Certified Information Systems Security Professional (CISSP), Skill Labs

Course Specifications

Course Number: ACI76-036SL_rev1.0
Lab Length: Approximately 24 hours

Introduction to CISSP (ISC2-CISSP)

Introduction
Objective

The Introduction to CISSP module provides you with the information required to support your hands-on learning in the following topics:

- The 8 Domains of CISSP

Our Certified Information Systems Security Professional (CISSP) practice lab has been designed to provide you with practical examples that can be applied alongside reference books and materials. The CISSP exam is heavily theory driven and vendor neutral, which effectively means it doesn't specify any particular tool or operating system, rather it considers best practice and details numerous techniques which should be considered within an information technology environment towards data protection.

It is strongly recommended that you use these labs as a supplement alongside (and not limited to) a training course and/or books and reference materials.

The aim of this practice lab is to reinforce and complement learning and development and to highlight some key aspects of security practices to assist the learner with their revision towards their exam.

Overview
Exam Objectives

No exam objectives are covered in this lab.

Security and Risk Management (ISC2-CISSP)

Introduction
Objective

The Security and Risk Management module provides you with the information required to support your hands-on learning.

- Security and Risk Management Support Materials

Overview
Exam Objectives

The following exam objectives will be discussed in this document:

- Understand and apply concepts of confidentiality, integrity, and availability.
- Apply security governance principles.
- Compliance
- Understand legal and regulatory issues that pertain to information security in a global context.
- Understand professional ethics.
- Develop and implement documented security policy, standards, procedures, and guidelines.
- Understand business continuity requirements.
- Contribute to personnel security policies.
- Understand and apply risk management concepts.
- Understand and apply threat modeling.
- Integrate security risk considerations into acquisition strategy and practice.
- Establish and manage information security education, training, and awareness.

Encryption and Hashing (ISC2-CISSP)

Introduction

Objective

The Encryption and Hashing module provide you with the instructions and devices needed to develop your hands-on skills in the following topics:

- Cryptographic Basics
- Comparing Hashing Algorithms
- Comparing Hash Values

This module refers to the CISSP Asset Security domain. In order to fully understand this topic, please refer to your course material or use your favorite search engine to research this topic in more detail.

Overview
Exam Objectives:

The following exam objectives are covered in this lab:

- Determine data security controls (e.g., data at rest, data in transit)

SCCM Configuration Items and Baselines (ISC2-CISSP)

Introduction
Objective

The SCCM Configuration Items and Baselines module provides you with the instructions and devices to develop hands-on skills in the following topics:

- Creating a Windows Configuration Item for Compliance Settings in SCCM 2012
- Creating and Deploying a Configuration Baseline
- Importing Configuration Data in SCCM 20012

This module refers to the Certified Information Systems Security Professional (CISSP) Asset Security domain. In order to fully understand this topic, please refer to your course material or use your favorite search engine to research this topic in more detail.

Overview
Exam Objectives

The following exam objectives are covered in this lab:

- Protect privacy.
- Classify information and supporting assets (e.g., sensitivity and criticality).

Implement OpenPGP (ISC2-CISSP)

Introduction
Objective

The module Implementing OpenPGP provide you with the instructions and devices to develop your hands-on skills in the following topics:

- Installation of OpenPGP
- OpenPGP Certificate Creation and Distribution
- OpenPGP Signing and Importation
- OpenPGP Verification, Encryption, and Decryption

This module refers to the CISSP Security Engineering domain. In order to fully understand this topic, please refer to your course material or use your favorite search engine to research this topic in more detail.

Overview
Exam Objectives

The following exam objectives are covered in this lab:

- Implement and manage engineering processes using secure design principles.
- Understand the fundamental concepts of security models (e.g., confidentiality, integrity, and multi-level models)
- Apply cryptography.
- Apply secure principles to site and facility design.

Two Factor Authentication with SSH (ISC2-CISSP)

Introduction
Objective

The Two Factor Authentication with SSH module provide you with the instructions and devices to develop your hands-on skills in the following topics.

- Connecting to Win10 and Kali
- Configure Google Authenticator

This module refers to the CISSP Security Engineering domain. In order to fully understand this topic, please refer to your course material or use your favorite search engine to research this topic in more detail.

