Cybersecurity Project

SOC Analysis, Blueteam

Home Lab for Elastic Stack SIEM (Security Information and Event Management)

Author

Emmanuel Sarpong

1. Project Overview

This project demonstrates the setup and usage of the Elastic Stack as a Security Information and Event Management (SIEM) solution in a home lab environment. The project involves using a Kali Linux Virtual Machine (VM) to generate security events, configuring an Elastic Agent to forward logs to the SIEM, and leveraging the Elastic Web portal to query, analyze, and visualize the logs.

Additionally, email alerts were set up for real-time notifications of significant security events.

Tools Used

2. Objectives

- Set up and configure an Elastic Stack SIEM environment.
- Generate and forward security events to the Elastic SIEM for analysis.
- Monitor and visualize security data through dashboards.
- Create email alerts for real-time security monitoring.
- Enhance understanding of SIEM capabilities through practical implementation.

3. Prerequisites

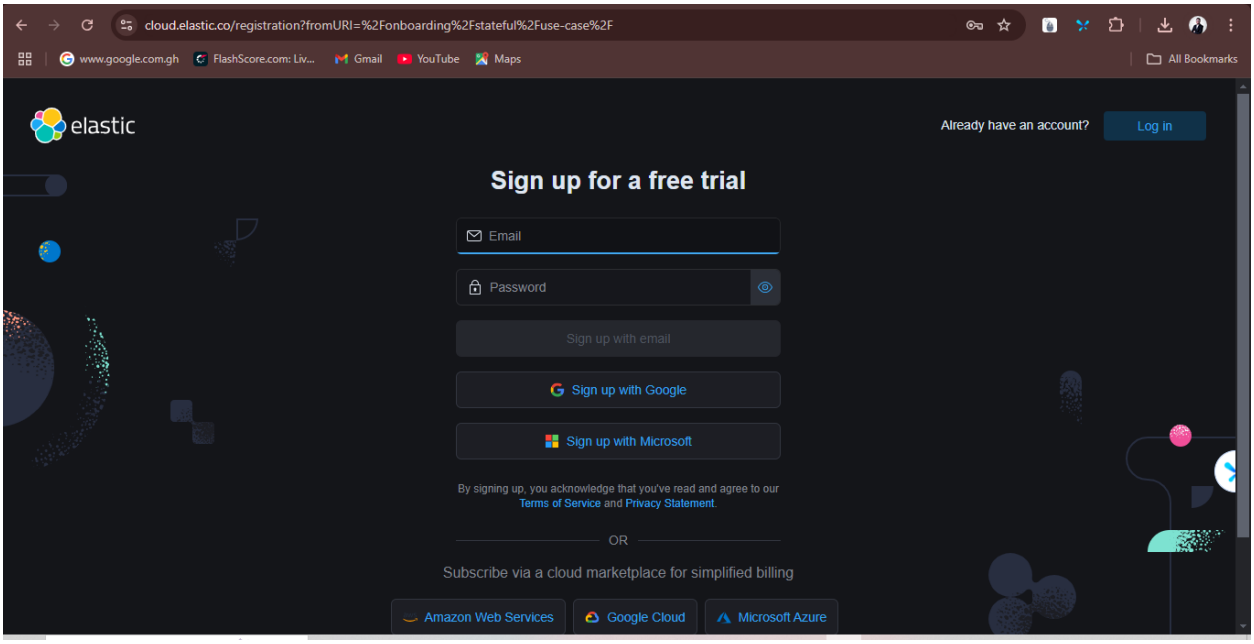
Before beginning the project, the following requirements were fulfilled:

- **Virtualization Software**: VirtualBox.
- **Elastic Account**: A free Elastic account was created for access to the Elastic Web portal.
- **Basic Linux Knowledge**: Understanding of Linux commands and virtualization software.
- **Software**: Kali Linux ISO for setting up the VM.

