BY LOVE SERVE ONE ANOTHER

Estd. 1864

FORMAN CHRISTIAN COLLEGE

(A CHARTERED UNIVERSITY)

DEPARTMENT OF COMPUTER SCIENCE

FORMAN CHRISTIAN COLLEGE

(A Chartered University)

Fall 2024

LAHORE, PAKISTAN

Cyber Sentinel

Onboarding Manual

1. Introduction

Cyber Sentinel is a security monitoring system designed for intrusion detection IN Local Area Networks (LANs) by leveraging open-source tools, including Wazuh, the ELK Stack (Elasticsearch, Logstash, Kibana), Suricata, and a partially integrated honeypot (Cowrie) for trapping attackers. The system runs on Kali Linux which can be deployed on various hardware platforms, including a Raspberry Pi 5, virtual machines, or any device supporting Kali Linux. It detects traditional cyberattacks such as aggressive scans, Distributed Denial of Service (DDoS) attacks, brute-force attacks, SQL injections, and Shellshock attacks. Alerts are sent via email, and a GUI allows local monitoring, while Kibana provides interactive dashboards for visualizing security data.

2. System Overview

Cyber Sentinel integrates multiple open-source components to create this security monitoring pipeline, each with a specific role:

- **Wazuh Manager**: The central server that collects logs from Wazuh agents installed on monitored devices (e.g., Windows, Linux). It applies security rules to detect suspicious activities and generates alerts, stored in /var/ossec/logs/alerts/alerts.json.
- **Wazuh Agents**: Lightweight programs installed on each monitored endpoint (Windows or Linux) that send system logs to the Wazuh Manager for analysis.
- **ELK Stack**:
  - **Elasticsearch**: Stores and indexes logs and alerts, enabling fast search and retrieval of security events.
  - **Logstash**: Processes Wazuh alerts, formats critical ones into HTML emails, and sends them to configured recipients via an SMTP server (e.g., Gmail).
  - **Kibana**: A web-based dashboard that visualizes security data through charts, timelines, and lists, allowing users to explore alerts and trends interactively.
- **Filebeat**: A lightweight shipper that forwards Wazuh alerts to Elasticsearch for indexing, ensuring efficient log transfer.
- **Suricata**: A high-performance Network Intrusion Detection System (NIDS) that monitors network traffic for attack signatures (e.g., port scans, SQL injections, DNS attacks) and sends logs to Wazuh for analysis, complementing host-based monitoring.
- **Cowrie (Honeypot)**: A partially integrated SSH/Telnet honeypot that simulates services to trap attackers, logging their activities (e.g., IP addresses, commands, timestamps). Full integration with Wazuh is planned for future releases.
- **GUI Manager**: A Python-based interface (WazuhManagerGUI.py) for administrators to manage agents, monitor services, and view real-time alerts locally.

3. System Requirements

To deploy Cyber Sentinel, ensure the following hardware and software requirements are met:

3.1 Hardware

Component	Description
Device	Any device supporting Kali Linux, such as Raspberry Pi 5 (recommended for physical deployment), virtual machine, or dedicated PC/laptop.
Storage	Minimum 32GB MicroSD card (for Raspberry Pi) or sufficient storage for other devices. Optional external USB drive for additional log storage.
Power Supply	5V, 3A power supply for Raspberry Pi to ensure stability. Otherwise use suitable PSU for selected device.
Peripherals	HDMI cable, monitor, keyboard, and mouse for initial setup.
Cooling	Optional heatsink or fan to prevent overheating during intensive tasks.
Processor	64-bit CPU (ARM or x86_64).
RAM	Minimum 4 GB (8 GB Recommended)

3.2 Software

Component	Version/Description
Operating System	Kali Linux (latest version compatible with the chosen device)
Wazuh Manager	Version 4.5.4 (Critical for compatibility)
ELK Stack	Version 7.17.13 (Elasticsearch, Logstash, and Kibana)
Suricata	Network Intrusion Detection System for network-based alerts.
Filebeat	For forwarding logs to Elasticsearch.
Logstash	For log filtering and email alert formatting.
Mail Server	Postfix or similar (e.g., Gmail SMTP) for sending email alerts.
Additional Tools	Python 3, Git (for installer), and a stable internet connection during setup.

