**Practice of Cybersecurity Fundamentals**

**Student Name**

**Student Id**

**Summary**

TryHackMe is a real attempt that help in investigate the topic of cyber security that covering subjects such as vulnerability assessment, recon techniques and computer forensics. DFIR is the training prioirity that was related to “Nmap Live Host Discovery”,”Passive Reconnaissance”, “Windows Forensics” and “Passive Reconnaissance” that offer more practice. An overview of the entire DFIR process that will include problem identification, data treatment, locking down, goal-setting and picking things up. At the time of evaluation, documents and screenshots were taken that will be also showed the use of of old forensic tools that include “Nmap”,”whois”, and “Nslookup”. Due to the practical expertise, I was also able to connect with the theory that I had learned in the class with the actual field of cyber security it was also fit with the “NIST CSF 2.0 framework”. So, it will help to found that technical problems that will already process with the fundamental abilities.

Table of Contents

[1. Introduction 4](#_Toc209613824)

[2. Problem/Challenge 4](#_Toc209613825)

[3. Project Goals/Objectives 5](#_Toc209613826)

[4. Methodology 6](#_Toc209613827)

[Step 1: Hands-On Execution 6](#_Toc209613828)

[Step 2: Evidence Collection 6](#_Toc209613829)

[Step 3: Documentation & Report Preparation 7](#_Toc209613830)

[5. Results/Outcomes 7](#_Toc209613831)

[6. Reflection 12](#_Toc209613832)

[a) What did you learn about cybersecurity concepts and tools from this exercise? 12](#_Toc209613833)

[b) How do you see this experience contributing to your professional growth as a future cybersecurity practitioner? 13](#_Toc209613834)

[c) Looking back, what would you do differently if you repeated the task? 13](#_Toc209613835)

[References 14](#_Toc209613836)

[Appendix 15](#_Toc209613837)

[Github Portfolio Link: 15](#_Toc209613838)

# Introduction

The needs of the increasing sophistication of data security threats and cybersecurity experts who unite theory and practical skills in the identification, investigation, and response to events. Universities typically focus on models such as NIST CSF 2.0 and fundamentals of security, yet once you apply those models directly to the field, your technical abilities and troubleshooting are given an extreme shot of adrenaline(Korzhuk, Arustamov and Petersburg, 2024).To bridge that knowledge gap, this project has resorted to TryHackMe, a trendy web-based platform that presents interactive and easy-to-learn industry-relevant laboratories. The site operates real-world attack and defence movements to ensure learners can dive into incident answers, computer forensics, reconstruction tactics, and vulnerability scanning in a non-lethal, instructed manner.

Focused on the DFIR: An Introduction room since it touches upon the fundamentals of Digital Forensics and Incident Response, one of the priorities of the day-to-day operations. Thereafter, attacked additional rooms such as Windows Forensics, Nmap Live Host Discovery, Passive Reconnaissance and Active Reconnaissance to expand our horizon(Hasan et al., 2024). The exercises were a definite roadmap to develop strong tech competencies, acumen and cybersecurity-savvy skills that would secure them a position.

# Problem/Challenge

It was the primary challenge of this project to put all that cyber theory into texts for practical uses in actual, non-theoretical, interactive laboratories. Overview of incident response, forensics, recon, and scanning, yet when it comes to the practical bit of it, the real world, it leaves you with no more than the basics.

1. **DFIR Introduction:** This is a room that takes you through each of the phases of the Digital Forensics and Incident Response lifecycle: preparation, identification, containment, eradication, recovery and the lessons you can apply(Google Books, 2022). It also demonstrates to you the tools and the real-life practice you would use in the case of the occurrence of a security incident.
2. **Windows Forensics 1:**This is a visit to windows registry forensics. Also learn how to extract, deconstruct and interpret artifacts such as user logs of activity(Sajin Shivdas, 2023), installed applications and logs of your logins to create a narrative.
3. **Nmap Live Host Discovery:** It is involved with scanning the network using tools such as ARP, ICMP and TCP / UDP. Also, get to know how to identify active hosts, locate unprotected ports, and map available weak areas within a test network.
4. **Passive Reconnaissance:**You are given a chance to play with OSINT tools, which are whois, nslookup and dig to snatch information off open sources without being pinged at the target.
5. **Active Reconnaissance:**In this section, you learn to get your hands on it by using ping, traceroute, telnet, including even browser tricks to explore networks, verify that everything is functioning, and identify services(Choi, 2024), without neglecting ethics and the law.

