Prabhav Nerurkar_TryHackMeIntro_Report.pdf

Cybersecurity Internship Assignment Report
Intern Name: Prabhav Nerurkar
Issued By: Digisuraksha Parhari Foundation
Powered By: Infinisec Technologies Pvt. Ltd.

TryHackMe Room: Hello World

Learning Objective

The primary goal of the "Hello World" room on TryHackMe is to introduce users to the platform and familiarize them with its structure, navigation, and basic cybersecurity concepts. This room serves as a starting point for beginners to understand how to interact with the labs effectively.

Key Tools/Commands Used

- **Web Browser:** Used to access the TryHackMe platform.
- **TryHackMe Dashboard:** Explored the interface and features.
- **Basic Navigation Commands:** Learned how to move through rooms and access content.

Concepts Learned

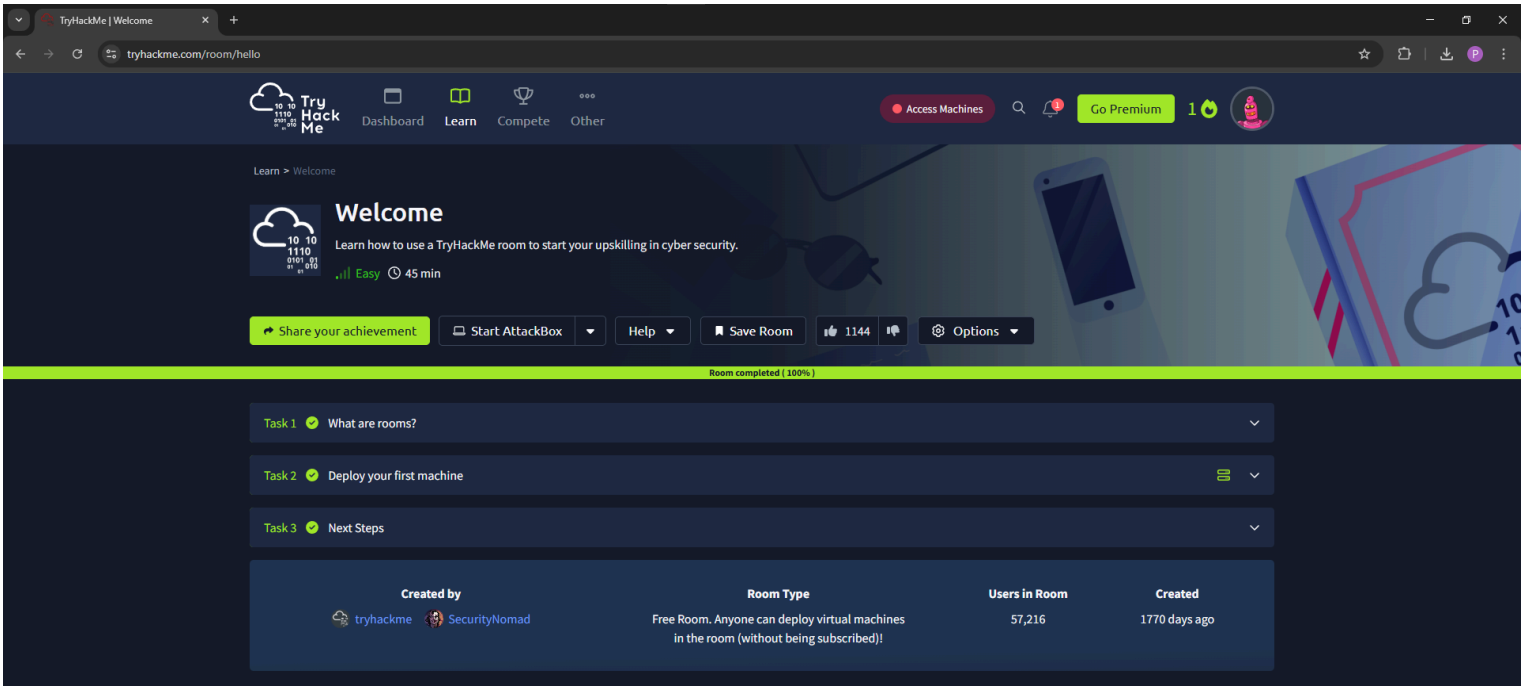
1. **Platform Overview:**
    - Understanding the purpose and structure of TryHackMe.
    - Introduction to its features such as learning paths, hands-on labs, and competitions like "King of the Hill."
2. **Room Navigation:**
    - How to join rooms, complete tasks, and track progress.
3. **Cybersecurity Basics:**
    - Introduction to ethical hacking concepts and system security principles.

