masterskill
education through innovation

aci LEARNING | SKILL LABS

CompTIA Security+ (Exam SY0-701), Skill Labs

Course Specifications

Course Number: ACI76-001SL_rev1.0
Lab Length: Approximately 18 hours

Security Concept Fundamentals

Introduction
Objective

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

Security fundamentals begin with confidentiality, integrity, and availability (CIA). These concepts are the pillars and promise of cyber security. CIA is often implemented through authentication, authorization, and accounting. All these processes require tools and configurations to ensure they provide the expected level of security.

Availability is enabled by redundant and resilient systems. One such system is the redundant array of independent disks (RAID). Certain RAID configurations, like RAID 1 and RAID 10, duplicate data across multiple disks, providing redundancy, meaning that if a disk fails, the system can continue to operate without data loss. This enables data availability even in the face of component and system failures.

File Integrity Monitoring (FIM) is a security practice that involves regularly checking and validating the integrity of files and system configurations. It's designed to detect unauthorized changes to critical and designated files, configurations, and directories. FIM enables early detection of breaches, regulatory compliance, and incident response.

In this module, you will enhance availability with a RAID configuration. You will then test FIM on a designated file system to ensure the integrity of the files being monitored.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 - Configure RAID 1
- Exercise 2 - Configure and Test File Integrity Monitoring

After completing this module, you should be able to:

- Create two unformatted VHDs.
- Configure RAID 1 across the unallocated disks.
- Prepare the SIEM manager.
- Install an agent on ACIWIN11 and configure FIM.
- Test FIM.

Exam Objectives:

The following exam objectives are covered in this module:

1.2 Summarize fundamental security concepts

- Confidentiality, integrity, and availability (CIA)
- Authentication, authorization, and accounting (AAA)
- Zero trust

3.1 Compare and contrast security implications of different architecture models

- Considerations

3.4 Explain the importance of resilience and recovery in security architecture

- High availability

4.5 Given a scenario, modify enterprise capabilities to enhance security

- File Integrity Monitoring

Cryptographic Solutions

Introduction
Objective

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

Cryptography provides the tools and techniques necessary to ensure the confidentiality, integrity, authenticity, and availability of data in the network. It forms the backbone of cybersecurity strategies, enabling safe and secure communication, transactions, and data management.

Two prominent cryptographic solutions used throughout the network are Digital Signatures and Certificates. In this module, you will explore how to create a digital signature and certificate signing request manually.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 - Create and Verify a Digital Signature
- Exercise 2 - Create and Approve a Certificate Signing Request

After completing this module, you should be able to:

- Create a private and public key pair.
- Create a digital signature.
- Receive and verify a digital signature.
- Observe a signature verification failure.
- Create a Certificate Signing Request (CSR).
- Receive and approve a CSR as a Certificate Authority (CA).

Exam Objectives:

The following exam objective is covered in this module:

1.4 Explain the importance of using appropriate cryptographic solutions

- Public key infrastructure (PKI)
- Encryption
- Hashing
- Digital signatures
- Certificates

Threat Vectors and Attack Surfaces

Introduction
Objective

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

Identifying threat vectors and attack surfaces is critical to network security. Understanding how to identify indicators of attack and vulnerable applications enables the administrator to apply mitigations and act proactively to protect the network environment.

In this module, you will identify potential attack surfaces and mitigate them.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 - Open Service Ports
- Exercise 2 - Default Credentials
- Exercise 3 - Vulnerable Applications

After completing this module, you should be able to:

- Discover unnecessary open ports.
- Close unnecessary open ports.
- Discover the Guest account.
- Disable the Guest account.
- Discover a recently installed application.
- Simulate an attack on the vulnerable application.
- Observe indicators of attack.

Exam Objectives:

The following exam objectives are covered in this module:

1.2 Summarize fundamental security concepts

- Authentication, Authorization, and Accounting (AAA)

2.2 Explain common threat vectors and attack surfaces

- Message-based
- File-based

- Vulnerable software
- Unsupported systems and applications
- Open service ports
- Default credentials
- Human vectors/social engineering

2.4 Given a scenario, analyze indicators of malicious activity

- Indicators

Identifying Security Vulnerabilities

Introduction
Objective

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

Identifying security vulnerabilities is a fundamental part of cybersecurity risk management. Identifying vulnerabilities can protect sensitive data, ensure business continuity, adhere to compliance requirements, prevent attacks, and save organizations from the costs of incident response.

