Exploitation Practice

This assignment is all about hands-on practice in the Exploitation Phase. I have located three great TryHackMe rooms, each focusing on important exploitation techniques we discussed. For this assignment, select either Options 1 or Option 2, depending on your specific area of interest.

Instructions

Choose Your Focus: Select between 'Option 1' or 'Option 2' based on your comfort level and interest in the topics. Please note that 'Option 1' contains two rooms. As 'Option 2' is a bit longer and more difficult, the other rooms have been combined to make it fair.

Complete the Room(s): Follow the instructions within the chosen room(s) to complete the exercises. Take your time to understand each concept and practice hands-on exploitation techniques. Use this opportunity to hone your skills in a safe environment.

Reflect: After completing the room, reflect on what you've learned. Consider the challenges you faced and how you overcame them. Identify the most intriguing aspects and areas where you'd like to delve deeper.

Room Options

Option 1: Metasploit Framework (Easy)

Metasploit: Introduction
https://tryhackme.com/room/metasploitintro

Gain an introduction to the main components of the Metasploit Framework. Explore the basics of Metasploit, including its main components such as Auxiliary, Encoders, Evasion, Exploits, NOPs, and Payloads. Familiarize yourself with msfconsole and working within these modules.

AND

Metasploit: Meterpreter
https://tryhackme.com/room/meterpreter

Take a deep dive into Meterpreter and discover how in-memory payloads can be used for post-exploitation. Learn about Meterpreter's different flavors, commands, and engage in post-exploitation challenges that provide a preview of upcoming Post-Exploitation Phase.

Option 2: SQL Injection (Medium)

SQL Injection
https://tryhackme.com/room/sqlinjectionlm

Learn how to detect and exploit SQL Injection vulnerabilities. Dive into the world of databases, SQL, and various types of SQL Injection attacks, including In-Band, Blind, and Out-of-Band SQLi. Understand the importance of remediation strategies to secure databases.

Happy hacking!