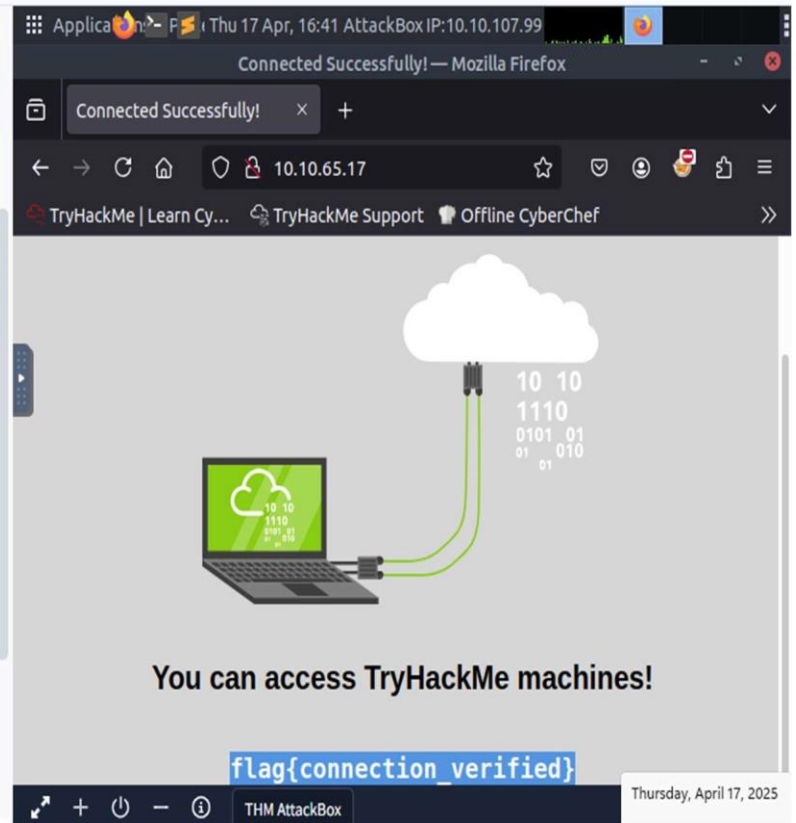
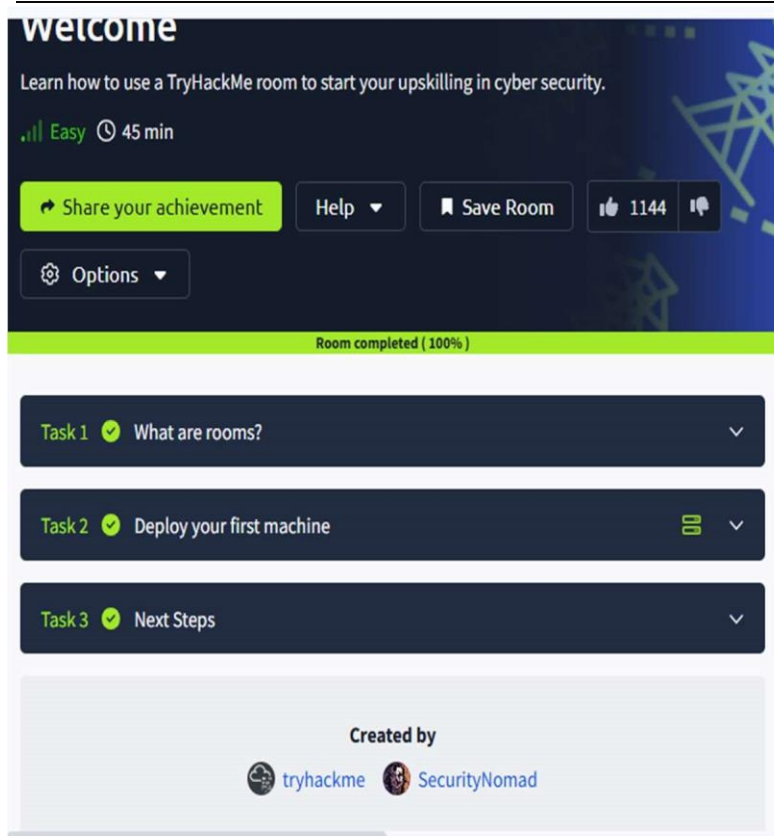


Name: Haria Dhruti Jagdish

Internship Program: Digisuraksha Parhari Foundation Powered
by: Infinisec Technologies Pvt. Ltd.