Many significant configuration vulnerabilities are quick and easy to inadvertently enable. As such, it is important to study configurations to understand what the vulnerability is and how a misconfiguration can enable the vulnerability.

In this module, you will enable Lan Manager (LM) hash storage on ACIDC01 and a DNS domain transfer capability in order to study the adverse effects of both misconfigurations.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 - Identify LM Hash Vulnerabilities
- Exercise 2 - Identify DNS Transfer Vulnerabilities

After completing this module, you should be able to:

- Extract hashes from ACIDC01.
- Update the domain policy to enable LM hashes.
- Extract and crack an LM hash.
- Add a record to the DNS Server.
- Configure the DNS Server to allow zone transfers.

Exam Objectives:

The following exam objectives are covered in this module:

2.3 Explain various types of vulnerabilities

- Cryptographic
- Misconfiguration

3.2 Given a scenario, apply security principles to secure enterprise infrastructure

- Infrastructure considerations

5.1 Summarize elements of effective security governance

- Policies

5.5 Explain types and purposes of audits and assessments

- Internal

Analyze Malicious Activity

Introduction
Objective

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

Recognizing indicators of network and application attacks is an essential cybersecurity skill. Indicators of compromise and attack enable organizations to respond to attacks effectively and protect sensitive information.

In this module, you will become familiar with brute force attacks, command injection, and a SYN flood network attack, as well as their indications.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 - Observe Indications of a Brute Force Attack
- Exercise 2 - Conduct Command Injection and Observe Indications
- Exercise 3 - Observe Indications of a SYN Flood Attack

After completing this module, you should be able to:

- Perform SMB enumeration and login attempt.
- Conduct and observe a scripted brute force attack.
- Conduct command injection.
- Create a reverse shell through command injection.
- Observe normal activity.
- Conduct and observe a SYN flood attack.

Exam Objectives:

The following exam objectives are covered in this module:

2.4 Given a scenario, analyze indicators of malicious activity

- Application attacks
- Password attacks
- Indicators

4.1 Given a scenario, apply common security techniques to computing resources

- Monitoring

4.9 Given a scenario, use data sources to support an investigation

- Log data

Security Architecture Models

Introduction
Objective

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

Virtualization and containerization are architecture models that are important to security. They provide efficient resource utilization, portability, rapid deployment, flexibility, and scalability.

In this module, you will install an Ubuntu virtual machine (VM) in the Hyper-V hypervisor and use Docker to create and manage containers in a command-line environment and Portainer to create and manage containers through a browser-based graphical user interface (GUI).

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 - Create a VM
- Exercise 2 - Use Containers
- Exercise 3 - Complete VM Deployment

After completing this module, you should be able to:

- Create a VM in Hyper-V.
- Launch Ubuntu installation.
- Create and manage containers from a command-line interface (CLI).
- Create and manage containers from a GUI.
- Manually relaunch the Ubuntu VM.
- Test the New VM.

Exam Objectives:

The following exam objectives are covered in this module:

2.5 Explain the purpose of mitigation techniques used to secure the enterprise

- Segmentation

3.1 Compare and contrast security implications of different architecture models

- Architecture and infrastructure concepts
- Considerations

Securing Enterprise Infrastructures

Introduction
Objective

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

A secure enterprise infrastructure enables the protection of production data and intellectual property, complying with regulations, minimizing legal liability, and ensuring business continuity.

In this module, you will learn how encryption and remote access can be used to ensure data is secure in transit.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 - Install and Configure a VPN Server
- Exercise 2 - Create a VPN User and Client
- Exercise 3 - Configure a L2TP/IPsec VPN

After completing this module, you should be able to:

- Install and configure the VPN server.
- Configure monitoring and the Windows Firewall.
- Create and configure a VPN user in Active Directory.
- Create and test VPN client connection.
- Configure and test an L2TP/IPsec VPN.

