Cybersecurity Internship Assignment Report

Intern Name: Prajot Kurhade

Program: Digisuraksha Parhari Foundation Internship Issued By: Digisuraksha Parhari Foundation Supported By: Infinisec Technologies Pvt. Ltd.Report Submission Date: 18th April 2025

🟩 **Room Name: Hello World**

🟩 **Room Link: https://tryhackme.com/room/hello**

● **Learning Objective**

The objective of this room was to introduce the fundamentals of TryHackMe, including deploying a machine, accessing it via the browser-based AttackBox or OpenVPN, and retrieving a simple flag. This serves as a beginner-friendly introduction to the platform and basic cybersecurity tasks.

🛠 Key Tools/Commands Used

- **TryHackMe AttackBox: Browser-based Kali Linux environment for interacting with deployed machines.**

- **OpenVPN: Alternative method for connecting to**

TryHackMe's network.

- **Firefox (Browser): Used to navigate to the deployed**

machine's IP and retrieve the flag.

- **Basic Navigation Commands: Learned how to move through rooms and access content.**

C ̫* Concepts Learned

1. **Machine Deployment:**
   - How to deploy a virtual machine (VM) on TryHackMe and wait for initialization.
2. **Access Methods:**
   - AttackBox: Quick browser-based access for free users
   - OpenVPN: Manual connection for persistent access
3. **Flag Retrieval:**
   - Understanding that flags (e.g., THM{FLAG_EXAMPLE}) validate task completion.
4. **Cybersecurity Basics:**
   - Introduction to ethical hacking concepts and system security principles.

•˙Q Walkthrough / How You Solved It

1. **Accessing the Room:**

   ➢ Logged into TryHackMe using credentials.

➢ **Navigated to the "Hello World" room via the provided link (TryHackMe Hello World).**

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.**

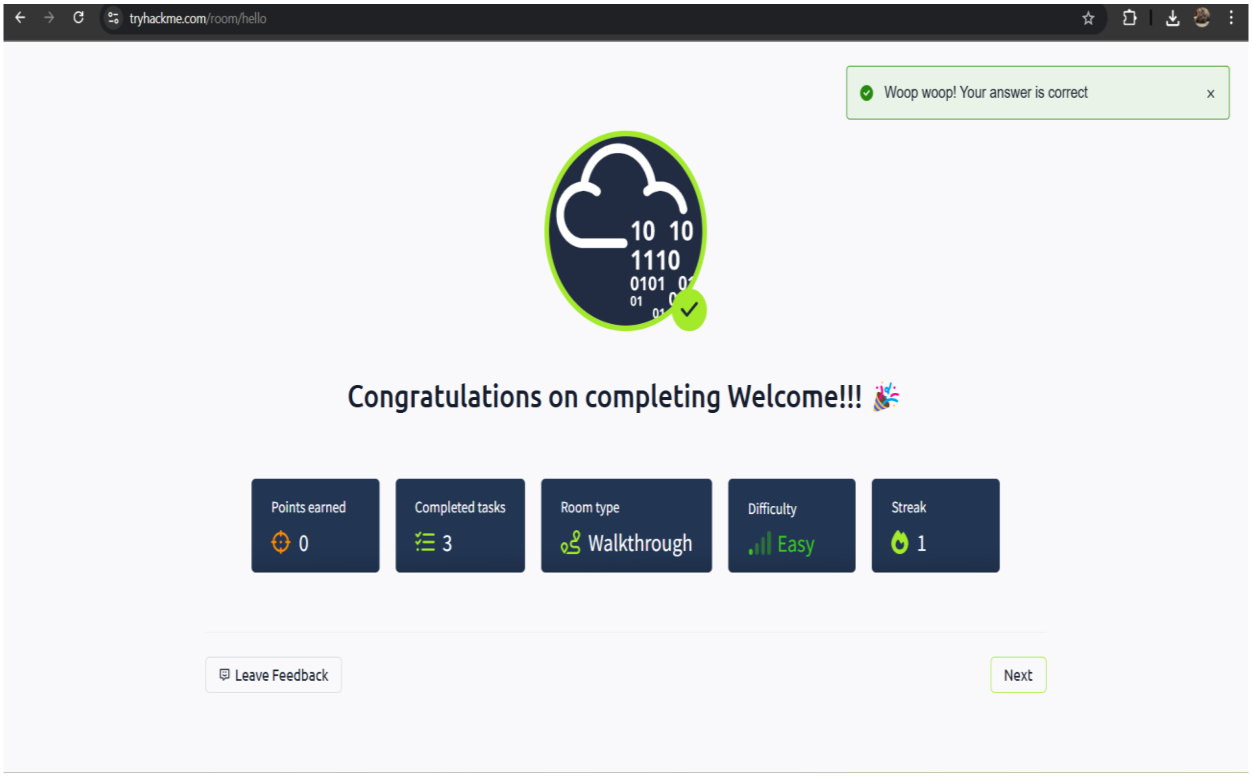
.•9„˙ Reflections or Notes

- **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.**



Woop woop! Your answer is correct

Congratulations on completing Welcome!!! 🎉

Points earned 0

Completed tasks 3

Room type Walkthrough

Difficulty Easy

Streak 1

🟩 **Room Name: How to Use TryHackMe**

🟩 **Room Link:**
https://tryhackme.com/room/howtousetryhackme

◎•´ ”' Learning Objective

The objective of this room was to provide hands-on experience with fundamental Linux commands while introducing the basics of interacting with TryHackMe machines. The tasks focused on file navigation and viewing file contents to build comfort with the command-line interface (CLI).

