ROOM (1)

ROOM NAME: HELLO WORLD

LINK: https://tryhackme.com/room/hello

LEARNING OBJECTIVES:

- Get introduced to TryHackMe's virtual environment
- Understand how rooms and machines work
- Learn to connect to a deployed machine and retrieve a flag

KEY TOOLS/COMMAND USED:

- OpenVPN (to connect to TryHackMe network)
- Web browser (to access the machine IP)

CONCEPTS LEARNED:

- How TryHackMe rooms are structured
- How to deploy a virtual machine (VM)
- How to access a VM using its IP address
- Introduction to retrieving flags

WALKTHROUGH / HOW YOU SOLVE IT:

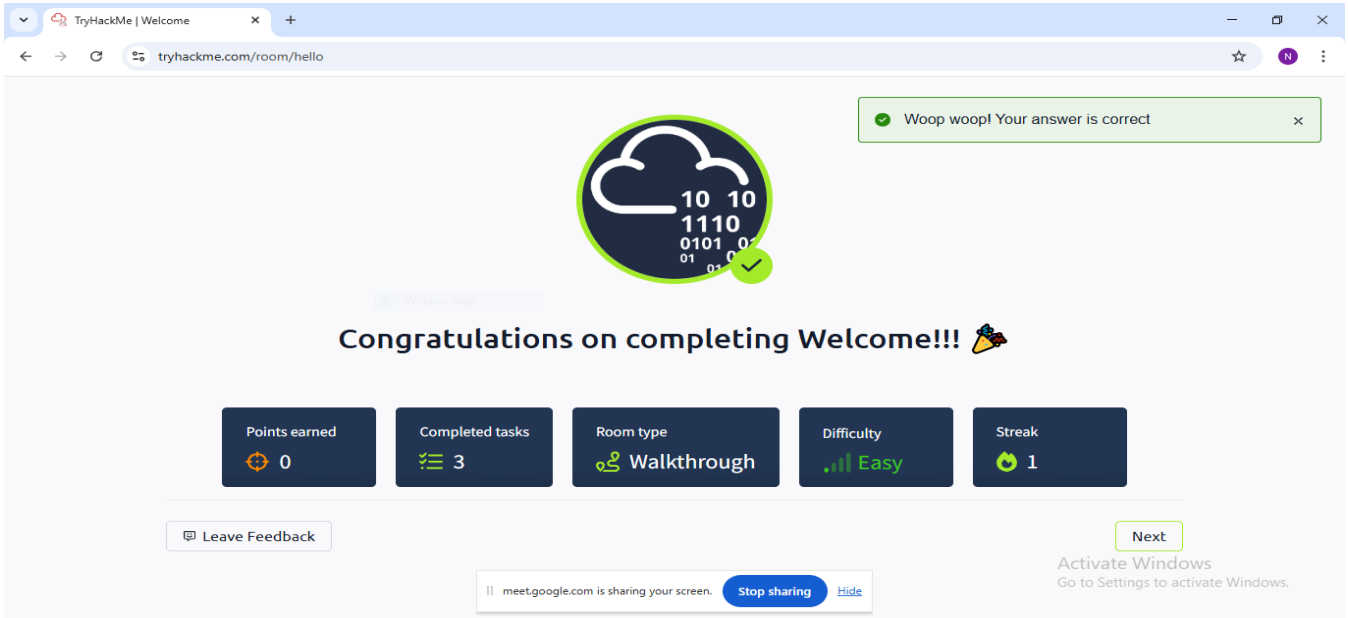
1. Joined the Hello World room on TryHackMe.
2. Started the machine by clicking the green "Start Machine" button.
3. Connected to the TryHackMe network using OpenVPN with a downloaded .ovpn file.
4. Once connected, copied the machine IP address (e.g., 10.10.135.165).
5. Opened the browser and visited: http://10.10.135.165
6. The web page loaded and displayed a flag in the format **flag{connection_verified}**
7. Copied and submitted the flag in the TryHackMe task for validation.

REFLECTIONS OR NOTES:

- VPN setup was a bit tricky, but once it was configured correctly, accessing machines was smooth.
  - Important to wait at least 30–60 seconds for machines to boot.
  - Make sure to use the right IP and check if the machine uses a different port like 8080.

