ROOM 1:

🧩 **Room Name**: Hello World

🔗 **Link**: TryHackMe | Welcome

🎯 Learning Objective

- Familiarize yourself with the TryHackMe platform's interface and navigation.
- Understand the structure of cybersecurity learning paths.
- Set up and configure the TryHackMe AttackBox for hands-on practice.

🛠 Key Tools/Commands Used

- **TryHackMe AttackBox**: A pre-configured virtual machine provided by TryHackMe for safe and isolated practice.
- **Web Browser**: For navigating the TryHackMe platform and accessing resources.

🧠 Concepts Learned

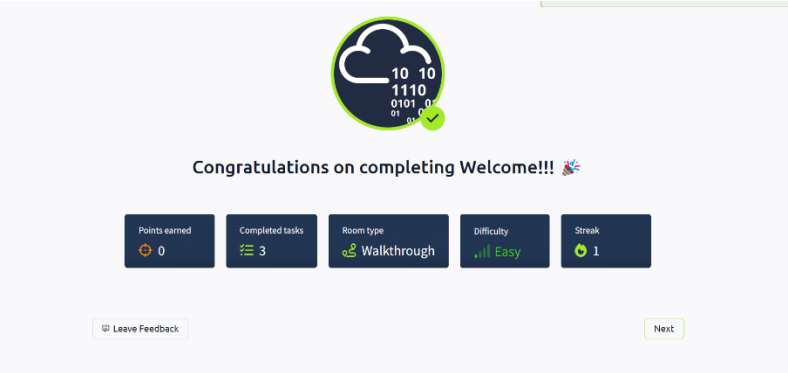
- **TryHackMe Interface**: Gained an understanding of the layout and features of the TryHackMe platform.
- **Room Structure**: Learned how rooms are organized and the progression of tasks within each room.
- **Basic Cybersecurity Terminology**: Introduced to fundamental terms and concepts in cybersecurity.

🥏 Walkthrough / How You Solved It

1. Account Setup: Created a TryHackMe account and logged in.
2. Room Navigation: Accessed the "Hello World" room from the dashboard.
3. Task Completion: Followed the guided instructions to complete the introductory tasks.
4. AttackBox Setup: Launched and configured the AttackBox for subsequent labs.

💡 Reflections or Notes

- The "Hello World" room serves as an excellent introduction to the TryHackMe platform.
- It provides a user-friendly environment to get accustomed to cybersecurity concepts.
- Looking forward to exploring more technical rooms in the learning path.



ROOM2:

🧩 **Room Name**: How to Use TryHackMe

🔗 **Link**: https://tryhackme.com/room/howtousetryhackme

🎯 **Learning Objective**

- Learn how to effectively navigate and utilize the TryHackMe platform.
- Understand how to start and interact with virtual machines (VMs) within TryHackMe.
- Familiarize yourself with the process of connecting to TryHackMe's network using OpenVPN.

🛠 **Key Tools/Commands Used**

- **TryHackMe Dashboard:** For accessing and managing rooms and machines.
- **AttackBox:** A web-based machine provided by TryHackMe for attacking other machines**.**
- **OpenVPN:** A VPN service used to securely connect to TryHackMe's network.

🧠 **Concepts Learned**

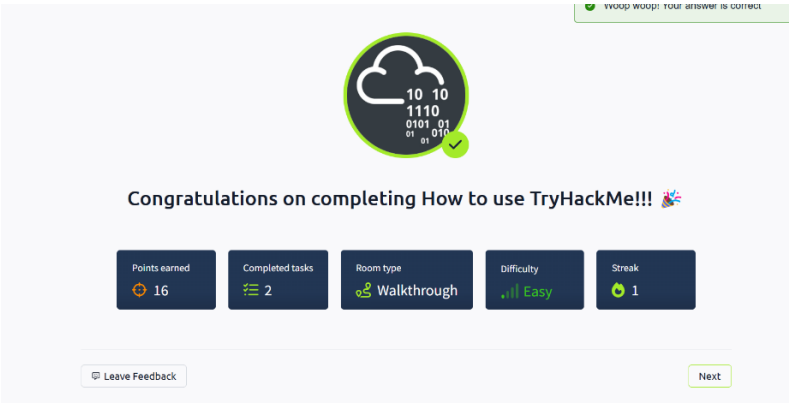
- **Starting Machines:** Learned how to start both AttackBox and target machines within TryHackMe.
- **Connecting via OpenVPN:** Understood the process of connecting to TryHackMe's network using OpenVPN.
- **Navigating the Platform:** Gained proficiency in moving through different rooms and tasks within TryHackMe.

