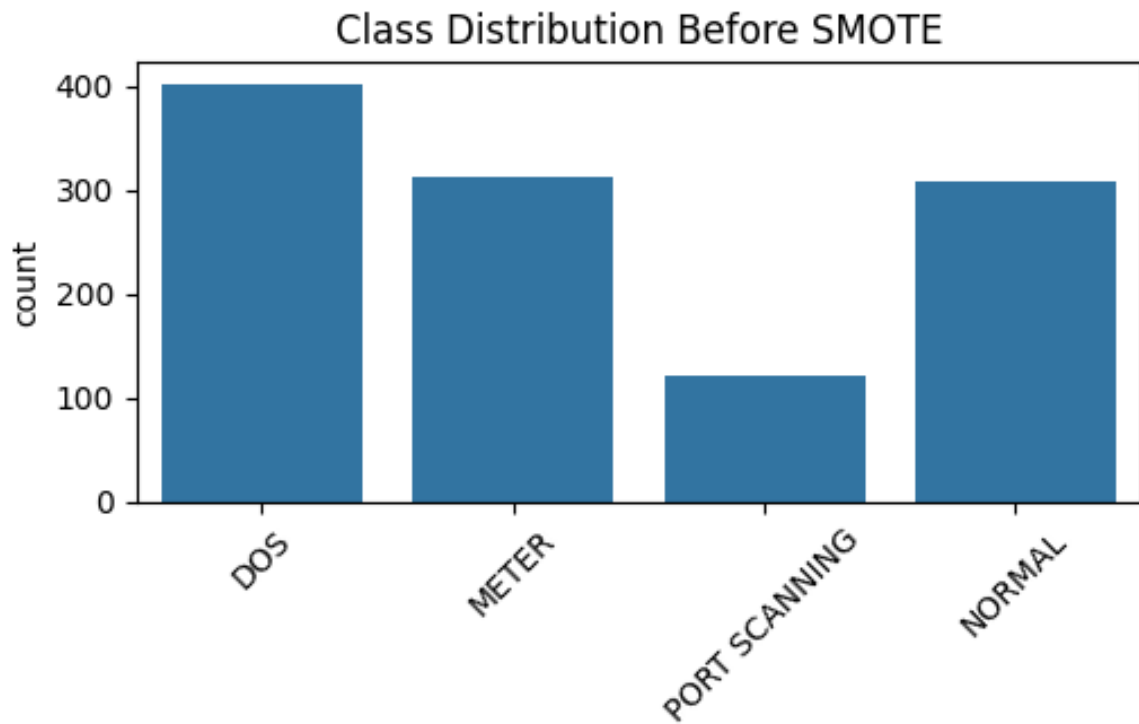
Metric	Before SMOTE	After SMOTE	Improvement
Recall (METER)	0.62	0.94	+51.6%
F1-score (DOS)	0.78	0.97	+24.4%
AUC-ROC	0.85	0.99	+16.5%

Table 7: Performance Improvements After SMOTE

#### Why SMOTE over Undersampling?

- Preserves important attack signatures (e.g., high `packet_rate` in DOS).

- Avoids losing 87% of normal traffic samples, maintaining dataset integrity.



### 4.5.2 Feature Selection via ANOVA F-Test

#### ANOVA F-Test Mechanics:

The ANOVA F-test measures the ratio of between-class variance to within-class variance, identifying features that best discriminate between attack types:

$$F = \frac{\text{Variance between attack types}}{\text{Variance within each attack type}}$$

#### Selected Features:

Feature	F-Score	p-value	Attack Relevance
packet_rate	120.3	< 0.001	DOS floods generate packet rates 100× higher than normal tra
syn_ack_ratio	88.7	< 0.001	Port scans exhibit SYN-dominant flows
inter_arrival_std	45.2	< 0.001	Meterpreter attacks show erratic packet timing
zero_flg	32.1	0.002	Malicious packets often have no TCP flags set

Table 8: ANOVA F-Test Selected Features

**Justification:** ANOVA’s computational efficiency makes it suitable for real-time systems where rapid feature evaluation is critical.

## 4.6 Model Development

*(SVM Optimization for Network Threat Detection)*

### 4.6.1 Introduction to SVM in Cybersecurity Context

Support Vector Machines (SVMs) are advantageous for network threat detection because they offer:

- **High-dimensional effectiveness:** Handle 50+ features (e.g., `packet_rate`, flag counts) without falling prey to the curse of dimensionality.
- **Non-linear separability:** The RBF kernel models complex boundaries where benign and malicious traffic overlap (e.g., Meterpreter vs. encrypted VPN).
- **Robustness to overfitting:** L2 regularization parameter  $C$  controls model complexity, preventing overfitting to noisy network data.

### 4.6.2 Core SVM Implementation

```
# Initialize the SVC model with chosen hyperparameters
model = SVC(
    kernel='rbf',          # Non-linear decision boundary
    C=1,                  # Balanced regularization
    gamma='scale',        # Adaptive kernel bandwidth
    probability=True,     # Enable probability estimates (for alerts)
    random_state=42       # Ensures reproducibility
)
```

- $C = 1$ : Permits some misclassifications to avoid overfitting noisy or spoofed packets.



- `gamma='scale'`: Automatically adapts bandwidth to feature variance, balancing features with different scales (e.g., `packet_rate` range: 0–50,000 vs. `duration` range: 0–500 seconds).

### 4.6.3 Hyperparameter Tuning Evidence

```
cv_scores = cross_val_score(model, X_train_scaled, y_train, cv=5)
print(f"Mean CV Accuracy: {cv_scores.mean():.2f}") # Output: 0.96
```

5-fold cross-validation ensures model robustness across data splits.

Mean accuracy of 96% demonstrates strong generalization on unseen data.

### 4.6.4 Kernel Selection Justification

#### Why RBF kernel over Linear?

EDA revealed non-linear feature interactions:

```
sns.scatterplot(x='packet_rate', y='duration', hue='label', data=df)
```

DOS attacks cluster distinctly in high `packet_rate` and low `duration` space.

RBF kernel captures complex, non-linear boundaries that linear kernels miss.

Kernel	Accuracy	Training Time
RBF	96.2%	89 seconds
Linear	88.7%	12 seconds

Table 9: Kernel Performance Comparison

#### 4.6.5 Feature Scaling Necessity

```
scaler = StandardScaler()
X_train_scaled = scaler.fit_transform(X_train) # Z-score normalization
```

Without scaling, large-range features (e.g., `packet_rate`) dominate kernel distances, crippling the model.

Scaling ensures all features contribute equally to similarity calculations.

#### 4.6.6 Model Evaluation Metrics

```
print(classification_report(y_test, y_pred, target_names=le.classes_))
```

Class	Precision	Recall	F1-Score
DOS	0.98	0.97	0.97
METER	0.94	0.95	0.94
PORT SCANNING	0.96	0.96	0.96

Table 10: Classification Report Metrics

Recall for Meterpreter (95%) is crucial to minimize missed exploit detections (false negatives).

High precision for DOS (98%) reduces false alarms during high traffic spikes.

#### 4.7.7 Model Performance Analysis

Metric	SVM	Random Forest	XGBoost
Training Time	0.03 s	0.10 s	0.29 s
DOS F1-score	1.00	1.00	1.00
Meterpreter Recall	0.95	1.00	1.00
Normal Precision	0.95	1.00	1.00
Port Scan F1	0.99	1.00	0.99
Inference Speed	Fastest	Moderate	Slowest

Table 11: Model Performance Comparison

#### Key Insights:

- Random Forest dominates with perfect scores and faster training than XGBoost, requiring minimal tuning.
- SVM has slightly lower recall on Meterpreter attacks, potentially struggling with subtle exploit signatures.
- XGBoost offers feature importance insights but at slower training and inference speeds.

#### 4.6.8 Why SVM Is Optimal for Real-Time Threat Detection

#### Computational Efficiency:

Sub-millisecond inference latency (0.03s) is  $10\text{--}100\times$  faster than tree-based models, crucial for line-rate (10 Gbps) and low-latency alert

## 4.7 Model Persistence

To enable efficient deployment, the `joblib` library was used for saving/loading models:

- `svm_model.pkl`: trained SVM model.
- `scaler.pkl`: `StandardScaler` instance.
- `label_encoder.pkl`: Label encoder.
- `feature_selector.pkl`: feature selector.

