Real-Time Threat Hunting and Incident Response Toolkit

Project Report by Jagadeesh Kumar S

1. Project Overview

This project is a Real-Time Threat Hunting and Incident Response Toolkit built using Suricata, a powerful open-source intrusion detection system (IDS) and intrusion prevention system (IPS). The system monitors real-time network traffic and sends alert notifications for high or medium severity threats detected from log files.

2. Installation and Setup

Follow these steps to set up the toolkit on a Kali Linux system:

1. Install Suricata:

   sudo apt update

   sudo apt install suricata -y

2. Verify installation:

   suricata --build-info

3. Start Suricata in live mode:

   sudo suricata -i eth0 -l /var/log/suricata/

4. Check if Suricata is generating logs:

   ls /var/log/suricata/

5. Capture a PCAP file for testing (optional):

   sudo tcpdump -i eth0 -w test.pcap -c 10

   sudo suricata -r test.pcap -l /tmp/suricata-log

6. Create a script to analyze alerts from eve.json and send emails.

Real-Time Threat Hunting and Incident Response Toolkit

3. Python Script Functionality

The script `/opt/threat-monitor/email-alert.py` reads Suricata's eve.json file and checks for high or medium severity alerts in the last hour. If such alerts are found, it sends an email notification using the `mail` utility.

Key Steps:

- Reads JSON logs.
- Filters alerts within the past hour.
- Sends formatted alerts via email.

4. User Manual

1. Ensure Suricata is running and logging to /var/log/suricata/eve.json.
2. Create the directory: sudo mkdir -p /opt/threat-monitor/
3. Save the Python script as email-alert.py in that directory.
4. Make the script executable: chmod +x /opt/threat-monitor/email-alert.py
5. Run the script: sudo /opt/threat-monitor/email-alert.py
6. Check your email for alerts if any threats were detected.

Ensure 'mailutils' is installed and configured correctly for sending emails.

5. Future Enhancements

- Add a web dashboard to view alerts visually.
- Include support for multiple alert types (DoS, brute force, etc.).
- Log all sent alerts in a separate file.
- Auto restart Suricata if it stops unexpectedly.