4. Tasks Overview

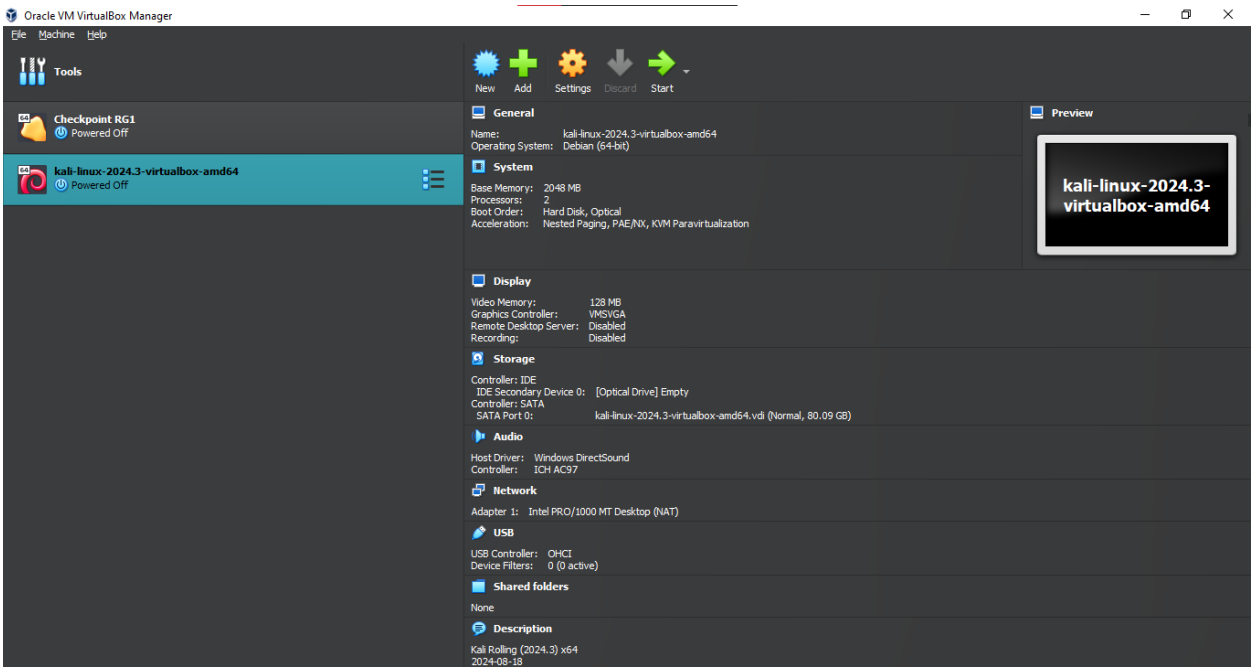
4.1. Set up Elastic Account

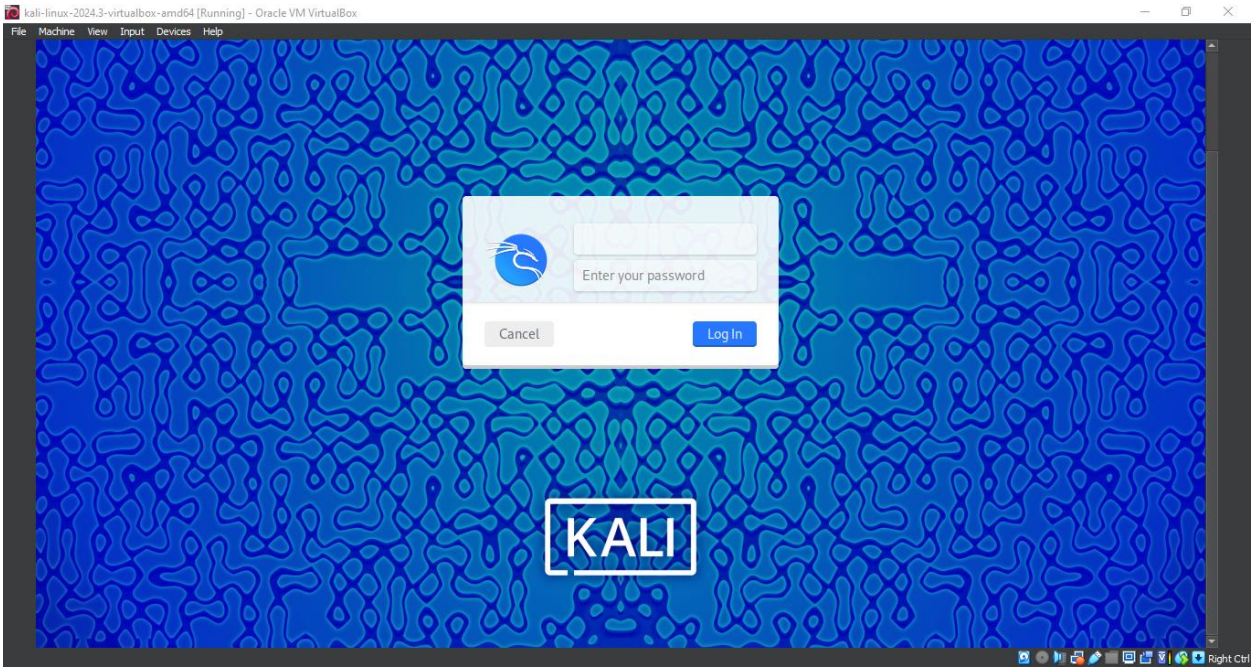
- Registered a free account on the Elastic platform.
- Configured the Elastic Cloud to manage and monitor