Submission Deadline: 18th April 2025

TRYHACKME INTRODUCTORY LABS REPORT



1) HELLO WORLD

Link: <https://tryhackme.com/room/hello> Learning
Objective

To get introduced to TryHackMe, understand how the platform works, and navigate through the interface effectively.

✂ Key Tools/Commands Used

- TryHackMe Web Interface

Concepts Learned

- TryHackMe's layout and platform design
- Task-based progression system
- Launching and accessing virtual machines (VMs)

Walkthrough / How You Solved It

- Logged into TryHackMe and joined the Hello World room
- Read through each section and followed the instructions
- Observed how tasks are marked as complete

Reflections or Notes

A beginner-friendly room that builds comfort with the TryHackMe interface.

2) 2Room Name: How to Use TryHackMe

Room Name and Link:

Room: How to use TryHackMe

Room Type: Walkthrough



Difficulty: Easy

Learning Objective:

To introduce users to the TryHackMe platform, its room structure, and how to deploy and access virtual machines via the AttackBox. This room helps new users get comfortable with the basics of interactive cybersecurity training.

✂ Key Tools/Commands Used:

- TryHackMe Platform Interface – for navigating the room
 - THM AttackBox – browser-based Linux machine for practical tasks □ Built-in VPN/Web Connection – for connecting to deployed machines □ No terminal or complex command-line tools used in this introductory room
-

Concepts Learned:

- The meaning and purpose of a "room" in TryHackMe
 - How to deploy a virtual machine (VM) from the TryHackMe environment
 - Using the AttackBox to interact with the VM
 - Importance of verifying connections using flags
-

Walkthrough / How You Solved It:

1. Accessed the room via the provided link.
 2. Task 1: What are Rooms?
 - Learned that rooms contain theory, instructions, and practical tasks.
 - Completed by reading and answering the quiz.
 3. Task 2: Deploy Your First Machine
 - Clicked “Start Machine” to deploy a VM.
 - Used the AttackBox to connect to the machine.
 - Found and submitted the flag `flag{connection_verified}` to verify connection.
 4. Task 3: Next Steps
 - Explored suggestions for further learning, including beginner-friendly rooms like “Introduction to Cyber Security.”
-

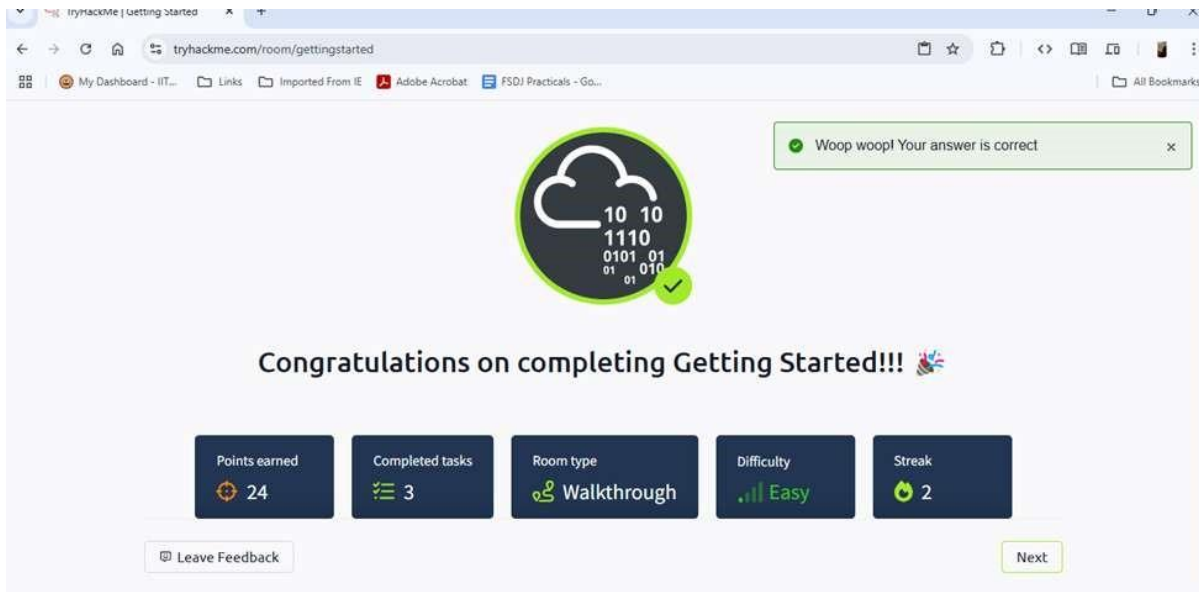
Reflections or Notes:

- Simple and beginner-friendly layout.

- Useful as a first step before diving into technical rooms.
- Only 2 main tasks but covers essential starting skills.
- Earned 16 points, completed 2 tasks, and started a 2-day streak

Highly recommend for anyone just starting their cyber journey!

3) getting started



Room Name and Link

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

Learning Objective

To introduce new users to the TryHackMe platform, including how to navigate rooms, complete tasks, and interact with the learning environment.

✂ Key Tools/Commands Used

- TryHackMe interface
 - Task completion buttons and interactive questions
 - Navigation and reading documentation
-

Concepts Learned

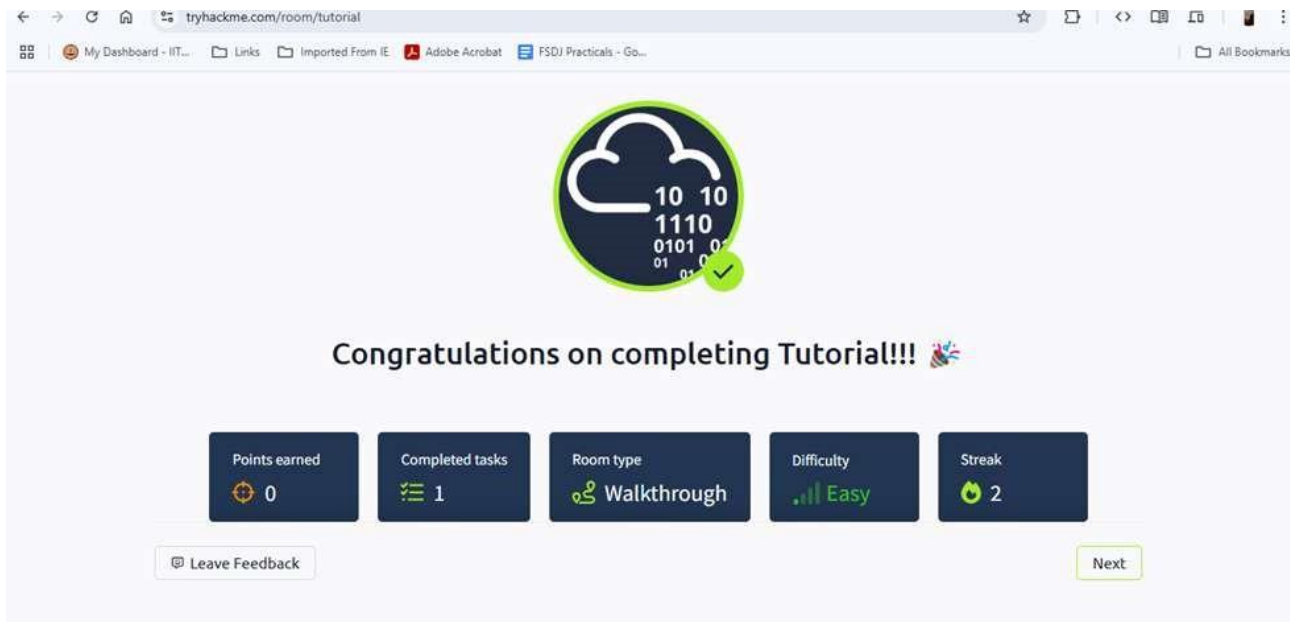
- Understanding the TryHackMe room structure (tasks, questions, answers)
 - Navigating and interacting with rooms
 - Basics of cybersecurity learning flow on TryHackMe
 - How to check answers and track progress
-

