

ASSIGNMENT 1: Cyber-security internship

TryHackMe Room: [Hello World](#)

➤ Learning Objective

The "Hello World" room on TryHackMe introduces to the platform and how it works. We learn how to interact with the terminal, use common Linux commands, and access tasks in a guided environment. The room also familiarizes beginners with the layout, hints, and flags used throughout TryHackMe.

➤ Key Tools/Commands Used

TryHackMe Web Interface – Includes tabs like Task, AttackBox and Deploy Machine.

THM AttackBox – A cloud-based hacking environment provided in-browser.

Split View – Helps with copying commands and viewing terminal alongside tasks.

Flags- Special strings hidden in files or outputs that you submit as proof of task completion.

➤ Concepts Learned

TryHackMe Interface Basics – Getting comfortable with the layout, AttackBox, VM deployment, and task structure.

Cybersecurity Lab Workflow – How to approach challenges step-by-step in a virtualized hacking environment.

Understanding Flags – Learning what "flags" are and how to find/submit them as proof of task completion.

➤ Walkthrough / How You Solved It

1. Joining the Room- Logged into TryHackMe using credentials. Navigated to the "Hello World" room via the provided the link ([TryHackMe helloworld](#)).
2. Click 'Start Machine' to deploy the virtual machine. If you're using the AttackBox, launch it from the top bar.
3. Use the terminal inside the AttackBox (or your own VM if connected via VPN). Wait for the target IP to appear.
4. Copy the flag string. Paste it into the answer box on TryHackMe.

➤ Reflections or Notes

This task provided a smooth, beginner-friendly introduction to the TryHackMe platform. It helped me understand how virtual machines are deployed and how the AttackBox works. I learned how challenges are structured around finding "flags" as proof of task completion , a common format in cybersecurity labs.

LINUX FIREWALLS.pdfTryHackMe | DashboardTryHackMe | WelcomeTryHackMe | Access

https://tryhackme.com/room/hello

Woop woop! Your answer is correct

Congratulations on completing Welcome!!! 🎉

Points earned0

Completed tasks3

Room typeWalkthrough

DifficultyEasy

Streak1

Leave Feedback

Next

TryHackMe Room: [How to use TryHackMe](#)

➤ Learning Objective

The "How to Use TryHackMe" lab helps users understand how to navigate the platform effectively. It teaches how to deploy virtual machines, use the AttackBox, and interact with tasks. Users learn how to find and submit flags, use hints, and follow a structured learning path. The lab also covers basic terminal usage and accessing in-browser tools. It's designed to build comfort with the TryHackMe environment before starting more technical rooms.

➤ Key Tools/Commands Used

AttackBox – In-browser hacking machine provided by TryHackMe.

TryHackMe VM – Deployed virtual machine you connect to and interact with.

Terminal (CLI) – For entering Linux commands.

Task Panel – Where instructions, questions, and hints are displayed.

File Viewer (in browser) – Used to see file structures or contents in some tasks.

➤ Concepts Learned

How to Deploy and Use Virtual Machines – Learned how to start and connect to lab environments on TryHackMe.

Basic Linux Navigation – Practiced using commands like ls, cd, cat a real terminal.

Using the AttackBox – Learned to work with the in-browser hacking tool provided by TryHackMe.

Platform Navigation – Became familiar with task layout, hints, and how to answer questions.

➤ Walkthrough / How You Solved It

Start the Lab:- Click on "Start Machine" to deploy the virtual machine.

Connect:- You're using the AttackBox, launch it. Wait for the target machine's IP to appear. Open the terminal (inside the AttackBox or your own system).

List the Files: ls command

Location: cd command

Read files: cat<filename> [hello.txt]


➤ Reflections or Notes

This room is an excellent resource for beginners to understand how to navigate and use TryHackMe effectively. The gamified approach makes learning engaging, while hands-on labs provide practical experience. The structured guidance ensures users can confidently explore more advanced rooms after completing this one.

TryHackMe | How to use TryHackMe

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

🔥 2

Leave Feedback

Next

2 🔥

Your streak has increased.
You're 5 streaks away from a badge!

TryHackMe Room: [Getting Started](#)

➤ Learning Objective

The "Getting Started with TryHackMe" lab introduces users to the platform's interface and features. It teaches how to deploy virtual machines and use the AttackBox for hands-on practice. Users learn how to navigate tasks, find and submit flags, and use built-in hints. Basic Linux command-line usage is also covered.

The lab builds foundational skills needed to confidently begin cybersecurity learning on TryHackMe.

The "Getting Started with TryHackMe" lab introduces users to the platform's interface and features. It teaches how to deploy virtual machines and use the AttackBox for hands-on practice. Users learn how to navigate tasks, find and submit flags, and use built-in hints. Basic Linux command-line usage is also covered. It covers essential topics like accessing labs, navigating rooms, and understanding basic cybersecurity concepts.