# Project Goals/Objectives

The objectives in establishing the project were rather clear to make it match what is studied and the industry requirements:

**Practical Implementation of Cybersecurity Concepts**

* Learn in practice by approaching an incident response, vulnerability tests, scan, and recon tasks on TryHackMe.

**Industry Tools and Processes**

* Test Argument Smart tools including Nmap, Whois and nslookup and other forensic usefulness applications using a sandbox that simulates real-life cyber processes.

**Cybersecurity Frameworks Integration**

* Keep all the things traced to NIST CSF 2.0 - Identify, Protect, Detect, Respond, and Recoverrelevant to the pro work.

**The Development of a Professional Portfolio**

* Have a GitHub portfolio with steps and results, notes, etc., you can prepare to present to an employer, internship or entry position.

**Continuous Improvement Critical Reflection**

* Unteach yourself what was and still is difficult, but also what you are yet to teach to continue becoming a cyber pro.

# Methodology

To make the whole thing practical, collect the necessary facts, and ensure thatoperate within the professional habits of the cybersecurity field, follow a step-by-step plan.

## Step 1: Hands-On Execution

* **DFIR: An Introduction**
  + Explored incident response phases: Preparation 🡪 Detection 🡪 Containment 🡪 Eradication 🡪 Recovery 🡪 Lessons Learned.
  + learned what organisations do with incident response processes to handle breaches.
* **Windows Forensics 1**
  + Performed a registry scan of Windows personal computers to find user activity, user logons, and user configuration items of interest to an investigation.
* **Nmap Live Host Discovery**
  + ARP scans, battery checks and TCP/UDP pings to discover live networks and open ports of the mock networks.
  + Tools used: nmap -sn was used to give a quick scan.
* **Passive Reconnaissance**
  + Conducted some OSINT of Whois, Nslookup, and Dig to retrieve domain information, all undercover.
* **Active Reconnaissance**
  + Pinged, Traceroute, and Telnet with used tools to directly strike network systems, map the topology and ensure everything is connected.

**Reasoning:**The combination of passive and active recon with scans and forensics allowed us to generate a workflow of realistic cyber-defence.

## Step 2: Evidence Collection

* **Systematic Screenshot Capture:**
  + **Start of the Room**🡪 To verify the chosen challenge and the initial setup.
  + **Tool Usage Stages**🡪 For example, Nmap scan commands, Whois lookups, Windows Registry analysis, and traceroute results.
  + **Key Results/Flags**🡪 Captured the outcomes (discovered hosts, registry entries)

## Step 3: Documentation & Report Preparation

* **Structured Recording of Activities:**

Once the wrapping of each room was completed recorded the details step by step:

* 1. **Objective of the Room**🡪Incident response fundamentals, OSINT gathering.
  2. **Tools Used**🡪 Nmap, Whois, Nslookup, Registry Explorer.
  3. **Steps Performed**🡪 Commands run, scans executed, artifacts analysed.
  4. **Findings**🡪important responses such as live host discoveries or odd registry entries.
* **NIST CSF 2.0 Functions:**
  + **Identify**🡪 Reconnaissance activities (Passive & Active)
  + **Protect**🡪 Forensics analysis for system hardening
  + **Detect**🡪 Incident detection via DFIR exercises
  + **Respond**🡪 Incident response workflows
  + **Recover**🡪 Lessons learned for system improvement
* **Integration into Final Report:**

All written materials and screenshots were gathered into a professionalised Word/PDF document with sections on methodology, findings, evidence and reflection.

# Results/Outcomes

The results of the project provided practical learning outcomes on all five rooms of TryHackMe, and all evidence was recorded in the format of screenshots, logs, and steps. These findings illustrate the practical use of cybersecurity solutions and methods according to the best practices in the industry.