Walkthrough / How You Solved It

1. Accessed the room via the provided link.
 2. Read the introductory content for each task.
 3. Completed 3 basic tasks designed to familiarize users with the interface.
 4. Answered a few questions to confirm understanding.
 5. Earned 24 points and completed the room with a difficulty rating of "Easy."
-

Reflections or Notes

- This room was a great introduction to the TryHackMe platform.
- The walkthrough helped me understand how to navigate and use rooms for learning.
- It's a perfect starting point for cybersecurity beginners.
- Looking forward to progressing to more technical rooms! 4) Tutorial



Room Name and Link

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

Learning Objective

To help users understand how to navigate and interact with a TryHackMe room by completing a basic tutorial.

✂ Key Tools/Commands Used

- ☐ None (basic interaction with platform UI)
-

Concepts Learned

- How to access tasks in a room
 - How to answer questions and mark tasks as complete
 - Understanding the layout and purpose of walkthrough rooms
-

Walkthrough / How You Solved It

1. Opened the Tutorial room using the link

2. Read the introduction to TryHackMe
3. Completed the single task provided
4. Marked it as done to complete the room

Reflections or Notes

- Very simple room but helpful to get comfortable with the platform interface.
- No points were earned, but it's crucial as the first step

5) OPENVPN



Room Name and Link

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

Learning Objective

To learn how to configure and connect to TryHackMe's network using OpenVPN, enabling access to machines for hands-on labs.

🔧 Key Tools/Commands Used

- OpenVPN
 - Terminal (CLI for VPN connection)
-

Concepts Learned

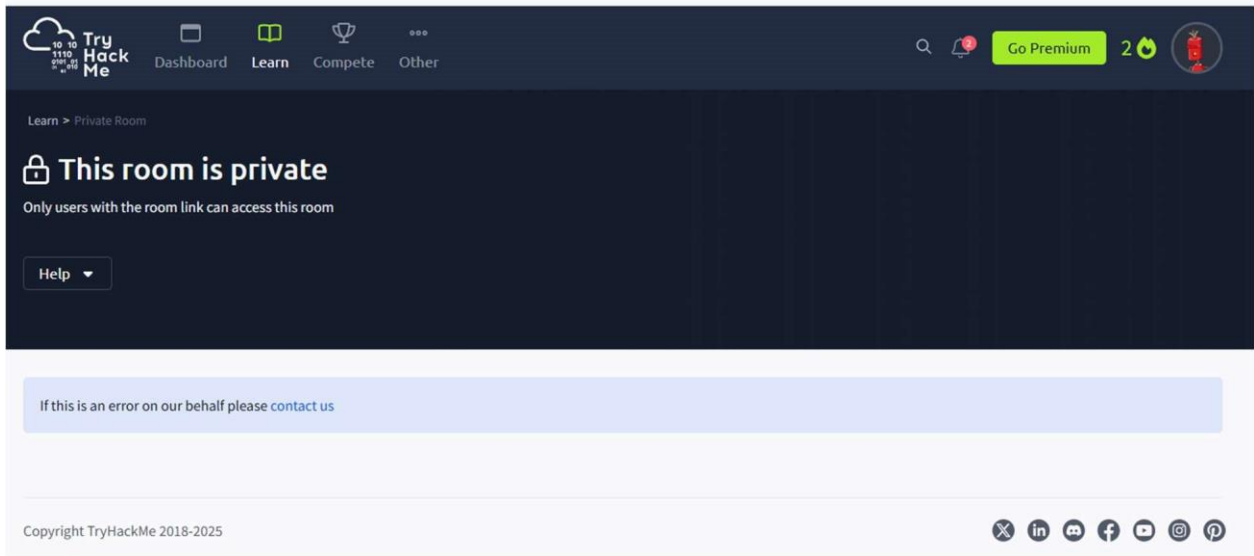
- What OpenVPN is and why it's used
 - How to download your configuration file
 - Command to start VPN connection
 - How to verify successful connection to TryHackMe's labs
-

Walkthrough / How You Solved It

1. Downloaded the .ovpn file from the dashboard
 2. Installed OpenVPN client
 3. Ran `sudo openvpn [filename].ovpn` in the terminal
 4. Verified the connection and completed all 6 tasks
-

Reflections or Notes

- Crucial setup step for TryHackMe labs
- No points earned, but vital for hands-on exercises
- Connection check helped ensure VPN is working before starting technical rooms



6)Cyber Security



Room Name and Link

Learning Cyber Security <https://tryhackme.com/room/beginnerpathintro>

Learning Objective

To introduce learners to the field of cybersecurity, explaining basic terms and setting the stage for further exploration.