➤ Key Tools/Commands Used

TryHackMe Platform – Web-based interface for completing tasks and tracking progress.

Deployed VM – Remote machine where you apply your commands.

Task Panel – Where questions, hints, and flag submission boxes are shown.

Terminal (CLI) – Command-line interface for interacting with the virtual machine.

VPN Configuration: Understood how to securely connect to TryHackMe labs using OpenVPN.

➤ Concepts Learned

1. Platform Navigation: How to find and join rooms, complete tasks, and track progress. Overview of features like "Learn," "Practice," "Compete," and "Networks."

2. Hands-On Labs: Deploying virtual machines for practical hacking exercises. Understanding the importance of secure connections via VPN.

3. Cybersecurity Basics: Introduction to ethical hacking principles and system security fundamentals.

4. Gamification Features: Earning points, maintaining streaks, and competing in leaderboards.

➤ Walkthrough / How You Solved It

1. Accessing the Room: Logged into TryHackMe and navigated to the "Getting Started" room via the provided link (TryHackMe Getting Started).

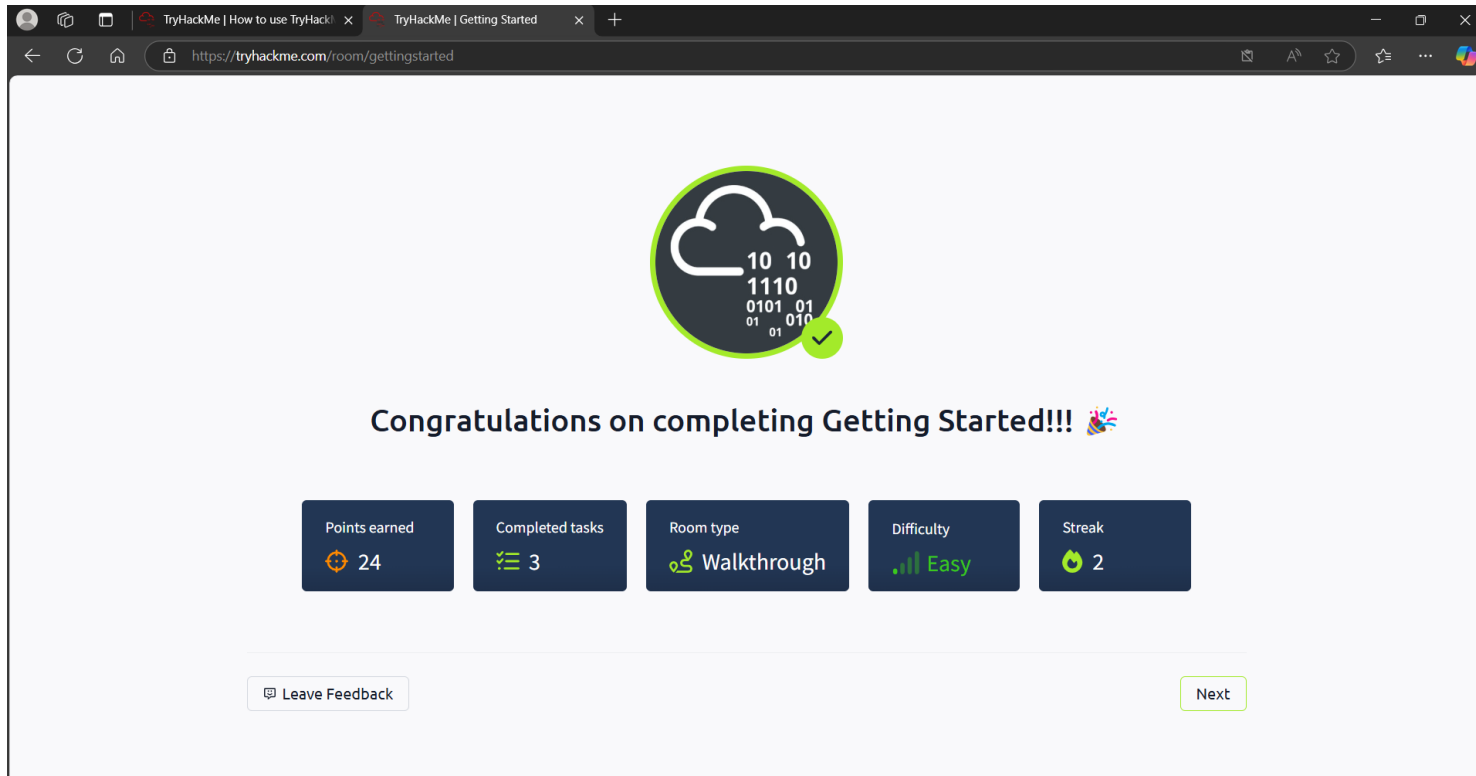
2. Exploring Content: Followed step-by-step instructions to understand the platform's features. Completed introductory tasks that demonstrated how to interact with labs.

