MODULE 3 Incidents, Events, and Logging LAB REPORT

Lara Alofi

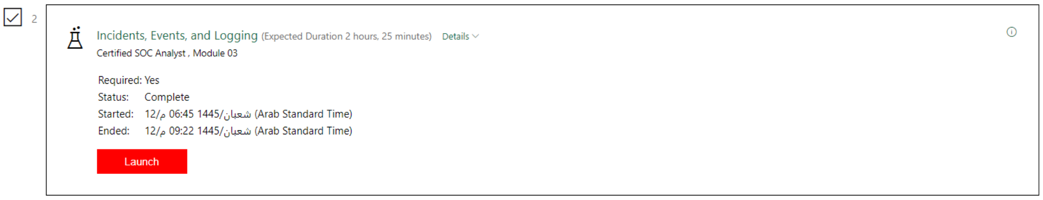
Module 03 Incidents, Events, and Logging

Lab Session Identifiers

1. https://labclient.labondemand.com/LabClient/b7452f46-f162-4970-9f56-4b3ceb29c02c?rc=10

Username on EC-Council System

1. 2110886@uj.edu.sa



☑ 2

Incidents, Events, and Logging (Expected Duration 2 hours, 25 minutes) Details

Certified SOC Analyst , Module 03

Required: Yes
Status: Complete
Started: 12/م 06:45 1445/شعبان (Arab Standard Time)
Ended: 12/م 09:22 1445/شعبان (Arab Standard Time)

Lab 01: During our initial lab session, we embarked on a comprehensive exploration of the critical role that logging mechanisms play within the Windows operating system (OS) for the purpose of security monitoring. We delved into the intricate process of configuring Windows audit policies to selectively capture specific security events, including both successful and failed login attempts. Through hands-on experimentation with the Event Viewer tool, we meticulously dissected Windows security logs to discern potential security incidents, such as brute force login attempts. This immersive analysis provided us with invaluable insights into the paramount importance of efficient log management and analysis in safeguarding system and network security. Furthermore, this lab equipped us with indispensable skills essential for Security Operations Center (SOC) analysts and cybersecurity professionals, including the ability to configure, interpret, and derive actionable insights from Windows security logs.

Lab 02: Our second lab session was dedicated to unraveling the complexities inherent in managing logs within Internet Information Services (IIS), a cornerstone web server within Windows environments. We delved deep into the multifaceted realm of IIS logs, underscoring their pivotal role in deciphering user behaviors, scrutinizing web application interactions, and alerting stakeholders to potential security breaches. Through a meticulous examination of the IIS Manager interface, we meticulously navigated through the labyrinth of options to enable logging, meticulously set log file locations, and judiciously defined the fields to be logged, ensuring a comprehensive coverage of pertinent data points. Through practical exercises leveraging tools like Notepad++, we honed our ability to access, scrutinize, and interpret log files, uncovering the nefarious nature of SQL injection vulnerabilities and illuminating the path toward robust security protocols. Emphasizing the imperative for stringent security measures and proactive validation protocols, this lab empowered us to fortify our skills in configuring, monitoring, and analyzing IIS logs, thereby enhancing our capacity to detect and mitigate potential security threats in real-world scenarios.

Lab 03: In this transformative lab, we embarked on a journey to unravel the intricacies of Network Intrusion Detection Systems (IDS), with a particular focus on the omnipotent Snort, hailed as a stalwart guardian against potential security threats lurking within network environments. We delved deep into the arcane art of installing and configuring Snort on a Windows server, meticulously configuring essential parameters such as network variables, rule paths, and output plugins. Armed with this newfound knowledge, we ventured into the realm of customizing detection rules, aligning them seamlessly with the idiosyncrasies of specific network security requirements. Through a series of meticulously orchestrated practical exercises leveraging formidable tools like Nmap, we simulated a gamut of network scan attacks, meticulously evaluating Snort's prowess in real-time threat detection and logging. Through a judicious analysis of Snort IDS logs, we gleaned insights into the intricate patterns, anomalies, and potential security breaches ensconced within the labyrinthine network traffic. This immersive experience underscored the cardinal importance of continuous monitoring and analysis of network traffic in the perpetual quest to thwart evolving security threats, thereby arming us with the tools and insights necessary to fortify the resilience of network infrastructure.

Lab 04: In our culminating exercise, we embarked on an odyssey into the realm of centralized logging, unveiling the transformative power of aggregating logs from disparate devices and applications into a centralized repository for streamlined monitoring and analysis. We meticulously traversed the labyrinth of installation and configuration processes, adeptly installing and configuring Splunk Universal Forwarder on Windows Server 2012 and Windows 10 machines, thereby facilitating the seamless forwarding of logs to a centralized Splunk instance. Through the judicious configuration of forwarding and receiving settings within Splunk, and the bespoke customization of log collection configurations using inputs.conf, props.conf, and transforms.conf files, we empowered ourselves to undertake a comprehensive analysis of log data sourced from diverse origins, including Windows Event Logs, IIS logs, and Snort IDS logs. Through a panoply of hands-on exercises, we adeptly identified security anomalies, demystified common vulnerabilities, and simulated a plethora of attack scenarios, thereby honing our skills in security monitoring and incident response within a centralized logging environment leveraging Splunk. This transformative experience not only equipped us with the tools and insights necessary to fortify our defenses against potential security threats but also underscored the imperative for continuous vigilance and proactive threat mitigation strategies in the perpetual battle to safeguard organizational assets and preserve network integrity.