Cybersecurity Internship Assignment Report

Name: Pratham Sangam

Program: Digisuraksha Parhari Foundation Internship

Issued By: Digisuraksha Parhari Foundation

Supported By: Infinisec Technologies Pvt. Ltd.

Report Submission Date: 18th April 2025

✅ Room Name and Link

Room Name: Hello World
Link: https://tryhackme.com/room/hello

🎯 Learning Objective

The main goal of this room was to get familiar with the TryHackMe platform. It explained how rooms work, how to deploy a virtual machine, and how to answer questions. It was like an orientation for new users.

🛠️ Key Tools/Commands Used

- No tools or external commands were needed for this room.
- Everything was done using the TryHackMe interface and the in-browser machine.

🧠 Concepts Learned

- How to navigate a TryHackMe room
- The basic structure of tasks and questions
- Deploying and connecting to a virtual machine
- Submitting answers directly in the room

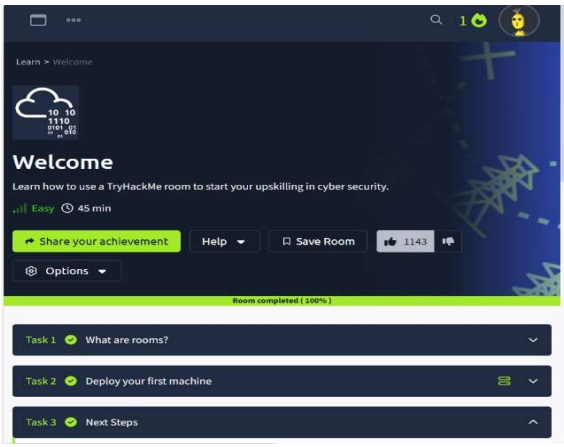
🔍 Walkthrough / How I Solved It

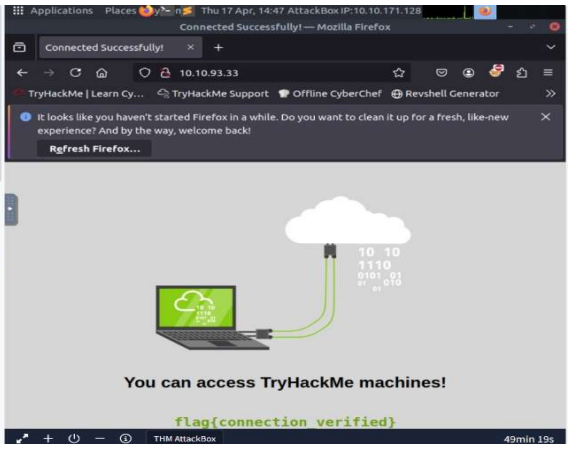
I started the room and read through the welcome message. Then, I clicked on the **"Start Machine"** button to deploy the virtual machine. After that, I went task by task, reading the content carefully and following the instructions. Since this was a beginner room, it

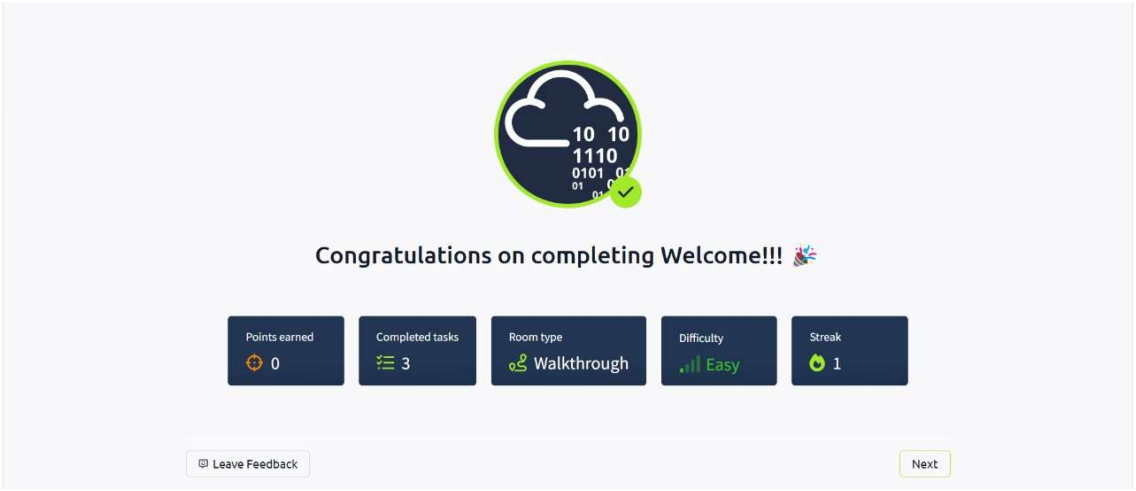
was mostly about understanding how things work rather than solving any technical challenges. I answered the questions as I went through each section.