3. Hands-On Practice: Deployed virtual machines for exercises. o Configured VPN for secure access to remote labs.

4. Task Completion: Answered questions based on room content and marked tasks as complete.

➤ Reflections or Notes

The "Getting Started" room is a valuable resource for beginners, providing clear guidance on using TryHackMe effectively. It emphasizes hands-on practice, which is crucial for building foundational cybersecurity skills. The gamified approach makes learning engaging while fostering a competitive spirit.



The screenshot shows a web browser window with two tabs: 'TryHackMe | How to use TryHackMe' and 'TryHackMe | Getting Started'. The address bar displays 'https://tryhackme.com/room/gettingstarted'. The main content area features a large circular icon with a cloud and binary code, and a green checkmark. Below the icon, the text 'Congratulations on completing Getting Started!!!' is displayed with a party popper emoji. A row of five dark blue boxes shows the following statistics: 'Points earned' (24), 'Completed tasks' (3), 'Room type' (Walkthrough), 'Difficulty' (Easy), and 'Streak' (2). At the bottom, there is a 'Leave Feedback' button and a 'Next' button.

Points earned: 24

Completed tasks: 3

Room type: Walkthrough

Difficulty: Easy

Streak: 2

Leave Feedback

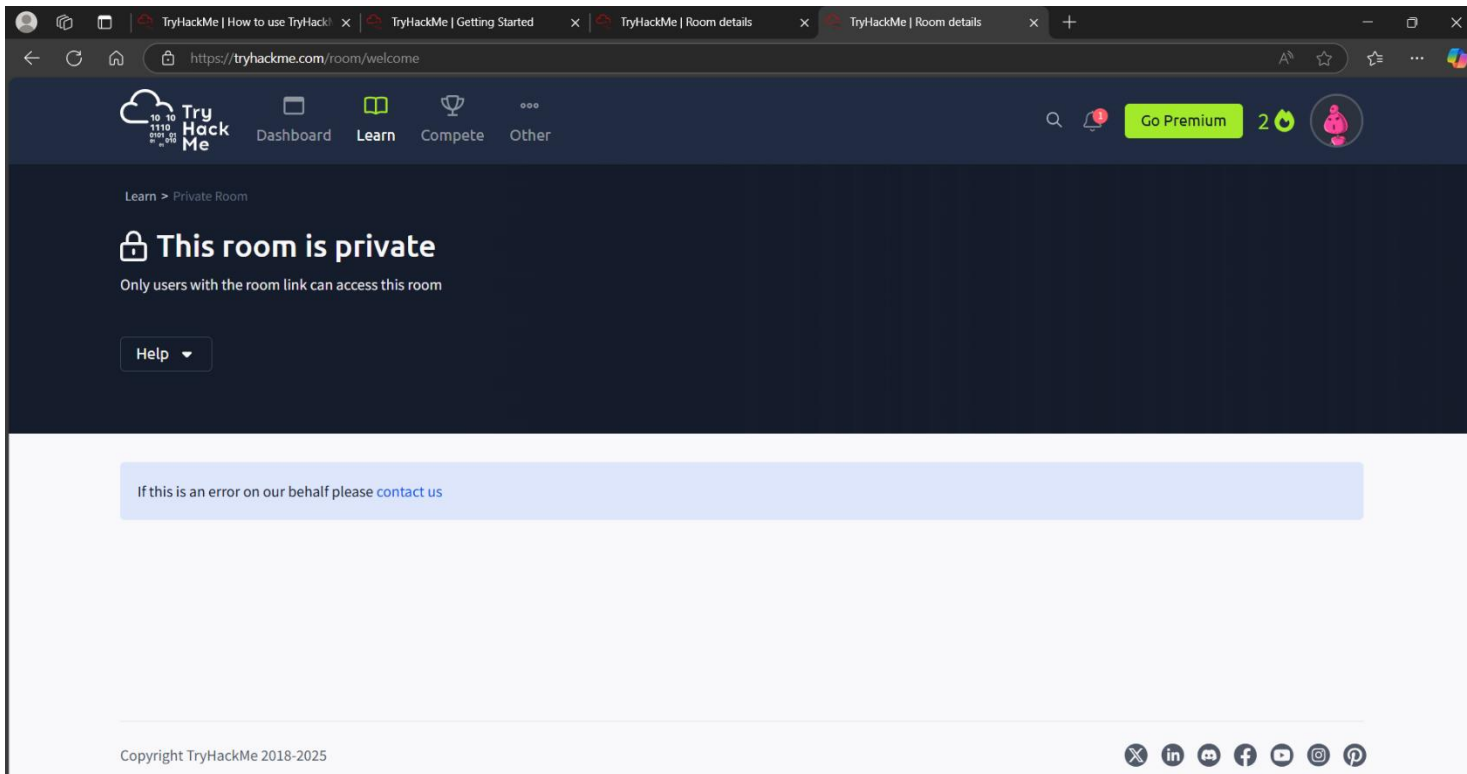
Next

TryHackMe Room:

TryHackMe Room: [Welcome](#)

➤ Learning Objective

The "Welcome" room on TryHackMe is designed as an introductory space for new users to familiarize themselves with the platform's goals and mission. It aims to provide a high-level overview of what TryHackMe offers and how it intends to help individuals learn cybersecurity in an engaging and practical way.



