CompTIA Security X (Exam CAS-005), Skill Labs

Course Specifications

Course Number: ACI76-010SL_rev1.0
Lab Length: Approximately 15 hours

Governance, Risk, and Compliance (CAS-005)

Introduction
Objective

Welcome to the 5 Theory Labs for the 1.0 Governance, Risk, and Compliance portion of the CAS-005 Security X exam. While the other 14 labs in this CAS-005 SecurityX course are hands-on labs, these topics are Theory-based but still an important component to the passing the exam.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Reading 1 - Cybersecurity Governance
- Reading 2 -Risk Management
- Reading 3 -Compliance
- Reading 4 -Threat Modeling
- Reading 5 -Risks and Challenges of AI

After completing these five readings, students should be able to explain the foundational role of cybersecurity governance in aligning security initiatives with organizational goals. They should understand how to define clear roles, responsibilities, and policies that guide secure operations across the enterprise (Objective 1.1).

Students will also be equipped to identify, assess, and prioritize risks using formal risk management frameworks. They should recognize how to implement controls and mitigation strategies that balance security with business objectives (Objective 1.2).

Through the compliance reading, students should understand how legal and regulatory obligations influence security policies, decision-making, and resource allocation. They should be able to explain the importance of aligning information security strategies with compliance requirements to reduce organizational exposure (Objective 1.3).

In the threat modeling section, students will learn how to analyze systems and applications to identify potential threats and vulnerabilities. They should be able to map attack surfaces and apply threat modeling techniques such as STRIDE or DREAD in real-world scenarios (Objective 1.4).

Finally, students should be able to summarize the unique risks and challenges associated with the adoption of artificial intelligence (AI), including concerns around data privacy, algorithmic bias, and model security. This knowledge helps ensure informed decision-making when integrating AI into enterprise environments (Objective 1.5).

Implement a Resilient System Architecture (CAS-005)

Introduction
Objective

Welcome to the Implement a Resilient System Architecture lab. In this lab, 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:

- Section 1 – Preparing the Active Directory Environment
- Section 2 – Backing Up Active Directory
- Section 3 – Object Deletion
- Section 4 – Recovery

After completing these modules, you should be able to:

- Configure and prepare an Active Directory environment for backup and recovery.
- Perform a System State backup of Active Directory using built-in Windows Server tools.
- Simulate accidental deletion of Active Directory objects in a controlled lab environment.
- Recover deleted Active Directory objects using System State restore and authoritative recovery techniques.

Exam Objectives:

The following exam objective from Domain 2.0: Security Architecture is covered in this module:

Objective 2.1 – Given a scenario, analyze requirements to design resilient systems.

This module supports the objective by guiding learners through backup, recovery, and restoration exercises that demonstrate how to maintain system availability and integrity in the face of failures or security incidents.

Deploy an Automated Software Deployment Solution (CAS-005)

Introduction
Objective

Welcome to the Deploy an Automated Software Deployment Solution lab. In this lab, 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:

- Section 1 – What is a SIEM
- Section 2 – Deploying Software to the Windows Machines
- Section 3 – Verifying the Automated Installation

After completing these modules, you should be able to:

- Explain the role and function of a Security Information and Event Management (SIEM) system.
- Deploy SIEM agent software across Windows systems in a networked environment.
- Verify that the deployment was successful and that the agents are communicating with the SIEM server.

Exam Objectives:

The following exam objective from Domain 2.0: Security Architecture is covered in this module:

Objective 2.2 – Given a scenario, implement security in the early stages of the systems life cycle and throughout subsequent stages.

This module reinforces the importance of integrating security considerations during system planning, deployment, and maintenance to ensure a resilient and secure architecture from start to finish.

