Intrusion Detection System (IDS) Project Report

# 1. Introduction

The objective of this project was to design and implement a small-scale Intrusion Detection System (IDS) using Suricata integrated with the ELK Stack (Elasticsearch, Logstash, Kibana).  
The goal was to capture and analyze malicious traffic between an attacker machine and a vulnerable target machine, visualize it in Kibana dashboards, and demonstrate how IDS rules detect different attack patterns.

# 2. Lab Setup

Virtual Machines Used  
1. Attacker VM – Kali Linux  
 - Purpose: Launches attacks such as SSH brute force, Nmap scanning, and Metasploit exploits.  
2. Victim VM – Metasploitable2  
 - Purpose: Intentionally vulnerable system to simulate real-world exploitation.  
3. IDS VM – Kali Linux (configured with Suricata, Filebeat, and ELK stack)  
 - Purpose: Monitors all traffic, generates alerts, and forwards logs to Elasticsearch for visualization in Kibana.  
  
Network Configuration  
- All three VMs were configured in the same VirtualBox internal network.  
- The IDS VM was positioned inline, ensuring that all attacker ↔ victim traffic passed through it.  
- This setup guaranteed complete visibility for Suricata, enabling it to capture packets, apply rules, and generate alerts.  
  
Key Idea: Traffic path = Attacker → IDS → Victim and Victim → IDS → Attacker

# 3. Tools and Technologies

- Suricata → Network-based IDS for traffic capture and rule-based detection.  
- Filebeat → Forwarder to send Suricata logs into Elasticsearch.  
- Elasticsearch → Stores and indexes logs for querying.  
- Kibana → Provides visualization dashboards for alerts and attack analysis.  
- Hydra / Nmap / Metasploit → Used on attacker VM to simulate malicious activity.

# 4. IDS Rules Implemented

Custom Suricata rules were written to detect different types of attacks. Some examples:  
  
SSH Brute Force Detection:  
alert tcp any any -> any 22 (msg:"Possible SSH Brute Force"; flow:to\_server; detection\_filter:track by\_src, count 5, seconds 60; sid:100001; rev:1;)  
  
Nmap Scan Detection:  
alert tcp any any -> any 80 (msg:"Nmap Scan Detected"; flags:S; sid:100002; rev:1;)  
  
Reverse Shell Activity:  
alert tcp any any -> any any (msg:"Reverse Shell Possible"; content:"/bin/sh"; sid:100003; rev:1;)

# 5. Attack Simulation

The following attacks were launched from the Attacker VM against the Victim VM:  
  
1. Nmap Reconnaissance Scan – Detected by the Suricata Nmap rule.  
2. SSH Brute Force Attack using Hydra – Detected by the SSH brute force rule.  
3. Metasploit Exploitation – Created alerts in Suricata for suspicious shell activity.  
  
Suricata successfully captured these malicious activities and logged them in the eve.json file.

# 6. Log Forwarding and Visualization

- Filebeat shipped the Suricata logs to Elasticsearch.  
- Kibana dashboards displayed alerts such as:  
 - Source and Destination IPs  
 - Top Alerts by Category  
 - Timeline of Attacks  
  
Screenshots taken:  
- Suricata alerts in Kibana dashboard.  
- Attack traffic graphs (top source/destination).  
- IDS rules being triggered.

# 7. Results and Analysis

- The IDS was able to detect reconnaissance (Nmap), brute-force (Hydra), and exploitation (Metasploit).  
- Visualization in Kibana made it easy to identify which machine was the attacker and which was the victim.  
- Placing the IDS inline ensured complete traffic capture.

