A COMPREHENSIVE CAPTURE THE FLAG GUIDE FOR UTAR STUDENTS

By

Ang Boon Keat

A REPORT

SUBMITTED TO

Universiti Tunku Abdul Rahman

in partial fulfillment of the requirements

for the degree of

BACHELOR OF INFORMATION TECHNOLOGY (HONOURS)
COMMUNICATIONS AND NETWORKING
Faculty of Information and Communication Technology
(Kampar Campus)

JUN 2024

UNIVERSITI TUNKU ABDUL RAHMAN

REPORT STATUS DECLARATION FORM

Title: A Comprehensive Capture The Flag Guide for UTAR Students

Academic Session: Year 4 Trimester 1

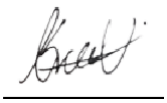
I ANG BOON KEAT

(CAPITAL LETTER)

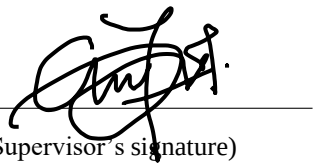
declare that I allow this Final Year Project Report to be kept in Universiti Tunku Abdul Rahman Library subject to the regulations as follows:

1. The dissertation is a property of the Library.
2. The Library is allowed to make copies of this dissertation for academic purposes.

Verified by,



(Author's signature)



(Supervisor's signature)

Address:

6, Laluan Lapangan Perdana 3

Bandar Cyber

Ipoh Perak

Puan.Nor 'Afifah Binti Sabri

Supervisor's name

Date: 20/08/2024

Date: 12/09/2024

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TUNKU ABDUL RAHMAN

Date: 2 September 2024

SUBMISSION OF FINAL YEAR PROJECT

It is hereby certified that ***Ang Boon Keat*** (ID No: **20ACB03822**) has completed this final year project/ dissertation/ thesis* entitled "*A Comprehensive Capture The Flag Guide For UTAR Students*" under the supervision of of Puan.Nor 'Afifah Binti Sabri (Supervisor) from the Department of Computer and Communication Technology, Faculty of Information and Communication Technology, and Dr. Aun YiChiet (Co-Supervisor) from the Department of Information and Communication Technology, Faculty of Information and Communication Technology.

I understand that University will upload softcopy of my final year project / dissertation/ thesis* in pdf format into UTAR Institutional Repository, which may be made accessible to UTAR community and public.

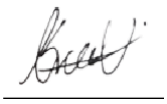
Yours truly,

(*Ang Boon Keat*)

*Delete whichever not applicable

DECLARATION OF ORIGINALITY

I declare that this report entitled "**A Comprehensive Capture The Flag Guide For UTAR Students**" is my own work except as cited in the references. The report has not been accepted for any degree and is not being submitted concurrently in candidature for any degree or other award.

Signature : 

Name : Ang Boon Keat

Date : 20/08/2024

ACKNOWLEDGEMENTS

I would like to express my sincere thanks and appreciation to my supervisors, **Puan Nor' Afifah Binti Sabri** and **Dr Aun Yi Chiet** who has given me this bright opportunity to engage in the development of CTF education platform project for UTAR Students. A million thanks to you.

Besides, I must say thanks to my parents and my family for their love, support, and continuous encouragement throughout the course.

ABSTRACT

This research paper explores the development and implementation of a comprehensive Capture the Flag (CTF) guide aimed at enhancing cybersecurity education for students at Universiti Tunku Abdul Rahman (UTAR). Motivated by the growing gap between theoretical cybersecurity knowledge and the practical skills required to navigate the complexities of real-world cyber threats, this project introduces an innovative, easy-to-understand CTF guide. The guide is designed to cater to both beginners and advanced learners to cover a wide range of cybersecurity topics including web application security, reverse engineering, digital forensics, cryptography, and steganography through hands-on challenges that simulate authentic cybersecurity scenarios. By providing a dynamic learning platform that bridges academic learning with practical application, this initiative not only aims to equip UTAR students with critical technical skills but also to inspire a deeper interest in cybersecurity while encouraging more students to pursue careers in this vital field. The project contributes significantly to cybersecurity education research, offering insights that can inform future educational initiatives and support the integration of practical cybersecurity exercises into academic curricula.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

CTF	Capture The Flag
UTAR	Universiti Tunku Abdul Rahman
GDB	GNU Debugger
PWN	Binary Exploitation
GCP	Google Cloud Platform

CHAPTER 1

Introduction

According to [1], the concept of CTF initially comes from a traditional outdoor team sport where participants are divided into two groups. Each group is tasked with both protecting their own flag located at their base and attempting to capture the flag of opposing team. The game itself has its roots in physical teamwork and strategy found a new arena in the digital world starting from the 1990s. In the realm of cybersecurity, CTF has evolved to encompass a wide variety of events that vary greatly in scope and format that range from competitive online challenges focused on attack strategies to educational exercises designed to support the learning process and even to events aimed purely at entertainment and outreach.

There are primarily two categories of CTF in the realm of cybersecurity: jeopardy and attack-defense. In the jeopardy-style CTF, the structure is straightforward. The participants tackle a variety of cybersecurity puzzles that are organized into distinct categories based on skill level. These puzzles might encompass areas like web application security, reverse engineering, digital forensics, cryptography and steganography. On the other hand, attack-defense format assigns each competitor or team a virtual machine or network to protect. These systems are intentionally designed with vulnerabilities which present opportunities for competitors to exploit each other's weaknesses.

In this paper, we will be focusing on jeopardy-style CTF rather than attack-defense CTF. According to [2], a CTF is typically hosted as competition where participants embark on a quest to discover "flags" hidden within a carefully designed environment. The flags are typically unique strings of characters which serve as a proof of the participant's ability to navigate and overcome specific cybersecurity challenges such as breaching a database and exploiting a vulnerability. CTFs can vary significantly in scale and complexity which ranges from single-domain challenges to expansive networks simulating real-world cybersecurity scenarios. Additionally, the integration of a scoring system adds a competitive edge to CTFs which allow participants to submit found flags

and earn points for each verified capture. This system not only facilitates the immediate recognition of participants' achievements, but also enables the real-time tracking of standings through online scoreboards. As a result, this will foster a sense of community and competition among participants.

1.1 Problem Statement and Motivation

In the rapidly evolving digital landscape, cybersecurity threats pose an increasing challenge to individuals, organizations and nations alike. Despite the growing recognition of the importance of cybersecurity, there remains a significant gap between theoretical knowledge and practical skills among students pursuing higher education in this field. At UTAR, like many academic institutions, the current curriculum emphasizes theoretical understanding of cybersecurity concepts in which while foundational, it does not fully equip students with the hands-on experience needed to navigate and counter real-world cyber threats effectively. This lack of practical exposure leaves students ill-prepared to apply their knowledge in practical scenarios. As a result, it will hinder their ability to effectively identify, analyze and mitigate cybersecurity vulnerabilities. Moreover, the conventional educational approaches may fail to fully engage students or inspire a deep and enduring interest in the field of cybersecurity. Hence, the CTF is an underutilized educational tool in the academic context. However, despite the abundance of CTF tutorials available online, the absence of easy-to-understand resources represents a critical barrier to enhance cybersecurity competence among UTAR students. Many of the available tutorials assume a level of prior knowledge or technical expertise that may not be present among all students, thereby limiting their effectiveness as learning tools. This emphasizes the need for a comprehensive easy-to-understand CTF tutorial that not only introduces students to practical cybersecurity challenges but also guides them through the process of developing the necessary skills to tackle these challenges head-on.

1.2 Project Objectives

The primary objective of this project is to propose and develop an educational framework that significantly enhances the cybersecurity competencies of students at UTAR. A key objective is to make cybersecurity learning accessible and appealing to a wide range of students regardless of their initial level of expertise. By offering a structured yet flexible curriculum, the project intends to cater to both beginners and more advanced learners to ensure that every student can progress at their own paces and according to their individual learning goals. Besides, this project also seeks to bridge the gap between theoretical knowledge and practical application to enable students to apply what they have learned in simulated real-world scenarios that reflect the current cybersecurity landscape. Finally, this project seeks to equip UTAR students with a solid foundation in cybersecurity and empowering them to protect themselves and their communities from cyber threats and paving their way for future innovations in cybersecurity education and practice.

1.3 Project Scope

The scope of this project is to design and implement an educational resource specifically to improve the cybersecurity skills of students at UTAR. This project covers several key activities, starting with a comprehensive literature review on CTF competitions, cybersecurity education methodologies and the impact of practical learning tools on skill enhancement. The foundational of this project lies in developing a structured tutorial curriculum that addresses a wide range of cybersecurity topics such as reverse engineering, binary exploitation, cryptography, digital forensics and steganography. Besides, a significant portion of the project involves the creation of CTF challenges that mirror real-world cybersecurity scenarios to provide students with an opportunity to apply theoretical concepts in a practical and engaging setting. To house these tutorials and challenges, an online platform will be developed that serves as the central access point for students to engage with the materials and track their progress. Finally, the outcomes and insights gained from this project will be thoroughly documented in a detailed report, outlining the development process, tutorial structure, along with recommendations for future enhancements. This documentation will not only serve as a roadmap for continuous improvement of the tutorial but also as a guide for UTAR administrators and educators looking to integrate practical cybersecurity

learning experiences into their curricular, thereby complementing and augmenting the traditional educational approach with hands-on, experiential learning opportunities.

1.4 Contributions

The contributions of this project are as follows:

1. Development of a Tailored CTF tutorial: This tutorial covers a wide range of cybersecurity topics, including but not limited to reverse engineering, binary exploitation, cryptography, digital forensics, and steganography. By breaking down complex concepts into accessible, manageable components, the tutorial aims to lower the barrier to entry for students new to cybersecurity making it an invaluable resource for both beginners and advanced learners.
2. Practical skill application through real-world challenges: Unlike traditional theoretical education, this project emphasizes the application of knowledge through hands-on challenges that simulate real-world cybersecurity scenarios. This practical orientation helps students develop critical thinking, problem-solving and technical skills that are directly applicable to their future careers in cybersecurity.
3. Contribution to cybersecurity education research: The insights gained from this project can inform future educational initiatives, both within UTAR and at other institutions that seek to integrate practical cybersecurity exercises into their curricula.

1.5 Report Organization

The report's organization is structurally meticulous to provide adequate understanding of the development which has been conducted. The second chapter commences with a review of literature examining previous studies, their limitations, and proposed solutions which build a foundation for the project. The third chapter outlines the proposed methodologies and approaches, including system requirements as well as unique implementation challenges. In chapter 4, preliminary work is documented covering software setup process and initial stages of development that give an insight into what happened. Finally, chapter 5 will summarize conclusions of the project by drawing together findings and implicating future research. This kind of an approach ensures logical progression within the report from foundational research to a culmination of the project.

CHAPTER 2

Literature Reviews

2.1 Previous Works

According to [3], many studies have focused on the design, implementation, and evaluation of CTF platforms, emphasizing their role in cybersecurity education and competition. These studies have consistently demonstrated the effectiveness of CTF platforms in fostering hands-on learning and skill development in areas such as offensive and defensive security. One key focus is on the customization of challenges, with research highlighting that the ability to tailor the difficulty level and provide meaningful feedback is crucial in enhancing both learning outcomes and participant motivation. Additionally, the article has explored the creation of challenges that cater to varying levels of cybersecurity skills and knowledge, ensuring that beginners and advanced users alike can benefit from the CTF experience. The article also discusses how different features of CTF platforms, such as real-time scoring and interactive game environments, contribute to participant engagement and deeper learning. Furthermore, the difficulty and complexity of challenges are often linked to participant retention, as well-designed challenge progressions can keep users motivated and engaged throughout the competition.

According to [4], CTF competitions have been recognized as an effective method to engage students in cybersecurity education. The article highlights the importance of using scenario-based CTF competitions as a hands-on, interactive approach to introduce secondary school students to technical cybersecurity concepts. These competitions provide an engaging platform for students with little or no technical background to develop essential skills such as problem-solving, teamwork, and critical thinking in a gamified environment. Specifically, the scenario-based approach utilized in the UNITEN Cyber Hunt CTF event proved effective in sparking interest among participants by presenting challenges in a real-world context, enhancing both learning and motivation. Furthermore, the article discusses how CTF competitions can be aligned with educational curricula, particularly in regions where cybersecurity

education is still nascent, such as Malaysia. By incorporating topics like cryptography, steganography, and web forensics, CTF challenges help to bridge the gap between theoretical knowledge and practical application, making the learning experience both informative and engaging. The study concludes that such competitions can significantly improve students' understanding of cybersecurity concepts and boost their interest in pursuing careers in STEM fields, particularly in the cybersecurity domain.

Based on [5], the author discusses the implementation of a CTF-based educational framework at Altai State University. The framework was designed to provide students with hands-on experience and practical knowledge in information security through extracurricular activities. The CTF Club sessions is held three times a week that offer students opportunities to engage in teamwork, solve real-world cybersecurity problems and develop skills such as script programming, system administration and networking. The framework successfully complements the traditional curriculum by filling in gaps where students lack practical experience. Feedback from students shows the success of the program, particularly in building teamwork and problem-solving skills in cybersecurity tasks such as attack-defense competitions and vulnerability exploitation.

In the article [6], the authors present a novel approach to introducing CTF competitions to individuals with little or no background in cybersecurity. By incorporating gamification techniques, the authors designed an entry-level CTF game that combines elements of a traditional escape room with cybersecurity challenges. The game was tested in both physical and online formats, showing positive engagement and learning outcomes among participants, including non-expert audiences such as high school students. The paper highlights the importance of creating interactive and accessible learning environments to foster cybersecurity awareness and skills development, especially for beginners.

Besides, based on [7], a detailed review of the strategies used in CTF competitions is presented in the article. The authors explore the tactical approaches adopted by participants to effectively solve various cybersecurity challenges. These strategies often involve collaborative teamwork, reverse engineering, and exploiting system vulnerabilities. The article emphasizes how CTF competitions foster a competitive yet

educational environment where participants must combine theoretical knowledge with practical skills to overcome intricate problems. By breaking down these strategies, the authors highlight the critical thinking and problem-solving abilities required in real-world cybersecurity scenarios, making CTFs an ideal tool for both training and evaluating participants in the field. Additionally, the article provides a taxonomy that categorizes the different types of challenges commonly found on CTF platforms. This classification includes key areas such as cryptography, binary exploitation, reverse engineering, web security, and others. Each category demands distinct skill sets, allowing participants to specialize in or rotate between different domains of cybersecurity. The taxonomy not only aids in understanding the wide range of topics covered in CTFs but also serves as a framework for developing educational programs that integrate gamified learning. Through this structured approach, CTFs help participants master both foundational knowledge and hands-on cybersecurity techniques, reinforcing their overall competence in the field.

Lastly, [8] describe the implementation of a CTF platform specifically designed for information security education. The platform aims to engage students in hands-on learning through challenges that simulate real-world cybersecurity problems. Key features of the platform include a dynamic challenge selection process, automated evaluation systems, and detailed feedback mechanisms that help students understand their strengths and weaknesses. The article emphasizes the pedagogical benefits of using CTFs, highlighting how they encourage active learning by integrating theory with practical exercises. The study presented in the article evaluates the platform's effectiveness as a training tool for information security education. The results indicate that CTF-based learning fosters student engagement, improves problem-solving skills, and deepens understanding of cybersecurity concepts. Students were able to apply theoretical knowledge in a competitive, gamified environment, which led to greater retention of information and practical skills development. This combination of education and competition makes CTF platforms a valuable addition to traditional learning methods in cybersecurity education.

