Elastic SIEM Home Lab Report

Introduction

This project aims to establish a home lab environment for Elastic Stack Security Information and Event Management (SIEM) using Elastic Cloud, Kali Linux, and VirtualBox. The lab demonstrates the setup of an Elastic SIEM instance, integration with a Linux virtual machine (VM) for data collection, and basic analysis of security events. It provides a hands-on learning platform for understanding SIEM functionality, log analysis, and alert configuration.

Tools Used

- **Kali Linux**: A Linux distribution optimized for penetration testing and security research.
- **Elastic SIEM**: A cloud-based platform for centralized log collection, analysis, and visualization.
- **VirtualBox**: An open-source virtualization software to run the Kali Linux VM.

Step-by-Step Setup Instructions

Prerequisites

1. VirtualBox or similar virtualization software installed.
2. Basic knowledge of Linux commands and virtualization.
3. Elastic account (free trial or paid plan).

Task 1: Setting up my Elastic Account

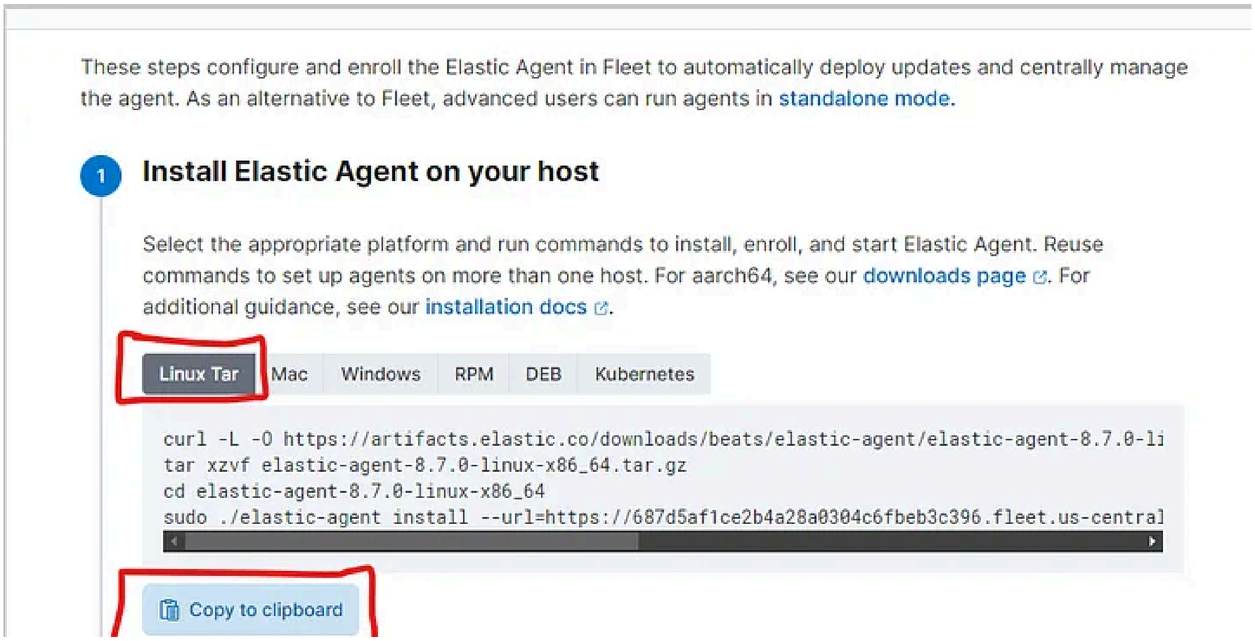
1. Signed up for an Elastic Cloud account.
2. Logged in and started a free trial.
3. Created a new deployment:
   - ○ Select **Elasticsearch** as the deployment type.
   - ○ Choose a suitable region and deployment size.
   - ○ Click **Create Deployment**.

Task 2: Installed and Configured the Kali Linux VM to run on Virtual Box

1. Downloaded the Kali Linux VM image from the official site.
2. Set up a new VM in VirtualBox application:
    - Import the VM image.
    - Configure resources (e.g., memory, CPU).
3. Started up the VM and completed the installation using default credentials.

Task 3: Install Elastic Agent on Kali VM

1. Log in to the Elastic console and navigate to **Integrations**.
2. Search for **Elastic Defend** and follow the installation guide for Linux.
3. On the Kali VM:
    - Copy the installation command from the Elastic console.
    - Run the command in the terminal to install the Elastic Agent.



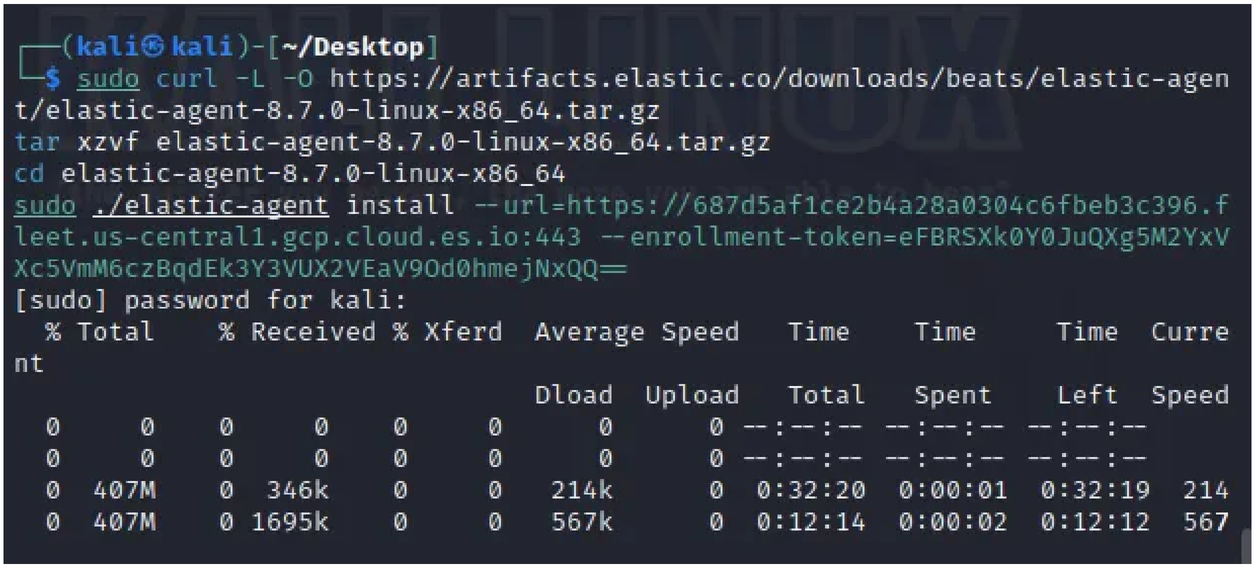
These steps configure and enroll the Elastic Agent in Fleet to automatically deploy updates and centrally manage the agent. As an alternative to Fleet, advanced users can run agents in standalone mode.