**1. DFIR: An Introduction**

* **Key Results:**
  + Understood the six phases of incident response:
    1. Preparation
    2. Detection & Analysis
    3. Containment
    4. Eradication
    5. Recovery
    6. Lessons Learned
  + Explored real-world use cases where DFIR processes mitigate cyber incidents efficiently.
* **Outcome:**Developed a much better understanding of how breaches are processed in orgs and the workflow involved.

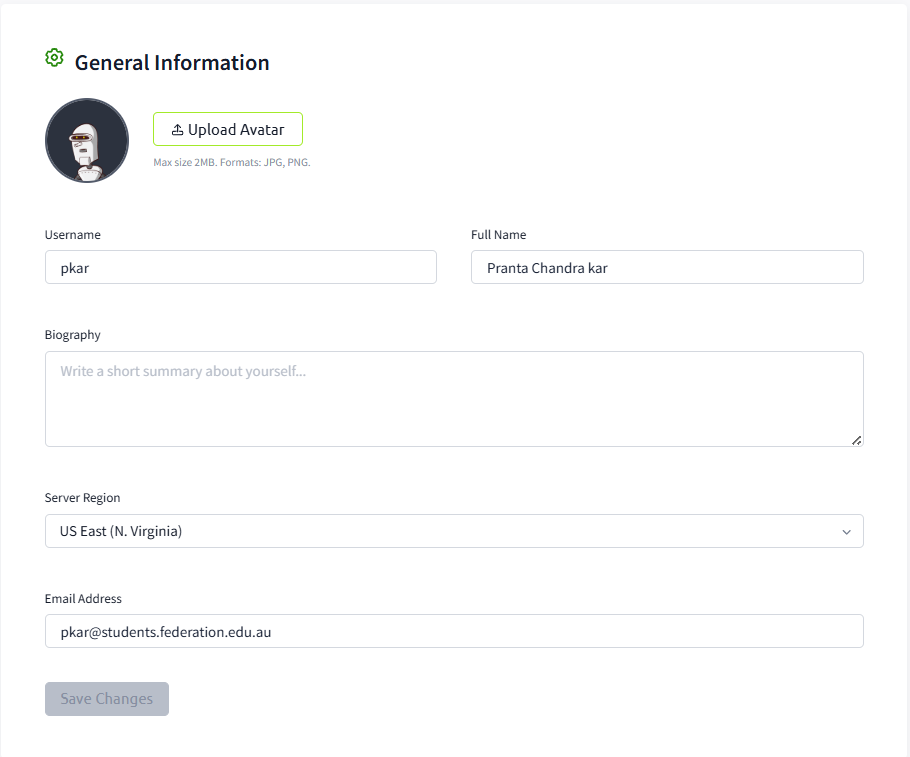


Figure 1: FedUni email for verification

(Source: Self-Created)

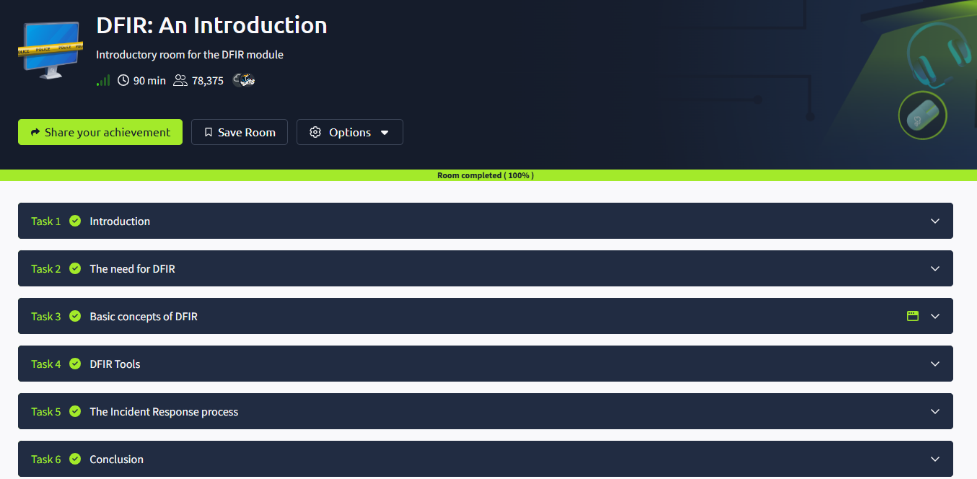


Figure 2: Completed DFIR room showing all tasks covering incident response phases