Overview
Exam Objectives

The following exam objectives are covered in this lab:

- Implement and manage engineering processes using secure design principles
- Understand the fundamental concepts of security models (e.g., confidentiality, integrity, and multi level models)
- Apply cryptography
- Apply secure principles to site and facility design
- Assess and mitigate the vulnerabilities of security architectures, designs, and solution

Implement SSL VPN using ASA Device Manager (ISC2-CISSP)

Introduction
Objective

The Implement SSL VPN using ASA device manager module provides you with the instructions and Cisco hardware to develop your hands-on skills in the following topics:

- Implement a Clientless SSL VPN using the Cisco ASA Device Manager
- Implement AnyConnect using the Cisco ASA Device Manager

This module refers to the Certified Information Systems Security Professional (CISSP) Communications and Network Security domain. In order to fully understand this topic, please refer to your course material or use your favorite search engine to research this topic in more detail.

Overview
Exam Objectives

The following exam objectives are covered in this lab:

- Apply secure design principles to network architecture (e.g., IP and non-IP protocols, segmentation).

- Secure network components.
- Design and establish secure communication channels.
- Prevent or mitigate network attacks.

Configure and Verify IPv4 and IPv6 Access Lists for Traffic Filtering (ISC2-CISSP)

Introduction
Objective

The Configure and verify IPv4 and IPv6 Access Lists for Traffic Filtering module provides you with the instructions and Cisco hardware to develop your hands-on skills in creating and applying access lists to routed interfaces. This module includes exercises that will cover the following topics:

- Configuring standard and extended access lists for IPv4
- Configure named access lists for IPv4
- Configuring and modifying IPv6 access lists

This module refers to the CISSP Communications and Network Security domain. In order to fully understand this topic, please refer to your course material or use your favorite search engine to research this topic in more detail.

Exam Objectives

The following exam objectives are covered in this lab:

- Apply secure design principles to network architecture (e.g., IP and non-IP protocols, segmentation)
- Secure network components
- Design and establish secure communication channels
- Prevent or mitigate network attacks

Configuring IPtables (ISC2-CISSP)

Introduction
Objective

The Configuring IPtables module provides you with the instructions and devices needed to develop your hands-on skills in the following topic:

- Linux IPtables.

This module refers to the CISSP Communications and Network Security domain. In order to fully understand this topic, please refer to your course material or use your favorite search engine to research this topic in more detail.

Exam Objectives

The following exam objectives are covered in this lab:

- Apply secure design principles to network architecture (e.g., IP & non-IP protocols, segmentation)

- Secure network components
- Design and establish secure communication channels
- Prevent or mitigate network attacks

Windows Command Line Tools (ISC2-CISSP)

Introduction
Objective

The Windows Command Line Tools module provides you with the instructions and devices to develop your hands-on skills in the following topics.

- IPconfig
- Netstat
- Ping
- Tracert and Route
- ARP and Whoami

From an internal perspective, we will use windows tools to investigate basic topology but also see in detail the services and processes happening within a windows system that are not directly visible without interrogation.

This module refers to the Certified Information Systems Security Professional (CISSP) Communications and Network Security domain. In order to fully understand this topic, please refer to your course material or use your favorite search engine to research this topic in more detail.

Overview
Exam Objectives

The following exam objectives are covered in this lab:

- Secure network components.

Administering and Deploying Endpoint Protection (ISC2-CISSP)

Introduction
Objective

The Administering and Deploying Endpoint Protection module provides you with the instructions and devices to develop hands on skills in the following topics:

- Create an Endpoint Protection site system role
- Configure alerts for Endpoint Protection
- Configure definition updates for Endpoint Protection
- Create and deploy antimalware policies for Endpoint Protection
- Configure custom client settings for Endpoint Protection
- Provision the Endpoint Protection client in a disk image

This module refers to the CISSP Communications and Network Security domain. In order to fully understand this topic, please refer to your course material or use your favorite search engine to research this topic in more detail.

Overview
Exam Objectives

The following exam objectives are covered in this lab:

- Apply secure design principles to network architecture (e.g., IP and non-IP protocols, segmentation)
- Secure network components
- Design and establish secure communication channels
- Prevent or mitigate network attacks

BitLocker on Portable Media (ISC2-CISSP)

Introduction
Objective

The BitLocker on Portable Media module provide you with the instructions and devices needed to develop your hands-on skills in the following topics.