🔍 **Walkthrough / How You Solved It**

1. Starting the AttackBox : Clicked the "Start AttackBox" button to initialize the AttackBox.
2. Deploying Target Machines : Used the "Start Machine" button to deploy target machines for tasks.
3. Connecting via OpenVPN : Installed OpenVPN on the local machine, downloaded the configuration file, and connected to TryHackMe's network.
4. Accessing Machines : Used the AttackBox or OpenVPN connection to access and interact with deployed machines.

💡 **Reflections or Notes**

- The room provided a comprehensive overview of TryHackMe's functionalities.
- Hands-on practice with starting and connecting to machines enhanced understanding.
- The OpenVPN setup was straightforward and well-documented.



ROOM 3:

🧩 **Room Name:** Getting Started

🔗 **Link:** https://tryhackme.com/room/gettingstarted

🎯 Learning Objective

- Understand the basics of connecting to TryHackMe's network using OpenVPN.
- Learn how to start and interact with machines within TryHackMe.
- Familiarize yourself with the process of accessing machines via a web browser.

🛠 Key Tools/Commands Used

- OpenVPN: For connecting to TryHackMe's network.
- Web Browser: For accessing deployed machines.

🧠 Concepts Learned

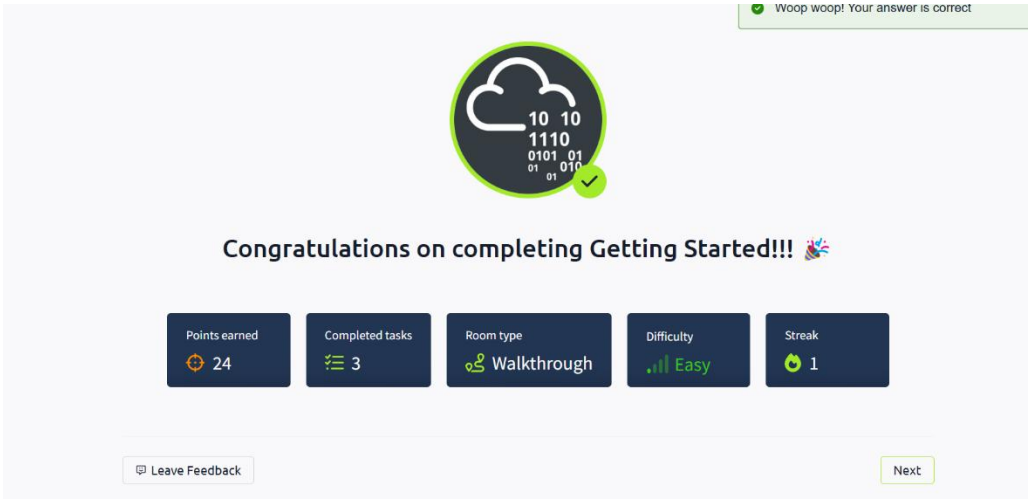
- **VPN Connection**: Learned how to securely connect to TryHackMe's network using OpenVPN.
- **Machine Deployment:** Understood how to deploy and access machines within TryHackMe.
- **Flag Capture**: Learned the concept of flags used to verify task completion.

🔍 Walkthrough / How You Solved It

1. Connecting via OpenVPN: Followed the steps to connect to TryHackMe's network using OpenVPN.
2. Deploying a Machine: Started a machine within the room and noted its IP address.
3. Accessing the Machine: Entered the machine's IP address into the web browser to access its web page.
4. Capturing the Flag: Located and submitted the flag displayed on the machine's web page.

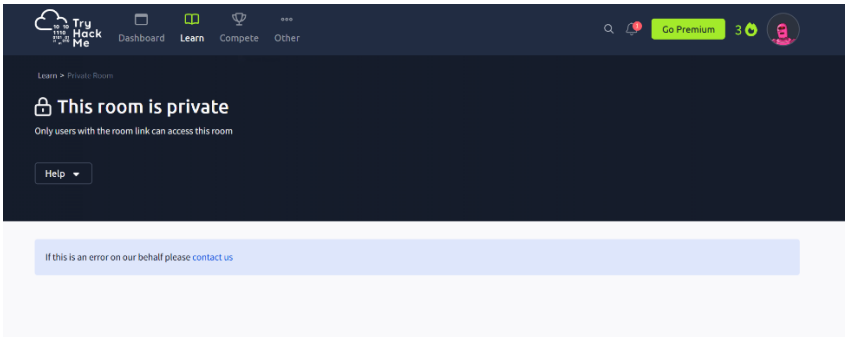
💡 Reflections or Notes

- The room reinforced the process of connecting to TryHackMe's network and accessing machines.
- Emphasis on capturing flags provided a clear goal for each task.
- The step-by-step approach made the learning process engaging.