EXAMPLE FLAG: WHAT I FOUND

flag{connection_verified}



ROOM(2)

ROOM NAME: HOWTOUSETRYHACKME

LINK: https://tryhackme.com/room/howtousetryhackme

LEARNING OBJECTIVES:

- Understand the basic layout and navigation of the TryHackMe platform
- Learn how rooms, tasks, and virtual machines are structured
- Get familiar with how to interact with the learning content and solve tasks

KEY TOOLS/COMMAND USED:

- TryHackMe's browser interface
- No external tools required
- Scroll, click, and answer-based interaction

CONCEPTS LEARNED:

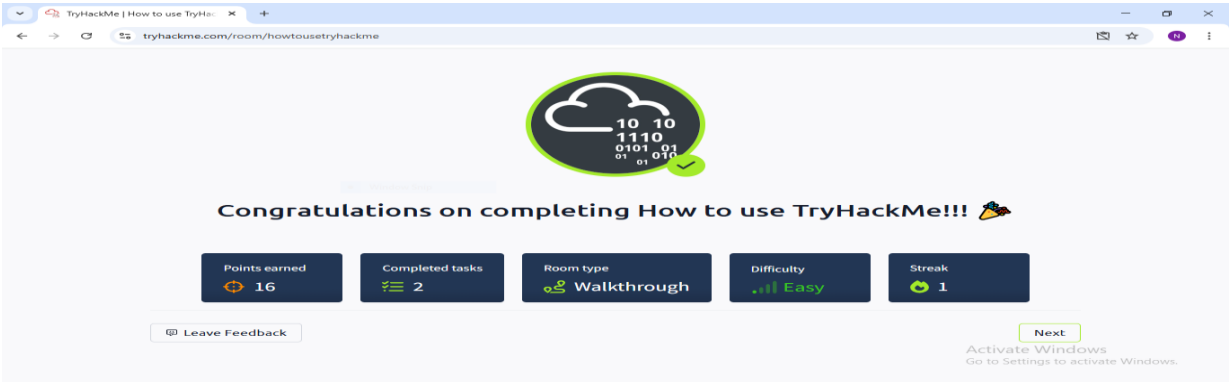
- What a TryHackMe "room" is
- How to interact with tasks inside a room
- What flags are and how to submit them
- Overview of deploying and accessing virtual machines
- How to use the in-browser AttackBox and connect using OpenVPN

WALKTHROUGH/HOW TO SOLVE IT:

1. Visited the room: How to Use TryHackMe
2. Read through the informational sections to understand:
    - The structure of rooms and tasks
    - What a deployed machine is
    - How to use the Answer boxes
3. Attempted each task in sequence:
    - Submitted simple answers like "TryHackMe" when prompted
    - Learned about using both the AttackBox and VPN setup
4. Recalled from experience how to:
    - Start a machine
    - Open it using the given IP
    - Submit the correct flag

REFLECTIONS OR NOTES:

- This room is extremely helpful for first-time users of TryHackMe
- The visual explanations make it easy to understand how to proceed in future rooms
- Clear and concise — a great onboarding experience
- Now confident in navigating the platform and submitting flags



ROOM (3)

ROOM NAME: Getting Started

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

LEARNING OBJECTIVES:

- Learn the basics of how TryHackMe rooms work
- Understand what tasks, flags, and machines are
- Practice answering questions and using hints
- Get comfortable with the learning flow on TryHackMe

KEY TOOLS/COMMANDS USED

- TryHackMe platform (Browser)
- OpenVPN
- Web Browser (to access VM via IP)