- **Walkthrough / How You Solved It**

1. **Accessing the Room:**
    - Logged into TryHackMe using credentials.
    - Navigated to the "Hello World" room via the provided link https://tryhackme.com/room/hello
2. **Exploring Content:**
    - Followed the guided instructions within the room.
    - Completed introductory tasks designed to familiarize users with TryHackMe's interface.
3. **Hands-On Practice:**
    - Engaged in simple exercises demonstrating basic cybersecurity principles.
4. **Completion:**
    - Marked tasks as complete after successfully understanding the content.

- **Reflections or Notes**

- The "Hello World" room is an excellent starting point for beginners in cybersecurity. It simplifies complex concepts and provides a user-friendly interface for learning.
- It highlights the importance of hands-on practice in building foundational skills.
- The interactive environment fosters curiosity and encourages further exploration of cybersecurity topics.



TryHackMe Room: [How to Use TryHackMe]

Learning Objective

The "How to Use TryHackMe" room is designed to help users understand the platform's structure, features, and navigation. It provides a step-by-step guide to effectively use TryHackMe for learning cybersecurity, completing tasks, and engaging with interactive labs.

Key Tools/Commands Used

- **TryHackMe Dashboard:** Explored the main interface and its components.
- **Interactive Labs:** Learned how to access and interact with virtual machines (VMs) and tasks.
- **VPN Configuration:** Understood the basics of connecting to the platform securely using OpenVPN.

Concepts Learned

1. **Platform Features:**
    - Overview of TryHackMe's core functionalities, including learning paths, challenges, and leaderboards.
    - Introduction to gamified elements like earning points and maintaining streaks.

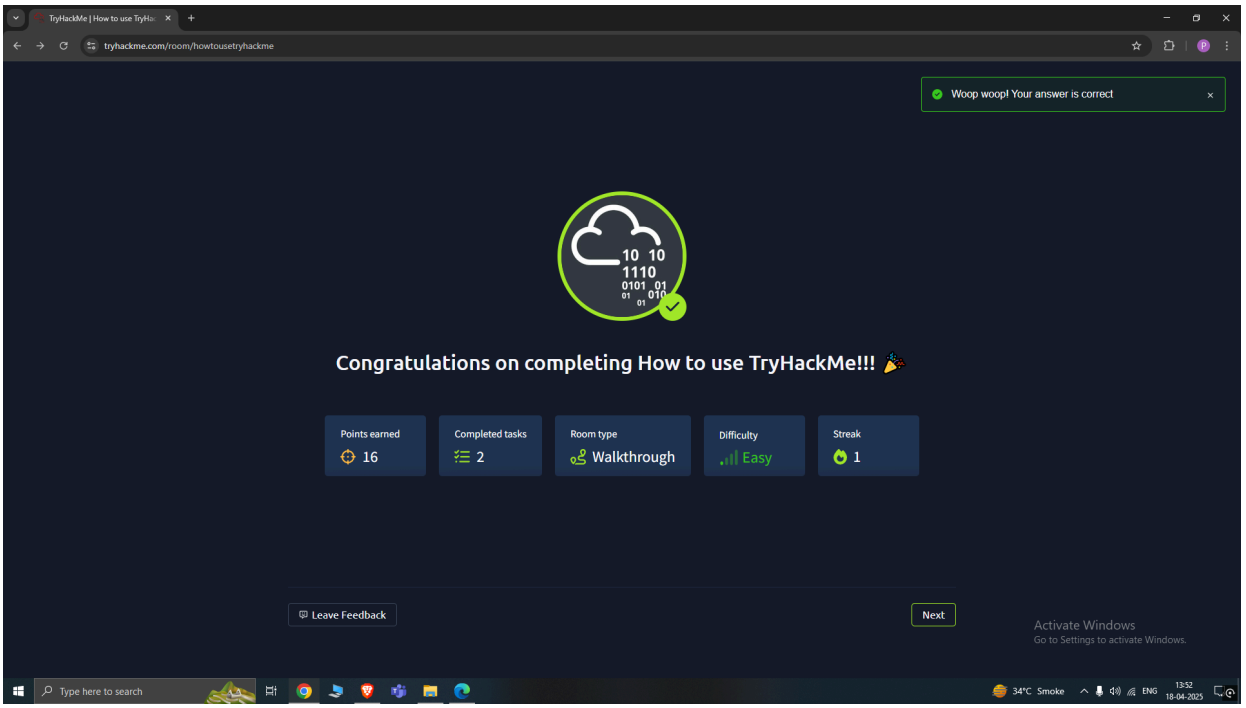
2. **Room Navigation:**
    - How to join rooms, complete tasks, and submit answers.
    - Understanding room types such as walkthroughs, challenges, and tutorials.
3. **Hands-On Practice:**
    - Accessing and using virtual environments for practical exercises.
4. **Security Basics:**
    - Setting up a secure connection using OpenVPN for accessing remote labs.

