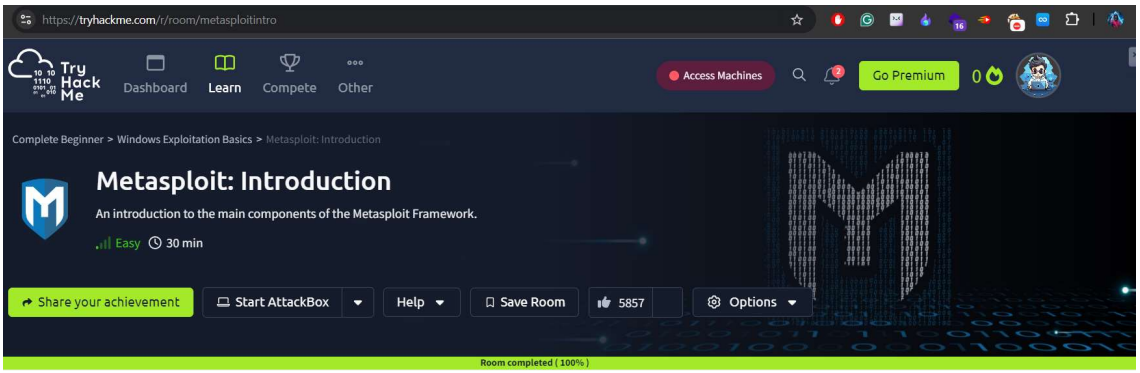
Internship Assignment Report: Cyber Security and Digital Forensics

Assignment 10: Metasploit

- **TryHackMe Rooms:**
    - Metasploit: Introduction

Try Hack Me Account:



1. Introduction

As part of my internship, I explored the Metasploit framework through a TryHackMe lab. Metasploit is a versatile tool that simplifies the exploitation process, and the lab focused on introducing its core components and usage. This report captures my experience and key takeaways from working through the room.

2. Overview of Metasploit

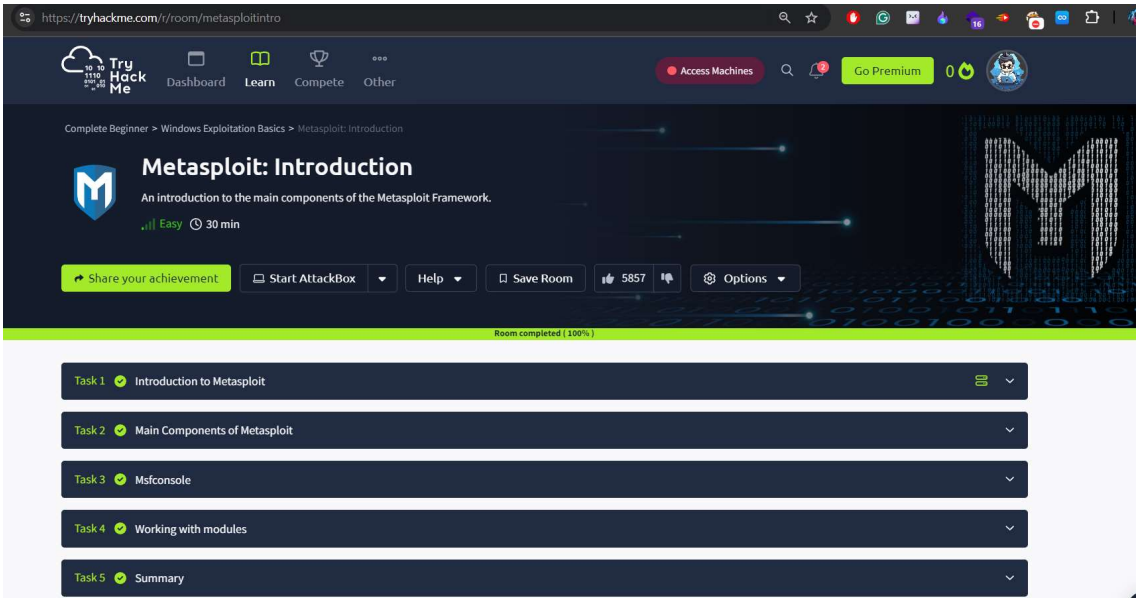
The exploitation process with Metasploit generally follows three main steps:

1. Finding the exploit – This involves scanning the target and identifying a suitable exploit that matches the vulnerability.
2. Customizing the exploit – Here, I adjusted parameters like the target IP address to ensure the exploit could work effectively.
3. Exploiting the vulnerable service – Once everything was set, I used the exploit to gain access to the target system.

Metasploit makes each of these steps more efficient by offering several modules, saving time compared to manual exploitation.

3. Practical Example: Using MS17-010 (EternalBlue)

In the lab, I applied the ms17_010_eternalblue exploit to gain access to a virtual machine (VM). This exploit targets a well-known vulnerability in SMB services on older Windows systems. When configured correctly, it allows remote code execution on the target machine. Working through this, I was able to see how Metasploit simplifies even complex attacks like EternalBlue.



4. Key Takeaways

Here are some of the things I learned during this lab:

- I became familiar with the basic components of Metasploit and how they fit together.
- I understood how to search for and run exploits against vulnerable services.
- It gave me hands-on practice with configuring an exploit to target a specific system successfully.