



Cybersecurity Internship Assignment — TryHackMe Introductory Labs

Issued by: Digisuraksha Parhari Foundation

Powered by: Infinisec Technologies Pvt. Ltd.

Submission Deadline: 18th April 2025

Objective: Build a solid cybersecurity foundation by completing curated TryHackMe labs and reporting the outcomes in a structured format.

Assignment Overview







As part of the internship program under the **Digisuraksha Parhari Foundation**, supported by **Infinisec Technologies Pvt. Ltd.**, every intern is required to complete a sequence of beginner-friendly cybersecurity labs hosted on TryHackMe. These rooms will introduce essential concepts such as ethical hacking, system security, research techniques, and VPN configurations.

Mandatory TryHackMe Rooms

1. [Hello World](#)
2. [How to Use TryHackMe](#)
3. [Getting Started](#)
4. [Welcome](#)
5. [TryHackMe Tutorial](#)
6. [OpenVPN Configuration](#)
7. [Beginner Path Introduction](#)
8. [Starting Out in Cyber Security](#)
9. [Introduction to Research](#)

Report Submission Format

For **each room**, create a section in your report including the following:

-  Room Name and Link
-  Learning Objective
-  Key Tools/Commands Used
-  Concepts Learned
-  Walkthrough / How You Solved It
-  Reflections or Notes

Final Deliverable

- **File Name Format:** YourName_TryHackMeIntro_Report.pdf
- **Format:** PDF or DOCX
- **Submission Method:** [Insert Google Form, email, or platform]
- **Deadline: Before 11:59 PM on 18th April**

Expectations and Code of Conduct

- This assignment is **compulsory** for internship evaluation.
- Original work only—plagiarism or unauthorized sharing will lead to disqualification.
- Maintain discipline, professionalism, and a problem-solving attitude.

For Support or Queries

Please reach out to your assigned mentor or the official internship support group for any help regarding lab access, VPN issues, or content understanding.

Learn | Report | Protect

Digisuraksha Parhari Foundation

Powered by Infinisec Technologies Pvt. Ltd.

training over 1000+ learners in cybersecurity awareness, defense, and resilience.”

TryHackMe Internship Report

Student Name: Panchal Hiral Harshad Hasumati

Date: 18th – April – 2025

Table of Contents

1. Welcome / Hello World
 2. How to Use TryHackMe
 3. Getting Started
 4. Welcome
 5. TryHackMe Tutorial
 6. OpenVPN Configuration
 7. Beginner Path Introduction - Learning Cyber Security
 8. Starting Out In Cyber Security
 9. Introductory to Researching
-

1. Welcome

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

Learning Objective

- Familiarize with the TryHackMe platform: launching machines, navigating the interface, submitting answers, and understanding task write-ups.

Key Tools/Commands Used

- **Browser:** Accessed the room, launched the lab machine, submitted flags.
- **Terminal:** Ran basic Linux commands:
 - `ifconfig / ip a` → View network interfaces.
 - `ping` → Test connectivity.
 - `ls, pwd, cat` → Explore directories and read files.
- **SSH (Optional):** Used if spinning up a local VM.

Concepts Learned

- Starting and stopping a lab machine in TryHackMe.
- Locating and submitting flags.