🛠 Key Tools/Commands Used

- **Linux CLI: Basic commands for file system interaction. ls: List directory contents**
  cd: Change directory cat: Display file contents

- **TryHackMe Machine Deployment:**

- **Starting/stopping machines via the web interface.**

C˛* Concepts Learned

1. **Linux Basics:**
   - **Navigating directories (cd), listing files (ls), and reading files (cat).**

2. **Machine Management:**
   - **Starting and terminating TryHackMe machines.**

3. **Task-Based Learning:**
   - **Answering questions by applying commands in a live environment.**

4. **Platform Workflow:**
   - **Understanding how rooms guide users through practical tasks.**

˙•Q Walkthrough / How You Solved It

Task 1: Listing Files (ls)

1. Started the Linux machine by clicking "Start Machine".
2. In the terminal, typed ls to list files/folders.
3. Submitted the folder name as the answer.

Task 2: Changing Directory (cd)

1. Used cd folder_name to enter the folder

Task 3: Viewing File Contents (cat)

1. Ran ls again inside the folder to see hello.txt.
2. Typed cat hello.txt to display its contents.

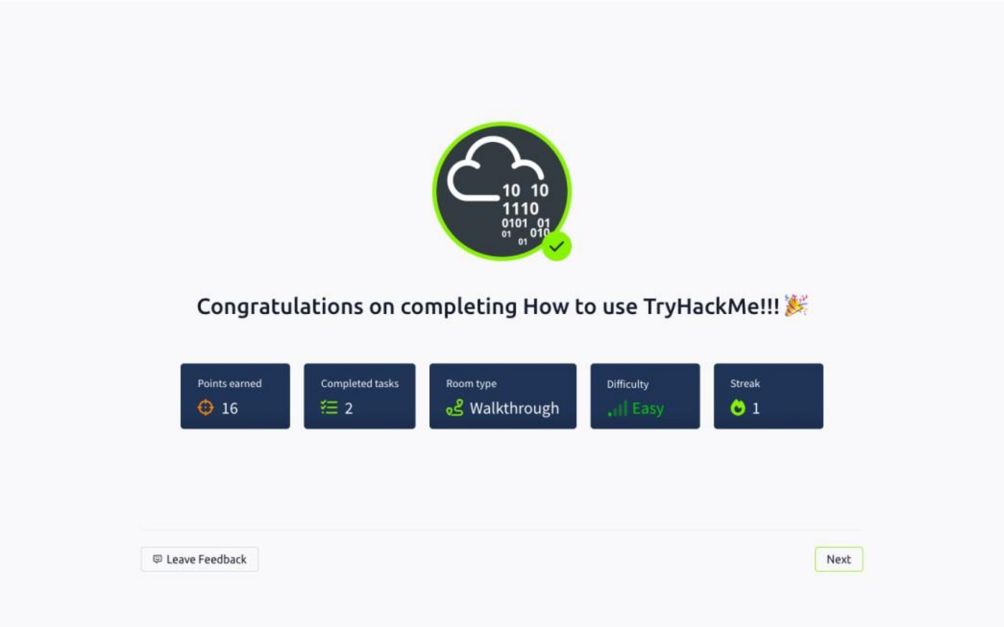
Task 4: Terminating the Machine

1. Clicked the red "Terminate" button to stop the machine.

˙•„9. Reflections or Notes

- Practical Introduction: The room effectively bridges theory (Linux commands) with practice (live machine interaction).

- User-Friendly Design: Step-by-step tasks build confidence for beginners.



Congratulations on completing How to use TryHackMe!!! 🎉

Points earned 16

Completed tasks 2

Room type Walkthrough

Difficulty Easy

Streak 1

🟩 Room Name: Getting Started

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

🎯 Learning Objective

The objective of this room was to introduce practical web application security testing by:

1. **Deploying and accessing a vulnerable VM.**
2. **Identifying hidden information in page source code.**
3. **Exploiting default credentials to gain unauthorized access.**
4. **Understanding the impact of poor security configurations.**

🛠 Key Tools/Commands Used

- **TryHackMe AttackBox: Browser-based Kali Linux environment.**

- **Firefox (Browser): Accessed the target website and inspected page source.**
- **Page Source Inspection: Used to find hidden comments/paths (Right-Click → View Page Source).**
- **Default Credentials Testing: Common username/password combinations (e.g., admin:admin).**

C˛* Concepts Learned

1. Reconnaissance:

- **How to inspect HTML source code for hidden comments/paths.**

2. Authentication Bypass:

- **Exploiting default credentials to access restricted admin panels.**

3. Impact of Misconfigurations:

- **Risks of leaving default credentials or debug comments in production.**

4. VM Workflow:

- **Launching TryHackMe machines and AttackBox for testing.**

•˙Q Walkthrough / How You Solved It

Task 1: Launching the Machine

1. **Clicked the "Start Machine" button to deploy the vulnerable VM.**
2. **Noted the machine's IP address from the "Active Machine Information" section.**

Task 2: Accessing the Website

1. **Launched the AttackBox (browser-based Kali VM).**
2. **Opened Firefox and navigated to the target IP (e.g., http://10.10.xx.xx).**

Task 3: Finding the Hidden Admin Page

1. **Inspected Page Source:**
   - **Right-clicked the webpage → "View Page Source".**

