TryHackMe Room Completion Report

User: Atharva Manish Naik
Platform: https://tryhackme.com
Course Path: Beginner Path
Date of Completion: 17th April 2025

---

1. Hello World

Tools Accessed:

- No external tools used; browser-based interaction only.

Access Method:

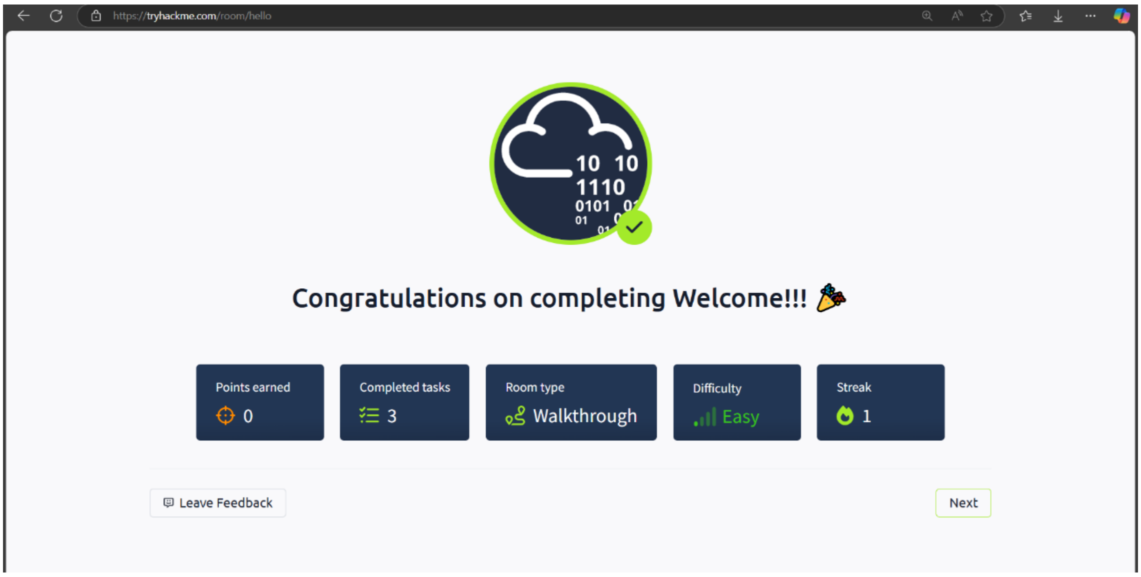
- Accessed directly through TryHackMe web interface (no VPN required).

Concepts Learned:

- Introduction to the TryHackMe interface
- How rooms and tasks are structured
- Understanding the deployment of virtual machines

Notes:

- Every room has a set of tasks, sometimes with deployed machines.
- Tasks often include hints and answers that reinforce concepts.
- A good starting point for absolute beginners.



Congratulations on completing Welcome!!! 🎉

Points earned	Completed tasks	Room type	Difficulty	Streak
0	3	Walkthrough	Easy	1

2. How to Use TryHackMe

🔧 Tools Accessed:

- None (browser-based walkthrough)

📥 Access Method:

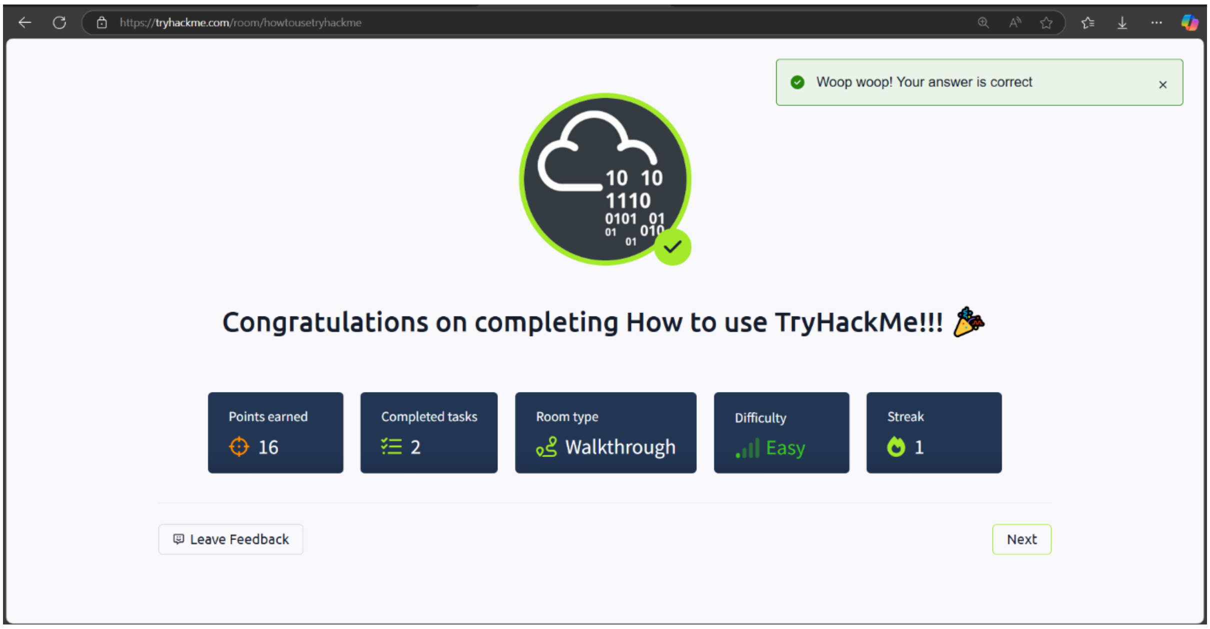
- Web interface with no machine deployment.