CONCEPTS LEARNED

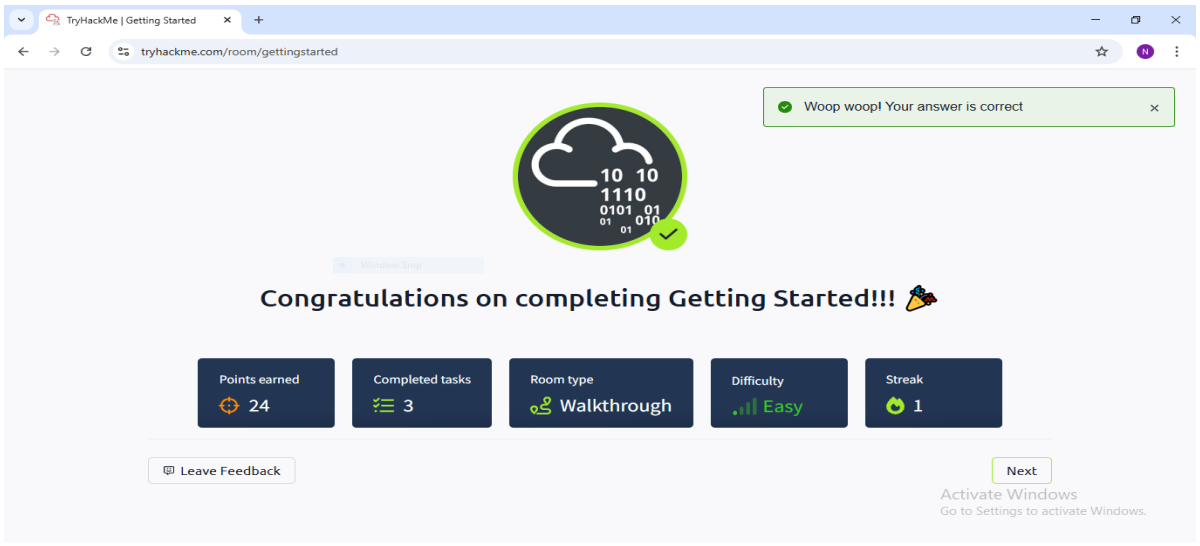
- Difference between informational and challenge-based tasks
- Importance of reading room descriptions carefully
- Using the web interface to deploy and interact with machines
- How to view and submit flags
- Understanding VM deployment timing and VPN connection importance

WALKTHROUGH / HOW YOU SOLVED IT

1. Accessed the room “Getting Started” on TryHackMe.
2. Read through the introduction which explains room structures.
3. Started the machine and copied its IP (e.g., 10.10.45.230).
4. Connected to the TryHackMe network using OpenVPN.
5. Opened the browser and visited the IP of the deployed VM.
6. Answered the question.

REFLECTIONS OR NOTES

- A very helpful beginner-level room that builds confidence
- The explanations are detailed and interactive
- Learned the importance of carefully reading task instructions
- Realized how hints can help without giving direct answers
- Reinforced the importance of being patient while waiting for machines to boot



