



**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

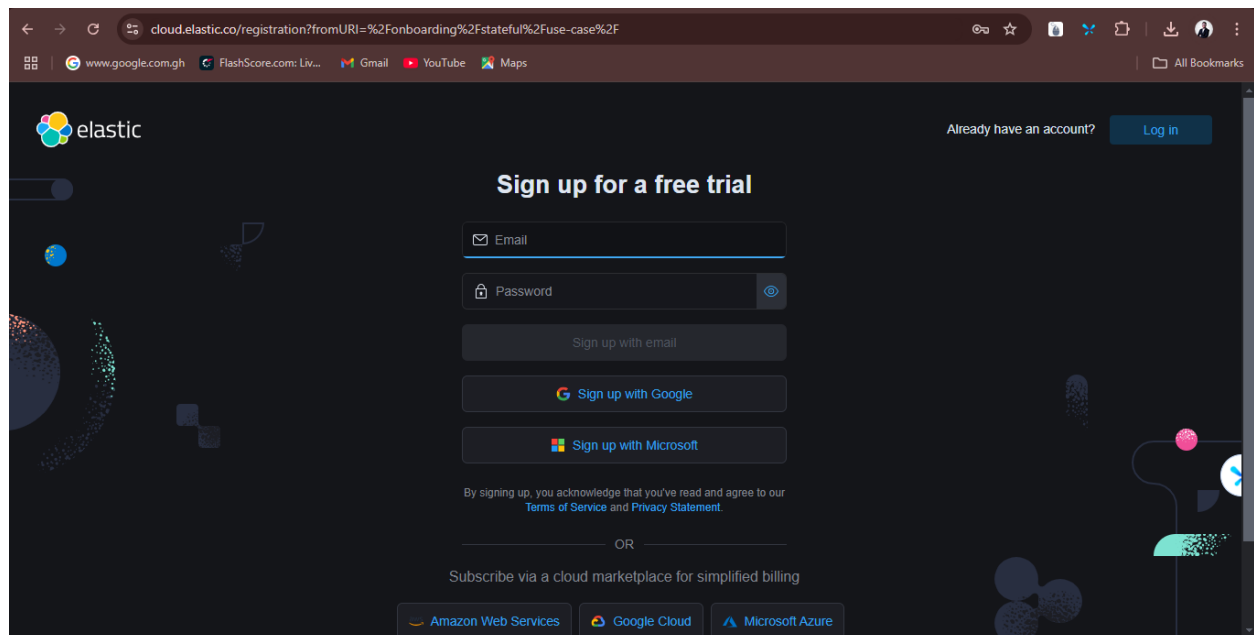
Before beginning the project, the following requirements were fulfilled:

