# IOT and Critical Infrastructure, Skill Labs

## Course Specifications

**Course Number:** ACI76-054SL_rev1.0
**Lab Length:** Approximately 3 hours

## IoT Hacking

### Introduction
### Objective

Welcome to the IoT Hacking Practice Lab. In this module, you will be provided with the information needed to develop your knowledge.

### Overview
### Learning Outcomes

In this module, you will complete the following exercises:

- Exercise 1 - Learn about different IoT Hacking Methods
- Exercise 2 - Preventing IoT Device Exploitation

In this module, you will complete the following exercises:

- Exercise 1 - Learn about different IoT Hacking Methods
- Exercise 2 - Preventing IoT Device Exploitation

### Exam Objectives

The following exam objective is covered in this lab:

- 4.2 Information Security Programs

**Note:** Our main focus is to cover the practical, hands-on aspects of the exam objectives. We recommend referring to course material or a search engine to research theoretical topics in more detail.

## Critical Infrastructure and IoT Lab 1

### Introduction
### Objective

Students will:

- Explore critical infrastructure/IoT devices.
- Examine network logs of critical infrastructure/IoT devices.

### Overview
### Learning Outcomes

Internet of Things, or IoT devices are connected to home and corporate networks. Typically these devices are not always secure and for that reason they can pose a threat to the security of your network as well as corporate networks. In this lab, we will scan and explore critical infrastructure/IoT devices.

| | Key Term | Description |
|---|---|---|
| 1 | IoT | Internet of Things (IoT) are devices connected to the Internet that are not traditional computers like Alexa, Google Home, Smart Thermostats, and other smart devices. |
| 2 | SCADA | Supervisory Control and Data Acquisition (SCADA) systems are used for controlling and monitoring industrial control systems. Think of power grid, solar panels, and other related devices. |
| 3 | SSH | Secure Shell (SSH) is a protocol that allows you to remoted connect to a device securely. |
| 4 | Log Analysis | The process of viewing entries in a system's logs to determine the type of activity |
| 5 | PuTTY | A GUI tool that is an SSH client which will allow machines to connect to SSH Servers. |

## Critical Infrastructure and IoT Lab 2

### Introduction
### Objective

Students will:

- Scan critical infrastructure devices for open ports.
- Examine critical infrastructure devices connection responses.

### Overview

Protecting the critical infrastructure of our country is vital to our nation's security. In 2022, there was a ransomware attack against the Colonial Pipeline that disrupted the gas supply in the Northeast. This lab examines using Kali Linux and some of its tools, including Metasploit, to perform a penetration test on a gas tank connected to a company's network.

| | Key Term | Description |
|---|---|---|
| 1 | IoT | Internet of Things (IoT) are devices connected to the Internet that are not traditional computers like Alexa, Google Home, Smart Thermostats, and other smart devices. |
| 2 | SCADA | Supervisory Control and Data Acquisition (SCADA) systems are used for controlling and monitoring industrial control systems. Think of power grid, solar panels, and other related devices. |
| 3 | Metasploit | A framework which has publicly available exploits for Windows, Linux, Cisco, and Mac systems. |
| 4 | Kali Linux | A version of Linux geared toward penetration testers. |

| | Key Term | Description |
|---|---|---|
| 5 | dirb | Directory Buster, or dirb, is a tool used to explore the security permissions of websites. |