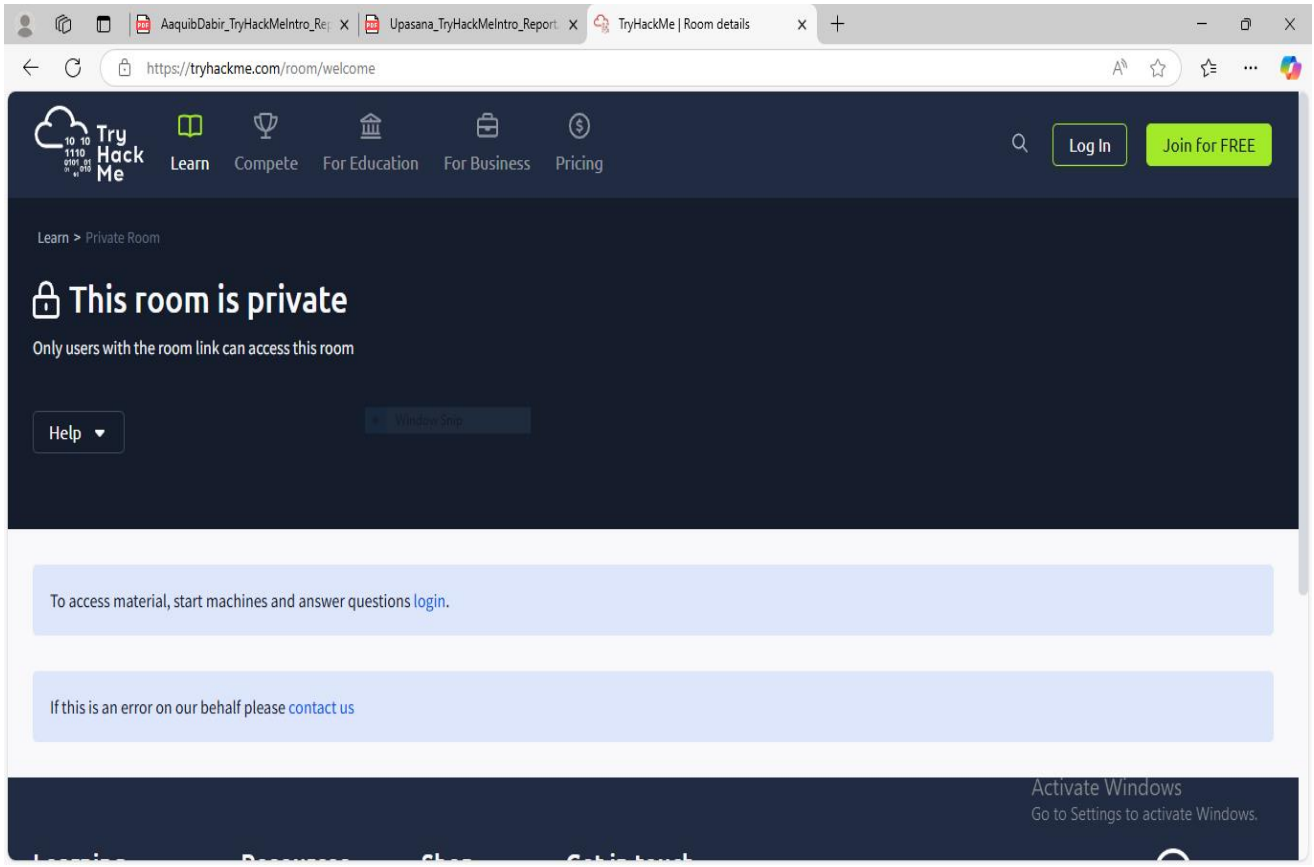
ROOM (4)

ROOM NAME: Welcome

Link: https://tryhackme.com/room/welcome

LEARNING OBJECTIVES:

- Understand the purpose of TryHackMe as a cybersecurity learning platform
- Learn about different learning paths and how to get started
- Get an overview of room types: theoretical, practical, CTFs, and challenges
- Know how to navigate the dashboard, profile, and progress tracking
- Begin your journey into cybersecurity with guided and hands-on learning



ROOM(5)

ROOM NAME: TRYHACKME TUTORIAL

LINK: https://tryhackme.com/room/tutorial

LEARNING OBJECTIVES:

- Learn how to use the TryHackMe interface effectively
- Understand how to interact with tasks, submit flags, and use hints
- Practice basic Linux commands in the in-browser terminal
- Navigate between tasks, rooms, and learning paths
- Learn the basics of how virtual machines and the AttackBox function.

KEY TOOLS/COMMANDS USED

- AttackBox (web-based virtual machine)
- Firefox (inside AttackBox)
- Linux Terminal
- OpenVPN (alternative method)