- **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

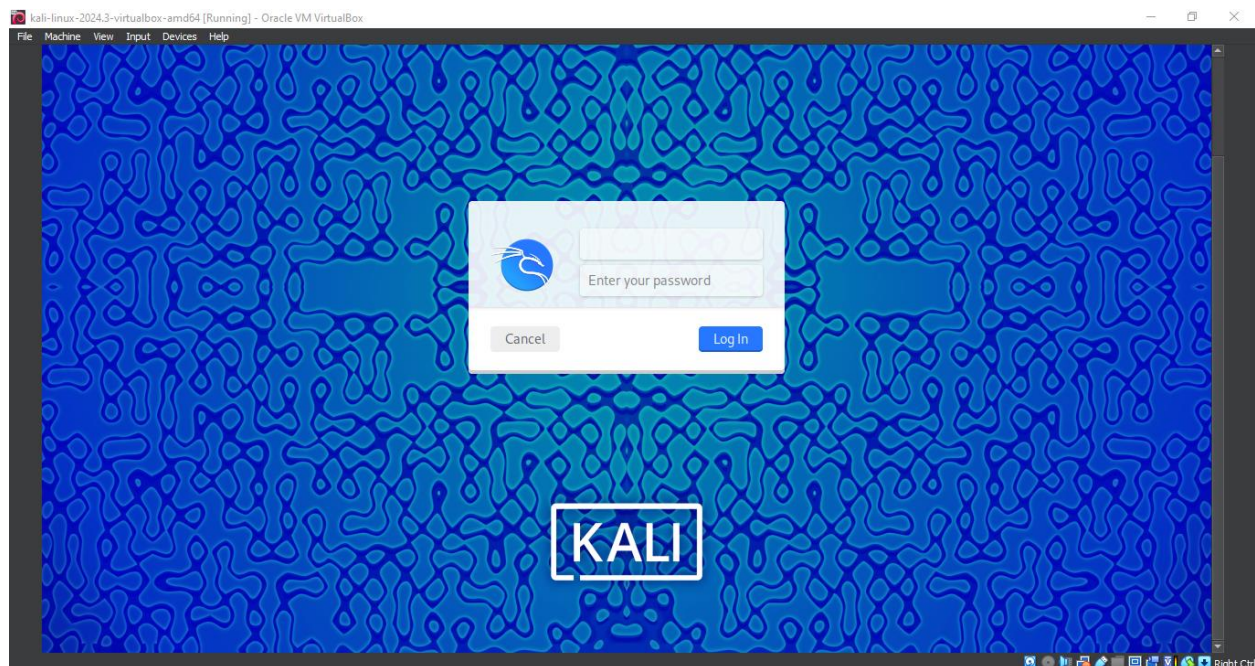
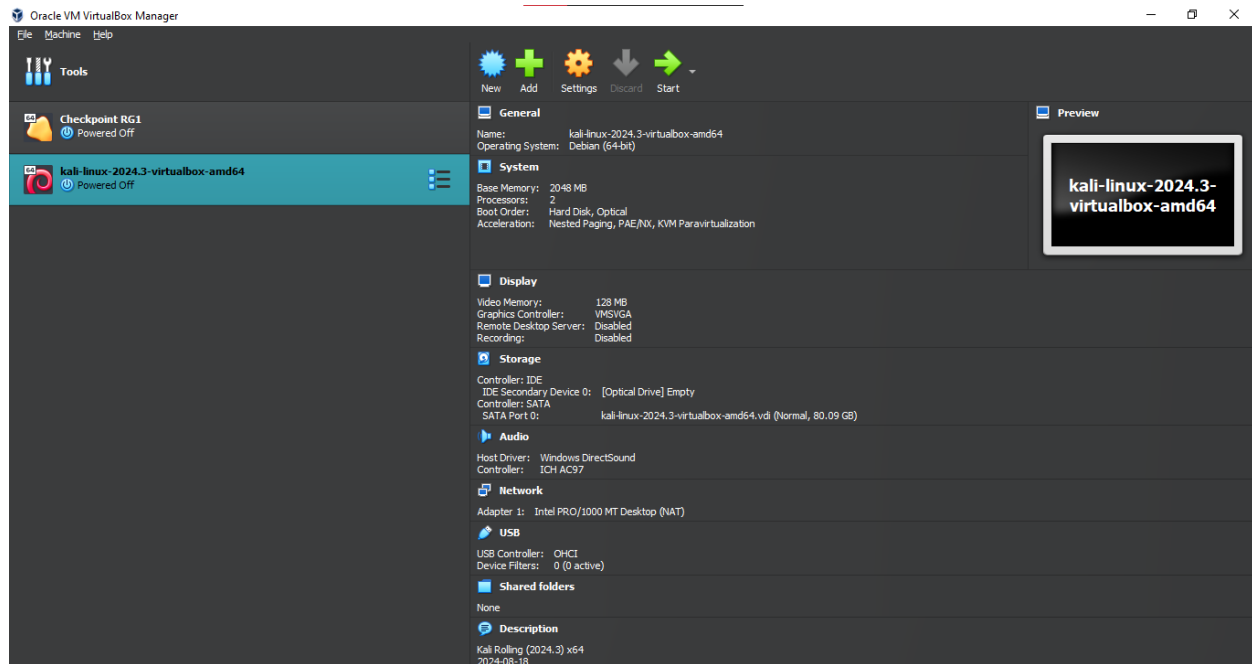
### 4.1. Set up Elastic Account

