MODULE 04 Incident Detection with Security Information and Event Management (SIEM) LAB SCREENSHOTS

Lara Alofi

Lab Session Identifiers

1. https://labclient.labondemand.com/LabClient/3aada99f-e14a-4100-88e7-d3773ed4557d
2. https://labclient.labondemand.com/LabClient/b3ba8a36-5153-495f-86da-c73a8bebf717
3. https://labclient.labondemand.com/LabClient/b26e6e1e-5a9d-48dd-b546-747f534910f6
4.

Username on EC-Council System

1. 2110886@uj.edu.sa

Lab 01

Lab Tasks:

1. **Login to WinServer2012 and SIEM1 Machines:**
    - Access the WinServer2012 and SIEM1 machines using provided credentials.
2. **Access Splunk Interface:**
    - Open Google Chrome and navigate to the Splunk sign-in page. Log in with provided credentials.
3. **Configure Search Query:**
    - Use Splunk's Search console to create a query detecting failed login attempts exceeding five times.
4. **Create Alert:**
    - Save the search query as an alert titled "Failed Login Attempts" indicating detection of more than five failed login attempts.
5. **Set Alert Parameters:**
    - Configure alert parameters such as permissions, type, throttle, and severity.
6. **Perform Brute-Force Attack:**
    - Launch a brute-force attack on the target server using Hydra in Kali Linux.
7. **Test the Alert:**
    - Attempt to log in to the target server using cracked credentials.
    - Monitor triggered alerts in Splunk to verify detection of the brute-force attempt.
8. **Review Results:**
    - View results of triggered alert in Splunk to confirm detection of the brute-force attempt.

Key Learnings:

- Understanding the importance of monitoring and detecting brute-force attempts on host systems.
- Utilizing Splunk SIEM to create use cases and alerts for detecting security incidents.
- Configuring search queries and alert parameters to detect specific security events.
- Testing effectiveness of detection mechanism through simulated attacks and alert triggering.
- Analyzing and investigating triggered alerts to confirm security incidents and escalate them accordingly.

Lab 02

Lab Tasks:

1. **Login to WinServer2012 and SIEM1 Machines:**
    - Access the WinServer2012 and SIEM1 machines using provided credentials.
2. **Access Splunk Interface:**
    - Open Google Chrome and navigate to the Splunk sign-in page. Log in with provided credentials.
3. **Configure Search Query:**
    - Use Splunk's Search console to create a query detecting SQL injection attempts in IIS logs on WinServer2012.
4. **Create Alert:**
    - Save the search query as an alert titled "SQL Injection Alert" indicating detection of SQL injection attempts.

5. **Set Alert Parameters:**
    - Configure alert parameters such as permissions, type, throttle, and severity.
6. **Perform SQL Injection Attack:**
    - Launch a SQL injection attack on the LuxuryTreats website using Kali Linux to simulate an attacker's actions.
7. **Test the Alert:**
    - Attempt a SQL injection attack on the LuxuryTreats website and observe if the alert is triggered in Splunk.
8. **Review Alert Details:**
    - View results of triggered alert in Splunk to confirm detection of the SQL injection attempt.
9. **Disable the Alert:**
    - Navigate to Splunk settings and disable the SQL Injection Alert to stop monitoring for such incidents.

Key Learnings:

- Understanding the importance of monitoring and detecting SQL injection attempts at the application level.
- Utilizing Splunk SIEM to create use cases and alerts for detecting security incidents related to SQL injection attacks.
- Configuring search queries and alert parameters to detect specific patterns or signatures indicative of SQL injection attempts.
- Simulating SQL injection attacks to test the effectiveness of the detection mechanism and alert triggering.
- Disabling alerts when they are no longer needed or relevant for ongoing monitoring.