Walkthrough / How You Solved It

1. **Accessing the Room:**
    - Logged into TryHackMe and navigated to the "How to Use TryHackMe" room via the provided link (TryHackMe How to Use TryHackMe).
2. **Exploring the Dashboard:**
    - Familiarized with key sections like "Learn," "Practice," "Compete," and "Networks."
    - Reviewed available learning paths and room categories.
3. **Completing Tasks:**
    - Followed the guided instructions within the room to complete tasks.
    - Practiced deploying VMs and connecting via VPN for hands-on activities.
4. **Submission Process:**
    - Answered questions based on the tasks completed and marked them as done.

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 Room: Getting Started

Learning Objective

The "Getting Started" room on TryHackMe aims to introduce users to the platform's functionality and guide them through the initial steps required to begin their cybersecurity learning journey. It covers essential topics like accessing labs, navigating rooms, and understanding basic cybersecurity concepts.

Key Tools/Commands Used

- **TryHackMe Dashboard:** Explored the interface and interactive sections.
- **Virtual Machines (VMs):** Learned how to deploy and interact with VMs for practical exercises.
- **VPN Configuration:** Understood how to securely connect to TryHackMe labs using OpenVPN.

Concepts Learned

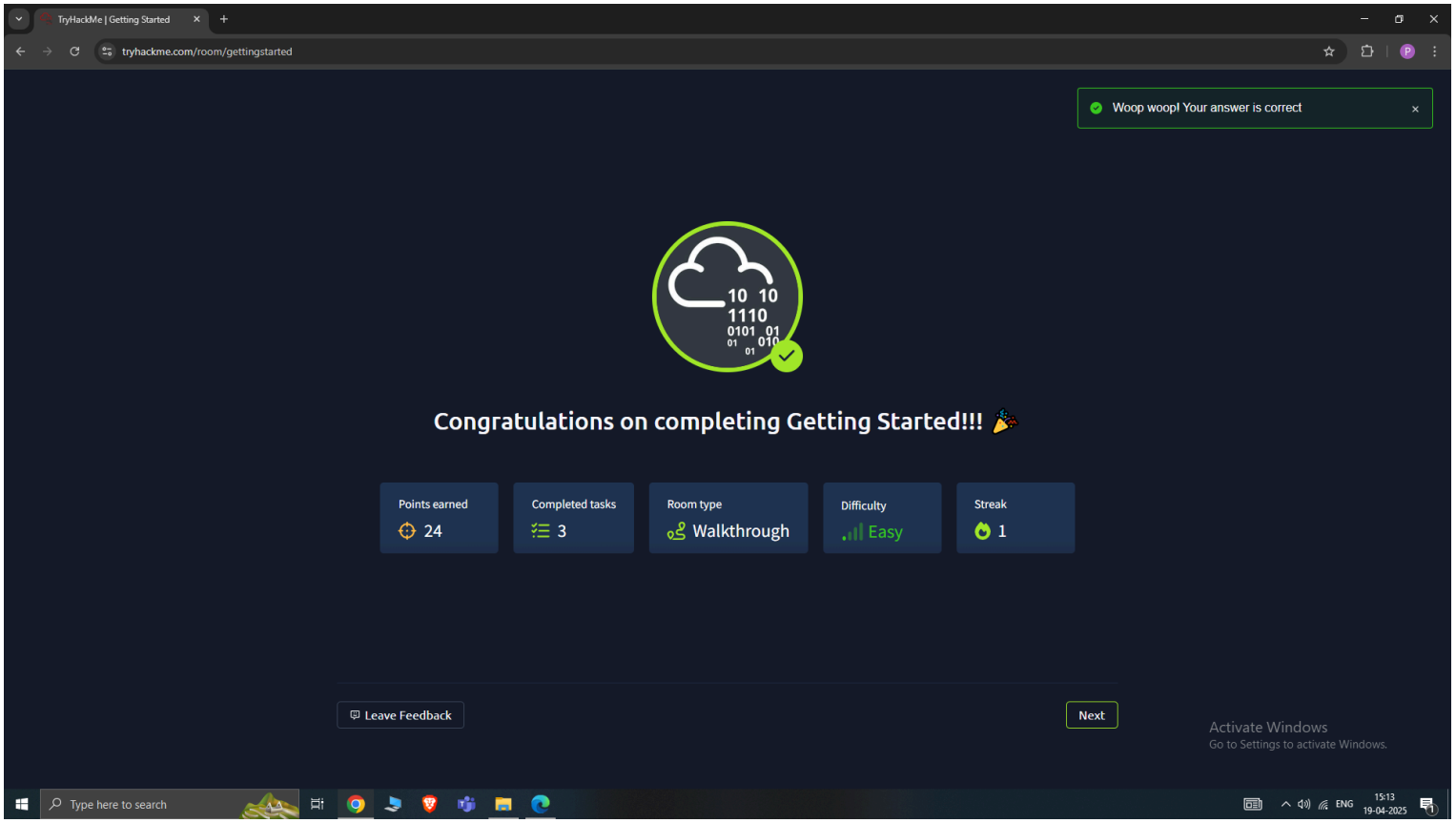
1. **Platform Navigation:**
    - How to find and join rooms, complete tasks, and track progress.
    - Overview of features like "Learn," "Practice," "Compete," and "Networks."
2. **Hands-On Labs:**
    - Deploying virtual machines for practical hacking exercises.
    - Understanding the importance 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.
    - 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**

