

A Simple Elastic SIEM Lab PROJECT REPORT

Report prepared by :

GAUTAM S

INDEX

- ❖ Set up a free Elastic account.
- ❖ Install the Kali VM.
- ❖ Configure the Elastic Agent on the Linux VM to collect the logs and forward it to the SIEM.
- ❖ Generate security events on the Kali VM.
- ❖ Query to find the security events in the Elastic SIEM.
- ❖ Create a Dashboard to visualize security events.
- ❖ Create alerts for security events.
- ❖ Conclusion

1. Set up an Elastic Account

Before we get started, we need to create a free account to set up a cloud Elastic instance that we can run the SIEM on. To do that, follow these steps:

1. Sign up for a free trial to use Elastic Cloud at <https://cloud.elastic.co/registration>
2. Once you have an Elastic account, log in to the Elastic Cloud console at <https://cloud.elastic.co>.
3. Click on “Start your free trial.”
4. Click on the “Create Deployment” button and select “Elasticsearch” as the deployment type.
5. Choose a region and deployment size that fits your needs and click on “Create Deployment.”
6. Wait for the configuration to complete.
7. Once the deployment is ready, click “continue.”

2.Setting up the Linux VM

Next, we need to set up the Linux VM. You can use any Linux OS and virtualization software for this, but I'll be using Kali Linux and Oracle VirtualBox.

To set it up, follow these steps:

1. Download the Kali Linux VM from the official Kali website at <https://www.kali.org/get-kali/#kali-virtual-machines>.
2. Create a new VM with the Kali VM file in your preferred virtualization platform, such as VirtualBox or VMware.
3. Start the VM and follow the on-screen prompts to install Kali.
4. Once the installation is complete, log in to the Kali VM using the credentials “kali” for both the username and password.

3.Setting up the Agent to Collect Logs

An agent is a software program that is installed on a device, such as a server or endpoint, to collect and send data to a centralized system for analysis and monitoring. In the context of Elastic SIEM, an agent is used to collect and forward security-related events from your endpoints to your Elastic SIEM instance.

To set up the agent to collect logs from your Kali VM and forward them to your Elastic SIEM instance, follow these steps:

- a. Log in to your Elastic SIEM instance and navigate to the Integrations page by: clicking on the Kibana main menu bar at the top left, then selecting “Integrations” at the bottom.
- b. Search for “Elastic Defend” and click on it to open the integration page.
- c. Click on “Install Elastic Defend” and follow the instructions provided on the integration page to install the agent on your Kali VM.
- d. Paste that command into the Kali terminal (command line).
- e. Once the agent is installed, which can take a few minutes, you’ll see a message that says “Elastic Agent has been successfully installed.” It will automatically start collecting and forwarding logs to your Elastic SIEM instance, although it might take a few minutes for the logs to appear in the SIEM.

```
(kali@kali)-[~/Desktop]
$ sudo curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/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.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=eFBR5Xk0Y0JuQXg5M2YxVXc5VmM6czBqdEk3Y3VUX2VEaV9Od0hmejNxQQ==
[sudo] password for kali:
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
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
```

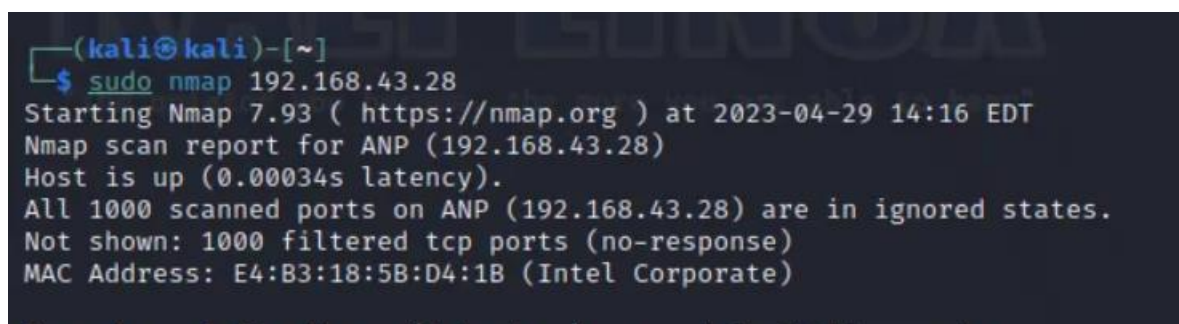
Fig : Kali linux interface

4. Generating Security Events on the Kali VM

To verify that the agent is working correctly, you can generate some security-related events on your Kali VM. To do this, we can use a tool like Nmap. Nmap (Network Mapper) is a free and open-source utility used for network exploration, management, and security auditing. It is designed to discover hosts and services on a computer network, thus creating a “map” of the network. Nmap can be used to scan hosts for open ports, determine the operating system and software running on the target system, and gather other information about the network.