Lab 03

Lab Tasks:

1. **Login to WinServer2012 and SIEM1 Machines:**
    - Access the WinServer2012 and SIEM1 machines using provided credentials.
2. **Access Splunk Interface:**
    - Open Google Chrome and navigate to the Splunk sign-in page. Log in with provided credentials.
3. **Configure Search Query:**
    - Use Splunk's Search console to create a query detecting XSS attempts in IIS logs on WinServer2012.
4. **Create Alert:**
    - Save the search query as an alert titled "XSS Attack Alert" indicating detection of XSS attempts.
5. **Set Alert Parameters:**
    - Configure alert parameters such as permissions, type, throttle, and severity.
6. **Perform XSS Attack:**
    - Launch an XSS attack on the LuxuryTreats website using Kali Linux to simulate an attacker's actions.
7. **Test the Alert:**

- Attempt an XSS attack on the LuxuryTreats website and observe if the alert is triggered in Splunk.

8. **Review Alert Details:**
    - View results of triggered alert in Splunk to confirm detection of the XSS attack attempt.
9. **Disable the Alert:**
    - Navigate to Splunk settings and disable the XSS Attack Alert to stop monitoring for such incidents.

Key Learnings:

- Understanding the importance of monitoring and detecting XSS attempts at the application level.
- Utilizing Splunk SIEM to create use cases and alerts for detecting security incidents related to XSS attacks.
- Configuring search queries and alert parameters to detect specific patterns or signatures indicative of XSS attack attempts.
- Simulating XSS attacks to test the effectiveness of the detection mechanism and alert triggering.
- Disabling alerts when they are no longer needed or relevant for ongoing monitoring.

Lab 04

Lab Tasks:

1. **Login to WinServer2012 and SIEM1 Machines:**
    - Access the WinServer2012 and SIEM1 machines using provided credentials.
2. **Access Splunk Interface:**
    - Open Google Chrome and navigate to the Splunk sign-in page. Log in with provided credentials.
3. **Configure Search Query for TCP Scan:**
    - Use Splunk's Search console to create a query detecting TCP scan attempts in Snort IDS logs on WinServer2012.
4. **Create Alert for TCP Scan:**
    - Save the search query as an alert titled "TCP Scan Alert" indicating detection of TCP scan attempts.
5. **Set Alert Parameters for TCP Scan:**
    - Configure alert parameters such as permissions, type, throttle, and severity.
6. **Configure Search Query for Xmas Scan:**
    - Create a new search query to detect Xmas scan attempts in Snort IDS logs.
7. **Create Alert for Xmas Scan:**
    - Save the search query as an alert titled "XMAS Scan Alert" indicating detection of Xmas scan attempts.
8. **Set Alert Parameters for Xmas Scan:**
    - Configure alert parameters including permissions, throttle, and severity.
9. **Configure Search Query for FIN Scan:**
    - Create a new search query to detect FIN scan attempts in Snort IDS logs.
10. **Create Alert for FIN Scan:**
    - Save the search query as an alert titled "FIN Scan Alert" indicating detection of FIN scan attempts.
11. **Set Alert Parameters for FIN Scan:**

- Configure alert parameters such as permissions, throttle, and severity.

12. **Start Snort on WinServer2012:**
    - Open Command Prompt on WinServer2012 and initiate Snort with appropriate parameters.
13. **Simulate Network Scanning from Kali Linux:**
    - Use Kali Linux to perform various network scans such as SYN, TCP Full connect, TCP Null, Xmas, and FIN on the target machine.
14. **Check for Triggered Alerts:**
    - Navigate to Splunk's Activity section and view triggered alerts for TCP Scan, Xmas Scan, and FIN Scan.
15. **Disable Alerts:**
    - Access Splunk settings to disable TCP Scan, Xmas Scan, and FIN Scan alerts when they are no longer needed.

Key Learnings:

- Understanding the use of Snort IDS logs to detect network scanning attempts.
- Configuring Splunk SIEM to create use cases and alerts for detecting different types of network scans.
- Setting up search queries and alert parameters to identify specific patterns indicative of network scanning activity.
- Conducting network scans using tools like Nmap from Kali Linux to simulate attacker behavior.
- Monitoring and analyzing triggered alerts to confirm and escalate potential security incidents.
- Disabling alerts when they are no longer required for ongoing monitoring.