Task 4: Exploiting Default Credentials

1. **Tried common credentials:**
   - **admin:admin → Success!**

Task 5: Counting Users

1. **After logging in, observed a user count on the admin dashboard**

Task 6: Terminating the Machine

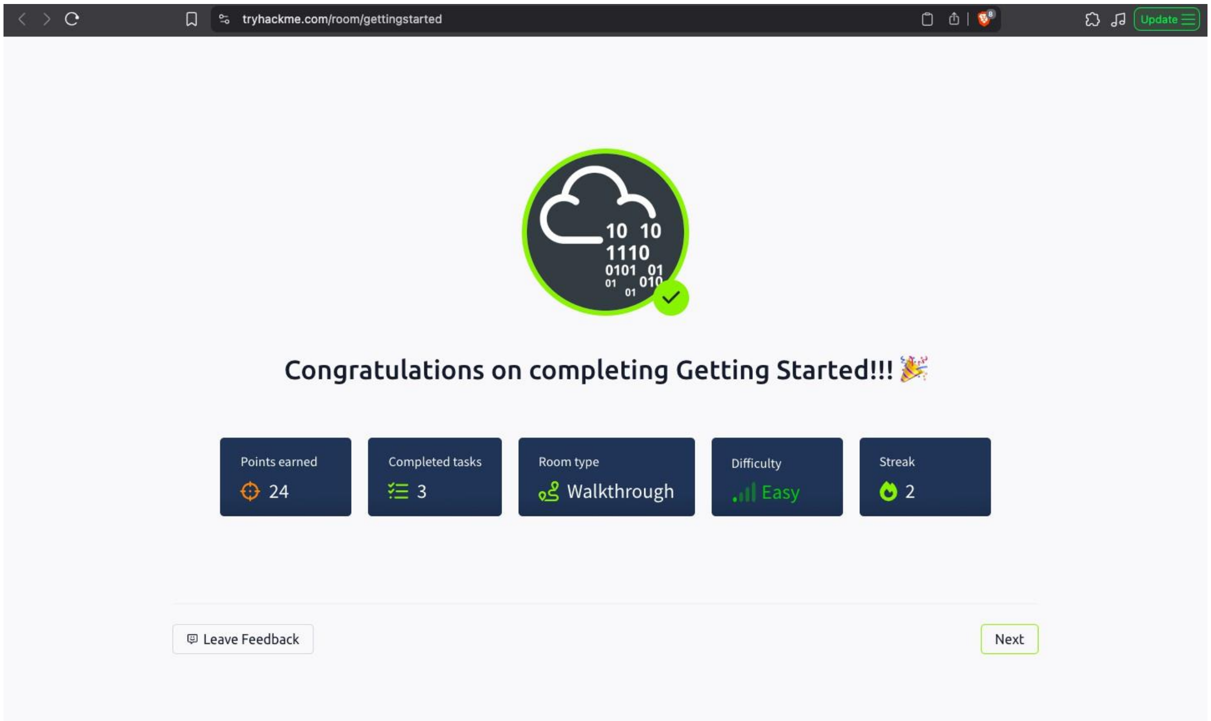
1. **Clicked "Terminate" to stop the VM.**

•.˙9„ Reflections or Notes

- **Practical Focus: The room effectively demonstrates real-world flaws (e.g., exposed admin pages, default creds).**

- **Beginner-Friendly: Step-by-step tasks build confidence in basic web app testing.**

- **Ethical Reminder: Highlighted the importance of fixing such issues in real applications.**



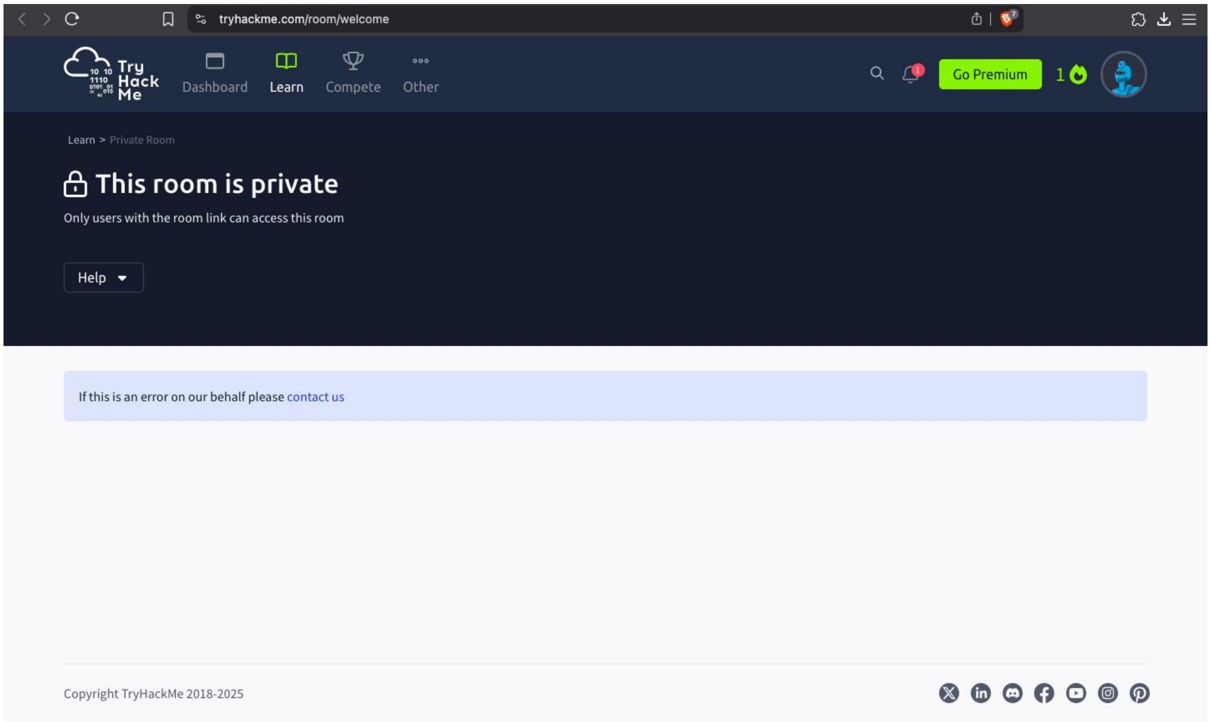
tryhackme.com/room/gettingstarted

Congratulations on completing Getting Started!!! 🎉

Points earned	Completed tasks	Room type	Difficulty	Streak
24	3	Walkthrough	Easy	2

