Setting Up a Home Lab Using Elastic SIEM, Kali VM and Windows 10(home) OS

This project demonstrates how to set up a home security information and event management (SIEM) lab using Elastic SIEM with a Kali Linux VM, sending data from the Kali VM to Elastic SIEM, generating security events, and analysing the logs through dashboards and alerts.

**Step 1: Setting Up the Elastic SIEM Environment**

1. Install Elastic Stack:

* Begin by downloading and setting up Elastic Stack (Elasticsearch, Kibana, and Logstash) on your system. This will act as the SIEM platform where the data is ingested, stored, and analyzed.

2. Install Elastic Defend:

* Deploy the Elastic Defend, a component of Elastic Security, which provides advanced threat detection and response capabilities. This tool helps in identifying malicious behavior by correlating system logs and network traffic.

A screenshot of a computer

Description automatically generated

A screenshot of a phone

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

3. Install the Elastic Agent:

* Install the Elastic Agent on your Kali VM to forward logs to Elastic SIEM.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A white background with black text

Description automatically generated

4. Verify Agent Installation:

* After installation, verify that the Elastic Agent is running and sending data. You should see data start populating in Kibana’s “Security” tab.

**Step 2: Generating Security Events Using Kali Linux VM**

1. Install Kali Linux:

* Set up a Kali Linux virtual machine using your preferred virtualization tool (e.g., VirtualBox or VMware).
* Ensure that Kali Linux has network access to allow communication with the SIEM and for running network scans.

2. Run an Nmap Scan:

* Use Nmap on the Kali VM to generate security events. This can simulate potential reconnaissance activity on your network.
* Command: `nmap -sP <target-ip>`

This will create network events which will be forwarded to Elastic SIEM by the Elastic Agent.

A screenshot of a computer

Description automatically generated

3. Monitor Logs in Elastic SIEM:

* Navigate to the Elastic web interface and check the logs from the Kali VM. The logs should reflect the Nmap scan, showing network activity details like IP addresses and ports scanned.

A screenshot of a phone

Description automatically generated

**Step 3: Analyzing the Logs in Elastic SIEM**

1. Access the Logs:

* Go to the “Discover” tab in Kibana to search and filter through the logs. Use Elastic’s powerful query language to narrow down specific security events (such as the Nmap scan you ran).

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

2. Set Up a Dashboard:

* To better visualize the data, create a custom dashboard in Kibana. Add widgets that display different aspects of the security events, such as:
* IP addresses involved in the events
* Ports scanned
* Types of network traffic detected
* You can also use pre-built dashboards to quickly visualize key security metrics.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a graph

Description automatically generated

A screenshot of a computer

Description automatically generated

**Step 4: Creating an Alert for Security Events**

1. Create Security Rules:

* Using Kibana, create a custom security rule that triggers when a specific type of event (such as an Nmap scan) is detected.
* Example rule: If more than 5 Nmap scan attempts are detected within a short timeframe, trigger an alert.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

2. Configure Alert Notifications:

* Set up email notifications for the alert. Whenever the rule is triggered, you will receive an email with details about the suspicious activity.
* Example configuration: Select "Email" as the action for your rule, and configure your SMTP settings to receive alerts.

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

3. Test the Alert:

* Trigger the rule by running another Nmap scan from the Kali VM. Check your email for the alert notification and review the details of the event.

**Step 5: Summary of Results**

After setting up the SIEM, running the Nmap scan, and analysing the results in Elastic SIEM, you should have a dashboard that visualizes the key security events. Additionally, you will have created an automated alerting system that notifies you of specific suspicious activity, such as port scans from the Kali VM.

**Conclusion**

This project involved setting up a home lab using Elastic SIEM and a Kali VM to simulate real-world security monitoring. By forwarding data from the Kali VM using the Elastic Beats agent, we were able to generate and analyze security events such as Nmap scans. The Elastic web interface provided a platform to visualize the security events through dashboards, and we created alerts to monitor and respond to these events in real-time.

This hands-on lab is a great way to practice essential skills in security monitoring and incident response.