SIEM logs via the web portal.



4.2. Install Kali Linux VM

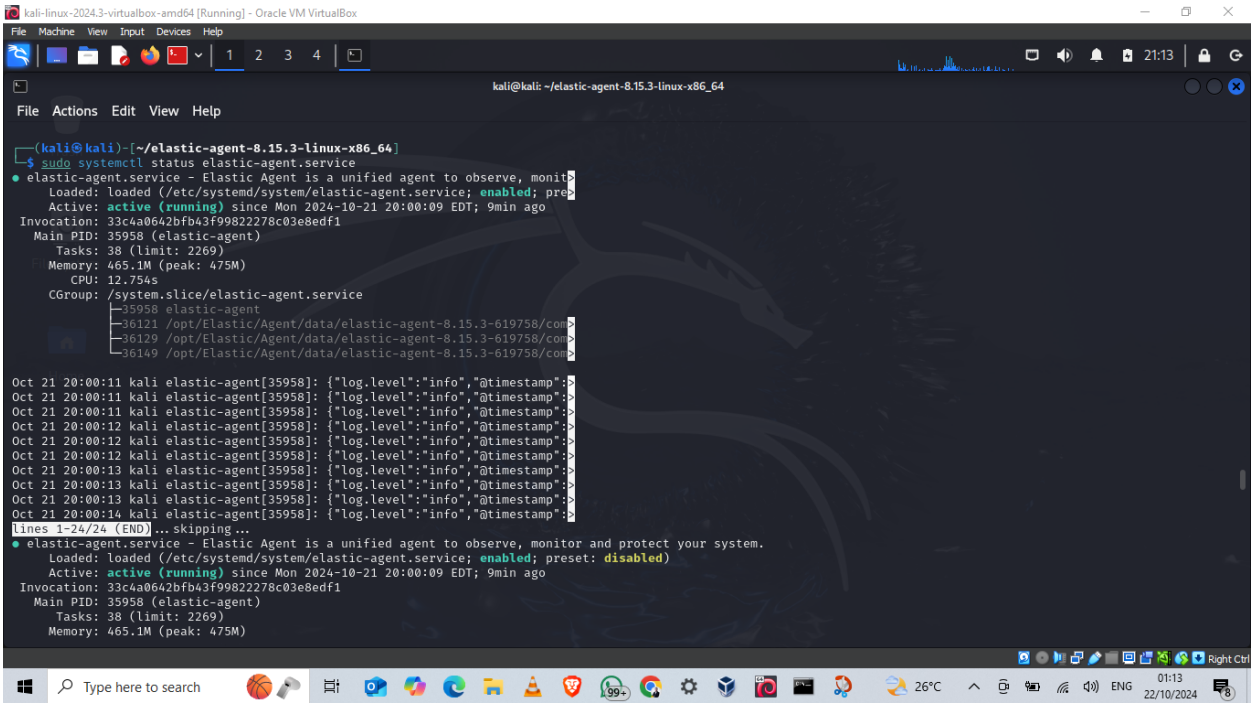
- Installed and configured Kali Linux on VirtualBox
- Ensured network connectivity between the Kali VM and the Elastic Stack.