Implement a Vulnerability Management Solution (CAS-005)

Introduction
Objective

Welcome to the Implement a Vulnerability Management Solution lab. In this lab, 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:

- Section 1 – Installing OpenVAS
- Section 2 – Using the Nmap Vulnerability Scripts
- Section 3 – Installing Nessus

After completing these modules, you should be able to:

- Install and configure OpenVAS as a vulnerability scanning solution.
- Use Nmap scripts to identify vulnerabilities and misconfigurations on network hosts.
- Install and prepare Nessus, a commercial-grade vulnerability scanner, for use in security assessments.
- Understand the role of vulnerability scanners in identifying and mitigating potential security risks.

Exam Objectives:

The following exam objective from Domain 2.0: Security Architecture is covered in this module:

Objective 2.3 – Given a scenario, integrate appropriate controls in the design of a secure architecture.

This objective focuses on identifying and implementing the necessary security controls to ensure systems and infrastructure are designed with security integrated from the ground up.

Implement a Secure Access Control Solution (CAS-005)

Introduction
Objective

Welcome to the Implement a Secure Access Control Solution lab. In this lab, 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:

- Section 1 – Examining Insecure Methods of SSH
- Section 2 – Configuring Key-Only Based Authentication
- Section 3 – Testing Public Key Authentication

After completing these modules, you should be able to:

- Identify insecure SSH authentication practices and understand the associated risks.
- Configure SSH servers to use public key authentication instead of password-based logins.
- Successfully test and verify secure SSH connections using key-based authentication methods.

Exam Objectives:

The following exam objective from Domain 2.0: Security Architecture is covered in this module:

Objective 2.4 – Given a scenario, apply security concepts to the design of access, authentication, and authorization systems.

This module reinforces the objective by exploring secure methods for managing user identities and access, including implementing public key authentication, and configuring authentication systems in alignment with enterprise security best practices.

Deploy a Secure Cloud Storage Solution (CAS-005)

Introduction
Objective

Welcome to the Deploy a Secure Cloud Storage Solution lab. In this lab, 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:

- Section 1 – Installing MSSQL for SharePoint Sever
- Section 2 – Prerequisites SharePoint Sever Installer
- Section 3 – Installing Microsoft SharePoint Sever
- Section 4 – SharePoint Products Configuration Wizard

After completing these modules, you should be able to:

- Install and configure Microsoft SQL Server as the backend database for SharePoint.
- Identify and install the required prerequisites for a successful SharePoint Server deployment.
- Perform a full installation of SharePoint Server in a lab environment.

- Run the SharePoint Products Configuration Wizard to finalize the setup and establish initial configuration settings for Central Administration.

Exam Objectives:

The following exam objective from Domain 2.0: Security Architecture is addressed in this module:

Objective 2.5 – Given a scenario, securely implement cloud capabilities in an enterprise environment.

This module focuses on evaluating and implementing secure cloud solutions, including best practices for authentication, data protection, resource access control, and integration within a secure enterprise architecture.

Detect and Troubleshoot Authentication and Authorization Issues (CAS-005)

Introduction
Objective

Welcome to the Detect and Troubleshoot Authentication and Authorization issues lab. In this lab, 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:

- Section 1 – Local User Management
- Section 2 – Domain Accounts
- Section 3 – Detect and Troubleshoot Authentication and Authorization issues

After completing these modules, you should be able to:

- Manage local user accounts, including creation, deletion, and permission settings.
- Understand the structure and purpose of domain user accounts in an Active Directory environment.
- Create, modify, and manage domain user accounts using administrative tools.
- Distinguish between local and domain account scopes and apply best practices for account security.

Exam Objectives:

The following exam objective from Domain 3.0: Security Engineering is addressed in this module:

Objective 3.1 – Given a scenario, troubleshoot common issues with identity and access management (IAM) components in an enterprise environment.

This module provides hands-on experience and troubleshooting strategies for resolving common IAM-related challenges, including authentication failures, permission misconfigurations, and account management issues in enterprise settings.