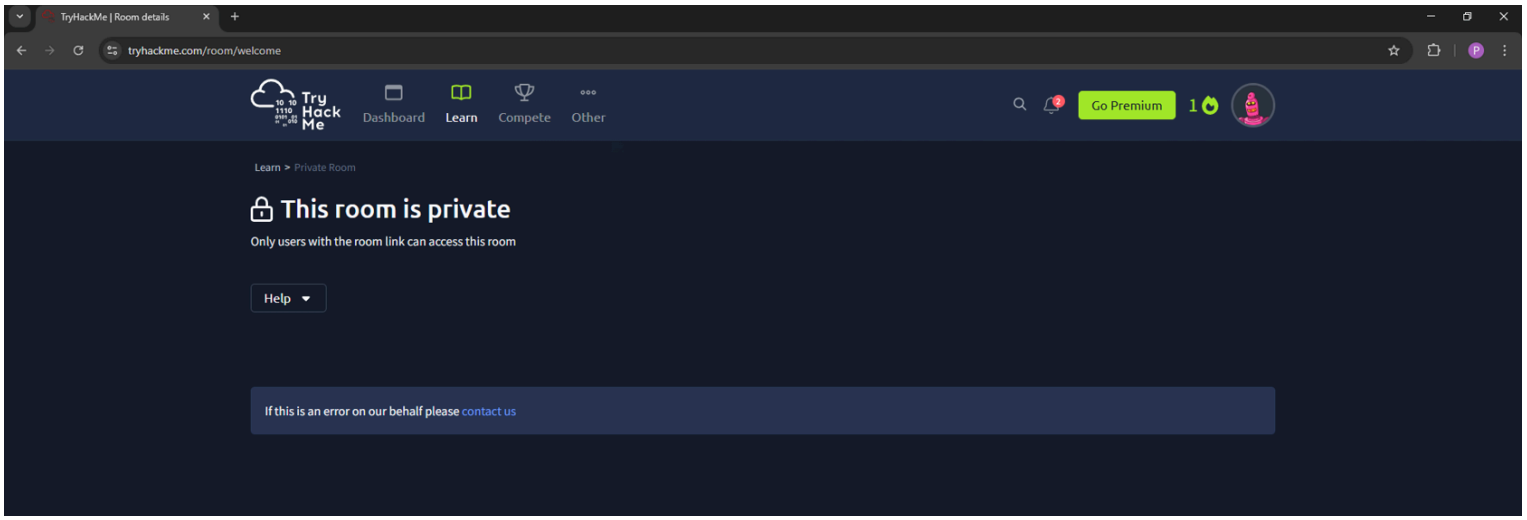
- The "Getting Started" room is a valuable resource for beginners, providing clear guidance on using TryHackMe effectively.
- It emphasizes hands-on practice, which is crucial for building foundational cybersecurity skills.
- The gamified approach makes learning engaging while fostering a competitive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



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 Interface:** Navigating through the dashboard and different sections.
- **Task Completion Interface:** Understanding how to answer questions and submit tasks.
- **Interactive Elements:** Utilizing hints, deployable machines, and attack boxes within the tasks.

