

 **Room Name and Link**

Hello World – <https://tryhackme.com/room/hello>

 **Learning Objective**

- Understand the basic structure of TryHackMe rooms and get familiar with how tasks and questions work on the platform.
- Learn to navigate the interface and complete beginner-friendly exercises.

 **Key Tools/Commands Used**

- No tools required
- Just a web browser and the TryHackMe interface

 **Concepts Learned**

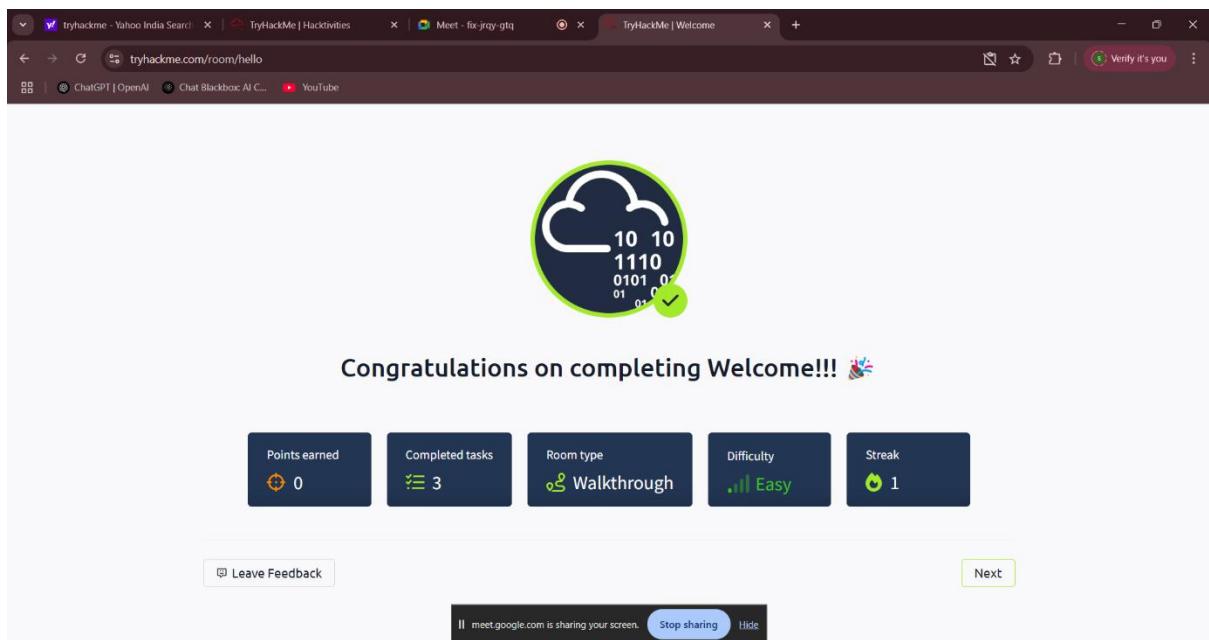
- How to navigate and interact with TryHackMe rooms
- Structure of rooms: tasks, questions, flags
- Importance of reading instructions carefully
- Basic idea of virtual machines used for challenges

 **Walkthrough / How You Solved It**

1. Opened the room and read the introductory material.
2. Went through each task step-by-step, clicking "complete" after reading.
3. Deployed the machine and used it to find and submit the flag as instructed.

 **Reflections or Notes**

- A great starting point to understand the TryHackMe platform.
- No technical difficulty, but a useful introduction to the process.
- Sets expectations for future rooms—flag format, VM usage, and structure.



 Room Name and Link

How to Use TryHackMe --

<https://tryhackme.com/room/howtousetryhackme>

 Learning Objective

Understand how to use TryHackMe's core features, including virtual machines, tasks, and interface layout.