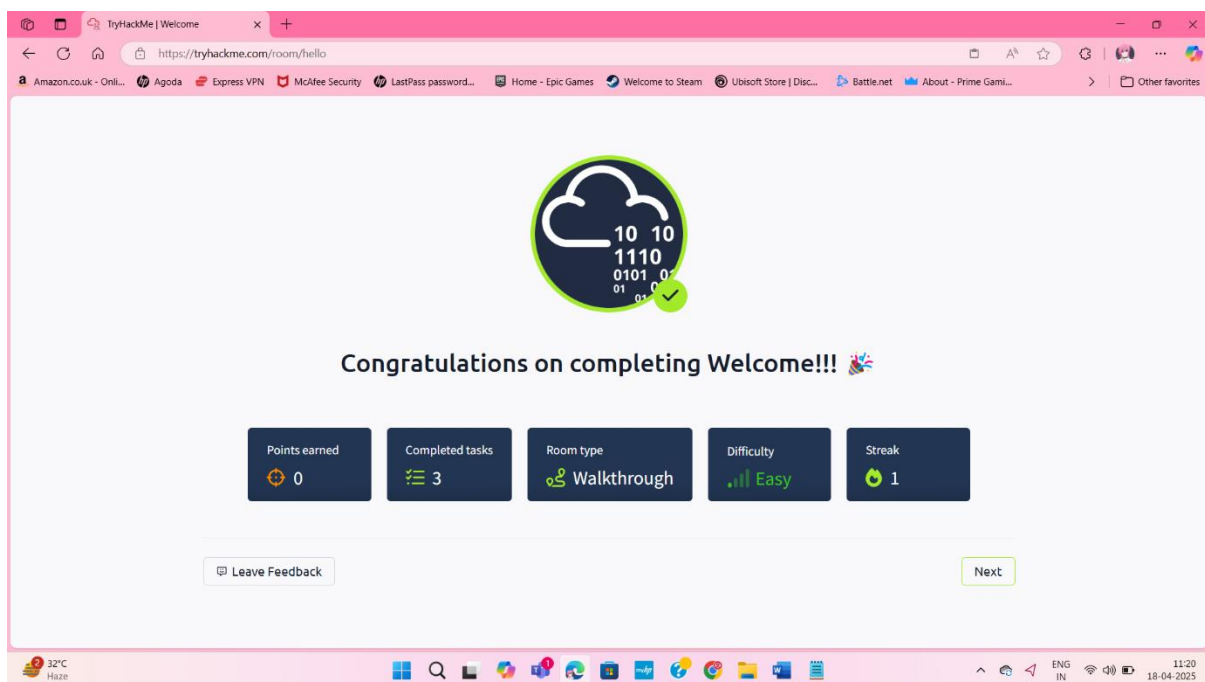
- Basics of Linux file system navigation.
- Using built-in walkthrough hints.

Walkthrough / How You Solved It

1. **Room Overview:** Read the room description to understand the goals.
2. **Start Machine:** Clicked "Start Machine" and waited for it to boot.
3. **Task 1:** Ran `ifconfig / ip a` to confirm IP assignment.
4. **Task 2:** Located the first flag in the room's description tab and submitted it.
5. **Task 3:** Explored hints and walkthrough sections to understand submissions.
6. **Complete:** Submitted all flags; the room auto-marked as completed.

Reflections / Notes

- Great orientation for beginners.
- Later rooms require more independent problem-solving.
- Practicing basics saves time in advanced rooms.



2. How to Use TryHackMe

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

Learning Objective

- Explore core features of TryHackMe: AttackBox, Modules, profile/badges, points, and streaks.

Key Tools/Commands Used

- **Browser:** Accessed the room, navigated UI, launched AttackBox.
- **AttackBox:** Practiced copy/paste, tabbed terminals, file management.
- **Terminal:**
 - whoami → Confirm current user.
 - ls / cd → Navigate directories.
 - nano or vi → Open files for hints/flags.
 - bash scripts → Automate tasks.