(Source: Self-Created)

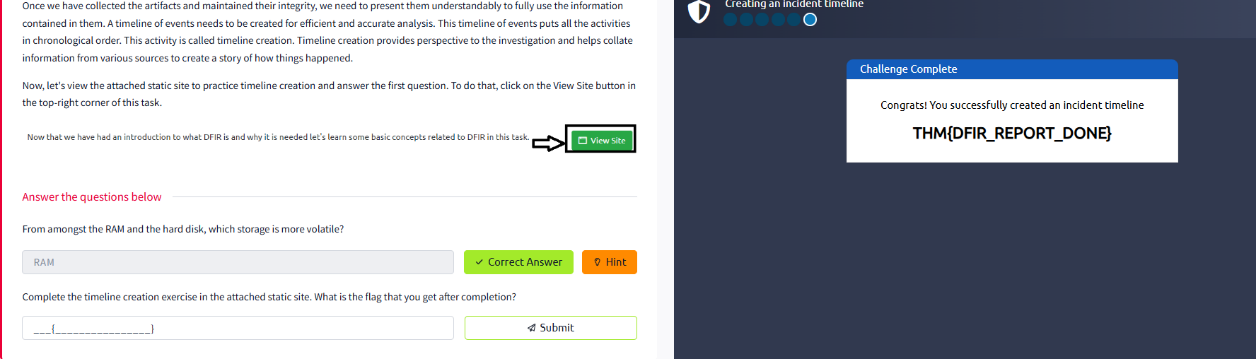


Figure 3: Flag submission in the DFIR room

(Source: Self-Created)

**2. Windows Forensics 1**

* **Key Results:**
  + Learned how to read Windows Registry artifactsto produce user access logs, system settings and clues of the forensic analysis.
  + Registry hives containing the checked user login timestamps, previously installed programmes, and web browser history.
* **Outcome:**learned the expertise to gather evidence online and reconstruct whether there was activity on a system.

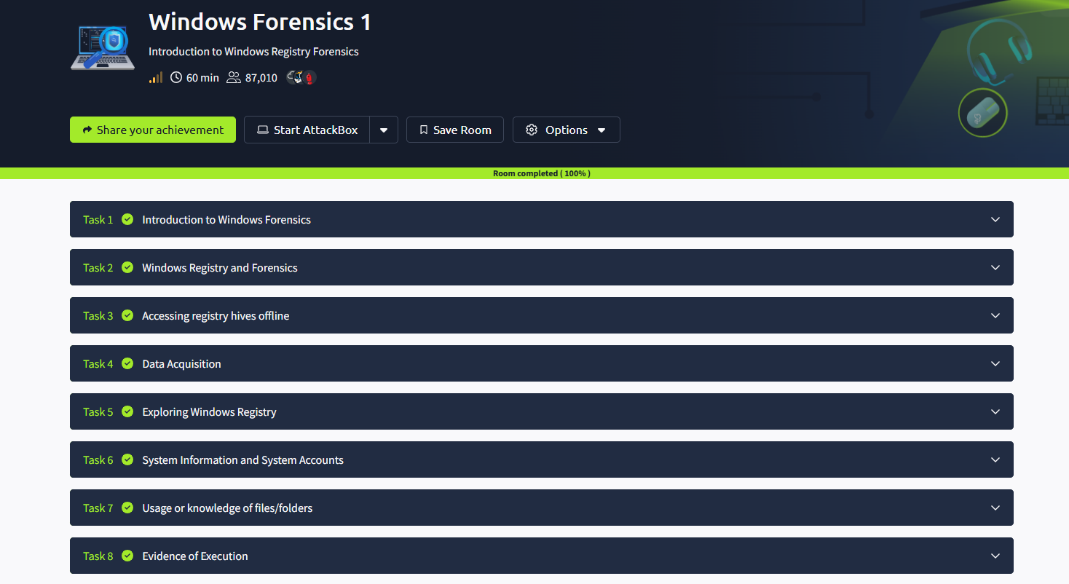


Figure 4: Completed Windows Forensics 1

(Source: Self-Created)