2.2 Review of the Existing Learning Platform for CTF

In the domain of CTF and cybersecurity education, various platforms and applications have been developed to facilitate learning, challenge-solving, and skill development. These existing applications provide users with hands-on experience in diverse cybersecurity topics such as cryptography, binary exploitation, forensics, and reverse engineering. By simulating real-world security scenarios, these platforms help learners develop critical thinking and problem-solving skills in a controlled, gamified environment. This section provides an in-depth review of some of the most popular and widely used CTF platforms, highlighting their features, advantages, and limitations. Understanding the current landscape of CTF applications is crucial for identifying gaps and opportunities to enhance the learning experience for both beginners and advanced users in future platform development.

2.2.1 PicoCTF

PicoCTF is a free learning platform developed by cybersecurity and software experts from Carnegie Mellon University designed to teach young people foundational concepts in computer security. According to [9], the authors also discuss the impact and success of picoCTF in terms of participation and educational outcomes. The competition not only garnered participation from many students but also effectively introduced advanced technical topics like command-line interfaces, cryptographic ciphers, and program representation, even to those without prior programming experience. Through this initiative, students were able to gain hands-on experience with real-world cybersecurity problems. Feedback from both students and teachers was overwhelmingly positive, with many highlighting the competition as a valuable learning tool that inspired students to further pursue studies and careers in computer science and cybersecurity.

2.2.2 TryHackMe

Based on [10], TryHackMe is an online platform that provides cybersecurity training, offering learning materials for individuals of all skill levels, from beginners to advanced users. Co-founders Ben Spring and Ashu Savani started TryHackMe to address the challenges of accessing the cybersecurity field. Prior to its launch, learning cybersecurity was often difficult due to the lack of clear guidance and hands-on

challenges, making it hard for newcomers to enter the industry and for professionals to continuously improve their skills. TryHackMe aims to bridge that gap.

2.2.3 HackTheBox (HTB)

According to [11], HTB is a gamified cybersecurity training platform designed to help individuals, businesses, and educational institutions improve their security skills. It offers interactive labs, CTF challenges, and certifications, focusing on both offensive and defensive security. HTB aims to bridge the gap between theoretical knowledge and practical experience by providing realistic hacking scenarios that sharpen problem-solving skills. Its global community of users benefits from continuous learning, upskilling, and networking opportunities.

2.2.4 SKRCTF

According to [12], SKR CTF is a CTF team from Malaysia which is active since 2018. Their website is designed to help beginners learn cybersecurity by solving CTF challenges through hands-on practice. The platform aims to teach fundamental cybersecurity skills and engage learners in practical exercises. SKR CTF emphasizes a learning community, encouraging participants to join their Discord channel for discussions and support.

2.3 Functionality of Existing Platform

Functionality	PicoCTF	TryHackMe	HTB	SKRCTF
Visualization	Challenges, categories, scores	Challenges, categories, scores	Challenges, categories, scores	Challenges, categories, scores
User Classification	No	Yes	Yes	No
Subscription	Free	Free and paid	Free and paid	Free
Learning Content	No	Yes	Yes	Limited

Table 2.3.1 Functionality of Existing Platform

The comparison of existing platforms, such as PicoCTF, TryHackMe, HTB, and SKR CTF, highlights their key functionalities. All four platforms offer visualization through challenges, categories, and scores. TryHackMe and HTB include user classification features, while PicoCTF and SKR CTF do not. Subscriptions for PicoCTF and SKR CTF are free, while TryHackMe and HTB offer both free and paid options. In terms of learning content, PicoCTF offers none, SKR CTF provides limited resources, while TryHackMe and HTB provide comprehensive learning materials for users.

2.4 Proposed Solution

The proposed solution centers on the development of a structured, modular approach to CTF guides. This structure would begin with the basics of cybersecurity, gradually building up to more complex concepts and challenges. By adopting a step-by-step approach, the guide would ensure that beginners are not overwhelmed and can build their knowledge base and confidence progressively. Each module could conclude with a set of CTF challenges that reinforce the concepts covered to provide immediate practical application and helping to solidify learning. This approach would not only cater to the learning pace of beginners but also accommodate varying levels of prior knowledge among learners.

Moreover, to bridge the gap between CTF exercises and real-world cybersecurity scenarios, the guide could include case studies and examples drawn from actual cybersecurity incidents. By illustrating how the skills developed through CTF challenges apply in real-world contexts, the guide would enhance learners' understanding of the practical relevance of their learning. This contextualization could also serve to motivate beginners by demonstrating the impact of cybersecurity skills in addressing genuine threats, thereby making the learning experience more meaningful and engaging.

Functionality	**UTAR CTF Guide**
Visualization	Challenges, categories, scores
User classification	No
Subscription	Free
Learning Content	Yes

Table 2.4.1 Functionality of UTAR CTF Guide Platform

2.5 Method

To develop beginner learning materials for your CTF learning website, we draw inspiration from the following resources:

- For **cryptography**, **CTF101** provides comprehensive beginner guides on key cryptographic concepts used in CTF challenges, including hashing, encryption, and decryption methods. These materials offer practical exercises that build foundational cryptography skills essential for cybersecurity. Source: https://ctf101.org/

- To cover **reverse engineering and binary exploitation**, **Guy in a Tuxedo** offers detailed resources focusing on program analysis, debugging, and exploitation techniques. These resources help learners tackle CTF challenges that require deep understanding of how software and systems operate. Source: https://guyinatuxedo.github.io/index.html

- For **forensics**, **Trail of Bits** provides excellent materials focusing on digital evidence recovery and analysis techniques used in CTF challenges. The guide covers key areas such as memory forensics, file carving, and network forensics. Source: https://trailofbits.github.io/ctf/forensics/

CHAPTER 3

System Methodology/Approach

The processes for this project were categorized into different phases in the development. Each phase is pivotal to the creation of the educational content. The project kicks off with the curriculum design and content development phases which is centered around constructing the educational framework for the CTF guide. This involves a meticulous literature review to pinpoint the crucial cybersecurity topics and skills for UTAR students. Concurrently, instructional materials and tailored CTF challenges are crafted to align with the curriculum to ensure a coherent and engaging learning journey. The second phase will be the development phase, which focuses on the technical construction of a web-based platform that will host the tutorial and challenges. This phase covers design, coding and integration of interactive elements to forge a user-friendly and stimulating educational environment.

3.1 System Design Diagram

In this section, the system architecture diagrams and the use-case diagram will be listed in this section to provide an overview of the system.

3.1.1 GCP System Architecture Diagram

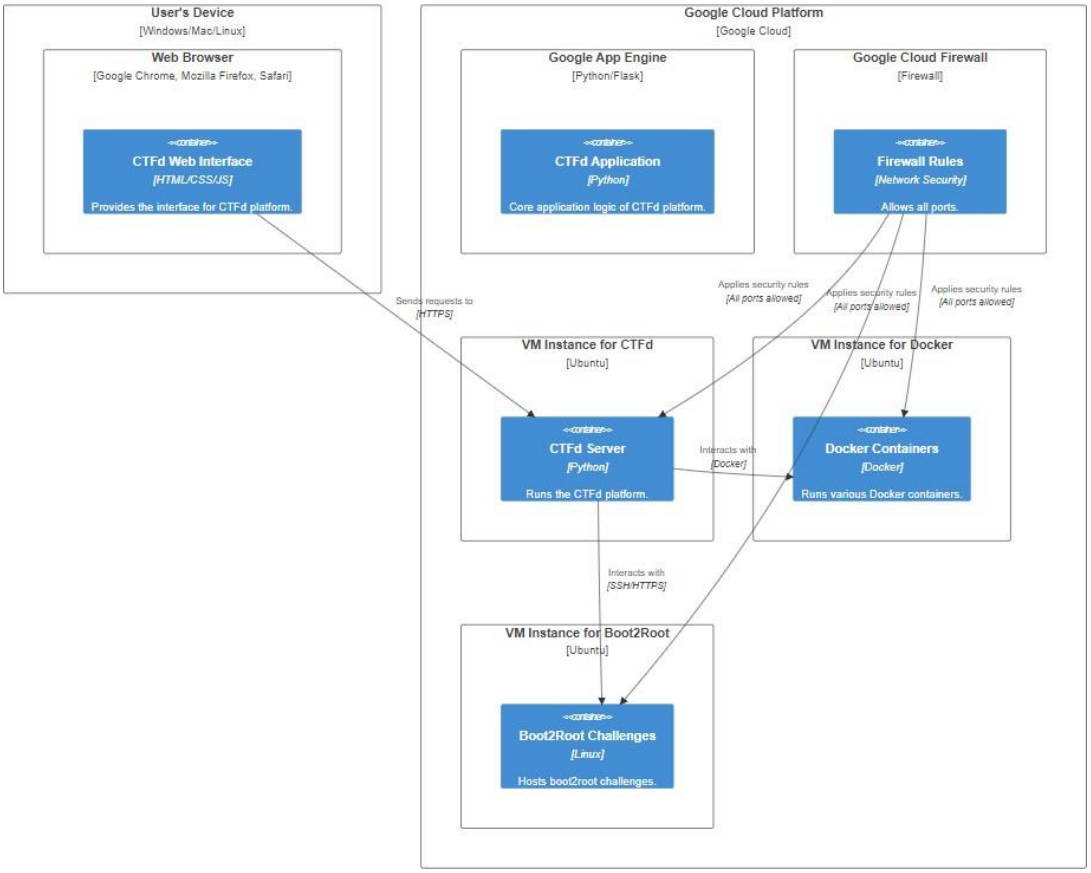


Figure 3.1.1.1 GCP Platform System Architecture Diagram

1) User's Device:

- Web Browser: Represents the end user's device (e.g., Windows, Mac, Linux) using a web browser like Google Chrome, Mozilla Firefox, or Safari to access the CTFd platform.
- CTFd Web Interface: This is the user-facing part of the CTFd platform, consisting of HTML, CSS, and JavaScript files. Users interact with this interface to solve challenges, manage accounts, and view scores.

2) Google Cloud Platform (GCP):

- Google App Engine: This is a managed platform service on GCP where the core CTFd application logic (written in Python using the Flask framework) is hosted.

App Engine automatically handles scaling, load balancing, and other infrastructure concerns.

- Google Cloud Firewall: A firewall that allows or restricts network traffic to and from the VM instances. In this scenario, it is configured to allow all ports to the VM instances. This setup ensures that the CTFd platform and related services can communicate without port restrictions, which might be necessary for the different challenges hosted on the platform.

3) Virtual Machine Instances:

- VM Instance for CTFd:
  - CTFd Server: A dedicated VM running the CTFd platform, responsible for managing the core functions, including challenge management, scoring, and user authentication.
- VM Instance for Docker:
  - Docker Containers: This VM runs various Docker containers that might host different services or microservices required by the CTFd platform, such as databases, auxiliary services, or even challenge environments.
- VM Instance for Boot2Root:
  - Boot2Root Challenges: A VM dedicated to hosting Boot2Root challenges, which are a specific type of security challenge where the goal is to gain root access to the system.

4) Relationships (Connections):

- CTFd Web Interface to CTFd Server: The user's browser sends HTTP/HTTPS requests to the CTFd server hosted on the VM. This interaction covers activities such as logging in, submitting flags, or viewing challenges.
- CTFd Server to Docker Containers: The CTFd server interacts with various Docker containers, possibly to execute certain services, run specific challenges, or manage microservices required by the platform.

- CTFd Server to Boot2Root Challenges: The CTFd server also communicates with the Boot2Root VM instance, likely to facilitate interactions between the platform and the challenges hosted on this VM.
- Google Cloud Firewall to VMs: The firewall applies security rules that allow traffic on all ports to the CTFd VM, Docker VM, and Boot2Root VM, ensuring no network traffic is blocked between these instances.

3.1.2 Boot2Root System Architecture Diagram

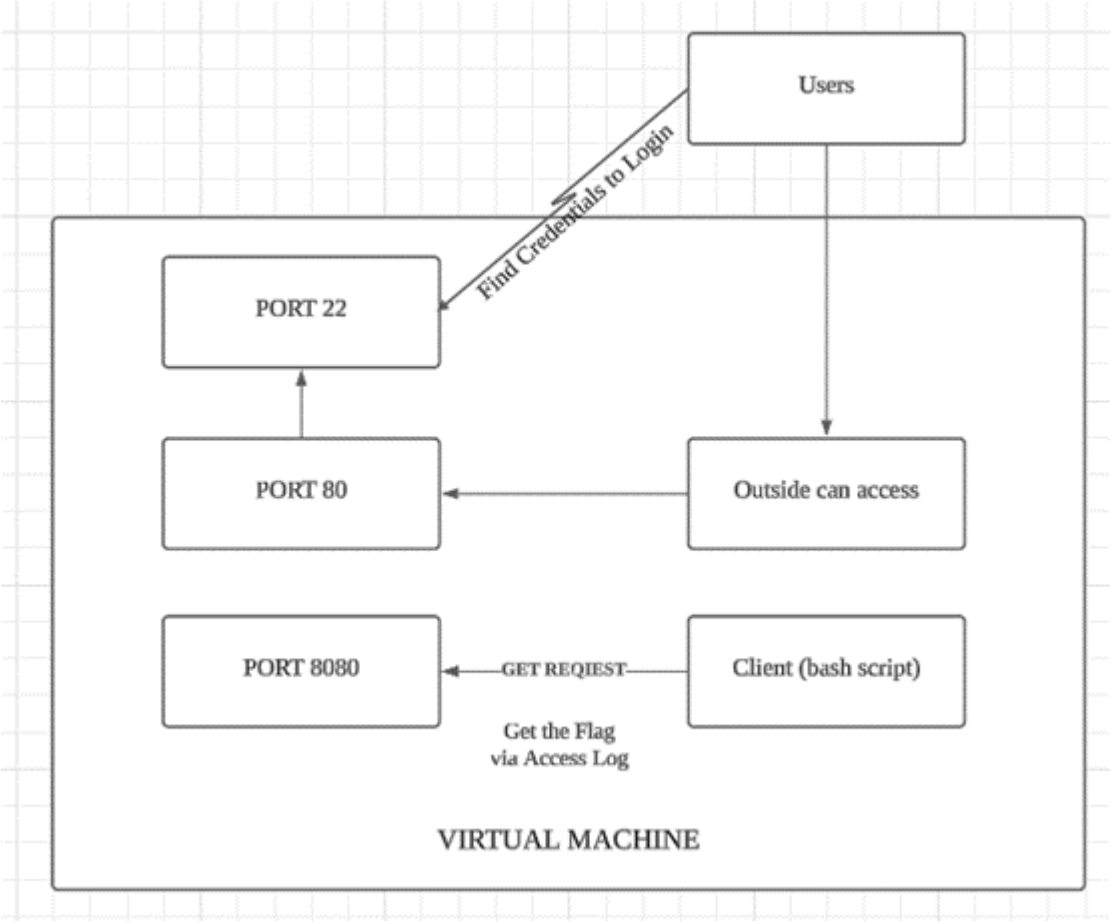


Figure 3.1.2.1 Boot2Root System Architecture Diagram

The system block diagram provided illustrates the architecture of a Boot2Root challenge, which involves a virtual machine with several open ports and services that participants must interact with to retrieve the flag. The challenge is structured to allow users to gain access by discovering login credentials and exploiting the system's services.

Components:

1. Virtual Machine (VM): The Boot2Root challenge is hosted on a virtual machine, which exposes multiple services via open ports. These ports represent different services that the user must interact with to progress in the challenge. The services are connected to facilitate various steps in the exploitation process, leading to the retrieval of the flag.

