SIEM Home Lab Implementation

Overview

This project demonstrates setting up a home lab for Elastic Stack Security Information and Event Management (SIEM) using an Elastic Cloud instance and a Kali Linux VM. The lab focuses on log collection, security event generation, threat analysis, dashboard visualization, and alerting to detect and respond to security incidents.

Tools & Technologies Used

- **SIEM Platform:** Elastic Stack (Elasticsearch, Kibana, Elastic Agent)
- **Operating System:** Kali Linux VM
- **Security Tools:** Nmap (Network Scanning)
- **Log Forwarding Agent:** Elastic Agent
- **Virtualization Software:** VirtualBox / VMware

Project Implementation Steps

1 Setting Up Elastic SIEM

- Created a **free Elastic Cloud account** and deployed an **Elasticsearch** instance.
- Configured **Kibana** to interact with the SIEM system.

2 Setting Up Kali Linux VM

- Downloaded and installed **Kali Linux** on **VirtualBox/VMware**.
- Configured networking settings to allow communication with Elastic SIEM.

3 Configuring Elastic Agent for Log Collection

- Installed and configured **Elastic Agent** on Kali Linux to forward logs to the SIEM.
- Verified successful agent installation using:
  sudo systemctl status elastic-agent.service

4 Generating Security Events

Used **Nmap** to perform active network scanning and generate security-related logs:
sudo nmap -sS <target-ip>

- sudo nmap -p- <target-ip>
- Observed log entries in **Elastic SIEM** capturing Nmap scan activities.

5 Querying Security Events in Elastic SIEM

- Used **Kibana Logs Query** to search for Nmap-related security events:
  event.action: "nmap_scan" OR process.args: "sudo"
- Validated log ingestion and accuracy of collected data.

6 Creating a Security Dashboard

- Built a **custom Kibana dashboard** to visualize:
  - Failed login attempts
  - Detected Nmap scans
  - Security event trends over time
- Used **Area/Line charts** to track **security events dynamically**.

7 Implementing Security Alerts

- Configured **Elastic SIEM Alerts** to detect Nmap scans in real time.
- Created an automated **alert rule** to trigger email/SMS notifications when malicious activity is detected.
- Alerting Query Example:
  event.action: "nmap_scan"

Key Findings & Takeaways

- **Hands-on experience with Elastic SIEM** – Configured, collected, and analyzed security logs.
- **Real-time threat detection** – Successfully identified and responded to Nmap scans.
- **SIEM log analysis proficiency** – Used **Kibana queries** to analyze security events effectively.
- **Incident response skills** – Implemented alerts to detect and mitigate potential security threats.

Next Steps & Enhancements

- Experiment with **different log sources** (Windows event logs, Syslog, AWS logs).
- Expand lab setup with **additional attack simulations** (e.g., Brute-force attacks, Privilege Escalation).
- Integrate **Threat Intelligence feeds** into Elastic SIEM for **enhanced security monitoring**.