 Key Tools/Commands Used

- TryHackMe Dashboard
- Web-based VMs
- OpenVPN (introductory mention)

 Concepts Learned

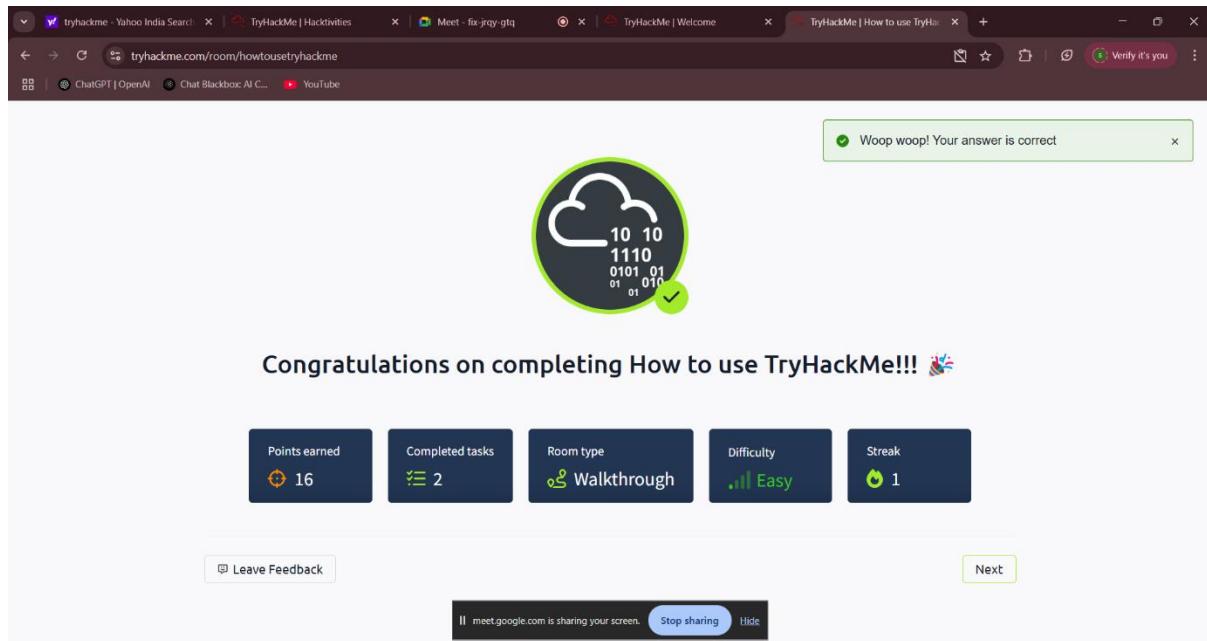
- Using and interacting with in-browser VMs
- Completing guided tasks and submitting answers
- Navigating the dashboard and tracking progress

 Walkthrough / How You Solved It

1. Accessed the room and launched the VM
2. Followed guided tutorials for VM interaction
3. Used task hints and completed multiple-choice and written answers

💡 Reflections or Notes

- Great for understanding the hands-on nature of the platform
- Helped reinforce how to navigate the dashboard and engage with content



 **Room Name and Link**

Getting Started -- <https://tryhackme.com/room/gettingstarted>

 **Learning Objective**

Introduction to Linux basics and core networking concepts within TryHackMe's virtual labs.

 **Key Tools/Commands Used**

- ls, cd, pwd
- cat, less
- TryHackMe in-browser terminal

 **Concepts Learned**

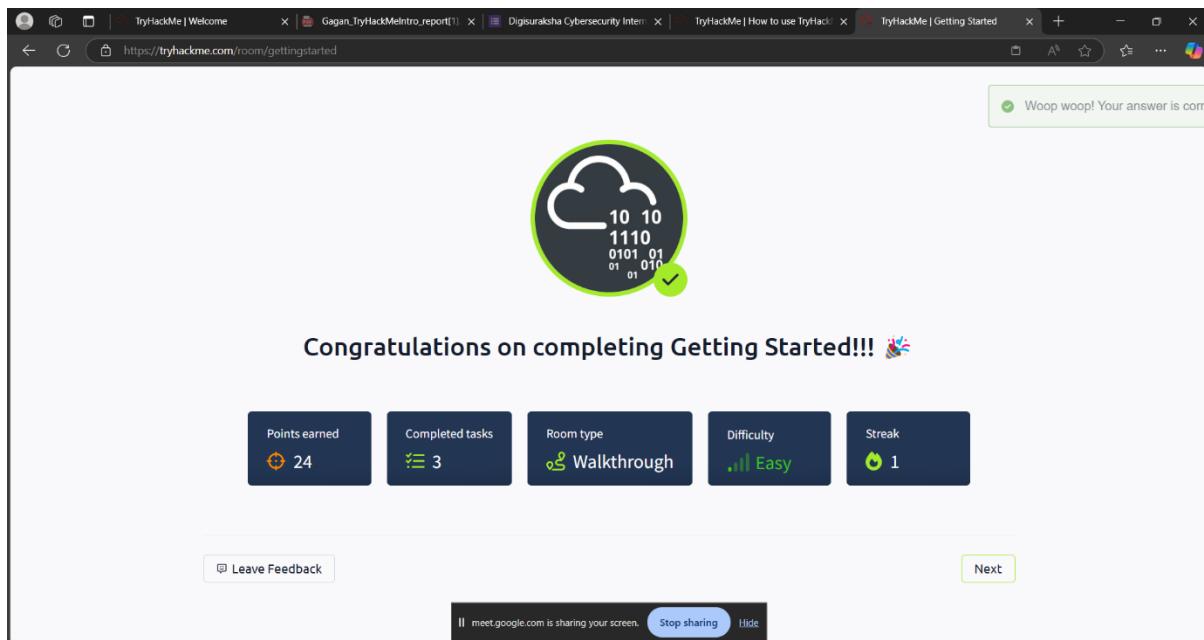
- Basic Linux command-line navigation
- Structure of files and directories
- IP addresses and port communication