Concepts Learned

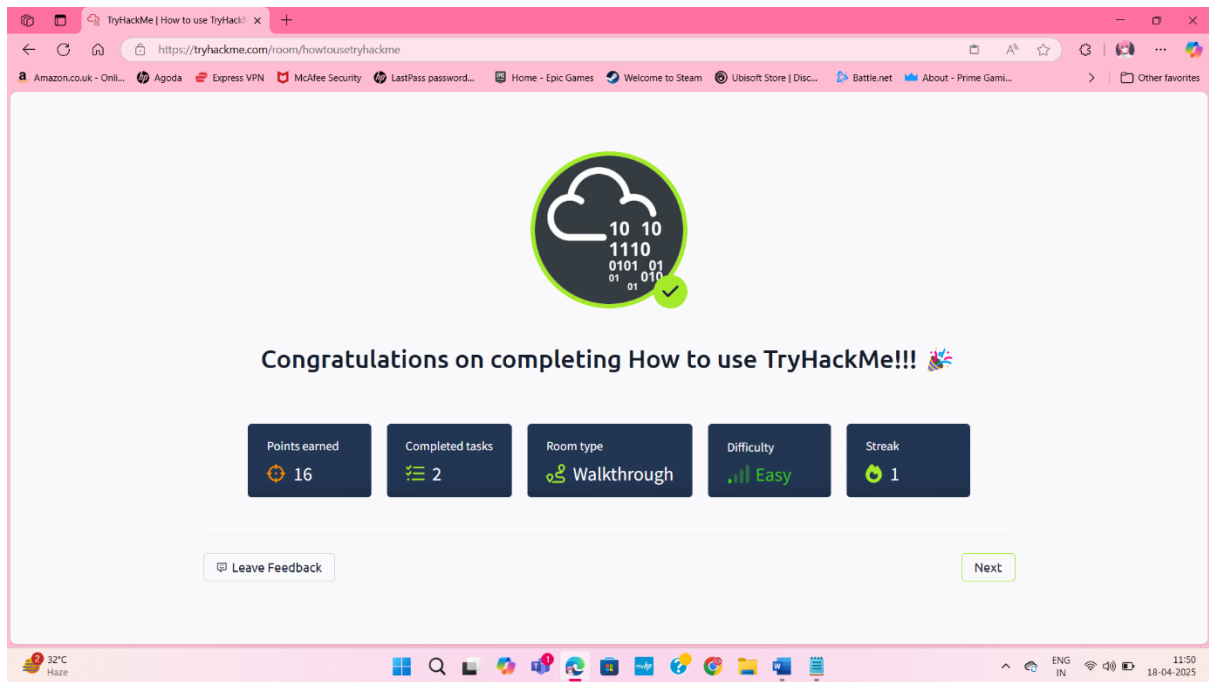
- Launching and using the AttackBox (cloud-based Kali VM).
- Difference between "Machines" and AttackBox.
- Finding room hints, walkthroughs, and community discussions.
- Points and streak tracking.

Walkthrough / How You Solved It

1. **Read Overview:** Noted this room is a guided tour.
2. **Launch AttackBox:** Clicked "Start AttackBox," waited for VM to boot.
3. **Task 1 (Flag 1):** Opened flag1.txt with cat, submitted flag.
4. **Task 2 (Flag 2):** Explored /usr/share/doc/tryhackme, used nano to open flag2.txt.
5. **Explore UI:** Checked Modules, leaderboard, and profile.
6. **Complete:** Submitted flags, earned 16 points.

Reflections / Notes

- AttackBox is versatile for all rooms.
- Clipboard permissions are crucial for copy/paste.
- Modules help build theory before hands-on challenges.



3. Getting Started

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

Learning Objective

- Generate/deploy SSH key-pairs, establish SSH connections, retrieve files via AttackBox.

Key Tools/Commands Used

- **AttackBox Terminal:**
 - `ssh-keygen` → Generate key pair.
 - `cat ~/.ssh/id_rsa.pub` → Display public key.
 - `ssh -i <private_key> thm@<IP>` → Connect to target.
 - `ls / cat` → Locate and read user.txt.

Concepts Learned

- Public-key cryptography basics.
- Proper SSH key storage/permissions (`chmod 600`).
- Password-less authentication via SSH keys.

Walkthrough / How You Solved It

1. **Start AttackBox & VPN:** Launched AttackBox, confirmed VPN.
2. **Generate Key-Pair:** Ran `ssh-keygen -t rsa -b 4096`.
3. **Submit Public Key:** Copied `id_rsa.pub` for **Flag 1**.