# 8. Limitations

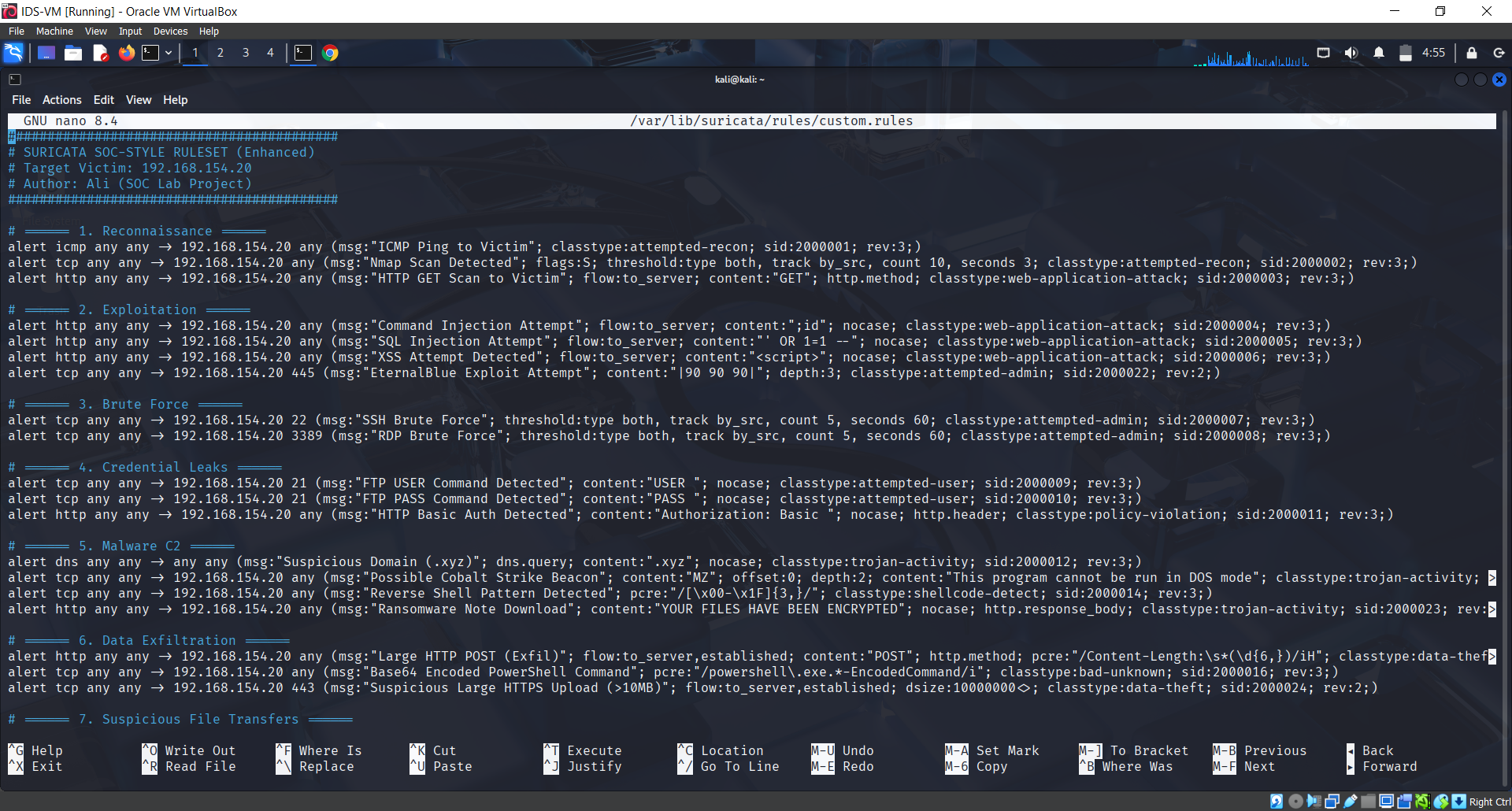
- Only a small set of rules were implemented.  
- Real-world IDS deployments require fine-tuning to reduce false positives.  
- Only one victim and one attacker were tested; larger networks would require more complex pipelines.

# 9. Conclusion

This project successfully demonstrated how an IDS can be deployed in a virtual lab to monitor and detect attacks. Using Suricata + ELK, we were able to:  
- Capture live traffic,  
- Detect multiple attack types,  
- Visualize security events in Kibana dashboards.  
  
This setup highlights the importance of intrusion detection in cybersecurity and shows how organizations can use open-source tools to strengthen their defenses.

# 10. Appendices (Screenshots)

- Suricata rule triggered for SSH brute force

  
- Suricata alert for Nmap scan

A screenshot of a computer

AI-generated content may be incorrect.  
- Kibana dashboard showing attacker and victim Ips

A screenshot of a computer

AI-generated content may be incorrect.

- Visualization of alerts timeline

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer screen

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.