4. Setup Instructions [NOT RECCOMENDED]

Note: Preferably don’t build from scratch and copy given Kali Image unless want to do learning of process. Installer installs core services but is outdated.

Follow these steps to deploy Cyber Sentinel on your chosen device:

4.1 Prepare the Hardware

- **For Raspberry Pi 5**:
  - Assemble the hardware: insert a 32GB+ MicroSD card, connect a 5V 3A power supply, HDMI cable, monitor, keyboard, and mouse.
  - Optional: Add a heatsink or fan to prevent overheating.
  - Prefer a wired Ethernet connection (use a static IP for reliability) to avoid Wi-Fi interruptions.
- **For Virtual Machine or Dedicated PC**:
  - Ensure the device meets requirements (8 GB RAM, 64-bit processor, 32GB storage)

4.2 Install Kali Linux

- Download the appropriate Kali Linux image for your hardware (ARM for Raspberry Pi, ISO for PCs/VMs) from Kali Linux Downloads.
- Flash the image to the boot medium (MicroSD card, USB, or VM disk) using a tool like Balena Etcher.
- Boot the device and follow on-screen prompts to complete the Kali Linux installation, setting up the root user, password, and locale.

4.3 Connect to the Internet

- Connect the device to the internet via Ethernet or Wi-Fi.
- Verify network connectivity to ensure access to package repositories.

4.4 Update the System

- Open a terminal and run:

```
sudo apt update && sudo apt upgrade -y
```

- This ensures all Kali Linux packages are up to date.

4.5 Install Cyber Sentinel

- Open a web browser on the Kali Linux device and visit the Cyber Sentinel Website.

- Download the executable installer (CyberSentinel_Installer) and run it, following on-screen instructions to install Wazuh (v4.5.4), ELK Stack (v7.17.13), Suricata, Filebeat, Logstash, and configuration files from the Cyber Sentinel GitHub.

Note: Installer is not updated, double check all installations or do manually if a step fails

Alternatively, clone the repository and run the GUI installer:

```
git clone https://github.com/Abdullah-Mehtab/Cyber-Sentinal

cd Cyber-Sentinal

sudo python3 installer_gui.py
```

The installer automates version compatibility and configuration file placement.

4.6 Configure Wazuh Agents

- Install Wazuh agents on devices to be monitored (e.g., Windows, Linux).
- Register each agent with the Wazuh Manager:
  - Generate an agent key on the Wazuh Manager using the manage_agents tool.
  - Configure the agent to communicate with the Wazuh Manager (Kali).
- Verify agent connectivity through the Wazuh Manager GUI's **Agent Management** tab.

4.7 Set Up Email Alerts

- Configure Logstash to filter logs and send email alerts for critical events:
  - Edit the Logstash configuration file (/etc/logstash/conf.d/wazuh.conf) to specify the email recipient (e.g., security@company.com) and SMTP settings (e.g., Gmail credentials).
- Test email functionality by generating a sample alert.

4.8 Access Kibana

- Open a web browser and navigate to http://localhost:5601 to access the Kibana dashboard.
- Log in with default credentials (username: elastic, password: CyberSenti) and change the password immediately for security.
- Create or verify index patterns (e.g., wazuh-template.json) to display Wazuh alerts and logs.

4.9 Verify Services

- Reboot the system (sudo reboot) to ensure all services start correctly.

- Launch the Wazuh Manager GUI:

```
python3 WazuhManagerGUI.py
```

- Log in using password: admin
- Check the **Services** tab to confirm that Wazuh Manager, Elasticsearch, Logstash, Kibana, Filebeat, and Suricata are running.
- From another machine on the same network, access http://<manager_ip>:5601 to verify the Kibana dashboard displays real-time data (agents, alerts, charts).

