Cybersecurity internship assignment report

Name: Sneha Madhukar Devkate

Program: Digisuraksha Parhari Foundation Internship

Issued by: Digisuraksha Parhari Foundation

Supported by: Infinisec Technologies Pvt . Ltd.

Report submission date: 18 April 2025

Room Name: hello world

- Learning Objective

  This room helped me understand how TryHackMe works. It was like a warm-up session for beginners. It showed me how to open rooms, read the tasks, and submit answers.

- Key Tools/Commands Used

  No tools or coding needed.

  I just used the TryHackMe website and followed the instructions.

- Concepts Learned

  How to use TryHackMe rooms.

  How to start and stop machines.

  How to submit flags (answers).

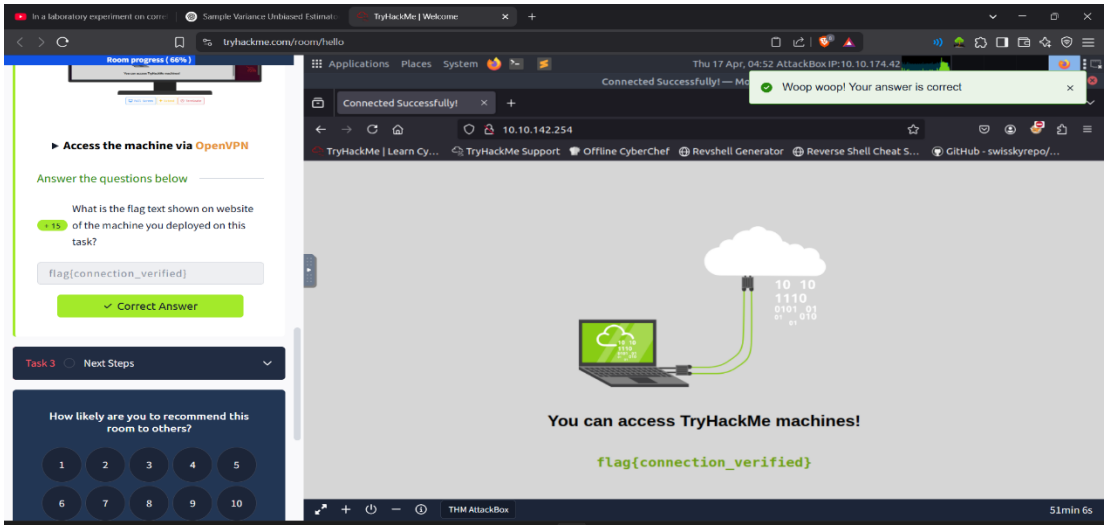
  How each room is divided into small tasks.

