CompTIA PenTest+ (PT0-003), Skill Labs

Course Specifications

Course Number: ACI76-005SL_rev1.0
Lab Length: Approximately 11 hours

Penetration Testing Information Gathering Techniques (PT0-003)

Introduction
Objective

Welcome to the Penetration Testing Information Gathering Techniques lab. In this lab, you will be provided with the instructions and devices needed to develop your hands-on skills.

Overview

One of the first phases of a cybersecurity attack is gathering information about the target that the attacker wants to exploit. Information gathering can be done by passive or active reconnaissance. Passive reconnaissance is done by not directly engaging with the target and gathering information covertly without alerting the target. Active reconnaissance is conducted by interacting directly with the target, for example, network or port scanning.

In this lab, different active and passive reconnaissance techniques will be explored.

Learning Outcomes:

In this lab, you will complete the following exercises:

- Exercise 1 – Passive Reconnaissance Techniques
- Exercise 2 - Active Reconnaissance Techniques

After completing these modules, you should be able to:

- Gather information using passive reconnaissance techniques.
- Gather information using active reconnaissance techniques.

Exam Objectives:

The following exam objectives are covered in this lab:

2.1 Given a scenario, apply information gathering techniques.

Enumeration Tools and Techniques (PT0-003)

Introduction
Objective

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

Overview

After the initial active and passive reconnaissance of the network, the next step is to enumerate the discovered network resources. Several tools are available that can be used by a pentester.

In this lab, different tools and techniques will be explored to enumerate network resources.

Learning Outcomes:

In this lab, you will complete the following exercises:

- Exercise 1 – Enumerating Network Resources

After completing these exercises, you should be able to:

- Enumerate network resources.

Exam Objectives:

The following exam objectives are covered in this lab:

2.2 Given a scenario, apply enumeration techniques.

2.3 Given a scenario, modify scripts for reconnaissance and enumeration.

2.4 Given a scenario, use the appropriate tools for reconnaissance and enumeration.

Vulnerability Scanning Techniques (PT0-003)

Introduction
Objective

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

Overview

To ensure hosts on the network are secure a vulnerability scan needs to be performed on a regular basis to detect possible vulnerabilities and to prevent these vulnerabilities from being exploited.

In this lab, different tools and techniques will be used to conduct a vulnerability scan and interpret the discovered results.

Learning Outcomes:

In this lab, you will complete the following exercises:

- Exercise 1 – Vulnerability Scanning Techniques Using OpenVAS
- Exercise 2 – Vulnerability Scanning Techniques Using Nikto

After completing these exercises, you should be able to:

- Scan hosts for vulnerabilities using OpenVAS (Greenbone).
- Scan hosts for vulnerabilities using Nikto.

Exam Objectives:

The following exam objectives are covered in this lab:

3.1 Given a scenario, conduct vulnerability discovery using various techniques.
3.2 Given a scenario, analyze output from reconnaissance, scanning, and enumeration phases.

Conducting Network Attacks (PT0-003)

Introduction
Objective

Welcome to the Conducting Network Attacks lab. In this lab, you will be provided with the instructions and devices needed to develop your hands-on skills.

Overview

After the initial discovery and enumeration of network resources, the next phase of the attack is the exploitation of the discovered network resources.

In this lab, different techniques will be explored on how to exploit network resources.

Learning Outcomes:

In this lab, you will complete the following exercises:

- Exercise 1 – Techniques for Exploiting an FTP Serve
- Exercise 2 – Compromising Network Resources

After completing these exercises, you should be able to:

- Use different techniques to exploit an FTP server.
- Use different techniques to compromise network resources.

Exam Objectives:

The following exam objectives are covered in this lab:

4.2 Given a scenario, perform network attacks using the appropriate tools.

Conducting Authentication Attacks (PT0-003)

Introduction
Objective

Welcome to the Conducting Authentication Attacks lab. In this lab, you will be provided with the instructions and devices needed to develop your hands-on skills.

Overview

After an attacker has enumerated the network resources, the next phase is to attack and exploit the discovered resources.

In this lab, discovered network resources will be exploited.

Learning Outcomes:

In this lab, you will complete the following exercises:

- Exercise 1–Conducting an SMB Brute-Force Password Attack
- Exercise 2 – Conducting an RDP Brute-Force Password Attack

After completing these exercises, you should be able to:

- Conduct an SMB Brute-Force Attack.
- Conduct an RDP Brute-Force Attack.

Exam Objectives:

The following exam objectives are covered in this lab:

4.3 Given a scenario, perform authentication attacks using the appropriate tools.

Conducting Host-Based Attacks (PT0-003)

Introduction
Objective

Welcome to the Conducting Host-Based Attacks lab. In this lab, you will be provided with the instructions and devices needed to develop your hands-on skills.