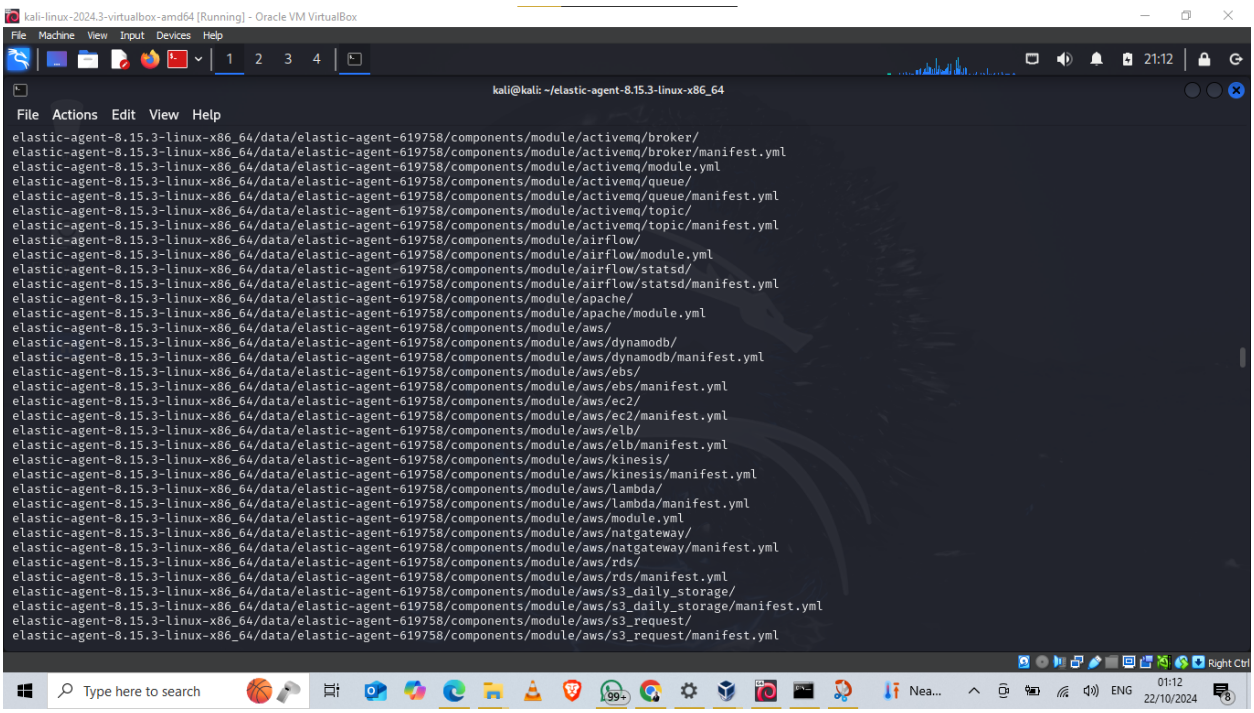




4.3. Configure Elastic Agent

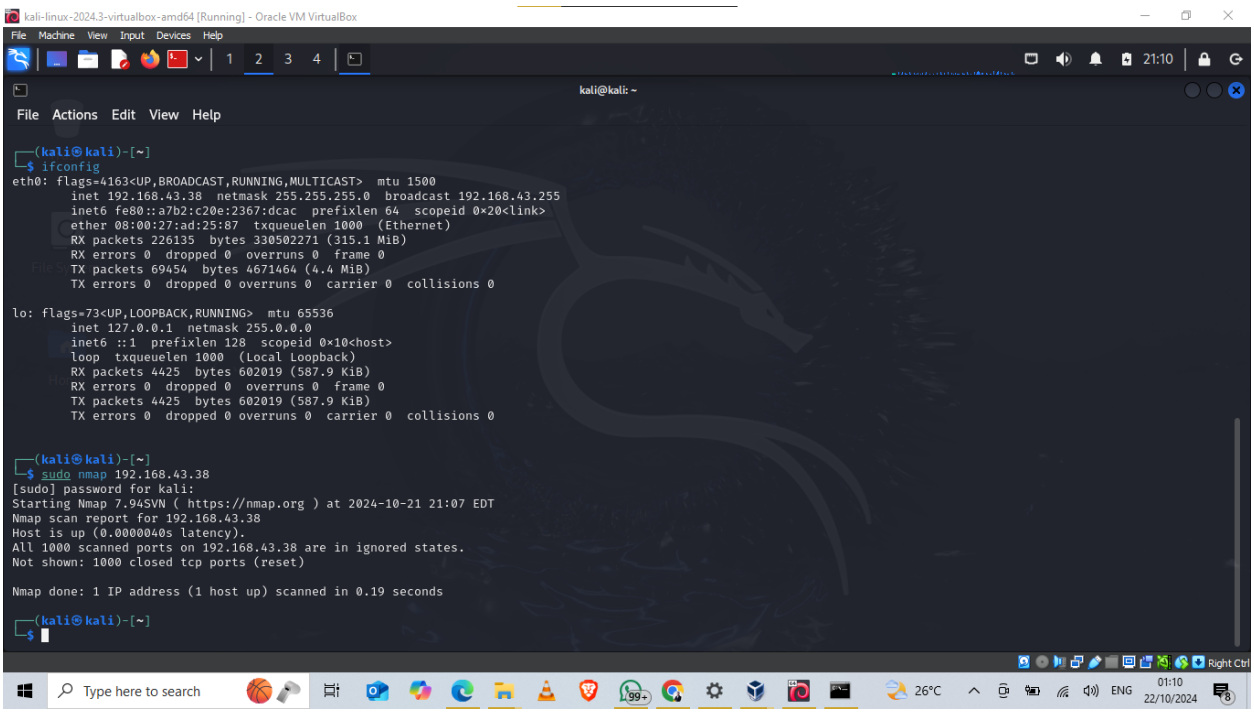
- Installed the Elastic Agent on the Kali Linux VM.
- Configured the agent to forward system logs, network logs, and security events to the Elastic Stack.
- Validated the agent's successful connection to the Elastic Web portal.