- Configuring BitLocker on portable media.

This module refers to the CISSP Communications and Network Security domain. In order to fully understand this topic, please refer to your course material or use your favorite search engine to research this topic in more detail.

Exam Objectives

The following exam objectives are covered in this lab:

- Apply secure design principles to network architecture (e.g., IP and non-IP protocols, segmentation)
- Secure network components
- Design and establish secure communication channels
- Prevent or mitigate network attacks

Managing Remote Desktop (ISC2-CISSP)

Introduction
Objective

The Managing Remote Desktop module provide you with the instructions and devices needed to develop your hands-on skills in the following topics:

- Working with RDP
- Administering Windows with PowerShell Remoting

This module refers to the CISSP Communications and Network Security domain. In order to fully understand this topic, please refer to your course material or use your favorite search engine to research this topic in more detail.

Overview
Exam Objectives

The following exam objectives are covered in this lab:

- Apply secure design principles to network architecture (e.g., IP & non-IP protocols, segmentation)
- Secure network components
- Design and establish secure communication channels
- Prevent or mitigate network attacks

Manage Role-Based Security (ISC2-CISSP)

Introduction
Objective

The Manage Role-based Security module provides you with the instructions and devices needed to develop your hands-on skills in the following topics:

- Creating a custom security role and configuring security scope.
- Creating a user with administrative rights.
- Modifying administrative scope of an administrative user.

This module refers to the CISSP Identity and Access Management domain. In order to fully understand this topic, please refer to your course material or use your favorite search engine to research this topic in more detail.

Overview
Exam Objectives

The following exam objectives are covered in this lab:

- Control physical and logical access to assets.
- Manage identification and authentication of people and devices.
- Implement and manage authorization mechanisms.

Configuring MBSA Scanner (ISC2-CISSP)

Introduction
Objective

The Configuring MBSA Scanner module provides you with the instructions and devices to develop your hands-on skills in the following topics.

- Introduction to Microsoft Baseline Security Analyzer
- Implementing Recommendations

- Saving Microsoft Baseline Security Analyzer Reports
- Reviewing Configuration Changes

This module refers to the CISSP Security Assessment and Testing domain. In order to fully understand this topic, please refer to your course material or use your favorite search engine to research this topic in more detail.

Overview
Exam Objectives

- The following exam objectives are covered in this lab:
- Design and validate assessment and test strategies
- Conduct security control testing
- Collect security process data (e.g., management and operational controls)
- Analyze and report test outputs (e.g., automated, manual)
- Conduct or facilitate internal and third party audits
- Implement and support patch and vulnerability management

Compliance Patching (ISC2-CISSP)

Introduction
Objective

The Compliance Patching module provides you with the instructions and devices to develop your hands-on skills in the following topics:

- Install and Configure WSUS
- WSUS Server Certificates Security
- Create Computer Groups for WSUS
- Configure GPO Policy for WSUS

This module refers to the CISSP Security Assessment and Testing domain. In order to fully understand this topic, please refer to your course material or use your favorite search engine to research this topic in more detail.

Overview
Exam Objectives

The following exam objectives are covered in this lab:

- Conduct security control testing
- Collect security process data (e.g., management and operational controls)
- Implement and support patch and vulnerability management

Passive Topology Discovery (ISC2-CISSP)

Introduction
Objective

The Passive Topology Discovery module provides you with the instructions and devices needed to develop your hands-on skills in the following topics:

- Packet Capture with Wireshark
- Output Logs
- Packet Analysis Part 1
- Packet Analysis Part 2

This module refers to the CISSP Security Assessment and Testing domain. In order to fully understand this topic, please refer to your course material or use your favorite search engine to research this topic in more detail.

Overview
Exam Objectives

The following exam objectives are covered in this lab:

- Design and validate assessment and test strategies
- Conduct security control testing
- Collect security process data (e.g., management and operational controls)

Scanning and Remediating Vulnerabilities with OpenVAS (ISC2-CISSP)

Introduction
Objective

The module Scanning and Remediating Vulnerabilities with OpenVAS provide you with the instructions and devices needed to develop your hands-on skills in the following topics:

- OpenVAS Scanning
- Applying Windows Secure Updates
- Validating Security Changes with OpenVAS

This module refers to the CISSP Security Assessment and Testing domain. In order to fully understand this topic, please refer to your course material or use your favorite search engine to research this topic in more detail.