 **Walkthrough / How You Solved It**

1. Launched the VM
2. Explored the file system using commands
3. Understood the use of ports and IPs via exercises

 **Reflections or Notes**

- Solid intro to command-line tools and VM interaction
- Helped build terminal confidence



 **Room Name and Link**

TryHackMe Tutorial -- <https://tryhackme.com/room/tutorial>

 **Learning Objective**

Understand TryHackMe's challenge format and gain exposure to enumeration techniques and flag capture.

 **Key Tools/Commands Used**

- ls, cd, cat
- ping, whoami

 **Concepts Learned**

- Navigating room content and tasks
- Importance of enumeration
- Flag location and format

 **Walkthrough / How You Solved It**

1. Deployed the VM and opened the terminal
2. Explored file directories and system info
3. Retrieved and submitted the flag

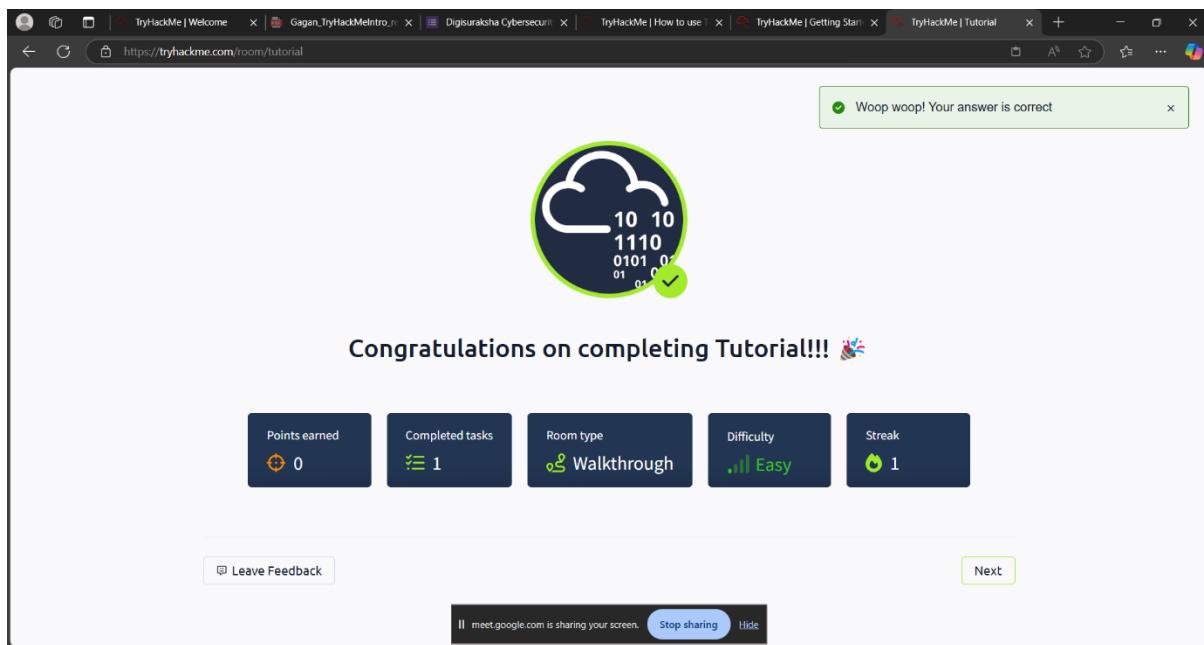
 **Reflections or Notes**

- Reinforced step-by-step problem-solving
- Simple but essential skills were practiced

248461

Cybersecurity Internship Assignment

Sneha Tambe



 **Room Name and Link**

OpenVPN Configuration -- <https://tryhackme.com/room/openvpn>

 **Learning Objective**

Learn to securely connect to TryHackMe's private network using OpenVPN.