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



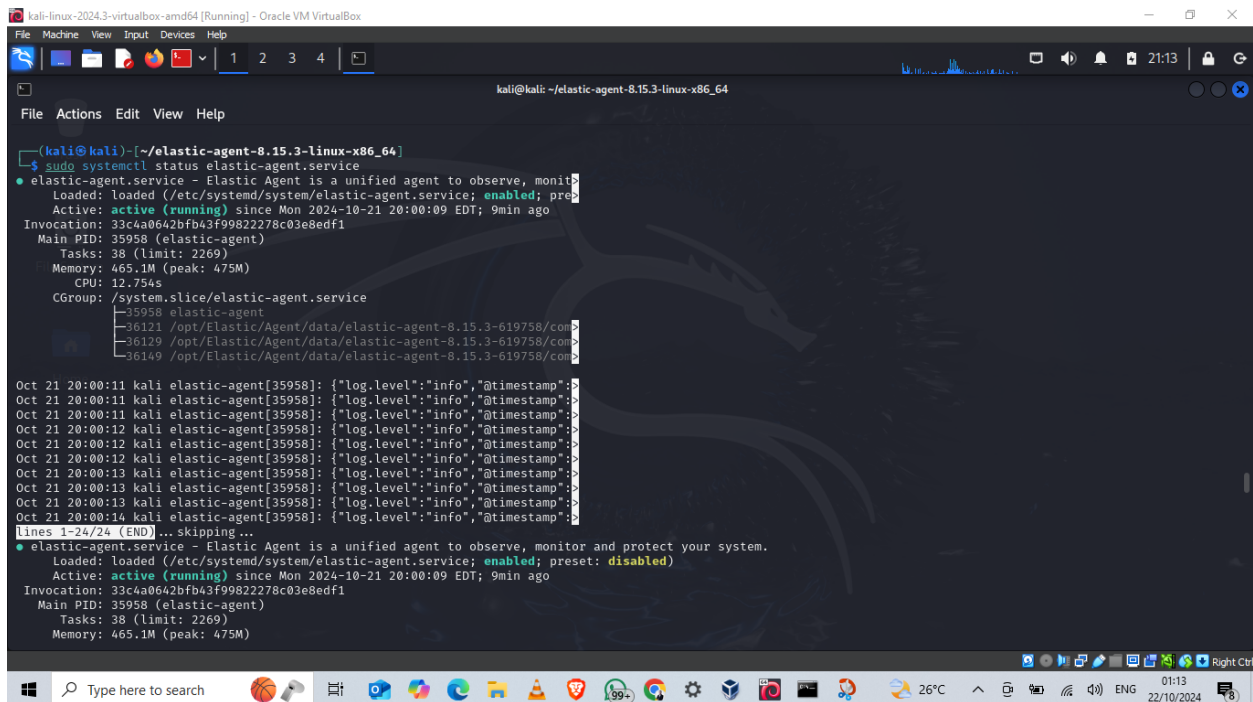
## 4.2. Install Kali Linux VM

- 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.



```

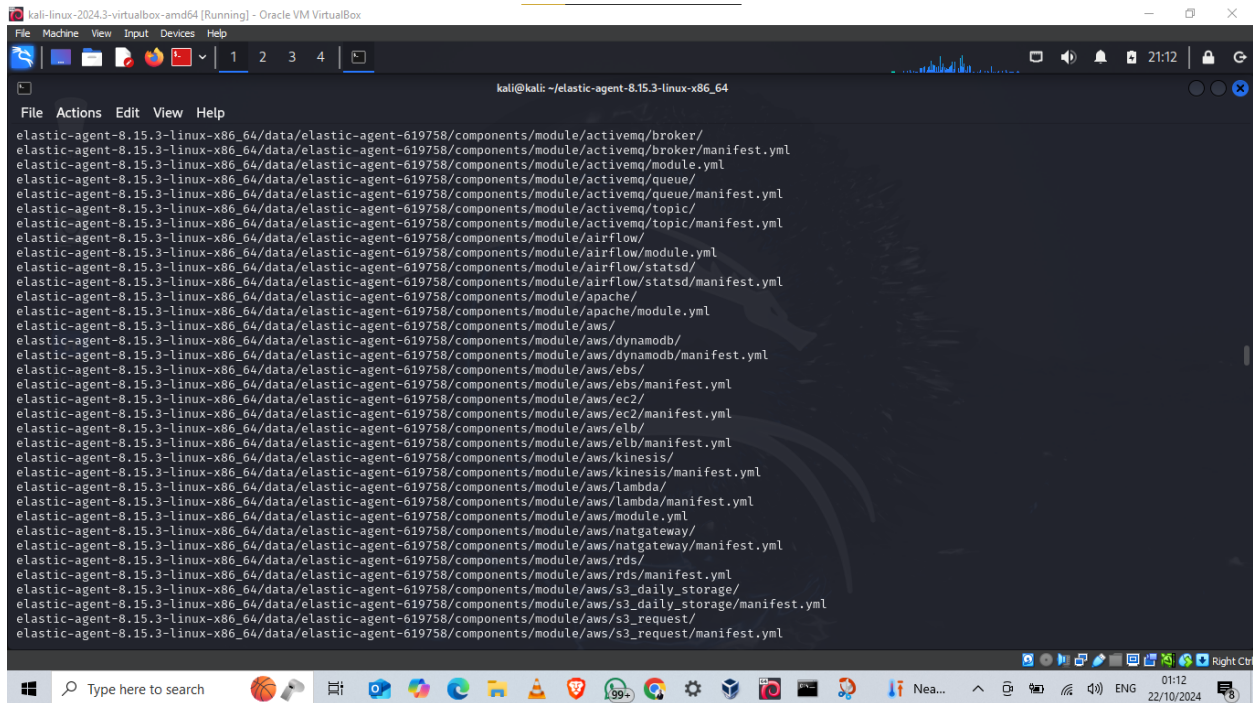
kali@kali: ~/elastic-agent-8.15.3-linux-x86_64
File Actions Edit View Help

(kali@kali)~/elastic-agent-8.15.3-linux-x86_64
$ sudo systemctl status elastic-agent.service
● elastic-agent.service - Elastic Agent is a unified agent to observe, monitor and protect your system.
   Loaded: loaded (/etc/systemd/system/elastic-agent.service; enabled; preset: disabled)
   Active: active (running) since Mon 2024-10-21 20:00:09 EDT; 9min ago
 Invocation: 33c4a0642bfb43f99822278c03e8edf1
    Main PID: 35958 (elastic-agent)
      Tasks: 38 (limit: 2269)
     Memory: 465.1M (peak: 475M)
        CPU: 12.754s
    CGroup: /system.slice/elastic-agent.service
            └─35958 elastic-agent
                └─36121 /opt/Elastic/Agent/data/elastic-agent-8.15.3-619758/comp
                  └─36129 /opt/Elastic/Agent/data/elastic-agent-8.15.3-619758/comp
                    └─36149 /opt/Elastic/Agent/data/elastic-agent-8.15.3-619758/comp