1 **Install Elastic Agent on your host**

Select the appropriate platform and run commands to install, enroll, and start Elastic Agent. Reuse commands to set up agents on more than one host. For aarch64, see our downloads page. For additional guidance, see our installation docs.

```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.7.0-li
tar xzvf elastic-agent-8.7.0-linux-x86_64.tar.gz
cd elastic-agent-8.7.0-linux-x86_64
sudo ./elastic-agent install --url=https://687d5af1ce2b4a28a0304c6fbeb3c396.fleet.us-central
```

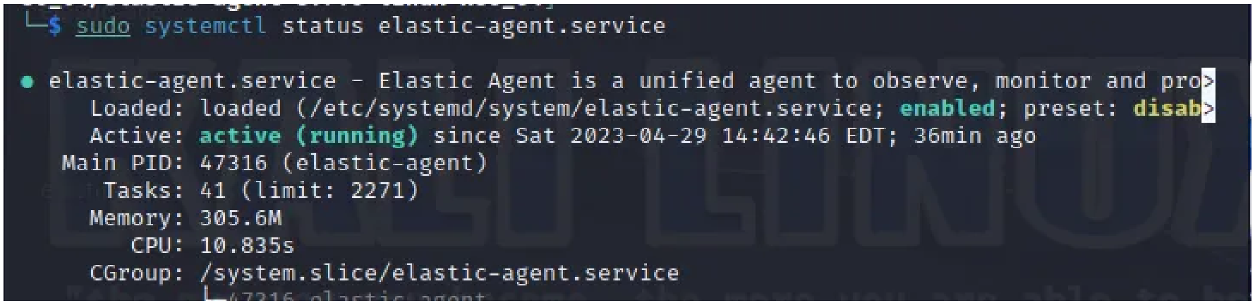
*Our Elastic Agent will be responsible for forwarding logs, telemetry data, and security-relevant information from endpoints to the Elastic Stack for centralized analysis and monitoring.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agen
t/elastic-agent-8.7.0-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.7.0-linux-x86_64.tar.gz
cd elastic-agent-8.7.0-linux-x86_64
sudo ./elastic-agent install --url=https://687d5af1ce2b4a28a0304c6fbeb3c396.f
leet.us-central1.gcp.cloud.es.io:443 --enrollment-token=eFBRSXk0Y0JuQXg5M2YxV
Xc5VmM6czBqdEk3Y3VUX2VEaV9Od0hmejNxQQ==
[sudo] password for kali:
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Curre
nt
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--
  0  407M    0  346k    0     0   214k      0  0:32:20  0:00:01  0:32:19  214
  0  407M    0 1695k    0     0   567k      0  0:12:14  0:00:02  0:12:12  567
```

Verify installation with:

```
sudo systemctl status elastic-agent.service
```



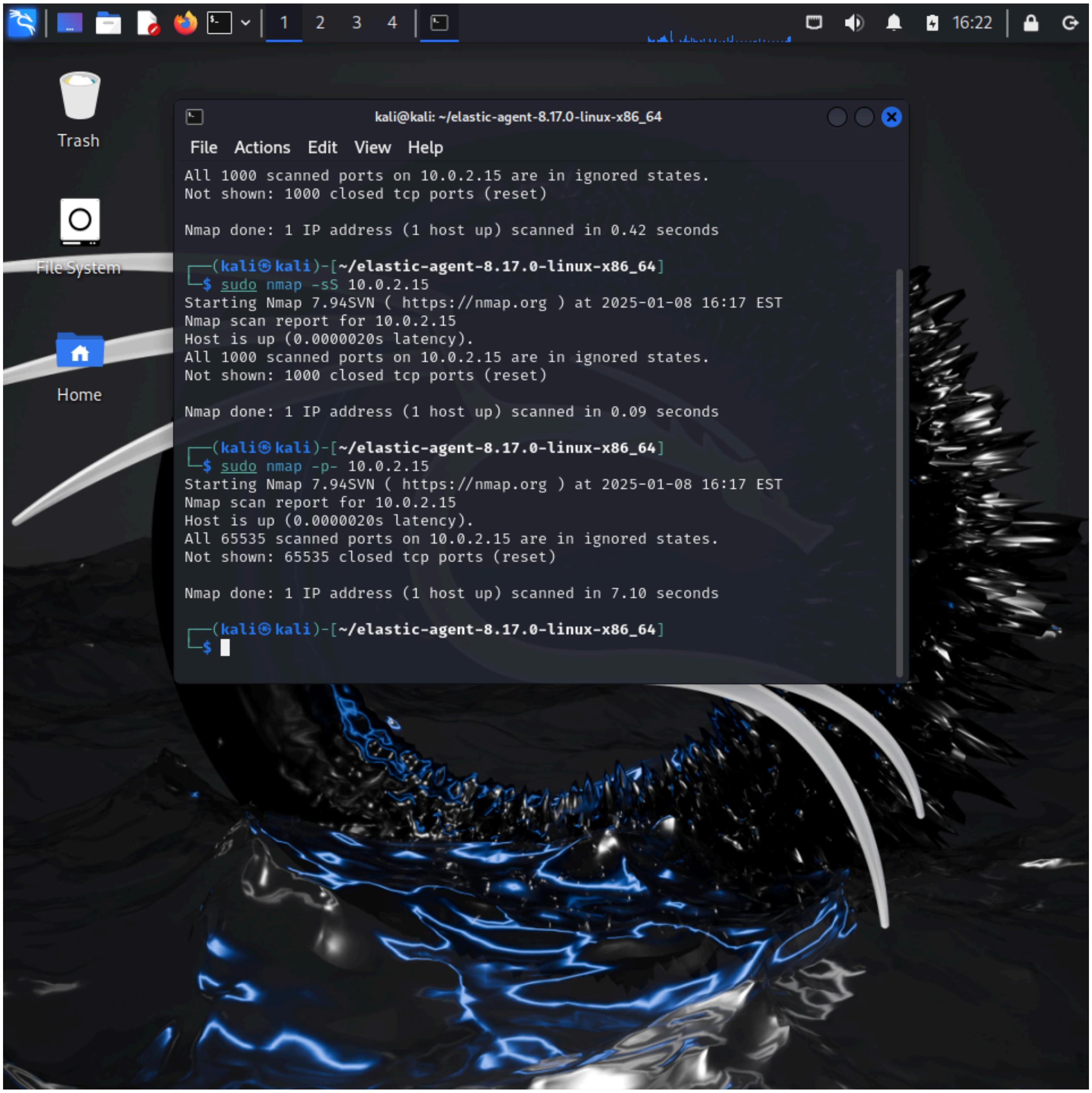
```
└─$ sudo systemctl status elastic-agent.service

● elastic-agent.service - Elastic Agent is a unified agent to observe, monitor and pro>
     Loaded: loaded (/etc/systemd/system/elastic-agent.service; enabled; preset: disab>
     Active: active (running) since Sat 2023-04-29 14:42:46 EDT; 36min ago
   Main PID: 47316 (elastic-agent)
      Tasks: 41 (limit: 2271)
     Memory: 305.6M
        CPU: 10.835s
     CGroup: /system.slice/elastic-agent.service
             └─47316 elastic-agent
```

Task 4: Generate Security Events on Kali Linux VM

1. Use **Nmap** (pre-installed on Kali) to simulate network scans:

Run commands like:

```
sudo nmap <target-ip>
sudo nmap -sS <target-ip>
sudo nmap -p- <target-ip>
```



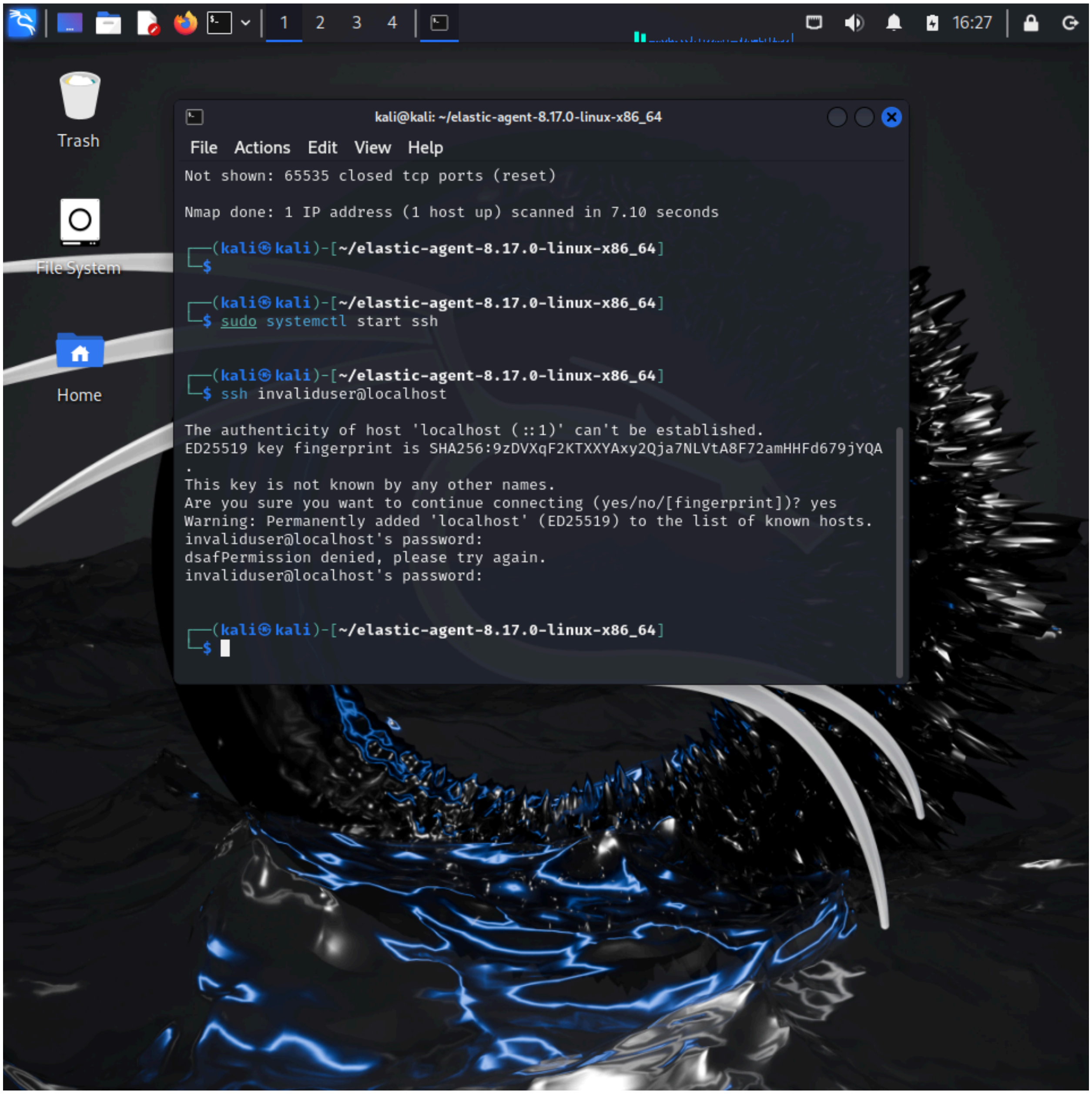
Trash
File System
Home
1
2
3
4
16:22
kali@kali: ~/elastic-agent-8.17.0-linux-x86_64
File Actions Edit View Help