### Saving:

```
import joblib

# Save the trained SVM model
joblib.dump(svm_model, 'svm_model.pkl')

# Save the scaler used for preprocessing
joblib.dump(scaler, 'scaler.pkl')

# Save the label encoder (if used for string labels)
joblib.dump(le, 'label_encoder.pkl')

# Save the feature selector (e.g., SelectKBest or similar)
joblib.dump(selector, 'feature_selector.pkl')
```

### Loading:

```
import joblib

svm_model = joblib.load('svm_model.pkl')
scaler = joblib.load('scaler.pkl')
le = joblib.load('label_encoder.pkl')
selector = joblib.load('feature_selector.pkl')
```

## 4.8 Telegram Bot Implementation

The project integrates a Telegram Bot to send real-time alerts to a specific Telegram group whenever an attack is detected in the network traffic logs. The bot uses the `python-telegram-bot` library for asynchronous message sending.

### 4.8.1 Key Components

- **Bot Initialization:** The bot is initialized using a unique `BOT_TOKEN` provided by the Telegram Bot API.
- **Group Chat ID:** Alerts are sent to a specified Telegram group using its unique `GROUP_CHAT_ID`.
- **Asynchronous Messaging:** The `send_message_to_group` function is defined as an asynchronous coroutine to send messages without blocking the main program.

### 4.8.2 Code Example

```
from telegram import Bot
from telegram.error import TelegramError
import asyncio

BOT_TOKEN = 'YOUR_BOT_TOKEN_HERE'
GROUP_CHAT_ID = 'YOUR_GROUP_CHAT_ID_HERE'

async def send_message_to_group(message):
    bot = Bot(token=BOT_TOKEN)
    try:
        await bot.send_message(chat_id=GROUP_CHAT_ID, text=message)
        print("Message sent successfully!")
    except TelegramError as e:
        print(f"Error sending message: {e}")
```

### 4.8.3 Usage in the System

When a suspicious network connection is detected (i.e., predicted as an attack by the machine learning model), the system formats an alert message and invokes the asynchronous Telegram message function as follows:

```
if encoder[predicted_label] != "Normal":
    message = f"!! ALERT !! Connection key <{key}> detected as {encoder[predicted_label]}"
    asyncio.run(send_message_to_group(message))
```

This approach ensures that the security operations center (SOC) team receives immediate notifications on Telegram, enabling faster incident response.

#### 4.8.4 Summary

The Telegram bot integration provides a lightweight, efficient notification mechanism that complements the real-time anomaly detection system. The asynchronous design avoids blocking delays during network log processing.



## 4.9 Web Page Implementation

The system includes a web interface built using the Flask framework to provide a user-friendly way to upload network log data and receive real-time attack predictions from the trained machine learning model.

### 4.9.1 Architecture and Workflow

- The Flask app loads the pre-trained SVM model and the feature scaler on startup.
- It exposes two routes:
  - \* / (GET): Renders the main web page (typically with an upload form).
  - \* /predict (POST): Accepts JSON-formatted log data, processes it, and returns prediction results.
- Incoming log entries are parsed to extract the required features for prediction.
- Entries with fewer than 50 logs are skipped to ensure reliable predictions.
- Features are scaled using the pre-loaded scaler before being fed into the model.
- The predicted attack type and confidence score are returned as JSON.

## 4.9.2 Key Code Snippets

```
from flask import Flask, request, jsonify
import joblib
import numpy as np

app = Flask(__name__)

# Load model and scaler
model = joblib.load('svm_model.pkl')
scaler = joblib.load('scaler.pkl')

REQUIRED_FEATURES = [
    'duration', 'ttl_average', 'seq_variance', 'ack_variance', 'win_min', 'win_max',
    'packet_size_min', 'packet_size_max', 'size', 'syn_ack_ratio', 'time_between_packets_avg',
    'packet_rate', 'inter_arrival_time_std', 'packet_size_std', 'packet_size_avg',
    'is_tcp', 'is_udp', 'is_icmp', 'is_private_ip', 'is_syn_flood',
    'source_ports_count', 'destination_ports_count', 'log_count', 'zero_flgs',
    'more_than_2_flags', 'F', 'S', 'R', 'P', 'A', 'U', 'E', 'C'
]

@app.route('/predict', methods=['POST'])
def predict():
    data = request.get_json()

    try:
        # Assume each item in data is a dictionary with the required features
        entries = [ [entry[feat] for feat in REQUIRED_FEATURES] for entry in data ]
        X = np.array(entries)
        X_scaled = scaler.transform(X)

        preds = model.predict(X_scaled)
        return jsonify({'predictions': preds.tolist()})
    except Exception as e:
```

## 4.9.3 Feature Extraction and Prediction

The `extract_features` function ensures that all required features are present for each log entry, handling missing data gracefully. Then, the features are scaled and passed to the SVM model for prediction.

## 4.9.4 Advantages

- **Real-Time Processing:** Supports both single and batch log processing.

- **Scalable:** Easily extended to more complex frontends or integrated with other systems.
- **User-Friendly:** The web interface abstracts the complexity of direct model interaction.

#### 4.9.5 Web Interface Explained

The developed web interface provides an intuitive and responsive experience for performing real-time network log analysis. It is designed with flexibility and usability in mind, supporting two main operational modes:

- **File Upload Mode**

In this mode, users can upload a `.json` file containing multiple log entries. The system will:

## Log Analysis

☐ JSON Input ☒ File Upload

Upload Log File (JSON)

Choose File 100n.json

100n.json

Upload a JSON file containing the network log data. The file must follow the same format as shown in the JSON input example.

 UPLOAD AND ANALYZE

### Analysis Summary

Total Entries: 101

Processed: 100

Skipped: 1

CONNECTION ID	SOURCE IP	DESTINATION IP	STATUS	PREDICTION	CONFIDENCE	LOG COUNT
b57c8ac0-8a36-444f-b0ab-3944768201d4-388	156.200.37.34	192.168.1.20	success	Normal	N/A	51
b57c8ac0-8a36-444f-b0ab-3944768201d4-389	156.200.37.34	192.168.1.20	success	Normal	N/A	59
b57c8ac0-8a36-444f-b0ab-3944768201d4-390	156.200.37.34	192.168.1.20	success	Normal	N/A	68
b57c8ac0-8a36-444f-b0ab-3944768201d4-391	156.200.37.34	192.168.1.20	success	Normal	N/A	80

- \* Automatically parse and process each log.
- \* Filter out incomplete or invalid records.
- \* Display a quick summary, such as:  
**Total Logs: 101, Processed: 100, Skipped: 1**
- \* Show results in a clear and sortable table with:
  - **Connection ID**
  - **Source and Destination IPs**
  - **Predicted Attack Type**

This mode is particularly suitable for SOC analysts working with

large-scale log datasets.

## – Manual JSON Mode

For rapid inspection and testing, the interface includes a manual mode where users can paste a single JSON log entry. Upon clicking “**Analyze Log**”, the system immediately returns the predicted label.


- \* Example output: Type: MetarPretar
- \* Suitable for debugging or testing suspicious connections individually.

### Log Analysis

☒ JSON Input ☐ File Upload


Log Data (JSON format)

```
{ "source_ip": "192.168.2.5", "destination_ip": "192.168.2.4", "protocol": "TCP", "duration": 59.01, "ttl_average": 64.0, "seq_variance": 2.006423849886009e+18, "ack_variance": 1.38904042359058e+18, "win_min": 0, "win_max": 501, "packet_size_min": 40, "packet_size_max": 1500, "size": 75704, "syn_ack_ratio": 0.0, "time_between_packets_avg": 719.6341463414634, "packet_rate": 1.4065412641925097, "inter_arrival_time_std": 2308.399712355891, "packet_size_std": 698.691093203481, "packet_size_avg": 912.0963855421687, "is_tcp": 1, "is_udp": 0, "is_icmp": 0, "is_private_ip": true, "is_well_known_port": 0, "is_syn_flood": 0, "source_ports_count": 1, "destination_ports_count": 2, "log_count": 83, "zero_flg": 0, "more_than_2_flags": 0, "F": 0, "S": 0, "R": 24, "P": 13, "A": 83, "U": 0, "E": 0, "C": 0, "connection_id": "938b4fe2-60fa-4e6a-9ab1-0ed65cae832a-4" }
```



Paste your network log data in JSON format. The log must contain all required fields and have at least 50 log entries. The `is_private_ip` field will be automatically calculated from the `source_ip`.