💡 Reflections or Notes

This was my first room on TryHackMe, and I found it really helpful. The instructions were easy to follow, and it gave me a good overview of how the platform functions. I didn't need any tools or deep knowledge to complete it, which made it perfect as a starting point. I'm excited to move on to the next rooms and start learning more about cybersecurity!







✅ Room Name and Link

Room Name: How to Use TryHackMe
Link: https://tryhackme.com/room/howtousetryhackme

🎯 Learning Objective

This room was designed to help us get hands-on practice with basic Linux commands while also learning how to use TryHackMe machines. It mainly focused on navigating files and folders using the command-line interface (CLI), which is super important for cybersecurity and ethical hacking tasks.

🛠️ Key Tools/Commands Used

- **Linux CLI** for basic file system navigation:
    - ls – to list directory contents
    - cd – to move between directories
    - cat – to read the contents of a file
- **TryHackMe Machine Deployment**:
    - Starting and stopping machines through the browser interface

🧠 Concepts Learned

1. **Linux Basics** – I got more comfortable using commands like ls, cd, and cat to explore the file system.
2. **Using Virtual Machines** – Learned how to start and stop the machines TryHackMe provides.
3. **Task-Oriented Learning** – Each task gave me a small goal to complete, which made it easy to follow.
4. **Understanding the Platform Flow** – I now understand how each room teaches step-by-step through interaction and problem-solving.

🔍 Walkthrough / How I Solved It

Task 1: Listing Files

- I started the virtual machine, then typed ls in the terminal. It showed a list of files/folders, and I used that to answer the first question.

Task 2: Changing Directory

- I used cd foldername to move into the directory shown from the previous step.

Task 3: Viewing File Contents

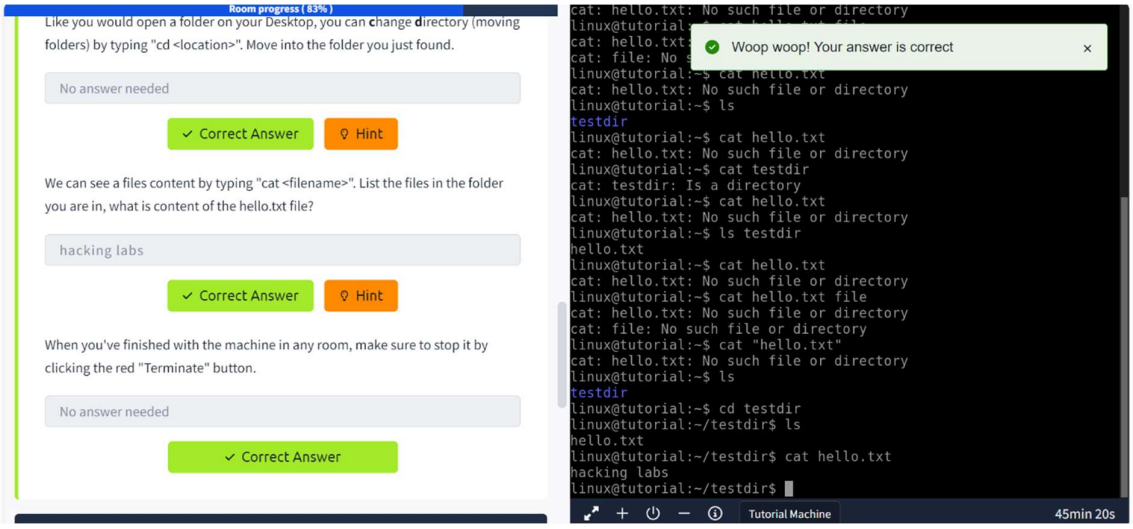
- Inside the folder, I ran ls again, saw a file named hello.txt, and used cat hello.txt to view what was inside.