```
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds

┌──(kali㉿kali)-[~/elastic-agent-8.17.0-linux-x86_64]
└─$ sudo nmap -sS 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 16:17 EST
Nmap scan report for 10.0.2.15
Host is up (0.0000020s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds

┌──(kali㉿kali)-[~/elastic-agent-8.17.0-linux-x86_64]
└─$ sudo nmap -p- 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 16:17 EST
Nmap scan report for 10.0.2.15
Host is up (0.0000020s latency).
All 65535 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 65535 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 7.10 seconds

┌──(kali㉿kali)-[~/elastic-agent-8.17.0-linux-x86_64]
└─$ 
```

Explanation of the Output

1. **"All 65535 scanned ports on 10.0.2.15 are in ignored states."**
   - Nmap found no open ports on the target IP during the scan.
   - The "ignored states" means the ports are either closed or filtered but not responding to Nmap's probes.
2. **"Not shown: 65535 closed tcp ports (reset)"**
   - The TCP ports responded with a **RST (reset)** packet, indicating they're closed

2. Generate additional events by attempting invalid SSH logins or other predefined activities.



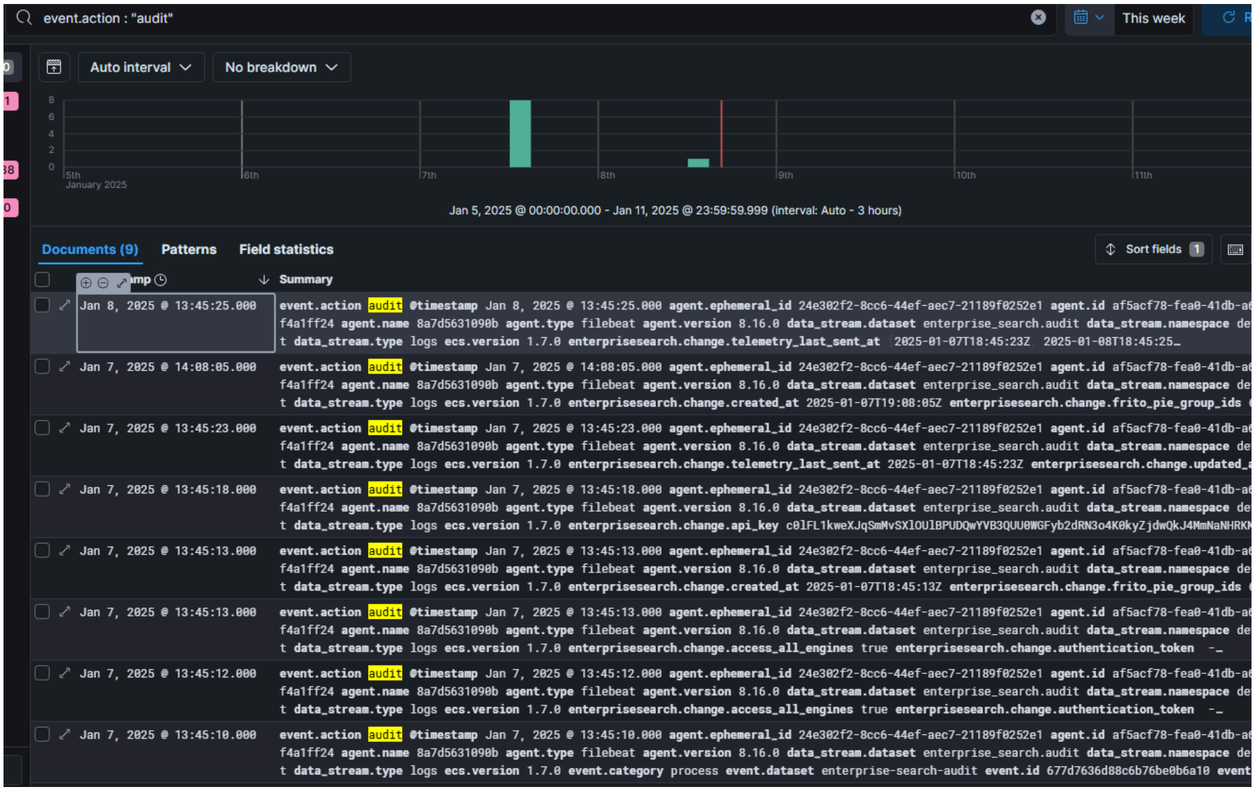
```
Not shown: 65535 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 7.10 seconds