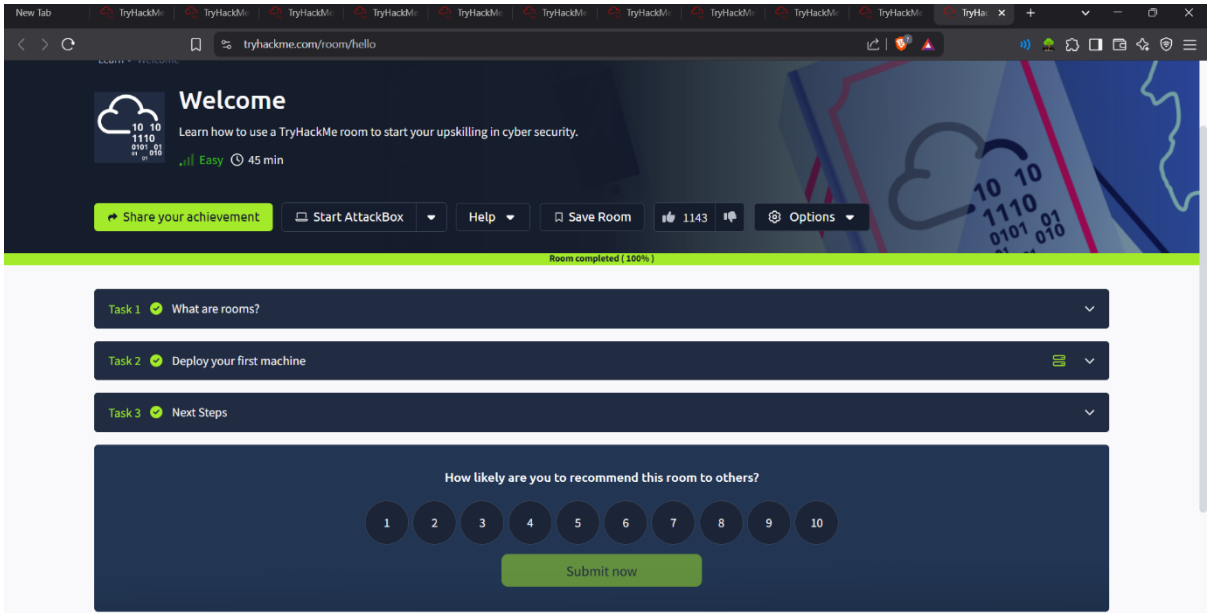
- Walkthrough / How I Solved It

  I started the room and clicked the "Start Machine" button. I read the given content and followed the steps. There were some basic questions at the end of each task. I answered them by understanding the instructions. It was simple and didn’t need any technical knowledge.

- Reflections or Notes

  This was my first TryHackMe room, and it was very helpful. Everything was easy to understand. I learned how to move forward in the platform and now I feel more confident to explore other rooms.





Room name: how to use tryhackme

- Learning objective

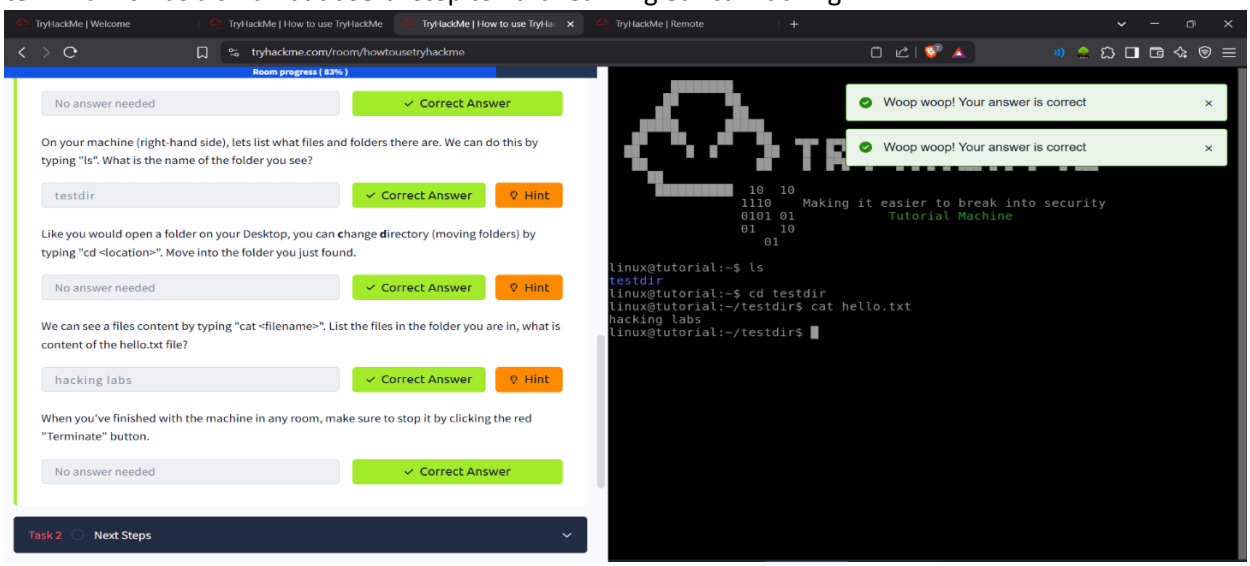
help users understand the platform's structure, features, and navigation. It provides a step-by-step guide to effectively use TryHackMe for learning cybersecurity, completing tasks, and engaging with interactive labs—whether through the in-browser AttackBox or by connecting with OpenVPN.