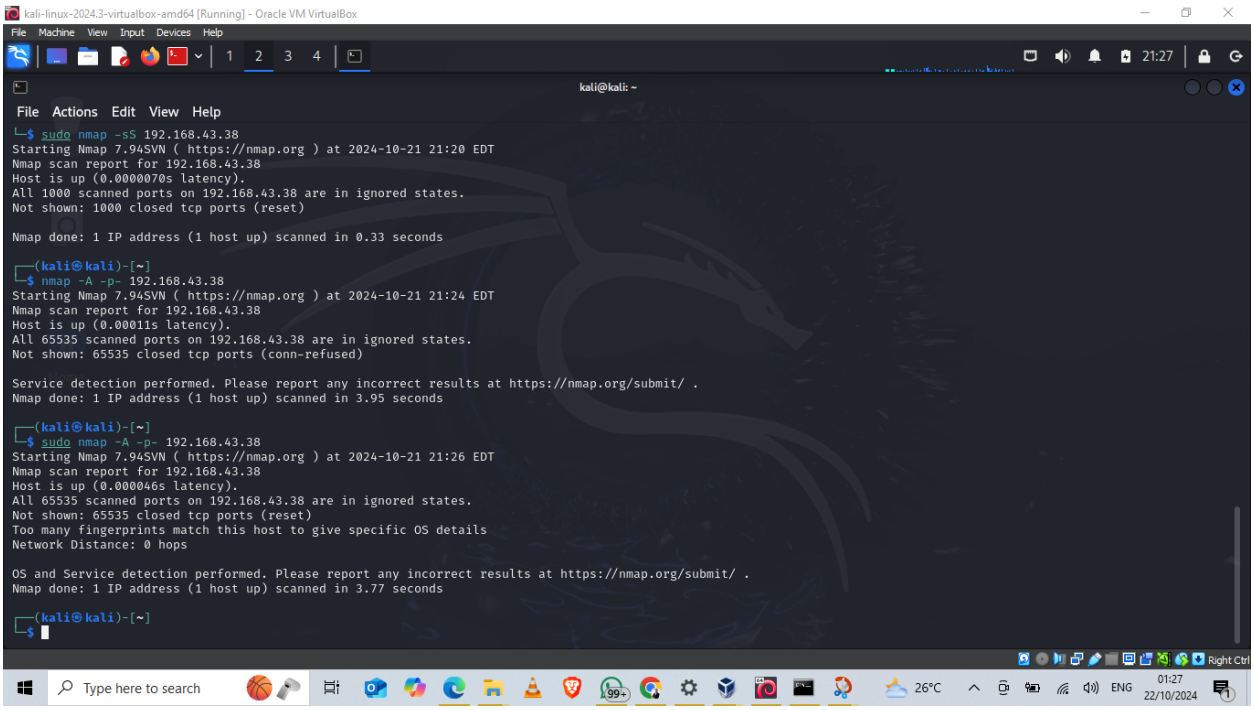


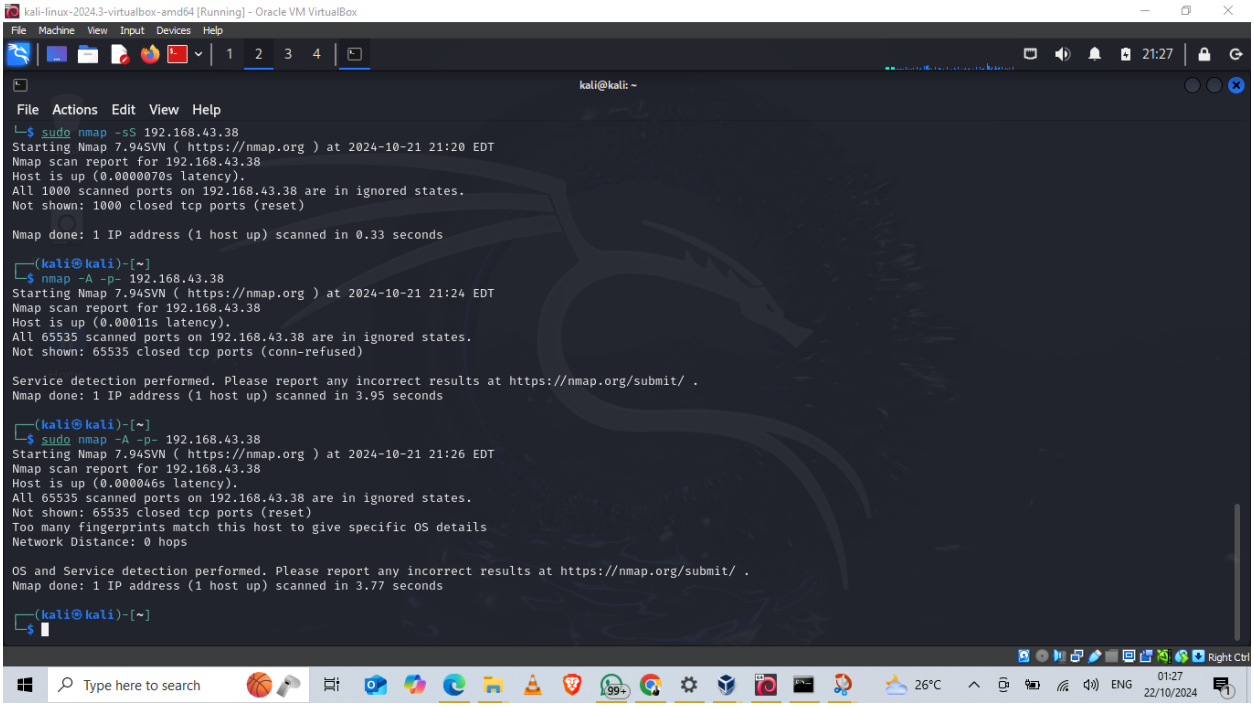


4.4. Generate Security Events

- Performed **Nmap scans** from the Kali Linux VM to simulate reconnaissance activity.
- Verified that logs for the scans were captured and forwarded to the Elastic SIEM.