┌──(kali㉿kali)-[~/elastic-agent-8.17.0-linux-x86_64]
└─$ 

┌──(kali㉿kali)-[~/elastic-agent-8.17.0-linux-x86_64]
└─$ sudo systemctl start ssh


┌──(kali㉿kali)-[~/elastic-agent-8.17.0-linux-x86_64]
└─$ ssh invaliduser@localhost

The authenticity of host 'localhost (::1)' can't be established.
ED25519 key fingerprint is SHA256:9zDVXqF2KTXXYAxy2Qja7NLVtA8F72amHHFd679jYQA
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
invaliduser@localhost's password:
dsafPermission denied, please try again.
invaliduser@localhost's password:


┌──(kali㉿kali)-[~/elastic-agent-8.17.0-linux-x86_64]
└─$ █
```

Task 5: Analyze Logs in Elastic SIEM

1. Open the Elastic console and go to **Observability > Logs**.

Query logs using filters such as:

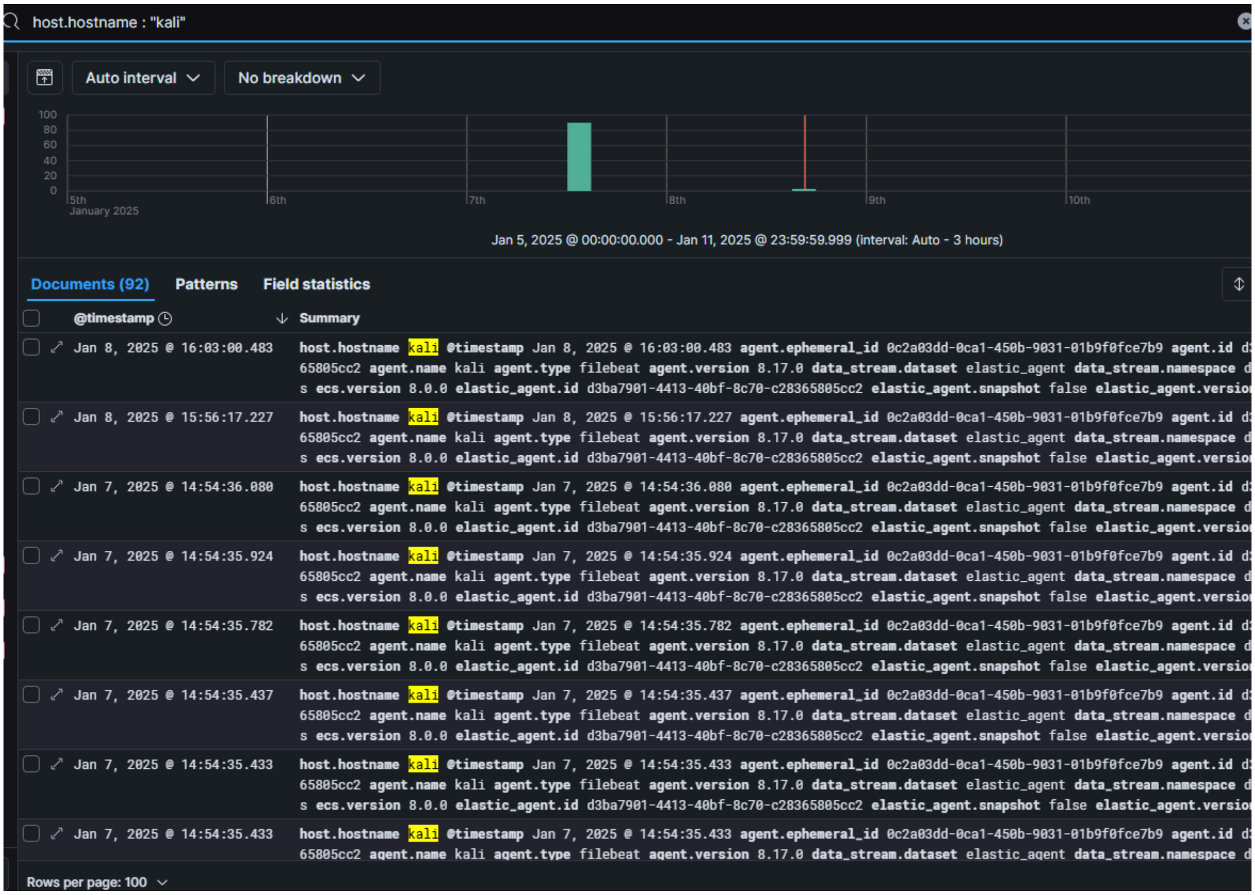
```
event.action: "audit"
```



Jan 5, 2025 @ 00:00:00.000 - Jan 11, 2025 @ 23:59:59.999 (interval: Auto - 3 hours)