- Key tools/commands used
  1.TryHackMe Dashboard: Explored core sections like Learn, Practice, Compete, and
  2.Networks. AttackBox: Used the built-in virtual machine for hands-on labs without needing an external setup.
  3.OpenVPN Configuration: Learned how to securely connect to TryHackMe's network from a personal machine.
  4. Basic Terminal Commands : e.g., cd, cat etc

- Concept learned
  1. Platform Features- Overview of TryHackMe's key areas: learning paths, rooms, challenges, and leaderboards. Gamified learning with points, streaks, and ranks.
  2. Room Navigation- How to join a room, navigate through tasks, and submit answers.o Differences between types of rooms: walkthroughs, challenges, and tutorials.
  3. Hands-On Practice- Using the AttackBox for in-browser hacking. Setting up and connecting a personal VM using OpenVPN for full control.

- Walkthrough
  I started the virtual machine. Then I typed ls to see what files are there. After that, I used cd to go inside folders. I also used cat to read what's written in a file. Finally, I shut down the machine using the Terminate button.

- Notes
  I really enjoyed learning these simple commands. I now feel more confident about using the terminal. It was a small but useful step toward learning ethical hacking.



Room name: getting started

- Learning Objective

This room taught me how hackers can take advantage of weak websites. I learned to check a page's code and try default login usernames and passwords.

- Key Tools/Commands Used

  Web browser (Firefox in TryHackMe AttackBox)