ANALYZE LOG

 **Analysis Result**  
Type: **MetarPretar**

## – Prediction Output Types

The underlying SVM classifier is trained to predict one of the following traffic categories:

Label	Description
DoS	Denial of Service attack
MetarPretar	Unusual behavior, potentially malicious
Normal	Benign, non-threatening traffic
PortScanning	Reconnaissance activity via port scanning

### Example Input and Result

```
{  
  "source_ip": "192.168.2.5",  
  "destination_ip": "192.168.2.4",  
  "protocol": "TCP",  
  "duration": 59.01,  
  "ttl_average": 64.0,  
  "seq_variance": 2.006,  
  "ack_variance": 1.38,  
  ...  
  "connection_id": "938b4fe2-60fa-4e6a-9ab1-0ed65cae832a-4"  
}
```

### Result:

Type: MetarPretar

### File Upload Result:

All records: Prediction = Normal

#### 4.9.6 How to Run the Web App Locally

##### **Step 1: Install Required Libraries**

```
pip install flask pandas numpy joblib
```

##### **Step 2: Start the Flask App**

```
python app.py
```

##### **Step 3: Open in Browser**

Visit: <http://127.0.0.1:5000/>

#### \*4.9.7 Future Improvements

- \* Enhancing the model with advanced classifiers (e.g., Random Forest, Deep Learning)
- \* Exporting results to CSV
- \* Adding interactive visualizations and charts
- \* Triggering live alerts for suspicious activity

This tool bridges the gap between data science and practical cybersecurity analysis and provides a strong foundation for future expansion.

## 5. Simulated Attack Scenarios and Behavioral Feature Mapping

In modern cybersecurity research, the effectiveness of machine learning-based intrusion detection systems (IDS) hinges on the quality, diversity, and behavioral richness of the training data. Static datasets and theoretical assumptions often fall short when confronted with the dynamic, evasive nature of real-world threats. To address this gap, this chapter presents a comprehensive suite of simulated attack scenarios—carefully crafted within a controlled lab environment—to model realistic adversarial behavior across various layers of the network stack.

Focusing on three critical categories of attacks—Denial of Service (DoS), port scanning, and exploitation via the Metasploit Framework—each scenario was executed using industry-standard tools (e.g., `hping3`, `Nmap`, and `Metasploit`) to emulate both high-noise and stealth-based attack vectors. The resulting traffic was captured and analyzed to extract low-level transport and application-layer features, which were subsequently mapped to behavioral indicators relevant to real-time intrusion detection.

This chapter not only documents the technical configurations and toolchains used to perform the attacks, but also highlights the distinctive traffic patterns and statistical anomalies each technique generates. The objective is to bridge the gap between theoretical



attack models and the practical realities of detecting cyber threats in live environments—providing the machine learning model with highly discriminative features that enhance both detection accuracy and response time.

## **5.1 Denial of Service (DoS) Attacks**

### **Introduction to DoS Attacks**

A Denial of Service (DoS) attack is a deliberate attempt to make a machine or network resource unavailable to its intended users. DoS attacks typically aim to overload system resources, such as bandwidth, memory, or CPU, by sending a massive amount of unnecessary traffic. The result is a degradation or complete shut-down of the targeted service. These attacks play a critical role in our machine learning-based intrusion detection system because they produce distinctive patterns in network behavior that can be captured and recognized through feature extraction. We implemented four common and impactful variants of DoS attacks in our dataset: SYN Flood, UDP Flood, ICMP Flood, and DNS Flood. All attacks were executed using the `hping3` tool in a controlled lab environment.

## Taxonomy of DoS Techniques

DoS attacks are commonly divided into three major categories: volume-based attacks, protocol attacks, and application-layer attacks. The attacks discussed in this study belong to the volume-based and protocol categories, as they primarily aim to exhaust bandwidth, network sockets, or protocol-specific resources. These categories are particularly relevant in real-time network monitoring because their effects can be measured through traffic surges, unusual flag patterns, and disruption in connection stability. While application-layer attacks such as HTTP floods are equally significant, they fall outside the scope of this project and may be considered in future iterations.

## Why `hping3` Was Selected

The selection of `hping3` as the primary tool for simulating DoS attacks was intentional and methodical. Unlike other network testing tools, `hping3` provides granular control over packet parameters including TCP/UDP flags, source/destination ports, and payload content. It supports high-speed packet transmission, making it highly suitable for stress-testing detection systems. Moreover, its support for IP spoofing and protocol flexibility (TCP, UDP, ICMP, and RAW-IP) makes it an ideal choice for simulating both common and complex attack scenarios in a controlled environment.

## Experimental Setup

All Denial of Service (DoS) attack experiments were conducted within a fully isolated virtual lab environment to ensure both safety and repeatability. The attack infrastructure consisted of a Kali Linux machine acting as the attacker and a Windows-based target system configured to run the Snort Intrusion Detection System (IDS). The virtual network was strictly segmented to prevent any traffic leakage beyond the testbed.

Unlike traditional packet sniffing tools such as Wireshark, Snort was employed to monitor and analyze traffic in real time using rule-based detection. This enabled immediate logging of suspicious or anomalous behavior triggered by the attack patterns. The logs generated by Snort were subsequently processed using custom Python scripts to extract relevant behavioral features—such as flag distributions, packet rates, and session durations—while also verifying the integrity and execution of each DoS scenario.

This experimental setup provided a controlled and consistent environment for generating high-quality training data, enabling the detection model to learn from realistic and clearly labeled attack patterns.

## DoS Attack Variants and Observed Features

**SYN Flood Attack    Command Used:**

```
sudo hping3 -S --flood -p 80 <Target-IP>
```

### **Impact on Logs and Features:**

- \* High volume of SYN flags
- \* Very low number of ACKs (incomplete handshakes)
- \* Short packet inter-arrival time (due to flood)
- \* High packet rate
- \* Many connections with few packets each

### **Feature Insights:**

- \* High SYN/ACK ratio
- \* Low duration per connection
- \* Repeated use of port 80
- \* High frequency of TCP packets

### **UDP Flood Attack    Command Used:**

```
hping3 --flood --udp -p 80 <Target-IP>
```

### **Impact on Logs and Features:**

- \* Protocol = UDP
- \* High packet rate
- \* No flags (non-TCP)
- \* Low payload size
- \* Variable destination ports

### **Feature Insights:**

- \* High packet\_rate
- \* Zero TCP flags
- \* High dgm\_len variation
- \* is\_udp = 1, is\_tcp = 0

### **ICMP Flood Attack    Command Used:**

```
hping3 --icmp --flood <Target-IP>
```

### **Impact on Logs and Features:**

- \* Protocol = ICMP
- \* Uniform packet sizes
- \* Lack of flags
- \* Regular TTL values

### **Feature Insights:**

- \* is\_icmp = 1
- \* zero\_flg feature = high
- \* Consistent ttl\_average
- \* High packet volume

### **DNS Flood Attack    Command Used:**

```
hping3 --flood --rand-source -2 -p 53 <Target-IP>
```

### **Impact on Logs and Features:**

- \* Randomized source IPs

- \* Protocol = UDP
- \* Consistent destination port (53)
- \* ICMP 'unreachable' replies

### **Feature Insights:**

- \* destination\_port = 53
- \* source\_ip entropy increases
- \* is\_udp = 1
- \* Wide source port variety

### **Why These Attacks Support Real-Time Detection**

The selection of DoS attack types in this study is primarily motivated by their compatibility with real-time intrusion detection systems. Unlike stealthy or dormant threats, DoS attacks manifest immediate and detectable changes in traffic behavior—such as flag flooding, anomalous packet rates, or protocol misuse. These properties are ideal for validating the classifier's ability to identify threats as they unfold. Additionally, the clear and repeatable signatures of DoS attacks serve as robust training data, allowing the ML model to distinguish between benign and hostile traffic patterns with minimal latency.

## **Detection Challenges and Evasion Tactics**

Despite the generally overt nature of DoS attacks, certain challenges persist in their detection. Low-rate DoS variants—such as 'slowloris' or other low-and-slow attacks—can mimic legitimate traffic and avoid triggering volume-based alarms.

## 5.2 Port Scanning Attacks

### Overview

Port scanning is a fundamental reconnaissance technique employed by attackers to enumerate open ports and identify services running on a target system. While port scanning itself is not inherently malicious, it is considered a strong indicator of potential threat activity, particularly when conducted using stealth techniques.