Concepts Learned

1. **Room Structure:**
    - Understanding the layout of a typical TryHackMe room, including tasks, questions, and hints.
    - Identifying different types of tasks, such as multiple-choice, answer-based, and hands-on challenges.
2. **Task Interaction:**
    - Utilizing available resources like hints and explanations to solve tasks.
    - Learning how to properly submit answers and track progress.
3. **Hands-On Practice:**
    - Deploying and interacting with virtual machines within the room.
    - Using attack boxes to engage in practical cybersecurity exercises.
4. **Navigation Techniques:**
    - Efficiently navigating through rooms, tasks, and learning paths.

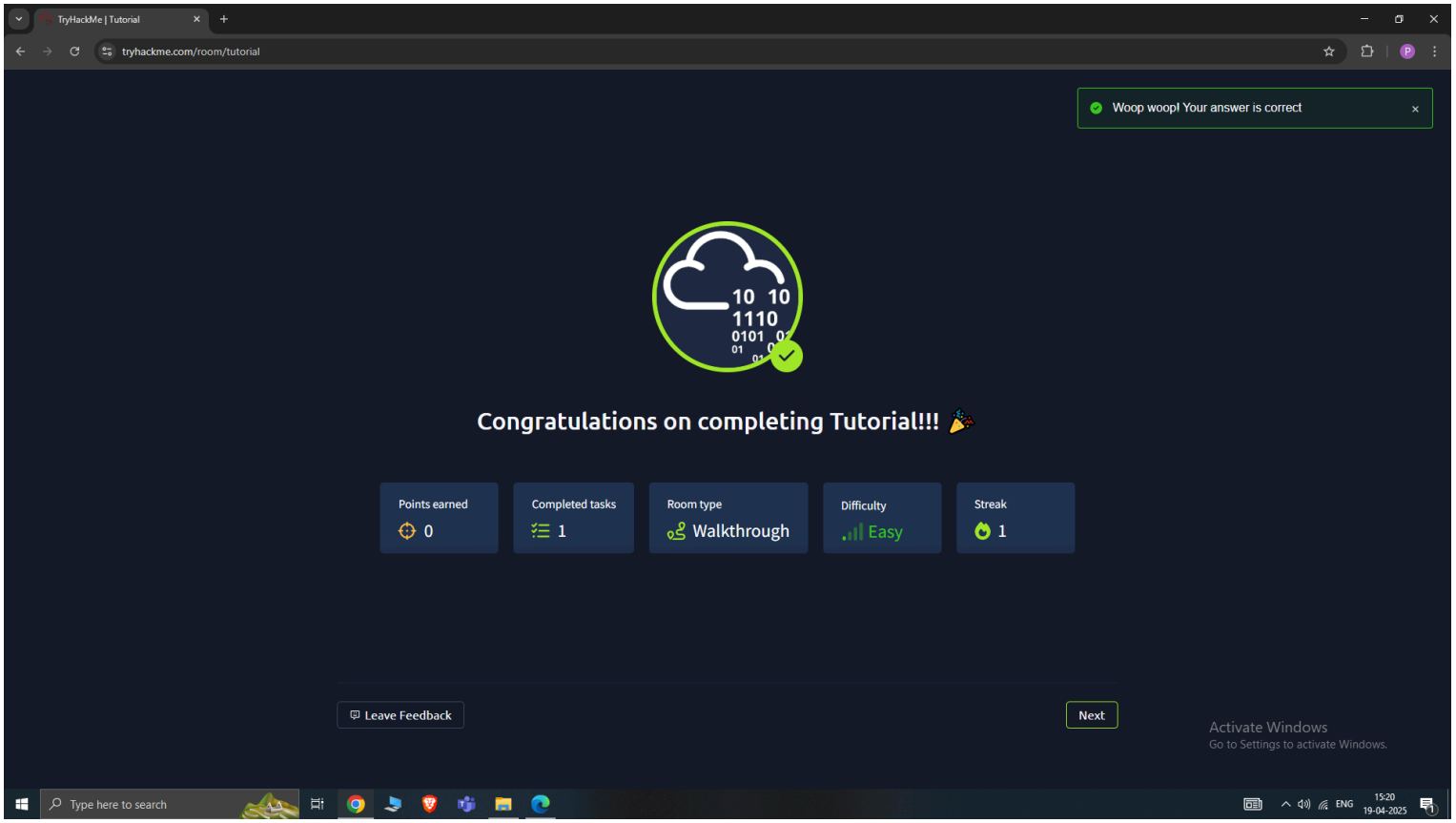
Walkthrough / How You Solved It

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

- Marked the room as complete after successfully finishing all tasks.