  Right-click → View Page Source

  Login page with username and password

- Concepts Learned

  How to find hidden links in website code

  How weak passwords like "admin" can be dangerous

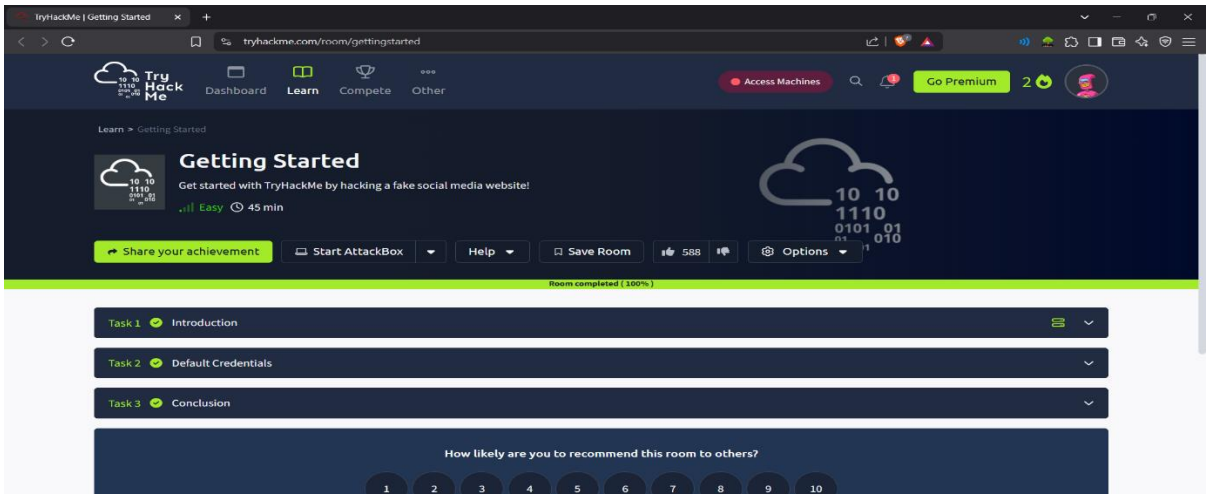
  Why website security is so important

- Walkthrough / How I Solved It

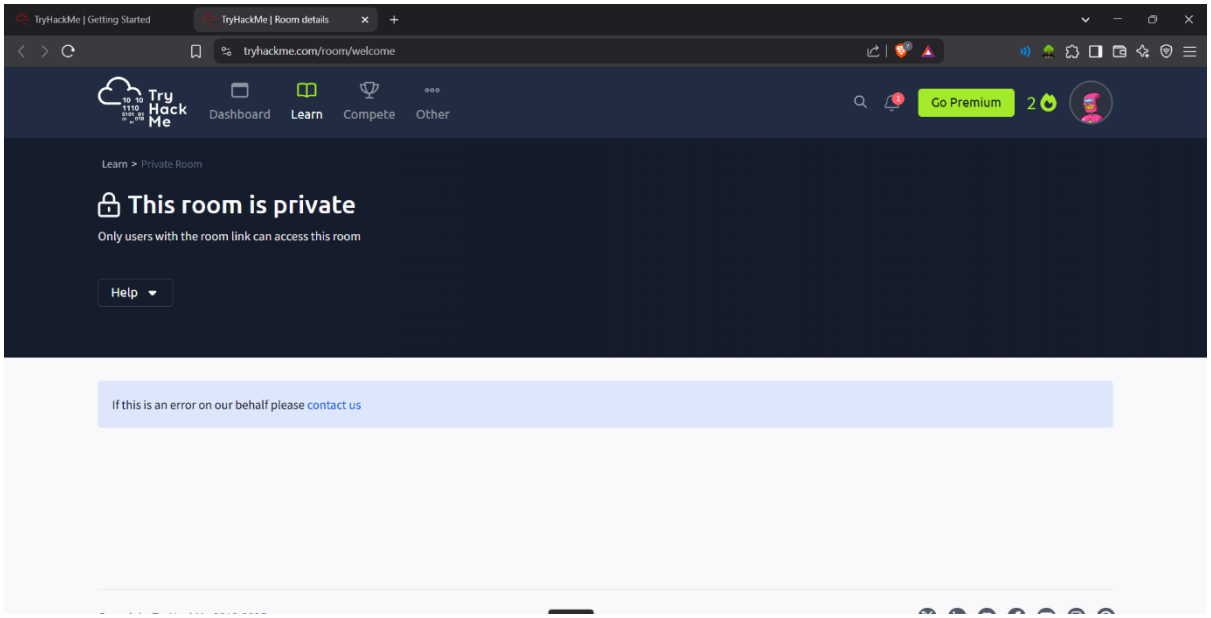
  I opened the target website in Firefox and checked its page source. I found a hidden link to the admin page. On the login page, I tried admin:admin and it worked! I then saw the user dashboard and completed the tasks.

- Reflections or Notes

  This was a fun and exciting room. It showed me how even small mistakes in websites can let hackers in. I'm now more curious to learn how to protect websites better.



Room name: welcome



Room name: Tryhackme tutorial

- Learning Objective

  To learn how to use the TryHackMe AttackBox and submit flags in CTF-style rooms.