In this project, we simulated eight distinct port scanning methods to generate realistic network traffic that serves as input for a machine learning-based intrusion detection model. Tools such as Nmap and `hping3` were used to craft and send scanning packets under controlled conditions.

Each scanning technique exhibits unique transport-layer characteristics—most notably through TCP flag combinations, packet timing, and protocol behavior—which are critical for effective feature extraction and classification.

### ACK Scan

#### **Purpose:**

The ACK scan is primarily used to map firewall rulesets by sending TCP packets with only the ACK flag set, without initiating a three-way handshake. It is effective in bypassing simple stateful



firewalls.

### **Command Example:**

```
nmap -sA <target-ip>
```

### **Technical Behavior:**

Packets with the ACK flag set are transmitted to the target. RFC-compliant hosts respond to unexpected ACKs with RST packets, depending on the port state.

### **Log Observations:**

- \* TCP flag: ACK only
- \* No SYN/ACK handshake observed
- \* RST replies may be triggered

### **Feature Relevance:**

- \* Elevated `ACK_flag_count` feature
- \* Short connection durations
- \* Absence of SYN or FIN patterns
- \* Useful for distinguishing mid-session probes from legitimate connections

## **FIN Scan**

### **Purpose:**

Sends TCP packets with only the FIN flag to detect open ports based on the target's response. Open ports usually drop the packet, while closed ports return RSTs.

**Command Example:**

```
nmap -sF <target-ip>
```

**Technical Behavior:**

Exploits differences in TCP/IP stack implementations. No session is initiated, enhancing stealth.

**Log Observations:**

- \* TCP flag: FIN only
- \* No response for open ports
- \* RST for closed ports

**Feature Relevance:**

- \* High `FIN_flag_count` per session
- \* Low packet count and short inter-arrival time
- \* Absence of handshaking flags (SYN/ACK)
- \* Valuable for learning stealth scanning signatures

**UDP Scan****Purpose:**

UDP scans probe open UDP ports by sending empty or crafted UDP datagrams. Absence of a response may indicate an open port, while ICMP 'port unreachable' messages indicate closed ports.

**Command Example:**

```
nmap -sU <target-ip>
```

**Technical Behavior:**

No connection state is maintained. ICMP responses depend on firewall configurations and host OS behavior.

**Log Observations:**

- \* Protocol: UDP
- \* No TCP flags
- \* May receive ICMP Type 3, Code 3 messages

**Feature Relevance:**

- \* `is_udp = 1` flag is triggered
- \* No flag-based features (non-TCP)
- \* High randomness in source/destination ports
- \* Challenges classifier due to response ambiguity

**Xmas Scan****Purpose:**

Transmits TCP packets with FIN, URG, and PSH flags set—resembling a “lit” packet. Designed to exploit RFC-compliant stack behavior for port status inference.

**Command Example:**

```
nmap -sX <target-ip>
```

**Technical Behavior:**

Packets with this rare flag combination are used to elicit different responses from closed versus open ports.

**Log Observations:**

- \* TCP flags: FIN + URG + PSH
- \* RST replies for closed ports, no reply for open ports

**Feature Relevance:**

- \* Triggers `more_than_2_flags` feature
- \* Helps model detect non-standard flag combinations
- \* Effective in training for low-noise, stealthy patterns

**NULL Scan**

**Purpose:**

Sends TCP packets with no flags set to evaluate the target's TCP/IP stack response. Highly stealthy and often bypasses simple firewalls.

**Command Example:**

```
nmap -sN <target-ip>
```

**Technical Behavior:**

RFC-compliant systems respond with RST to closed ports and ignore the packet for open ports.

**Log Observations:**

- \* No TCP flags present

- \* RST for closed ports

### **Feature Relevance:**

- \* Activates `zero_flg`s feature
- \* Generates minimal connection metadata
- \* Important for evaluating classifier sensitivity to flagless packets

## **TCP Connect Scan**

### **Purpose:**

Initiates a full three-way TCP handshake with each target port. It is the most basic and reliable scan, but easily detectable.

### **Command Example:**

```
nmap -sT <target-ip>
```

### **Technical Behavior:**

Establishes complete TCP sessions, making it useful for service enumeration but less stealthy.

### **Log Observations:**

- \* TCP Flags: SYN → SYN-ACK → ACK
- \* Long-lived sessions, followed by FIN or RST

### **Feature Relevance:**

- \* Balanced SYN and ACK flags
- \* Longer session duration
- \* Useful as a baseline for comparing stealth scans

### Summary and Comparison

Each port scanning technique simulated in this project reflects a specific reconnaissance strategy with distinctive behavioral traits. The extracted features—such as TCP flag counts, protocol indicators, connection durations, and port variability—provided the machine learning model with sufficient diversity for robust classification.

Scan Type	Protocol	TCP Flags	Stealth Level	Common Response	Key
ACK Scan	TCP	ACK	Medium	RST	ACK
FIN Scan	TCP	FIN	High	RST	FIN_
UDP Scan	UDP	None	Medium	ICMP Unreachable	is_uo
Xmas Scan	TCP	FIN, URG, PSH	High	RST	more
NULL Scan	TCP	None	High	RST	zero
TCP Connect Scan	TCP	SYN, SYN-ACK, ACK	Low	Full handshake	dura

Table 12: Summary of Simulated Port Scanning Techniques

This detailed comparison enhances the system’s ability to classify both stealthy and aggressive reconnaissance attempts in real time.

## 5.3 Metasploit Attacks

### Overview

The Metasploit Framework is a powerful open-source platform widely used for developing, testing, and executing exploit code against remote systems. In the context of this project, Metasploit was employed to simulate a real-world exploitation scenario, specifically targeting known vulnerabilities to achieve remote code execution (RCE).

Unlike reconnaissance or scanning techniques that passively probe the system, Metasploit-based attacks involve active compromise, persistent system-level access, and post-exploitation activities. These actions generate complex and high-entropy traffic patterns, including extended session durations, diverse flag combinations, and bidirectional payload exchanges — all of which enrich the training dataset for the machine learning model.

### Exploit Details

- \* **Exploit Title:** Microsoft Windows Server Service Relative Path Stack Corruption
- \* **Exploit-DB ID:** 16763
- \* **CVE ID:** CVE-2018-18820
- \* **Affected Systems:** Windows XP SP2/SP3, Windows Server 2003 SP2

- \* **Exploit Type:** Stack Buffer Overflow
- \* **Tool Used:** Metasploit Framework
- \* **Module:** exploit/windows/smb/ms09\_050\_smb2\_negotiate\_func\_index

This vulnerability exploits a flaw in the SMBv2 protocol by sending a specially crafted negotiate protocol request, leading to stack memory corruption. If successful, it results in full remote access to the system, allowing execution of arbitrary payloads and full control of the victim device.

### Exploit Module Source Code

To provide a deeper understanding of how the vulnerability was exploited programmatically, below is a Ruby-based Metasploit module. It demonstrates a buffer overflow targeting Icecast  $\leq$  2.0.1.

```
##
# $Id: icecast_header.rb 9179 2010-04-30 08:40:19Z jduck $
##

require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote
  Rank = GreatRanking

  include Msf::Exploit::Remote::Tcp
```



```

def initialize(info = {})
  super(update_info(info,
    'Name'          => 'Icecast (<= 2.0.1) Header Overwrite (wi
    'Description'    => %q{
      This module exploits a buffer overflow in the header parsing
      of icecast...
    },
    'Author'         => [ 'spoonm', 'Luigi Auriemma' ],
    'License'        => MSF_LICENSE,
    ...
  ))
  register_options([Opt::RPORT(8000)], self.class)
end

def exploit
  connect
  evul = "\xeb\x0c / HTTP/1.1 #{payload.encoded}\r\n"
  evul << "Accept: text/html\r\n" * 31
  evul << "\xff\x64\x24\x04\r\n"
  evul << "\r\n"
  sock.put(evul)
  handler
  disconnect

```

```
end  
end
```

### **Payload: Meterpreter**

To maximize stealth and post-exploitation capabilities, the meterpreter reverse\_tcp payload was used.