Oct 21 20:00:11 kali elastic-agent[35958]: {"log.level":"info","@timestamp":"2024-10-21T20:00:11.111Z","@version":"8.15.3","agent.id":"33c4a0642bfb43f99822278c03e8edf1","agent.type":"fleet_server","log.offset":0}
Oct 21 20:00:11 kali elastic-agent[35958]: {"log.level":"info","@timestamp":"2024-10-21T20:00:11.111Z","@version":"8.15.3","agent.id":"33c4a0642bfb43f99822278c03e8edf1","agent.type":"fleet_server","log.offset":0}
Oct 21 20:00:11 kali elastic-agent[35958]: {"log.level":"info","@timestamp":"2024-10-21T20:00:11.111Z","@version":"8.15.3","agent.id":"33c4a0642bfb43f99822278c03e8edf1","agent.type":"fleet_server","log.offset":0}
Oct 21 20:00:12 kali elastic-agent[35958]: {"log.level":"info","@timestamp":"2024-10-21T20:00:12.111Z","@version":"8.15.3","agent.id":"33c4a0642bfb43f99822278c03e8edf1","agent.type":"fleet_server","log.offset":0}
Oct 21 20:00:12 kali elastic-agent[35958]: {"log.level":"info","@timestamp":"2024-10-21T20:00:12.111Z","@version":"8.15.3","agent.id":"33c4a0642bfb43f99822278c03e8edf1","agent.type":"fleet_server","log.offset":0}
Oct 21 20:00:12 kali elastic-agent[35958]: {"log.level":"info","@timestamp":"2024-10-21T20:00:12.111Z","@version":"8.15.3","agent.id":"33c4a0642bfb43f99822278c03e8edf1","agent.type":"fleet_server","log.offset":0}