🟩 Room Name: Welcome

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



This room is private

Only users with the room link can access this room

If this is an error on our behalf please contact us

Copyright TryHackMe 2018-2025

🟩 Room Name: TryHackMe Tutorial

🟩 Room Link: https://tryhackme.com/room/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 AttackBox: Web-based Kali Linux environment**
- **Firefox Browser: Accessed the target machine's web interface**
- **Machine Management: Starting/terminating VMs via TryHackMe interface**
- **Basic Web Navigation: IP address entry in browser**

˛C* Concepts Learned

1. **Platform Fundamental:**
   - **Difference between AttackBox (attacker) and target machines**
   - **Purpose of flags in CTF challenges**

2. **Workflow Process:**
   - **Machine deployment → Access → Flag retrieval → Termination**

3. **Access Methods:**
   - **Browser-based AttackBox vs. OpenVPN options**

•˙Q Walkthrough / How You Solved It

1. **Started Resources:**
   - **Launched AttackBox (blue button)**
   - **Deployed target machine (green button)**

2. **Accessed Target:**
   - **Copied target machine's IP from Active Machine Info**
   - **In AttackBox's Firefox, navigated to http://[target_IP]**

3. Retrieved Flag:

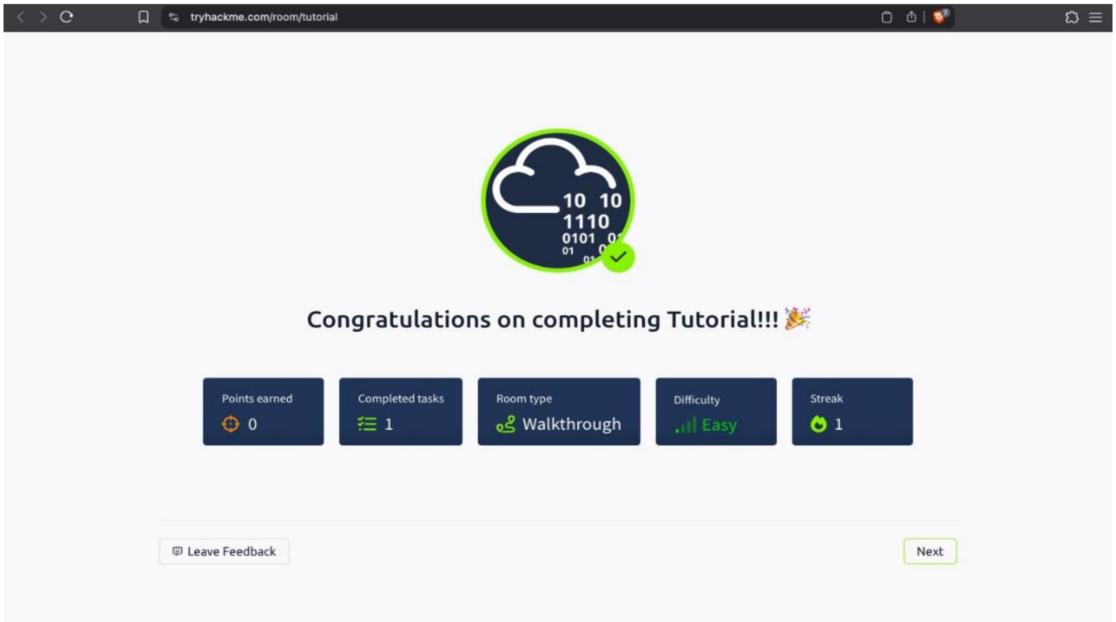
- **Found flag displayed on webpage: flag{connection_verified}**

4. Cleaned Up:

- **Terminated both AttackBox and target machine**

.•9„˙ Reflections or Notes

- **Effective Onboarding: Perfect introduction to TryHackMe's core workflow**
- **Clear Instructions: Well-structured for absolute beginners**
- **Understanding the tutorial's content is crucial for effectively utilizing TryHackMe's resources and progressing through more advanced cybersecurity topics.**



Congratulations on completing Tutorial!!! 🎉

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

🟩 Room Name: OpenVPN Configuration

🟩 Room Link: https://tryhackme.com/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 GUI: Client application for VPN connectivity**
- **Terminal (Linux): sudo openvpn /path/to/config.ovpn**
- **AttackBox: Browser-based alternative to VPN**
- **Network Verification: Checking connection status via Access Page**

*˛C Concepts Learned

1. **VPN Fundamentals:**
    - **Purpose of VPNs in ethical hacking**
    - **Differences between THM's OpenVPN and corporate VPNs**
2. **Platform Access Methods:**
    - **Native OpenVPN connection (Windows/Mac/Linux)**
    - **Browser-based AttackBox alternative**
3. **Connection Verification:**
    - **Checking network status**
    - **Testing connectivity via machine deployment**

˙•Q Walkthrough / How You Solved It Task 1-3: OpenVPN Setup

1. Downloaded Configuration:
   - Retrieved .ovpn file from TryHackMe Access page

2. Installed OpenVPN:
   - Windows: Installed GUI client via executable
   - Linux: sudo apt install openvpn

3. Connected to VPN:
   - Imported config file in GUI client
   - Established connection (verified by green tick on Access page)