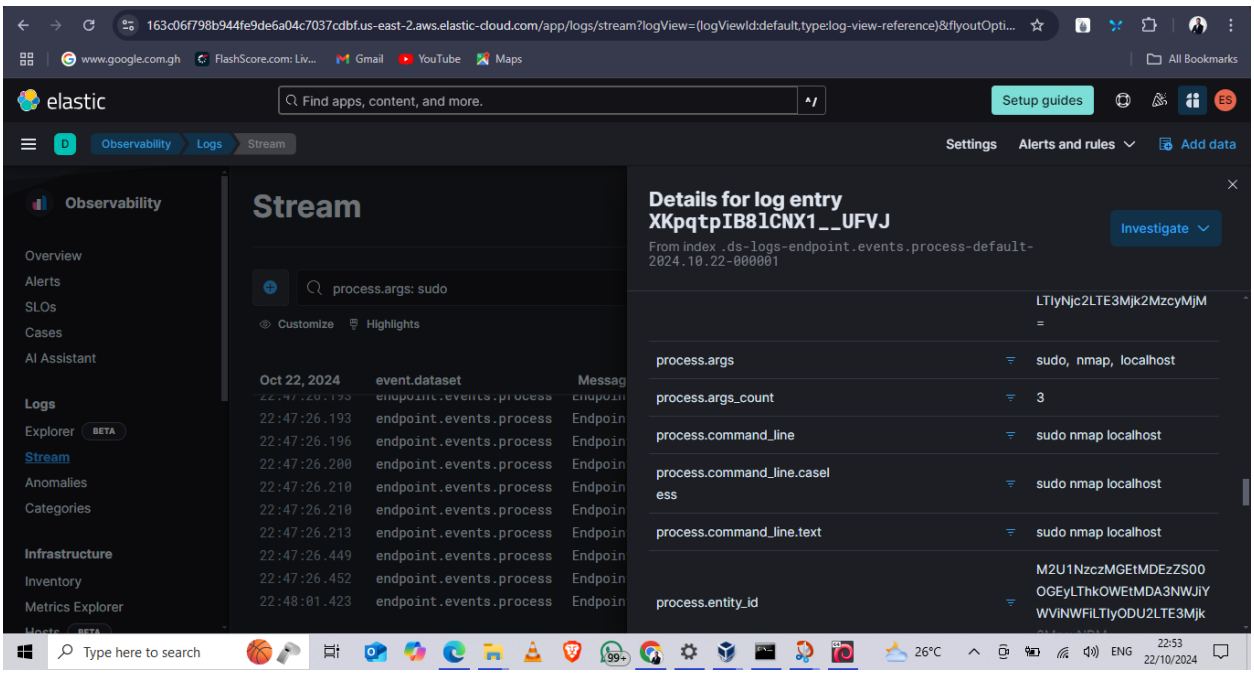


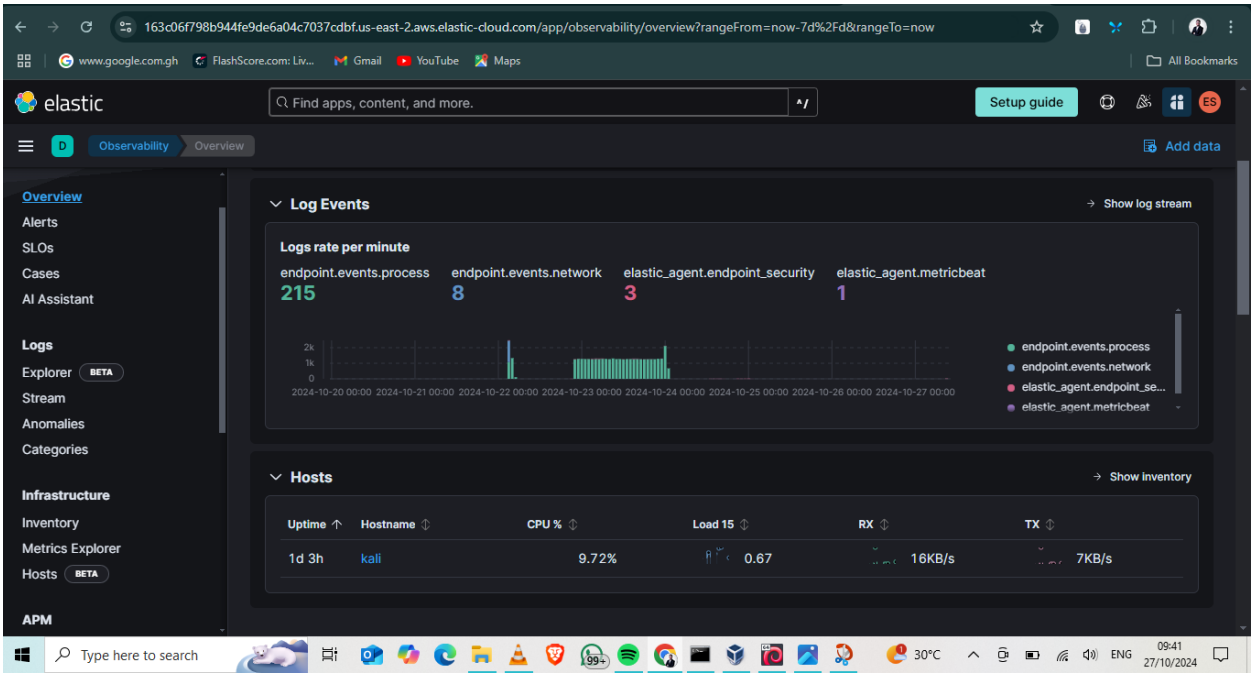


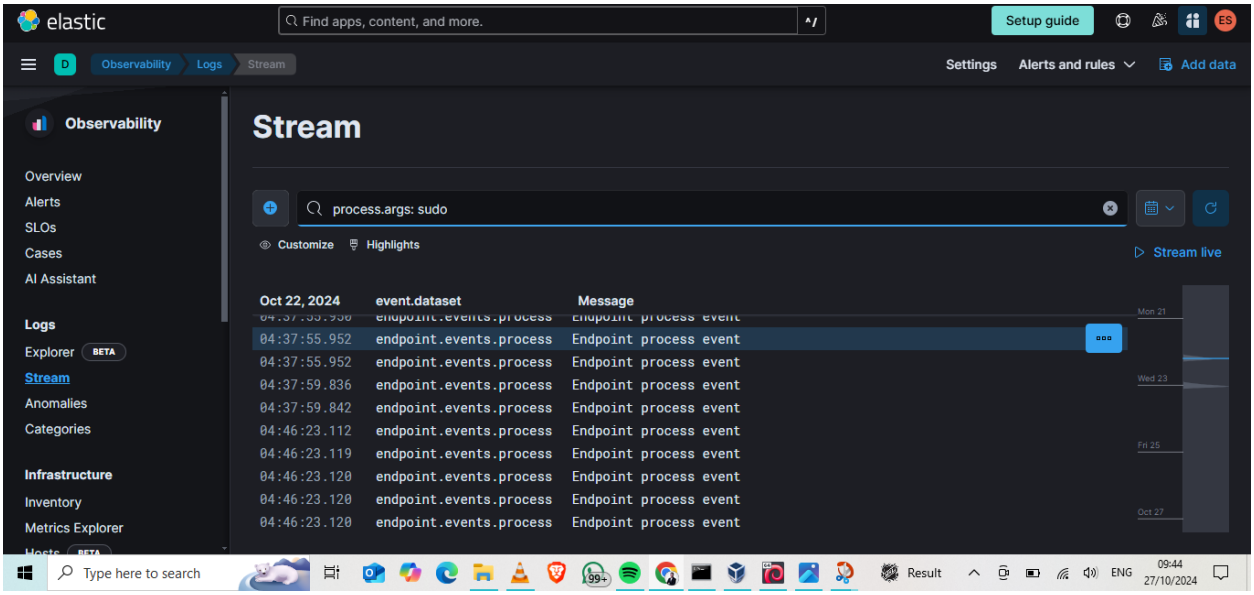
4.5. Query and Analyze Logs

- Used the Elastic Web portal to query logs for specific events, such as Nmap scans.

- Analyzed logs for insights into potential security incidents and endpoint activity.