Task 4: Stopping the Machine

- Once I was done, I simply clicked on the red **Terminate** button to shut down the machine.

💡 Reflections or Notes

This room was really helpful for someone like me who's new to Linux. It broke everything down nicely and made the learning process smooth. I liked how interactive it was — instead of just reading about commands, I got to use them directly on a live machine. That made it a lot easier to understand and remember.



✅ Room Name and Link

Room Name: Getting Started
Link: https://tryhackme.com/room/gettingstarted

🎯 Learning Objective

This room introduced me to the basics of web application security by allowing me to interact with a vulnerable virtual machine (VM). The main focus was on practical skills like finding hidden information in the page source, testing for default credentials, and understanding how small misconfigurations can lead to big security issues. It was a hands-on way to see how attackers can take advantage of weak setups.

🛠️ Key Tools/Commands Used

- **TryHackMe AttackBox** – Used for launching a virtual hacking environment
- **Firefox (within AttackBox)** – To access the target website

- **Page Source Inspection** – (Right-click → View Page Source) to look for hidden paths or comments
- **Default Credential Testing** – Tried basic login combos like admin:admin

🧠 **Concepts Learned**

1. **Reconnaissance** – Learned to check a webpage's HTML source to find clues like hidden URLs or comments.
2. **Authentication Bypass** – Realized how dangerous it is when websites use default login credentials.
3. **Security Misconfigurations** – Saw firsthand how exposed admin pages and unsecure setups can be easily exploited.
4. **Using the Platform** – Got more comfortable launching machines and using the AttackBox effectively.

🔍 **Walkthrough / How I Solved It**

Task 1: Launching the Machine

- Started the vulnerable machine and noted the IP address.

Task 2: Accessing the Website

- Opened Firefox inside the AttackBox and went to the target IP (e.g., http://10.10.xx.xx).

Task 3: Finding the Hidden Admin Page

- Right-clicked the webpage and selected **"View Page Source"**.
- Found a hidden path that pointed to an admin login page.

Task 4: Exploiting Default Credentials

- At the login page, I tried admin:admin and it worked! I was logged into the admin panel.

Task 5: Counting Users

- After logging in, I saw a dashboard with user statistics. Counted the number of users as asked.

Task 6: Terminating the Machine

- Once everything was completed, I clicked the **Terminate** button to shut down the machine

💡 **Reflections or Notes**

This room was super interesting because it showed how real-world websites can sometimes have simple but dangerous flaws. It also made me realize how important it is to never leave default settings in a live environment. I really liked how everything was step-by-step — easy to follow and beginner-friendly. Definitely a confidence booster for getting started with web app security!

✅ Room Name and Link

Room Name: Welcome Room

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

✅ Room Name and Link

Room Name: TryHackMe Tutorial
Link: https://tryhackme.com/room/tutorial

🎯 Learning Objective

This room was mainly focused on helping me understand how to use the TryHackMe platform effectively. It introduced the core features like the AttackBox, machine deployment, how flags work in challenges, and how to access target machines. It basically walked me through the workflow I'll be following in most rooms on TryHackMe.