Task 4: Connection Verification

1. Deployed Test Machine:
   - Started machine via green button
   - Accessed http://[MACHINE_IP] in browser

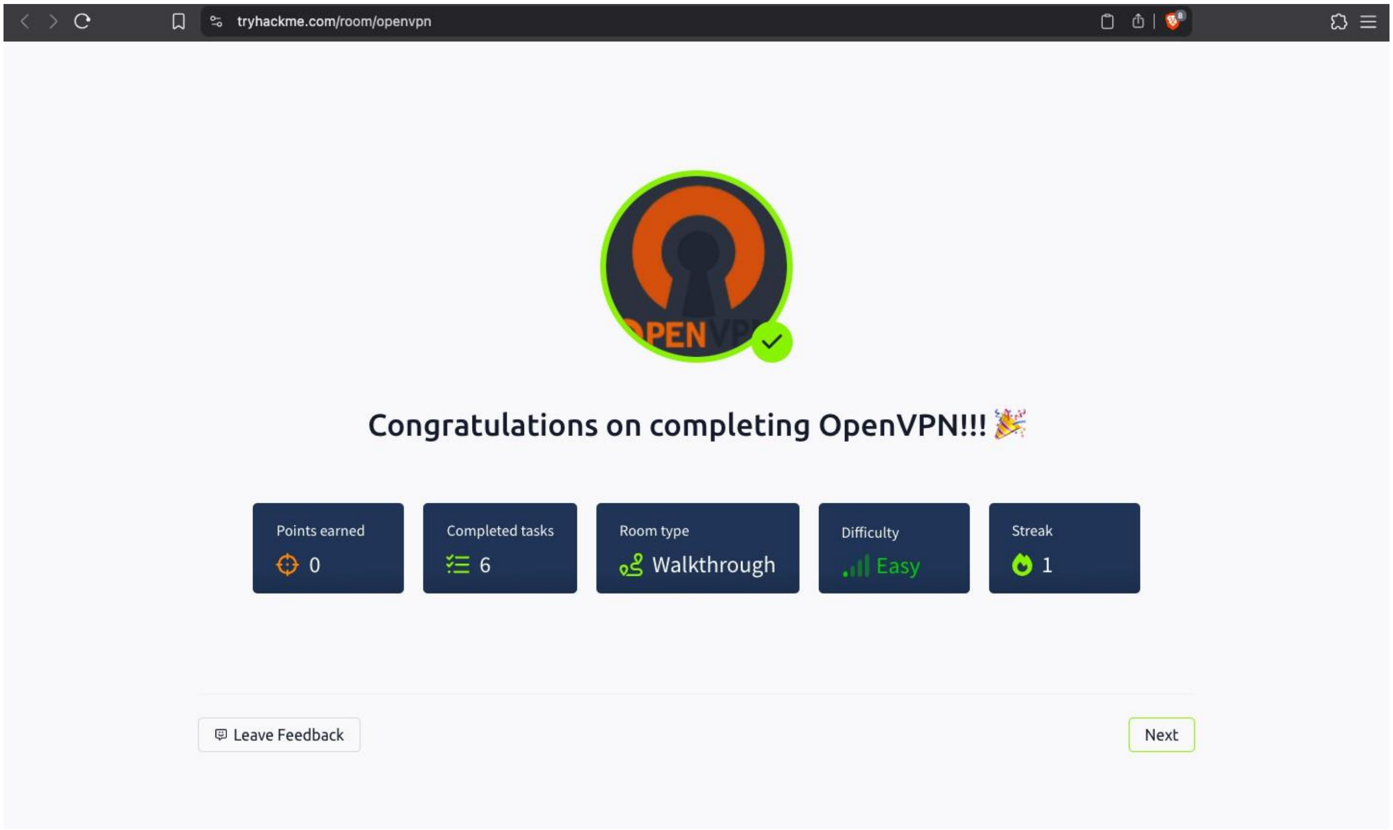
2. Retrieved Flag:
   - Found displayed flag: flag{connection_verified}

.•9„˙ Reflections or Notes

- Cross-Platform Learning: Covered Windows, Mac, and Linux methods

- Practical Orientation: Hands-on VPN setup is crucial for real- world engagements

- **Troubleshooting: Learned to verify connections and use fallback options**



Congratulations on completing OpenVPN!!! 🎉

■ Room Name: Beginner Path Introduction

■ Room Link: https://tryhackme.com/room/beginnerpathintro

?● Learning Objective

- **Introduce fundamental web application security concepts**

- **Demonstrate real-world impacts of vulnerabilities through interactive scenarios**

- **Highlight the importance of networking knowledge in cybersecurity**

- **Provide hands-on experience with basic exploitation techniques**

🛠 Key Tools/Commands Used

- **Interactive Web Interface: Accessed vulnerable "BookFace" and Target breach simulation**

- **Basic Web Inspection: Browser developer tools**

- **Critical Thinking: Analyzing scenarios to identify security weaknesses**

C˛* Concepts Learned

1. **Web Application Security:**

   - **Understanding how vulnerabilities emerge in web apps**
   - **Real-world consequences of security flaws**

2. Social Media Exploitation:

- **Account takeover techniques**

3. Networking Importance:
    - How network knowledge aids in attack detection/prevention

4. Business Impact:
    - Financial costs of data breaches

•˙Q Walkthrough / How You Solved It Task 1: BookFace Account Takeover

1. Clicked "View Site" to access the vulnerable BookFace interface
2. Identified the target account username through interface exploration:

