MODULE 05 Enhanced Incident Detection with Threat Intelligence LAB REPORT

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=

Username on EC-Council System

1. 2110886@uj.edu.sa

Lab 01: Incorporating IoCs into ELK Stack

Access the SIEM1 machine: Start the SIEM1 virtual machine.

1. Use the default login credentials (admin account: Pa$$w0rd).
2. Duplication of ELK organizer: Check E:\SOC-Tools\Module 05
3. Updated location with threat information.
4. Copy the ELK shell. Paste and extract records: Paste a copy of the ELK envelope to the C: drive.
5. Right-click and center all packages into the C:\ELK folder.
6. Introducing NSSM: Go to E:\SOC-Tools\Module 05 Advanced Episode Detection with Threat Information\NSSM.
7. Copy shell nssm-2.24. Paste it in C:\ELK.
8. To deploy Elasticsearch Management: Open PowerShell as administrator.
9. Run the command to enable Elasticsearch management.
10. Run the tool and schedule it to run on a schedule.
11. Elasticsearch Design: Configure the elasticsearch.yml document to configure the organization settings. Accept the Elasticsearch configuration by going to http://localhost:9200/.
12. To configure the Logstash pipeline: Open PowerShell and create a new logstashpipeline.conf entry. Include information and output options.
13. Introducing Logstash management: Use NSSM to introduce Logstash management.
14. Plan important limits of help.
15. Deploy Kibana Administration: Deploy Kibana Administration with NSSM.
16. Arrange the main boundaries of the aid.
17. Configuring Kibana: Edit the kibana.yml entry to configure the server.
18. Starting Logstash, Elasticsearch, and Kibana Administration: Start Logstash, Elasticsearch, and Kibana Administration in the Administration window.
19. Winlogbeat Introduction and Design in WinServer2012: Copy the Beats Organizer to C:. Extract items from winlogbeat-6.5.4-windows-x86_64.zip.
20. Configure Elasticsearch and Kibana by editing the winlogbeat.yml file.
21. Introduce and run Winlogbeat management.
22. Record layout stacking and Kibana dashboard organization: Physically download the record layout. Organize your Kibana dashboard in a predetermined order.
23. To configure Logstash to include the malware channel: Copy the malware.yml document to the Logstash directory. Edit the logstashpipeline.conf file to include the malware pipeline.
24. Restart Logstash Manager: Restart Logstash Manager from the Administrator window.
25. Confirming your Kibana subscription: You can access Kibana through an Internet browser.
26. Make a disk image for Winlogbeat.
27. Check logs related to Winlogbeat and search for IoCs.
28. How to run Vindictive Movement on WinServer2012: Copy the wikiworm envelope to WinServer2012's C: drive.
29. Run the wikiworm.exe entry.
30. Restart Kibana to see the event log showing the wikiworm running and malware detection.

What I noticed:

- incorporating Malware IoCs into the ELK Stack.

- Introduction and compatibility of Elasticsearch, Logstash, Kibana and Winlogbeat.
- Designing Logstash channels to isolate malicious practices.
- Accepting the agreement by entering Kibana and searching for IoCs.

Lab2: Incorporating OTX Threat Data in OSSIM

1. Access SIEM2 VM: Introduce the SIEM2 VM.
2. Enter default reviews (chairman account: Pa$$w0rd).
3. To run AlienVault OTX: Open Chrome and go to https://otx.alienvault.com.
4. Use the necessary subtleties of the closing structure and click Join to join the AlienVault OTX website.
5. Activate your list using the initial email sent from the email address you provided.
6. Once you have activated it, log in to your AlienVault OTX account.
7. Copy the OTX key from the settings page to your OTX entry and close the program.
8. Access the OSSIM server: Bring up the OSSIM server virtual machine.
9. Enter root as username and raw as password.
10. OSSIM Arrangement for AlienVault OTX: Open the AlienVault Arrangement screen.
11. Go back to the SIEM2 VM. Open the program and examine the address https://192.168.1.55.
12. Click Continue to connect to 192.168.1.55 (dangerous).
13. Enter the expected information on the Administrative Record Creation page and click Start Using ALIENVAULT.
14. Log in with the provided credentials.
15. When the Help US Developing ALIENVAULT OSSIM pop-up appears, click Drop.
16. Avoid the AlienVault wizard on the Welcome to AlienVault OSSIM Getting Started page.
17. To organize an OTX combination in OSSIM: Explore to Design -> Open the Dangerous Business menu. Paste the copied OTX key into the OTX Key text box and tap Interface OTX Storage.
18. Trust OSSIM to connect the OTX record and start loading the OTX bits.
19. The refresh page shows the download of the purchased beats.
20. Currently, OSSIM extracts and reports OTX tats purchased from online exercises.
21. Close a task: Close all open windows to complete a task.

What I noticed:

- The most efficient way to find and launch an AlienVault OTX account.
- Step-by-step instructions for adding OTX bits to input threat information into the OSSIM system.
- Instructions for configuring OSSIM to connect to an OTX account and load threat location bit.