ROOM 4:

- 🧩 Room name: Welcome
- 🔗 Link: [TryHackMe | Room details]



ROOM 5

🧩 **Room Name:** TryHackMe Tutorial

🔗 **Link:** https://tryhackme.com/room/tutorial

🎯 Learning Objective

- Learn how to use TryHackMe's platform features effectively.
- Practice launching and interacting with machines.
- Understand how to navigate room content and submit answers.

🛠 Key Tools/Commands Used

- TryHackMe AttackBox
- Browser Navigation

🧠 Concepts Learned

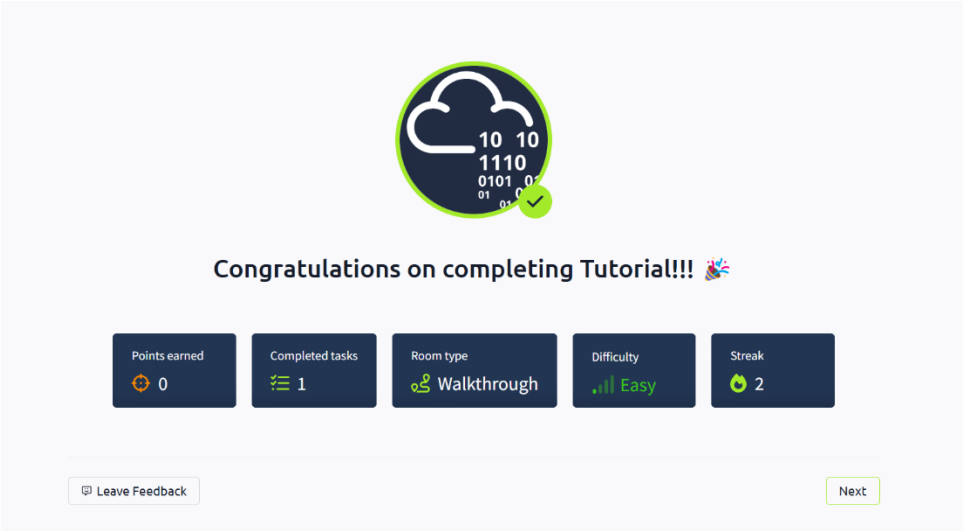
- ➢ Navigating through different tasks in a room
- ➢ Submitting flags and answering quiz-style questions
- ➢ Starting/stopping machines and recognizing their IPs

🔍 Walkthrough / How You Solved It

1. Joined the tutorial room.
2. Launched the AttackBox and started the target machine.
3. Explored the machine via its IP using a browser or terminal.
4. Located a sample flag and submitted it.
5. Completed mini-tasks and answered simple questions about usage.

💡 Reflections or Notes

- The hands-on format made learning fun and intuitive.
- The tutorial helped reinforce how to find, copy, and submit flags.
- Felt more confident navigating the rooms and using the AttackBox.



ROOM 6

🧩 **Room Name:** OpenVPN Configuration

🔗 **Room Link:** https://tryhackme.com/room/openvpn

🎯 Learning Objective

- ➢ Set up and configure OpenVPN to connect your local machine to TryHackMe's virtual network.

🛠 Key Tools/Commands Used

- OpenVPN
- browser

🧠 Concepts Learned

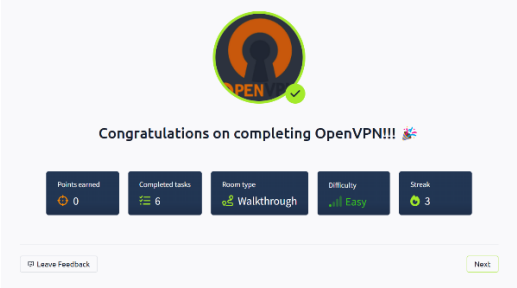
- VPN technology and how it provides a secure tunnel.
- Downloading and configuring `.ovpn` files
- Troubleshooting VPN connection errors

🔍 Walkthrough / How You Solved It

1. Downloaded the `.ovpn` config file from my profile.
2. Installed OpenVPN (if not already installed).
3. Run the software.
4. Verified connection to TryHackMe's network.

