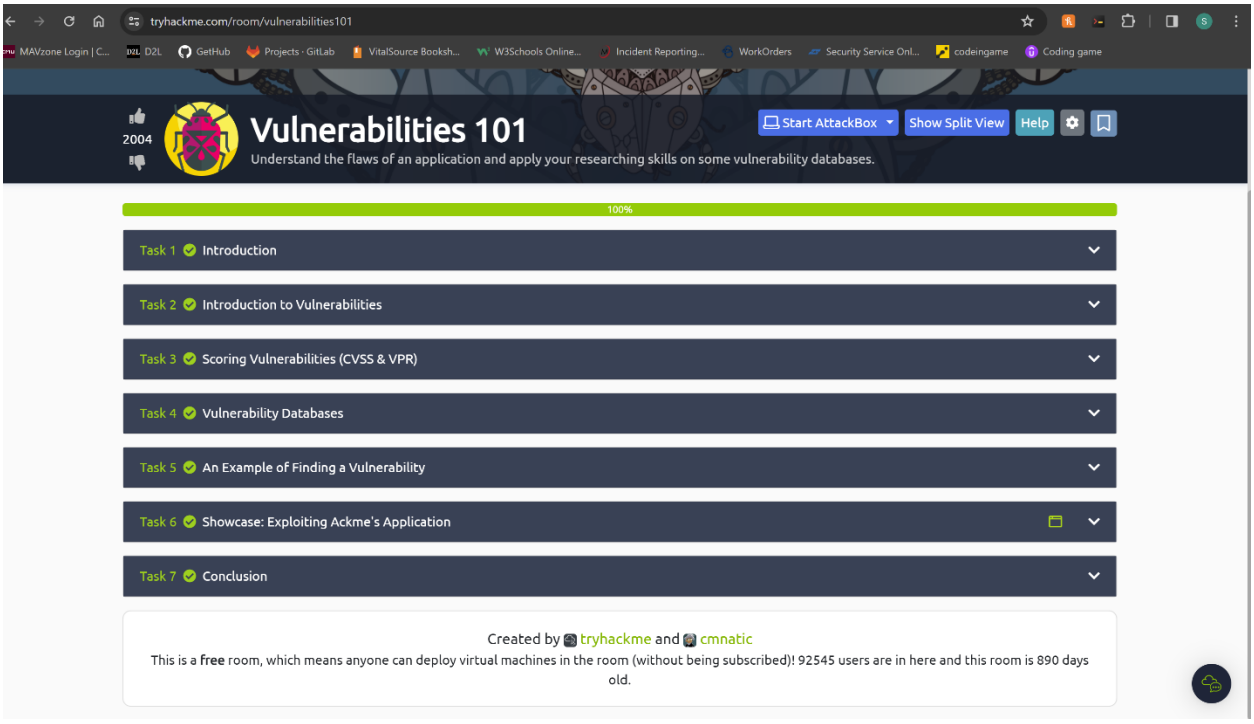
Vulnerability Scanning and Penetration Testing

By Sebastian Medina

Contents:

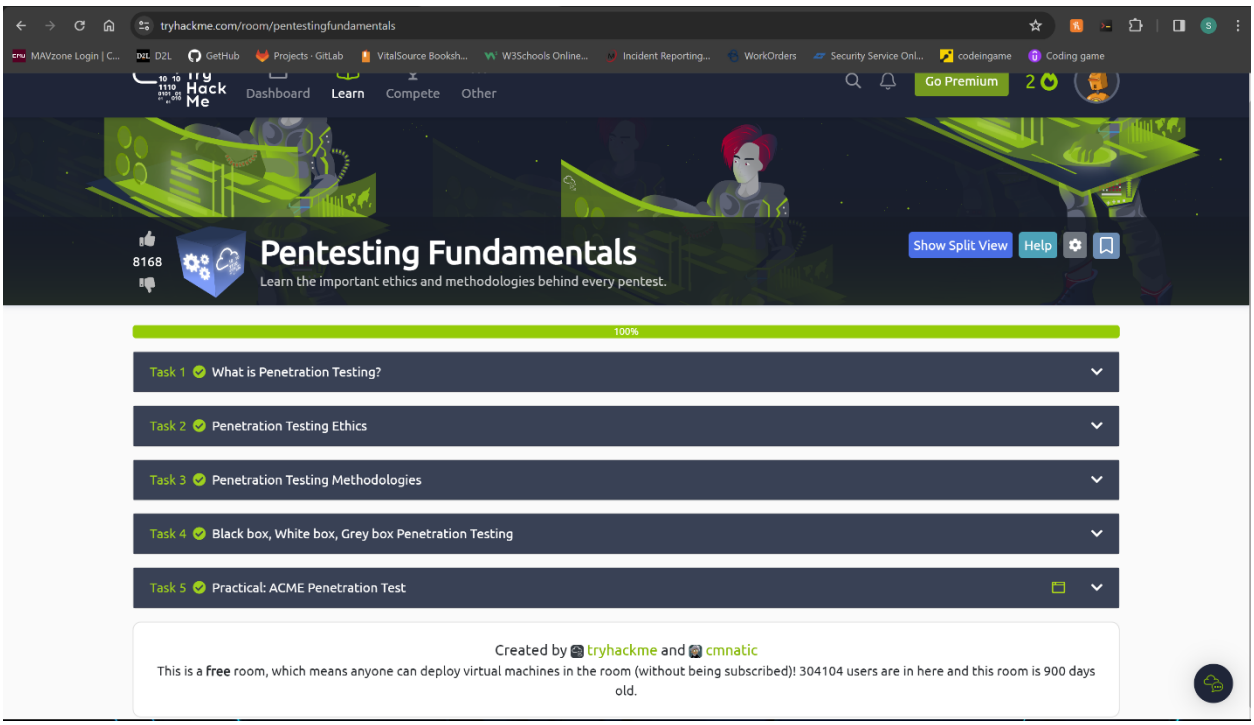
1. Vulnerability 101

The goal of this module is to 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.



3. Metasploit: Introduction

Within this module it explains that Metasploit is a powerful tool that facilitates the exploration 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.