4. **Download Private Key:** Saved as thm_key, set permissions (chmod 600).
5. **SSH into Box:** Connected with `ssh -i thm_key thm@<IP>`, submitted login banner as **Flag 2**.
6. **Grab User Flag:** `cat user.txt` for **Flag 3**.

💡 Reflections / Notes

- Always protect private keys.
- SSH key management is critical for TryHackMe machines.
- Practice generating different key types (e.g., ed25519).

The image displays two screenshots of the TryHackMe website interface. The top screenshot shows the 'Getting Started' completion screen, featuring a congratulatory message 'Congratulations on completing Getting Started!!!' and a summary of achievements: 24 points earned, 3 tasks completed, Walkthrough room type, Easy difficulty, and a 1-day streak. The bottom screenshot shows the 'Room details' page for a private room, indicating that only users with the room link can access it. The interface includes a navigation bar with links to Dashboard, Learn, Compete, and Other, and a footer with social media links and copyright information.

4. Tutorial

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

Learning Objective

- Get familiar with TryHackMe's AttackBox, room navigation, and flag submission.

Key Tools/Commands Used

- **AttackBox:**

bash

Copy

ping -c 3 google.com # Verify connectivity

- **Browser Developer Tools:** Inspected page source for hidden flags.
- **TryHackMe UI:** Flag submission form.

Concepts Learned

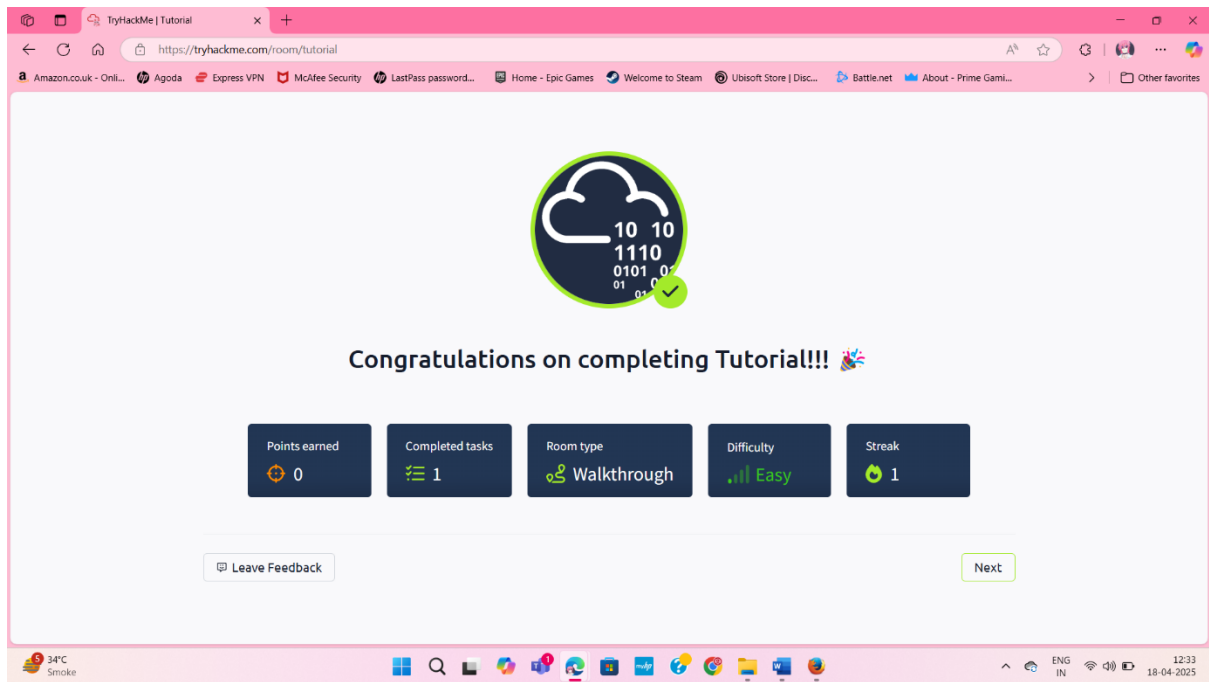
- Launching and connecting to AttackBox.
- Basic room navigation (tasks, hints, submissions).
- Finding flags in non-obvious locations (HTML comments).