💡 Reflections or Notes

- This room was very practical and crucial for using TryHackMe from your own machine.
- Learned to monitor VPN status and IP configuration.



ROOM 7

🧩 **Room:** Beginner Path Introduction

🔗 **Room Link**: https://tryhackme.com/room/beginnerpathintro

🎯 Learning Objective

- Familiarize yourself with the basics of cybersecurity and the TryHackMe platform, including navigation and the types of challenges available.

🛠 Key Tools/Commands Used

- TryHackMe Platform: The main interface for accessing rooms and challenges.

🧠 Concepts Learned

- Overview of cybersecurity concepts and terminology.
- Understanding the structure of TryHackMe rooms and how to approach challenges.
- Introduction to web security and network security

🔍 Walkthrough / How You Solved It

1. Access the Room: I logged into my TryHackMe account and navigated to the Beginner Path Introduction room.
2. Read the Content: I carefully read through the introductory materials provided in the room to understand the objectives and layout.
3. Complete the Challenges: I engaged with the interactive challenges, practicing basic terminal commands and familiarizing myself with the platform's features.
4. Review Resources: I utilized the additional resources and links provided in the room to deepen my understanding of the topics covered.

💡 Reflections or Notes

- This room was an excellent starting point for anyone new to cybersecurity, providing a solid foundation.
- I appreciated the structured approach to learning, which made it easy to follow along.

ROOM 8

🧩 Room Name: Starting Out in Cyber Security

🔗 Room Link: https://tryhackme.com/room/startingoutincybersec

🎯 Learning Objective

- Learn about different areas of cybersecurity.
- Understand the various job roles and career paths available.

🛠 Key Tools/Commands Used

- None required—primarily reading and quiz-based.

🧠 Concepts Learned

- **Common cybersecurity fields**: Penetration Testing, SOC Analyst, Malware Analyst, etc.
- **Career Paths in Cybersecurity**: Overview of various roles and specializations within the cybersecurity field.
- Importance of certifications and continuous learning

🔍 Walkthrough / How You Solved It

1. Read each task explaining job roles, responsibilities, and required skills.
2. Answered simple multiple-choice questions.
3. Marked each task complete after finishing.

💡 Reflections or Notes

- The breakdown of roles helped identify interests in the field.
- Motivated me to explore more about certifications like CompTIA and OSCP.
- Reinforced that cybersecurity is a broad and growing field.

ROOM 9

🧩 **Room Name:** Introduction to Research
🔗 **Link:** [TryHackMe - Introduction to Research]

🎯 Learning Objective

To develop research skills in cybersecurity by exploring various information sources and answering questions based on that research. The room emphasizes the importance of research in cybersecurity, including understanding vulnerabilities and using Linux manual pages.

🛠 Key Tools/Commands Used

- **Search Engines:** Google and others for gathering info
- **CVE Databases:** Researching specific software vulnerabilities
- **Linux Manual Pages:** Accessing command documentation via man

🧠 Concepts Learned

- **Research Methodology:** Systematic approach to solving research tasks
- **Evaluating Sources:** Identifying credible and reliable information
- **Common Vulnerabilities:** Understanding CVEs and their impact
- **Linux Manual Pages:** Using man for command syntax and options

🔍 Walkthrough / How You Solved It

Task 2 – Example Research Question

1. Read the task instructions and used search engines to find answers
2. Focused on reliable sources to ensure correct responses

Task 3 – Vulnerability Searching

1. Explored the concept of software vulnerabilities and exploitation
2. Used databases like the **National Vulnerability Database (NVD)** to look up specific CVEs
3. Reviewed CVE details

Task 4 – Manual Pages

1. Learned to use the man command in Linux
2. Ran commands like man ls and man grep to explore their usage, flags, and examples
3. Applied this info to answer related questions

Final Step – Compiling and Submitting Answers

💡 Reflections or Notes

- This room significantly improved my cybersecurity research skills
- Reinforced the importance of credible sources and CVE analysis
- The man command proved to be a valuable resource for learning Linux tools

- Overall, a foundational and practical room for anyone beginning their cybersecurity journey