🔧 Key Tools/Commands Used

- ☐ No tools or commands required (informational room)

Concepts Learned

- What cybersecurity is and why it matters
- Different areas within the cybersecurity field
- Skills required for a cybersecurity professional
- Overview of attack vectors and defensive roles

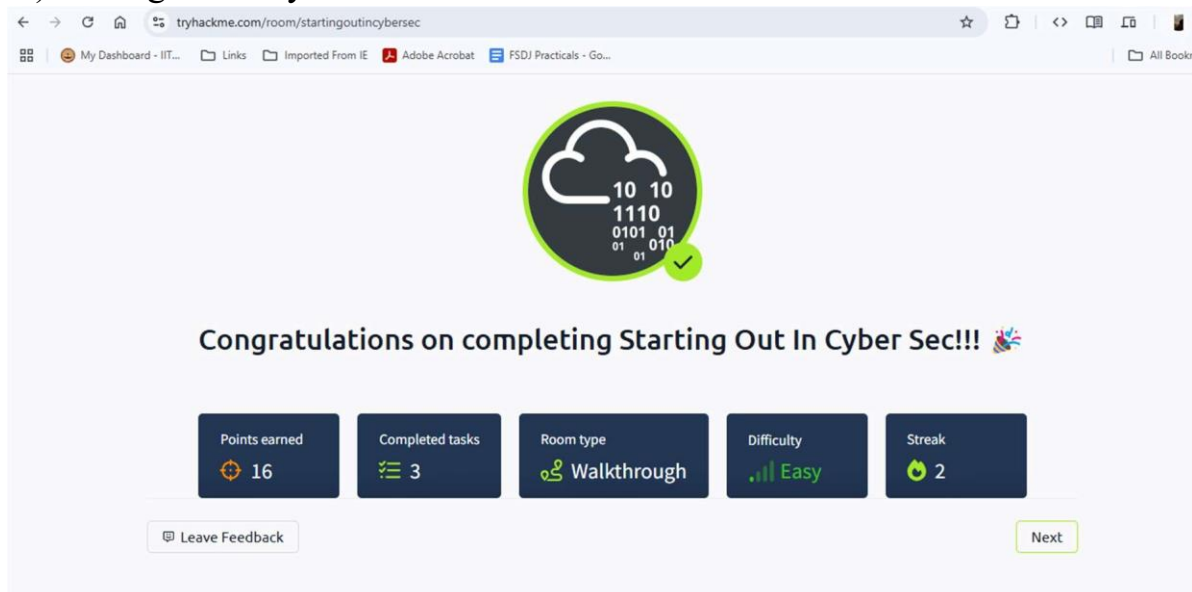
Walkthrough / How You Solved It

1. Read all provided materials across the 3 tasks
2. Answered verification questions
3. Understood the structure of the learning path
4. Marked tasks as complete and submitted answers

Reflections or Notes

- Clear and motivating introduction to the field
- Earned 24 points
- A good primer before diving into hands-on tasks

7) Starting out in cybersec



tryhackme.com/room/startingoutincybersec

My Dashboard - IIT... Links Imported From IE Adobe Acrobat FSDJ Practicals - Go... All Bookmarks

10 10
1110
0101 01
01 010

Congratulations on completing Starting Out In Cyber Sec!!!

| | | | | |
|---------------------|----------------------|--------------------------|--------------------|-------------|
| Points earned 16 | Completed tasks 3 | Room type Walkthrough | Difficulty Easy | Streak 2 |
|---------------------|----------------------|--------------------------|--------------------|-------------|

Leave Feedback Next

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

Learning Objective

- Overview of offensive/defensive domains and entry-level roles.