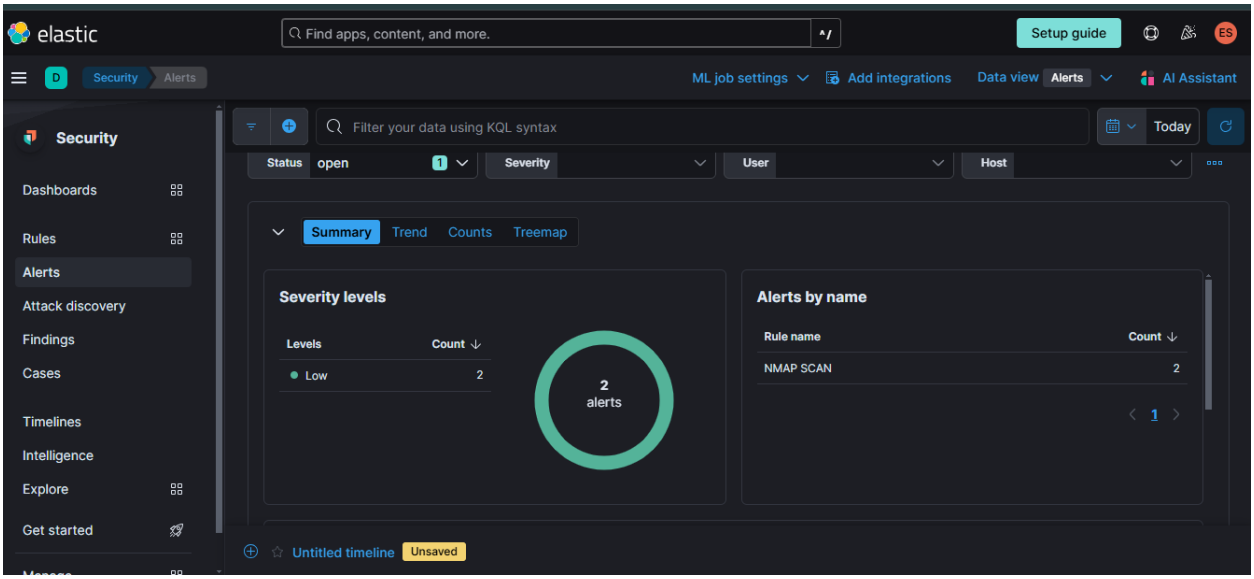


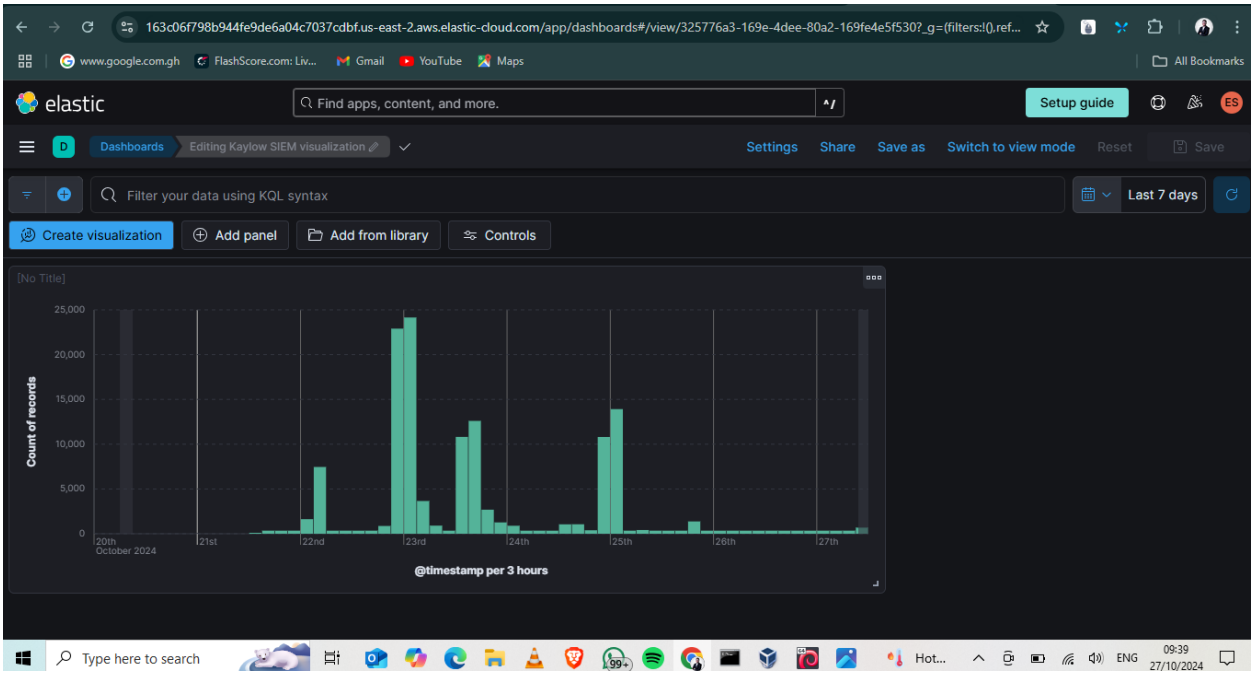




4.6. Create Dashboards

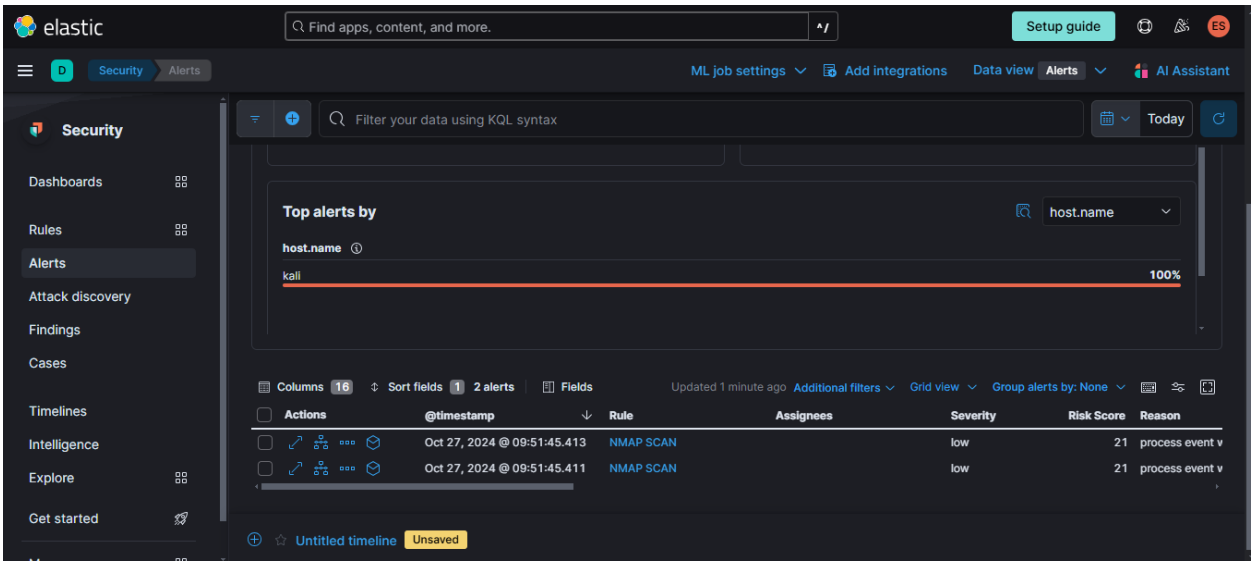
- Developed a custom dashboard on the Elastic portal to visualize security data, including:
  - System logs.
  - Network activity.
  - Security events like Nmap scans.