Task 2: Target Data Breach Analysis

1. Accessed the Target breach simulation via "View Site"
2. Reviewed breach details to find financial impact:

Task 3: Networking Fundamentals

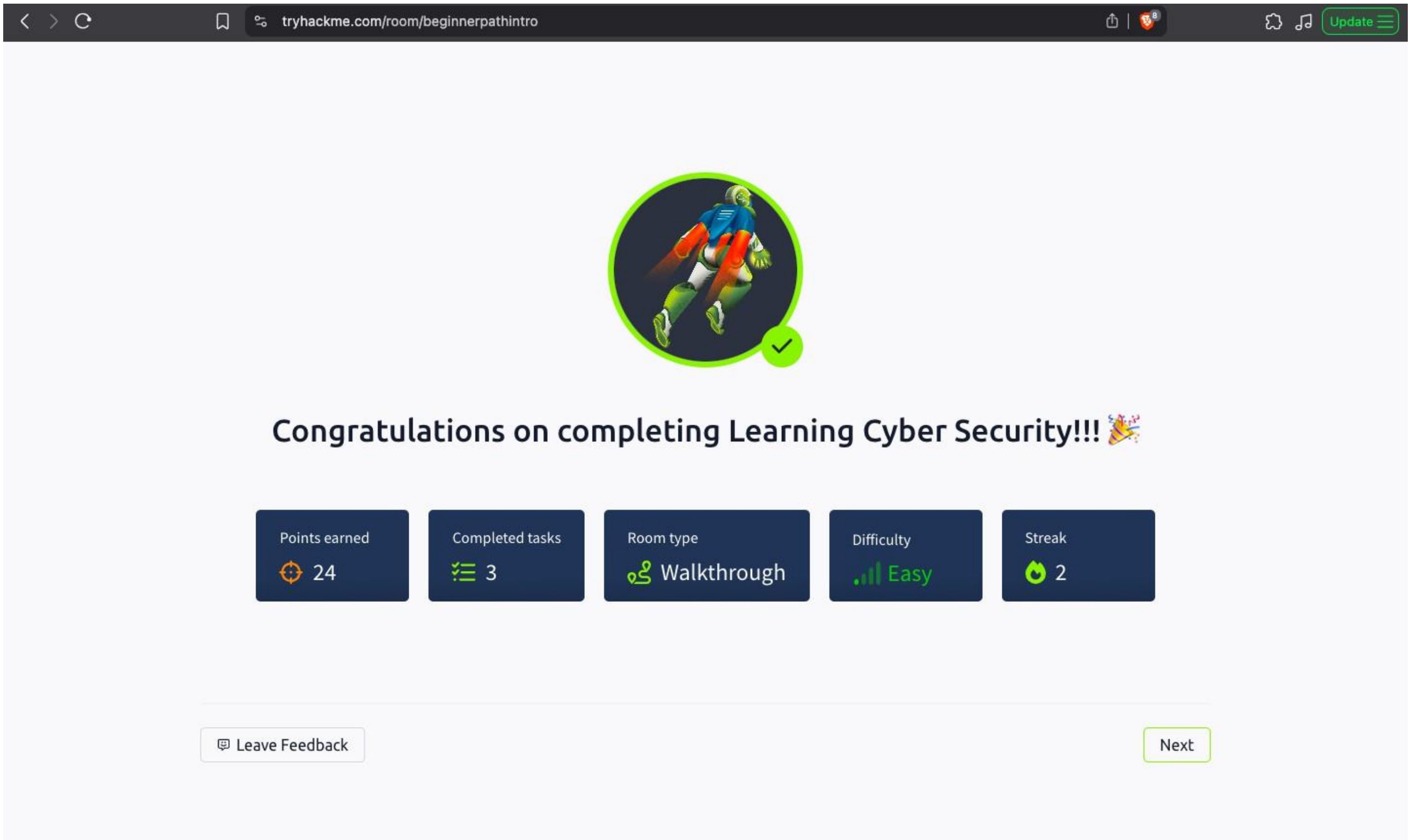
1. Explored introductory networking concepts through room content
2. Recognized the importance of network knowledge for:
    - Log analysis
    - Intrusion detection
    - Vulnerability scanning

˙„•9. Reflections or Notes

- Effective Introduction: Well-structured for absolute beginners

- **Real-World Relevance: BookFace and Target scenarios demonstrate tangible impacts**

- **Knowledge Gaps Identified:**
    - **Need to deepen web app security understanding**
    - **Requires more networking fundamentals**



Congratulations on completing Learning Cyber Security!!! 🎉

Points earned	Completed tasks	Room type	Difficulty	Streak
24	3	Walkthrough	Easy	2

■ **Room Name: Starting Out in Cyber Security**

■ **Room Link: https://tryhackme.com/room/startingoutincybersec**

⍰●´ ’" Learning Objective

- **Provide a comprehensive overview of cybersecurity career paths**
- **Differentiate between offensive and defensive security roles**
- **Highlight essential skills and knowledge areas for each specialization**
- **Guide beginners toward appropriate learning resources on TryHackMe**

🛠 Key Tools/Commands Used

- **Career Path Exploration:**
  - ○ **Offensive Security (Penetration Testing, Cloud Security)**
  - ○ **Defensive Security (Security Analysis, Incident Response, Malware Analysis)**
- **Platform Resources:**
  - ○ **Beginner Learning Path**
  - ○ **SOC Level 1 Path**
  - ○ **Specialized Rooms (Splunk, Volatility, Malware Analysis)**

***C˛ Concepts Learned**

1. **Offensive Security:**

- **Role of penetration testers in vulnerability discovery**
- **Required knowledge areas: web/network security, scripting, cloud security**

