Practice Labs - Ethical Hacker v10

IoT Hacking

Introduction

Ethical Hacking
IoT
Hacking Methods
Exploitation
OWASP

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

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

After completing this lab, you will have further knowledge of:

- OWASP Top 10 IoT Vulnerabilities
- Methods to prevent 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.

Lab Duration

It will take approximately **30 minutes** to complete this lab.

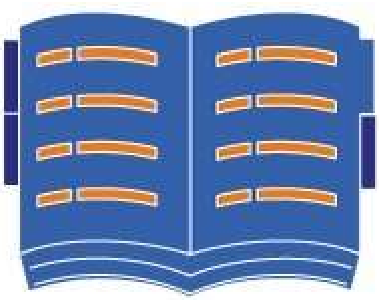
Help and Support

For more information on using Practice Labs, please see our **Help and Support** page. You can also raise a technical support ticket from this page.

Click **Next** to view the Lab topology used in this module.

Lab Topology

This lab contains supporting materials for Certified Ethical Hacker v10.



Click **Next** to proceed to the first exercise.

Exercise 1 - Learn About Different IoT Hacking Methods

IoT stands for the Internet of Things. IoT allows a device to be accessible on the Internet, just like a system or a mobile device. IoT devices can communicate with each other, as well as gather information that can be used for analysis. For example, a smartwatch could be used to track the number of hours of sleep and the number of steps taken by a person. The data can then be analyzed by the IoT device, for example, displaying the average number of hours of sleep and the average number of steps daily.

More recently, IoT devices are being used for different purposes. These include:

- Smart thermostats
- Medical devices
- Connected cars
- Activity trackers
- Smart refrigerators
- Parking sensors
- Medical sensors
- Smart security systems

Despite their popularity and extensive use, the security of IoT devices remains a concern. Some of the key issues are:

- Hardware hacking via exposed ports
- Extracting information from flash memory
- Access to the root terminal using exposed ports
- Use of vulnerable Application Programming Interface (API)
- Insecure authentication and authorization
- Web interface vulnerabilities
- Hardcoded credentials
- Unnecessary and insecure services running
- Sniffing information from the protocols, such as BLE and ZigBee

In this exercise, you will learn about the OWASP Top 10 IoT Vulnerabilities.

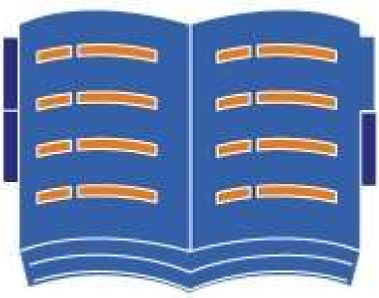
Learning Outcomes

After completing this exercise, you will have further knowledge of:

- OWASP Top 10 IoT Vulnerabilities

Your Devices

This exercise contains supporting materials for different IoT hacking methods.



Task 1 - OWASP Top 10 IoT Vulnerabilities

The Open Web Application Security Project (OWASP), has released the Top 10 IoT Vulnerabilities in 2018. While there are more vulnerabilities than just these, OWASP performs extensive research to bring out the major vulnerabilities and rank them. For example, weak, guessable, or hardcoded passwords has been on top of the list for many years. It is a known fact that ‘123456’ and ‘password’ are the most common passwords used worldwide.

Weak, guessable, or hardcoded passwords

The password used with the IoT device is weak or easily guessable. Some IoT devices have hardcoded passwords, which are used as backdoor access to the device’s firmware or the installed software.

Insecure network services

IoT devices can run unnecessary unsecure network services that are prone to an attack. If this happens, then the confidentiality, availability, and integrity of the information on the IoT device are at stake. The danger to the IoT devices increases when they are exposed to the network. There are websites available that will track these IoT devices for attackers to use, then conduct an attack.