 **Key Tools/Commands Used**

- OpenVPN client
- sudo openvpn <configfile>.ovpn
- ip a, ifconfig

 **Concepts Learned**

- VPN fundamentals and encryption
- Config file usage
- Troubleshooting VPN connection issues

 **Walkthrough / How You Solved It**

1. Downloaded the OpenVPN config file
2. Installed OpenVPN client
3. Connected via terminal and verified connectivity

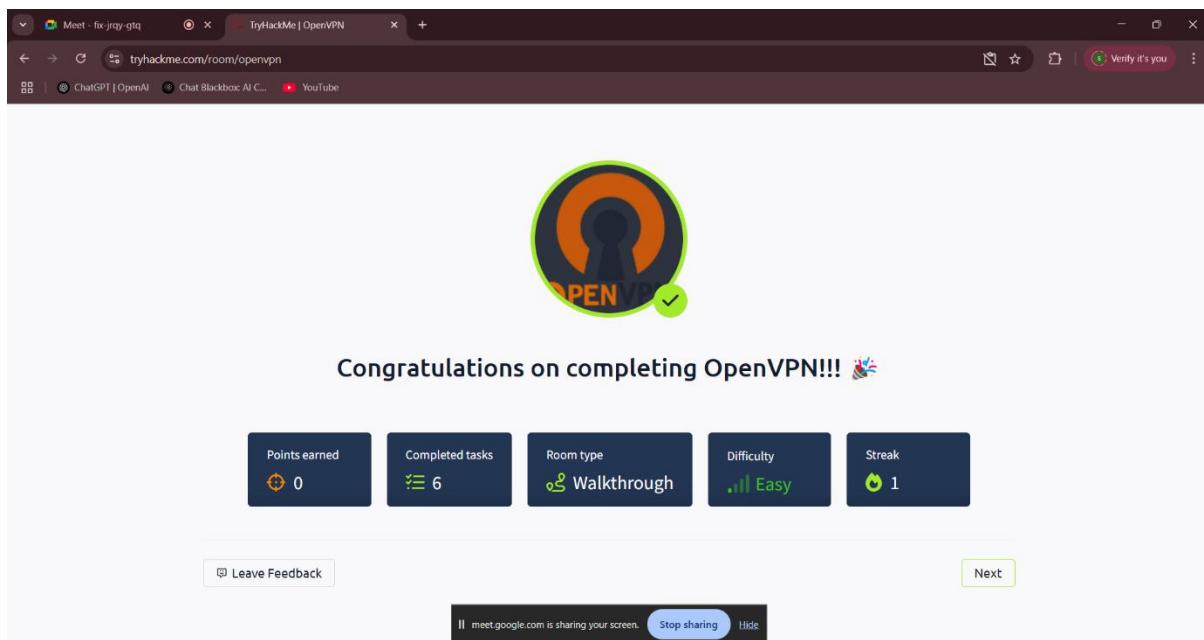
 **Reflections or Notes**

- Crucial for advanced labs
- Great introduction to real-world VPN use in cybersecurity

248461

Cybersecurity Internship Assignment

Sneha Tambe



 **Room Name and Link**

Beginner Path Introduction -- <https://tryhackme.com/room/beginnerpathintro>

 **Learning Objective**

Gain a roadmap of the TryHackMe Beginner Path including covered skills and learning flow.

 **Key Tools/Commands Used**

- Navigation through the TryHackMe platform

 **Concepts Learned**

- Modular structure of beginner labs
- Skill-building flow: Linux → Networking → Web → Security
- Self-paced learning strategies

 **Walkthrough / How You Solved It**

1. Read the roadmap and module outlines
2. Identified relevant skills to build
3. Marked the room as complete after absorbing the plan

 **Reflections or Notes**

- Sets expectations for the whole path
- Makes learning feel structured and achievable

248461

Cybersecurity Internship Assignment

Sneha Tambe



 **Room Name and Link****Starting Out in Cyber Security --**

<https://tryhackme.com/room/startingoutincybersec>

 **Learning Objective**

Understand different cybersecurity career paths, roles, and required skills.