**3. Nmap Live Host Discovery**

* **Key Results:**
  + Used nmap commands to perform:
    - **ARP scans**: Detect devices in local networks.
    - **ICMP scans**: Identify live hosts via ping sweeps.
    - **TCP/UDP scans**: Discover open ports and services.
  + Example: nmap -sn 192.168.1.0/24 to detect all live hosts in a subnet.
* **Outcome:**Learned how to outline network equipment and identify potential vulnerabilities in a simulation.

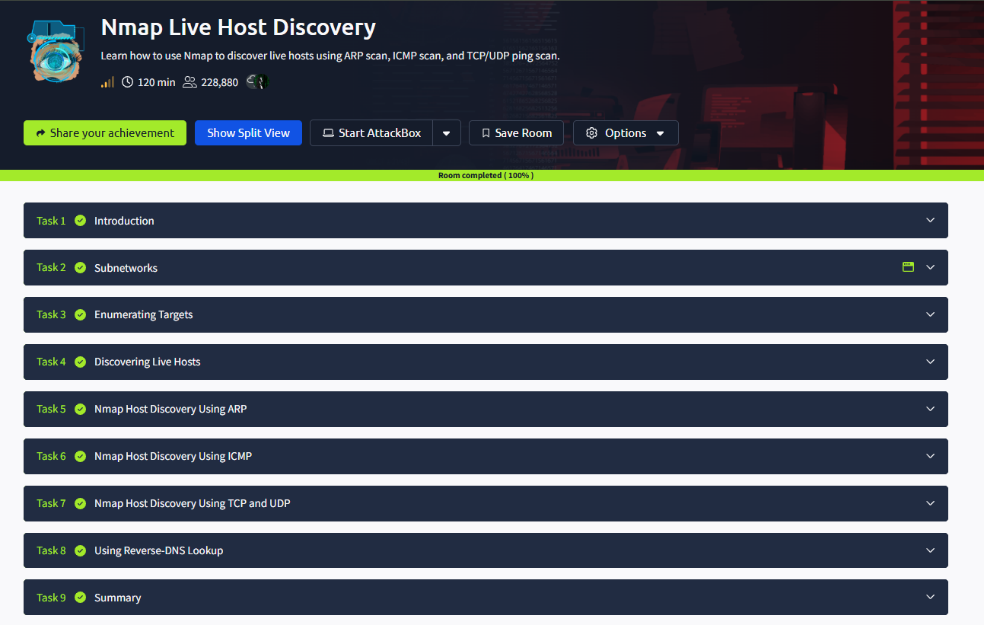


Figure 5: Completed Nmap room scans for live host detection.

(Source: Self-Created)

**4. Passive Reconnaissance**

* **Key Results:**
  + Used Whois, Nslookup, and Dig for collecting DNS and domain records without active engagement.
  + Example: nslookup example.com for DNS resolution details.
* **Outcome:**Awareness of the use of OSINT in the initial stages of gathering information related to a pre-attack reconnaissance.