Insecure ecosystem interfaces

IoT devices can be configured to use insecure web or mobile interfaces. There can also be an issue with an insecure application programming interface (API), which could lead to data compromise when the IoT device connects to the Internet and communicates with other devices. It is generally weak, or has no encryption being used. It could also be that there is a lack of authentication and authorization.

Lack of secure update mechanism

Some of the common issues with the secure update mechanism include:

- There are no or minimal updates to the IoT devices.
- Updates are not securely delivered to the IoT device. This can include sending the updates to the device without encrypting them. A man-in-the-middle attack can be conducted, and update can be modified.
- There are no or minimal security change notifications.

Use of insecure or outdated components

When an outdated software or operating system is being used, its vulnerabilities are known and can be exploited.

Insufficient privacy protection

IoT devices can store the user's personal information. For example, a smartwatch can store the user's health information. If the information is not encrypted, it can be hacked. The information must be securely stored with appropriate permissions.

Insecure data transfer and storage

Another issue about the information in the IoT devices is the lack of encryption, which is applicable for the data in storage (at rest), during processing, or while in transit.

At all times, the data must be secure and encrypted.

Lack of device management

IoT devices can also lack security while they are deployed with the users. The issue is also applicable for asset management, monitoring, and update management.

Insecure default settings

Just like mobile devices, IoT devices also come with the factory default settings. Most users do not know that the factory default settings can be compromised. Therefore, the IoT devices are used with their default settings which could allow a hacker to gain access. For example, each manufacturer uses a specific default password, which if not changed, can be accessed by any hacker that finds the device on the Internet.

Lack of physical hardening

Physical hardening is usually not performed on IoT devices. If it is not done, the hacker can gain control of the IoT device using various methods, such as remote access. The hacker can exploit services like Universal Plug and Play (UPnP) and User Datagram Protocol (UDP) and are prone to various attacks, such as buffer overflow, Denial of Service (DoS), and network device fuzzing. If an IoT device is not physically hardened, it can be exploited using a simple method, such as inserting a USB with malicious software. When malicious software is executed, it can provide access to the device and its data.

Exercise 2 - Preventing IoT Device Exploitation

IoT is a new technology that has surfaced and expanded greatly in recent years. It is predicted that by the year 2020, there will be 31 billion IoT devices on the Internet. With such a large number of devices, the number of attacks will also rise and it is crucial to use preventive measures for protection.

In this exercise, you will learn about some of the common methods to prevent IoT device exploitation.

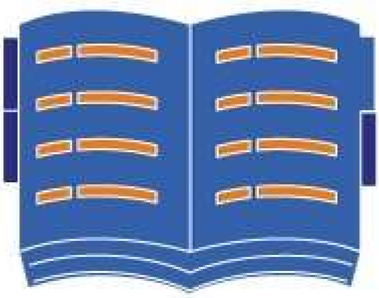
Learning Outcomes

After completing this exercise, you will have further knowledge of:

- Methods to prevent IoT device exploitation

Your Devices

This exercise contains supporting materials for preventing IoT device exploitation.



Task 1 - Methods to Prevent IoT Device Exploitation

Just like a normal system or mobile device, you need to protect IoT devices as well. It is critical for an IoT device to be protected before it is exploited by an attacker. There are several methods, similar to a system or a mobile device, that can be used to protect an IoT device.

Here is a list of methods that can be used to protect IoT devices:

- Update the firmware as and when required
- Block unnecessary open ports
- Disable Telnet, UPnP, and other vulnerable services
- Use encrypted communication
- Use a strong password
- Use two-factor authentication
- Use drive encryption
- Configure user account lockout
- Perform periodic device assessment
- Use the secure password recovery
- Configure two-factor authentication
- Use secure coding practices to develop IoT applications

Review

Well done, you have completed the **IoT Hacking** Practice Lab.

Summary

You completed the following exercises:

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

You should now have further knowledge of:

- OWASP Top 10 IoT Vulnerabilities
- Methods to prevent IoT device exploitation

Feedback

Shutdown all virtual machines used in this lab. Alternatively, you can log out of the lab platform