Exam Objectives:

The following exam objectives are covered in this module:

1.2 Summarize fundamental security concepts

- Authentication, authorization, and accounting (AAA)

1.4 Explain the importance of using appropriate cryptographic solutions

- Encryption

3.2 Given a scenario, apply security principles to secure enterprise infrastructure

- Infrastructure considerations
- Secure communication/access

4.5 Given a scenario, modify enterprise capabilities to enhance security

- Firewall

Data Protection Strategies

Introduction
Objective

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

Data protection strategies are implemented to protect the confidentiality, integrity, and availability of production data. These strategies are implemented through risk management to protect the data from cyber threats, maintain customer trust, and comply with laws and regulations.

In this module, you will explore the data protection strategies of encryption, hashing, and code obfuscation.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 - Encryption
- Exercise 2 - Hashing
- Exercise 3 - Obfuscation

After completing this module, you should be able to:

- Encrypt a file.
- Encrypt a folder.
- Conduct hashing in Windows.
- Conduct hashing in Linux.
- Execute JavaScript code.
- Obfuscate and execute JavaScript code.

Exam Objectives:

The following exam objective is covered in this module:

3.3 Compare and contrast concepts and strategies to protect data

- General data considerations
- Methods to secure data

Resilience in Security Architecture

Introduction
Objective

Welcome to the Resilience in Security Architecture practice lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

A resilient security architecture can withstand, adapt, and recover from security incidents, threats, and disruptions. This enables critical systems and production data to remain functional during incidents and disruption, enabling a continuity of operations.

In this module, you will explore resilience through production data backups.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 - Prepare WIN11 and Install EaseUS Todo Backup
- Exercise 2 - Conduct and Restore from Incremental Backups
- Exercise 3 - Conduct Differential Backups and Examine All Backup Files
- Exercise 4 - Investigate the Archive Bit

After completing this module, you should be able to:

- Partition the ACIWIN11 hard drive.
- Create the test production data and recovery folder structure.
- Install EaseUS Todo Backup.
- Conduct incremental backups.
- Restore from incremental backups and examine restoration files
- Conduct differential backups.
- Examine incremental and differential backup files.
- View the archive bit in Windows Explorer and the command line.

Exam Objectives:

The following exam objectives are covered in this module:

3.4 Explain the importance of resilience and recovery in security architecture

- Continuity of operations
- Backups

5.2 Explain elements of the risk management process

- Business impact analysis

Securing Computing Resources

Introduction
Objective

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

Securing computing resources ensures the confidentiality, integrity, and availability of data and resources. It includes practices such as implementing security policies, vulnerability management, network security, and access control.

In this module, you will explore securing computing resources through the establishment of a baseline in performance monitor, exploring input validation in a web application, and installing and using a sandbox.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 - Establish a Baseline
- Exercise 2 - Input Validation
- Exercise 3 - Sandboxing

After completing this module, you should be able to:

- Configure a baseline.
- Capture a baseline.
- View cookie parameters.
- Explore input validation code.
- Test input validation.
- Install Sandboxie Plus.
- Use and observe Sandboxie Plus.

Exam Objectives:

The following exam objective is covered in this module:

4.1 Given a scenario, apply common security techniques to computing resources

- Secure baselines
- Application security
- Sandboxing

Asset Management Techniques

Introduction
Objective

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

IT asset management helps organizations effectively manage and optimize their IT resources, which can lead to improved operational efficiency, cost savings, and enhanced cybersecurity. From a security perspective, it is impossible to apply effective security until all network assets are tracked and managed. In addition, as assets and applications are deprovisioned, secured data destruction is essential, although it is not always an intuitive process.

In this module, you will use Snipe-IT to create and manage assets and SDelete and Cipher to securely destroy files.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 - Deploy an Asset and License
- Exercise 2 - Secure Data Sanitization

After completing this module, you should be able to:

- Create a company and configure admin settings.
- Create an asset and license.
- Issue an asset and license.
- Securely delete files.
- Overwrite unallocated data.