2. **Defensive Security:**
   - **Security Analyst responsibilities in attack detection**
   - **Incident Responder workflows for post-attack analysis**
   - **Malware analysis techniques**

3. **Career Alignment:**
   - **Matching personal strengths (analytical thinking, problem- solving) to roles**

4. **Learning Pathways:**
   - **Structured vs. self-directed learning options on TryHackMe**

•˙Q Walkthrough / How You Solved It Task 1: Offensive Security Overview

1. **Studied the offensive security career track description**

Task 2: Defensive Security Exploration

1. **Reviewed defensive security roles:**
   - **Security Analyst**
   - **Incident Responder**
   - **Malware Analyst**

2. **Explored linked rooms:**
   - **Splunk for attack detection**

- **Volatility for memory analysis**

- **Malware analysis fundamentals**

Task 3: Learning Path Identification

1. Noted recommended pathways:

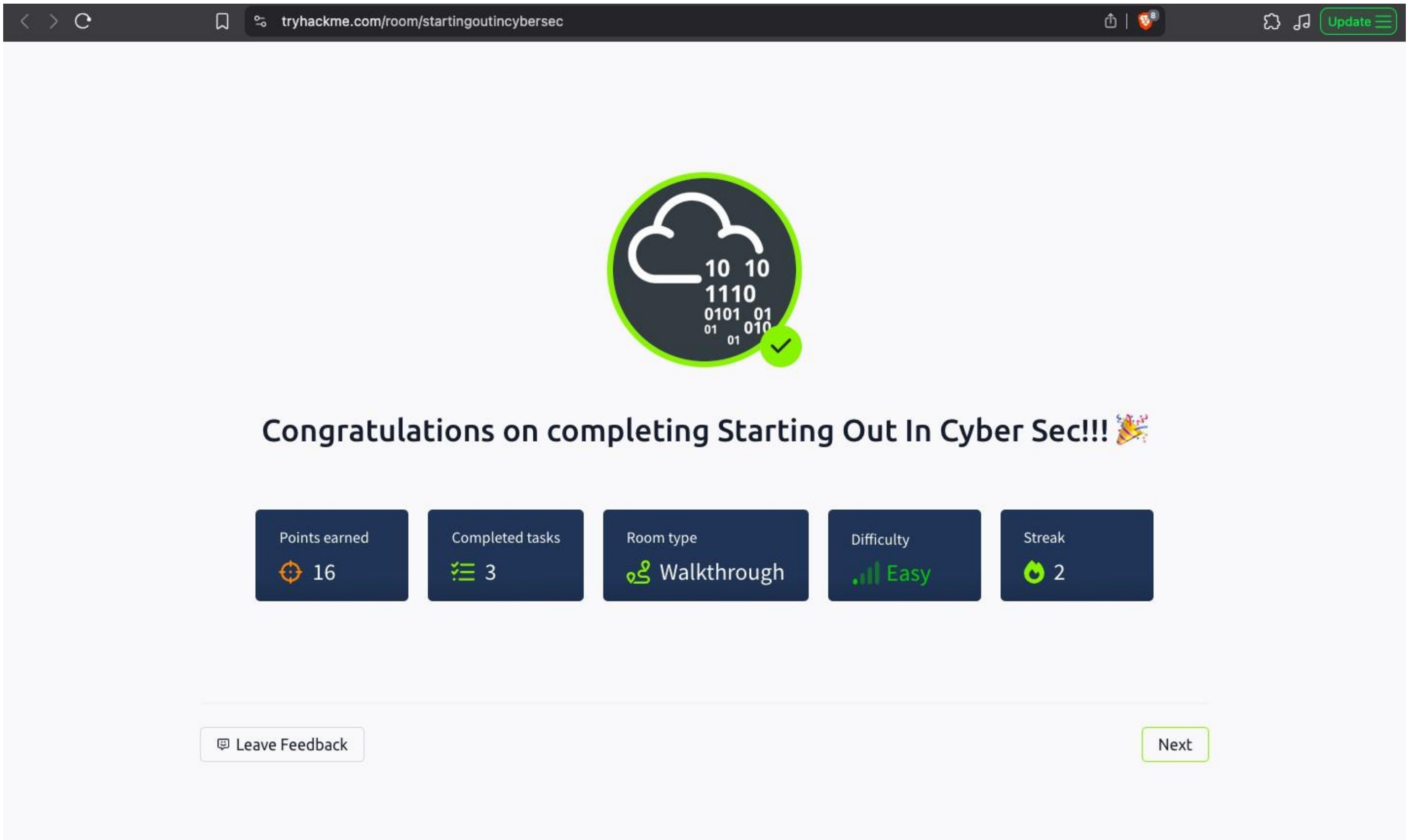
- **Beginner Path for broad offensive skills**
- **SOC Level 1 Path for blue team fundamentals**

„˙9•. Reflections or Notes

- **Career Clarity: Effectively distinguishes between red/blue team roles**

- **Practical Guidance: Directs users to relevant learning resources**

- **Self-Assessment Value: Helps identify suitable career paths based on skills/interests**



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

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

■ **Room Name: Introduction to Research**

■ **Room Link: https://tryhackme.com/room/introtoresearch**

´ Learning Objective

- **Develop essential research skills for cybersecurity professionals**
- **Learn effective vulnerability discovery techniques**
- **Master Linux manual (man) pages usage**
- **Understand how to leverage exploit databases (ExploitDB, CVE)**

🛠 Key Tools/Commands Used

- **Search Engines: Google-fu for cybersecurity queries**
- **Vulnerability Databases:**
    - **ExploitDB**
    - **NVD (National Vulnerability Database)**
    - **CVE Mitre**
- **Linux Tools:**
    - **searchsploit (Offline ExploitDB)**
    - **man command (Manual pages)**
    - **steghide (Steganography tool)**