Lab 05

Lab Tasks:

1. **Access WinServer2012:**
    - Log in to the WinServer2012 machine using provided credentials.
2. **Create Script to Monitor Ports:**
    - Create a batch script named "watch.bat" containing the command "Netstat -ano" and save it in the Splunk Universal Forwarder's script directory.
3. **Configure Inputs for Splunk Forwarder:**
    - Edit the "inputs.conf" file in the Splunk Universal Forwarder's configuration directory to include the script as an input source.
4. **Restart SplunkForwarder Service:**
    - Restart the SplunkForwarder service to apply the new configuration.
5. **Access SIEM1 Machine:**
    - Log in to the SIEM1 machine using provided credentials.
6. **Access Splunk Interface:**
    - Open Google Chrome and navigate to the Splunk sign-in page. Log in with provided credentials.
7. **Run Search Query for Telnet Port:**
    - Use Splunk's Search console to execute a query detecting open Telnet ports based on Netstat data.
8. **Create Alert for Telnet Port:**

- Save the search query as an alert titled "The Telnet port has been found opened" indicating detection of open Telnet ports.

9. **Set Alert Parameters for Telnet Port:**
    - Configure alert parameters such as description, type, and severity.
10. **Configure Telnet Service on WinServer2012:**
    - Access the Services window on WinServer2012 and set the Telnet service to start automatically with a delayed startup.
11. **Start Telnet Service:**
    - Start the Telnet service on WinServer2012.
12. **Check Triggered Alerts:**
    - Navigate to Splunk's Activity section and view triggered alerts related to open Telnet ports.
13. **Disable Telnet Port Alert:**
    - Access Splunk settings to disable the alert for open Telnet ports.
14. **Stop Telnet Service:**
    - Access the Services window on WinServer2012 and stop the Telnet service.

Key Learnings:

- Utilizing Netstat data to monitor ports and services on a target machine.
- Implementing a script to regularly capture Netstat output and forward it to Splunk for analysis.
- Configuring Splunk SIEM to create alerts for insecure ports and services detected through Netstat data.
- Setting up alert parameters such as severity and description to classify and prioritize alerts.
- Adjusting Telnet service settings on WinServer2012 to ensure automatic startup and monitoring.
- Monitoring triggered alerts in Splunk to detect and respond to potential security threats.
- Disabling alerts and taking corrective actions as necessary to address identified security issues.

Lab 06

Lab Tasks:

1. **Access WinServer2012:**
    - Log in to the WinServer2012 machine using provided credentials.
2. **Install and Configure Sysmon:**
    - Copy the Sysmon.zip file from the provided location to the C:\ drive.
    - Unzip the Sysmon.zip file in the Sysmon folder.
    - Modify the sysmonconfig-export.xml file to monitor LSASS.exe events.
    - Install Sysmon and configure it to start automatically.
3. **Install and Configure Winlogbeat:**
    - Copy the Beats folder from the provided location to the C:\ drive.
    - Unzip the winlogbeat-6.5.4-windows-x86_64.zip file in the Beats folder.
    - Modify the winlogbeat.yml file to specify event logs and Elasticsearch settings.
    - Install Winlogbeat as a service and start it.
4. **Configure Firewall on Security Onion:**
    - Log in to the Security Onion machine using provided credentials.
    - Open Terminal and configure the firewall to allow connections to specific ports.

5. **Access Kibana Interface:**
    - Launch Kibana from the desktop shortcut.
    - Proceed past any security warnings and log in using provided credentials.
    - Create an index pattern for Winlogbeat data.
6. **Execute PowerShell Command on WinServer2012:**
    - Launch PowerShell as an administrator.
    - Execute a PowerShell command to simulate a download from the internet.
7. **View Events in Kibana:**
    - Switch to the Security Onion machine and access Kibana.
    - Search for events related to PowerShell commands connecting to the internet.
    - Analyze the details of the events to identify the host and destination IP addresses.