```
Jan 8, 2025 @ 13:45:25.000   event.action audit @timestamp Jan 8, 2025 @ 13:45:25.000 agent.ephemeral_id 24e302f2-8cc6-44ef-aec7-21189f0252e1 agent.id af5acf78-fea0-41db-a6
                             f4a1ff24 agent.name 8a7d5631090b agent.type filebeat agent.version 8.16.0 data_stream.dataset enterprise_search.audit data_stream.namespace de
                             t data_stream.type logs ecs.version 1.7.0 enterprisesearch.change.telemetry_last_sent_at  2025-01-07T18:45:23Z  2025-01-08T18:45:25…
Jan 7, 2025 @ 14:08:05.000   event.action audit @timestamp Jan 7, 2025 @ 14:08:05.000 agent.ephemeral_id 24e302f2-8cc6-44ef-aec7-21189f0252e1 agent.id af5acf78-fea0-41db-a6
                             f4a1ff24 agent.name 8a7d5631090b agent.type filebeat agent.version 8.16.0 data_stream.dataset enterprise_search.audit data_stream.namespace de
                             t data_stream.type logs ecs.version 1.7.0 enterprisesearch.change.created_at 2025-01-07T19:08:05Z enterprisesearch.change.frito_pie_group_ids
Jan 7, 2025 @ 13:45:23.000   event.action audit @timestamp Jan 7, 2025 @ 13:45:23.000 agent.ephemeral_id 24e302f2-8cc6-44ef-aec7-21189f0252e1 agent.id af5acf78-fea0-41db-a6
                             f4a1ff24 agent.name 8a7d5631090b agent.type filebeat agent.version 8.16.0 data_stream.dataset enterprise_search.audit data_stream.namespace de
                             t data_stream.type logs ecs.version 1.7.0 enterprisesearch.change.telemetry_last_sent_at 2025-01-07T18:45:23Z enterprisesearch.change.updated_a
Jan 7, 2025 @ 13:45:18.000   event.action audit @timestamp Jan 7, 2025 @ 13:45:18.000 agent.ephemeral_id 24e302f2-8cc6-44ef-aec7-21189f0252e1 agent.id af5acf78-fea0-41db-a6
                             f4a1ff24 agent.name 8a7d5631090b agent.type filebeat agent.version 8.16.0 data_stream.dataset enterprise_search.audit data_stream.namespace de
                             t data_stream.type logs ecs.version 1.7.0 enterprisesearch.change.api_key c0lFL1kweXJqSmMvSXlOUlBPUDQwYVB3QUU0WGFyb2dRN3o4K0kyZjdwQkJ4MmNaNHRKM
Jan 7, 2025 @ 13:45:13.000   event.action audit @timestamp Jan 7, 2025 @ 13:45:13.000 agent.ephemeral_id 24e302f2-8cc6-44ef-aec7-21189f0252e1 agent.id af5acf78-fea0-41db-a6
                             f4a1ff24 agent.name 8a7d5631090b agent.type filebeat agent.version 8.16.0 data_stream.dataset enterprise_search.audit data_stream.namespace de
                             t data_stream.type logs ecs.version 1.7.0 enterprisesearch.change.created_at 2025-01-07T18:45:13Z enterprisesearch.change.frito_pie_group_ids
Jan 7, 2025 @ 13:45:13.000   event.action audit @timestamp Jan 7, 2025 @ 13:45:13.000 agent.ephemeral_id 24e302f2-8cc6-44ef-aec7-21189f0252e1 agent.id af5acf78-fea0-41db-a6
                             f4a1ff24 agent.name 8a7d5631090b agent.type filebeat agent.version 8.16.0 data_stream.dataset enterprise_search.audit data_stream.namespace de
                             t data_stream.type logs ecs.version 1.7.0 enterprisesearch.change.access_all_engines true enterprisesearch.change.authentication_token  -…
Jan 7, 2025 @ 13:45:12.000   event.action audit @timestamp Jan 7, 2025 @ 13:45:12.000 agent.ephemeral_id 24e302f2-8cc6-44ef-aec7-21189f0252e1 agent.id af5acf78-fea0-41db-a6
                             f4a1ff24 agent.name 8a7d5631090b agent.type filebeat agent.version 8.16.0 data_stream.dataset enterprise_search.audit data_stream.namespace de
                             t data_stream.type logs ecs.version 1.7.0 enterprisesearch.change.access_all_engines true enterprisesearch.change.authentication_token  -…
Jan 7, 2025 @ 13:45:10.000   event.action audit @timestamp Jan 7, 2025 @ 13:45:10.000 agent.ephemeral_id 24e302f2-8cc6-44ef-aec7-21189f0252e1 agent.id af5acf78-fea0-41db-a6
                             f4a1ff24 agent.name 8a7d5631090b agent.type filebeat agent.version 8.16.0 data_stream.dataset enterprise_search.audit data_stream.namespace de
                             t data_stream.type logs ecs.version 1.7.0 event.category process event.dataset enterprise-search-audit event.id 677d7636d88c6b76be0b6a10 event
```

```
host.hostname: "kali"
```



host.hostname : "kali"

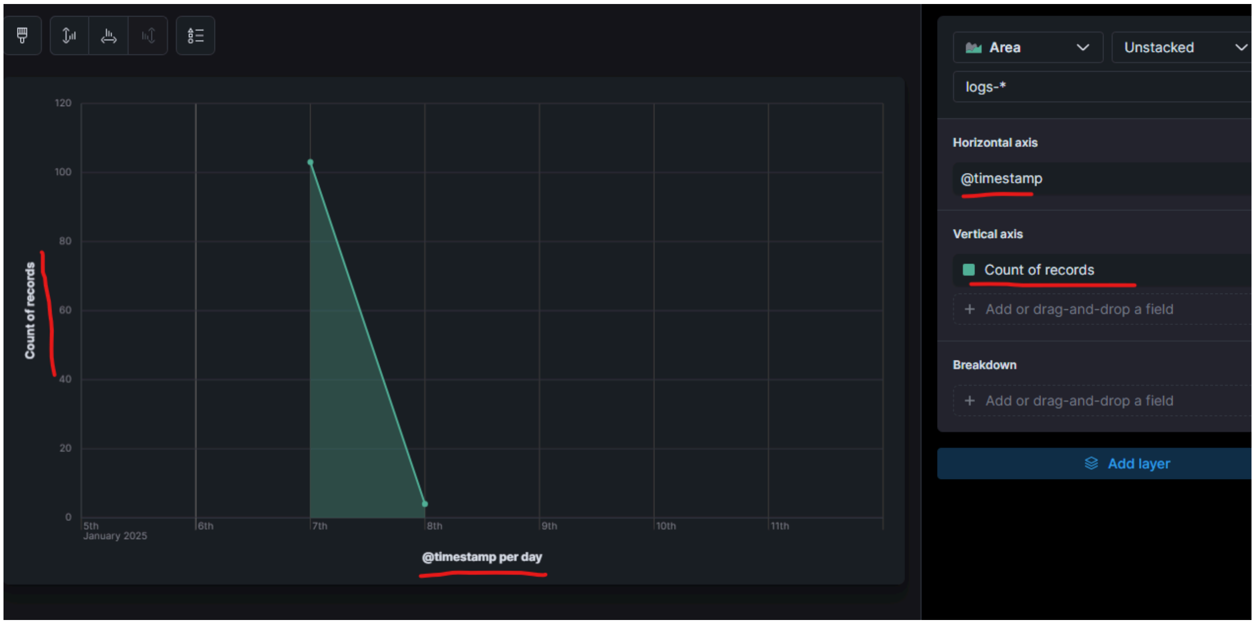
Jan 5, 2025 @ 00:00:00.000 - Jan 11, 2025 @ 23:59:59.999 (interval: Auto - 3 hours)