C˛* Concepts Learned

1. Research Methodology:
   - Progressive query refinement (broad → specific)
   - Example: "hiding data in images" → steganography → steghide → installation/usage

2. Vulnerability Research:
   - CVE identification and interpretation (CVE-YEAR-ID)
   - Using searchsploit for exploit discovery

3. Linux Fundamentals:
   - Manual page navigation (man)
   - Common tool switches (SCP, fdisk, nano)

•Q˙ Walkthrough / How You Solved It Task 1: Research Techniques

1. Steganography Example:

Searched "hiding things inside images" → Learned about

steganography

Found steghide via research and installed via apt Task 2: Vulnerability Databases

1. ExploitDB/NVD Usage:
   - Searched FuelCMS → Found RCE exploit (CVE-2018-16763)

2. CVE Identification:

- **WPForms XSS: CVE-2020-10385**
- **Apache Tomcat LPE: CVE-2016-1240**
- **VLC’s first CVE: CVE-2007-0017**
- **Sudo buffer overflow: CVE-2019-18634**

Task 3: Linux Manual Pages

1. man Command Practice:

- **SCP directory copy: -r**
- **fdisk partition list: -l**
- **nano backup: -B**
- **Netcat listen mode: nc -lvnp 12345**

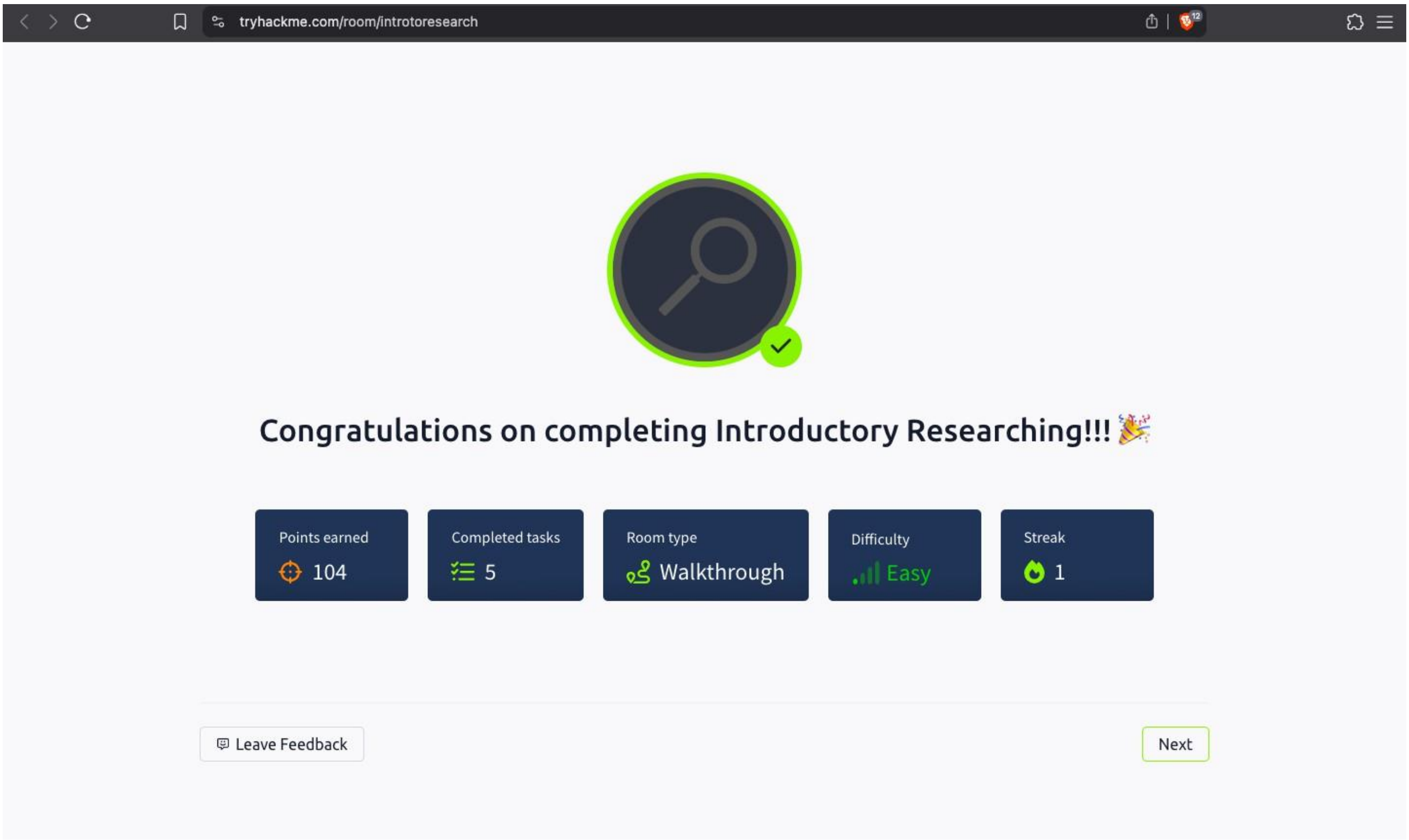
•.˙9„ Reflections or Notes

- **Critical Skill: Research is foundational for both offensive/defensive roles**

- **Tool Familiarity: searchsploit and man save significant time in real-world engagements**

- **Practical Application:**
    - **CVE research directly applicable to CTFs/pentests**

- **Manual pages eliminate memorization burden**



Congratulations on completing Introductory Researching!!! 🎉

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