🛠️ Key Tools/Commands Used

- **TryHackMe AttackBox** – Web-based Kali Linux machine
- **Firefox (inside AttackBox)** – To open the target machine's website
- **Machine Deployment Tools** – Start/stop buttons provided by the platform
- **Web Navigation** – Entering IP in browser to access a running VM

🧠 Concepts Learned

1. **Platform Basics** –
    - Learned the difference between the **AttackBox** (which we control) and the **target machine** (which we are attacking).
    - Understood what "flags" are and how they're used in CTF-style challenges.

2. **TryHackMe Workflow** –
    - The standard process: Start AttackBox → Start Target → Find Flag → Submit → Terminate
3. **Access Methods** –
    - Learned I can use either the in-browser AttackBox or connect using OpenVPN if I want to use my own machine.

🔍 Walkthrough / How I Solved It

Step 1: Starting Resources

- I clicked the **blue button** to launch the AttackBox, then hit the **green button** to start the target machine.

Step 2: Accessing the Target

- Once the target machine was up, I copied its IP address from the info panel.
- Opened Firefox in the AttackBox and visited http://[target_IP].

Step 3: Retrieving the Flag

- The flag was clearly shown on the webpage. I copied flag{connection_verified} and submitted it in the answer box.

Step 4: Clean-Up

- After everything was done, I terminated both the AttackBox and the target machine.

💡 Reflections or Notes

This tutorial room was a great introduction to how everything works on TryHackMe. It didn't require any technical skills but taught me the workflow that I'll need for all the future rooms. The step-by-step guidance was super helpful, especially for someone just getting started with cybersecurity. I now feel more confident about using the platform and solving challenges on my own.

✅ Room Name and Link

Room Name: OpenVPN Configuration
Link: https://tryhackme.com/room/openvpn

🎯 Learning Objective

The main goal of this room was to walk me through the process of setting up an OpenVPN connection to the TryHackMe network. It taught me how to download the VPN config file, use the OpenVPN client to connect, and verify if the connection was successful so that I could access TryHackMe's machines directly from my local system.

🛠️ Key Tools/Commands Used

- **OpenVPN GUI** – Used on Windows to import and connect using the config file
- **Linux Terminal** – sudo openvpn /path/to/config.ovpn for manual connection
- **TryHackMe AttackBox** – A browser-based option if OpenVPN setup isn't preferred
- **Connection Checker** – On the Access Page, to confirm whether VPN is working

🧠 Concepts Learned

1. **VPN Basics**
    - Understood why VPNs are used in ethical hacking — to simulate being inside the target network.
    - Learned the difference between TryHackMe's VPN and corporate VPNs (THM's is for lab access).
2. **Access Methods**
    - Learned two main ways to connect:
      a) Using OpenVPN on my own machine
      b) Using the AttackBox directly from the browser
3. **Verification Process**
    - How to check if the VPN is connected properly
    - How to test access by launching a test machine and opening its IP in a browser

🔍 Walkthrough / How I Solved It

Tasks 1–3: OpenVPN Setup

- First, I went to the **Access Page** on TryHackMe and downloaded the .ovpn configuration file.

- On Windows, I installed the **OpenVPN GUI** and imported the config file.
- On Linux, I ran the command:
  sudo openvpn ~/Downloads/[filename].ovpn
- Once connected, I went back to the Access Page and saw the green tick mark showing that the VPN was working.

Task 4: Connection Verification

- I launched a **Test Machine** from the platform.
- Then, using my browser (or Firefox in AttackBox), I visited http://[MACHINE_IP].
- The flag on the machine's webpage was:
  flag{connection_verified}
- I submitted it and completed the room.

💡 **Reflections or Notes**

- This room helped me understand how OpenVPN works and why it's important for hacking labs.
- I now know how to set up a VPN connection on both Windows and Linux, which is very useful for other platforms too.
- It also gave me confidence in troubleshooting — like checking connection status if something isn't working.
- Although the AttackBox is simpler, learning OpenVPN setup is great for a more realistic hacking environment.