- Key Tools/Commands Used

  TryHackMe AttackBox

  Firefox browser inside the AttackBox

  The concept of “flags” as answers

- Concepts Learned

  How to open and control the AttackBox

  How to connect to a machine and look for answers

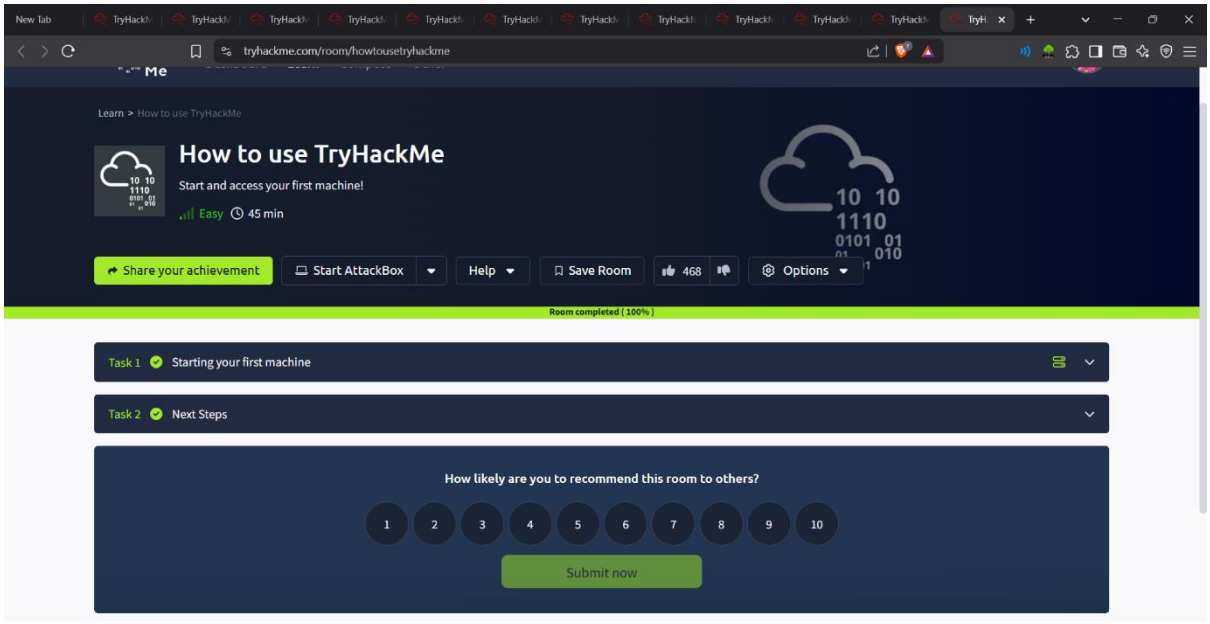
  What a flag is and how to submit it.

- Walkthrough / How I Solved It

  I launched both the AttackBox and the target machine. Then I copied the IP and opened it in Firefox. The flag was shown on the page. I copied and pasted it in the answer box.

- Reflections or Notes

It was a very helpful room to understand the whole TryHackMe system. Now I know how to use machines and complete tasks.



Room name: OpenVPN configuration

- Learning Objective
  To teach users how to securely connect to TryHackMe labs using OpenVPN.

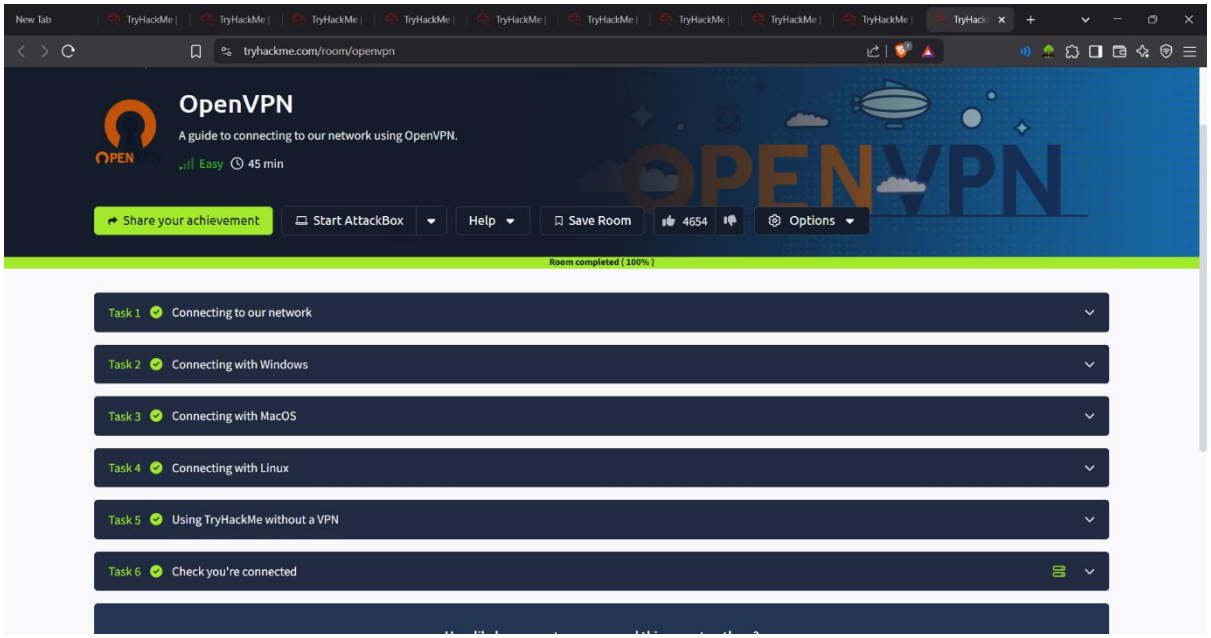
- Key Tools Used
  OpenVPN VPN Configuration File (.ovpn) Terminal/Command Prompt .