4.10 Notes on Setup

- **Version Compatibility**: Use Wazuh 4.5.4 and ELK Stack 7.17.13 to avoid plugin compatibility issues.
- **Resource Management**: On Raspberry Pi, reduce Elasticsearch heap size to 1GB (edit jvm.options in Elasticsearch configuration) to prevent system freezes.
- **Network Configuration**: Ensure ports 1514/UDP (Wazuh agents), 1515/TCP (Wazuh), 9200/TCP (Elasticsearch), 5601/TCP (Kibana), and 25/587/TCP (SMTP) are open on any firewall.

5. Core Workflow

1. **Data Collection**:
   - Wazuh agents → Send logs to Wazuh Manager.
   - Suricata → Monitors network traffic → Alerts to Wazuh.
2. **Processing**:
   - Wazuh applies rules → Generates alerts in /var/ossec/logs/alerts/alerts.json.
   - Filebeat → Ships alerts to Elasticsearch.
3. **Output**:
   - **Kibana**: Visualizes data at http://<MANAGER_IP>:5601.
   - **Email**: Logstash formats critical alerts → Sends via SMTP.
   - **GUI**: Real-time monitoring via WazuhManagerGUI.py.

5. Basic Testing

To verify that Cyber Sentinel is operational, perform the following tests to confirm detection and alerting capabilities:

5.1 Start the System

- Log in as root on the Kali Linux device.
- Launch the Wazuh Manager GUI (password: admin):

```
python3 WazuhManagerGUI.py
```

- Verify that all services (Wazuh Manager, Elasticsearch, Logstash, Kibana, Filebeat, Suricata) are running in the **Services** tab.

5.2 Verify Alerts

- **Kibana Dashboard**:
    - Open a browser and navigate to http://localhost:5601.
    - Log in and check the Wazuh or Alerts dashboard to view security events.
- **GUI Alerts**:
    - In the Wazuh Manager GUI, open the **Alerts** tab to see real-time alerts from monitored agents.
- **Email Alerts**:
    - Verify the Logstash configuration (/etc/logstash/conf.d/wazuh.conf) to confirm the email recipient.
    - Check the configured email account for alert notifications.

5.3 Perform Test Attacks

Use a separate Kali Linux machine (attacker) with tools like Nmap or Hydra to simulate attacks on a monitored agent (e.g., a Windows or Linux machine with a Wazuh agent).

- **Port Scan**:
    - Run a stealth port scan:

```
sudo nmap -sS -p 1-1000 <agent_ip>
```

    - Expected alert: “Successful Remote Logon Detected” or “Portscan detected” (Level 6) in the Wazuh Manager GUI, Kibana dashboard, and email.
- **Brute-Force SSH Attack**:
    - Ensure the rockyou.txt password list is available:

```
ls /usr/share/wordlists/rockyou.txt
gzip -d /usr/share/wordlists/rockyou.txt.gz
```

  - Run a brute-force attack using Hydra:

```
hydra -l Administrator -P /usr/share/wordlists/rockyou.txt
ssh://<agent_ip> -t 8 -f
```

  - Expected alert: “Logon failure - Unknown user or bad password” (Level 5) in the GUI, Kibana, and email.

- **Web Attack (SQL Injection)**:
  - If the agent hosts a web service, simulate a SQL injection:

```
curl -XGET "http://<agent_ip>/users/?id=SELECT+*+FROM+users"
```

  - Expected alert: “SQL Injection” in Kibana and email, detailing the payload.

- **DDoS (SYN Flood)**:
  - Simulate a SYN flood attack:

```
sudo hping3 -S --flood <agent_ip>
```

  - Expected alert: “Agent event queue flooded” (Level 12) in the GUI, Kibana, and email.

5.4 Verify Outputs

- Confirm that alerts appear in:
  - The Wazuh Manager GUI’s **Alerts** tab with details (e.g., IP, timestamp).
  - The Kibana dashboard under the **Security Events** or **Alerts Overview** section, with visualizations like charts and timelines.
  - Email notifications with HTML-formatted details (e.g., rule, agent, timestamp).
- Use Kibana’s **Discover** tab to filter alerts by agent, time, or rule level.