2. Users Participants begin by interacting with the virtual machine from an external environment. Their initial objective is to discover valid credentials that will allow them to log into the machine via one of the open ports. Users will use various tools and techniques to discover these credentials and proceed further into the system.

3. Port 22 (SSH): Port 22 is open for SSH access, but users must first find valid credentials to log in. This port allows secure access to the virtual machine, and gaining access to it is a crucial step in progressing through the challenge. The task likely involves discovering the login credentials through information leakage or other vulnerabilities.

4. Port 80 (HTTP Server): Port 80 runs a web service, which the outside world can access. The users can interact with the web service to gather information, such as web pages or logs, that might help them find the necessary credentials for SSH access or other services. It is common for challenges to include vulnerable web applications or misconfigurations that reveal sensitive information or allow for further exploitation.

5. Port 8080 (Web Service for Flag Access): Port 8080 runs another web service, and the client communicates with it using a GET request to obtain the flag. The user need read to the access log to extract the flag.

6. Client (Bash Script): A bash script is used by challenge creator to send GET requests to the web service on port 8080 and it is used to retrieve the flag by accessing log files.

3.1.3 Use Case Diagram

The use case diagram for the functions and relationships in Figure 3.1.3.1 shows the function of the system of by differentiating between the capabilities given to the user / participants and the administrators / challenge creators. Users interact with the platform through several key activities. They have access to the learning materials on what is required knowledge for the challenges ahead of them. They will be able to download the challenge files when they are ready which contains all the challenges that need to be solved. In the process, the users can monitor their performance by viewing the leaderboards. On the other hand, the administrators or challenge creator design and upload new challenges to the platform. They ensure the content remains fresh and engaging through the ability to update existing challenges. Besides creating the challenges, they are also able to configure the platform by tailoring the platform to the evolving needs of the users and just like user, they can view the leaderboard.

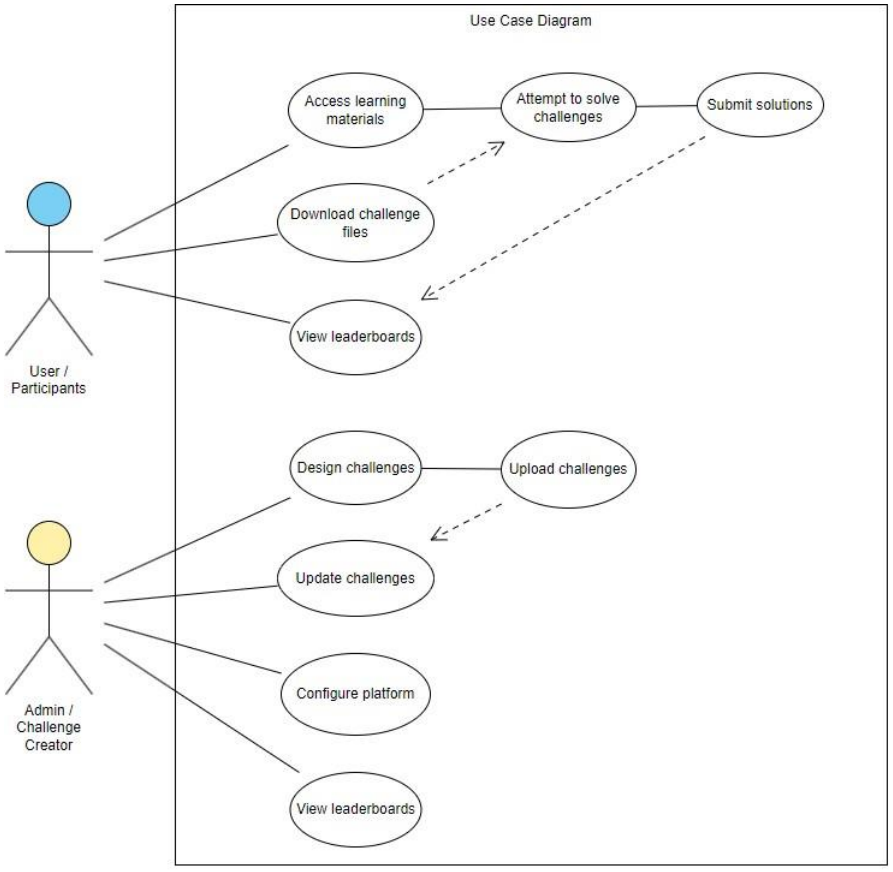


Figure 3.1.3.1 Use Case Diagram

CHAPTER 4

System Design

4.1. System Block Diagram

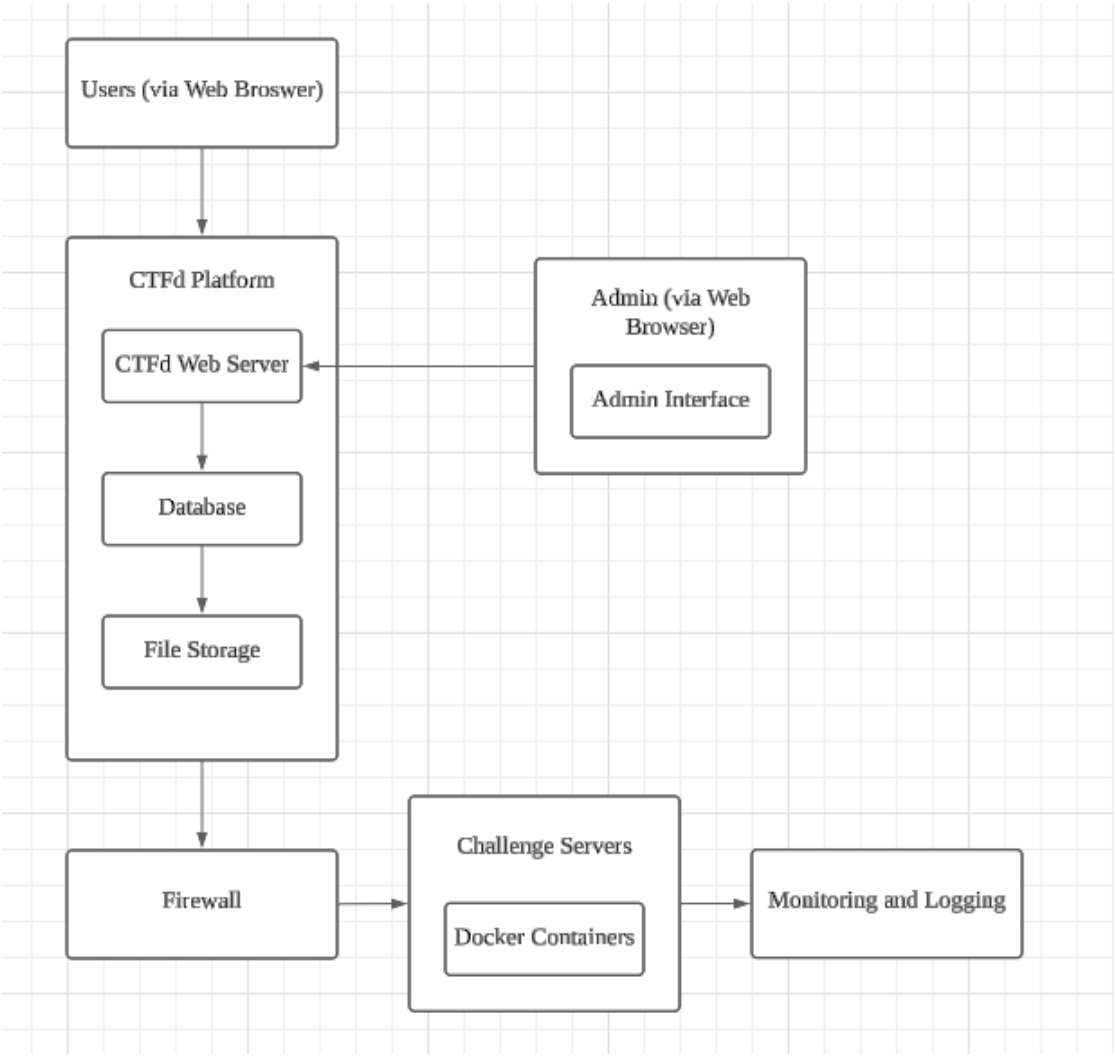


Figure 4.1.1 CTFd System Block Diagram

1) Users

The users are the participants in the CTF competition. The users can interact with the CTFd platform using a standard web browser. They register, log in, view challenges and submit flags through the web interface. For certain types of challenges, particularly "pwn" challenges, users may need to connect directly to a server via a command-line tool like netcat. This allows them to interact with the challenge environment, which might involve exploiting a vulnerability in a running service.

2) CTFd Platform

The heart of the CTFd platform is composed of several key components: the web server, the database, and the file storage system. The CTFd web server hosts the application and serves the user interface, handling all HTTP/HTTPS requests from users. This includes user authentication, challenge management and flag submission. The database is crucial for storing all the data related to the platform such as user information, challenge details and scores. This ensures that all participant progress is accurately tracked and displayed. The file storage system complements this setup by holding any files that users may need to download as part of the challenges, such as binaries or scripts, which are essential for solving the tasks.

3) Firewall

To ensure that the platform can handle the potentially high volume of traffic during a competition and remain secure, a firewall and load balancer are implemented as part of the network infrastructure. The firewall protects the platform by filtering incoming and outgoing traffic according to predefined security rules, which helps prevent unauthorized access and potential attacks.

4) Challenge servers

The actual challenges especially those requiring advanced exploitation techniques are hosted on separate challenge servers. These servers are often isolated within Docker containers, which provide a lightweight and secure environment for each challenge. By using Docker containers, each challenge runs independently, which not only enhances security by isolating each environment but also simplifies deployment and management. The containers ensure that any unintended behavior such as an exploit, is confined within a controlled environment to reduce the risk of affecting other parts of the system.

5) Admin

Administrators play a crucial role in maintaining and managing the CTFd platform. They access the system through a dedicated admin interface, which is a web-based tool that allows them to create, modify and manage challenges, monitor user activity and configure system settings. This interface provides administrators with the ability to oversee the entire platform to ensure that everything runs smoothly and that any issues

are promptly addressed. Through the admin interface, administrators also have access to logs and monitoring tools, which help them track system performance and identify potential problems.

6) Monitoring and Logging

The architecture includes a comprehensive monitoring and logging system. Monitoring tools continuously check the performance and availability of the CTFd platform and challenge servers, providing real-time data that helps in maintaining the system's health. The logging system collects and stores logs from all components of the platform, including the web server, challenge servers, and user interactions. These logs are invaluable for security purposes, allowing administrators to detect and investigate suspicious activities, as well as for debugging and resolving any technical issues that arise during the competition.

4.2 System Framework

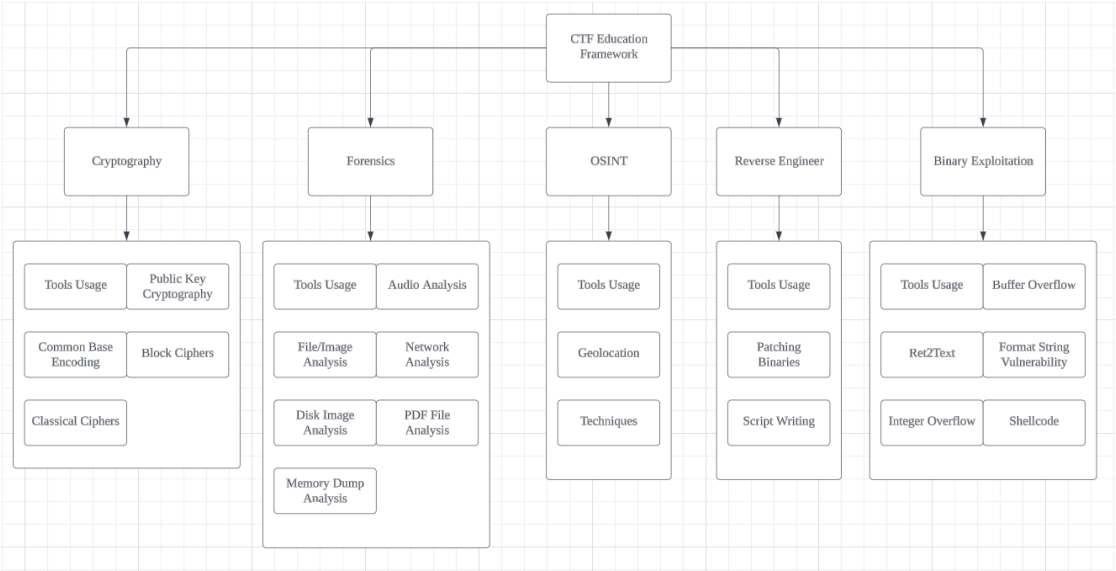


Figure 4.2.1 CTF Education Block Diagram

The CTF Education System Framework illustrated in the diagram outlines a comprehensive structure for teaching key cybersecurity concepts through CTF challenges. The framework is divided into several core categories, each of which targets specific areas of cybersecurity knowledge, allowing learners to build skills progressively in different domains.

1) Cryptography

The cryptography section provides foundational knowledge for understanding both classical and modern cryptographic techniques. The framework suggests focusing on tools usage for practical experience, which is essential for decoding and encoding messages. Key topics include Public Key Cryptography, Block Ciphers, and Common Base Encoding methods, such as base64 or hexadecimal. Additionally, Classical Ciphers are included to cover historical encryption techniques such as Caesar or Vigenère ciphers, which are often featured in beginner-level cryptography challenges. Together, these topics provide learners with the skills needed to recognize and break encryption schemes used in CTF challenges.

2) Forensics

Forensics in CTF involves analyzing digital artifacts to uncover hidden data or understand how an attack occurred. The framework emphasizes using tools to analyze different types of digital files. Subtopics in this section include File/Image Analysis, Disk Image Analysis, Memory Dump Analysis, and PDF File Analysis, covering a wide range of forensic investigation techniques. Additionally, Network Analysis and Audio Analysis provide learners with the skills to dissect network traffic and audio files, often used in forensic CTF challenges to hide or transmit data covertly.

3) OSINT (Open-Source Intelligence)

The OSINT category equips learners with skills to gather publicly available information for security-related tasks. This section focuses on Tools Usage, which is key in OSINT challenges to automate information gathering and reconnaissance. Geolocation and Techniques for gathering open-source intelligence are also covered, providing learners with the ability to track locations, analyze metadata, and find relevant information using publicly accessible resources. OSINT challenges often revolve around social media data, public records, or other internet-based resources, making these skills vital for success in the field.

4) Reverse Engineering

Reverse engineering plays a crucial role in cybersecurity by allowing learners to deconstruct binaries to understand how a program works. The reverse engineering section focuses on practical skill development through Tools Usage and Patching Binaries which is the process of modifying binaries to change their behavior or fix vulnerabilities. Learners will also explore Script Writing, which is often necessary for automating repetitive tasks when reversing binaries. By mastering these skills, participants will be able to analyze software and identify weaknesses, which is a common task in reverse engineering CTF challenges.

5) Binary Exploitation (PWN)

Binary exploitation is one of the most challenging but rewarding areas in CTF competitions. The framework outlines several crucial exploitation techniques, starting

with Tools Usage for debugging and analyzing binaries. Participants will also learn about specific attack vectors such as Buffer Overflows, Integer Overflows, Format String Vulnerabilities, and Shellcode, which are fundamental in crafting exploits. Advanced topics include Ret2Text (Return-to-text attack) for exploiting memory vulnerabilities. Mastery in these areas equips learners with the knowledge to exploit security flaws in binaries which is a core skill required for success in advanced PWN challenges.