To run an Nmap scan, follow these steps:

1. Install Nmap on the Linux VM if you’re not using Kali, Nmap already comes preinstalled in Kali. Open a new Terminal and run this command to install it: `sudo apt-get install nmap`.
2. Run a scan on Kali machine by running the command: `sudo nmap <vm-ip>`. You can also run a scan of your host machine if you place your Kali VM on a “bridged” network.
3. This scan generates several security events, such as the detection of open ports and the identification of services running on those ports. **Run a few more Nmap scans** (“`nmap -sS <ip address>`”, “`nmap -sT <ip address>`”, “`nmap -p- <ip address>`”etc..”



```
(kali@kali)-[~]
$ sudo nmap 192.168.43.28
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-29 14:16 EDT
Nmap scan report for ANP (192.168.43.28)
Host is up (0.00034s latency).
All 1000 scanned ports on ANP (192.168.43.28) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: E4:B3:18:5B:D4:1B (Intel Corporate)
```

Fig : An Nmap scan of my host machine.

5. Querying for Security Events in the Elastic SIEM

Now that we have forwarded data from the Kali VM to the SIEM, we can start querying and analyzing the logs in the SIEM.

To do this, follow these steps:

1. Inside your Elastic Deployment, click on the menu icon at the top-left with the three horizontal lines and then click on the “Logs” tab under “Observability” to view the logs from the Kali VM.
2. In the search bar, enter a search query to filter the logs. For example, to search for all logs related to Nmap scans, enter the query: `event.action: “nmap_scan”` or `process.args: “sudo”`.
3. Click on the “Search” button to execute the search query.
4. But please note that it can sometimes take a while for the events to populate and show up on the SIEM, so this query might not work right away.
5. The results of the search query will be displayed in the table below. You can click on the three dots next to each event to view more details.
6. By generating and analyzing different types of security events in Elastic SIEM like the one below, or generating authentication failures by typing in the wrong password for a user or attempting SSH logins an incorrect password, you can gain a better understanding of how security incidents are detected, investigated, and responded to in real-world environments.

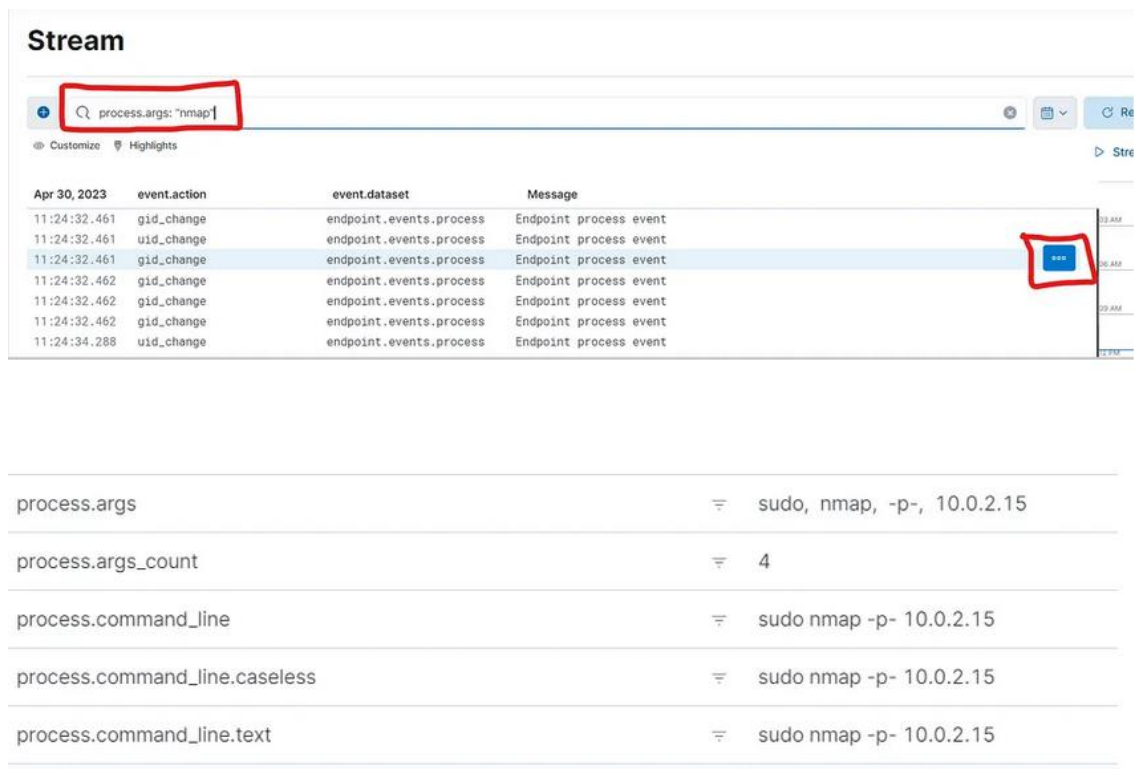


Fig : security events in Elastic SIEM

6. Create a Dashboard to Visualize the Events

You can also use the visualizations and dashboards in the SIEM app to analyze the logs and identify patterns or anomalies in the data. For example, you can create a simple dashboard that shows a count of security events over time.