🗃 Concepts Learned:

- Site navigation
- Dashboard, streaks, and room organization
- How progress and ranks work
- How to submit answers

📝 Notes:

- Rooms can be public or private (linked or invited).
- Flags are usually in the form of **THM{}** or clear answers.
- Questions are usually case-insensitive.



https://tryhackme.com/room/howtousetryhackme

Woop woop! Your answer is correct

Congratulations on completing How to use TryHackMe!!! 🎉

Points earned 16

Completed tasks 2

Room type Walkthrough

Difficulty Easy

Streak 1

3. Getting Started

🔧 Tools Accessed:

- None required initially

📥 Access Method:

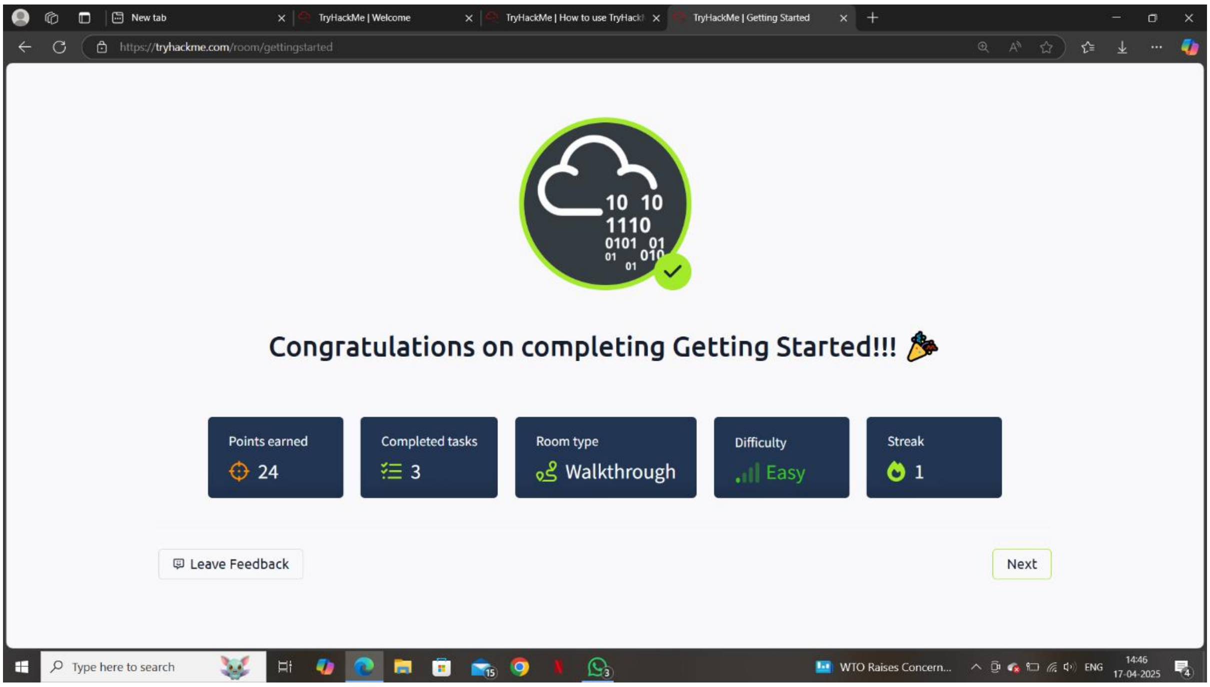
- Some tasks included deploying a machine (access via in-browser Kali or your own terminal using OpenVPN)

