MODULE 06 Understanding Cyber Threats, IoCs, and Attack Methodology LAB SCREENSHOTS

Lara Alofi

Lab Session Identifiers

1. https://labclient.labondemand.com/LabClient/eb92f436-2228-4322-a004-3daaa9608b9f
2.

Username on EC-Council System

1. 2110886@uj.edu.sa

Exercise 1: Generating Tickets for Incidents

1. **Launch OSSIM Server**: Access AlienVault web interface.
    - **Learning**: Understanding the initial setup of OSSIM for incident management.
2. **Login to WinServer2012 and SIEM2 Machines**: Access virtual machines and log in.
    - **Learning**: Familiarization with accessing different systems in the network environment.
3. **Create IRT User Account (Martin)**: Configure user permissions.
    - **Learning**: Understanding user management for incident response team members.
4. **Configure HIDS Agent**: Deploy HIDS agent on WinServer2012.
    - **Learning**: Deployment of Host-based Intrusion Detection System for monitoring host activity.
5. **Create Correlation Directives**: Define rules for triggering alarms.
    - **Learning**: Configuring correlation rules to detect specific security events.
6. **Generate Alarms**: Simulate security incidents by triggering alarms.
    - **Learning**: Identification and investigation of security alarms for potential incidents.
7. **Create Incident Tickets**: Generate incident tickets for escalated issues.
    - **Learning**: Understanding the importance of ticketing in incident escalation and resolution.

Exercise 2: Containing Data Loss Incidents

1. **Access WinServer2012 Machine**: Log in to WinServer2012.
2. **Edit Configuration Files**: Modify inputs.conf, props.conf, and transforms.conf files to monitor FTP activity.
    - **Learning**: Understanding configuration adjustments for monitoring FTP connections.
3. **Restart SplunkForwarder Service**: Restart the SplunkForwarder service to apply configuration changes.
    - **Learning**: Learning to apply configuration changes in SplunkForwarder for real-time monitoring.
4. **Simulate Unauthorized Access**: Use Kali Linux to perform a brute force attack on the FTP server.
    - **Learning**: Understanding security vulnerabilities and attack simulations.
5. **Gain FTP Access**: Attempt to log in to the FTP server using cracked credentials.
    - **Learning**: Understanding the importance of strong authentication mechanisms.
6. **Transfer Data**: Copy files from an unauthorized host (Windows10) to the FTP server.
    - **Learning**: Understanding potential data loss scenarios.
7. **Monitor FTP Connections**: Check for FTP connections from unauthorized hosts in Splunk.
    - **Learning**: Understanding the importance of real-time monitoring for detecting unauthorized activities.
8. **Terminate Unauthorized Activity**: Stop the FTP service to prevent further unauthorized data transfer.
    - **Learning**: Learning containment strategies to prevent data loss incidents.
9. **View Error Logs**: Check Splunk for logs indicating unauthorized data transfer attempts.
    - **Learning**: Understanding how logs help in incident investigation and analysis.

10. **Closure**: Close all windows and end the exercise.
    - **Learning**: Wrapping up the containment phase and understanding the importance of incident response processes.

Exercise 3: Eradicating SQL Injection and XSS Incidents

1. **Install UrlScan Tool**: Install UrlScan 3.1 on WinServer2012 to prevent SQL Injection and XSS attacks.
    - **Learning**: Understanding the use of web filters for preventing common web attacks.
2. **Configure UrlScan**: Modify the UrlScan.ini file to add custom rules for preventing SQL Injection attacks.
    - **Learning**: Learning to configure web filters to block malicious requests.
3. **Integrate UrlScan with IIS**: Configure UrlScan with IIS by adding it as an ISAPI filter.
    - **Learning**: Understanding the integration of security tools with web servers.
4. **Access LuxuryTreats Website**: Log in to the LuxuryTreats website as a registered user.
    - **Learning**: Understanding the user experience in a web application.
5. **View Order Details**: Navigate to order details and ensure proper access control.
    - **Learning**: Understanding the importance of access control in web applications.
6. **Perform SQL Injection**: Attempt SQL Injection on the website to bypass security measures.
    - **Learning**: Understanding SQL Injection vulnerabilities and their implications.
7. **Observe Filtered Request**: Notice the UrlScan tool filtering the SQL Injection attempt and returning an HTTP error.
    - **Learning**: Understanding how web filters prevent SQL Injection attacks.
8. **Perform XSS Attack**: Attempt XSS attack by injecting malicious script into the website.
    - **Learning**: Understanding XSS vulnerabilities and their consequences.
9. **Observe Filtered XSS Attack**: Notice UrlScan filtering the XSS attack and returning an HTTP error.
    - **Learning**: Understanding how web filters prevent XSS attacks.
10. **Remove UrlScan Filter**: Remove UrlScan filter from the LuxuryTreats website.
    - **Learning**: Understanding the process of reverting security configurations after mitigating threats.
11. **Closure**: Close all windows and end the exercise.
    - **Learning**: Wrapping up the eradication phase and understanding the importance of continuous security measures.