Here's how you can do that:

1. Navigate to the Elastic web portal at <https://cloud.elastic.co/>.
2. Click on the menu icon on the top-left, then under “Analytics,” click on “Dashboards.”
3. Click on the “Create dashboard” button on the top right to create a new dashboard.

4. Click on the “Create Visualization” button to add a new visualization to the dashboard.
5. Select “Area” or “Line” as the visualization type, depending on your preference. This will create a chart that shows the count of events over time.
6. In the “Metrics” section of the visualization editor on the right, select “Count” as the vertical field type and “Timestamp” for the horizontal field. This will show the count of events over time.
7. Click on the “Save” button to save the visualization and then complete the rest of the settings.

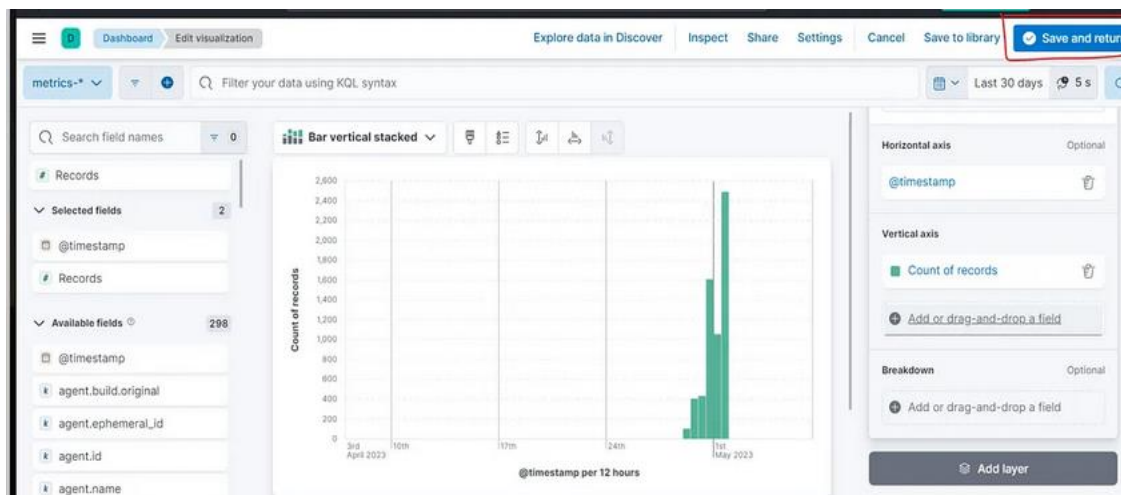


Fig : visualization of events

7. Create an Alert

In a SIEM, alerts are a crucial feature for detecting security incidents and responding to them in a timely manner. Alerts are created based on predefined rules or custom queries, and can be configured to trigger specific actions when certain conditions are met. In this task, we will walk through the steps of creating an alert in the Elastic SIEM instance to detect Nmap scans. By following these steps, you can create an alert that will monitor your logs for Nmap scan events and then notify you when they are detected.

Here are the steps:

1. Click on the menu icon on the top-left, then under “Security,” click on “Alerts.”
2. Click on “Manage rules” at the top right. Click on the “Create new rule” button at the top right.
3. Under the “Define rule” section, select the “Custom query” option from the dropdown menu.
4. Under “Custom query,” set the conditions for the rule. You can use the following query to detect Nmap scan events.



5. This query will match all events with the action “nmap_scan.” Then click “Continue.”

6. Under the “About rule” section, give your rule a name and a description (Nmap Scan Detection).
7. Set the severity level for the alert, which can help you prioritize alerts based on their importance. Keep all the other default settings under “Schedule rule” and click “Continue.”
8. In the “Actions” section, select the action you want to take when the rule is triggered. You can choose to send an email notification, create a Slack message, or trigger a custom webhook.
9. Finally, click the “Create and enable rule” button to create the alert.

Once you’ve created the alert, it will monitor your logs for Nmap scan events. If an Nmap scan event is detected, the alert will be triggered and the selected action will be taken. You can view and manage your alerts on the “Alerts” section under “Security.”

Conclusion

In this project, we have set up a home lab using Elastic SIEM and a Kali VM. We forwarded data from the Kali VM to the SIEM using the Elastic Beats agent, generated security events on the Kali VM using Nmap, and queried and analyzed the logs in the SIEM using the Elastic web interface. We also created a dashboard to visualize security events and then created an alert to detect security events.

This home lab provides a valuable environment for learning and practicing the skills necessary for effective security monitoring and incident response using Elastic SIEM. By following these steps, I gained hands-on experience with using a SIEM and has improved security monitoring skills which help me become a successful security analyst or SOC analyst.