Implement a Secure System Architecture Solution (CAS-005)

Introduction
Objective

Welcome to the Implement a Secure System Architecture Solution lab. In this lab, 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:

- Section 1 – Installing WSUS
- Section 2 – Configuring WSUS
- Section 3 – Configuring the Group Policy Settings

After completing these modules, you should be able to:

- Install and configure Windows Server Update Services (WSUS) on a Windows Server system.
- Configure WSUS synchronization settings and product/classification selections to manage updates for Windows clients.
- Approve and deploy updates from the WSUS console to domain-joined machines.
- Create and apply Group Policy Objects (GPOs) that direct client machines to use WSUS as their update source.
- Verify client connectivity to the WSUS server and confirm that update settings are being enforced via Group Policy.

Exam Objectives:

The following exam objective from Domain 3.0: Security Engineering is covered in this module:

Objective 3.2 – Given a scenario, analyze requirements to enhance the security of endpoints and servers.

This module supports that objective by demonstrating how to use WSUS and Group Policy to securely manage and control the distribution of updates across domain-joined servers and workstations, helping ensure systems are protected against known vulnerabilities.

Troubleshoot and Remediate Network Infrastructure Issues (CAS-005)

Introduction
Objective

Welcome to the Troubleshoot and Remediate Network Infrastructure Issues lab. In this lab, 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:

- Section 1 – Identifying Network Issues
- Section 2 – Fixing Internet Connection Issues
- Section 3 – Fixing DNS Issues in the Enterprise

After completing these modules, you should be able to:

- Diagnose common network issues using basic and advanced troubleshooting techniques.
- Resolve internet connectivity problems affecting individual systems or network segments.
- Identify and fix DNS-related issues that impact name resolution and domain functionality in enterprise environments.

Exam Objectives:

The following exam objective from Domain 3.0: Security Engineering is covered in this module:

Objective 3.3 – Given a scenario, troubleshoot complex network infrastructure security issues.

This module aligns with the objective by providing hands-on experience in diagnosing and resolving security-related problems within enterprise network environments, including connectivity, configuration, and DNS issues.

Implement an Automated Security Monitoring Solution (CAS-005)

Introduction
Objective

Welcome to the Implement an Automated Security Monitoring Solution lab. In this lab, 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:

- Section 1 – Connecting to the WAZUH Server (SIEM)
- Section 2 – Installing a Windows Agent
- Section 3 – Making an Agent Active
- Section 4 – Triggering an Alert

After completing these modules, you should be able to:

- After completing these exercises, you should be able to:
- Connect to and navigate the Wazuh SIEM interface.
- Install and configure a Wazuh agent on a Windows machine.
- Successfully register and activate an agent within the Wazuh platform.
- Generate and analyze alerts to validate agent functionality and event monitoring.

Exam Objectives:

The following exam objective from Domain 3.0: Security Engineering is covered in this module:

Objective 3.6 – *Given a scenario, use automation to secure the enterprise.*

This module supports the objective by demonstrating how automation tools and techniques can be used to improve the efficiency, consistency, and scalability of enterprise security operations.

Deploy a Secure Cryptographic Solution (CAS-005)

Introduction
Objective

Welcome to the Deploy a Secure Cryptographic Solution lab. In this lab, 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:

- Section 1 – Joining the Domain
- Section 2 – Domain Accounts
- Section 3 – Implementing BitLocker on Windows 11

After completing these modules, you should be able to:

- Join a Windows machine to an Active Directory domain.
- Create, manage, and troubleshoot domain user accounts.
- Configure BitLocker encryption on a Windows system and understand how to integrate it with enterprise tools like Group Policy and Active Directory for recovery key management.

Exam Objectives:

The following exam objective from Domain 3.0: Security Engineering is covered in this module:

Objective 3.8 – Given a scenario, apply the appropriate cryptographic use case and/or technique.

This module supports the objective by demonstrating how to implement encryption technologies like BitLocker, and by exploring the practical use of cryptographic techniques to protect data at rest in enterprise environments.