CHAPTER 5

System Implementation

This section focuses on the software setup details, providing comprehensive guidelines for system implementation. All these contribute critically to giving the detailed steps of development, hence fostering a deeper understanding of the development of the system. In this, there is an intention to afford the reader the basic knowledge he needs to be able to replicate or understand the complexity and functionality of the system, hence bringing out its operational framework and considerations made during the design phase.

5.1 System Requirement

5.1.1 Hardware

The hardware involved in this project is a laptop. A laptop is crucial for the research and development of the platform. For example, the laptop is utilized for the design, coding, testing and development of the platform.

Table 5.1.1.1 Specifications of laptop

Description	Specifications
Model	HP Victus 15
Processor	AMD Ryzen 5600H
Operating System	Windows 11
Graphic	AMD Radeon RX 6500M (4GB GDDR6)
Memory	16 DB DDR4 3200 MHz RAM (2 x 8 GB)
Storage	512 GB SSD

5.1.2 Software

According to [13], the author stated that Oracle VM VirtualBox is formerly known as Sun VirtualBox, and it is a hypervisor for x86 computers developed by Oracle Corporation. It allows users to run multiple operating systems simultaneously on a single physical machine, facilitating the testing, development, demo, and deployment of applications across different environments without the need for multiple physical machines. VirtualBox supports Windows, macOS, Linux, and Oracle Solaris as host operating systems, offering a versatile solution for IT professionals looking to learn new technologies or simulate network environments for testing purposes. The utilization of Oracle VM VirtualBox enables the deployment of an Ubuntu virtual machine, specifically the 22.04.4 version which acts as the primary operating environment for the project. The choice of Ubuntu is due to it being open source and it offers a stable and user-friendly Linux distribution that is well-suited for both development and cybersecurity tasks.

Additionally, front-end languages such as HTML, CSS and JavaScript is utilized for the development of the platform. Besides, the C programming language is employed for the creation of reverse engineering and binary exploitation challenges. After challenge creation is completed, Ghidra and GNU Debugger (which allows us to know what the program is doing when it crashed) enhanced with the pwn-dbg plugin is incorporated to ensure that the challenges to prevent the challenges being unsolvable. As mentioned by Rohleder [14], Ghidra was originally a software reverse engineering framework by and for the NSA and it was made public on March 5, 2019 while giving a presentation at the RSA conference. It was open sourced under a very permissive Apache v2 license. There were many tools and frameworks in terms of reverse engineering. However, what made Ghidra different is that it became the first one that could offer a reliable decompiler that would handle many architectures. Other features were that it was free and open-source software, designed for any platform, and had high customizability through a rich plug-in system. The project also integrates Python programming language due to its versatility and wide support for cybersecurity tools and libraries to solve some of the challenges that require scripting.

5.2 Setting up locally

5.2.1 Software setup

Before starting to develop the platform, there are **five** software needed to be installed and downloaded in the machine:

1. Oracle VM Virtual Box:
https://www.virtualbox.org/wiki/Downloads

2. Ubuntu 22.04.4 LTS:
https://ubuntu.com/download/desktop

3. CTFd Platform:
https://github.com/CTFd/CTFd

4. GNU Debugger (Pwndbg + GEF + Peda):
https://github.com/apogiatzis/gdb-peda-pwndbg-gef?source=post_page-----714d71bf36b8

5. Sublime Text or IDE that you prefer:
https://www.sublimetext.com/docs/linux_repositories.html

5.2.2 Software setup demonstration

Visit the official Ubuntu website and download the ISO image file for the Ubuntu 22.04.4 LTS version.

Figure 5.2.2.1: Download Ubuntu 22.04.4 LTS Version

After that installation has been completed, click on the "New" button to create a virtual machine.

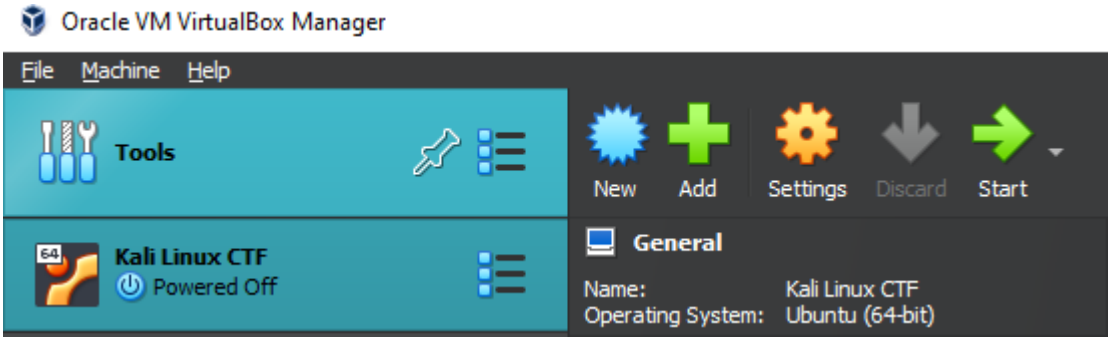


Figure 5.2.2.2: Creating a New Virtual Machine

For ISO Image, select the one that you had just downloaded from the official website.

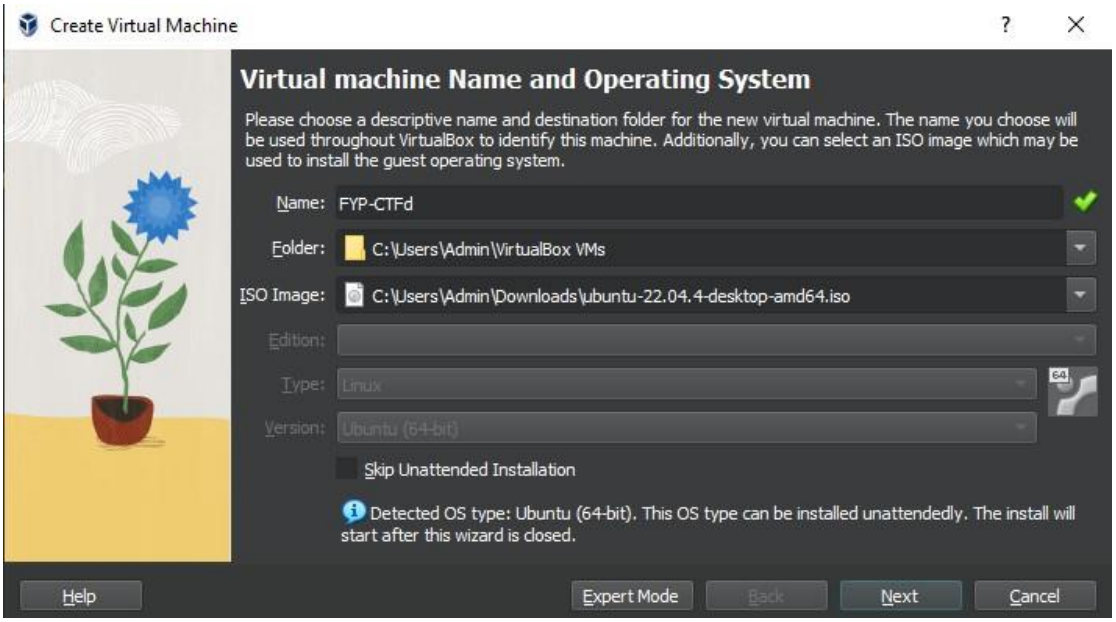


Figure 5.2.2.3: Create Virtual Machine Window

After that, user sets up an unattended guest OS by configuring the username, password and hostname.

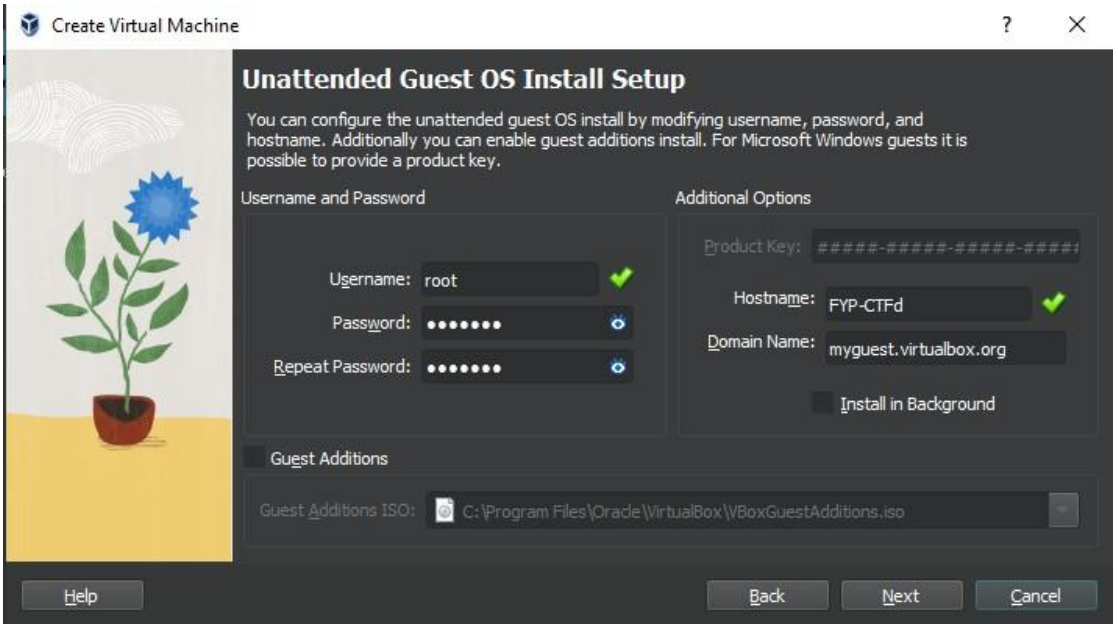


Figure 5. 5.2.2.4: Unattended Guest OS Setup

For optimal performance, allocate 4096 MB of base memory and configure the virtual machine to use 2 processors.

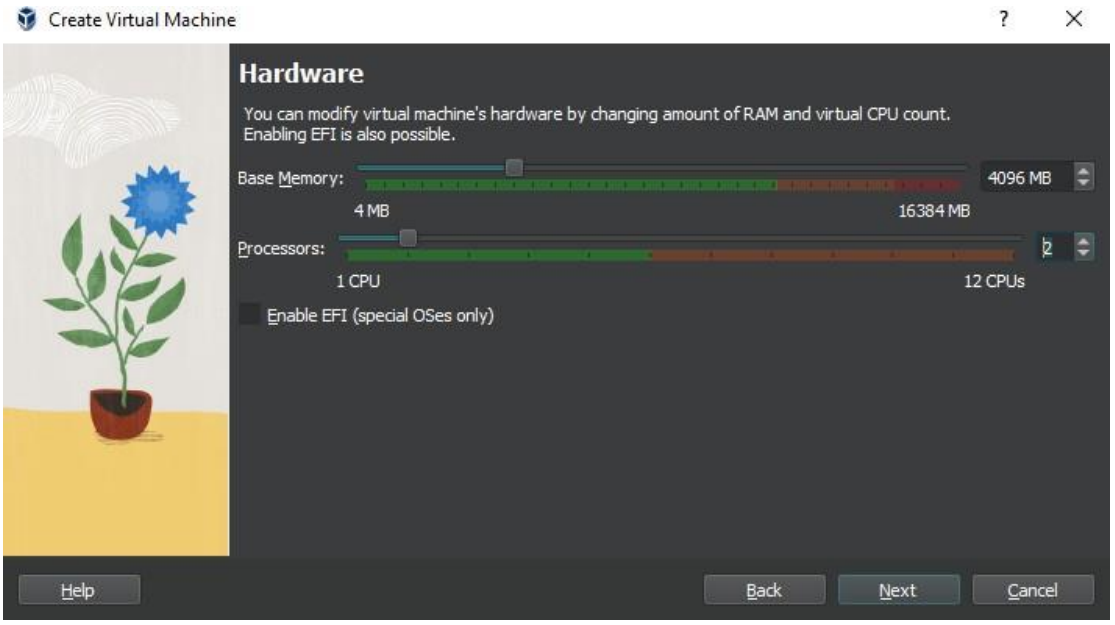


Figure 5.2.2.5: Hardware for Virtual Machine

For the virtual hard disk, we can leave it as default which is 25 GB.

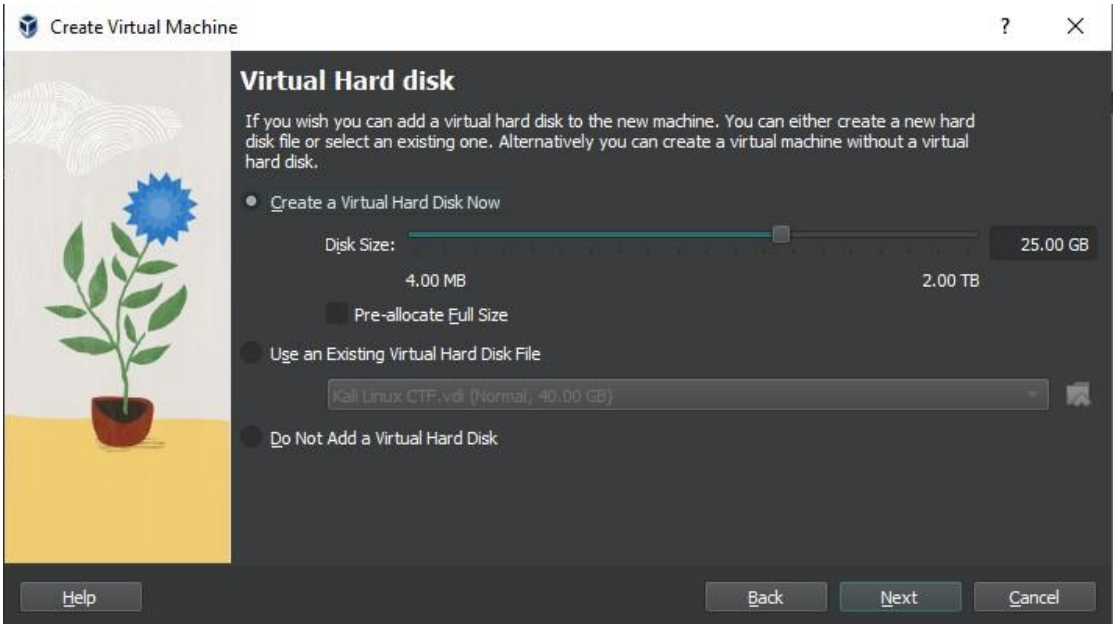


Figure 5.2.2.6: Creating Virtual Hard Disk

Figure 4.7 presents the summary of the virtual machine settings which allow users to confirm the configuration details such as machine name, memory allocation, processor count and OS specifications before finalization.