5.5 Optional: Test Honeypot

- The Cowrie honeypot is partially integrated, logging attacker activities (e.g., IP, commands, timestamps). An alert is generated but doesn’t specify attacker details.
- Check Wazuh Manager logs for honeypot activity.
- For honeypot’s trap and attacker details use

```
tail -f /home/kali/cowrie/var/log/cowrie/cowrie.json | jq .
```

6. User Manual

6.1 For Administrators

- **Starting the GUI**:
  - Launch the Wazuh Manager GUI on the Kali Linux desktop (password: admin):

  ```
  python3 WazuhManagerGUI.py
  ```

  - Log in with admin credentials to access tabs for **Agents**, **Services**, and **Alerts**.
- **Managing Agents**:
  - In the **Agents** tab, add a new agent by entering the device name or IP and generating a key using the manage_agents tool.
  - Remove an agent by selecting it and clicking **Remove Agent**.
  - Ensure agents are installed on monitored endpoints and have exchanged keys with the Wazuh Manager.
- **Checking Services**:
  - In the **Services** tab, verify that Wazuh Manager, Elasticsearch, Logstash, Filebeat, Kibana, and Suricata are listed as "Running."
  - Use the **Start** button to launch any stopped service.
  - The system's health-check monitors Wazuh and ELK connectivity.

6.2 For End-Users

- **Email Alerts**:
  - Critical events trigger HTML email alerts containing details like event type (e.g., "Brute-force login detected"), timestamp, and affected agent.
  - Ensure valid email settings are configured in Logstash (/etc/logstash/conf.d/wazuh.conf) and check the spam folder if emails are missing.
- **Using the Kibana Dashboard**:
  - Access the dashboard from any device on the network at http://<manager_ip>:5601.
  - Log in to view the Cyber Sentinel dashboards (e.g., **Alerts Overview**), which display lists of recent alerts, event count charts, and search filters.
  - Use the **Discover** tab to query alerts by time, rule, or agent for detailed analysis.

7. Troubleshooting

Common issues and their solutions include:

Issue	Solution
No Email Alerts	- Verify SMTP settings in /etc/logstash/conf.d/wazuh.conf (e.g., Gmail credentials, port 25/587). - Ensure "less secure apps" is enabled in Gmail settings. - Check Wazuh rules in /var/ossec/logs/alerts/alerts.json to confirm events are logged. - Review Logstash logs (/var/log/logstash) for SMTP errors.
Kibana Dashboard Unavailable	- Ensure the Manager is powered on and connected to the network. - Check Kibana's status in the **Services** tab or via sudo systemctl status kibana. - Verify Elasticsearch health: curl http://localhost:9200. - Ensure port 5601 is not blocked by a firewall. - Reset the Kibana password if login fails. - Verify index patterns (wazuh-template.json) are installed via curl.
Agent Connection Failures	- Re-register agents using the manage_agents tool in the Wazuh Manager GUI. - Check the agent's ossec.conf for the correct Manager IP. - Ensure port 1514/UDP or 1515/TCP is open. - Verify network connectivity between the agent and Manager.
Services Not Running	- Restart services via the Wazuh Manager GUI's **Services** tab or CLI: sudo systemctl start <service> (e.g., wazuh-manager, elasticsearch). - Check system logs: sudo journalctl -u <service>. - Ensure sufficient disk space (minimum 32GB) and check MicroSD card integrity.
GPG Key Errors	- Manually download and import keys using curl and gpg commands as per Wazuh Documentation.
TLS/Certificate Issues	- Ensure the hostname matches the certificate. - Temporarily disable strict SSL for local setups if issues persist.
System Freezes (Raspberry Pi)	- Reduce Elasticsearch heap size to 1GB in jvm.options. - Monitor RAM usage (aim for <6GB combined for Wazuh/ELK). - Ensure a stable 5V 3A power supply and consider a small UPS for power stability.

