**Configuring a SIEM lab at home via Virtual Box and Elastic**

**Overview/ Purpose:**

The goal of this project was to generate an at-home cybersecurity laboratory where I could develop a deeper understanding of security information and event management (SIEM) tools, how security incidents are detected, investigated, and responded to in operational environments. Additionally, going through this project would enable me to conduct follow on cyber skills building exercises and gain hands-on experience.

**Skills Demonstrated:**

* *Elastic Stack SIEM Configuration and Management:*

Successfully set up and configured Elastic Stack SIEM in a home lab environment. Demonstrated proficiency in deploying a Kali Linux VM, configuring Elastic Agents for log collection, and forwarding data to the SIEM for effective security event monitoring.

* *Security Event Simulation and Analysis:*

Acquired hands-on experience in generating and analyzing security events using Nmap on Kali Linux. Proficient in querying Elastic SIEM to identify and investigate security incidents, enhancing skills in network security monitoring and threat detection.

* *Visualization and Alerting in SIEM:*

Developed a custom dashboard in Elastic SIEM to visualize security events, demonstrating skills in data interpretation and pattern recognition. Successfully created and tested alert rules for detecting specific security events, showing competency in proactive incident response and alert management.

**Tools used:**

Virtual Box Kali Linux Elastic Cloud Nmap

**Phase 1: Set up a cloud account and deployment where the SIEM can be run.**

The first step in setting up this type of home lab was to gain access to a cloud environment. For my limited needs, purposes, and resources, I chose to utilize a free trial cloud instance via cloud.elastic.co.

<A screenshot of a computer

Description automatically generated>

Once the account has been made the next step was to initiate a new deployment and then choose which configuration to integrate.

<A screenshot of a computer

Description automatically generated >

<A screenshot of a computer

Description automatically generated>

<A screenshot of a computer

Description automatically generated>

**Phase 2: Set up the Linux Virtual Machine (VM)**

* The second phase of the project consists of creating a Kali Linux VM. This VM will allow us to conduct security testing activities and generate data for you, the security professional, to collect and analyze via the cloud security agent. The process begins with downloading and installing the latest version of the appropriate VM software and Kali image. As I am familiar with Oracle’s Virtual Box software this is the route I chose. As a rule of thumb, remember to check/compare the hash values of your downloads to confirm their integrity.

<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>

With kali Linux added to Virtual box, I ran the machine and began configuring it, installing kali by following the on-screen prompts. For good measure, I also checked to see if the VM was able to connect to the internet.

<A screenshot of a computer

Description automatically generated>

**Phase 3: Configuring the cloud agent to collect logs.**

With the Kali VM operational, it was time to head back to the elastic cloud and begin configuring the agent to collect logs. Essentially, by the end of this phase, a reporting agent should be installed on the Kali VM which will push logs and other telemetry to the Elastic SIEM.

First, we click on the “Install elastic agent” button at the Elastic Defend Integration page.

<A screenshot of a computer

Description automatically generated>

Next, I copied the Linux command provided by Elastic and pasted it into my Kali terminal to install, enroll, and start the service agent on the VM.

<A screenshot of a computer

Description automatically generated>

<A screenshot of a computer

Description automatically generated>

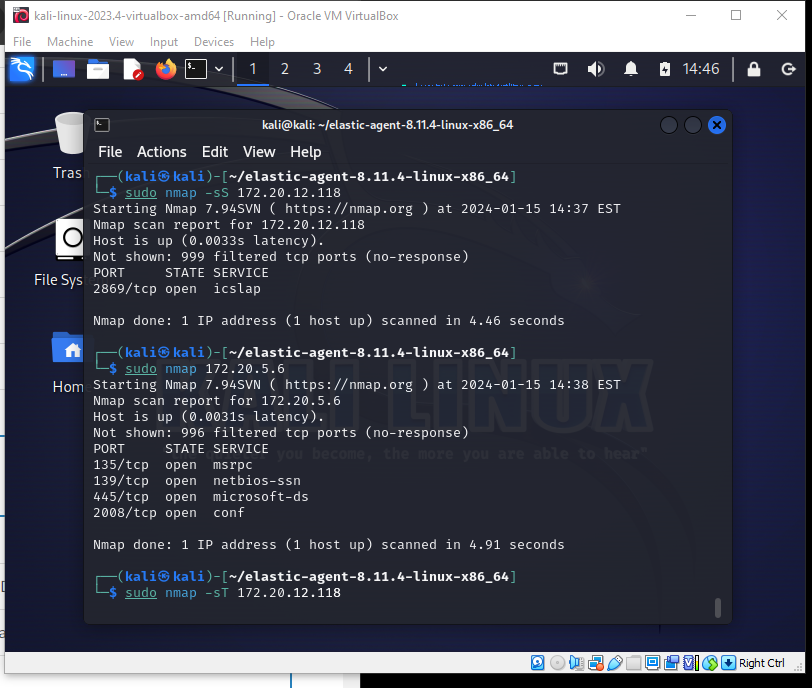
With the installation of the agent complete, I also ran a check command to verify that the elastic agent was in fact operational.

