Enterprise-Level Security Monitoring Project Report

By,

Name: Eldho Babu
Email: eldhobabu2016@gmail.com
Submitted To: Infotact Solutions Pvt. Ltd, Bangalore

1. Introduction

This project aims to design and implement an enterprise-level security monitoring system using open-source tools and virtual environments. It integrates log forwarding, intrusion detection, honeypots, and firewall management into a centralized SIEM (Splunk) to detect and analyze potential security threats.

---

2. Tools and Technologies Used

- **Ubuntu (VirtualBox VM)**: Linux environment for logging, honeypot, IDS, and traffic monitoring.
- **Splunk Enterprise (Windows Host)**: Central SIEM server.
- **Splunk Universal Forwarder**: To forward logs from Ubuntu to Splunk.
- **Syslog and Auth Logs**: Linux system logs for authentication and syslog events.
- **Cowrie Honeypot**: To detect SSH brute-force attempts.
- **Snort IDS**: To detect network-based threats (e.g., TCP SYN scan).
- **tcpdump**: To capture browser traffic.
- **pfSense Firewall**: To block malicious domains

---

3. Setup and Configuration Steps

3.1 Ubuntu VM Installation

- Installed Ubuntu 22.04 LTS on VirtualBox.

3.2 Install Splunk Universal Forwarder

```
wget -O splunkforwarder.deb
'https://download.splunk.com/products/universalforwarder/releases/9.0.0/linux/splunkforwarder-9.0.0-deb.deb'
sudo dpkg -i splunkforwarder.deb
sudo /opt/splunkforwarder/bin/splunk start --accept-license
sudo /opt/splunkforwarder/bin/splunk enable boot-start
```

3.3 Configure Log Forwarding (Syslog & Auth.log)

```
sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/syslog
sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/auth.log
sudo /opt/splunkforwarder/bin/splunk add forward-server <SPLUNK_SERVER_IP>:9997 -auth admin:changeme
```

3.4 Install and Configure Cowrie Honeypot

```
sudo apt update && sudo apt install python3-virtualenv git -y
git clone https://github.com/cowrie/cowrie.git
cd cowrie
virtualenv cowrie-env
source cowrie-env/bin/activate
pip install --upgrade pip
pip install -r requirements.txt
cp etc/cowrie.cfg.dist etc/cowrie.cfg
vi etc/cowrie.cfg  # Change port to 2222
```

- Start Cowrie:

```
bin/cowrie start
```

- Add Cowrie logs to Splunk Forwarder:

```
sudo /opt/splunkforwarder/bin/splunk add monitor /home/cowrie/cowrie/var/log/cowrie.log
```

3.5 Install Snort IDS

```
sudo apt install snort -y
```

- Edit /etc/snort/rules/local.rules:

```
alert tcp any any -> any any (msg:"TCP SYN Scan"; flags:S; threshold:type threshold, track by_src, count 20,
seconds 3; sid:1000001; rev:1;)
```

- Add Snort logs to Splunk Forwarder:

```
sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/snort/
```

3.6 Install and Use tcpdump

```
sudo apt install tcpdump -y
sudo tcpdump -i eth0 -w /var/log/browser_traffic.pcap
```

- Add pcap log file to Splunk Forwarder:

```
sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/browser_traffic.pcap
```

3.7 pfSense Firewall Configuration

- pfSense installed on VirtualBox with dual NICs (LAN and WAN).
- Connected Ubuntu to pfSense LAN interface.
- Configured DNS Resolver:
    - Blocked domains (e.g., maliciousdomain.com)

---

4. Attack Simulation and Detection

- SSH brute-force attack launched on Cowrie port 2222.
- Snort detected TCP SYN scanning using custom rule.
- DNS query to malicious domain blocked by pfSense.
- tcpdump captured web traffic for inspection.
- All logs successfully forwarded to Splunk for analysis.

---

5. SIEM Configuration (Splunk)

- **Log Sources Indexed**:
    - Syslog and Auth.log (from Ubuntu)
    - Cowrie logs
    - Snort alerts
    - tcpdump pcap file
- **Dashboards and Alerts Created**:
    - SSH brute-force attempts
    - TCP SYN scan detections
    - Access to blocked domains
    - Traffic analysis

---

6. Conclusion

This project demonstrates how to build a layered security monitoring setup using open-source tools. It simulates real-world attacks and integrates logs into a SIEM for detection, analysis, and alerting. It provides hands-on experience in log forwarding, honeypot deployment, IDS rule writing, firewall configuration, and SIEM management.

---

7. Future Enhancements

- Integrate threat intelligence feeds into Splunk
- Use Splunk Enterprise Security or Wazuh for correlation
- Automate response via pfSense blocking scripts or SOAR
- Expand honeypot variety (e.g., web honeypots like Glastopf)

Submitted by:
Eldho Babu
eldhobabu2016@gmail.com