CONCEPTS LEARNED

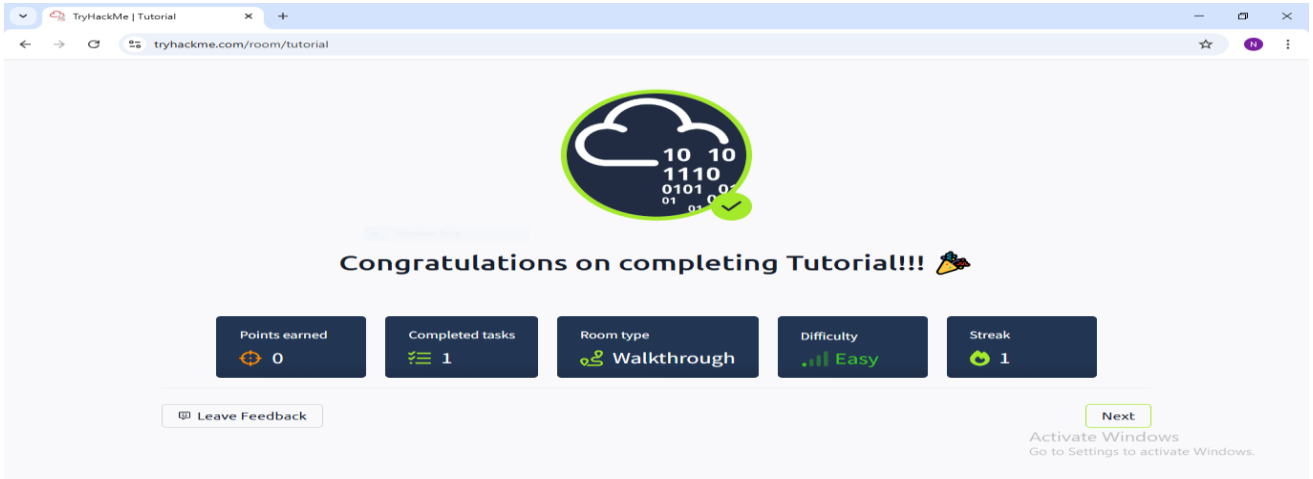
- How to start and use the AttackBox
- Accessing target machines via browser using internal IPs
- Understanding the concept of flags in cybersecurity
- Difference between target machines and the AttackBox
- Importance of terminating machines after use

WALKTHROUGH / HOW YOU SOLVED IT

1. Launched the **AttackBox** using the blue button at the top of the room.
2. Started the **target machine** using the green "Start Machine" button.
3. Waited for around 1 minute for the machine to be fully deployed.
4. Copied the IP address of the target machine.
5. Opened **Firefox** inside the AttackBox and pasted the IP in the browser's address
6. The web page loaded and displayed a **flag.**
7. Copied the flag and submitted it in the task for validation.
8. Terminated the machine after use.

REFLECTIONS OR NOTES

- The distinction between AttackBox and target machines became clearer
- Helpful room to visualize the structure of TryHackMe challenges
- Browser access via IP was a fun and practical way to engage
- Always remember to wait before accessing the VM and terminate after use



ROOM(6)

ROOM NAME: OpenVPN Configuration

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

LEARNING OBJECTIVES

- Understand what OpenVPN is and how it enables secure access to TryHackMe
- machines
- Learn to download your unique .ovpn configuration file
- Practice setting up a VPN connection using your terminal
- Verify successful VPN connection to access TryHackMe's internal network
- Troubleshoot basic connectivity issues

KEY TOOLS/COMMANDS USED

- OpenVPN (for secure connection to TryHackMe network)
- sudo openvpn your_file.ovpn
- Terminal / Command Line Interface
- Web browser (to test machine access)

CONCEPTS LEARNED

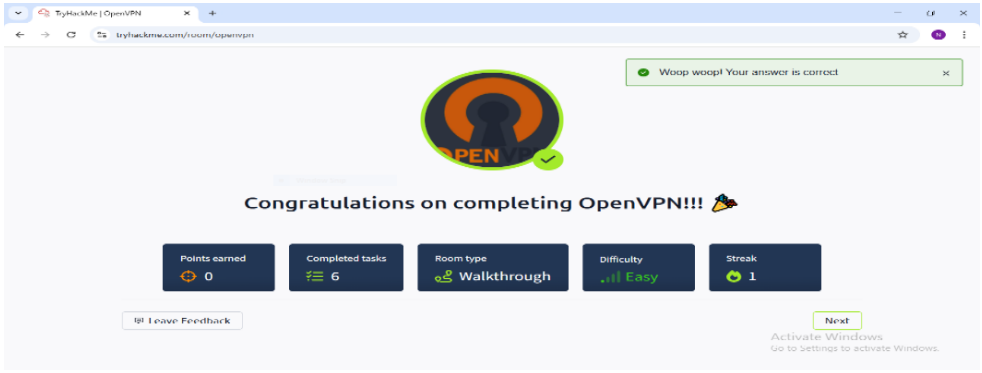
- The purpose of a VPN in cybersecurity labs
- How to download and store .ovpn configuration files securely
- How OpenVPN tunnels your traffic to TryHackMe machines
- Verifying the VPN tunnel using Initialization Sequence Completed
- Testing access by pinging internal IPs or loading machine IPs in the browser