Oct 21 20:00:13 kali elastic-agent[35958]: {"log.level":"info","@timestamp":"2024-10-21T20:00:13.111Z","@version":"8.15.3","agent.id":"33c4a0642bfb43f99822278c03e8edf1","agent.type":"fleet_server","log.offset":0}
Oct 21 20:00:13 kali elastic-agent[35958]: {"log.level":"info","@timestamp":"2024-10-21T20:00:13.111Z","@version":"8.15.3","agent.id":"33c4a0642bfb43f99822278c03e8edf1","agent.type":"fleet_server","log.offset":0}
Oct 21 20:00:13 kali elastic-agent[35958]: {"log.level":"info","@timestamp":"2024-10-21T20:00:13.111Z","@version":"8.15.3","agent.id":"33c4a0642bfb43f99822278c03e8edf1","agent.type":"fleet_server","log.offset":0}
Oct 21 20:00:14 kali elastic-agent[35958]: {"log.level":"info","@timestamp":"2024-10-21T20:00:14.111Z","@version":"8.15.3","agent.id":"33c4a0642bfb43f99822278c03e8edf1","agent.type":"fleet_server","log.offset":0}
lines 1-24/24 (END) ... skipping...
● elastic-agent.service - Elastic Agent is a unified agent to observe, monitor and protect your system.
   Loaded: loaded (/etc/systemd/system/elastic-agent.service; enabled; preset: disabled)
   Active: active (running) since Mon 2024-10-21 20:00:09 EDT; 9min ago
 Invocation: 33c4a0642bfb43f99822278c03e8edf1
    Main PID: 35958 (elastic-agent)
      Tasks: 38 (limit: 2269)
     Memory: 465.1M (peak: 475M)

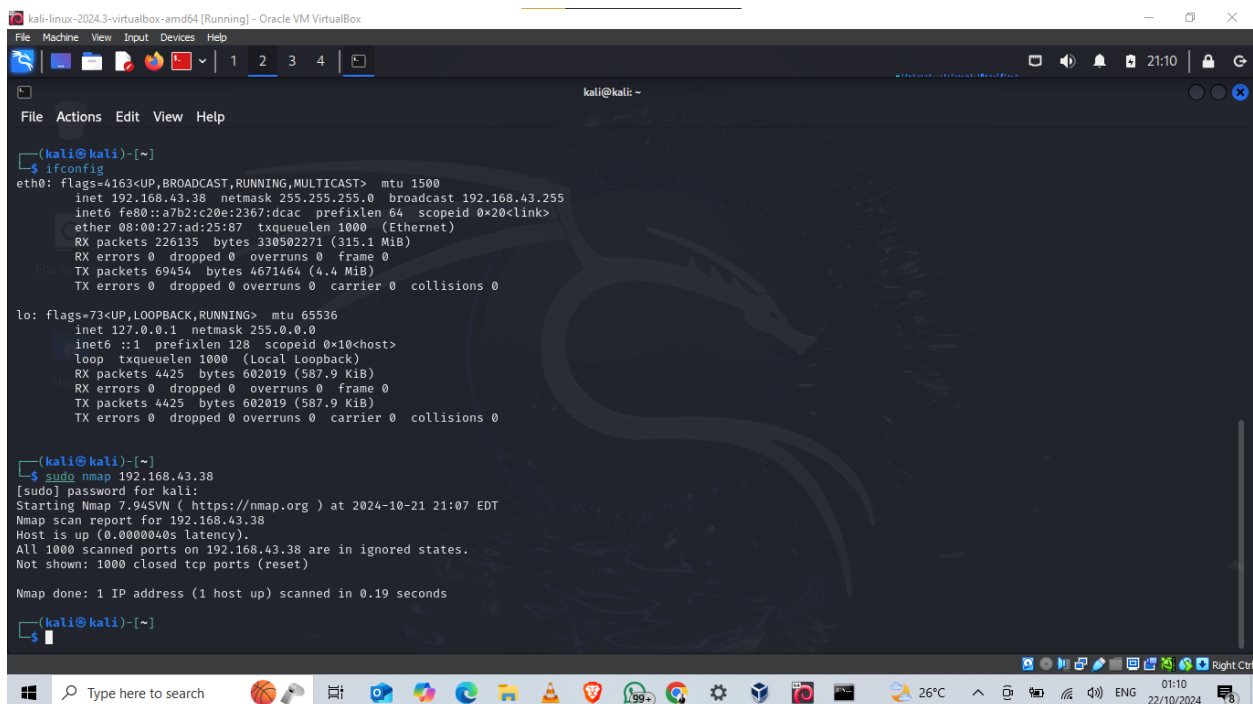
```