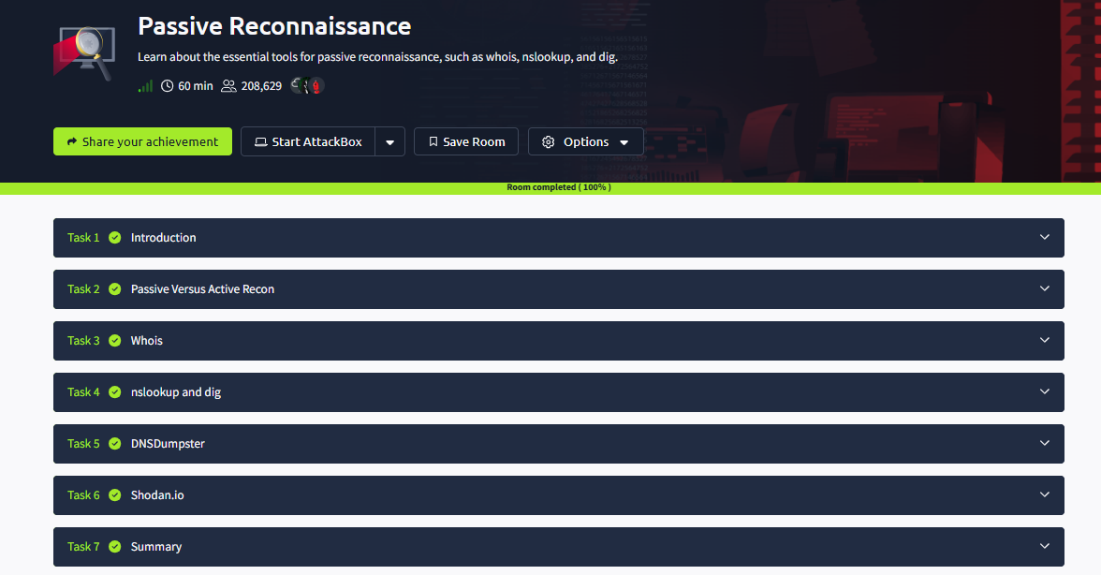


Figure 6: Completed Passive Recon room

(Source: Self-Created)

**5. Active Reconnaissance**

* **Key Results:**
  + Ping, Traceroute, and Telnet were also read to access the hosts using tapped tools and makeconnections with network extensions.
  + Example: traceroute example.com to trace network paths.
* **Outcome:**Learned direct engagement methods while emphasising ethical and legal boundaries in active reconnaissance.

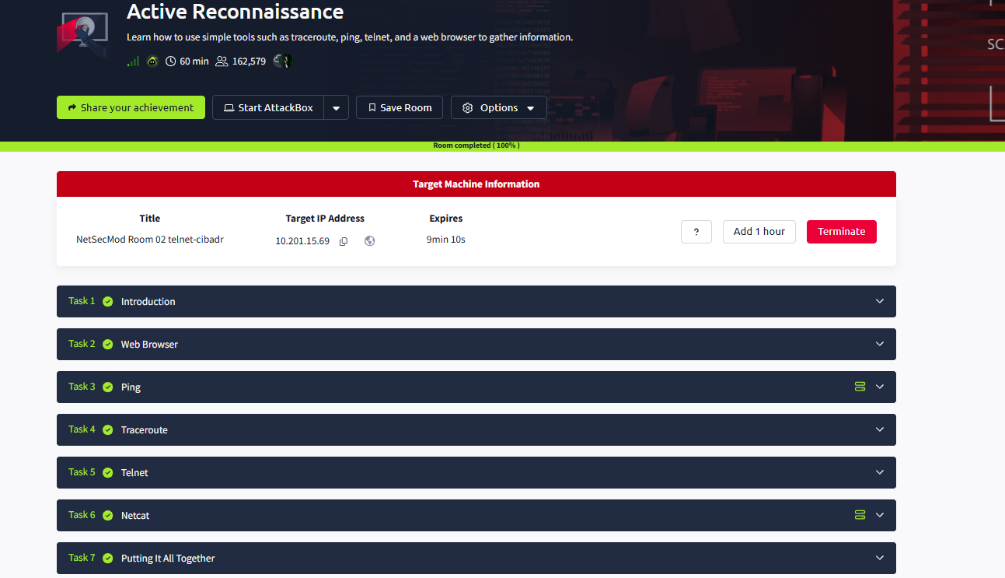


Figure 7: Completed Active Recon room web-based reconnaissance tasks

(Source: Self-Created)

# 6. Reflection

## a) What did you learn about cybersecurity concepts and tools from this exercise?

A completion of the five TryHackMe rooms provided a practical experience of the tools and processes involved in the field:

* **Incident Response:**Became familiar with the six-stage incident response lifecycle (Preparation, Detection, Containment, Eradication, Recovery, Lessons Learned) and how it is applied in real-world breach scenarios(Google Books, 2022).
* **Forensics:**Learned to process Windows Registry artifacts to create timelines of user activity, spot suspicious actions, and preserve digital evidence for investigation.
* **Vulnerability Scanning:**Found practical ways to use Nmap in locating hosts that are alive, open ports, and networked environments that might contain vulnerabilities.
* **Reconnaissance:** Utilisation of direct engagement tools such as Traceroute, Ping and Telnet to active OSNIT and reconnaissance techniques such as Nslookup, Whois and Dig that was used for passive intelligence collection.

Those activities enhanced theoretical ideas with practical expertise by connecting the gap within classroom instruction and real world application.

## b) How do you see the experience contributing to your professional growth as a future cybersecurity practitioner?

The number of career-relevant abilities which an entry-level expert might be easily affected like those are applicable to the positions such as Incident Responser, SOC Analyst and Cyber security consultant, that will also enhanced the results of the project:

* **Technical Proficiency:** By knowing how to use well-known tools such as Nmap and forensic programs that will opens the door of the real-world cyber security problems.
* **Problem-solving :** Analytical thinking may be improved by integrating reconnaissance correlational of the data, forensic evidence and scan results into process of incident – response.
* **Professional Portfolio:** By this employers can view a career-ready portfolio that basically represents the technical and documentation skills by posting the full project on GitHub.

Therefore by gaining greater practical ability and trust to do most basic responsibility of cyber security in a work setting.

## c) Looking back, what would you do differently if you repeated the task?

1. **Attempt Advanced Rooms:**Explore more complex labs such as Incident Response Fundamentals or Blue Team Labs to gain deeper technical skills.
2. **Automate Scans & Reports:**Use Python or Bash to automate tedious tasks, such as Nmap scanning or evidence collection.
3. **Collaborate with Peers:**Perform group-based challenges simulating a real-world SOC culture and incident management team workflow.
4. **Integrate SIEM Tools:**Using Splunk or ELK Stack for centralised log analysis and incident detection.

# References

Choi, B. (2024). Cisco IOS, Linux, TFTP, and Telnet Labs. *Introduction to Python Network Automation Volume I - Laying the Groundwork*, pp.753–802. doi:https://doi.org/10.1007/979-8-8688-0146-4\_11.

Google Books. (2022a). *CEH Certified Ethical Hacker Cert Guide*. [online] Available at: https://books.google.com/books?hl=en&lr=&id=YPXOEAAAQBAJ&oi=fnd&pg=PT22&dq=Became+familiar+with+the+six-stage+incident+response+lifecycle+(Preparation [Accessed 24 Sep. 2025].

Google Books. (2022b). *Digital Forensics and Incident Response*. [online] Available at: https://books.google.com/books?hl=en&lr=&id=1N-fEAAAQBAJ&oi=fnd&pg=PP1&dq=:+This+is+a+room+that+takes+you+through+each+of+the+phases+of+the+Digital+Forensics+and+Incident+Response+lifecycle:+preparation [Accessed 24 Sep. 2025].

Hasan, M., Arifin, M., Khan, R., Hussain, M., Al Mamun, A., Hossain, Islam, S. and Nurazzaman, K. (2024). A COMPREHENSIVE INVESTIGATION OF RECONNAISSANCE THREATS AND ITS REMEDIATION. *International Journal of Advanced Research in Management and Social Sciences Impact*, [online] 13(11). Available at: https://garph.co.uk/IJARMSS/Nov2024/G-3092.pdf.

Korzhuk, V., Arustamov, S. and Petersburg, S. (2024). Available at: https://books.ifmo.ru/file/pdf/3294.pdf.

Sajin Shivdas (2023). A Complete Handbook for Digital Forensics Investigator. *International Journal for Research in Applied Science and Engineering Technology*, 11(8), pp.813–832. doi:https://doi.org/10.22214/ijraset.2023.55257.

# Appendix

## Github Portfolio Link:

<https://github.com/pkar412/Cybersecurity_Portfolio/blob/main/README.md>