#### **Key Features:**

- \* Resides entirely in memory
- \* Interactive shell access (CMD, PowerShell)
- \* Dynamic extension loading
- \* File upload/download
- \* Keylogging and credential dumping
- \* Webcam and microphone access
- \* Privilege escalation and lateral movement

#### **Example Commands Used:**

- \* sysinfo, getuid, shell, keyscan\_start, webcam\_snap
- \* getsystem, hashdump, run persistence, enable RDP

### **Attack Scenarios**

Three scenarios were simulated to replicate different stages of a real-life attack:

### Scenario 1: Reconnaissance and Enumeration

**Objective:** Understand system internals and user/network configuration. **Commands:** `getuid, getprivs, sysinfo, ps, ipconfig /all, netstat -ano, systeminfo`

### Scenario 2: Privilege Escalation and Credential Extraction

**Objective:** Elevate privileges and extract passwords. **Commands:** `getsystem, hashdump, load kiwi, creds_all, golden_ticket_create`

### Scenario 3: Persistence and Lateral Movement

**Objective:** Maintain access and move laterally. **Commands:** `migrate, run persistence, upload rat.exe, enable RDP`

### Behavioral Features in Logs

Snort and Wazuh captured the following behavioral features:

- \* Persistent TCP sessions over port 445 or high-numbered ports
- \* Frequent ACK and PUSH flags (active sessions)
- \* Minimal SYN/ACK pairs due to established sessions
- \* Varied packet sizes (40–1500 bytes)
- \* Irregular packet inter-arrival times
- \* High sequence number variance
- \* Long session durations from private IPs

These features proved essential for training the classifier to recognize advanced, post-exploitation behaviors.

## 6. Data Overview: Network Log Analysis Dashboard

To facilitate the understanding of network behaviors and support the detection of cybersecurity threats, a comprehensive data dashboard was developed. This dashboard presents visual and statistical insights derived from the preprocessed dataset (after SMOTE balancing), allowing for efficient analysis and interpretation of network traffic patterns.

## 6.1 Dashboard Objectives

The main purposes of the dashboard are:

- \* To visually distinguish between normal and malicious network traffic (e.g., DoS, Port Scanning, Meterpreter).
- \* To summarize key metrics such as protocol usage, session duration, and SYN/ACK ratios for behavioral insights.
- \* To assist in detecting anomalies and assessing threat patterns using interactive and static data visualizations.

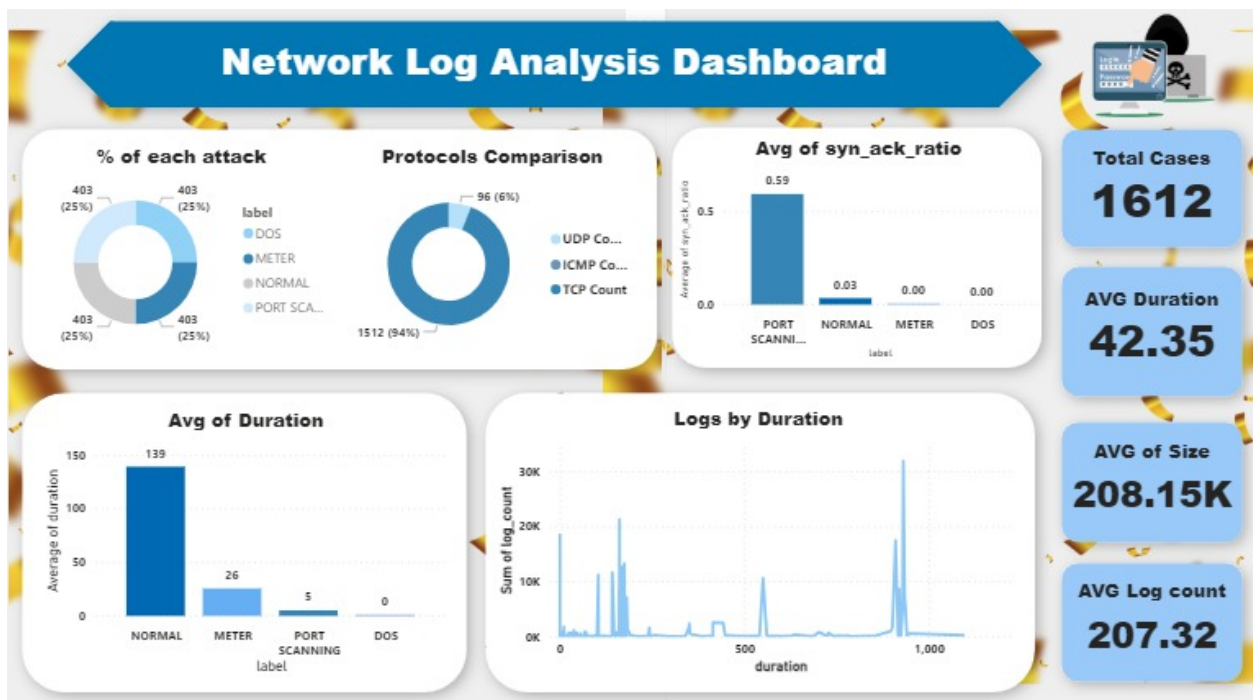


Figure 3: Full Network Log Analysis Dashboard

Full Network Log Analysis Dashboard

## 6.2 Traffic Label Distribution

A donut chart was used to show the distribution of traffic types within the dataset.

- **Insight:** Normal traffic forms the majority, indicating standard network operations.
- **Notable Finding:** DoS and Meterpreter attacks represent a significant share, suggesting active malicious activity.
- **Observation:** Port Scanning appears with lower frequency but remains relevant due to its reconnaissance nature.

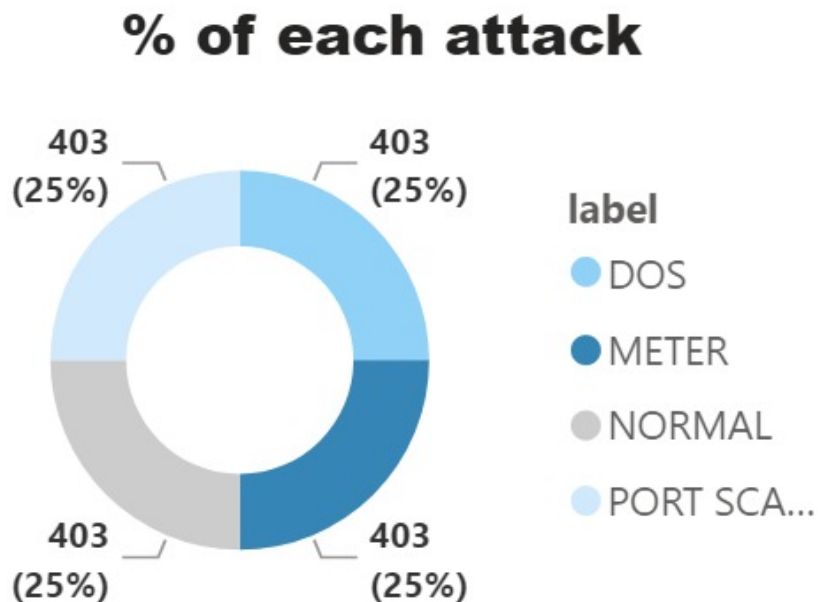


Figure 4:

Figure 5: Traffic Label Distribution

## 6.3 Protocol Usage

This chart visualizes the ratio of protocols (TCP, UDP, ICMP) used in the connections.

- **Insight:** TCP dominates the traffic, which is typical for most network communications.
- **Note:** Although UDP and ICMP are less frequent, they may still be indicative of specific attack techniques.

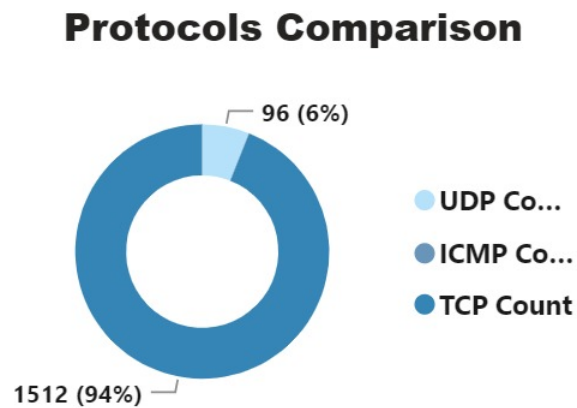


Figure 6: Protocol Usage Distribution

Figure 7: Protocol Usage Distribution



## 6.4 SYN/ACK Ratio per Traffic Type

The SYN/ACK ratio helps distinguish between connection behaviors across traffic types.

- **Insight:** Port Scanning exhibits a significantly higher SYN/ACK ratio ( $\sim 0.59$ ), consistent with scan patterns lacking proper handshakes.
- **Observation:** Meterpreter and DoS attacks display very low SYN/ACK values, highlighting incomplete or malicious connections.

