Network-Based Intrusion Detection System (NIDS) Using Suricata

1. Introduction

A Network-Based Intrusion Detection System (NIDS) is a security solution that monitors network traffic to detect suspicious or malicious activities such as brute-force attacks, scanning, and unauthorized access attempts.
In this project, **Suricata**, an open-source, high-performance IDS, is used to monitor live network traffic, detect SSH brute-force attacks, generate alerts, and log intrusion events.

2. Objective

The objectives of this project are:

- To set up a network-based intrusion detection system using Suricata
- To configure custom rules for detecting malicious activities
- To monitor network traffic continuously
- To generate alerts for detected intrusions
- To implement basic response and analysis mechanisms

3. Tools and Environment

Component	Description
Operating System	Zorin OS (Linux – Ubuntu based)
IDS Tool	Suricata 7.0.3
Network Interface	wlp0s20f3
Log Files	Fast.log
Attack Type	SSH brute-force attack

4. System Architecture

The IDS system operates in **passive monitoring mode**:

1. Suricata listens to network traffic on the active network interface.
2. Incoming packets are compared against predefined and custom rules.
3. When a rule matches, an alert is generated.
4. Alerts are logged for further analysis.

5. Installation and Configuration of Suricata

5.1 Installing Suricata

Suricata was installed using the package manager on Zorin OS.

5.2 Verifying Configuration

The configuration file was validated using:

```
sudo suricata -T -c /etc/suricata/suricata.yaml
```

Result:

```
Configuration provided was successfully loaded.
```

This confirms that Suricata is correctly configured.

6. Rule Configuration and Alert Setup

6.1 Custom SSH Brute-Force Detection Rule

A custom rule was created to detect multiple SSH login attempts from the same source IP within a short period.

Rule Location:
/var/lib/suricata/rules/local.rules

Rule Used:

```
alert tcp any any -> any 22 (
 msg:"Possible SSH brute-force attack";
 flow:to_server,established;
 detection_filter:track by_src, count 5, seconds 60;
 sid:1000003;
 rev:1;
)
```

6.2 Rule Explanation

- tcp any any -> any 22 → Monitors SSH traffic (port 22)
- flow:to_server,established → Tracks established connections to server
- detection_filter → Triggers alert if 5 attempts occur in 60 seconds
- msg → Alert message displayed in logs

7. Continuous Network Monitoring

Suricata was started in live monitoring mode on the active network interface:

sudo suricata -c /etc/suricata/suricata.yaml -i wlp0s20f3

Suricata continuously inspected all network packets in real time.