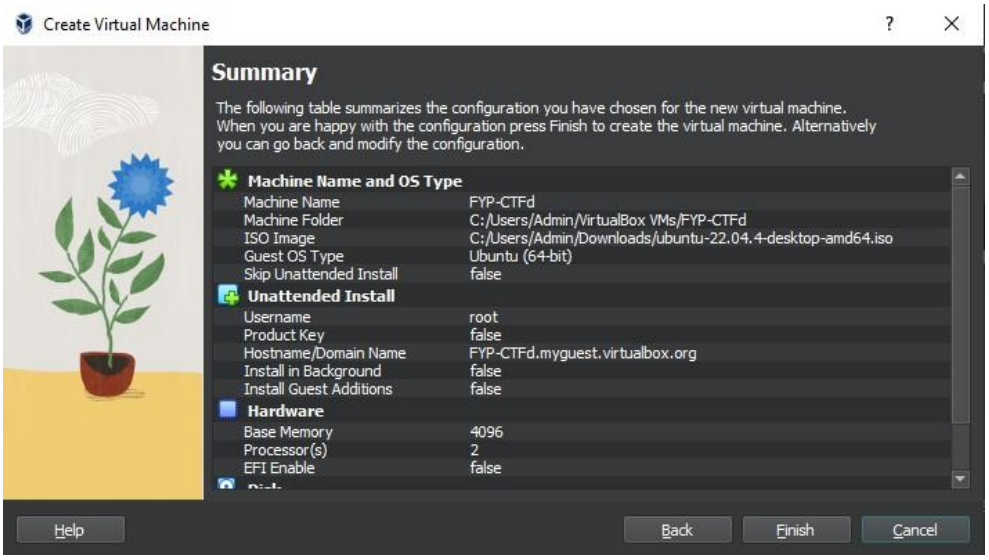


Figure 5.2.2.7: Summary of the Virtual Machine

Upon completion of the configuration summary, the virtual machine will run automatically and proceed with the installation process while prompting the user to enter their credentials to log in to the Ubuntu.

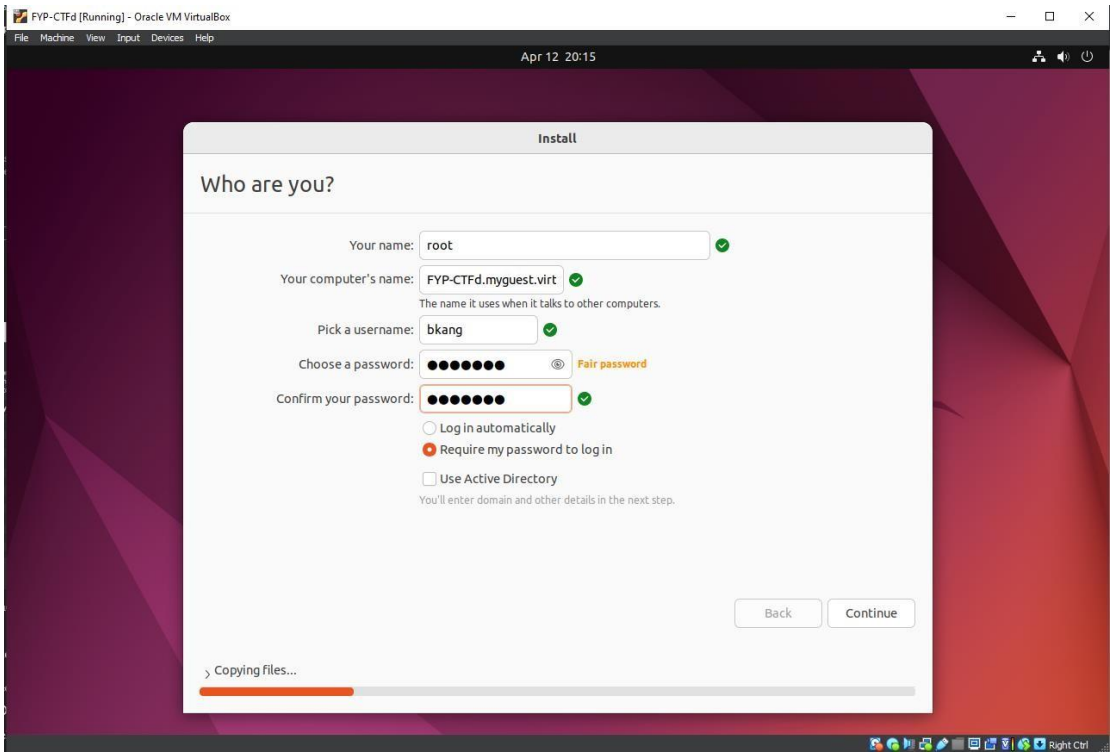


Figure 5.2.2.8: Setting Username and Password for Ubuntu

Next, open the terminal and type the following commands to enable root access for your username.

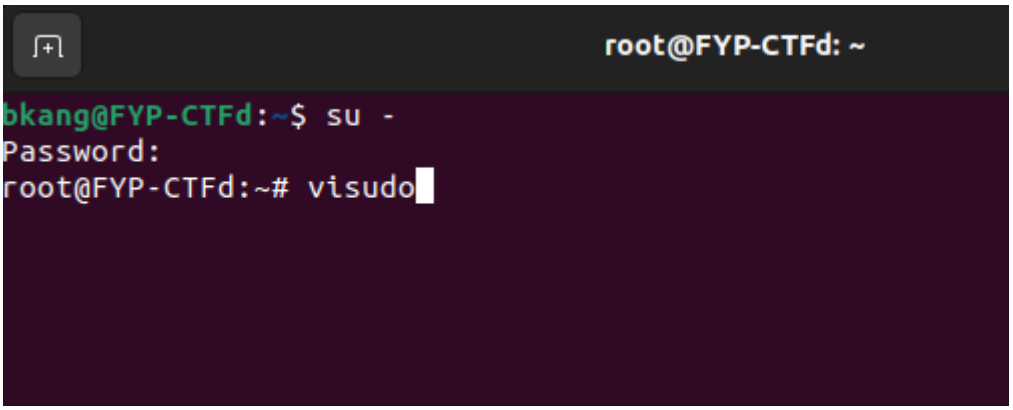


Figure 5.2.2.9: Enable root access

Scroll down to the section labeled "# User privilege specification" and input the following line, replacing <your username> with your chosen username: <your username> ALL=(ALL:ALL) ALL. This grants the user full administrative privileges.

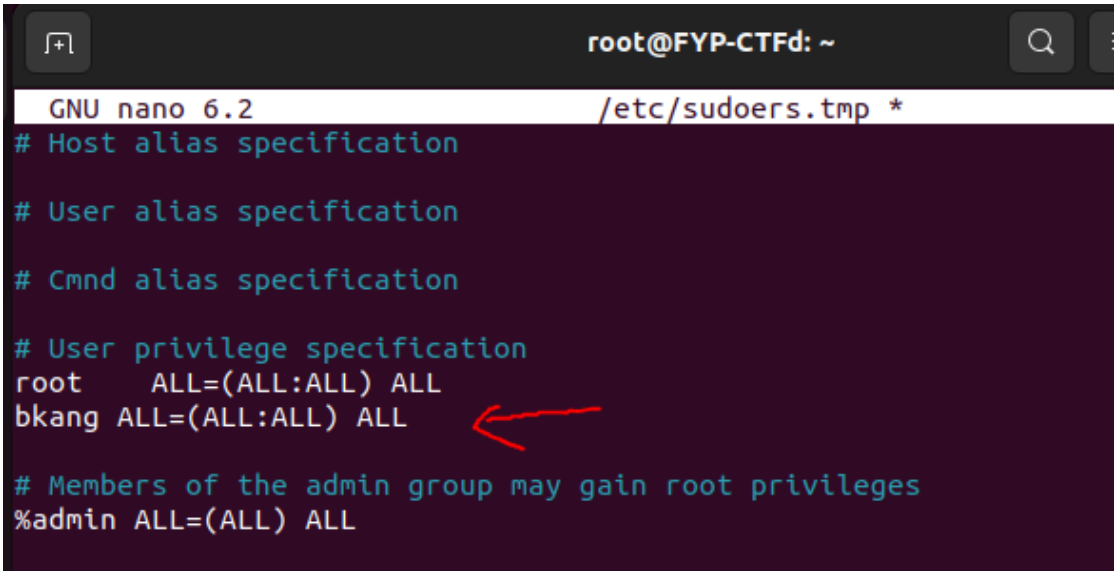


Figure 5.2.2.10: Allow default username to have root access

5.2.3 CTFd Platform Installation

First, type the following command to update available packages.

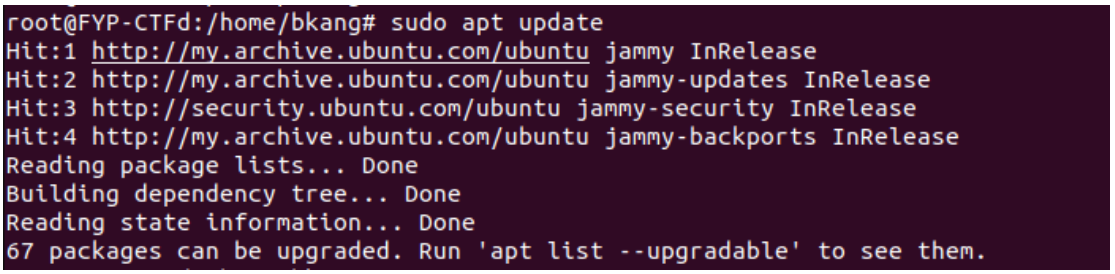


Figure 5.2.3.1: Update available packages

Install net-tools to enable network interface management.

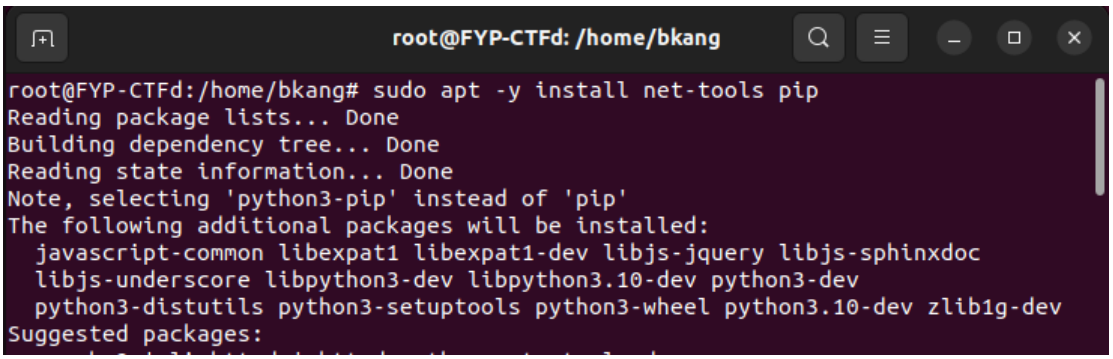


Figure 5.2.3.2: Installing net-tools

After that, install docker-compose by typing the following command. Docker-compose is a tool for defining and running multi-container Docker applications.

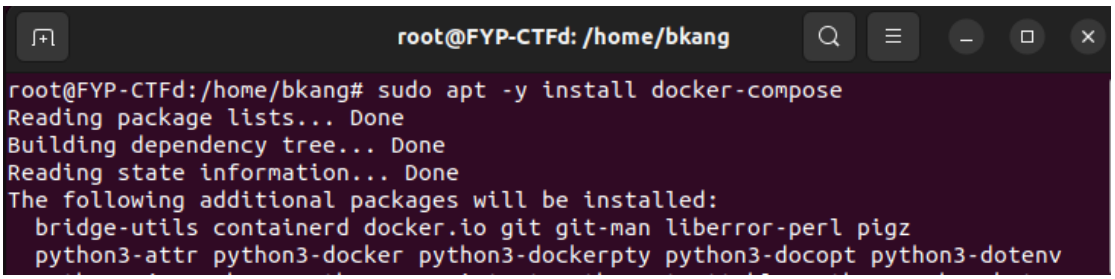


Figure 5.2.3.3: Installing docker-compose

Install CTFd platform via “git clone” to retrieve the latest version of the platform directly from the repository to ensure we have all the necessary files to deploy a CTF environment.

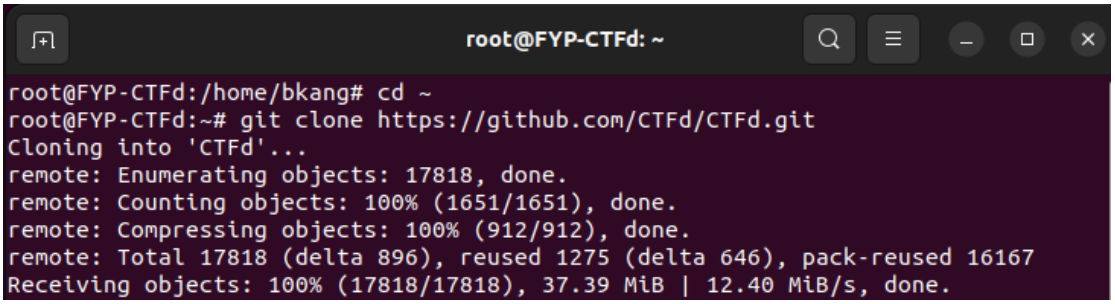


Figure 5.2.3.4: Installing CTFd platform

After the installation is completed, enter the prescribed commands as shown in Figure 5.2.3.5 to run CTFd.

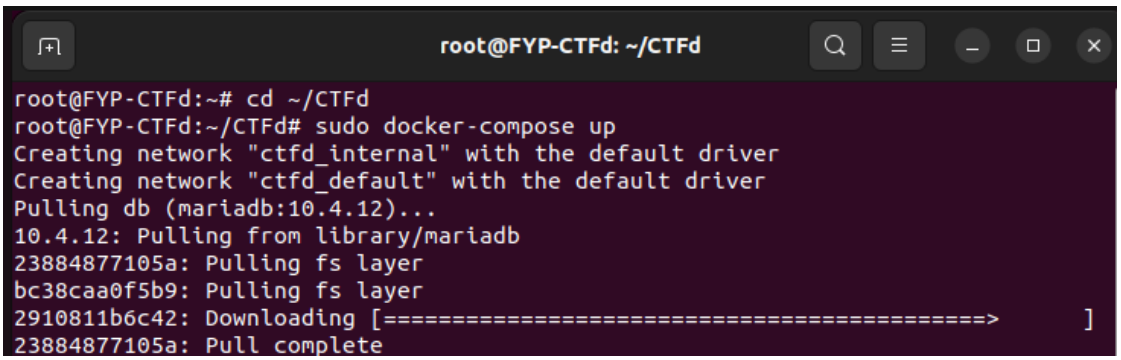


Figure 5.2.3.5: Run CTFd

After executing the commands, the service will start and we should be able to access the local host with the specific details highlighted in Figure 5.2.3.6.

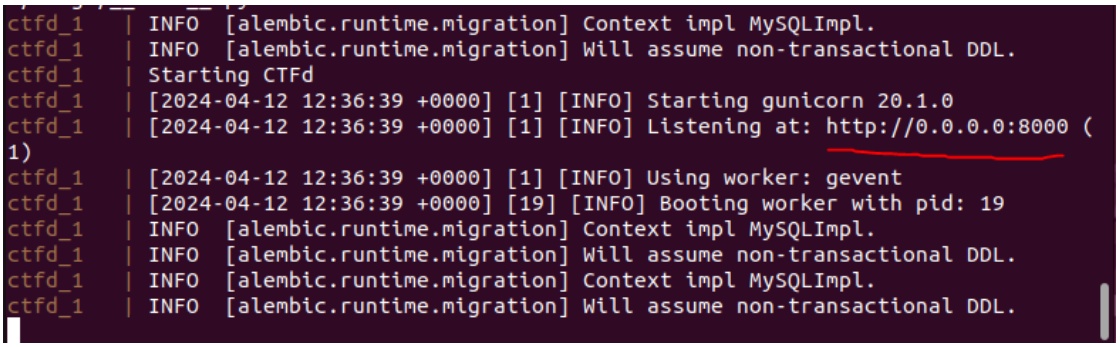


Figure 5.2.3.6: Localhost IP for CTFd

After launching CTFd in the local host, we will be greeted with the setup page. Fill in the details and press “Next” until we reached the end of the setup page. With that, the CTFd installation is completed.