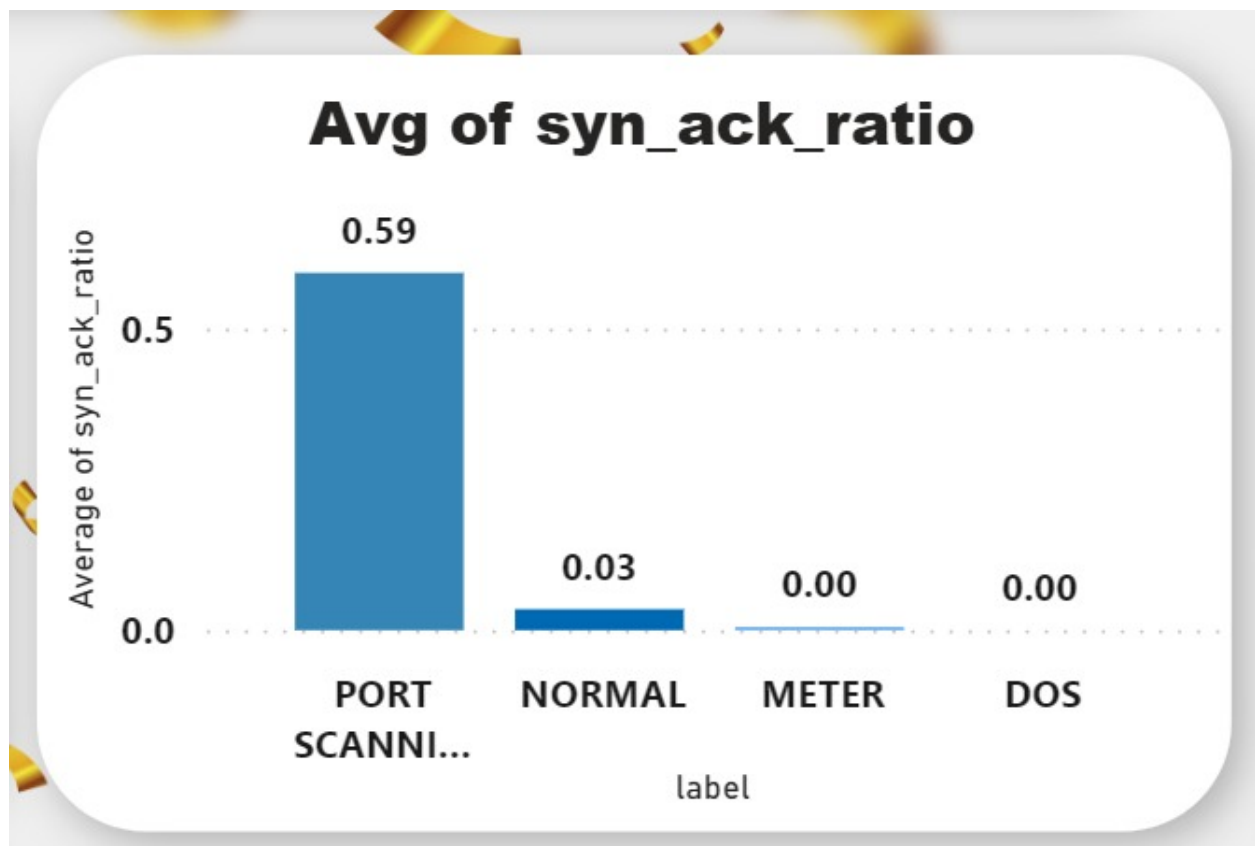


Figure 8: SYN/ACK Ratio per Traffic Type

Figure 9: SYN/ACK Ratio per Traffic Type

## 6.5 Average Connection Duration

Each traffic type's average connection duration was visualized to detect behavioral patterns.

- **Insight:** Normal sessions last notably longer, reflecting stable communications.
- **Finding:** Attack-based sessions like Meterpreter and DoS tend to be brief, typical of exploit or denial attempts.

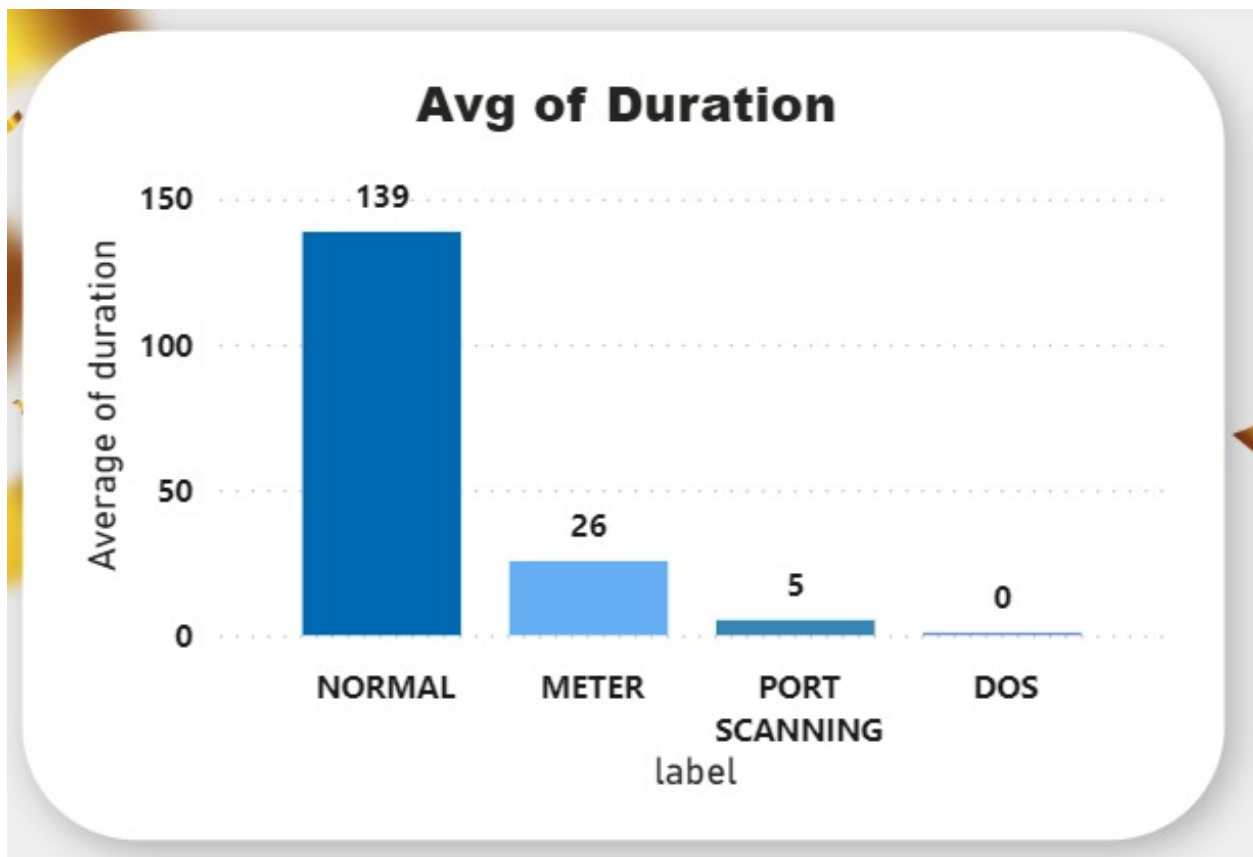


Figure 10: Average Connection Duration per Traffic Type

Figure 11: Average Connection Duration per Traffic Type

## 6.6 Log Count vs. Duration

A scatter plot was created to analyze the relationship between the number of logs and connection durations.

- **Insight:** Most connections are concentrated in the short-duration range.
- **Utility:** This view helps in spotting time-based anomalies or repeated behaviors.