✅ **Room Name and Link**

Room Name: Beginner Path Introduction
Link: https://tryhackme.com/room/beginnerpathintro

🎯 **Learning Objective**

The purpose of this room was to give a basic introduction to web application security, explain the real-world effects of security flaws, and show why networking knowledge is important for cybersecurity. It also provided some hands-on practice with simple exploitation scenarios.

🛠️ **Key Tools/Commands Used**

- **Interactive Web Interface** – Used to explore BookFace and a data breach simulation
- **Browser Developer Tools** – Helped with inspecting the web pages
- **Critical Thinking Skills** – Used for analyzing and identifying vulnerabilities

🧠 Concepts Learned

1. **Web Application Security**
    - Learned how vulnerabilities are introduced in web apps.
    - Understood how these flaws can lead to serious real-world problems.
2. **Social Media Exploitation**
    - Saw how attackers can take over accounts by finding weaknesses in web apps.
3. **Networking Importance**
    - Realized how crucial basic networking knowledge is for things like log analysis, intrusion detection, and vulnerability scanning.
4. **Business Impact**
    - Got a sense of how much financial damage a data breach can cause a company.

🔍 Walkthrough / How I Solved It

Task 1: BookFace Account Takeover

- Clicked on **"View Site"** to open the vulnerable BookFace platform.
- Explored the website to find the username of the target account needed for the answer.

Task 2: Target Data Breach Analysis

- Accessed the Target data breach simulation by clicking **"View Site"**.
- Reviewed the information provided and identified the financial impact of the breach.

Task 3: Networking Fundamentals

- Went through the networking basics given in the room.
- Learned how networking knowledge helps with log checking, spotting attacks, and running scans for vulnerabilities.

💡 Reflections or Notes

- This room was an excellent starting point — especially because it connected technical skills with real-world examples like the BookFace and Target cases.
- It made me realize how important both web security and networking knowledge are for cybersecurity.
- I also figured out that I need to improve my understanding of web application security and study more networking basics to get better at detecting and preventing attacks.

Would you also like me to help you structure all these reports into a neat final document once we're done with all rooms? 🚀
Ready for the next one if you are!

✅ Room Name and Link

Room Name: Starting Out in Cyber Security
Link: https://tryhackme.com/room/startingoutincybersec

🎯 Learning Objective

The main aim of this room was to provide a beginner-friendly introduction to cybersecurity career paths. It clearly explained the difference between offensive (red team) and defensive (blue team) roles, highlighted the key skills needed in each field, and pointed out useful learning paths available on TryHackMe to get started.

🛠️ Key Tools/Commands Used

- **Career Path Exploration**:
  - **Offensive Security**: Penetration Testing, Cloud Security
  - **Defensive Security**: Security Analysis, Incident Response, Malware Analysis
- **TryHackMe Learning Resources**:
  - Beginner Path
  - SOC Level 1 Path
  - Individual rooms like Splunk, Volatility, and Malware Analysis

🧠 Concepts Learned

1. **Offensive Security (Red Team)**

    - Learned about ethical hackers who find vulnerabilities before real attackers do.
    - Required skills include web and network security, some scripting knowledge, and an understanding of cloud environments.
2. **Defensive Security (Blue Team)**
    - Got introduced to roles like Security Analyst and Incident Responder.
    - Learned how these professionals detect, respond to, and analyze attacks.
    - Also learned the basics of malware analysis and memory forensics.
3. **Matching Skills to Roles**
    - Understood that strengths like problem-solving, attention to detail, and analytical thinking are useful across both sides, but especially important in defensive roles.
4. **Learning Pathways**
    - Discovered structured learning routes:
        - **Beginner Path** for those leaning toward offensive roles.
        - **SOC Level 1 Path** for those interested in defensive cybersecurity.

🔍 **Walkthrough / How I Solved It**

Task 1: Offensive Security

- Read through the descriptions provided in the room about penetration testing and ethical hacking.
- Understood how red teamers approach systems to find weaknesses.