Additional Troubleshooting Tips

- **Version Compatibility**: Use Wazuh 4.5.4 and ELK Stack 7.17.13 to avoid plugin issues. Refer to Wazuh Documentation and Elastic Stack Guides for version details.
- **Storage Space**: Configure log rotation to prevent storage issues. Use a USB drive for additional space if needed.
- **Network Connectivity**: Ensure the Manager is reachable and ports are open. Wazuh agents cache up to ~100MB of logs during network interruptions and resend them when connectivity is restored.

8. Future Work

Cyber Sentinel has significant potential for enhancement, with the following planned improvements:

8.1 Immediate Pipeline

- **Honeypot Integration**: Fully integrate the Cowrie honeypot to provide detailed attacker information (e.g., IP addresses, commands, timestamps) into Wazuh alerts, enhancing threat intelligence.
- **Machine Learning**: Implement models like LogBERT and TabNet for anomaly detection in logs and network traffic, optimized for Raspberry Pi's resources to identify patterns beyond rule-based detection.

8.2 Long-Term Goals

- **Multi-OS Agent Support**: Extend Wazuh agent support to macOS, iOS, and IoT devices.
- **Mobile Alerts**: Enable push notifications to platforms like Telegram or WhatsApp for real-time alerts.
- **Cloud Dashboard**: Provide secure remote access to the Kibana dashboard for broader accessibility.
- **Automatic Response**: Enhance Wazuh's active-response feature to automatically block malicious IPs (e.g., during brute-force attacks).
- **Enhanced Attack Detection**: Improve detection of web-based attacks (e.g., zero-days) and phishing attempts, addressing limitations with outdated systems like Metasploitable-3.
- **User Interface Improvements**: Develop a more intuitive GUI for managing agents, services, and logs, potentially integrating with chatbots (e.g., Telegram, React app) for interactive alerts.
- **WAN Expansion**: Explore secure methods to extend monitoring to Wide Area Networks, addressing associated security risks.

- **Scalability**: Support clustering of multiple Raspberry Pis or stronger hardware (e.g., NVIDIA Jetson Nano) for larger networks.

9. Additional Notes

- **Resource Constraints**: On Raspberry Pi, monitor RAM usage (Elasticsearch can be resource-intensive) and adjust heap size to 1GB if freezes occur. Use a 32GB+ MicroSD card and configure log rotation to manage storage.
- **Version Compatibility**: Stick to recommended versions (Wazuh 4.5.4, ELK 7.17.13) to avoid plugin issues. Check compatibility details in Wazuh Documentation and Elastic Stack Guides.
- **Ethical Considerations**: Obtain consent for monitoring devices, especially in environments with employee data, and avoid capturing sensitive information (e.g., keylogging).
- **Legacy Systems**: Testing on outdated systems like Metasploitable-3 may require custom Wazuh rules to improve detection accuracy.
- **Contribution**: Future students can contribute by enhancing ML integration, honeypot logging, or multi-platform support, making Cyber Sentinel more robust and scalable.

10. Resources

- **GitHub Repository**: Access the installer, configurations, and source code at Cyber Sentinel GitHub. https://github.com/Abdullah-Mehtab/Cyber-Sentinal
- **Cyber Sentinal Manager Image;** https://drive.google.com/drive/folders/15uBKQwGSm9JnIhiNd8Ahtbww7eq9xbZm?usp=sharing
- **Official Documentation**:
  - Wazuh Documentation for setup, rules, and troubleshooting.
  - Elastic Stack Guides for ELK Stack configuration and management.
  - Kali Linux Downloads for OS installation.
- **Project Website**: Visit the Cyber Sentinel Website for downloads and other details.
- **Advisor Contact**: For further guidance, contact raufbutt@fccollege.edu.pk / abdullahmehtab666@gmail.com / m.nabeelmahmood@gmail.com

This comprehensive guide enables users to deploy, test, and extend Cyber Sentinel effectively, providing enterprise-grade security monitoring for small networks at a low cost.

Key Citations

- Cyber Sentinel Project Website
- Cyber Sentinel GitHub Repository