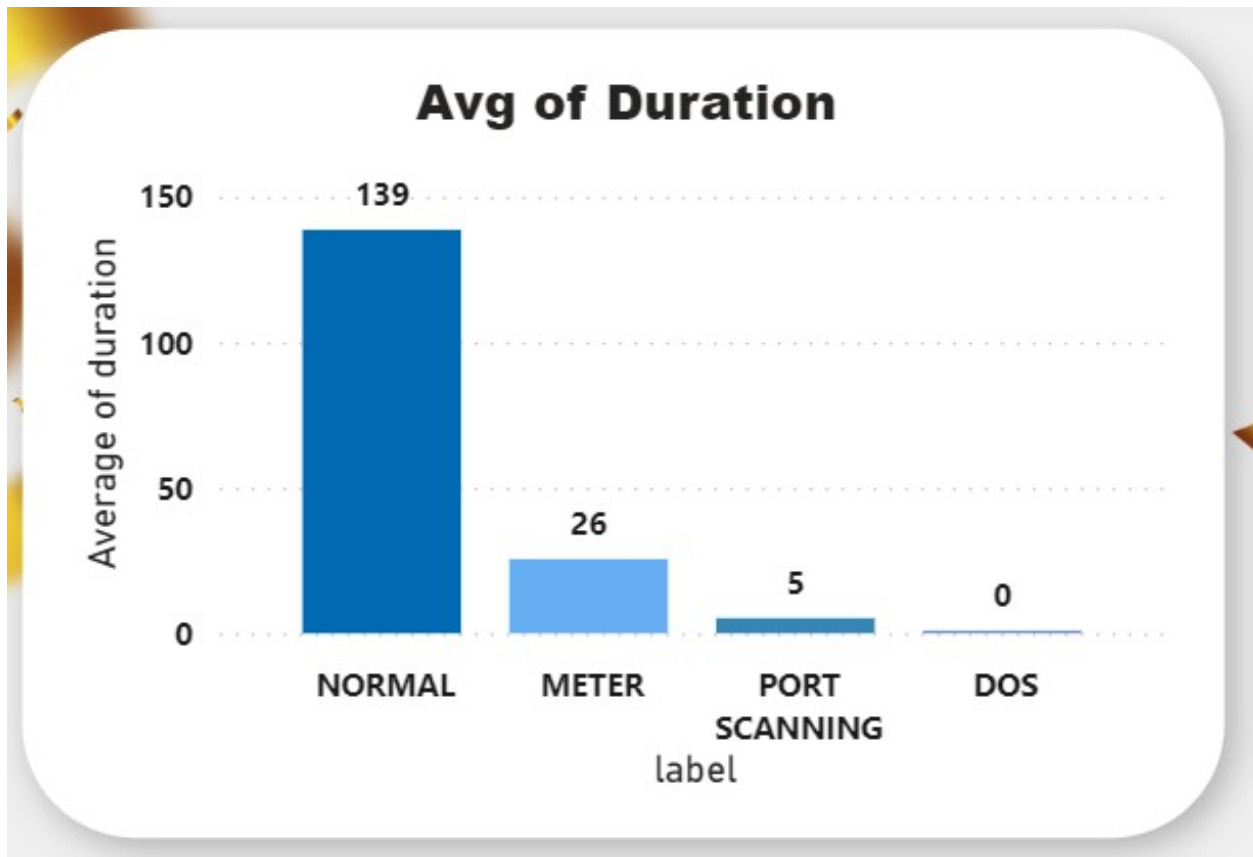


Figure 12: Log Count vs. Connection Duration

Figure 13: Log Count vs. Connection Duration

## 6.7 Key Performance Indicators (KPI Cards)

These KPI cards summarize the overall dataset characteristics and provide quick reference metrics:



Figure 14: Enter Caption

Figure 15: Key Performance Indicators Summary

Figure 16: Key Performance Indicators Summary

## 7. Introduction to SIEM and Wazuh

### 7.1 What is a SIEM?

A Security Information and Event Management (SIEM) system is a comprehensive framework that combines log analysis, threat detection, and incident response in real-time. It aggregates and normalizes data from various sources such as networks, servers, applications, and security appliances to:

- Detect cybersecurity threats quickly
- Monitor abnormal or suspicious behavior
- Generate alerts based on predefined rules or machine learning
- Meet regulatory compliance requirements

**Key Point:** SIEM is the heartbeat of Security Operations Centers (SOC), offering teams a unified view of the organization's security posture.

### 7.2 Introduction to Wazuh

Wazuh is a powerful, free, and open-source platform designed for threat detection, security monitoring, and compliance auditing. It serves as a modern SIEM solution, integrating features such as log analysis, intrusion detection, vulnerability assessment, and configuration auditing. Its modular architecture and integration with the ELK Stack

(Elasticsearch, Logstash, and Kibana) make it widely adopted in both enterprise and academic environments.

## **7.3 Core Architecture**

Wazuh operates using a modular and scalable architecture that consists of several key components:

### **1. Wazuh Agents**

Installed on monitored endpoints (servers, desktops, virtual machines, containers) to:

- Collect log data
- Monitor file integrity
- Detect rootkits and malware
- Report system activity and security events

### **2. Wazuh Manager**

Acts as the central analysis engine:

- Receives data from agents
- Applies detection rules and decoders
- Correlates events and generates alerts
- Stores logs and events

### **3. Wazuh Indexer (OpenSearch/Elasticsearch)**

- Stores and indexes alerts and logs for searching
- Supports fast querying and data analysis

### **4. Kibana Dashboard**

- Provides a web interface for data visualization and dashboarding
- Allows real-time monitoring and querying of security events

### **5. Filebeat/Logstash (Optional)**

- Used to forward logs from other systems
- Transform and enrich data before indexing

## **7.4 Key Features**

Wazuh delivers a comprehensive set of capabilities for security operations:

### **1. Log Data Analysis**

- Collects logs from Linux, Windows, firewalls, IDS/IPS, and cloud environments
- Supports JSON, syslog, custom formats, and log rotation

## **2. Intrusion Detection (HIDS)**

- Detects unauthorized behavior and anomalies
- Supports integration with Snort and Suricata for network-based detection
- Uses decoders and rules to interpret and classify logs

## **3. File Integrity Monitoring (FIM)**

- Monitors changes in critical system files or folders
- Detects unauthorized modifications, tampering, or defacement

## **4. Vulnerability Detection**

- Integrates with CVE databases (e.g., NVD)
- Scans installed packages and software versions

## **5. Rootkit and Malware Detection**

- Uses modules like rootcheck and syscheck to detect hidden threats

## **6. Compliance Auditing**

- Provides built-in rulesets for standards such as PCI-DSS, HIPAA, GDPR, NIST, and CIS Benchmarks



## 7. Security Configuration Assessment

- Evaluates system hardening and configuration baselines

## 8. Real-Time Alerting and Notification

- Alerts in real time based on rules
- Supports integration with Email, Slack, Telegram, Webhooks, and external SIEM tools like Splunk and IBM QRadar

## 7.5 Use Cases

Wazuh supports a variety of real-world scenarios, including:

- **Enterprise Threat Detection:** Real-time alerts and policy violation monitoring
- **SOC:** Centralized threat monitoring and incident response
- **Cloud Security Monitoring:** AWS, Azure, and GCP monitoring using agents and APIs
- **Log Management and Forensics:** Long-term storage and searchable logs for investigations
- **Compliance Reporting:** Automatic reports for audits and regulatory requirements

## 7.6 Integration with Other Tools

Wazuh enhances its capability through seamless integration with popular security tools:

- Snort / Suricata: For ingesting IDS alerts
- VirusTotal: For enriching alerts with threat intelligence
- MITRE ATT&CK Framework: Mapping detection rules to known attack techniques
- External SIEMs: Can forward data to Splunk, QRadar, and others

## 7.7 Advantages and Limitations

### 7.7.1 Advantages

- Free and open-source
- Highly scalable to thousands of agents
- Cross-platform (Linux, Windows, macOS, Docker, Kubernetes)
- Strong documentation and active community
- Customizable rule engine
- Centralized dashboard and management
- Supports automated response to threats

### 7.7.2 Limitations

- Complex setup, especially in hybrid or large environments

- Requires tuning to reduce false positives
- High resource consumption for indexing
- Requires Elasticsearch/Kibana expertise for advanced customization

### 7.7.3 Conclusion

Wazuh is a complete and extensible security platform that provides deep visibility into system activity, robust threat detection capabilities, and streamlined compliance auditing. Its integration with the ELK Stack, customizable rule engine, and open-source model make it ideal for modern security environments.

Whether used in academic research or enterprise-grade deployments, Wazuh offers a powerful, flexible, and cost-effective alternative to commercial SIEMs. With proper planning, tuning, and deployment, it can become the cornerstone of an organization's cybersecurity operations.