✂ Key Tools/Commands Used

- Web Browser: Read content, submitted form-based answers.

Concepts Learned

- Offensive: Penetration Tester role.
- Defensive: Security Analyst responsibilities.
- Blue Team pathways (Splunk, Volatility).

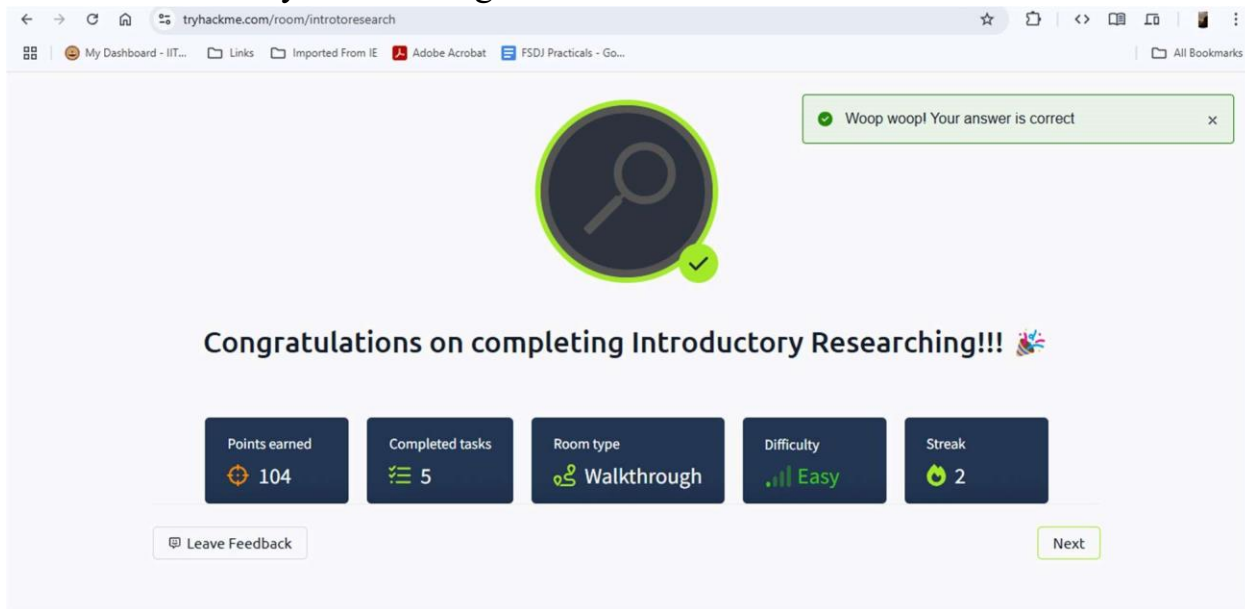
Walkthrough / How You Solved It

1. Task 1: Read beginner path overview (no submission).
2. Task 2 (Offensive): Submitted Penetration Tester.
3. Task 3 (Defensive): Submitted Security Analyst.

Reflections / Notes

- Clear framing of cybersecurity "sides".
- Encourages exploration of both paths.

8. Introductory Researching



Link: <https://tryhackme.com/room/introtoresearch>

Learning Objective

- Develop research/recon skills: vulnerability searching, Linux man pages.

🔧 Key Tools/Commands Used

- Search Tools:

bash

Copy

```
searchsploit -w # Exploit lookup curl
```

```
| grep CVE # Remote CVE search
```

- Linux Manuals:

bash

Copy

```
man scp # Learned '-r' for recursive copy
```

```
man fdisk # Learned '-l' for partitions
```

Concepts Learned

- Crafting pentesting research questions.

- Finding exploits via searchsploit and CVEs.
- Extracting usage from man pages.

Walkthrough / How You Solved It

1. Task 2 (Research):

o Burp Suite mode: Repeater. o

Windows hash format: NTLM.

2. Task 3 (CVEs): Found:

o WPForms XSS: CVE-2020-10385. o Sudo overflow: CVE-2019-18634.

3. Task 4 (Man Pages): Submitted flags like -r (scp) and -b (nano).

Reflections / Notes

- Recon skills uncover initial footholds.
- searchsploit speeds up exploit hunting.
- Regular man use deepens tool knowledge.