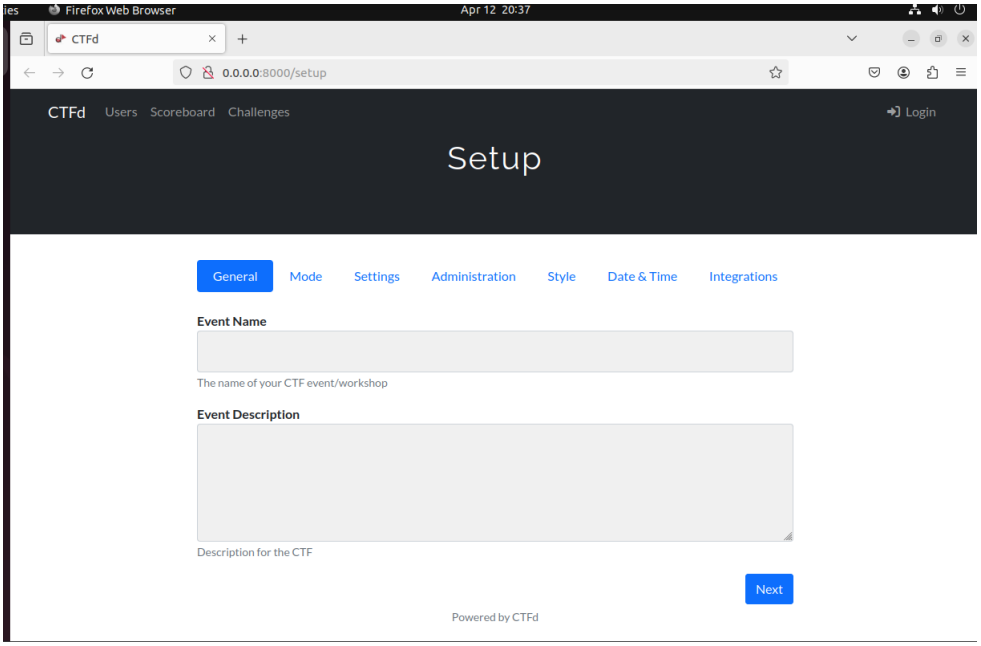


Figure 5.2.3.7: CTFd Setup Page

To stop the CTFd, hit “Ctrl + C” and wait for the processes to stop.

```
ctfd_1    | 172.19.0.1 - - [12/Apr/2024:12:37:29 +0000] "GET /themes/core-beta/static/
img/favicon.ico?d=2c4c045e HTTP/1.1" 200 0 "http://0.0.0.0:8000/setup" "Mozilla/5.0 (
X11; Ubuntu; Linux x86_64; rv:123.0) Gecko/20100101 Firefox/123.0"
^CGracefully stopping... (press Ctrl+C again to force)
Stopping ctfd_nginx_1 ... done
Stopping ctfd_ctfd_1  ... done
Stopping ctfd_db_1    ... done
Stopping ctfd_cache_1 ... done
root@FYP-CTFd:~/CTFd#
```

Figure 5.2.3.8: Stopping CTFd

To start CTFd again, type the following command as shown in Figure 5.2.3.9 and wait until it shows the localhost as highlighted in Figure 5.2.3.6.

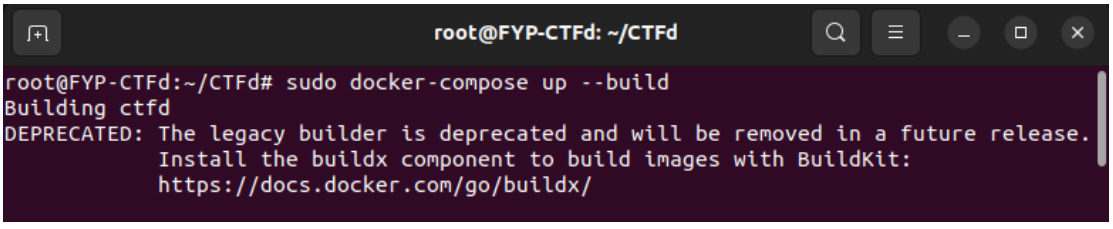


Figure 5.2.3.9: Starting CTFd

5.2.4 Sublime Text Installation

Follow the set of instructions to install Sublime Text through the apt repository as shown in Figure 5.2.4.1. It includes to commands for installing the GPG key while selecting the stable channel repository (recommended for general use) for the software and updating the apt sources, followed by the command to install Sublime Text.

Figure 5.2.4.1: Step by step installation for Sublime Text

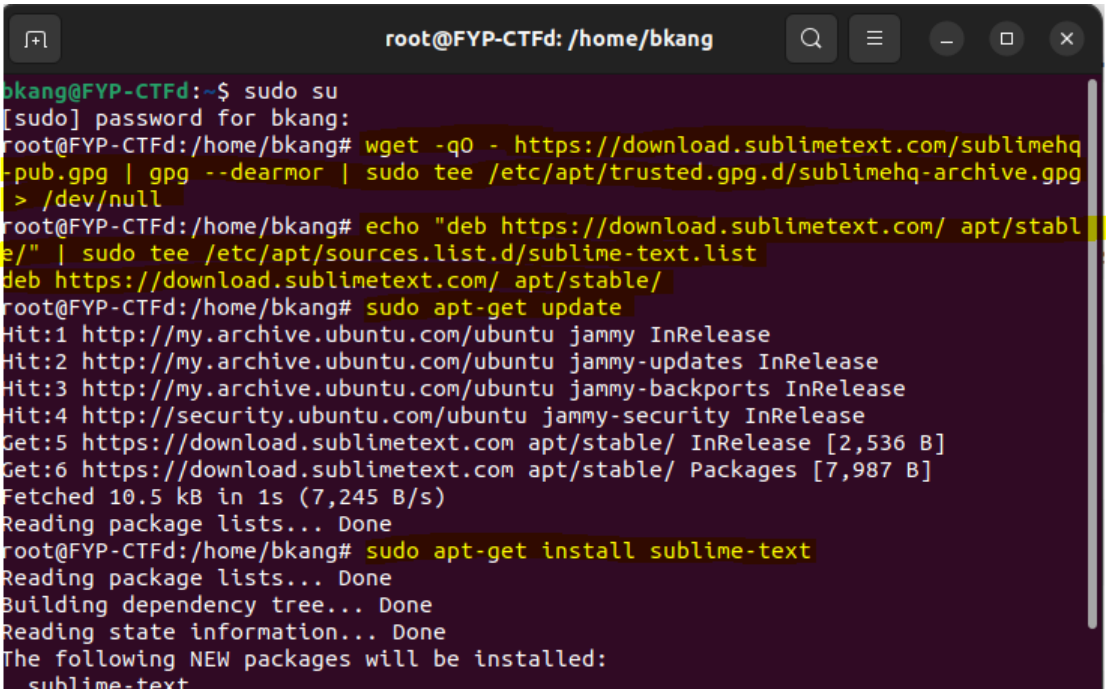


Figure 5.2.4.2: Copy the commands into the terminal

To run Sublime Text through the terminal, simply type “subl <file that we want to create>”. Example is shown in Figure 5.2.4.3, where we created a “test.txt” file.

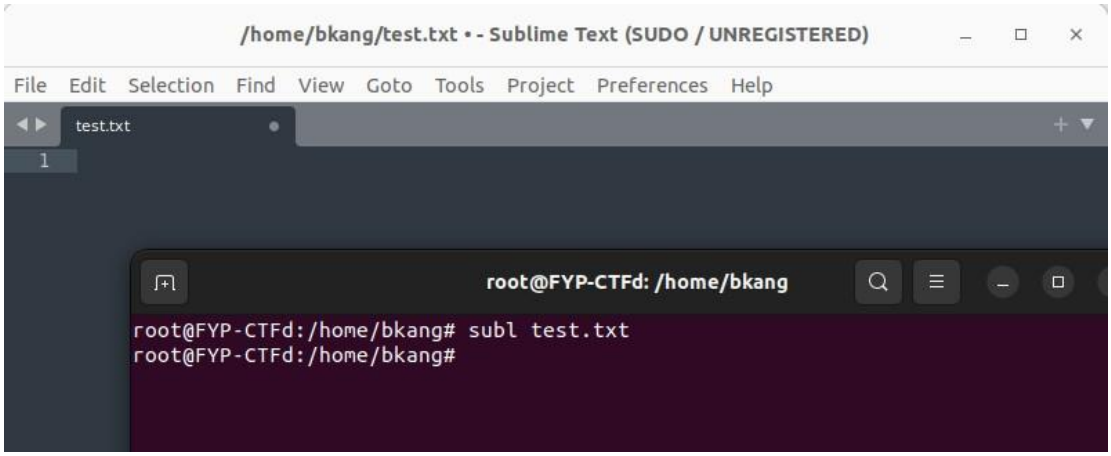


Figure 5.2.4.3: Running Sublime Text

5.2.5 GDB Plugins Installation

To install the GDB plugins including pwndbg, peda and gef, follow the installation instructions as shown in Figure 5.2.5.1.

Figure 5.2.5.1: Step by step installation for pwndbg, peda and gef

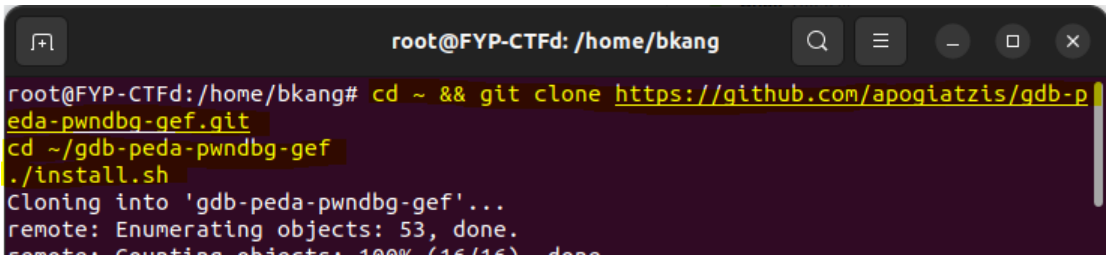


Figure 5.2.5.2: Copy the commands into the terminal

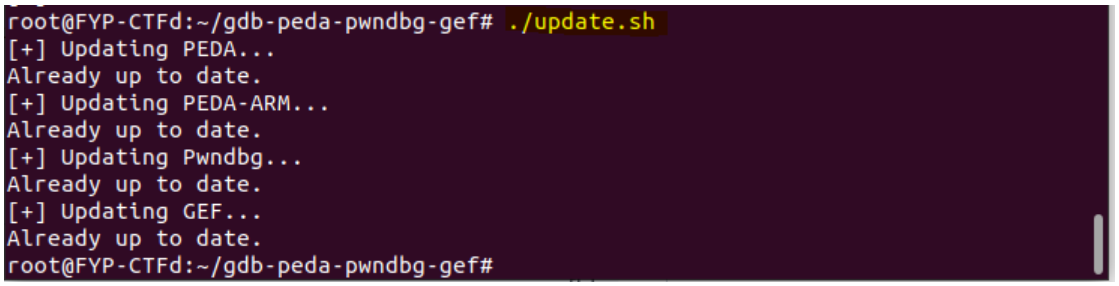


Figure 5.2.5.3: Copy the commands into the terminal

Pwndbg is an essential tool for debugging binary challenges on the platform. To verify its functionality, type “gdb-pwndbg” into the terminal and observe the output to ensure that it is operational. If everything is done correctly, we can see the output as shown in Figure 5.2.5.4.

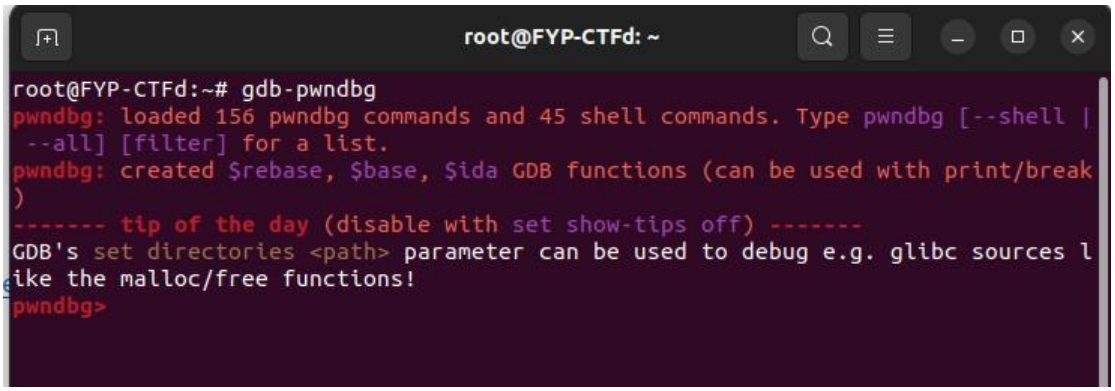


Figure 5.2.5.4: Testing pwndbg

5.3 Hosting CTFd via Google Cloud Platform

The platform that we chose to host the CTFd is via Google Cloud Platform (GCP). Hosting the CTF platform CTFd on GCP offers several advantages which makes it an ideal choice for both small-scale educational use and larger competitive events. One of the primary reasons for choosing GCP is the $300 in free credits provided to new users, which can significantly offset the initial hosting costs. This credit allows developers and educators to explore GCP's powerful features and deploy a fully functional CTFd instance without immediate financial commitment, making it an attractive option for budget-conscious projects.

Beyond the initial cost savings, GCP provides a highly scalable and flexible infrastructure, which is crucial for hosting CTFd. The platform’s ability to scale resources dynamically ensures that the CTF environment can handle varying loads, from a handful of users in a classroom setting to hundreds or thousands of participants during a large-scale competition. GCP's global network of data centers also enhances performance by reducing latency, offering participants a smooth and responsive experience no matter their geographic location. Additionally, GCP integrates seamlessly with various tools and services, such as Cloud SQL for database management and Cloud Storage for secure and efficient handling of challenge files, ensuring that the CTFd platform remains robust, secure, and easy to manage. The comprehensive security features of GCP, including advanced firewalls, DDoS protection, and encryption, further enhance the safety of the platform, protecting sensitive user data and maintaining the integrity of the competition. In this sub-section, we will be looking at the most important steps to host CTFd on GCP platform successfully.

First, go to the GCP website:

https://console.cloud.google.com/welcome/new?project=celtic-acumen-433519-n8

Next, go and create a VM in Compute Engine.

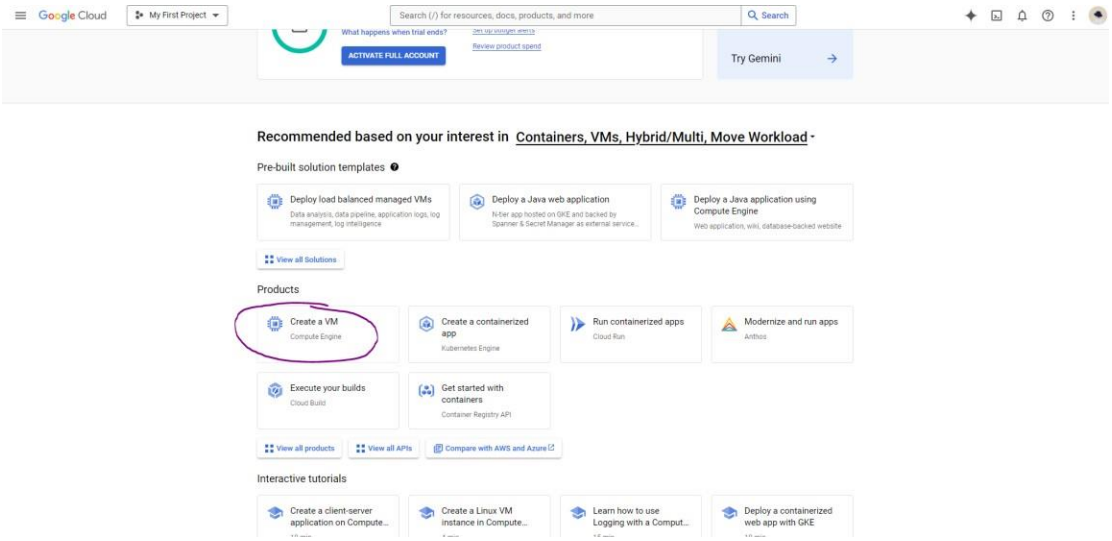


Figure 5.3.1: Create VM in Compute Engine

After that, create a VM instances.