Overview
Exam Objectives

The following exam objectives are covered in this lab:

- Design and validate assessment and test strategies
- Conduct security control testing

- Collect security process data (e.g., management and operational controls)
- Analyze and report test outputs (e.g., automated, manual)
- Conduct or facilitate internal and third party audits
- Implement and support patch and vulnerability management

Installing Kali (ISC2-CISSP)

Introduction
Objective

The Installing Kali module provides you with the instructions and devices needed to develop your hands-on skills in the following topic:

- Installing Kali on Hyper-V

This module refers to the CISSP Security Operations domain. In order to fully understand this topic, please refer to your course material or use your favorite search engine to research this topic in more detail.

Overview
Exam Objectives

The following exam objectives are covered in this lab:

- Secure the provisioning of resources

Implement Backup and Recovery (ISC2-CISSP)

Introduction
Objective

The Implement Backup and Recovery module provides you with the instruction, and server hardware, to develop your hands-on skills in the defined topics.

This module includes the following exercises:

- View Disk Allocation Information to Review Storage Pool Data
- Create a Protection Group, Add Members, and Client Computers to a Protection Group

This module refers to the CISSP Security Operations domain. In order to fully understand this topic, please refer to your course material or use your favorite search engine to research this topic in more detail.

Exam Objectives

The following exam objectives are covered in this lab:

- Secure the provisioning of resources
- Understand and apply foundational security operations concepts
- Employ resource protection techniques
- Conduct incident management
- Operate and maintain preventative measures

Installation and Verification of Snort (ISC2-CISSP)

Introduction
Objective

The Installation and Verification of Snort module provide you with the instructions and devices to develop your hands-on skills in the following topics:

- Installation of Assistance Programs
- Configuring Snort
- Snort Verification and Results

This module refers to the CISSP Security Operations domain. In order to fully understand this topic, please refer to your course material or use your favorite search engine to research this topic in more detail.

Overview
Exam Objectives:

The following exam objectives are covered in this lab:

- Conduct logging and monitoring activities
- Conduct incident management
- Operate and maintain preventative measures

Configuring and Securing IIS (ISC2-CISSP)

Introduction
Objective

The module Configuring and Securing IIS will provide you with the instructions and devices to develop your hands-on skills in the following topics:

- IIS Setup
- IIS Platform Tour
- Inetpub Configuration

- IIS Configuration and Security Practices

Overview
Exam Objectives

The following exam objectives are covered in this lab:

- Secure the provisioning of resources
- Understand and apply foundational security operations concepts
- Employ resource protection techniques

Upgrading and Securing SSH Connection (ISC2-CISSP)

Introduction
Objective

The Upgrading and Securing SSH Security module provide you with the instructions and devices needed to develop your hands-on skills in the following topics:

- Connecting to Kali
- Upgrading OpenSSH
- Adding Sudo User
- Regenerate SSH Keys to Avoid Man-in -the-Middle (MITM) Attacks
- MOTD (Message of the Day)
- Change the SSH Port for Safety

This module refers to the CISSP Security Operations domain. In order to fully understand this topic, please refer to your course material or use your favorite search engine to research this topic in more detail.

Overview
Exam Objectives

The following exam objectives are covered in this lab:

- Employ resource protection techniques
- Operate and maintain preventative measures
- Implement and support patch and vulnerability management

DVWA - Manual SQL Injection and Password Cracking (ISC2-CISSP)

Introduction
Objective

The DVWA - Manual SQL Injection and Password Cracking module provides you with the instructions and devices needed to develop your hands-on skills in the following topics:

- DVWA Usage
- Performing an SQL Injection Attack
- Password Cracking with John

This module refers to the CISSP Software Development Security domain. In order to fully understand this topic, please refer to your course material or use your favorite search engine to research this topic in more detail.

Overview

Exam Objectives

The following exam objectives are covered in this lab:

- Assess the effectiveness of software security
- Assess security impact of acquired software