```
@timestamp                 Summary
Jan 8, 2025 @ 16:03:00.483 host.hostname kali @timestamp Jan 8, 2025 @ 16:03:00.483 agent.ephemeral_id 0c2a03dd-0ca1-450b-9031-01b9f0fce7b9 agent.id d
                           65805cc2 agent.name kali agent.type filebeat agent.version 8.17.0 data_stream.dataset elastic_agent data_stream.namespace d
                           s ecs.version 8.0.0 elastic_agent.id d3ba7901-4413-40bf-8c70-c28365805cc2 elastic_agent.snapshot false elastic_agent.versio
Jan 8, 2025 @ 15:56:17.227 host.hostname kali @timestamp Jan 8, 2025 @ 15:56:17.227 agent.ephemeral_id 0c2a03dd-0ca1-450b-9031-01b9f0fce7b9 agent.id d
                           65805cc2 agent.name kali agent.type filebeat agent.version 8.17.0 data_stream.dataset elastic_agent data_stream.namespace d
                           s ecs.version 8.0.0 elastic_agent.id d3ba7901-4413-40bf-8c70-c28365805cc2 elastic_agent.snapshot false elastic_agent.versio
Jan 7, 2025 @ 14:54:36.080 host.hostname kali @timestamp Jan 7, 2025 @ 14:54:36.080 agent.ephemeral_id 0c2a03dd-0ca1-450b-9031-01b9f0fce7b9 agent.id d
                           65805cc2 agent.name kali agent.type filebeat agent.version 8.17.0 data_stream.dataset elastic_agent data_stream.namespace d
                           s ecs.version 8.0.0 elastic_agent.id d3ba7901-4413-40bf-8c70-c28365805cc2 elastic_agent.snapshot false elastic_agent.versio
Jan 7, 2025 @ 14:54:35.924 host.hostname kali @timestamp Jan 7, 2025 @ 14:54:35.924 agent.ephemeral_id 0c2a03dd-0ca1-450b-9031-01b9f0fce7b9 agent.id d
                           65805cc2 agent.name kali agent.type filebeat agent.version 8.17.0 data_stream.dataset elastic_agent data_stream.namespace d
                           s ecs.version 8.0.0 elastic_agent.id d3ba7901-4413-40bf-8c70-c28365805cc2 elastic_agent.snapshot false elastic_agent.versio
Jan 7, 2025 @ 14:54:35.782 host.hostname kali @timestamp Jan 7, 2025 @ 14:54:35.782 agent.ephemeral_id 0c2a03dd-0ca1-450b-9031-01b9f0fce7b9 agent.id d
                           65805cc2 agent.name kali agent.type filebeat agent.version 8.17.0 data_stream.dataset elastic_agent data_stream.namespace d
                           s ecs.version 8.0.0 elastic_agent.id d3ba7901-4413-40bf-8c70-c28365805cc2 elastic_agent.snapshot false elastic_agent.versio
Jan 7, 2025 @ 14:54:35.437 host.hostname kali @timestamp Jan 7, 2025 @ 14:54:35.437 agent.ephemeral_id 0c2a03dd-0ca1-450b-9031-01b9f0fce7b9 agent.id d
                           65805cc2 agent.name kali agent.type filebeat agent.version 8.17.0 data_stream.dataset elastic_agent data_stream.namespace d
                           s ecs.version 8.0.0 elastic_agent.id d3ba7901-4413-40bf-8c70-c28365805cc2 elastic_agent.snapshot false elastic_agent.versio
Jan 7, 2025 @ 14:54:35.433 host.hostname kali @timestamp Jan 7, 2025 @ 14:54:35.433 agent.ephemeral_id 0c2a03dd-0ca1-450b-9031-01b9f0fce7b9 agent.id d
                           65805cc2 agent.name kali agent.type filebeat agent.version 8.17.0 data_stream.dataset elastic_agent data_stream.namespace d
                           s ecs.version 8.0.0 elastic_agent.id d3ba7901-4413-40bf-8c70-c28365805cc2 elastic_agent.snapshot false elastic_agent.versio
Jan 7, 2025 @ 14:54:35.433 host.hostname kali @timestamp Jan 7, 2025 @ 14:54:35.433 agent.ephemeral_id 0c2a03dd-0ca1-450b-9031-01b9f0fce7b9 agent.id d