WALKTHROUGH / HOW YOU SOLVED IT

1. Navigated to the OpenVPN Configuration room and read the tasks thoroughly.
2. Downloaded my personal .ovpn configuration file from the Access page on TryHackMe.
3. Installed OpenVPN on my system (if not already installed).
4. Opened a terminal and navigated to the directory where the .ovpn file was stored.
5. Ran the command: sudo openvpn your_file.ovpn
6. Waited until the terminal showed: Initialization Sequence Completed, which confirmed the VPN tunnel was successfully created.
7. Started a machine in any room (e.g., Hello World), copied its IP, and accessed it in a browser to confirm the VPN connection worked.
8. Used Ctrl+C to terminate the VPN session after testing.
9. Marked all tasks as complete in the room.

REFLECTIONS OR NOTES

- The VPN setup was essential for accessing TryHackMe machines outside the AttackBox
- OpenVPN gives you full terminal and browser control for advanced use cases
- Remember to always start the VPN before launching rooms (if not using the AttackBox)



ROOM(7)

ROOM NAME: BEGINNER PATH INTRODUCTION

LINK: https://tryhackme.com/room/beginnerpathintro

LEARNING OBJECTIVES

- Understand what the TryHackMe Beginner Path is and who it's for
- Get a high-level overview of cybersecurity learning categories (e.g., networking, Linux, web hacking, etc.)
- Learn how the path is structured and how rooms gradually build knowledge
- Gain confidence as a beginner to follow a clear, guided path in cybersecurity

KEY TOOLS/COMMANDS USED

- OPENVPN used in this room
- Navigation through TryHackMe platform and learning interface CONCEPTS LEARNED
- TryHackMe Beginner Path is tailored for those with little or no cybersecurity experience
- The path is divided into modules like "Introduction to Cyber Security," "Web Hacking," "Pre-Security," etc.
- The approach is hands-on and interactive, making it easier to grasp foundational topics
- Helps identify the learner's interest—whether it's ethical hacking, Blue Team, or Red Team
- Understanding learning progression and certification preparation (like CompTIA Security+ or CEH)

WALKTHROUGH / HOW YOU SOLVED IT

1. Opened the Beginner Path Introduction room on TryHackMe.
2. Read through the entire room content to understand the path's purpose and layout.
3. Noted the structure of modules and submodules.
4. Explored a few linked modules such as "Introduction to Cyber Security" and "Web Fundamentals".
5. Completed all the tasks by marking them as done.
6. Reflected on how the path aligns with my cybersecurity goals and interests.

REFLECTIONS OR NOTES

- This room helped clarify how to proceed with my learning journey in cybersecurity
- Motivating to see a clear roadmap from beginner to advanced topics
- It was helpful in identifying which topics I'm most curious about (especially web and ethical hacking)
- The path system takes away the overwhelm and makes learning structured and achievable

ROOM(8)

ROOM NAME: STARTING OUT WITH CYBERSEC

LINK: https://tryhackme.com/room/startingoutincybersec

LEARNING OBJECTIVES

- Understand what cybersecurity is and why it's important in today's world
- Explore different roles in the cybersecurity industry (e.g., Penetration Tester, SOC Analyst, Security Engineer)
- Learn about key areas such as hacking, networking, Linux, web application security, and more
- Discover how to get started based on your background—technical or nontechnical
- Get tips on building a learning path and accessing resources to grow in cybersecurity