TryHackMe Room: [TryHackMe Tutorial](#)

➤ Learning Objective

The "TryHackMe Tutorial" room aims to guide users through the fundamental features of the TryHackMe platform. It introduces key concepts, navigation techniques, and interactive elements necessary for effectively engaging with the platform's cybersecurity learning content.

➤ Key Tools/Commands Used

- TryHackMe Task Panel – Where instructions, questions, and hints are displayed.
- AttackBox – In-browser virtual machine provided for hands-on practice.
- Deployed Virtual Machine (VM) – Remote system you interact with using terminal commands.
- Flag Submission Field – Where you enter answers or flags to complete tasks.

➤ Concepts Learned

- How to Navigate the TryHackMe Platform – Understanding the layout, task sections, and how to interact with labs.
- Using the AttackBox and VMs – Learning how to launch and work inside a virtual hacking environment
- Using Hints and Guided Help – Learning how to use built-in hints and walkthroughs effectively.
- Getting Comfortable with Hands-On Cybersecurity Learning – Building confidence in using tools and commands safely.

➤ Walkthrough / How You Solved It

- Accessing the Room: o Logged into TryHackMe and navigated to the "TryHackMe Tutorial" room via the provided link (TryHackMe Tutorial).
- Exploring Content: o Followed the tutorial's instructions to understand the room's structure and available features. o Completed tasks step-by-step, using hints when needed to clarify concepts.
- Hands-On Practice: o Deployed provided machines and utilized attack boxes to solve practical challenges. o Submitted answers for each task and tracked progress.
- Review and Completion: o Reviewed completed tasks and ensured all concepts were understood.

➤ Reflections or Notes

I learned how TryHackMe uses flags, hints, and a guided step-by-step format to help learners build cybersecurity skills at their own pace. The friendly, gamified approach sparked curiosity and motivated me to explore more rooms and start learning actual security concepts. This task provided a simple and interactive way to understand how TryHackMe works, including deploying machines and answering task questions.

✓ Woop woop! Your answer is correct x



Congratulations on completing Tutorial!!! 🎉

Points earned 🎯 0	Completed tasks 📋 1	Room type 👤 Walkthrough	Difficulty 📶 Easy	Streak 🔥 2
----------------------	------------------------	----------------------------	----------------------	---------------

🗉 Leave Feedback

Next

TryHackMe Room: [TryHackMe OpenVPN](#)

➤ Learning Objective

The OpenVPN task teaches you how to connect your local machine to TryHackMe's network using a secure VPN. You'll learn how to download and run your unique OpenVPN configuration file. This enables access to private lab machines outside the AttackBox. It prepares you for hands-on practice using your own device.

➤ Key Tools/Commands Used

OpenVPN – A VPN client used to connect your local machine to TryHackMe's network.

TryHackMe OpenVPN Configuration File– A unique file that contains connection settings for your account.

Terminal / Command Prompt – Used to run the VPN connection command.

TryHackMe Dashboard – For downloading your .ovpn file and checking connection status.

➤ Concepts Learned

- What a VPN Is – Learned the purpose of a VPN and how it creates a secure tunnel to TryHackMe's network.
- Downloading a Config File – Understood how to download and use the .ovpn file unique to your account.
- Using the Terminal to Connect – Practiced running the `openvpn` command to start a VPN connection.
- Verifying VPN Connection – Learned how to confirm a successful VPN connection to access TryHackMe labs.
- Troubleshooting Basics – Gained awareness of common issues (permissions, file paths, sudo) when using OpenVPN.
- Working from Your Own Machine – Built confidence in setting up a safe, remote lab environment on a personal device.

➤ Walkthrough / How You Solved It

1.Accessing the Room: Logged into TryHackMe and navigated to the "OpenVPN" room via the provided link (TryHackMe OpenVPN).

2.Downloading Configuration File: Followed instructions to download the appropriate OpenVPN configuration file.

3. Installing OpenVPN Client: Installed the OpenVPN client on the local machine (e.g., using `apt-get install openvpn` on Linux).