Exercise 4: Recovering from Data Loss Incidents

1. **Setup Enhanced PowerShell Logging**: Configure enhanced PowerShell logging using Group Policy Editor to capture PowerShell activities.
    - **Learning**: Understanding the importance of logging for detecting malicious activities.
2. **Enable PowerShell Remoting**: Configure WinRM service on both Windows10 and WinServer2012 machines for remote PowerShell execution.
    - **Learning**: Enabling remote administration capabilities for incident response actions.
3. **Forward Logs to Splunk**: Configure Splunk Universal Forwarder to forward PowerShell logs for central monitoring.
    - **Learning**: Integrating log management solutions for centralized incident detection and response.

4. **Simulate Data Deletion**: Simulate data deletion by executing a remote PowerShell command to delete a folder on Windows10.
    - **Learning**: Understanding the simulation of data loss incidents for recovery testing.
5. **Monitor PowerShell Logs**: Use Splunk to monitor PowerShell logs for detecting the remote script execution.
    - **Learning**: Monitoring logs for detecting and investigating suspicious activities.
6. **Verify Data Loss**: Verify that the folder "MyFolder" has been deleted from the E: drive on Windows10.
    - **Learning**: Verifying the impact of the simulated data loss incident.
7. **Install Data Recovery Tool**: Install EaseUS Data Recovery Wizard on Windows10 for recovering the deleted data.
    - **Learning**: Understanding the use of data recovery tools in the incident recovery process.
8. **Recover Deleted Data**: Use EaseUS Data Recovery Wizard to scan for and recover the deleted folder "MyFolder".
    - **Learning**: Performing data recovery actions to restore lost data.
9. **Verify Recovered Data**: Verify that the deleted data has been successfully recovered on the C: drive.
    - **Learning**: Verifying the success of the data recovery process.
10. **Closure**: Close all windows and end the exercise.
    - **Learning**: Wrapping up the recovery phase and ensuring business continuity after data loss incidents.

Exercise 5: Creating Incident Reports using OSSIM

---

1. **Access OSSIM Server**: Log in to the OSSIM Server using the provided credentials (root/toor).
    - **Learning**: Understanding how to access the OSSIM interface for report generation.
2. **Accessing SIEM2 Machine**: Log in to the SIEM2 machine using the provided credentials (Admin/Pa$$w0rd).
    - **Learning**: Accessing the machine where reports will be viewed or exported.
3. **Proceed with Unsecure Connection**: Accept the security warning and proceed to the OSSIM login page.
    - **Learning**: Overcoming security warnings to access the OSSIM interface.
4. **Skip AlienVault Wizard**: Skip the initial setup wizard to go directly to the OSSIM login page.
    - **Learning**: Skipping unnecessary setup steps to access the main functionality quickly.
5. **Login to OSSIM**: Enter the admin credentials to log in to the OSSIM interface.
    - **Learning**: Logging in to the OSSIM interface to access report generation features.
6. **Navigate to Reports Overview**: Go to the Reports section and select Overview to access report options.
    - **Learning**: Understanding where to find report options within the OSSIM interface.
7. **Select Report Options**: Choose the desired reports from the available options, such as Alarms Report and SIEM Events.
    - **Learning**: Selecting the specific reports to generate based on requirements.
8. **Customize Date Range**: Adjust the date range for the reports as needed before generating them.
    - **Learning**: Customizing report parameters to capture data within specific timeframes.

9. **Download PDF**: Download the selected report as a PDF file for offline viewing or sharing.
    - **Learning**: Exporting reports in different formats for distribution or archival purposes.
10. **Send by Email**: Send the generated report via email to the concerned person, providing their email address.
    - **Learning**: Sharing reports with relevant stakeholders for further analysis or action.
11. **Close All Windows**: Conclude the exercise by closing all open windows.
    - **Learning**: Properly concluding tasks and closing applications after completing report generation activities.