📚 Concepts Learned:

- Launching and connecting to target machines
- Differences between AttackBox (browser VM) vs own Kali/Parrot setup
- Using the split view for labs and reading content

📝 Notes:

- Recommended to test both AttackBox and VPN access.
- Focus on understanding how to connect to TryHackMe virtual labs.



Congratulations on completing Getting Started!!! 🎉

Points earned	Completed tasks	Room type	Difficulty	Streak
24	3	Walkthrough	Easy	1

4. TryHackMe Tutorial

Tools Accessed:

- AttackBox or Local Kali Linux
- Terminal / Browser

Access Method:

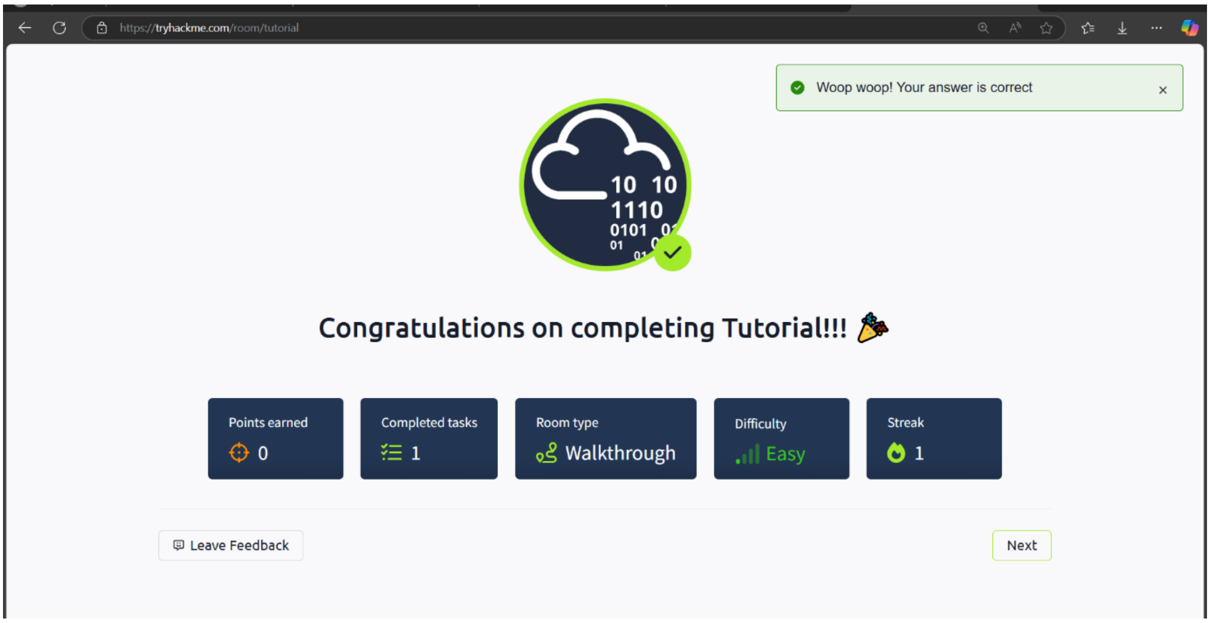
- Used the AttackBox and OpenVPN for local machine access
- Deployed beginner-friendly target machines

Concepts Learned:

- How to interact with a VM via SSH and web services
- Basic Linux commands like ls, cd, cat
- Submitting answers from machine output

Notes:

- First hands-on experience with interacting with machines
- Learned to use web browser to interact with vulnerable services
- SSH command: **ssh user@MACHINE_IP**



Woop woop! Your answer is correct

Congratulations on completing Tutorial!!! 🎉

Points earned 0

Completed tasks 1

Room type Walkthrough

Difficulty Easy

Streak 1

5. OpenVPN Configuration

🔧 Tools Accessed:

- OpenVPN
- Terminal (Linux or WSL)

📥 Access Method:

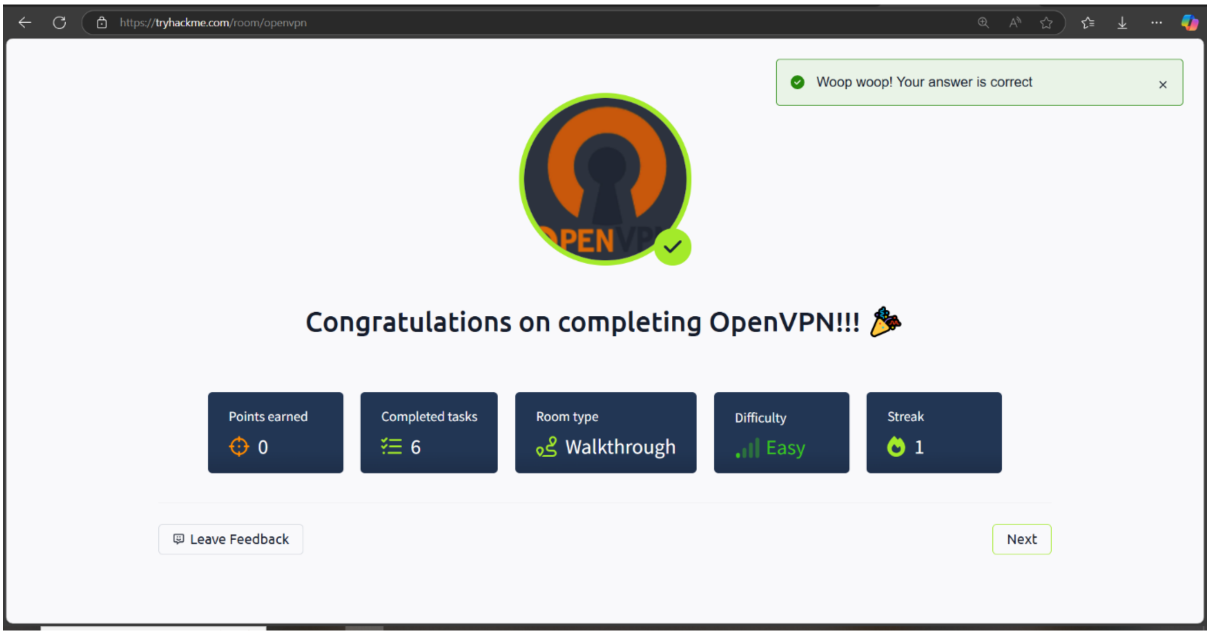
- Config file downloaded from THM and connected via terminal using

📚 Concepts Learned:

- How VPN tunnels work
- Connecting to the TryHackMe network from a personal machine
- Troubleshooting connectivity issues (firewall, permissions)

📝 Notes:

- Always run OpenVPN with sudo
- Keep the connection active during the entire session
- Make sure tun0 interface appears with **ifconfig**



https://tryhackme.com/room/openvpn

✓ Woop woop! Your answer is correct ×

Congratulations on completing OpenVPN!!! 🎉

Points earned 0

Completed tasks 6

Room type Walkthrough

Difficulty Easy

Streak 1

6. Beginner Path Introduction

Tools Accessed:

- No tools, informational room

Access Method:

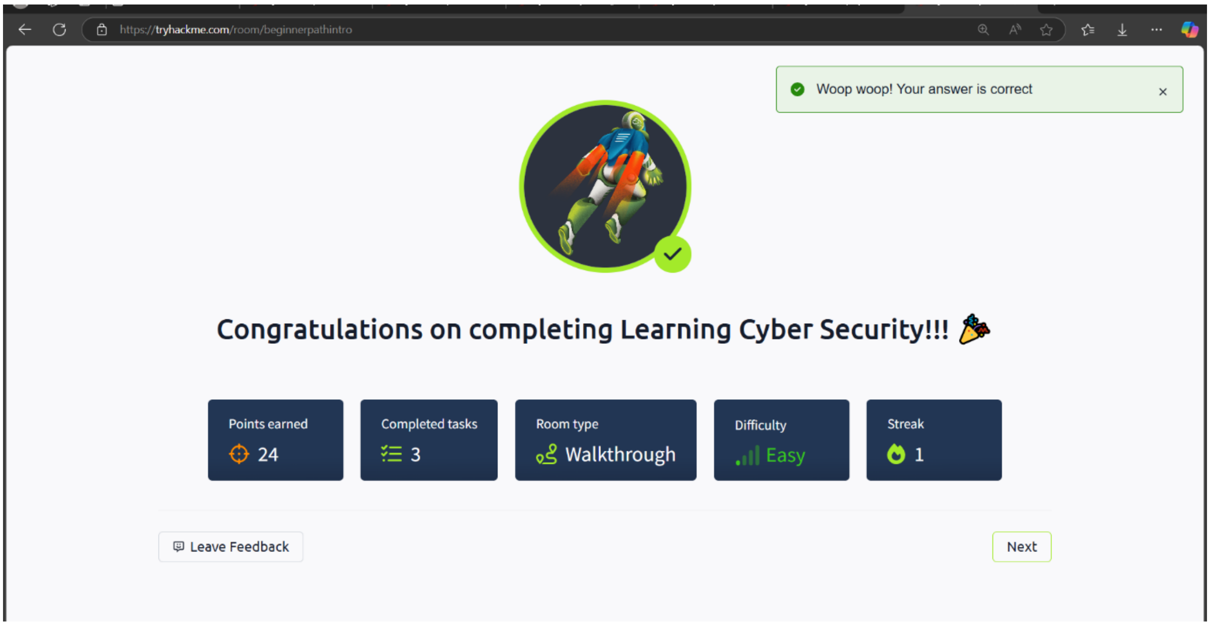
- Web-based room with written content

Concepts Learned:

- Overview of what to expect in the Beginner Path
- Basic cybersecurity fields: networking, web hacking, Linux
- Importance of hands-on learning

Notes:

- This room serves as a map for your journey.
- Encourages practice and not just theory.
- Beginner path is designed for newcomers, no prior experience needed.



https://tryhackme.com/room/beginnerpathintro

Woop woop! Your answer is correct

Congratulations on completing Learning Cyber Security!!! 🎉

Points earned 24

Completed tasks 3

Room type Walkthrough

Difficulty Easy

Streak 1

7. Starting Out in Cyber Security

🔧 Tools Accessed:

- None directly required; browser and terminal references only.

📥 Access Method:

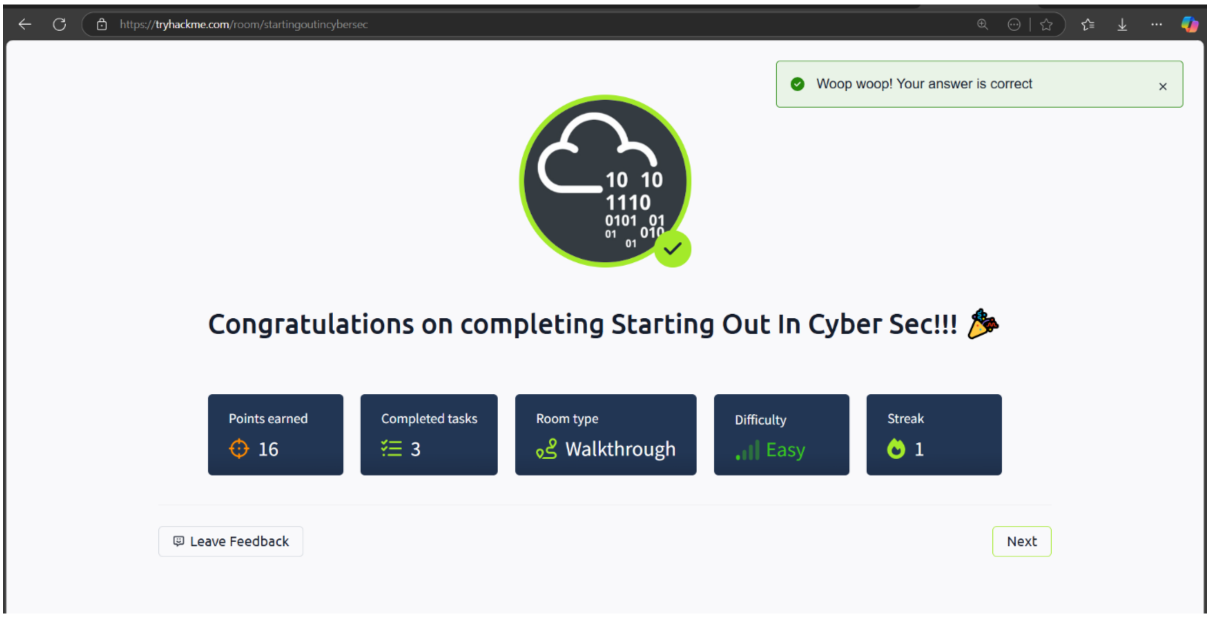
- Web-based content, no machine interaction

