

# **Vulnerability Scanning and Penetration Testing**

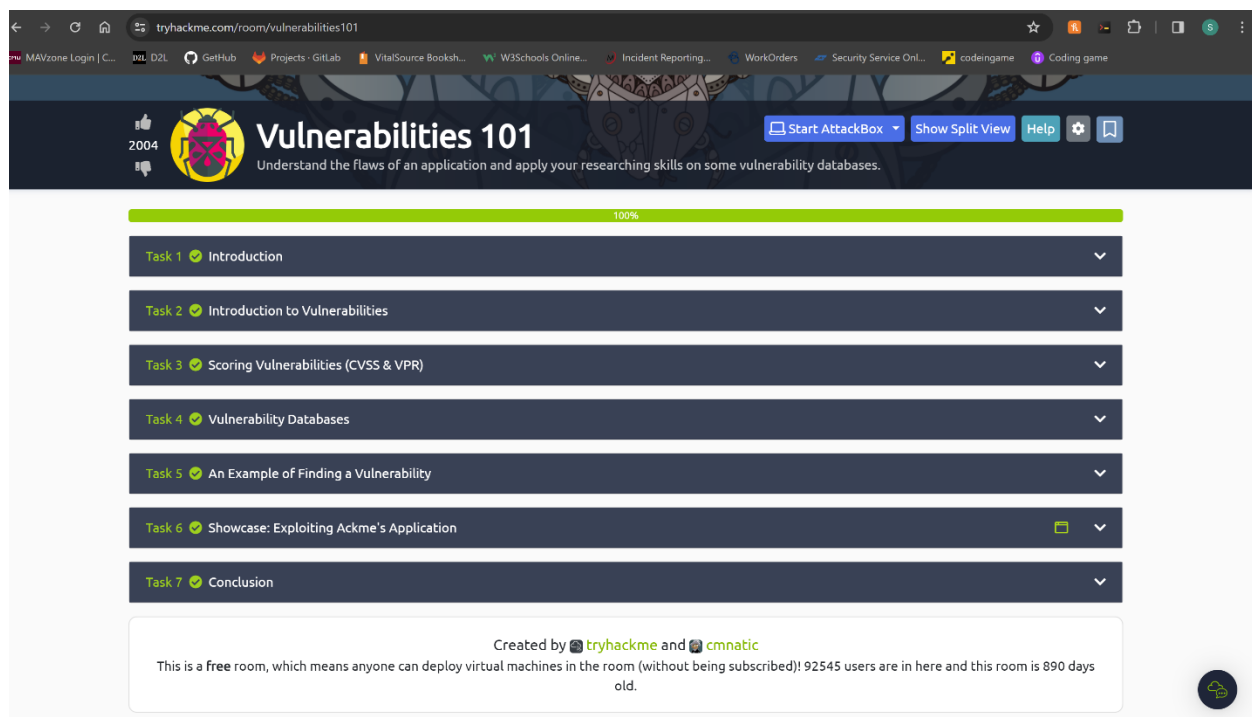
**By Sebastian Medina**

## **Contents:**

- 1. Vulnerability 101**
- 2. Pentesting Fundamentals**
- 3. Metasploit: Introduction**

# 1. Vulnerability 101

The goal of this module is to explain what exactly a vulnerability and the different types of vulnerabilities. To start of the module, it explains that a vulnerability in cybersecurity is a weakness or flaw in the design, implementation or behaviors of a system or application. In this module it also various types of vulnerabilities like operating system, (Mis)Configuration-based, Weak or Default Credentials, Application Logic, and Human-Factor. Lastly in this Module it went over Vulnerability databases like NVD or Exploit-DB. Vulnerability databases are used to look up existing vulnerabilities discovered in an application. This module accomplished its goal of being a introductory to vulnerability research and skills.



## 2. Pentesting Fundamentals

In this module you learn what Penetration Testing (Pentesting) is, the ethics of pentesting, and the methodologies of pentesting. The module starts with explaining that a pentest is an attempt to test and analyze the security defenses to protect their assets. In simpler terms you look for vulnerabilities for somebody's application and then rank how severe it is to the company. When it comes to hacking into something legally there you must consider the ethics in it. For example, before you hire someone to start hacking your applications right away you first must have a meeting to go over the Rules of Engagement so that the hacker knows what is allowed and what is not. Lastly in this module it talks about methodologies in pentest and how the steps you take to complete a pentest. The steps are Information Gathering, Enumeration/Scanning, Exploitation, Privilege Escalation, and lastly post-exploitation. This module shows you the first things you need to know about pentesting.

The screenshot shows a web browser window with the URL `tryhackme.com/room/pentestingfundamentals`. The browser's address bar and tabs are visible at the top. The main content area features a dark-themed header with the 'tryhackme' logo and navigation links like 'Dashboard', 'Learn', 'Compete', and 'Other'. A large banner image depicts a person at a computer with glowing green circuitry. Below the banner, the room title 'Pentesting Fundamentals' is displayed with the subtitle 'Learn the important ethics and methodologies behind every pentest.' A progress bar at the top of the task list shows 100% completion. The task list contains five items, each with a green checkmark and a dropdown arrow:

- Task 1: What is Penetration Testing?
- Task 2: Penetration Testing Ethics
- Task 3: Penetration Testing Methodologies
- Task 4: Black box, White box, Grey box Penetration Testing
- Task 5: Practical: ACME Penetration Test

At the bottom of the interface, a message states: 'Created by tryhackme and cmnatic. This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 304104 users are in here and this room is 900 days old.' A small circular icon with a green plus sign is located in the bottom right corner.

### 3. Metasploit: Introduction

Within this module it explains that Metasploit is a powerful tool that facilitates the exploitation process. This process comprises three main steps: finding the exploit, customizing the exploit, and the vulnerable service. Metasploit has many modules that help throughout the exploitation process. This room does a great job at showing you the basics of Metasploit and their respective use.

The screenshot shows the tryhackme.com interface for a room titled "Metasploit: Introduction". The browser address bar shows the URL "tryhackme.com/room/metasploitintro". The top navigation bar includes links for "Dashboard", "Learn", "Compete", and "Other", along with a "Go Premium" button and a user profile icon. The room title "Metasploit: Introduction" is prominently displayed, with a subtitle "An introduction to the main components of the Metasploit Framework." Below the title, a list of tasks is shown, each with a green checkmark indicating completion:

- Task 1 ✓ Introduction to Metasploit
- Task 2 ✓ Main Components of Metasploit
- Task 3 ✓ Msfconsole
- Task 4 ✓ Working with modules
- Task 5 ✓ Summary

At the bottom, a note states: "Created by tryhackme and am03bam4n. This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 177886 users are in here and this room is 886 days".