- **Reflections or Notes**

  - The "TryHackMe Tutorial" room is essential for new users, offering a structured introduction to the platform's core elements.
  - It emphasizes hands-on learning through interactive tasks and virtual machines, enhancing the learning experience.
  - Understanding the tutorial's content is crucial for effectively utilizing TryHackMe's resources and progressing through more advanced cybersecurity topics.



TryHackMe Room: [OpenVPN]

Learning Objective

The "OpenVPN" room on TryHackMe aims to guide users through the process of setting up and configuring an OpenVPN connection. It covers downloading the necessary configuration files, establishing a VPN connection, and verifying that the connection is working correctly to access TryHackMe's network.

Key Tools/Commands Used

- **OpenVPN Client:** Software used to establish a VPN connection.
- **Terminal/Command Line:** Used to execute OpenVPN commands.
- **ifconfig or ip addr:** Command-line tools to check the VPN interface and IP address.

Concepts Learned

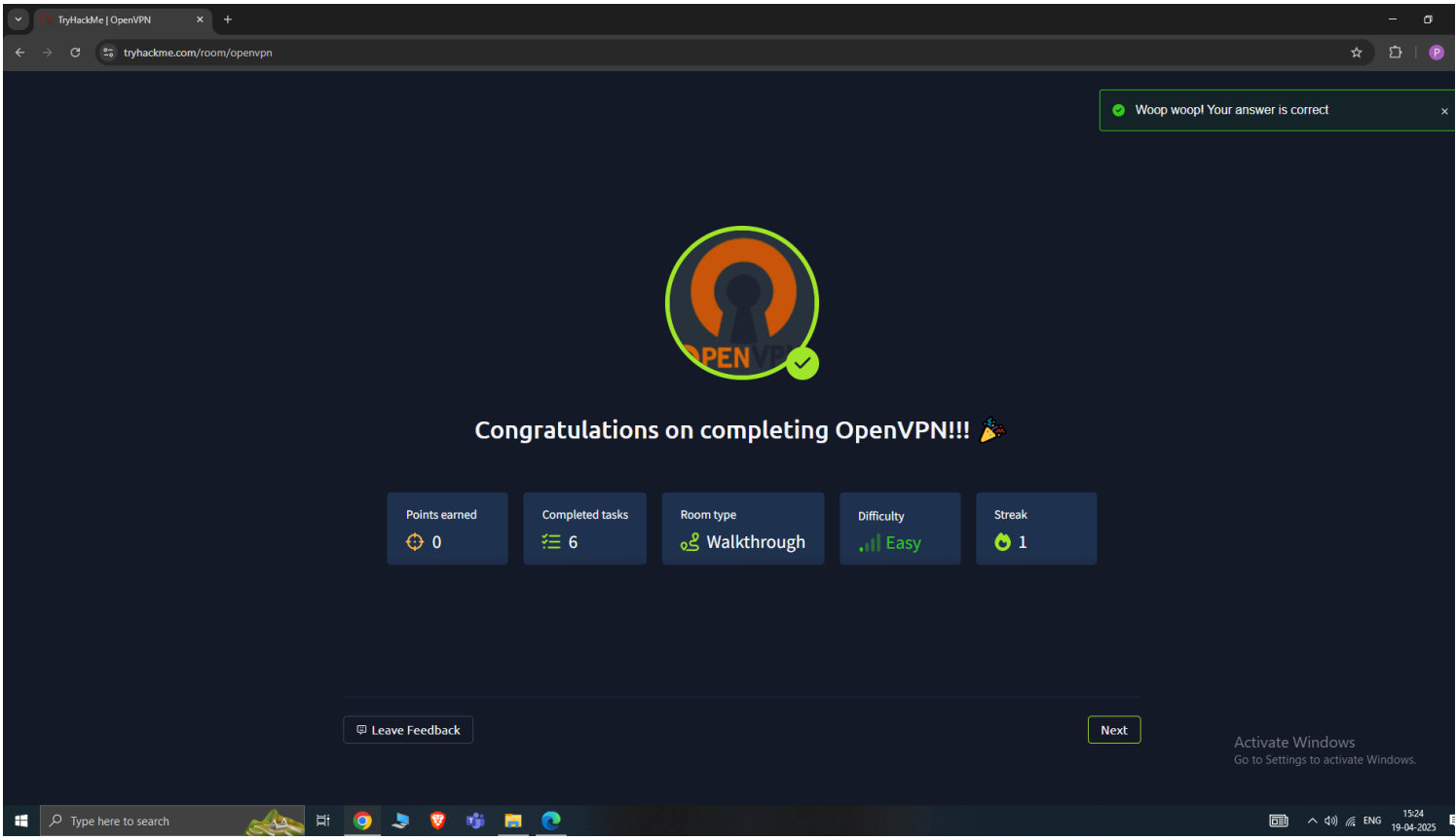
1. **VPN Basics:**
    - Understanding what a VPN is and its purpose in cybersecurity.
    - Learning how VPNs provide secure and encrypted connections.
2. **OpenVPN Configuration:**
    - Downloading and using OpenVPN configuration files.
    - Configuring the OpenVPN client to connect to TryHackMe's network.
3. **Connectivity Verification:**
    - Checking the assigned IP address and verifying the VPN connection.
    - Ensuring that the VPN is active and routing traffic correctly.
4. **Troubleshooting:**
    - Identifying and resolving common VPN connection issues.