Implement a Security Information Event Management (SIEM) Enterprise Solution (CAS-005)

Introduction
Objective

Welcome to the Implement a Security Information Event Management (SIEM) Enterprise Solution lab. In this lab, 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:

- Section 1 – What is a SIEM
- Section 2 – Installing a Windows Agent
- Section 3 – Adding A Linux Agent

After completing these modules, you should be able to:

- Explain the purpose and function of a Security Information and Event Management (SIEM) system.
- Successfully install and configure a SIEM agent on a Windows machine.
- Add and verify a SIEM agent on a Linux system to enable centralized monitoring and log collection.

Exam Objectives:

The following exam objective from Domain 4.0: Security Operations is covered in this module:

Objective 4.1 – Given a scenario, analyze data to enable monitoring and response activities.

This module supports the objective by demonstrating how to collect, interpret, and act on system and network data using SIEM tools to enhance an organization's ability to detect and respond to security events.

Detect Vulnerabilities in an Enterprise Infrastructure (CAS-005)

Introduction
Objective

Welcome to the Detect Vulnerabilities in an Enterprise Infrastructure lab. In this lab, 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:

- Section 1 – Checking Security Status with PowerShell
- Section 2 – Using Lynis to Check Linux System Security
- Section 3 – Vulnerability Scanning with Nessus
- Section 4 – Vulnerability Scanning with OpenVAS

After completing these modules, you should be able to:

- Use PowerShell commands to assess and report on Windows system security status.
- Run Lynis to evaluate the security posture of a Linux system.
- Perform vulnerability scans with Nessus and interpret the results.
- Use OpenVAS to identify security weaknesses and generate reports for remediation planning.

Exam Objectives:

The following exam objective from Domain 4.0: Security Operations is covered in this module:

Objective 4.2 – Given a scenario, analyze vulnerabilities and attacks, and recommend solutions to reduce the attack surface.

This module supports the objective by guiding learners through vulnerability scanning, analysis of security findings, and the implementation of mitigation strategies to strengthen system defenses and minimize exposure to threats.

Investigate Threat-hunting Resources (CAS-005)

Introduction
Objective

Welcome to the Investigate Threat-hunting Resources lab. In this lab, 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:

- Section 1 – The Hacker Prepares an Attack
- Section 2 – Malicious Activity of an Insider
- Section 3 – Finding the Threat

After completing these modules, you should be able to:

- Understand the techniques and steps an external attacker may take to prepare and launch an attack.
- Recognize the signs and behaviors associated with insider threats and malicious internal activity.
- Use monitoring and analysis tools to identify, investigate, and respond to suspicious behavior within a networked environment.

Exam Objectives:

The following exam objective from Domain 4.0: Security Operations is covered in this module:

Objective 4.3 – Given a scenario, apply threat-hunting and threat intelligence concepts.

This module supports the objective by introducing key techniques in threat-hunting and demonstrating how to leverage threat intelligence to proactively detect, investigate, and respond to suspicious activities within an enterprise environment.

Malware Detection and Analysis (CAS-005)

Introduction
Objective

Welcome to the Malware Detection and Analysis lab. In this lab, 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:

- Section 1 – Creating the Malware Payload
- Section 2 – Basic Malware Analysis
- Section 3 – Deploying Malware

After completing these modules, you should be able to:

- Understand how simple malware payloads are created and packaged.
- Analyze basic malware behavior using sandboxing or static/dynamic analysis tools.
- Safely deploy and observe malware in a secure, controlled lab environment for educational or research purposes.
- Recognize the importance of containment, monitoring, and ethical boundaries in malware experimentation.

Exam Objectives:

The following exam objective from Domain 4.0: Security Operations is covered in this module:

Objective 4.4 – Given a scenario, analyze data and artifacts in support of incident response activities.

This module supports the objective by providing hands-on practice with identifying, interpreting, and correlating security data and digital artifacts to support effective incident detection, investigation, and response.