Key Learnings:

- Monitoring PowerShell commands connecting to the internet using Sysmon and Winlogbeat.
- Configuring Sysmon to log events related to LSASS.exe.
- Installing and configuring Winlogbeat to send event logs to Elasticsearch.
- Configuring the firewall on Security Onion to allow connections to specific ports.
- Accessing and navigating the Kibana interface to view and analyze event data.
- Identifying potential security threats by examining PowerShell command execution events in Kibana.

Lab 07

Lab Tasks:

1. **Access WinServer2012:**
    - Log in to the WinServer2012 machine using provided credentials.
2. **Install Mimikatz Tool:**
    - Copy the mimikatz_trunk.Zip file from the provided location to the C:\ drive.
    - Unzip the mimikatz_trunk.Zip file in the C:\ drive and delete the zip file after extraction.
    - Navigate to the C:\mimikatz_trunk\x64 folder and double-click on mimikatz.exe to launch the tool.
    - In the mimikatz console window, execute the commands "privilege::debug", "log Userdetails.log", and "sekurlsa::logonpasswords" to enable debug privileges, specify a log file, and dump user credentials, respectively.
3. **Access Security Onion Machine:**
    - Launch Kibana from the desktop shortcut.
    - Log in using provided credentials.
    - Navigate to the Discover tab and search for events with event ID 10 and GrantedAccess value of 0x1010.
4. **Analyze Events in Kibana:**
    - Review the events displayed in the search results, which indicate attempts to read memory in a process.
    - Expand the details of the first event to examine the specifics, such as LSASS being accessed with a GrantedAccess value of 0x1010.
5. **Conclude the Exercise:**
    - Close all open windows and conclude the exercise.

Key Learnings:

- Monitoring the execution of lsass.exe with a GrantedAccess flag when using Mimikatz tool to retrieve credentials from memory.
- Installing and using Mimikatz tool to dump user credentials from memory.
- Analyzing events in Kibana to identify attempts to read memory in a process, particularly LSASS, with specific access permissions.
- Understanding the significance of LSASS access with GrantedAccess flag in detecting potential credential dumping activities.

Lab 08

Lab Tasks:

1. **Access WinServer2012:**
    - Log in to the WinServer2012 machine using provided credentials.
2. **Install Mimikatz Tool:**
    - Copy the mimikatz_trunk.Zip file from the provided location to the C:\ drive.
    - Unzip the mimikatz_trunk.Zip file in the C:\ drive and delete the zip file after extraction.
    - Navigate to the C:\mimikatz_trunk\x64 folder and double-click on mimikatz.exe to launch the tool.
    - In the mimikatz console window, execute the commands "privilege::debug", "log Userdetails.log", and "sekurlsa::logonpasswords" to enable debug privileges, specify a log file, and dump user credentials, respectively.
3. **Access Security Onion Machine:**
    - Launch Kibana from the desktop shortcut.
    - Log in using provided credentials.
    - Navigate to the Discover tab and search for events with event ID 10 and GrantedAccess value of 0x1010.
4. **Analyze Events in Kibana:**
    - Review the events displayed in the search results, which indicate attempts to read memory in a process.
    - Expand the details of the first event to examine the specifics, such as LSASS being accessed with a GrantedAccess value of 0x1010.
5. **Conclude the Exercise:**
    - Close all open windows and conclude the exercise.

Key Learnings:

- Monitoring the execution of lsass.exe with a GrantedAccess flag when using Mimikatz tool to retrieve credentials from memory.
- Installing and using Mimikatz tool to dump user credentials from memory.
- Analyzing events in Kibana to identify attempts to read memory in a process, particularly LSASS, with specific access permissions.
- Understanding the significance of LSASS access with GrantedAccess flag in detecting potential credential dumping activities.