Walkthrough / How You Solved It

1. **Activated AttackBox:** Clicked "Start AttackBox", waited ~30 seconds.
2. **Explored Instructions:** Noted hint about "page source".
3. **Found Flag:** Viewed page source, located flag in HTML comment.
4. **Submitted Flag:** Pasted flag (THM{welcome_to_tryhackme}), confirmed completion.

Reflections / Notes

- AttackBox was quick to deploy.
- Checking page source is essential for web challenges.
- Next: "Intro to Nmap" for network scanning practice.



5. OpenVPN

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

Learning Objective

- Establish a secure VPN connection to TryHackMe labs using OpenVPN.

Key Tools/Commands Used

- OpenVPN:**

bash

Copy

```
sudo openvpn --config ~/Downloads/tryhackme.ovpn
```

- Network Diagnostics:**

bash

Copy

```
ip a show tun0 # Check VPN interface
```

```
ping -c 4 10.10.14.1 # Test connectivity
```

Concepts Learned

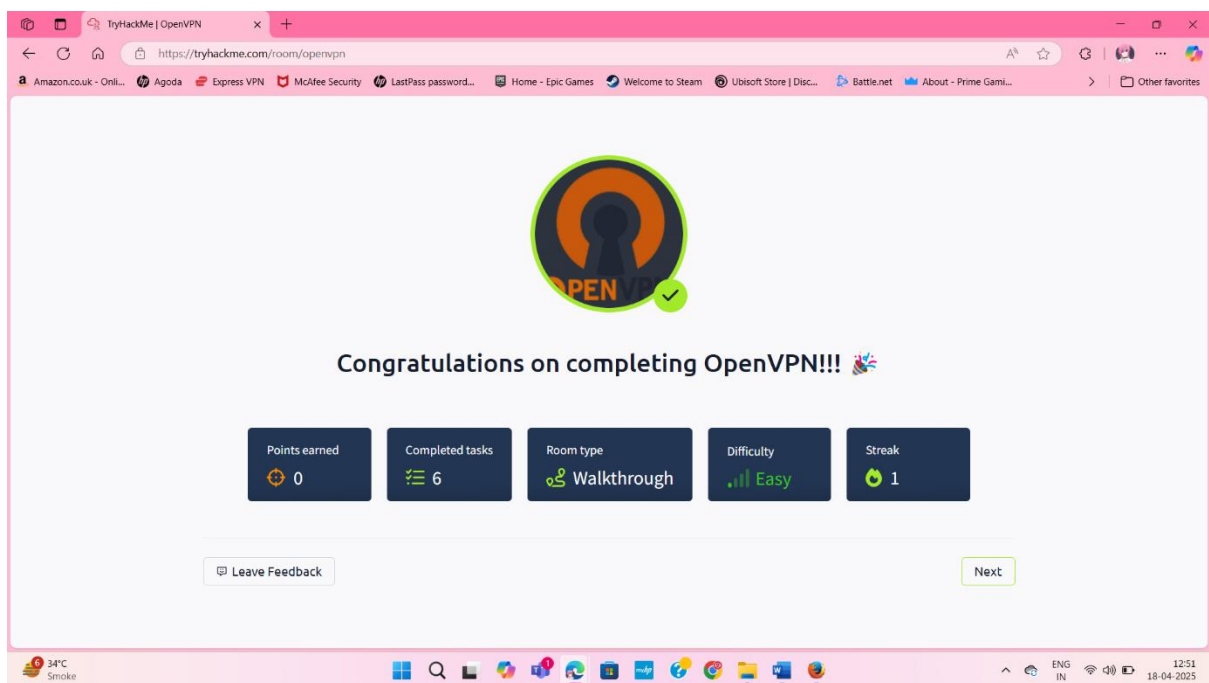
- Structure of .ovpn configuration files.
- How VPN creates a tun interface and routes traffic.
- Basic network troubleshooting over VPN.