- **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 <your_username>.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: [Beginner Path Introduction]

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.

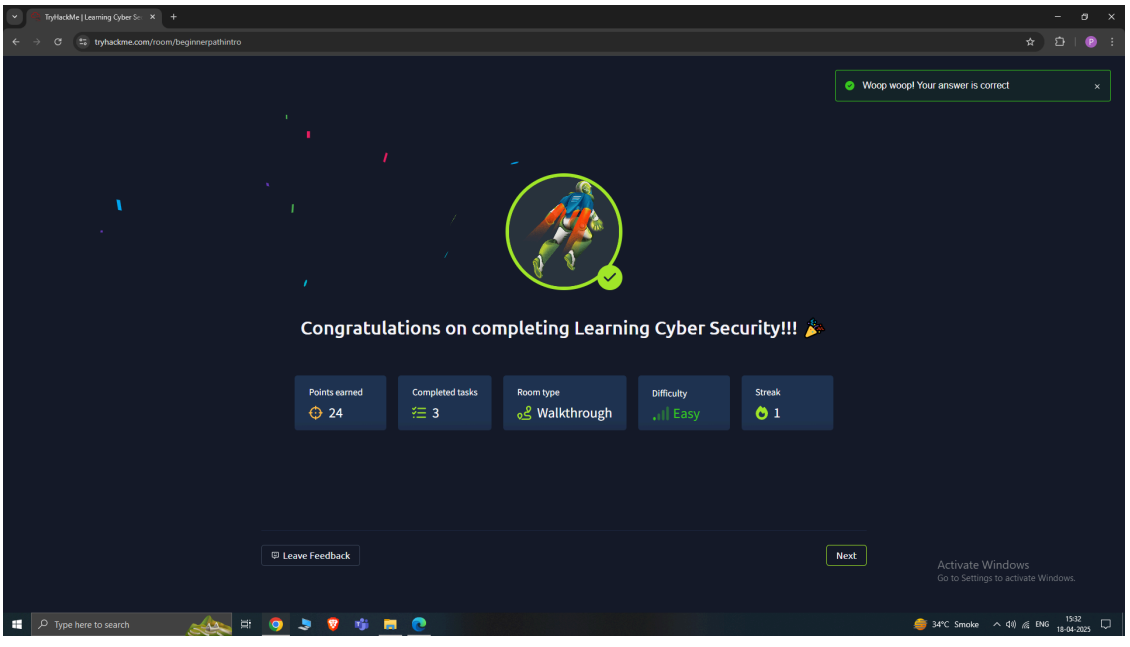
4. **Resource Utilization:**
    - Identifying key resources within the learning path, such as tutorials, walkthroughs, and supplementary materials.

- **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: Starting Out in Cyber Security

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 Learning Paths:** Exploring different learning paths relevant to various cybersecurity roles.
- **Cybersecurity Role Descriptions:** Reviewing the responsibilities and requirements of different roles.
- **Skill Assessments:** Identifying key skills needed for specific cybersecurity positions.

