LAB4 SIEM

This lab is designed to introduce students to security solutions, specifically a SIEM. In this lab, students can use any SIEM of choice; regardless, a solid recommendation is to use the open source security platform Wazuh as this provides a fleet of capabilities at no cost.

In this lab, students will interact with additional tools such as virustotal, YARA, osquery, SOAR and also gain experience with SIEM log analysis, vulnerability detection and more.

Part A

Task 1 - Introduction

a. Give a brief explanation of the architecture of your SIEM solution.

b. Provide 3 advantages of open source solutions and how do these vendors actually make money?

Task 2 - Setup infrastructure

a. Configure a SIEM solution with 3(or more) unique devices. e.g Windows, Linux and a Network device. Can you view log data from each connected device? If yes show this.

b. Why specifically are you able to view these logs i.e select two visible logs, explain these logs, and explain why and how you are able to view it on the SIEM.

Task 3 - Use cases <select any 2>

a. Demonstrate how to block malicious IP addresses from accessing web resources on a web server. To do this ,you will set up your web servers on select endpoints within your infrastructure, and try to access them from an external endpoint.

b. Simulate a brute force attack against your infrastructure and demonstrate how you would detect the attack on each of the devices within your infrastructure. Are you able to detect the attack? If not, ensure you are able to.

c. Demonstrate how you would use the SIEM to detect existing CVEs within devices in your infrastructure. i.e vulnerability detection. Ensure you remediate at least 1 vulnerability on each device and prove this in an updated scan.

Part B

Select 1 task only between task 4 and 5

Task 4 - SIEM integration <select any 1>

1. Get a sample of the Sysjoker malware and infect any single chosen endpoint. Utilize Osquery with your SIEM in other to detect this malware.
2. Get a sample of the whispergate malware. Utilize YARA or Virustotal with your SIEM in other to detect and remove this malware. Here, there will be no need to run the malware on the endpoint before you can detect and mitigate it.

NOTE1: A sample incident alert should be sent to the owner(you) of the attacked endpoint when these alerts are detected for every use case.

NOTE2:**Please be careful when you run them, THESE ARE REAL MALWARE.**

Task 5 - SOC integrations <select any 1>

a. Integrate the SIEM with a case management system of your choice? e.g theHive. Show that you are able to automatically open cases from SIEM alerts.

b. Integrate the SIEM with a SOAR solution of your choice? e.g. shuffle.

c. Integrate the SIEM with a WAF and simulate a scenario to test the integration. e.g use of Modsecurity.

Bonus

- Automate your sample incident alert sent in the use cases section using any platform of choice.
- Design an incident response playbook for ransomware attacks.