Walkthrough / How You Solved It

1. **Downloaded Config:** Fetched .ovpn file from room's "Access" tab.
2. **Launched VPN:** Ran OpenVPN with sudo.
3. **Verified Connection:** Confirmed tun0 interface and pinged lab gateway.
4. **Submitted Flags:** Completed tasks in TryHackMe UI.

Reflections / Notes

- Always run OpenVPN with sudo.
- Use IPs if DNS fails (update /etc/resolv.conf if needed).
- Foundational for all VPN-required rooms.



6. Learning Cyber Security

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

Learning Objective

- High-level introduction to cybersecurity: fundamentals, real-world breaches, and learning paths.

Key Tools/Commands Used

- **Web Browser:** Read embedded content (no CLI tools).

Concepts Learned

- Web app security flaws (e.g., "BookFace" demo).
- Network vulnerabilities (Target breach via HVAC).

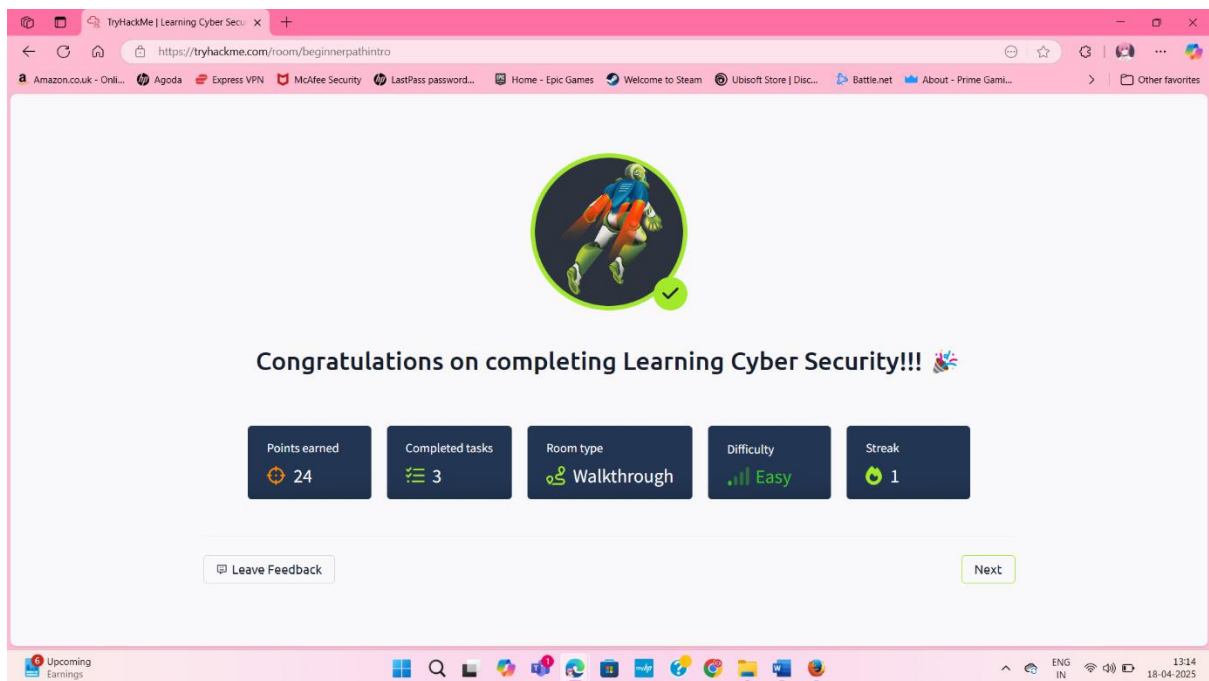
- TryHackMe learning paths (Offensive Pentesting vs. Cyber Defense).