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**

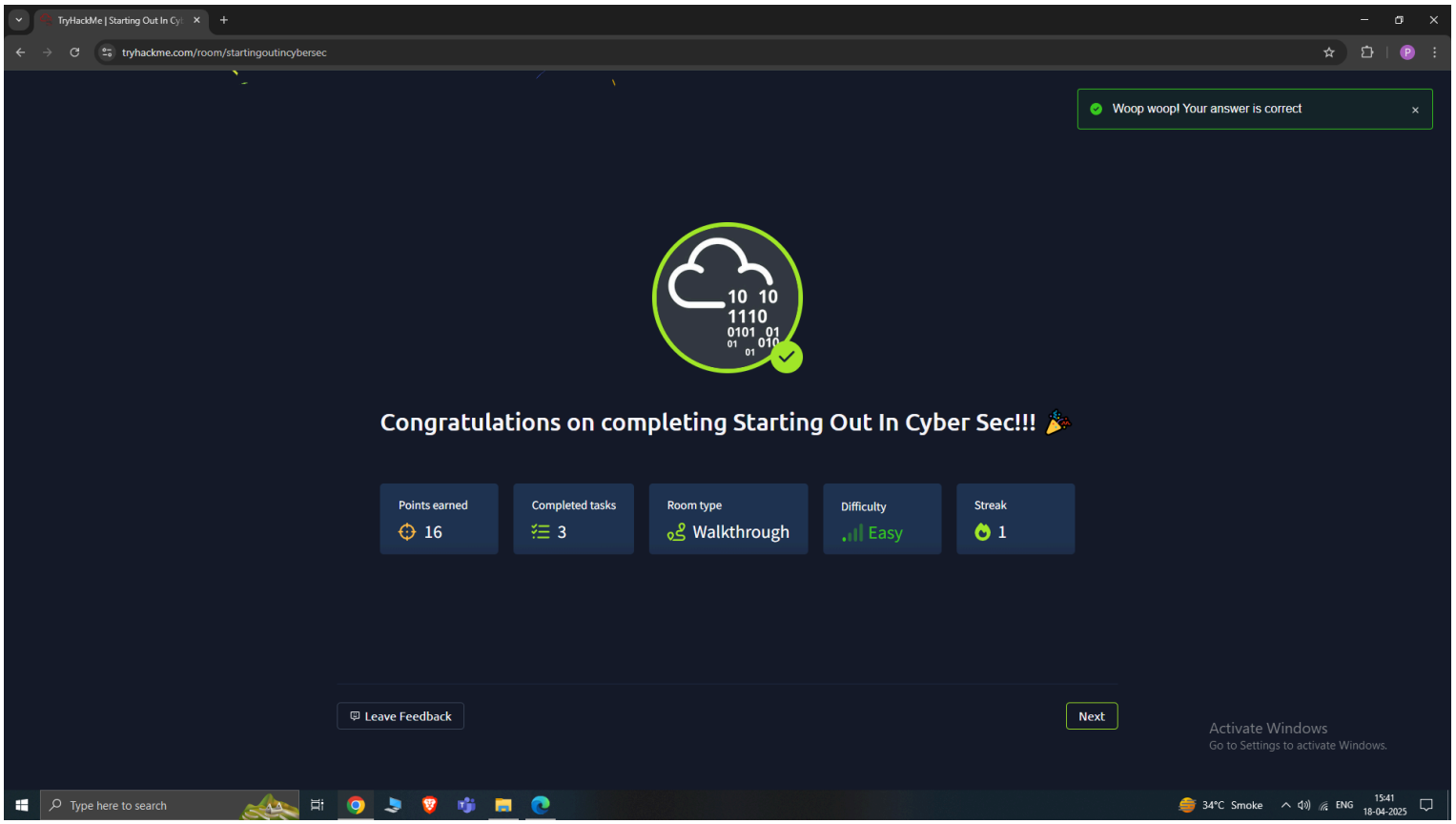
1. **Accessing the Room:**
    - Logged into TryHackMe and navigated to the "Starting Out in Cyber Security" room via the provided link (TryHackMe Starting Out in Cyber Security).
2. **Exploring Roles:**
    - Reviewed the descriptions of different cybersecurity roles and their responsibilities.
    - 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.



TryHackMe Room: Introduction to Research

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.

Concepts 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.