- Concepts Learned
  Downloading VPN config from TryHackMe Connecting to labs using OpenVPN Verifying successful connection.

- Walkthrough Summary
  Downloaded .ovpn file from dashboard Connected via terminal: Checked connectivity Completed tasks based on successful setup .

- Notes

Essential for users not using AttackBox Secure and stable method to access labs from your own machine.



Room name: beginner path introduction

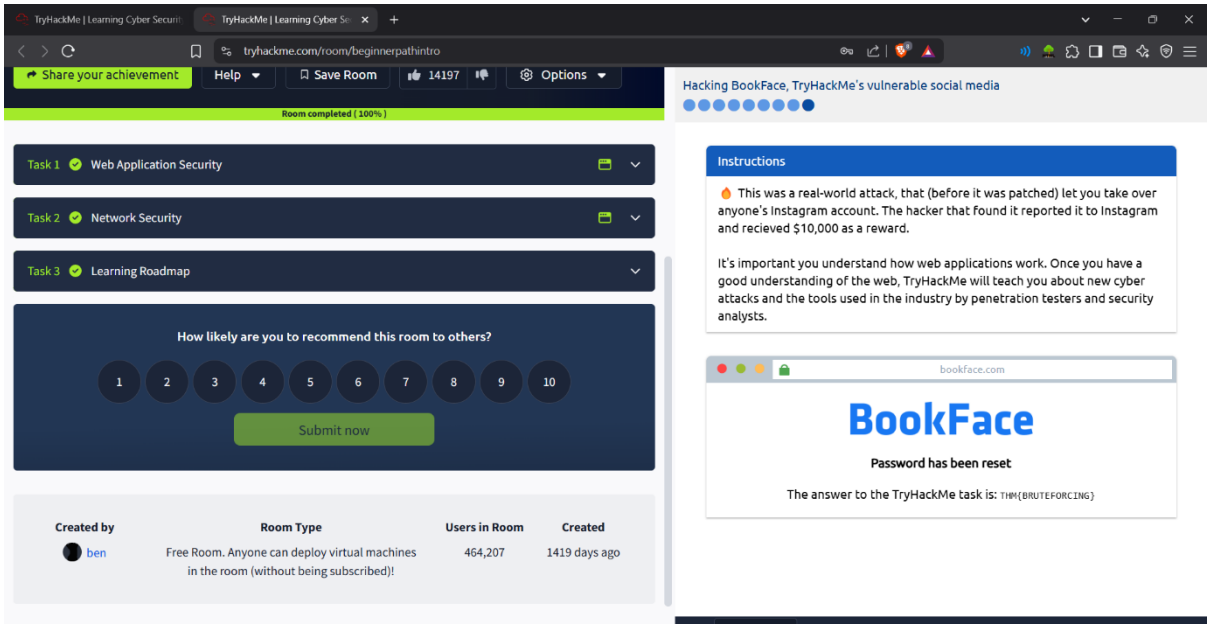
- Learning Objective
  To learn what the Beginner Path is and how it helps new students like me.