#### 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.



```

kali@kali: ~
File Actions Edit View Help
└─$ sudo nmap -sS 192.168.43.38
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-21 21:20 EDT
Nmap scan report for 192.168.43.38
Host is up (0.0000070s latency).
All 1000 scanned ports on 192.168.43.38 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds

kali@kali:~]
└─$ nmap -A -p- 192.168.43.38
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-21 21:24 EDT
Nmap scan report for 192.168.43.38
Host is up (0.000111s latency).
All 65535 scanned ports on 192.168.43.38 are in ignored states.
Not shown: 65535 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.95 seconds

kali@kali:~]
└─$ sudo nmap -A -p- 192.168.43.38
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-21 21:26 EDT
Nmap scan report for 192.168.43.38
Host is up (0.000046s latency).
All 65535 scanned ports on 192.168.43.38 are in ignored states.
Not shown: 65535 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.77 seconds

kali@kali:~]
└─$

```

```

kali@kali: ~
File Actions Edit View Help
└─$ sudo nmap -sS 192.168.43.38
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-21 21:20 EDT
Nmap scan report for 192.168.43.38
Host is up (0.0000070s latency).
All 1000 scanned ports on 192.168.43.38 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds

kali@kali:~]
└─$ nmap -A -p- 192.168.43.38
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-21 21:24 EDT
Nmap scan report for 192.168.43.38
Host is up (0.000111s latency).
All 65535 scanned ports on 192.168.43.38 are in ignored states.
Not shown: 65535 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.95 seconds

kali@kali:~]
└─$ sudo nmap -A -p- 192.168.43.38
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-21 21:26 EDT
Nmap scan report for 192.168.43.38
Host is up (0.000046s latency).
All 65535 scanned ports on 192.168.43.38 are in ignored states.
Not shown: 65535 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.77 seconds

kali@kali:~]
└─$

```

#### 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.

The screenshot shows the Elastic Observability interface. The left sidebar contains navigation links for Overview, Alerts, SLOs, Cases, AI Assistant, Logs, Explorer (BETA), Stream, Anomalies, Categories, Infrastructure, Inventory, Metrics Explorer, and Hosts. The main content area is titled 'Stream' and displays a list of log entries. A search filter 'process.args: sudo' is applied. The 'Details for log entry' panel on the right shows the following fields:

Field	Value
process.args	sudo, nmap, localhost
process.args_count	3
process.command_line	sudo nmap localhost
process.command_line.caseless	sudo nmap localhost
process.command_line.text	sudo nmap localhost
process.entity_id	M2U1Nzc2MGEtMDEzZS00 OGEyLThkOWE1MDA3NWJiY WVlNWFlTiyODU2LTE3Mjk

The screenshot shows the Elastic Observability Overview view. The left sidebar contains navigation links for Overview, Alerts, SLOs, Cases, AI Assistant, Logs, Explorer (BETA), Stream, Anomalies, Categories, Infrastructure, Inventory, Metrics Explorer, and Hosts. The main content area is titled 'Overview' and displays two sections:

### Log Events

Logs rate per minute

Log Type	Rate
endpoint.events.process	215
endpoint.events.network	8
elastic_agent.endpoint_security	3
elastic_agent.metricbeat	1

A bar chart shows the logs rate per minute over time from 2024-10-20 00:00 to 2024-10-27 00:00. The legend indicates the following series:

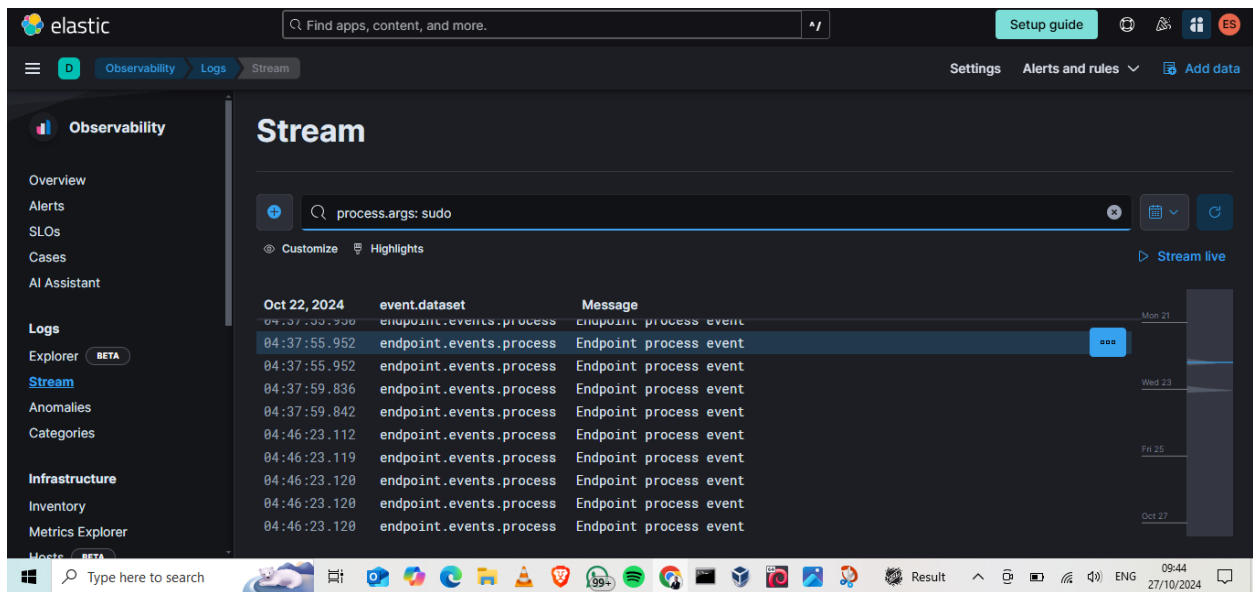
- endpoint.events.process (green)
- endpoint.events.network (blue)
- elastic\_agent.endpoint\_security (red)
- elastic\_agent.metricbeat (purple)