Overview

After the attacker has harvested the credentials for the host, the next phase of the attack is to escalate the credentials and use these credentials to gather further information on the compromised network.

In this lab, a brute-force password attack will be conducted, and access to a remote host will be gained. Further information will be gained from the compromised system.

Learning Outcomes:

In this lab, you will complete the following exercises:

- Exercise 1 – Conducting a Brute-Force Password Attack
- Exercise 2 –Compromise a Remote Host

After completing these exercises, you should be able to:

- Conduct a brute-force password attack.
- Compromise a remote host.

Exam Objectives:

The following exam objectives are covered in this lab:

4.4 Given a scenario, perform host-based attacks using the appropriate tools.

Conducting Web Application Attacks (PT0-003)

Introduction
Objective

Welcome to the Conducting Web Application Attacks lab. In this lab, you will be provided with the instructions and devices needed to develop your hands-on skills.

Overview

In this lab, you will learn about the different types of application vulnerabilities and perform an exploitation of these vulnerabilities.

Learning Outcomes:

In this lab, you will complete the following exercises:

- Exercise 1 – Brute-Force Attack
- Exercise 2 – SQL Injection Attack

After completing these exercises, you should be able to:

- Conduct a brute-force attack.
- SQL injection attack.

Exam Objectives:

The following exam objectives are covered in this lab:

4.5 Given a scenario, perform web application attacks using the appropriate tools.

Performing a Social Engineering Attack (PT0-003)

Introduction
Objective

Welcome to the Performing a Social Engineering Attacks lab. In this lab, you will be provided with the instructions and devices needed to develop your hands-on skills.

Overview

Social engineering is the deliberate manipulation of people and the human psyche, tricking victims into releasing information or providing access to an organization.

In this lab, social engineering techniques will be used to harvest users' credentials.

Learning Outcomes:

In this lab, you will complete the following exercises:

- Exercise 1 – Social Engineering Using Phishing Attacks
- Exercise 2 - Simulating a Social Engineering Attack Using a USB Drop

After completing these exercises, you should be able to:

- Conduct social engineering attacks

Exam Objectives:

The following exam objectives are covered in this lab:

4.8 Given a scenario, perform social engineering attacks using the appropriate tools.

Automating Attacks Using Scripts (PT0-003)

Introduction
Objective

Welcome to the Automating Attacks Using Scripts lab. In this lab, you will be provided with the instructions and devices needed to develop your hands-on skills.

Overview

For automated tasks, scripts can be created and can be repurposed when a penetration test is being conducted.

In this lab, the creation of automated scripts and the use of PowerSploit scripts will be explored.

Learning Outcomes:

In this lab, you will complete the following exercises:

- Exercise 1 – Creating Automated Network Scan Scripts
- Exercise 2 – Exfiltrating Data Using PowerSploit

After completing these exercises, you should be able to:

- Create automated network scan scripts.
- Exfiltrate data using PowerSploit.

Exam Objectives:

The following exam objectives are covered in this lab:

4.10 Given a scenario, use scripting to automate attacks.

Compromising a System and Maintaining Persistence (PT0-003)

Introduction
Objective

Welcome to the Compromising a System and Maintaining Persistence lab. In this lab, you will be provided with the instructions and devices needed to develop your hands-on skills.

Overview

After the initial reconnaissance phase has been completed, the attacked will compromise the detected systems. The final phase of the attack is to maintain a persistent foothold on the compromised system.

In this lab, a system will be compromised and a persistent foothold will be gained.

Learning Outcomes:

In this lab, you will complete the following exercises:

- Exercise 1 – Compromising a System
- Exercise 2 – Maintaining Persistence on a Compromised System

After completing these exercises, you should be able to:

- Compromise a system.
- Maintain persistence on a compromised system.

Exam Objectives:

The following exam objectives are covered in this lab:

5.1 Given a scenario, perform tasks to establish and maintain persistence.

5.2 Given a scenario, perform tasks to move laterally throughout the environment.

Penetration Testing Management Engagement (PT0-003)

Introduction
Objective

Welcome to the Penetration Testing Management Engagement lab. In this lab, you will be provided with the instructions and devices needed to develop your hands-on skills.

Overview

Exam Objectives:

The following exam objectives are covered in this lab:

1.1 Summarize pre-engagement activities.

1.2 Explain collaboration and communication activities.

1.3 Compare and contrast testing frameworks and methodologies.

1.4 Explain the components of a penetration test report.

1.5 Given a scenario, analyze the findings and recommend the appropriate remediation within a report.