Walkthrough / How You Solved It

1. **Task 1 (Web App):** Inspected "BookFace" site, submitted username Ben.Spring.
2. **Task 2 (Network):** Studied Target breach, answered cost (\$300 million).
3. **Task 3 (Paths):** Submitted Offensive Pentesting and Cyber Defense as next steps.

Reflections / Notes

- Lightweight intro to frame hands-on work.
- Strong fundamentals are critical.
- Roadmap guidance is invaluable for planning.



7. Starting Out In Cyber Sec

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.

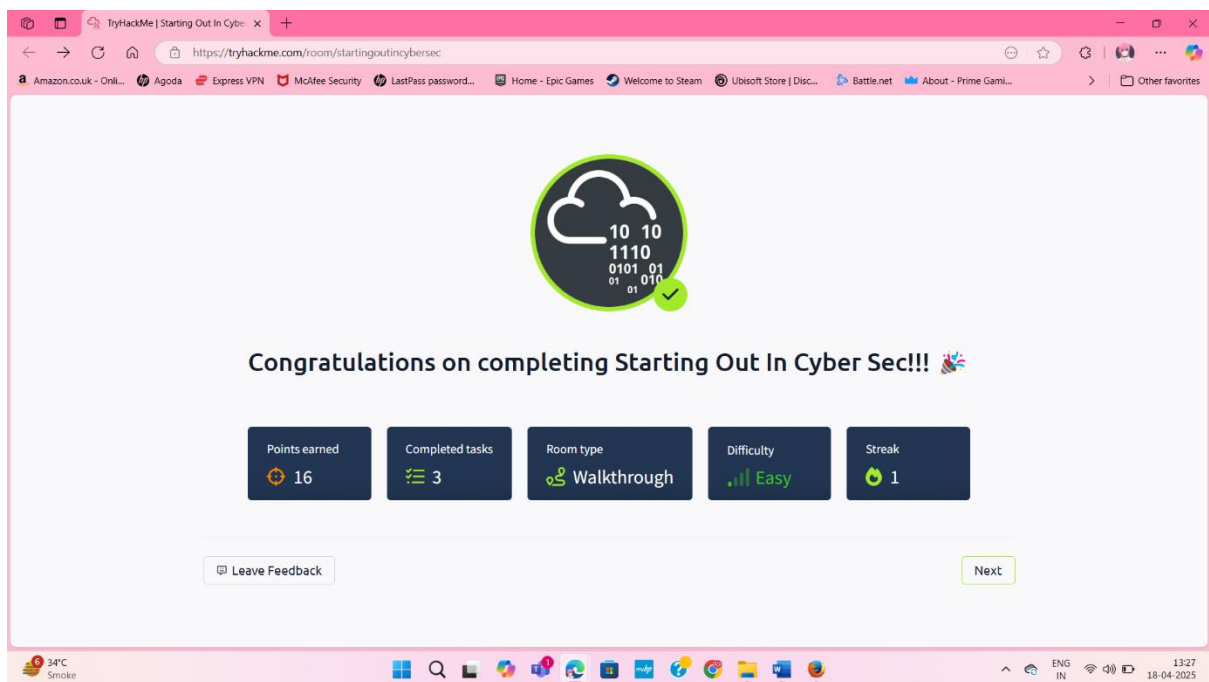
- Blue Team pathways (Splunk, Volatility).

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):

- Burp Suite mode: Repeater.
- Windows hash format: NTLM.

2. Task 3 (CVEs): Found:

- WPForms XSS: CVE-2020-10385.
- 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.

TryHackMe | Introductory Research

https://tryhackme.com/room/intrototherearch

Amazon.co.uk - Onli...AgodaExpress VPNMcAfee SecurityLastPass password...Home - Epic GamesWelcome to SteamUbisoft Store | Disc...Battle.netAbout - Prime Gami...Other favorites

Congratulations on completing Introductory Researching!!! 🎉

Points earned
104

Completed tasks
5

Room type
Walkthrough

Difficulty
Easy

Streak
1

Leave Feedback

Next

Sports headline
Delhi Capitals' b...

ENG
IN

14:32
18-04-2025