MODULE 05 Enhanced Incident Detection with Threat Intelligence

LAB SCREENSHOTS

Lara Alofi

Lab Session Identifiers

1. https://eccouncil.learnondemand.net/Lab/Launch/30851?AssignmentId=1340520&lang=
2. https://eccouncil.learnondemand.net/Lab/Launch/30851?AssignmentId=1340520&lang=
3.

Username on EC-Council System

1. 2110886@uj.edu.sa

Lab 01: Incorporating IoCs into ELK Stack

Accessing SIEM1 Machine:

Initiate the SIEM1 virtual machine. Utilize the default login credentials (Administrator account: Pa$$w0rd). Copying ELK Folder:

Navigate to E:\SOC-Tools\Module 05 Enhanced Incident Detection with Threat Intelligence. Duplicate the ELK folder. Pasting and Extracting Files:

Paste the ELK folder copy into the C: drive. Right-click and extract all the zip files within C:\ELK. Installing NSSM:

Go to E:\SOC-Tools\Module 05 Enhanced Incident Detection with Threat Intelligence\NSSM. Copy the nssm-2.24 folder. Paste it within C:\ELK. Deploying Elasticsearch Service:

Open PowerShell as Administrator. Execute the command to install the Elasticsearch service. Initiate the service and configure it for Automatic startup. Configuring Elasticsearch:

Modify the elasticsearch.yml file to set up the network settings. Validate the Elasticsearch configuration by accessing http://localhost:9200/. Creating Logstash Pipeline Configuration:

Open PowerShell and generate a new logstashpipeline.conf file. Include the input and output configurations. Installing Logstash Service:

Utilize NSSM to install the Logstash service. Configure the necessary parameters for the service. Deploying Kibana Service:

Use NSSM to install the Kibana service. Configure the essential parameters for the service. Configuring Kibana:

Edit the kibana.yml file to set up the server host. Starting Logstash, Elasticsearch, and Kibana Services:

Commence the Logstash, Elasticsearch, and Kibana services from the Services window. Installing and Configuring Winlogbeat on WinServer2012:

Copy the Beats folder to the C: drive. Extract the contents of winlogbeat-6.5.4-windows-x86_64.zip. Edit the winlogbeat.yml file to configure Elasticsearch and Kibana hosts. Install and commence the Winlogbeat service. Loading Index Template and Configuring Kibana Dashboard:

Manually load the index template. Configure the Kibana dashboard using the provided command. Configuring Logstash to Include Malware Filter:

Copy the malware.yml file to the Logstash directory. Edit logstashpipeline.conf to include the malware filter. Restarting Logstash Service:

Restart the Logstash service from the Services window. Verifying Setup in Kibana:

Access Kibana via the web browser. Create an index pattern for Winlogbeat. Check for Winlogbeat-associated logs and search for IoCs. Executing Malicious Activity on WinServer2012:

Copy the wikiworm folder to the C: drive on WinServer2012. Execute the wikiworm.exe file. Refresh Kibana to view the event log indicating the execution of wikiworm and the detection of malware. What I learned:

Integrating malware IoCs into the ELK stack.

Installing and configuring Elasticsearch, Logstash, Kibana, and Winlogbeat.

Configuring Logstash filters to identify malicious activities.

Validating the setup by accessing Kibana and searching for IoCs.

Lab2: Incorporating OTX Threat Data in OSSIM

Accessing SIEM2 Virtual Machine:

Launch the SIEM2 virtual machine. Enter the default credentials (Administrator account: Pa$$w0rd). Signing Up for AlienVault OTX:

Open Chrome browser and navigate to https://otx.alienvault.com. Fill in the required details in the SIGN UP form and click on SIGN UP to register for the AlienVault OTX website. Activate your account using the activation email sent to your provided email address. After successful activation, log in to your AlienVault OTX account. Copy the OTX Key from the Settings page of your OTX account and close the browser. Accessing OSSIM Server:

Launch the OSSIM Server virtual machine. Enter root as the username and toor as the password. Configuring OSSIM for AlienVault OTX:

Access the AlienVault Setup screen. Switch back to the SIEM2 virtual machine. Open a browser and navigate to https://192.168.1.55. Click on Proceed to 192.168.1.55 (unsafe) link. Enter the required information on the Administrator Account Creation page and click START USING ALIENVAULT. Log in with the provided credentials. If a HELP US IMPROVE ALIENVAULT OSSIM popup appears, click CANCEL. Skip the AlienVault Wizard on the Welcome to the AlienVault OSSIM Getting Started Wizard page. Configuring OTX Integration in OSSIM:

Navigate to CONFIGURATION --> OPEN THREAT EXCHANGE menu. Paste the copied OTX Key into the OTX Key text box and click on CONNECT OTX ACCOUNT. Wait for OSSIM to connect to the OTX account and start downloading the OTX pulses. Refreshing the page will display the subscribed pulses being downloaded. OSSIM will now automatically detect and notify network activities against the subscribed OTX pulses. Concluding the Exercise:

Close all open windows to conclude the exercise.

What I learned:

- How to sign up for and activate an AlienVault OTX account.
- How to integrate OTX pulses into OSSIM to consume threat intelligence feed.
- How to configure OSSIM to connect to the OTX account and download pulses for threat detection.