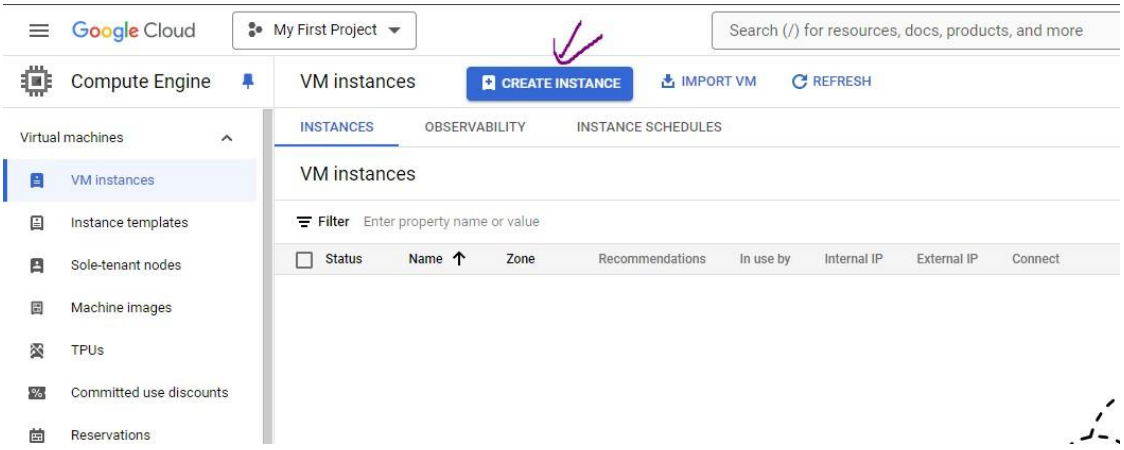


Figure 5.3.2: Create a VM instance

Next, set up the settings for the VM.

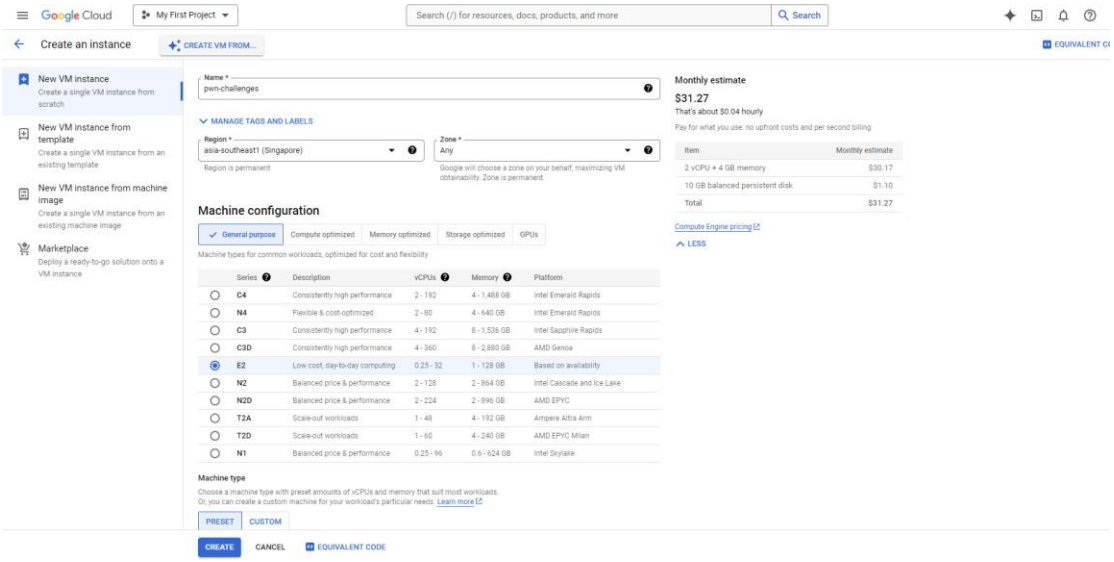


Figure 5.3.3: Setting up the configurations for the VM

Choose your preferred machine type. In this case, we will go for the default settings.

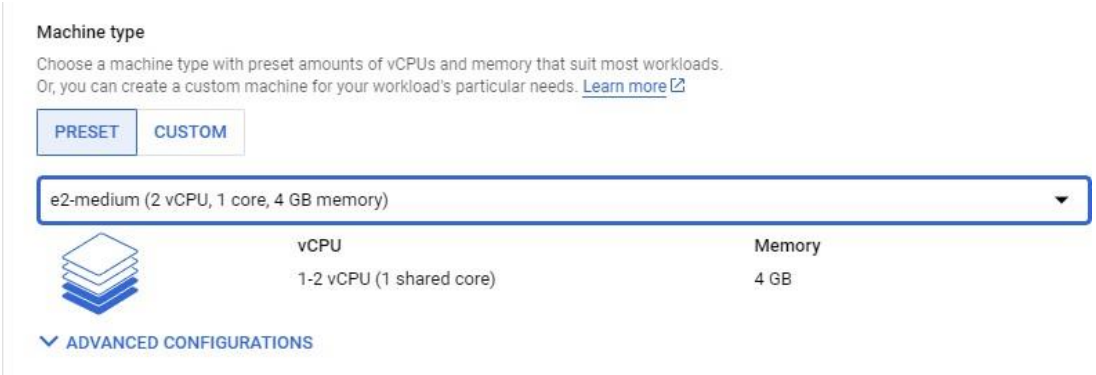


Figure 5.3.4: Choosing preferred machine type

It is recommended that we use Ubuntu version 22.04 or above otherwise there will be a lot of bugs.

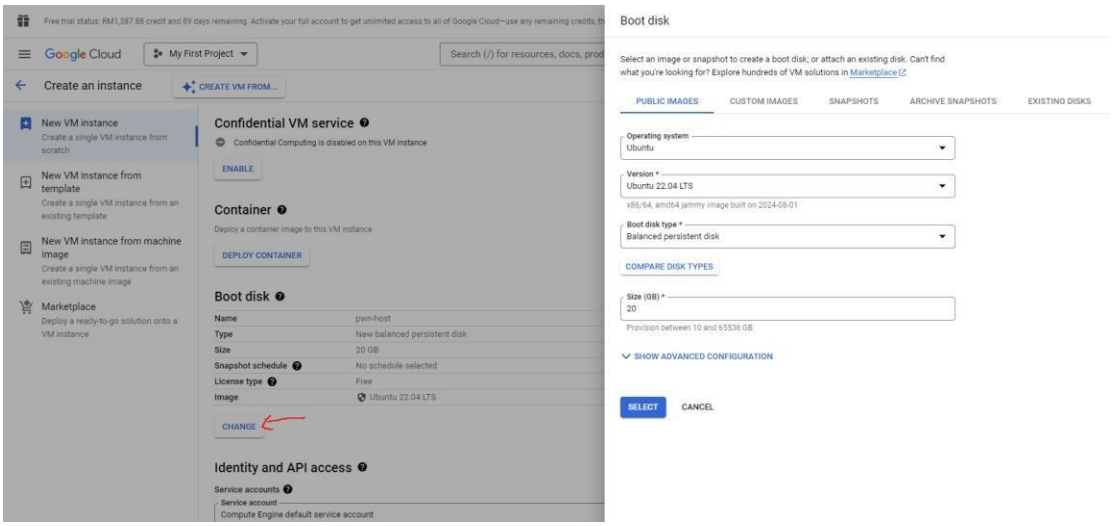


Figure 5.3.5: Choosing VM version

Set the Firewall, you may tick all three options. After that, hit the “CREATE” button to create a VM instance.

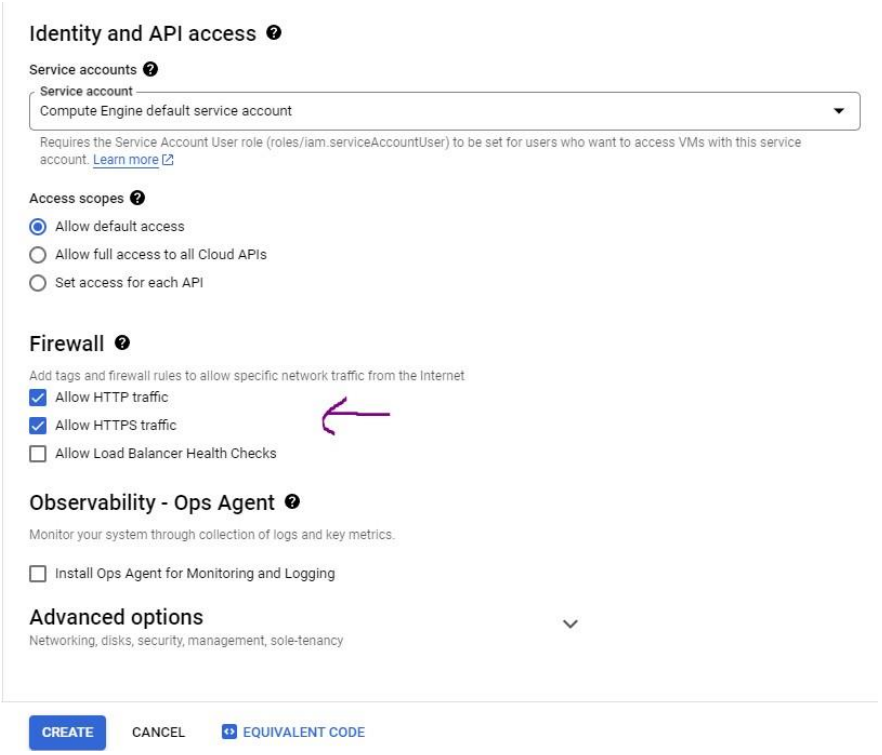


Figure 5.3.6: Setting up Firewall

Here, press on the “SSH” button to launch a SSH session in your browser.

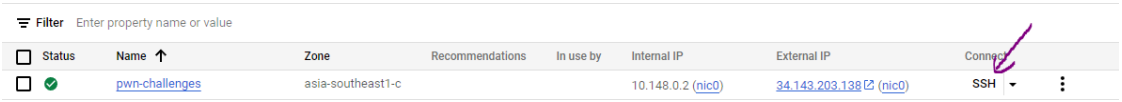


Figure 5.3.7: Clicking on SSH button

After that, type the following commands:

- sudo su
- cd
- nano /etc/ssh/sshd_config

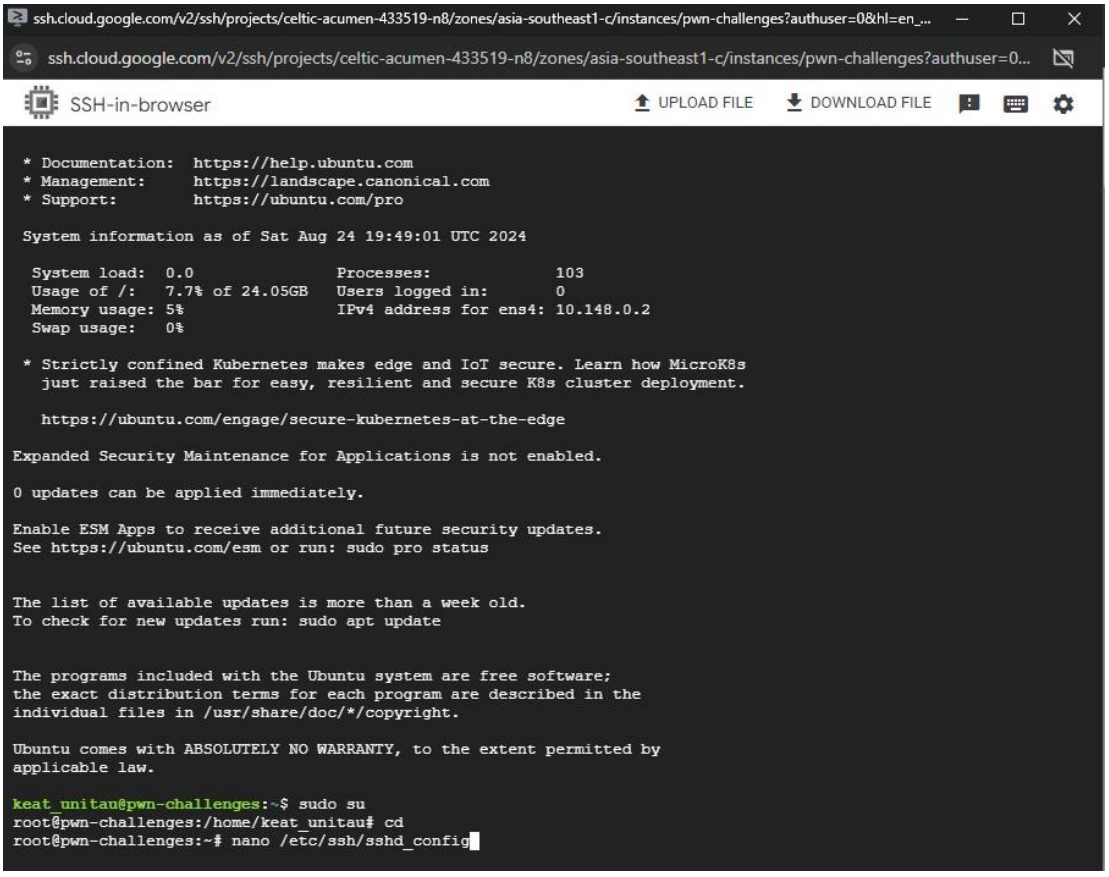


Figure 5.3.8: SSH browser interface

The most important part is here. Change the settings to “PermitRootLogin yes” and “PasswordAuthentication yes” .