 **Key Tools/Commands Used**

- No commands/tools used — informational room

 **Concepts Learned**

- Common job roles (SOC analyst, pentester, etc.)
- Key skills: networking, Linux, scripting, etc.
- Career planning and certification paths

 **Walkthrough / How You Solved It**

1. Read each section on cybersecurity roles and paths
2. Reflected on personal interests
3. Completed the room's quiz and self-assessments

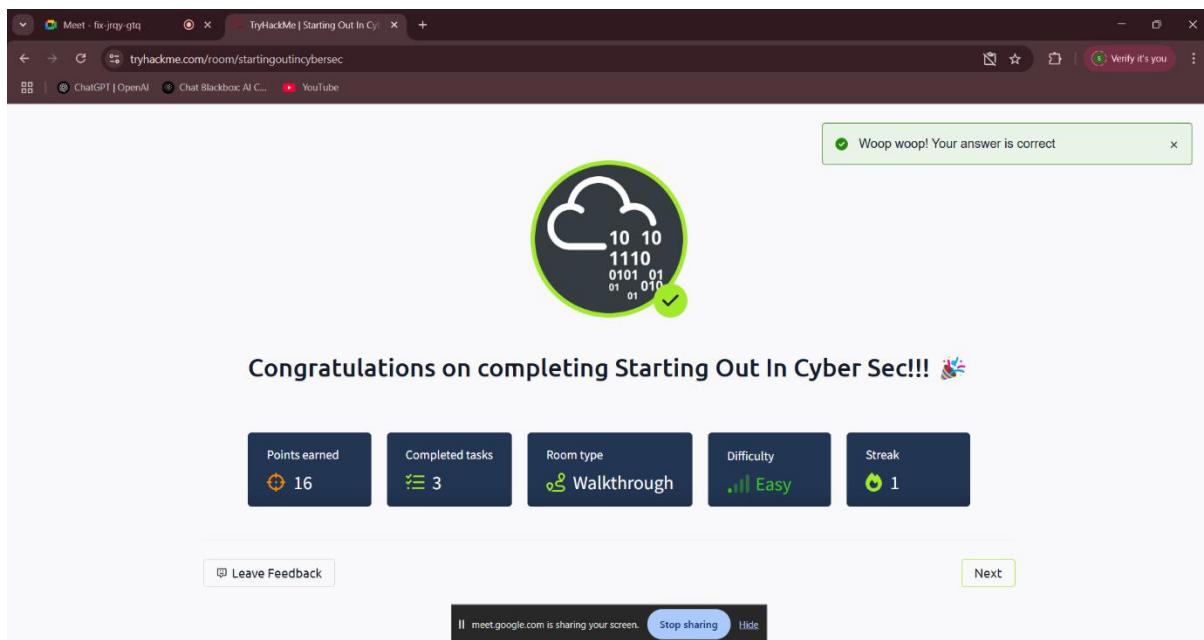
 **Reflections or Notes**

- Very motivating for newcomers
- Helped create a vision for long-term learni

248461

Cybersecurity Internship Assignment

Sneha Tambe



 **Room Name and Link**

Introduction to Research -- <https://tryhackme.com/room/introtoresearch>

 **Learning Objective**

Develop research skills needed to solve technical problems independently in cybersecurity.

 **Key Tools/Commands Used**

- Web search engines: Google, DuckDuckGo
- Cybersecurity databases: NIST NVD, CVE
- Documentation: vendor websites, cheat sheets, whitepapers

 **Concepts Learned**

- How to craft precise and effective search queries
- Evaluating the credibility of online sources
- Navigating technical databases to extract relevant vulnerability information
- Applying research methods to real-world cybersecurity problems

 **Walkthrough / How You Solved It**

1. Accessed and read through the instructional material
2. Practiced forming effective search queries for finding technical answers
3. Explored NIST and CVE databases to find known vulnerabilities
4. Referred to trusted sources like official docs, GitHub repos, and whitepapers
5. Completed tasks and questions based on applied research

💡 Reflections or Notes

- Reinforces the reality that cybersecurity professionals need strong research habits
- Helps develop confidence in self-directed problem solving
- Vital for ongoing learning, especially in a fast-evolving field like cybersecurity
- Being resourceful is just as important as being technically skilled