<A screenshot of a computer

Description automatically generated>

**Phase 4: Generating Security Events on my Kali VM**

With the elastic agent installed on the VM, it’s now time to generate some security related events. To do this, I used Nmap to simulate possible network reconnaissance activities such as port scanning and OS/service/host discovery. Target machines included items like my host system and other local network devices.

<>

<A screenshot of a computer

Description automatically generated>

**Phase 5: Querying the generated Security Events in the Elastic SIEM**

Now that data has been generated and forwarded from the Kali VM to the Elastic SIEM app, I re- accessed my Elastic deployment and navigated to the “logs” tab located under the “Observability drop down menu.

<A screenshot of a computer

Description automatically generated>

To query the events I generated previously, I entered process.args: “nmap”. By opening the details button to the right of the event in question, I was able to further simulate an investigation into what occurred on the VM and produce additional clues surrounding the activities which took place. For example, which nmap commands were executed by the potential offender.

<A screenshot of a computer

Description automatically generated>

<A screenshot of a computer

Description automatically generated>

**Phase 6: Creating a SIEM Dashboard to better visualize the Events.**

While event details expressed through text can be useful in discovering more intimate security-related semantics, data patterns and anomalies can often be better understood through visualization. Creating an easy-to-read display of data can help analysts more readily identify the relationships between events.

To begin visualizing my data, I navigated to the “Dashboard” tab located within the “Analytics” drop down menu.

<A screenshot of a computer

Description automatically generated>

Next, we can choose which visualization type suits our purposes. For this exercise I chose the “Area” visualization type.

<A screenshot of a computer

Description automatically generated>

Once you select the type of graph you want to create, the data source and axis are labeled appropriately according to the behavior that we want to analyze.

<A screenshot of a computer

Description automatically generated>

Here is the finished result. From the graph we can better visualize when the target VM experienced the spike in Nmap activity.

<A screenshot of a computer

Description automatically generated>

**Phase 7: Creating an Alert for the Elastic SIEM**

When utilizing a SIEM, event alerts are an essential feature for detecting potential security incidents and producing a timely, effective response. Within a system or network monitored by a SIEM, alerts are triggered when a set of predefined conditions are met. These conditions are outlined by the predetermined rules or queries set by security practitioners. Since I previously generated event activity using Nmap scans, I decided to explore the related alert rule generation process.

To begin making my alert rule I navigated to the “Alerts” tab, located under the Elastic “Security” menu, and selected “Manage rules”.

<A screenshot of a computer

Description automatically generated>

Next, I opened a new rule by clicking “Create New rule”. From the drop down menu, I selected “Define Rule” >>>”Custom Query”. Within the search bar I entered ‘event.action: “nmap\_scan” ‘ to query all the related events.

<A screenshot of a computer

Description automatically generated>

<A screenshot of a computer

Description automatically generated>

After setting the query flag for the Nmap actions to be reported, I assigned some descriptors to the rule which included severity, a brief description of the act, and a risk severity rating.

<A screenshot of a computer

Description automatically generated>

With the other elements of the alert rule finalized, I decided to have the SIEM alert me via email so that I could later test if the rule was effective. At this point, the frequency settings of the alert rule were also established.

<A screenshot of a computer

Description automatically generated>

**Phase 8: Testing the Rule**

With the new rule created and enabled, it was time to test. To test the alert system, I went back to the target virtual machine and conducted additional Nmap iterations. A few moments later my email account received an alert that another suspicious Nmap event had occurred, and the project was complete.

<A screenshot of a computer

Description automatically generated>

<A screenshot of a computer

Description automatically generated>