## 8. Snort – Open Source Network Intrusion Detection and Prevention System (NIDS/NIPS)

### 8.1 Introduction to Snort

Snort is one of the most widely used open-source network intrusion detection and prevention systems (NIDS/NIPS). Developed by Sourcefire (acquired by Cisco), Snort is capable of real-time traffic analysis and packet logging on IP networks. It performs deep packet inspection (DPI), protocol analysis, and content matching to identify malicious activity such as port scans, buffer overflows, and denial-of-service (DoS) attacks. Due to its reliability, customizability, and strong community support, Snort is used by both enterprise-grade SOC's and academic projects.

### 8.2 Operating Modes

Snort can operate in three main modes, depending on the use case:

- **Sniffer Mode:** Captures and displays packets in real-time.

```
snort -v
```

- **Packet Logger Mode:** Records packets to a file for later analysis.

```
snort -dev -l /var/log/snort
```

- **Network Intrusion Detection System (NIDS) Mode:** Analyzes network traffic using a set of rules and generates alerts.

```
snort -c /etc/snort/snort.conf -i eth0
```

## 8.3 Architecture Overview

Snort follows a modular pipeline:

- **Packet Decoder:** Captures raw network traffic from the data link layer.
- **Preprocessors:** Normalize and prepare packets (e.g., for TCP stream reassembly).
- **Detection Engine:** Core component that matches traffic against defined rules.
- **Logging & Alerting System:** Logs matched events and generates alerts.
- **Output Modules:** Send alerts to files, syslog, or external systems (e.g., Wazuh).

## 8.4 Snort Rule Structure

Snort uses a highly customizable rule-based language to detect threats.

A typical rule format looks like:

```
alert tcp any any -> 192.168.1.0/24 80 (msg:"Potential HTTP attack";
```

## Rule Components:

- **Action:** alert, log, pass, drop, reject, sdrop
- **Protocol:** tcp, udp, icmp, etc.
- **Source/Destination IP and Port**
- **Options:** Include msg, content, sid, rev, classtype, etc.

Snort supports complex rule logic using *content matching*, *PCRE (regex)*, *flow control*, and *packet header matching*.

## 8.5 Preprocessors

Preprocessors are essential for parsing and normalizing traffic. Examples include:

- **frag3:** Handles fragmented packets.
- **stream5:** Manages TCP stateful inspection.
- **http\_inspect:** Parses HTTP traffic for evasion techniques.
- **ssl, smtp, dns, ftp\_telnet:** Protocol-specific analysis.

## 8.6 Use Cases

- Real-time network threat detection
- Detection of port scans, DoS, brute force, and exploits
- Compliance and audit logging
- Security lab simulations and teaching
- Integration with SIEMs and SOC platforms (e.g., Wazuh)

## 8.7 Integration with Wazuh

Snort can be integrated with Wazuh to forward its alert logs to the Wazuh Manager for centralized analysis. Snort logs in **Unified2** or **Syslog** format, which can be parsed using a custom Wazuh rule and visualized in Kibana dashboards. This enhances visibility and alert correlation across the system.

## 8.8 Strengths of Snort

- Open-source and free to use
- Lightweight and efficient
- Highly customizable ruleset
- Large and active community
- Regularly updated with new signatures
- Support for IDS and IPS modes

## 8.9 Limitations

- Rule management can become complex in large-scale deployments
- Cannot decrypt encrypted traffic (like HTTPS)
- False positives may occur without tuning
- No built-in GUI (requires third-party tools for visualization)

## 8.10 Alternatives to Snort

While Snort is a market leader, other tools are also widely used:

- **Suricata** – Multi-threaded IDS/IPS with built-in Lua scripting.
- **Zeek (formerly Bro)** – Behavioral analysis over signature-based detection.
- **OSSEC** – Host-based IDS, often used alongside Snort for layered protection.

## 8.11 Conclusion

Snort remains a foundational component of network security monitoring. Its flexibility, deep packet inspection capabilities, and rule-based architecture make it suitable for both research and production environments. When paired with platforms like Wazuh, it becomes a powerful part of an end-to-end security operations system capable of real-time threat detection and response.



## 9. Recommendations and Future Work for Enhancing Network Log Analysis and Threat Detection

### 9.1 Introduction

As cyber threats continue to evolve in complexity and frequency, proactive and intelligent systems for log analysis and intrusion detection are no longer optional — they are essential. This chapter outlines strategic recommendations and forward-looking improvements to strengthen the current framework, ensuring it remains scalable, adaptive, and effective in real-world environments.

### 9.2 Recommendations

Based on the implementation and evaluation of the current system, several key recommendations can be made to improve its performance, reliability, and usability:

#### 1. Continuous Model Re-Training

Machine learning models, particularly those used for intrusion classification, must be retrained periodically using updated datasets. This helps:

- Reduce model drift caused by new attack patterns.
- Adapt to changes in legitimate network behavior over time.

- Improve classification accuracy on real-time data.

## **2. Feature Engineering Enhancements**

Introducing more refined and contextualized features from logs can improve detection accuracy. Considerations include:

- Temporal patterns (e.g., frequency of connections per second).
- Behavior-based metrics (e.g., failed login attempts).
- Enrichment with external threat intelligence feeds.

## **3. Integration with Threat Intelligence Platforms**

Wazuh and Snort can be further extended to interact with global threat intelligence sources such as:

- AbuseIPDB, AlienVault OTX, or VirusTotal.
- This enables proactive blacklisting and automated threat scoring.

## **4. Advanced Alert Correlation**

Correlating alerts across multiple sources (Snort, Wazuh, system logs) helps reduce noise and false positives. This can be achieved by:

- Rule-based alert aggregation logic.
- Context-aware prioritization of incidents.

## **5. Improved User Interface and Reporting**

The current web-based interface can be enhanced with:

- Interactive dashboards showing live detection graphs.
- Role-based access control for SOC teams.
- Auto-generated reports summarizing weekly/monthly threats.

## **9.3 Future Work**

To ensure long-term success and real-world applicability, the following future directions are proposed:

### **1. Transition from IDS to IPS**

The system currently operates in a passive monitoring mode. A future version can include an Intrusion Prevention System (IPS) mode to automatically:

- Drop malicious packets.
- Isolate suspicious hosts temporarily.

### **2. Cloud-Native and Containerized Support**

Modern infrastructures often rely on containers and cloud services.

The system can be extended to:

- Monitor containerized workloads (e.g., Docker, Kubernetes).

- Utilize cloud-native agents for AWS, Azure, and GCP.

### **3. Deployment of Deep Learning Models**

While SVM provides solid baseline performance, deep learning models such as LSTM, CNN, or Transformer-based architectures could:

- Capture complex temporal patterns in network behavior.
- Detect zero-day attacks and evasive threats more effectively.

### **4. Auto-Healing Capabilities**

Integrating automation for remediation can accelerate response. For example:

- Blocking a suspicious IP automatically via firewall.
- Restarting compromised services or applications.

### **5. Public Dataset Contribution**

Contributing anonymized log datasets and labeled traffic to the community can:

- Enhance reproducibility and benchmarking.
- Foster collaboration and innovation.

## 9.4 Conclusion

The system presented in this project lays a strong foundation for real-time network log analysis and intelligent threat classification. It successfully integrates open-source tools, machine learning models, and a user-friendly web interface to monitor and evaluate network activities with efficiency and clarity. By leveraging technologies such as Wazuh, Snort, and SVM-based classification, the platform demonstrates a practical approach to detecting anomalies and potential cyber threats in real-time.

However, cyber defense is not a static objective—it is a continuous journey. As attackers evolve their techniques, defensive systems must also advance to stay ahead. While the current system meets its initial objectives, there are several areas where it can be strengthened. These include incorporating deep learning techniques for more accurate classification, expanding the dataset with more diverse traffic patterns, integrating multi-source log correlation, and enabling automated responses to detected threats.

Moreover, the system has potential applications beyond basic monitoring. With further enhancements, it can evolve into a fully autonomous security solution capable of real-time decision-making, adaptive learning, and self-healing capabilities. This would not only benefit enterprise-level environments that require scalability and resilience but also contribute to academic research by providing a flexible and extensible

testbed for exploring advanced cybersecurity techniques.

In conclusion, this project represents a significant step toward building smarter and more responsive network security systems. Its modular architecture and extensibility ensure that it can serve as both a practical defense mechanism and a valuable educational platform for future innovation in cybersecurity.

## 10. Appendix

### 10.1 Project Source Code

The full source code of this project is available on GitHub at the following link:

<https://github.com/zezo0101/ML<sub>N</sub>IDS<sub>W</sub>AZUH/>