Task 2: Defensive Security

- Explored different blue team roles.
- Went through the overviews of the **Splunk** room for attack detection, **Volatility** for memory forensics, and **Malware Analysis** for understanding malicious files.

Task 3: Finding the Right Path

- Looked at the suggested paths and picked out the **Beginner Path** for offensive learning and **SOC Level 1 Path** for defensive skills.

💡 **Reflections or Notes**

- This room really helped me understand what the cybersecurity world looks like.

- I liked how it split the career options into two main sides—it made things much clearer for a beginner like me.
- The links to other rooms and paths were very helpful in planning what I want to learn next.
- I think I might be more interested in blue team roles like analysis and response, but I want to explore both sides a bit more before deciding.

✅ Room Name and Link

Room Name: Introduction to Research
Link: https://tryhackme.com/room/introtoresearch

🎯 Learning Objective

The goal of this room was to develop essential research skills for cybersecurity professionals. This involved learning how to effectively discover vulnerabilities, mastering the use of Linux manual (man) pages, and utilizing exploit databases like ExploitDB and CVE databases for research.

🛠️ Key Tools/Commands Used

- **Search Engines**: Used "Google-fu" to refine and find cybersecurity-related queries
- **Vulnerability Databases**:
  - **ExploitDB**
  - **NVD (National Vulnerability Database)**
  - **CVE Mitre**
- **Linux Tools**:
  - **searchsploit** (Offline ExploitDB tool)
  - **man** command (Manual pages)
  - **steghide** (Steganography tool)

🧠 Concepts Learned

1. **Research Methodology**

- Learned how to start with a broad search and progressively narrow it down for specific topics.
- Example: Started by searching "hiding data in images" → learned about steganography → found **steghide** as a tool for the task.

2. **Vulnerability Research**
    - Understood how to identify and interpret CVEs (Common Vulnerabilities and Exposures).
    - Used **searchsploit** to find exploit information and learned how to utilize **ExploitDB** and **NVD** to investigate vulnerabilities.
    - Examples:
        - **FuelCMS RCE**: CVE-2018-16763
        - **WPForms XSS**: CVE-2020-10385
        - **Apache Tomcat LPE**: CVE-2016-1240
        - **VLC CVE-2007-0017**
        - **Sudo buffer overflow**: CVE-2019-18634
3. **Linux Fundamentals**
    - Gained practical experience with **man** command navigation.
    - Learned tool switches like:
        - **SCP** for directory copying: -r
        - **fdisk** for partition listing: -l
        - **nano** for backup: -B
        - **Netcat listen mode**: nc -lvnp 12345

🔍 Walkthrough / How I Solved It

Task 1: Research Techniques

- Searched **"hiding things inside images"** and learned about **steganography**.
- Found **steghide** as the tool for this, and installed it via apt.

Task 2: Vulnerability Databases

- Used **ExploitDB** and **NVD** to search for vulnerabilities in specific software.
- Example: Found an **RCE exploit (CVE-2018-16763)** for FuelCMS.

- Identified various other CVEs like **CVE-2020-10385** for WPForms and **CVE-2016-1240** for Apache Tomcat.

Task 3: Linux Manual Pages

- Practiced using **man** to navigate through commands for:
    - **SCP** (-r for recursive copy)
    - **fdisk** (-l for listing partitions)
    - **nano** (-B for backups)
    - **Netcat** (nc -lvnp 12345 for listening mode)

💡 **Reflections or Notes**

- **Critical Skill**: Research is key in both offensive and defensive cybersecurity roles.
- **Tool Familiarity**: Tools like **searchsploit** and **man** pages save a lot of time in real-world scenarios.
- **Practical Application**:
    - **CVE research** directly applies to CTFs and pentesting engagements.
    - **Manual pages** help reduce the need to memorize commands, making it easier to focus on problem-solving.

This room gave me a solid foundation for cybersecurity research, and I feel more confident about using databases and Linux tools for future tasks.