                           65805cc2 agent.name kali agent.type filebeat agent.version 8.17.0 data_stream.dataset elastic_agent data_stream.namespace d
```

2. Explore and validate logs to confirm data ingestion.

Task 6: Creating a Visualization Dashboard of Findings

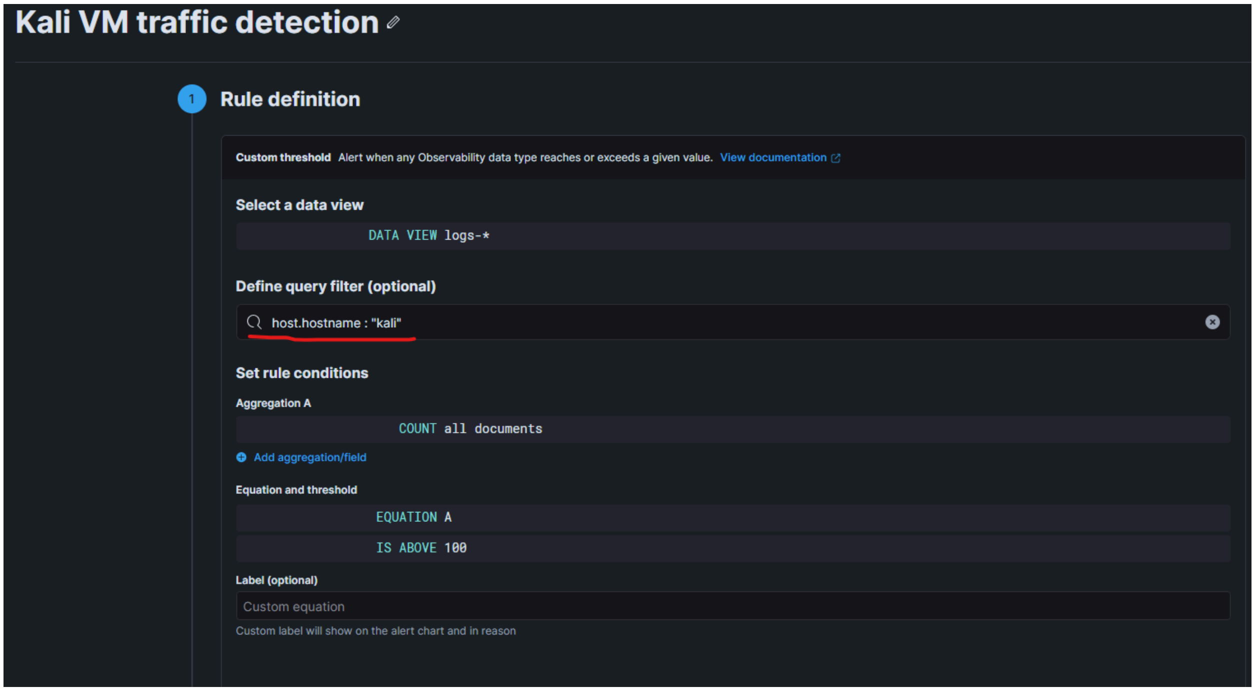
1. Navigate to **Analytics > Dashboards** in the Elastic console.
2. Click **Create Dashboard** and add visualizations:
    - Choose metrics like event counts over time.
    - Customize charts (e.g., line or bar graphs).
3. Save the dashboard for ongoing analysis.



This displays the count of security events recorded for the week. We can see events taking place on 1-7-25 and 1-8-25 with noticeably higher counts for 1-7-25.

Task 7: Configure Alerts

1. Go to **Security > Alerts > Manage Rules** and create a custom query-based rule to detect Nmap scans based on our findings: `Host.hostname: “kali”`



Kali VM traffic detection

1 Rule definition

Custom threshold Alert when any Observability data type reaches or exceeds a given value. View documentation

Select a data view

DATA VIEW logs-*

Define query filter (optional)

host.hostname : "kali"

Set rule conditions

Aggregation A

COUNT all documents

Add aggregation/field

Equation and threshold

EQUATION A

IS ABOVE 100

Label (optional)

Custom equation

Custom label will show on the alert chart and in reason

2. Define actions (e.g., email notifications) and enable the rule.

Future Uses of the Home Lab

1. **Incident Response**: Simulate attacks and analyze responses to refine detection strategies.
2. **Threat Hunting**: Expand capabilities by integrating more data sources and experimenting with threat intelligence feeds.
3. **Skill Development**: Practice advanced SIEM use cases, including anomaly detection and automated workflows.
4. **Certification Preparation**: Use the lab to prepare for cybersecurity certifications requiring SIEM expertise.

Conclusion

This Elastic SIEM home lab provides a robust platform for learning and practicing SIEM concepts. By integrating a Kali Linux VM with Elastic SIEM, we demonstrated log collection, security event analysis, dashboard creation, and alert setup. This hands-on experience is invaluable for building cybersecurity expertise and preparing for real-world scenarios. The lab's modular nature ensures it can be expanded and adapted to meet evolving learning needs.

References:

1. **Elastic Documentation**
   Elastic.co, “Elastic SIEM Guide,” https://www.elastic.co.
   (Used for understanding Elastic SIEM setup, integrations, and querying methods.)
2. **Kali Linux Official Website**
   Offensive Security, “Kali Linux Virtual Machines,” https://www.kali.org/get-kali.
   (Resource for downloading and configuring the Kali Linux virtual machine.)
3. **Nmap Documentation**
   Gordon Lyon, “Nmap Reference Guide,” https://nmap.org.
   (Provided guidance on generating security events with Nmap.)
4. **Oracle VirtualBox Documentation**
   Oracle, “VirtualBox User Manual,” https://www.virtualbox.org.
   (Utilized for setting up the virtualization environment.)
5. **Cybersecurity Training Resources**
   Various YouTube tutorials and cybersecurity forums for troubleshooting and additional insights into using Elastic Stack and configuring agents.
6. **Elastic Integrations Reference**
   Elastic.co, “Elastic Agent and Integrations Overview,” https://www.elastic.co/guide/en.
   (Helped in setting up the Elastic Agent to forward logs to Elastic SIEM.)