### Hosts

Uptime ↑ Hostname ↓ CPU % ↓ Load 15 ↓ RX ↓ TX ↓

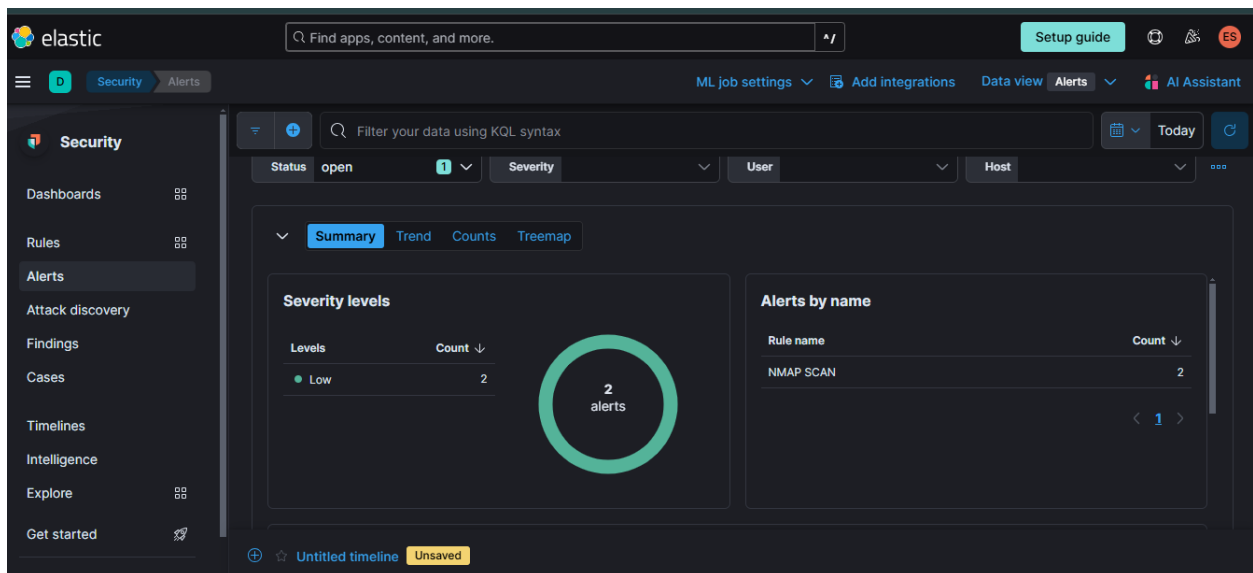
Uptime	Hostname	CPU %	Load 15	RX	TX
1d 3h	kali	9.72%	0.67	16KB/s	7KB/s





