LAB RECORD

Experiment No: 4

Title: Implementation of Network Intrusion Detection System (NIDS) using Suricata

Subject: Cyber Security / Network Security Lab

Aim

The aim of this experiment is to design and implement a Network-Based Intrusion Detection System (NIDS) using the Suricata tool.

The experiment focuses on configuring detection rules, monitoring real-time network traffic, detecting malicious activities,

and generating alerts for potential intrusions.

Tools and Software Required

1. Operating System: Ubuntu / Kali Linux

2. Suricata IDS/IPS

3. Network Interface Card

4. Root or sudo access

5. Basic networking knowledge

Theory

A Network Intrusion Detection System (NIDS) is a security mechanism that monitors incoming and outgoing network traffic

and analyzes it for signs of malicious activities. Unlike host-based IDS, a NIDS monitors traffic across the entire network.

Suricata is an open-source, high-performance intrusion detection and prevention system capable of real-time packet inspection,

deep protocol analysis, and signature-based detection. It supports multi-threading, making it suitable for high-speed networks.

Suricata works by capturing network packets, decoding protocols, matching traffic against predefined rules, and generating alerts

whenever suspicious behavior is detected.

Types of Attacks Detected

1. Port scanning attacks

2. Denial of Service (DoS) attacks

3. ICMP flooding

4. Unauthorized access attempts

5. Malicious payload detection

Procedure

Step 1: Installation of Suricata

The Suricata IDS is installed using the apt package manager. Proper installation ensures required dependencies are configured.

Step 2: Configuration of Network Parameters

The HOME_NET variable is configured to define the protected network range. The active network interface is specified

for packet capture.

Step 3: Rule Configuration

Custom detection rules are written to identify ICMP pings, TCP SYN scans, and HTTP traffic.

Step 4: Validation

Configuration files are validated to ensure no syntax errors exist.

Step 5: Execution

Suricata is started in IDS mode to monitor live traffic.

Commands Used

```
sudo apt update

sudo apt install suricata

sudo nano /etc/suricata/suricata.yaml

sudo nano /etc/suricata/rules/local.rules
sudo suricata -T -c /etc/suricata/suricata.yaml
```

```
sudo suricata -c /etc/suricata/suricata.yaml -i eth0
```

Sample Suricata Rules

Rule 1: ICMP Ping Detection

```
alert icmp any any -> $HOME_NET any (msg:"ICMP Ping Detected"; sid:1000001; rev:1;)
```

Rule 2: TCP Port Scan Detection

```
alert tcp any any -> $HOME_NET any (flags:S; msg:"Possible Port Scan Detected"; sid:1000002; rev:1;)
```

Rule 3: HTTP Traffic Detection

```
alert http any any -> $HOME_NET any (msg:"HTTP Traffic Detected"; sid:1000003; rev:1;)
```

Output

Upon detecting suspicious traffic, Suricata generates alerts that are stored in log files such as fast.log and eve.json.

These alerts include information about the source IP, destination IP, protocol, and type of attack.

Result

The Network Intrusion Detection System using Suricata was successfully implemented.

The system effectively detected ICMP pings, port scanning attempts, and HTTP traffic.

Alerts were generated and logged, confirming proper functioning of the IDS.

Precautions

1. Ensure correct network interface selection.

2. Maintain unique rule IDs.

3. Run Suricata with root privileges.

4. Regularly update rule sets.

5. Monitor logs frequently.

Applications

1. Enterprise network security monitoring

2. Data center protection

3. Security Operations Center (SOC)

4. Threat detection and analysis

Advantages

1. Open-source and cost-effective

2. High performance and scalability

3. Real-time intrusion detection

4. Supports multiple protocols

Limitations

1. Requires manual rule tuning

2. False positives may occur

3. Needs skilled administration

Conclusion

This experiment demonstrates the successful implementation of a Network Intrusion Detection System using Suricata.

The IDS provides real-time monitoring and alerting, enhancing overall network security.

Viva Voce Questions

1. What is an Intrusion Detection System?

2. Difference between IDS and IPS?

3. What is HOME_NET in Suricata?

4. What are Suricata rules?

5. What types of attacks can NIDS detect?