Exam Objectives:

The following exam objectives is covered in this module:

4.2 Explain the security implications of proper hardware, software, and data asset management

- Assignment/accounting
- Monitoring/asset tracking
- Disposal/decommissioning

Vulnerability Management

Introduction
Objective

Welcome to the Vulnerability 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 - Detect Web Application Vulnerabilities
- Exercise 2 - Monitor Devices for Vulnerabilities

After completing this module, you should be able to:

- Scan the network for available Hosts using Nmap.
- Scan detected hosts for vulnerabilities with Nikto.
- Scan detected hosts for vulnerabilities with OWASP ZAP.
- Scan detected hosts for vulnerabilities with Metasploit and Nmap.
- Prepare the SIEM manager.
- Install the SIEM agent on a Windows device.
- Detect vulnerabilities on a Windows device.

Exam Objectives:

The following exam objectives is covered in this module:

4.3 Explain various activities associated with vulnerability management

- Identification methods
- Analysis
- Vulnerability response and remediation
- Validation of remediation
- Reporting

Monitoring Computing Resources

Introduction
Objective

Welcome to the Monitoring Computing Resources 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 Device Resource Utilization

After completing this module, you should be able to:

- Monitor Alma Linux device's resource utilization.
- Monitor device resource utilization on Kali Linux.
- Monitor resource utilization on a Microsoft device.

Exam Objectives:

The following exam objective is covered in this module:

4.4 Explain security alerting and monitoring concepts and tools

- Monitoring computing resources
- Activities
- Tools

Enhancing Enterprise Security

Introduction
Objective

Welcome to the Enhancing Enterprise Security 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 - Linux Server Hardening Techniques
- Exercise 2 - Windows Server Hardening Techniques

After completing this module, you should be able to:

- Harden a Linux Server.
- Manage a Linux Firewall.
- Harden a Windows Server.
- Manage a Windows Server Firewall.

Exam Objectives:

The following exam objectives is covered in this module:

4.5 Given a scenario, modify enterprise capabilities to enhance security

- Firewall
- Operating system security
- Implementation of secure protocols

Implement Identity & Access Management

Introduction
Objective

Welcome to the Implement Identity & Access 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 - Provisioning User Accounts on a Microsoft Server
- Exercise 2 - Provisioning User Accounts on a Linux Server

After completing this module, you should be able to:

- Create a domain user account using Active Directory users and computers.
- Create a user using Windows PowerShell.
- Create a user account on a Linux Server using the terminal window.
- Create a user account on a Linux Server using the GUI.

Exam Objectives:

The following exam objectives are covered in this module:

4.6 Given a scenario, implement and maintain identity and access management

- Provisioning/de-provisioning user accounts
- Permission assignments and implications

Implementation of Automation & Orchestration for Security Operations

Introduction
Objective

Welcome to the Implementation of Automation & Orchestration for Security Operations 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 - Creating automation scripts.

After completing this module, you should be able to:

- Create a Linux automation script.
- Create a basic PowerShell automation script.
- Create users using a script.

Exam Objectives:

The following exam objective is covered in this module:

4.7 Explain the importance of automation and orchestration related to secure operations

- Use cases of automation and scripting
- Benefits

Investigative Data Sources

Introduction
Objective

Welcome to the Investigative Data Sources 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 File Analysis

After completing this module, you should be able to:

- Analyze log files on a Linux device.
- Analyze log files on a Microsoft device.

Exam Objectives:

The following exam objective is covered in this module:

4.9 Given a scenario, use data sources to support an investigation.

- Log data
- Data sources

Mitigation Techniques

Introduction
Objective

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

Mitigation techniques are used to secure the enterprise environment. Concepts such as segmentation, access control, patching, encryption, configuration, and hardening keep the network protected. This module focuses on access control, encryption and monitoring through the process of hardening a network router.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 - Configure Router Access

- Exercise 2 - Harden Router Access
- Exercise 3 - Configure Router Logging

After completing this module, you should be able to:

- Review router configuration and create local credentials.
- Configure SSH remote access.
- Disable unused services.
- Restrict router access.
- Configure NTP.
- Configure and test logging.

Exam Objectives:

The following exam objectives are covered in this module:

2.5 Explain the purpose of mitigation techniques used to secure the enterprise

- Access control
- Encryption
- Monitoring
- Configuration enforcement
- Hardening techniques

4.1 Given a scenario, apply common security techniques to computing resources

- Hardening targets

4.4 Explain security alerting and monitoring concepts and tools

- Activities

4.5 Given a scenario, modify enterprise capabilities to enhance security

- Firewall