- Key Tools/Commands Used
  Browser
  TryHackMe interface only

- Concepts Learned
  TryHackMe has a learning path with many beginner rooms
  Each room teaches something new
  The path is made to go step-by-step from easy to hard

- Walkthrough / How I Solved It
  I opened the room and read all the content. I explored the suggested rooms and clicked on the links to learn what each one teaches.

- Reflections or Notes
  It gave me a good map of how to learn. I now have a clear plan to follow on TryHackMe.



Room name: starting out in cyber security

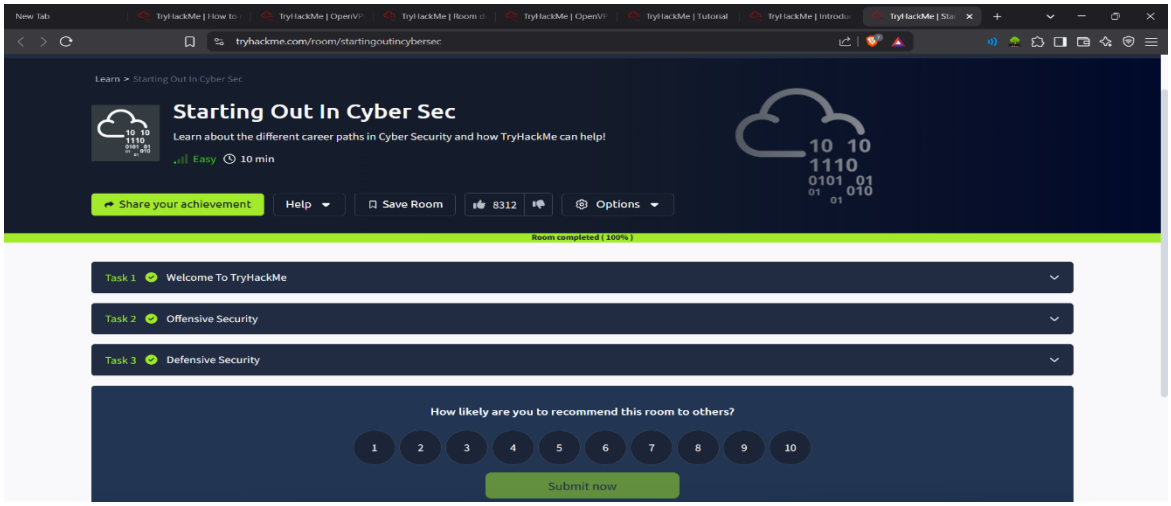
- Learning Objective
  Learn about the two sides of cybersecurity: Red Team and Blue Team, and figure out which one suits me better.

- Key Tools/Commands Used
  None
  Just explored career paths and room links

- Concepts Learned
  Red Team does ethical hacking and testing
  Blue Team protects systems and investigates attacks
  Different skills are needed for each team

- Walkthrough / How I Solved It
  I read about both teams. I checked out suggested learning paths like SOC Level 1 and Beginner Path. I learned about tools like Splunk and Volatility.

- Reflections or Notes
  This room helped me think about my future career in cybersecurity. I liked the Blue Team work more but will explore both sides.



Room name: introduction to research

- Learning Objective
  Learn how to research cybersecurity topics and find information about vulnerabilities.

- Key Tools/Commands Used
  Google
  CVE databases
  ExploitDB
  man command in Linux
  searchsploit tool

- Concepts Learned
  How to search smartly using Google
  What CVEs are and how to read them
  How to find vulnerabilities in software

- Walkthrough / How I Solved It
  I searched for cybersecurity terms using Google. I looked for known exploits in ExploitDB. I also learned to use Linux manual pages for learning new commands.

- Reflections or Notes
  This room taught me how important research is. I feel more confident now to find answers online when I'm stuck.

Task 1 Introduction

Task 2 Example Research Question

Task 3 Vulnerability Searching

Task 4 Manual Pages