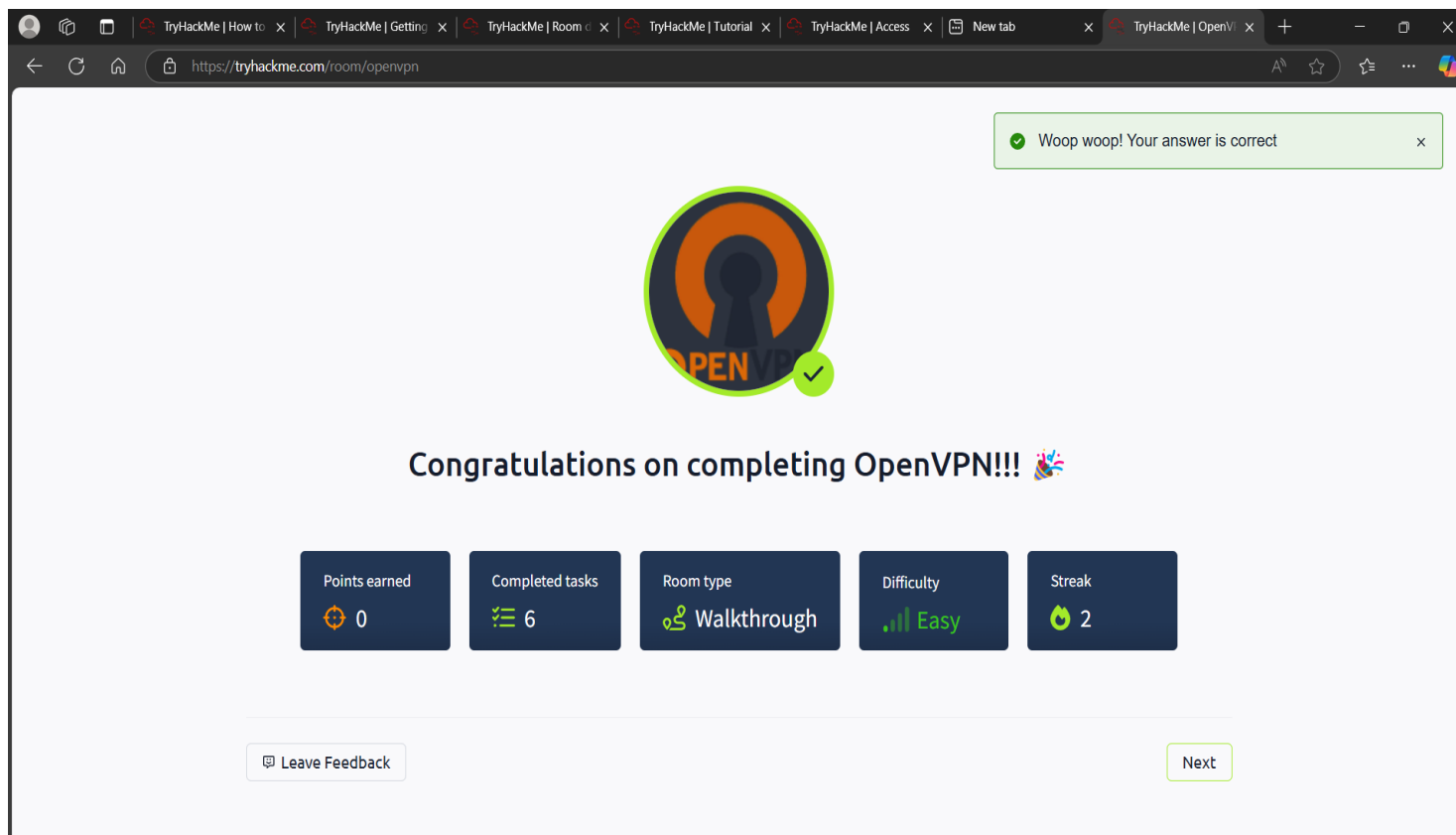
4. Connecting to VPN: Used the command line to connect to TryHackMe's network using the downloaded configuration file (`sudo openvpn .ovpn`).

5. Verifying Connection: Used `ifconfig` or `ip addr` to confirm the VPN interface (usually `tun0`) and assigned IP address. Verified the connection was successful by accessing TryHackMe resources.

6. Task Completion: Answered questions related to VPN setup and configuration.

➤ Reflections or Notes

This room is crucial for ensuring secure access to TryHackMe's labs and resources. It provides hands-on experience in configuring and verifying VPN connections, which is an essential skill in cybersecurity. Understanding how to troubleshoot VPN issues is valuable for maintaining a stable and secure connection.



TryHackMe Room: [TryHackMe Learning Beginner Path Intro](#)

➤ Learning Objective

The "Beginner Path Introduction" room on TryHackMe is designed to provide a comprehensive overview of the beginner learning path offered on the platform. It introduces users to the various modules, topics, and skills they will acquire as they progress through the path, setting a foundation for more advanced cybersecurity concepts.

➤ Key Tools/Commands Used

TryHackMe Learning Paths: Navigating and understanding the structure of learning paths.

Module Overviews: Reviewing the content and objectives of different modules within the path.

Room Previews: Exploring individual rooms and tasks included in the beginner path.