📚 Concepts Learned:

- Introduction to various cybersecurity careers:
  - Penetration Testing
  - Security Operations (SOC)
  - Malware Analysis
- Basic terminology: Threat, Vulnerability, Exploit
- Certifications and learning roadmap (e.g., CompTIA, OSCP)

📝 Notes:

- Great room to decide which cyber domain interests you
- Set expectations for learning pace and discipline
- Practical experience is more valuable than just theory



https://tryhackme.com/room/startingoutincybersec

✓ Woop woop! Your answer is correct

Congratulations on completing Starting Out In Cyber Sec!!! 🎉

Points earned: 16

Completed tasks: 3

Room type: Walkthrough

Difficulty: Easy

Streak: 1

8. Introduction to Research

Tools Accessed:

- Google
- Terminal (for some optional exercises)
- Cybersecurity platforms like MITRE ATT&CK, CVE database

Access Method:

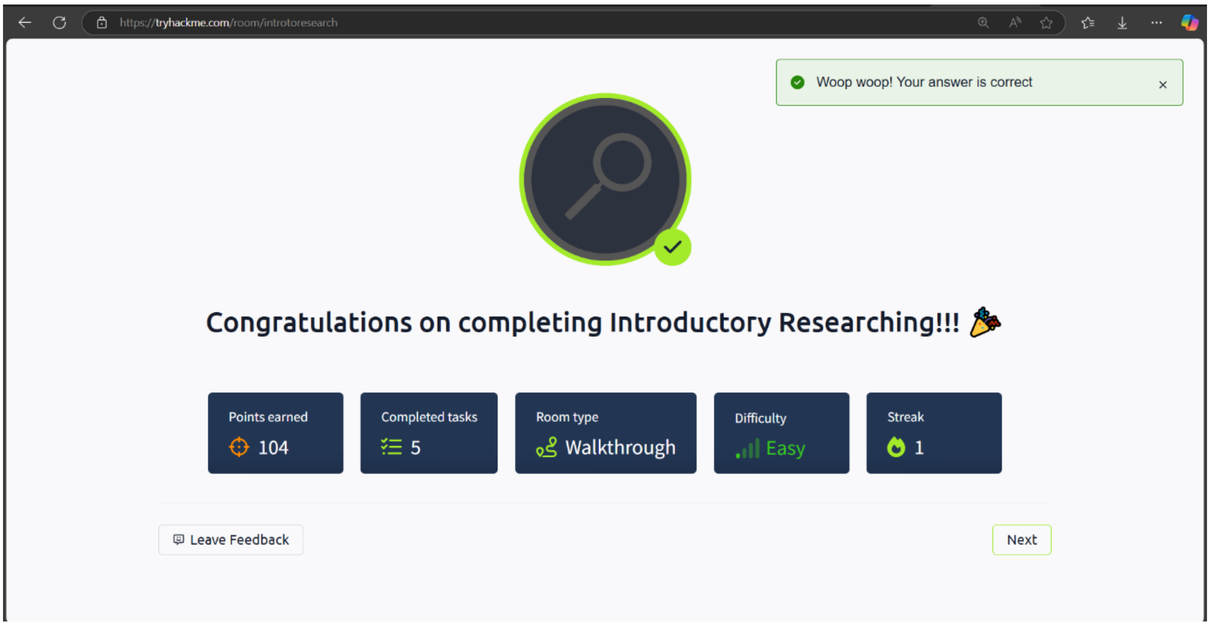
- Web-based tasks; optional practical exercises

Concepts Learned:

- How to Google efficiently (using site:, filetype:, etc.)
- How to research vulnerabilities, exploits, and tools
- Importance of understanding terminology when Googling

Notes:

- Research is a key skill for any security role
- Tools change; researching helps you keep up



Woop woop! Your answer is correct

Congratulations on completing Introductory Researching!!! 🎉

Points earned	Completed tasks	Room type	Difficulty	Streak
104	5	Walkthrough	Easy	1

Conclusion

Completing these initial TryHackMe rooms has provided a solid foundation in cybersecurity principles, lab navigation, and beginner tools. The guided, hands-on approach helps solidify theoretical concepts. From using VPN connections and interacting with VMs to beginning research techniques, these rooms lay the groundwork for the more technical challenges ahead.