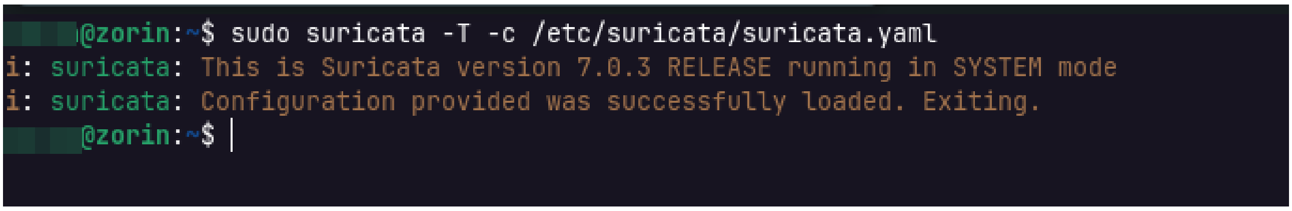
8. Detection Results and Alerts

8.1 Log Monitoring

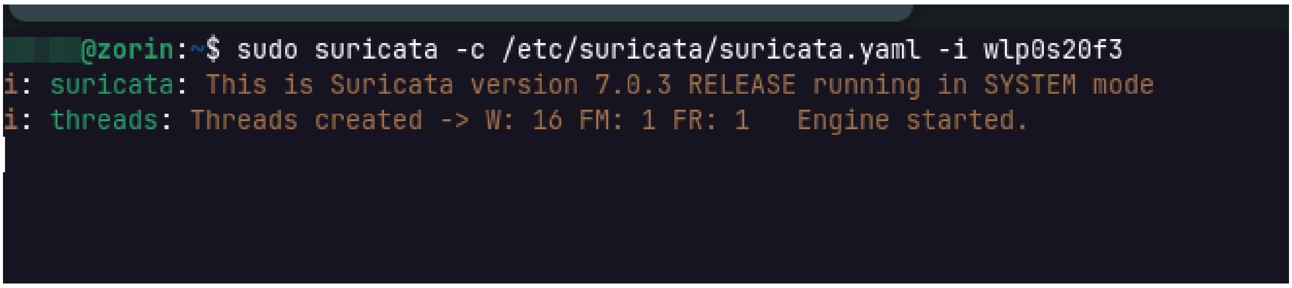
Alerts were monitored using:

tail -f /var/log/suricata/fast.log

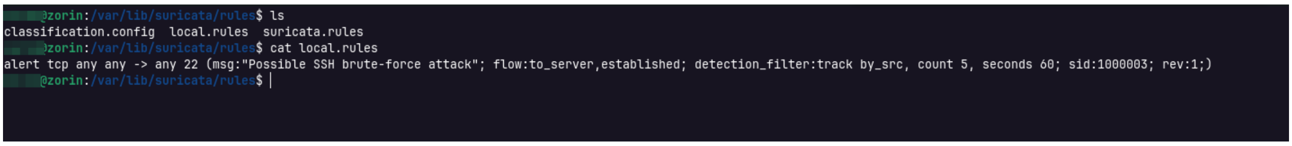
8.2 Sample Alert Output



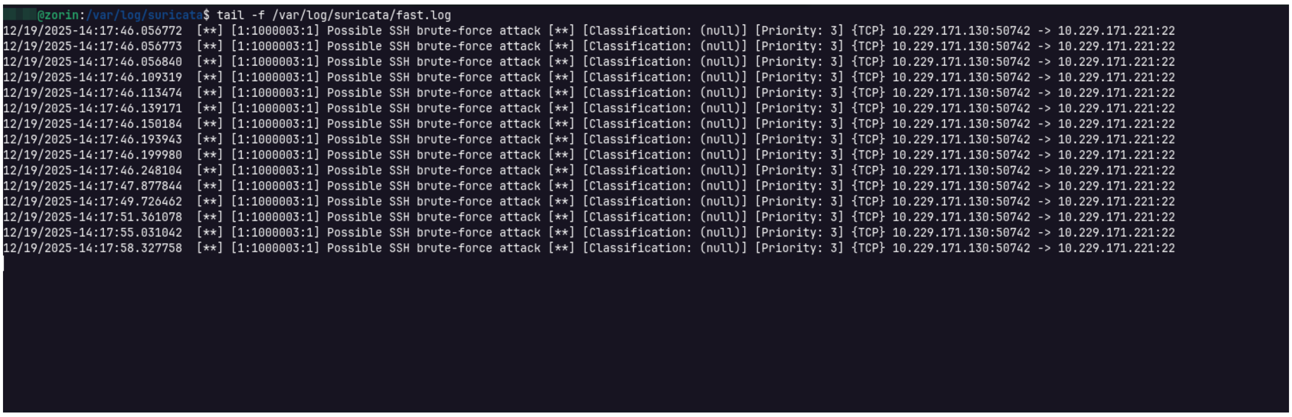
```
[redacted]@zorin:~$ sudo suricata -T -c /etc/suricata/suricata.yaml
i: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
i: suricata: Configuration provided was successfully loaded. Exiting.
[redacted]@zorin:~$ |
```



```
[redacted]@zorin:~$ sudo suricata -c /etc/suricata/suricata.yaml -i wlp0s20f3
i: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
i: threads: Threads created -> W: 16 FM: 1 FR: 1   Engine started.
```



```
[redacted]@zorin:/var/lib/suricata/rules$ ls
classification.config  local.rules  suricata.rules
[redacted]zorin:/var/lib/suricata/rules$ cat local.rules
alert tcp any any -> any 22 (msg:"Possible SSH brute-force attack"; flow:to_server,established; detection_filter:track by_src, count 5, seconds 60; sid:1000003; rev:1;)
[redacted]@zorin:/var/lib/suricata/rules$ |
```



```
[redacted]@zorin:/var/log/suricata$ tail -f /var/log/suricata/fast.log
12/19/2025-14:17:46.056772  [**] [1:1000003:1] Possible SSH brute-force attack [**] [Classification: (null)] [Priority: 3] {TCP} 10.229.171.130:50742 -> 10.229.171.221:22
12/19/2025-14:17:46.056773  [**] [1:1000003:1] Possible SSH brute-force attack [**] [Classification: (null)] [Priority: 3] {TCP} 10.229.171.130:50742 -> 10.229.171.221:22
12/19/2025-14:17:46.056840  [**] [1:1000003:1] Possible SSH brute-force attack [**] [Classification: (null)] [Priority: 3] {TCP} 10.229.171.130:50742 -> 10.229.171.221:22
12/19/2025-14:17:46.109319  [**] [1:1000003:1] Possible SSH brute-force attack [**] [Classification: (null)] [Priority: 3] {TCP} 10.229.171.130:50742 -> 10.229.171.221:22
12/19/2025-14:17:46.113474  [**] [1:1000003:1] Possible SSH brute-force attack [**] [Classification: (null)] [Priority: 3] {TCP} 10.229.171.130:50742 -> 10.229.171.221:22
12/19/2025-14:17:46.139171  [**] [1:1000003:1] Possible SSH brute-force attack [**] [Classification: (null)] [Priority: 3] {TCP} 10.229.171.130:50742 -> 10.229.171.221:22
12/19/2025-14:17:46.150184  [**] [1:1000003:1] Possible SSH brute-force attack [**] [Classification: (null)] [Priority: 3] {TCP} 10.229.171.130:50742 -> 10.229.171.221:22
12/19/2025-14:17:46.193943  [**] [1:1000003:1] Possible SSH brute-force attack [**] [Classification: (null)] [Priority: 3] {TCP} 10.229.171.130:50742 -> 10.229.171.221:22
12/19/2025-14:17:46.199980  [**] [1:1000003:1] Possible SSH brute-force attack [**] [Classification: (null)] [Priority: 3] {TCP} 10.229.171.130:50742 -> 10.229.171.221:22
12/19/2025-14:17:46.248104  [**] [1:1000003:1] Possible SSH brute-force attack [**] [Classification: (null)] [Priority: 3] {TCP} 10.229.171.130:50742 -> 10.229.171.221:22
12/19/2025-14:17:47.877844  [**] [1:1000003:1] Possible SSH brute-force attack [**] [Classification: (null)] [Priority: 3] {TCP} 10.229.171.130:50742 -> 10.229.171.221:22
12/19/2025-14:17:49.726462  [**] [1:1000003:1] Possible SSH brute-force attack [**] [Classification: (null)] [Priority: 3] {TCP} 10.229.171.130:50742 -> 10.229.171.221:22
12/19/2025-14:17:51.361078  [**] [1:1000003:1] Possible SSH brute-force attack [**] [Classification: (null)] [Priority: 3] {TCP} 10.229.171.130:50742 -> 10.229.171.221:22
12/19/2025-14:17:55.031042  [**] [1:1000003:1] Possible SSH brute-force attack [**] [Classification: (null)] [Priority: 3] {TCP} 10.229.171.130:50742 -> 10.229.171.221:22
12/19/2025-14:17:58.327758  [**] [1:1000003:1] Possible SSH brute-force attack [**] [Classification: (null)] [Priority: 3] {TCP} 10.229.171.130:50742 -> 10.229.171.221:22
```

Observation

- Multiple SSH connection attempts were detected
- Alerts were generated in real time
- Source and destination IP addresses were clearly logged

This confirms the IDS successfully detected suspicious activity.

12. Conclusion

This project successfully implemented a **Network-Based Intrusion Detection System using Suricata**. Custom rules were configured to detect SSH brute-force attacks, and real-time alerts were generated upon detecting suspicious behavior. The system effectively demonstrated how NIDS can be used to enhance network security by identifying and responding to potential threats.