➤ Concepts Learned

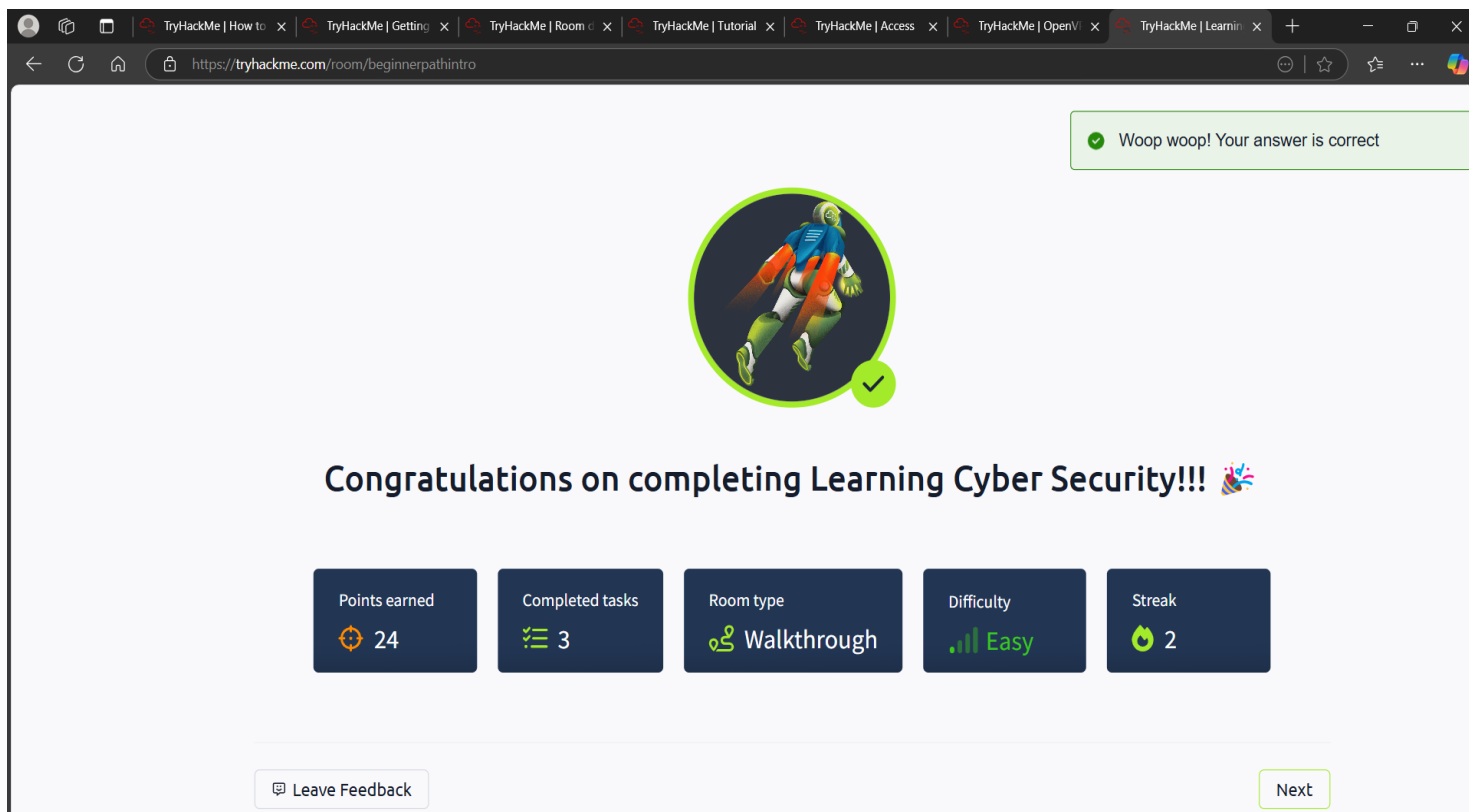
1. Learning Path Structure: Understanding how TryHackMe organizes content into structured learning paths. Identifying the different modules and topics covered in the beginner path.
2. Module Content: Reviewing the objectives and skills taught in each module, such as Linux fundamentals, web exploitation, and network security. Understanding the progression from basic to more advanced topics.
3. Skill Development: Recognizing the core cybersecurity skills that will be developed throughout the path. Understanding how to apply these skills in practical exercises and hands-on labs.
4. Resource Utilization: Identifying key resources within the learning path, such as tutorials, walkthroughs, and supplementary materials.

➤ Walkthrough / How You Solved It

1. Accessing the Room: Logged into TryHackMe and navigated to the "Beginner Path Introduction" room via the provided link (TryHackMe Beginner Path Introduction).
2. Exploring the Path Overview: Reviewed the introduction to the beginner path and its overall objectives. Navigated through the different modules to understand the content covered in each.
3. Reviewing Module Content: Examined the topics and skills taught in modules such as "Cybersecurity Fundamentals," "Web Hacking," and "Network Security." Understood the progression from basic to more advanced concepts.
4. Identifying Key Resources: Identified available resources, including tutorials, walkthroughs, and supplementary materials. Understood how to utilize these resources to enhance learning.
5. Task Completion: Answered questions related to the beginner path and its modules.

