CompTIA CySA+ (CS0-003), Skill Labs

Course Specifications

Course Number: ACI76-004SL_rev1.0
Lab Length: Approximately 12 hours

System & Network Security Implementation Concepts (CS0-003)

Introduction

Objective

Welcome to the System & Network Security Implementation Concepts practice lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

Overview

Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – Log Collection with Splunk
- Exercise 2 – Encrypting Sensitive Data
- Exercise 3 – Enable Multifactor Authentication

After completing these modules, you should be able to:

- Collect Logs from Devices on the Network using the Splunk Enterprise Application
- Encrypt a Local Drive using BitLocker Drive Encryption
- Enable Multifactor Authentication

Exam Objectives:

The following exam objectives are covered in this module:

1.1 Explain the importance of system and network architecture concepts in security operations.

Threat Intelligence & Threat Gathering Concepts (CS0-003)

Introduction

Objective

Welcome to the Threat Intelligence & Threat Gathering Concepts Practice Lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

Overview

Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – Collection Methods and Sources
- Exercise 2 – Threat Intelligence Hunting and Sharing

After completing this module, you should be able to:

- Know about Open Source Intelligence (OSINT)
- Work with OSINT Tools
- Employ Incident Response using SIEM
- Use a Honeypot Tool
- Use MITRE ATT&CK to Identify Tactics, Techniques, and Procedures (TTPs)
- Access and Research Logs using Windows Event Viewer
- Enable Firewall Logging

Exam Objectives:

The following exam objectives are covered in this module:

- 1.4 Compare and contrast threat-intelligence and threat-hunting concepts

Techniques to Determine Malicious Activity (CS0-003)

Introduction

Objective

Welcome to the Techniques to Determine Malicious Activity Practice Lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

As a Cyber Security Analyst, it is important to constantly monitor the environment for malicious activity and be proactive to advert threats and exploits.

In this module, different techniques will be explored for detecting malicious activity.

Overview

Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – Monitor Windows Event Log with a PowerShell Script
- Exercise 2 – Monitor Login Events on Linux Devices

After completing this module, you should be able to:

- Enable Audit Logon Events
- Generate Logs for Evaluation
- Create a Logon Events Script using PowerShell ISE
- Prevent a Brute-Force Attack
- Monitor Login Events on a Linux Device

Exam Objectives:

The following exam objectives are covered in this module:

1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity.

- Common techniques

Vulnerability Scanning Tools & Techniques (CS0-003)

Introduction

Objective

Welcome to the Vulnerability Scanning Tools & Techniques practice lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

Overview

Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – Network Asset Detection Tools
- Exercise 2 – Detecting Network Vulnerabilities

After completing this module, you should be able to:

- Use NMAP to Detect Devices on the Network.
- Use Zenmap to Discover Devices on the Network.
- Scan Network Devices for Vulnerabilities with OWASP Zap.
- Detect Network Vulnerabilities using NMAP.
- Scan Network Devices with Nessus.
- Detect Vulnerabilities using Metasploit and NMAP.

Exam Objectives:

The following exam objectives are covered in this module:

2.1 Given a scenario, implement vulnerability scanning methods and concepts.

- Asset discovery

2.2 Given a scenario, analyze output from vulnerability assessment tools

- Tools

Identifying & Analyzing Malicious Activity (CS0-003)

Introduction

Objective

Welcome to the Identifying & Analyzing Malicious Activity practice lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

Overview

Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – Analyze Resource Utilization
- Exercise 2 – Detecting Unauthorized User Privilege Escalation

After completing this module, you should be able to:

- Monitor Resource Utilization on a Windows Device
- Monitor Resource Utilization on a Linux Device
- Enable User Privilege Monitoring
- Generate Auditing Logs
- Detect an Unauthorized User Privilege Escalation

Exam Objectives:

The following exam objectives are covered in this module:

1.2 Given a scenario, analyze indicators of potentially malicious activity.

- Network-related
- Host-related
- Application-related

Tools for Identifying Malicious Activity (CS0-003)

Introduction

Objective

Welcome to the Tools for Identifying Malicious Activity practice lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

Overview

Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – Monitoring Network Activity
- Exercise 2 – Using a Sandbox for Analyzing Malicious Files
- Exercise 3 – Validating Domain Names and IP Addresses

After completing this module, you should be able to:

- Customize the Wireshark Application
- Capture Network Traffic using the Wireshark Application
- Capture Network Traffic using Tcpdump
- Analyze Malicious Code
- Use WHOIS to Validate Domain Names
- Use AbuseIPDB to Validate Domain Names
- Use the Virustotal Website to Verify Links

Exam Objectives:

The following exam objectives are covered in this module:

1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity.