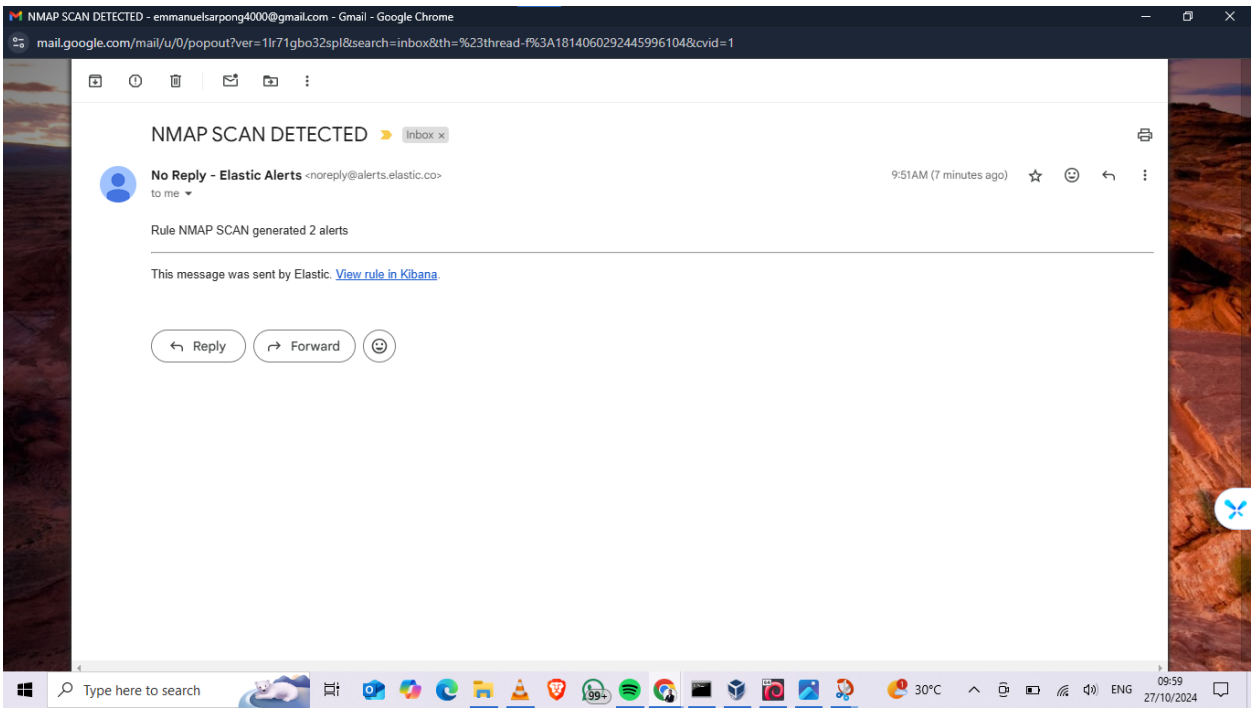




4.7. Configure Alerts

- Set up email alerts in Elastic for real-time notifications of critical security events.
- Verified that email notifications were received when Nmap scans were executed on the Kali VM.





5. Implementation Details

5.1. Setting up Elastic Agent

1. Downloaded and installed the Elastic Agent package on the Kali Linux VM.
2. Edited configuration files to define the Elastic endpoint and authentication keys.
3. Tested agent functionality by generating sample logs.

5.2. Generating Security Events

1. Ran various Nmap scan commands, such as:
   - `nmap -sS <target_ip>`: SYN scan.
   - `nmap -A <target_ip>`: Aggressive scan.
2. Confirmed the logs in Elastic SIEM, which showed details like:
   - Source IP.
   - Scan type.
   - Ports targeted.

5.3. Querying and Analyzing Logs

- Used Elastic Query Language (EQL) to find specific events.
- Examples:

- Query for Nmap events: `source.event.dataset: "nmap"`.
- Search for alerts triggered by suspicious network activity.

5.4. Dashboard Creation

- Designed a dashboard with the following visualizations:
  - Event counts by type.
  - Timeline of events.
  - Geographical map of source/destination IPs (if applicable).

5.5. Setting Up Alerts

1. Configured rules in the Elastic SIEM for predefined triggers, such as Nmap scans.
2. Linked an email account to receive notifications.
3. Verified alerts by performing real-time scans on the Kali VM and observing email notifications.

---

6. Results

- Successfully forwarded logs from the Kali Linux VM to the Elastic SIEM.
- Nmap scans were detected in real-time, triggering email notifications.
- Custom dashboard provided insights into the security events, making analysis intuitive.
- The project demonstrated the value of SIEM for detecting and analyzing security events in a controlled environment.

---

7. Conclusion

This project highlights the effectiveness of the Elastic Stack as a SIEM solution for monitoring and analyzing security events. The setup provided hands-on experience with log forwarding, querying, visualization, and alerting. The integration of email notifications further enhanced the responsiveness to potential incidents.

---

8. Future Enhancements

- Expand the lab to include more endpoints and a variety of operating systems.
- Implement additional security event generation tools, such as Metasploit.
- Explore advanced Elastic Stack features, like machine learning for anomaly detection.