➤ Reflections or Notes

This room provides a valuable roadmap for users starting their cybersecurity journey on TryHackMe. It highlights the structured approach of the beginner path, ensuring a solid foundation in essential cybersecurity concepts. Understanding the path's content and objectives is crucial for effectively progressing through the modules and developing key skills.



TryHackMe Room: [TryHackMe Starting Out In Cyber Sec](https://tryhackme.com/room/beginnerpathintro)

➤ Learning Objective

The "Starting Out in Cyber Security" room on TryHackMe is designed to introduce users to the cybersecurity field. It provides an overview of different cybersecurity roles, essential skills, and learning paths, helping beginners understand the landscape and plan their career trajectory.

➤ Key Tools/Commands Used

- TryHackMe AttackBox – Browser-based virtual machine for solving tasks.
- Linux Terminal / Command Line – For interacting with remote systems.
- File System Navigation – Working with directories and files using terminal commands.
- Cybersecurity Role Descriptions: Reviewing the responsibilities and requirements of different roles.

➤ Concepts Learned

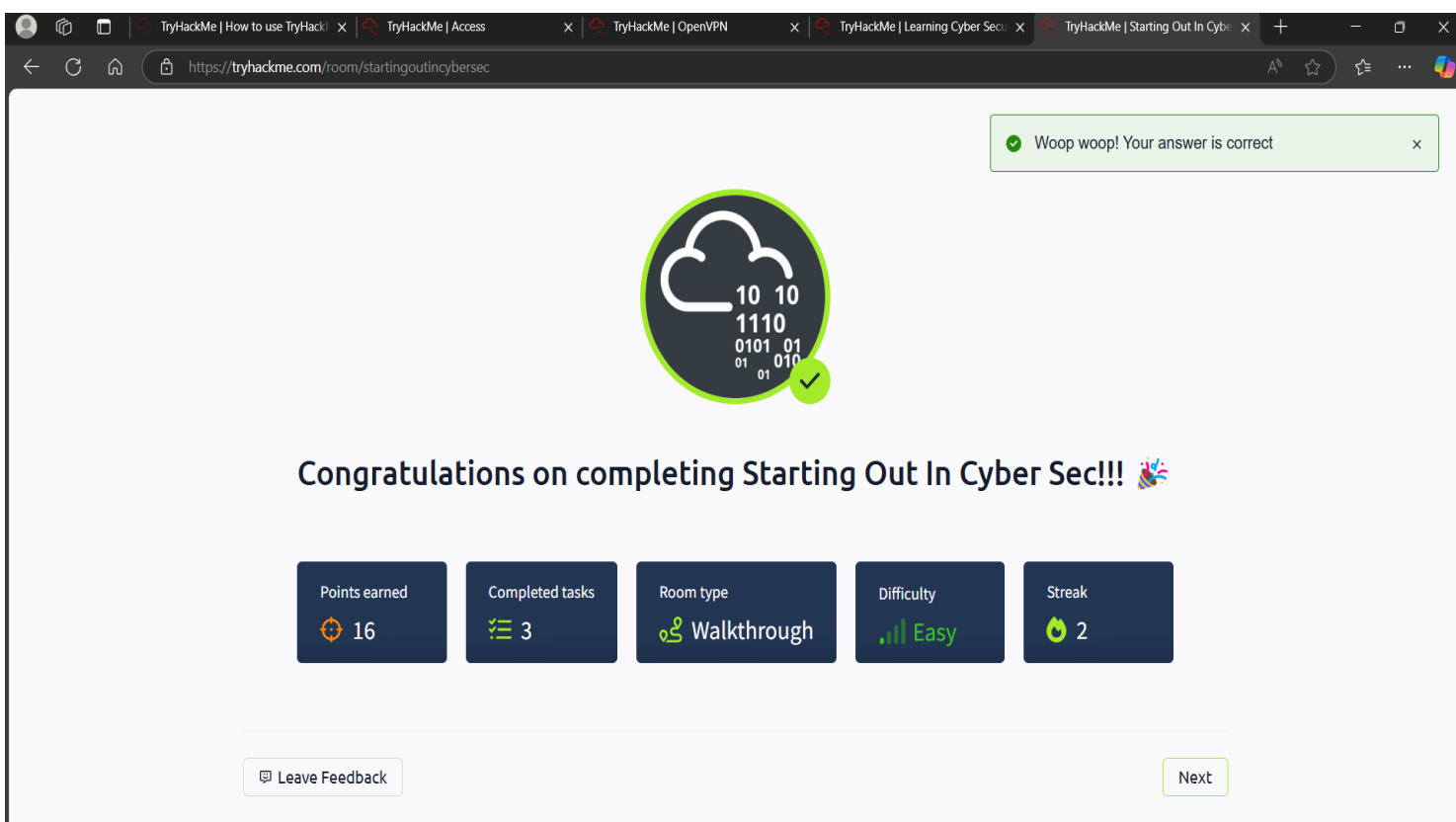
1. Cybersecurity Roles: Understanding the different roles within cybersecurity, such as security analyst, penetration tester, and security engineer. Identifying the responsibilities and tasks associated with each role.
2. Essential Skills: Recognizing the key skills required for a successful career in cybersecurity, including technical, analytical, and problem-solving abilities. Understanding the importance of continuous learning and skill development.
3. Learning Paths: Exploring the recommended learning paths for various cybersecurity roles on TryHackMe. Understanding how to structure learning to achieve specific career goals.
4. Career Planning: Developing a basic understanding of how to plan a career in cybersecurity. Identifying the steps needed to acquire the necessary skills and experience.