- Tools

Attack Methodology Frameworks (CS0-003)

Introduction
Objective

Welcome to the Attack Methodology Frameworks practice lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – Attack Methodology Frameworks
- Exercise 2 – OWASP Testing Framework

After completing this module, you should be able to:

- Explore the MITRE ATT&CK Website
- Detect Web Server Vulnerabilities

After completing this exercise, you should have further knowledge of:

- Cyber Kill Chain
- Diamond Model of Intrusion Analysis
- MITRE ATT&CK Framework

Exam Objectives:

The following exam objectives are covered in this module:

3.1 Explain concepts related to attack methodology frameworks

- Cyber kill chain
- Diamond Model of Intrusion Analysis
- MITRE ATT&CK
- Open Source Security Testing Methodology Manual (OSS TMM)
- OWASP Testing Guide

Vulnerability Data Analysis and Prioritization (CS0-003)

Introduction
Objective

Welcome to the Vulnerability Data Analysis and Prioritization practice lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – Common Vulnerability Scoring System (CVSS) Calculator
- Exercise 2 – Detecting Web Application Vulnerabilities

After completing this module, you should be able to:

- Determine the Severity of a Discovered Vulnerability
- Detect Web Application Vulnerabilities and Analyze the Results

Exam Objectives:

The following exam objectives are covered in this module:

- 2.3 Given a scenario, analyze data to prioritize vulnerabilities.
- 2.4 Given a scenario, recommend controls to mitigate attacks and software vulnerabilities.

Incident Response Management Techniques (CS0-003)

Introduction

Objective

Welcome to the Incident Response Management Techniques practice lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

Overview

Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – Review Incident Response Playbooks
- Exercise 2 – Use Splunk to Monitor for Port Scanning
- Exercise 3 – Create a Forensic Image for Investigation

After completing this module, you should be able to:

- Review the NIST Incident Handling Guide
- Implement the CISA Cybersecurity Incident & Vulnerability Response Playbook
- Implement Microsoft Incident Response Playbooks
- Install Splunk Enterprise and the Splunk Universal Forwarder
- Install and Configure TA-winfw
- Identify Port Scanning using Splunk Enterprise
- Prepare a Data Source Partition for Forensic Imaging
- Install the OS Forensics Application and Create a New Case
- Conduct a Forensic Image and Mount the Image on a Partition for Forensic Investigation

Exam Objectives:

The following exam objectives are covered in this module:

- 3.2 Given a scenario, perform incident response activities
- 3.3 Explain the preparation and post-incident activity phases of the incident management life cycle

Incident Response Communication & Reporting (CS0-003)

Introduction
Objective

Welcome to the Incident Response Communication & Reporting Practice Lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – Review Guidance for Coordination and Information Sharing
- Exercise 2 – Review Required Reports
- Exercise 3 – Review the IBM Security Cost of a Data Breach Report 2022

After completing this module, you should be able to:

- Review the NIST Incident Handling Guide
- Review the CISA Cybersecurity Incident & Vulnerability Response Playbook
- Review the Federal Incident Notification Guidelines
- Review the CISA Incident Reporting Forms
- Review an Information Security Incident Report Form
- Review the Cost of a Data Breach Report 2022

Exam Objectives:

The following exam objectives are covered in this module:

- 4.2 Explain the importance of incident response reporting and communication

Vulnerability Reporting Concepts (CS0-003)

Introduction
Objective

Welcome to the Vulnerability Reporting Concepts Practice Lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – Log Collection with Splunk
- Exercise 2 – Creating a Vulnerability Report with Splunk

After completing this module, you should be able to:

- Install and Configure the Splunk Enterprise Application
- Configure a Splunk Client
- Collect Logs using Splunk Enterprise
- Generate a Vulnerability Report

Exam Objectives:

The following exam objectives are covered in this module:

4.1 Explain the importance of vulnerability management reporting and communication.

- Vulnerability management reporting

Vulnerability Patching & Attack Surface Management (CS0-003)

Introduction

Objective

Welcome to the Vulnerability Patching & Attack Surface Management Practice Lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

Overview

Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 Windows Patch Management Techniques
- Exercise 2 Linux Patch Management Techniques

After completing this module, you should be able to:

- Create a Production Workstation
- Create a Windows Workstation Update Group Policy
- Create an Update Script
- Create a Scheduled Update Task

Exam Objectives:

The following exam objectives are covered in this module:

2.5 Explain concepts related to vulnerability response, handling, and management.

- Patching and configuration management
- Attack surface management