KEY TOOLS/COMMANDS USED

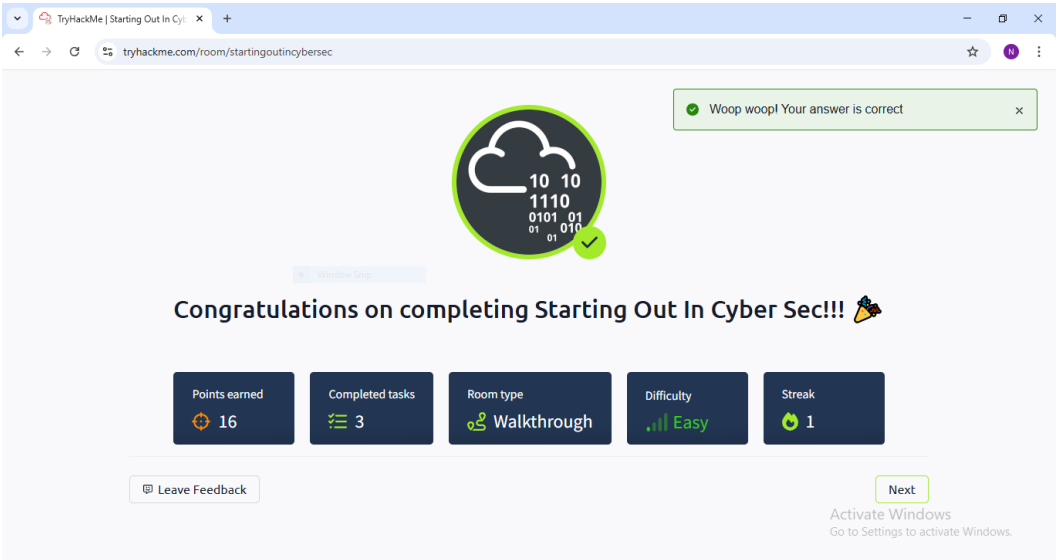
- No technical tools required
- Platform navigation and resource exploration through TryHackMe interface

CONCEPTS LEARNED

- Cybersecurity is a field focused on protecting digital assets and systems
- There are multiple career paths: Red Team (offensive), Blue Team (defensive), and more
- Essential skills include knowledge of networking, operating systems (especially Linux), and understanding vulnerabilities
- Soft skills like curiosity, consistency, and problem-solving are equally important
- Learning platforms like TryHackMe help bridge the gap between theory and practical hands-on experience

WALKTHROUGH / HOW YOU SOLVED IT

1. Opened the Starting Out in Cyber Security room on TryHackMe.
2. Carefully read through all sections explaining different domains and career roles.
3. Took note of beginner-friendly recommendations (e.g., learning Linux, basic networking, web hacking).
4. Explored career advice on building a cybersecurity resume and using platforms like LinkedIn and GitHub.
5. Completed the tasks and questions within the room to solidify understanding.
6. Reflected on which domain excites me most—in this case, Red Team (offensive security).



ROOM(9)

ROOM NAME: Introduction to Research

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

LEARNING OBJECTIVES

- Learn the importance of research in cybersecurity
- Understand how to effectively search for information and troubleshoot issues
- Develop skills to analyse problems, read documentation, and use community resources
- Get introduced to responsible disclosure and professional conduct while researching vulnerabilities
- Build self-reliance and confidence in solving cybersecurity problems independently

KEY TOOLS/COMMANDS USED

- Google Search and other search engines
- TryHackMe rooms and documentation
- Community platforms (Reddit, Stack Overflow, GitHub, etc.)
- Keywords and operators for more efficient searching (e.g., site:, intitle:, file type:)

CONCEPTS LEARNED

- Research is a core skill in cybersecurity—used for troubleshooting, learning, and discovering vulnerabilities
- Effective research includes: identifying the problem, using precise keywords, reading multiple sources, and verifying findings
- Reading documentation is more helpful than relying on just tutorials
- Communities and forums are great places to learn, ask, and contribute
- Always give credit, act ethically, and follow responsible disclosure when discovering security issues

WALKTHROUGH / HOW YOU SOLVED IT

1. Accessed the Introduction to Research room on TryHackMe
2. Went through the concepts and real-world use cases of research in cybersecurity
3. Practiced using Google Dorking techniques to narrow down search results
4. Explored examples of how research helped in Capture The Flag (CTF) challenges
5. Completed tasks that required using external resources and documentation to find solutions
6. Applied learned research techniques to a basic problem scenario given in the room

REFLECTIONS OR NOTES

- This room made me realize how powerful self-guided research is in cybersecurity
- I feel more capable of tackling unfamiliar problems by knowing where and how to look for help
- Responsible behaviour and ethics while researching were key takeaways