#### 4.6. Create Dashboards

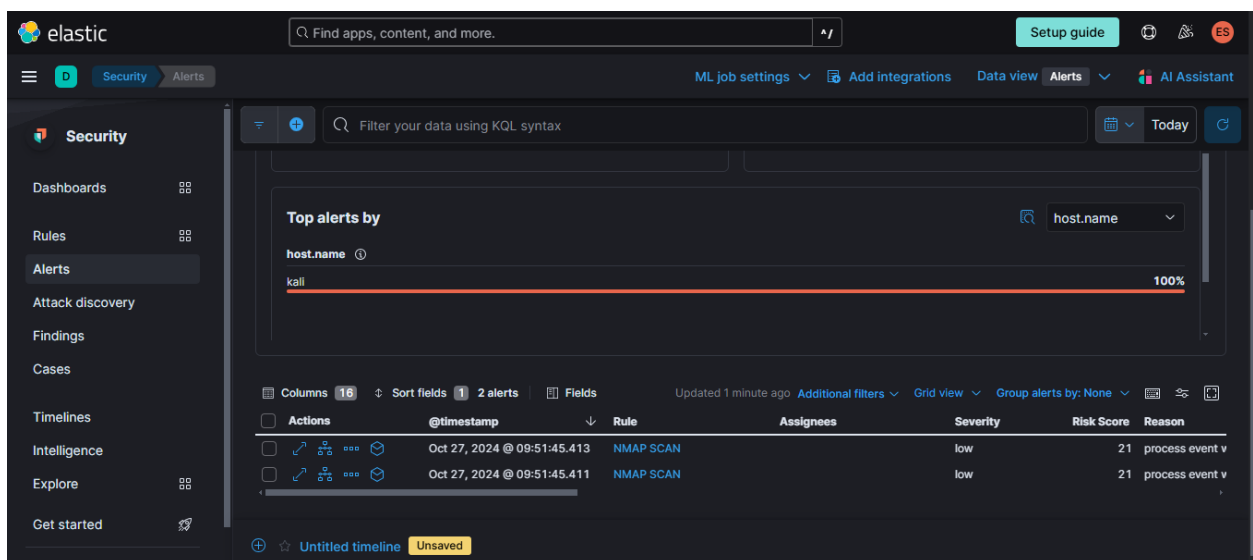
- Developed a custom dashboard on the Elastic portal to visualize security data, including:
  - System logs.
  - Network activity.
  - Security events like Nmap scans.

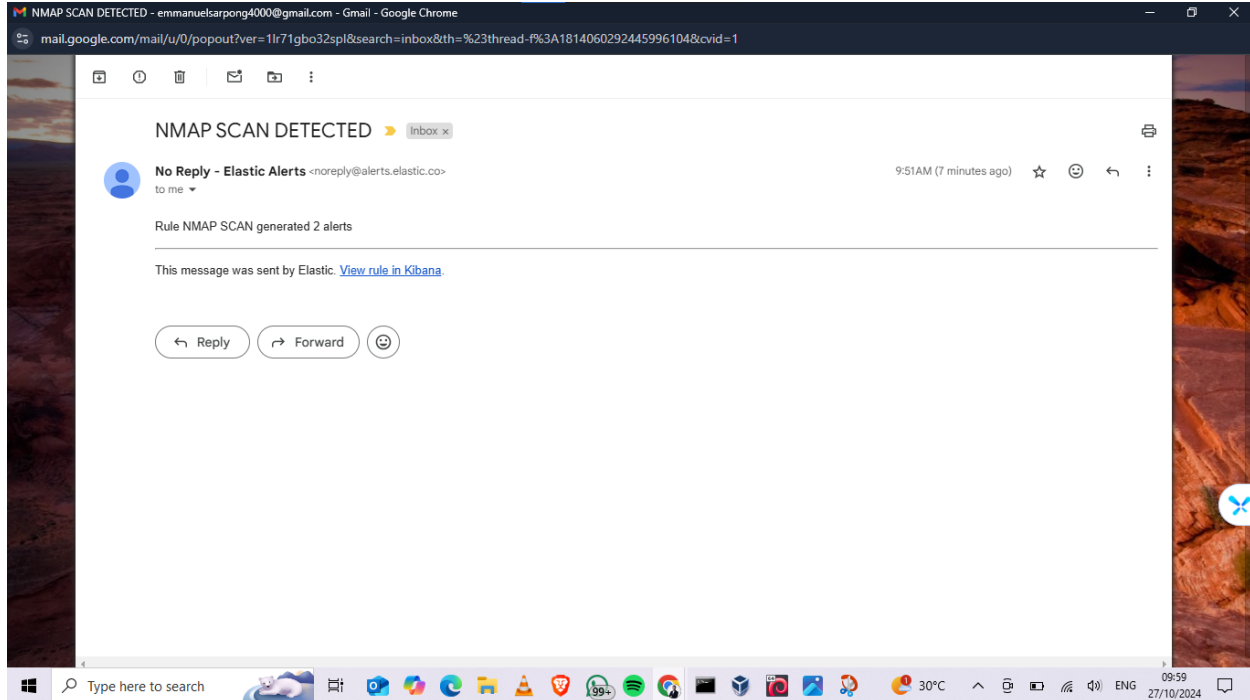




#### 4.7. Configure Alerts

- 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:
  - o `nmap -sS <target_ip>`: SYN scan.
  - o `nmap -A <target_ip>`: Aggressive scan.
2. Confirmed the logs in Elastic SIEM, which showed details like:
  - o Source IP.
  - o Scan type.
  - o 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.



## Components and Capabilities of SIEM