➤ Walkthrough / How You Solved It

1. Accessing the Room: Logged into TryHackMe and navigated to the "Starting Out in Cyber Security" room via the provided link (TryHackMe Starting Out in Cyber Security).
2. Exploring Roles: Reviewed the descriptions of different cybersecurity roles and their responsibilities.
 - o Identified roles that align with interests and skills.
3. Identifying Skills: Recognized the essential skills needed for each role, including technical knowledge, analytical abilities, and soft skills. Assessed personal skills and identified areas for improvement.
4. Exploring Learning Paths: Explored the recommended learning paths for different cybersecurity careers. Understood how to structure learning to acquire the necessary skills.
5. Task Completion: Answered questions related to cybersecurity roles, skills, and learning paths.

➤ Reflections or Notes

This room is invaluable for individuals starting their journey in cybersecurity, offering a clear overview of the field. It helps beginners understand the different roles available, the skills required, and how to structure their learning. Understanding this information is crucial for making informed decisions and planning a successful career in cybersecurity.



The screenshot shows the TryHackMe web interface in a browser. The address bar displays the URL <https://tryhackme.com/room/startingoutincybersec>. A green notification box at the top right says "Woop woop! Your answer is correct". In the center, there is a circular icon with a cloud and binary code (1010110101010101) and a green checkmark. Below this, the text "Congratulations on completing Starting Out In Cyber Sec!!!" is displayed with a party popper emoji. At the bottom, there are five dark blue boxes showing completion statistics: "Points earned 16", "Completed tasks 3", "Room type Walkthrough", "Difficulty Easy", and "Streak 2". At the very bottom, there are two buttons: "Leave Feedback" and "Next".

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

TryHackMe Room: [TryHackMe Introductory Researching](#)

➤ Learning Objective

The "Introduction to Research" room on TryHackMe aims to equip users with fundamental research skills essential for cybersecurity. It covers effective searching, understanding credible sources, and utilizing search engines and databases to gather relevant information for security-related tasks.

➤ Key Tools/Commands Used

- Search Engines (Google, DuckDuckGo): Used to find information on the internet.
- Online Databases (e.g., NIST, CVE): Explored to access vulnerability and security information.
- Documentation and Whitepapers: Utilized to gather in-depth technical details on specific topics.

➤ Concept Learned

1. Effective Searching: Understanding how to formulate effective search queries using relevant keywords and operators. Learning how to refine search results to find accurate and relevant information.
2. Credible Sources: Identifying and evaluating the credibility of online sources, including documentation, academic papers, and vendor websites. Understanding the importance of using reputable sources for reliable information.
3. Utilizing Databases: Exploring and using online databases such as NIST's National Vulnerability Database (NVD) and the Common Vulnerabilities and Exposures (CVE) database. Understanding how to search for specific vulnerabilities and security-related information.
4. Research Methodologies: Learning basic research methodologies for cybersecurity tasks, such as threat analysis, vulnerability assessment, and incident response.

➤ Walkthrough / How You Solved It

1. Accessing the Room: Logged into TryHackMe and navigated to the "Introduction to Research" room via the provided link (TryHackMe Introduction to Research).
2. Understanding Search Techniques: Learned how to use search engines effectively by formulating relevant queries. Practiced refining search results to find specific information.
3. Evaluating Sources: Identified and assessed the credibility of different online sources. Understood the importance of using reputable sources for accurate information.
4. Exploring Databases: Explored online databases such as NIST NVD and CVE to search for vulnerabilities. Learned how to use these databases to gather information for security-related tasks.
5. Task Completion: Answered questions related to research techniques, credible sources, and database utilization.

➤ Reflections or Notes

This room is crucial for developing essential research skills needed for any cybersecurity professional. It highlights the importance of effective searching, evaluating sources, and utilizing databases to gather reliable information. Mastering these skills is fundamental for staying informed about emerging threats, vulnerabilities, and security best practices.

✓ Woop woop! Your answer is correct



Congratulations on completing Introductory Researching!!! 🎉

Points earned	Completed tasks	Room type	Difficulty	Streak
🕒 104	📋 5	👤 Walkthrough	📶 Easy	🔥 2

🗉 Leave Feedback

Next