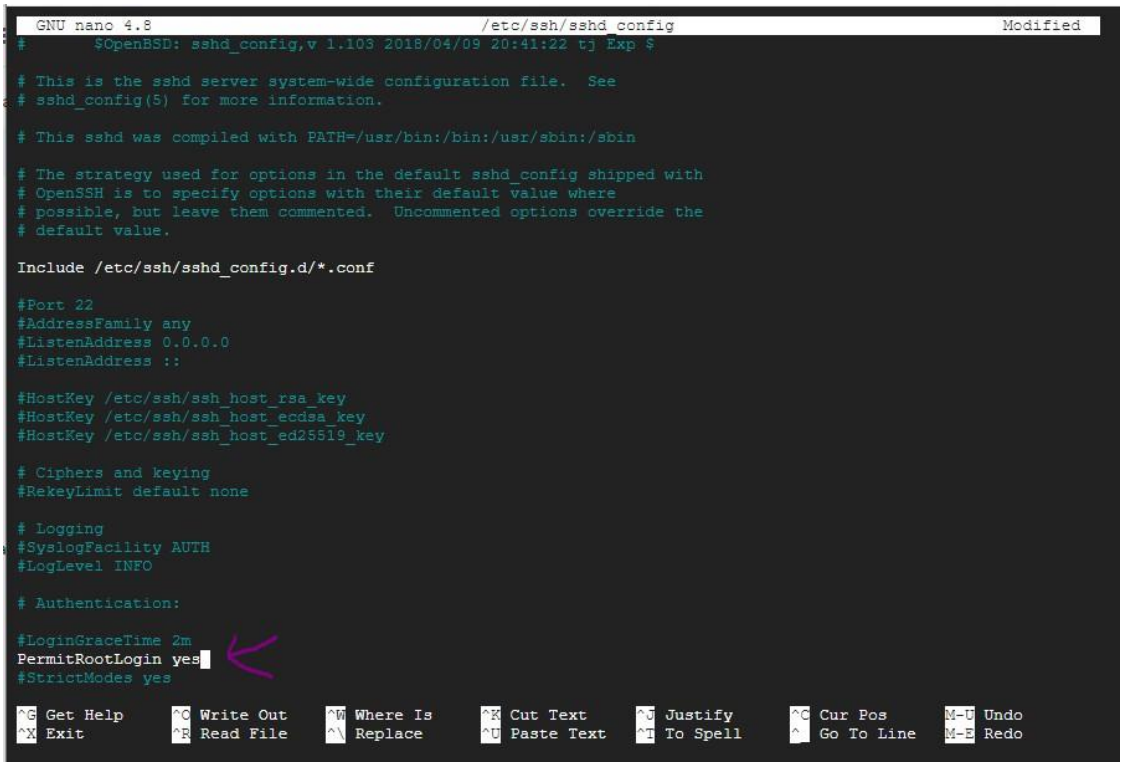


Figure 5.3.9: Changing PermitRootLogin

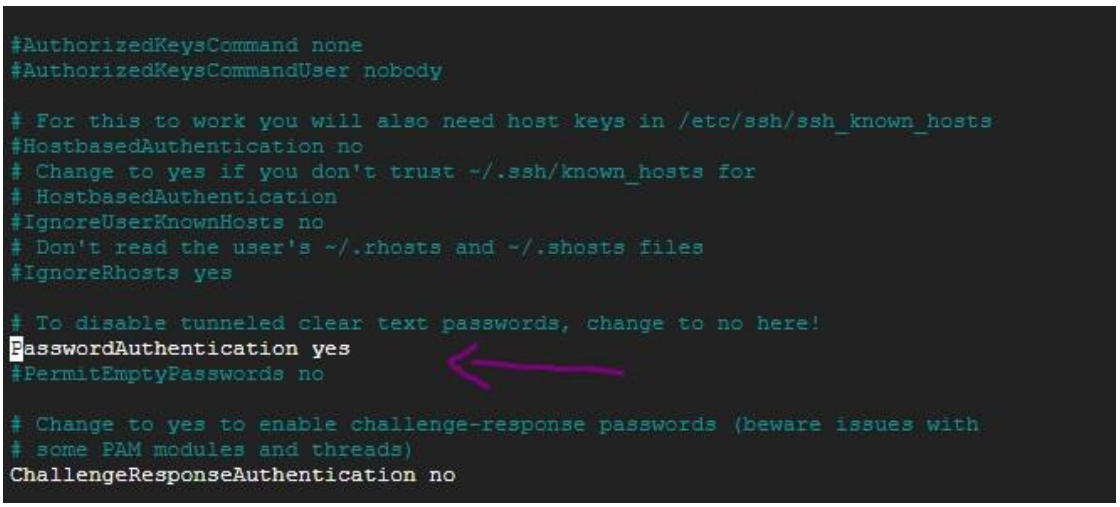


Figure 5.3.10: Changing PasswordAuthentication

Now, type the following:

- nano /etc/ssh/sshd_config
- systemctl restart sshd
- passwd

After that, enter your password and we should be good.

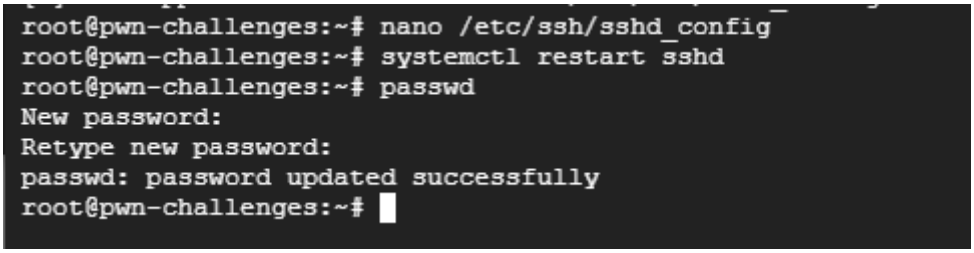


Figure 5.3.11: Changing SSH password

5.4 Common Errors

In case when you connect to the IP via your workstation, it shows “permission denied (publickey)”, do the following:

- ssh-keygen
- cd ~/.ssh
- cat the file that you just saved

Figure 5.4.1: Keygen

Next, click on your VM instance.

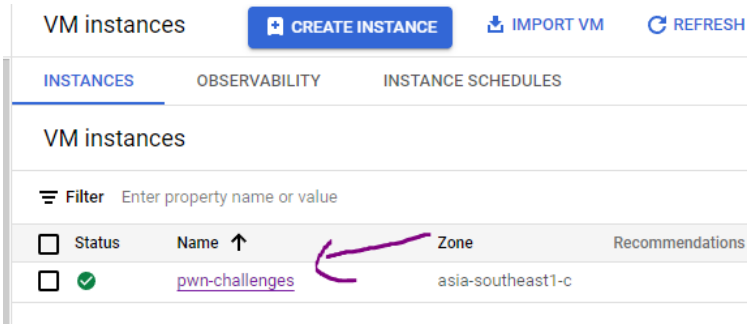


Figure 5.4.2: Click on VM instance

Click on Edit.

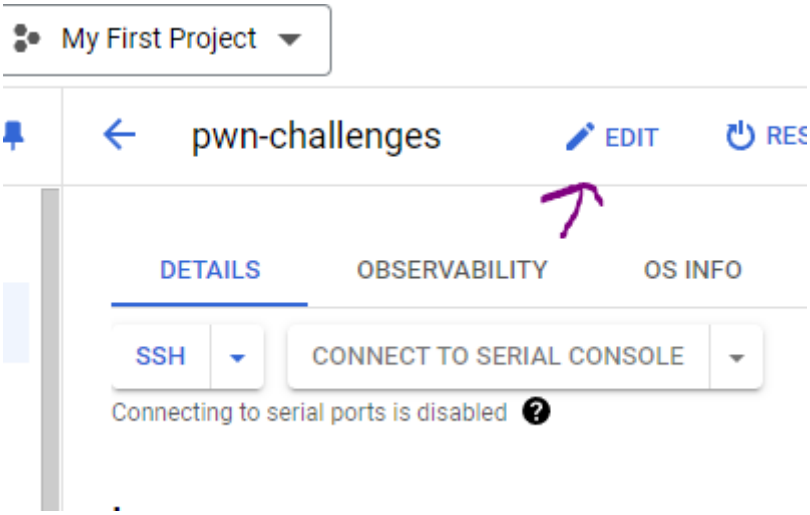


Figure 5.4.3: Editing VM instance

Scroll down until we see the “SSH Keys” option, click on “ADD ITEM” and paste in your SSH key in Figure 5.4.4.

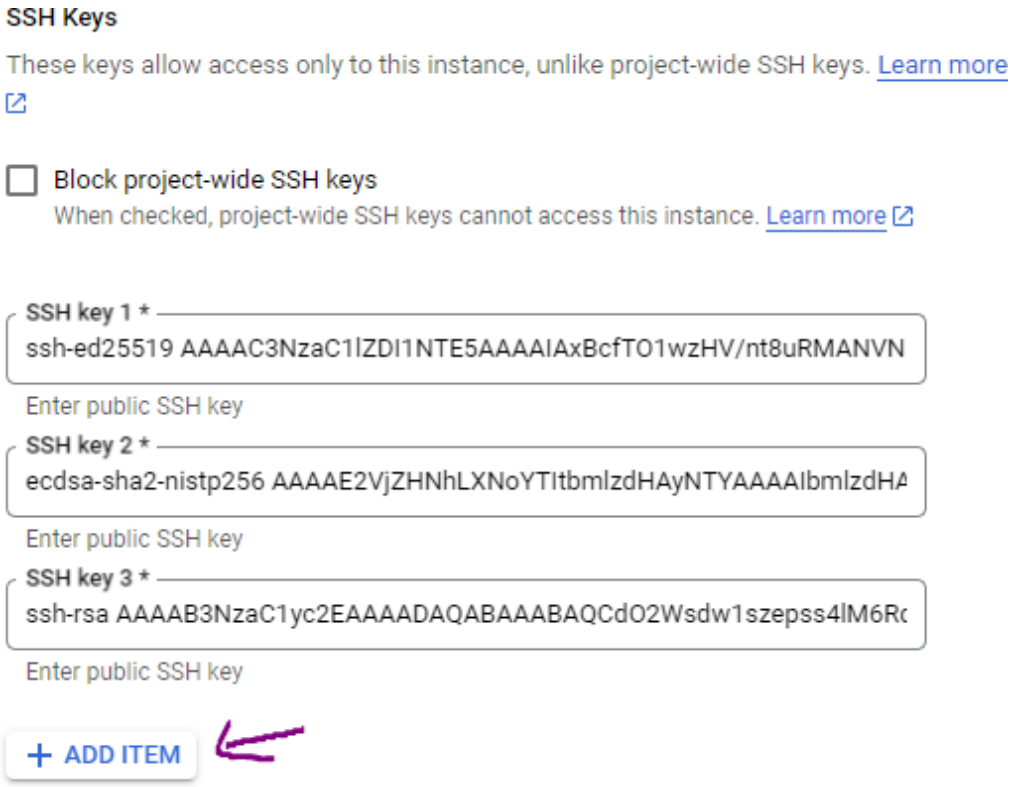


Figure 5.4.4: Adding SSH key

Now, try to connect again via ssh in your workstation. It should be working now.

5.4.1 Disabling Public Key Authentication

In case you want to disable public key authentication, do the following steps, otherwise we can skip this part:

- enable root on your VM instance
- nano /etc/ssh/sshd_config
- Go to the line “PubKeyAuthentication” and change to “PubKeyAuthentication no”

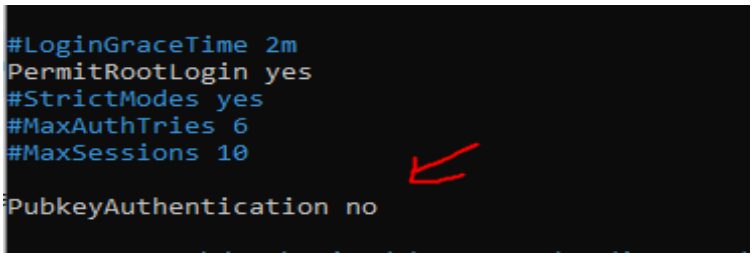


Figure 5.4.1.1: Changing PubKeyAuthentication

Save and exit, do “systemctl restart sshd”.

If we do not get root permission after disabling the public key authentication, we need to go to another file which is:

- nano /etc/ssh/sshd_config.d/60-cloudimg-settings.conf
- Change “PasswordAuthentication no” to “PasswordAuthentication yes”
- Save and exit, do “systemctl restart sshd”
- We can restart the ssh service by typing “service ssh restart”

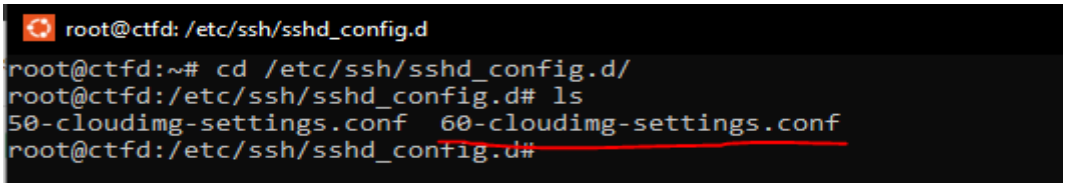


Figure 5.4.1.2: Editing 60-cloudimg-settings.conf

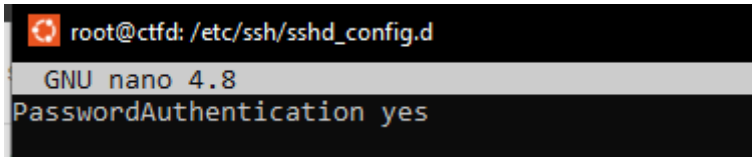


Figure 5.4.1.3: Changing PasswordAuthentication

5.4.2 Migrating CTFd Platform from Locally to GCP VM

To migrate the CTFd platform that we have set locally, we need to go to the machine that we have set up the CTFd platform locally, go to the "ADMIN PANEL".

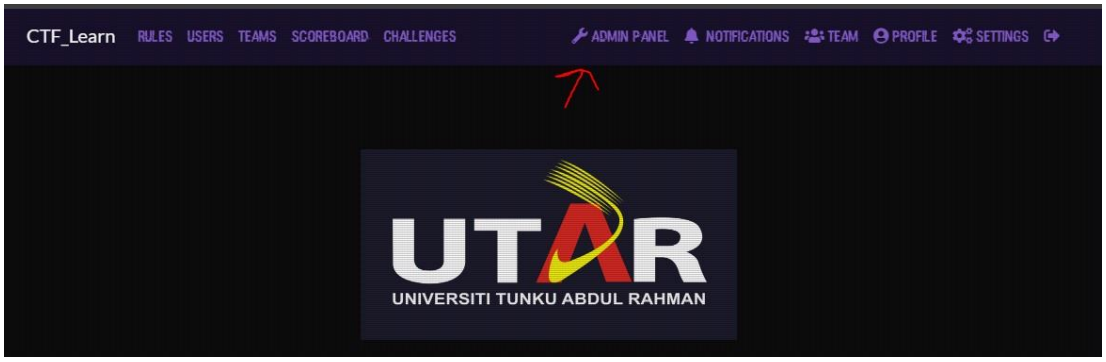


Figure 5.4.2.1: Click on ADMIN PANEL

After that, click on the "Config" tab.

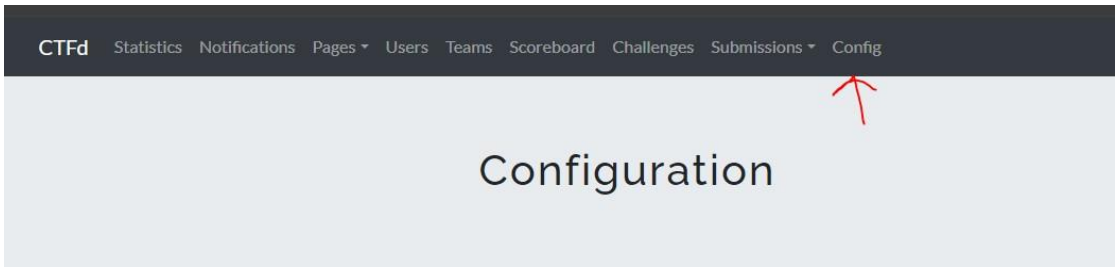


Figure 5.4.2.2: Click on Config tab

Scroll down onto “Backup” and click on the “Import & Export” settings. Then, click on the “Export” button to export the current configuration so that we can load it onto the VM instance in GCP. The downloaded file will be a “zip” file.

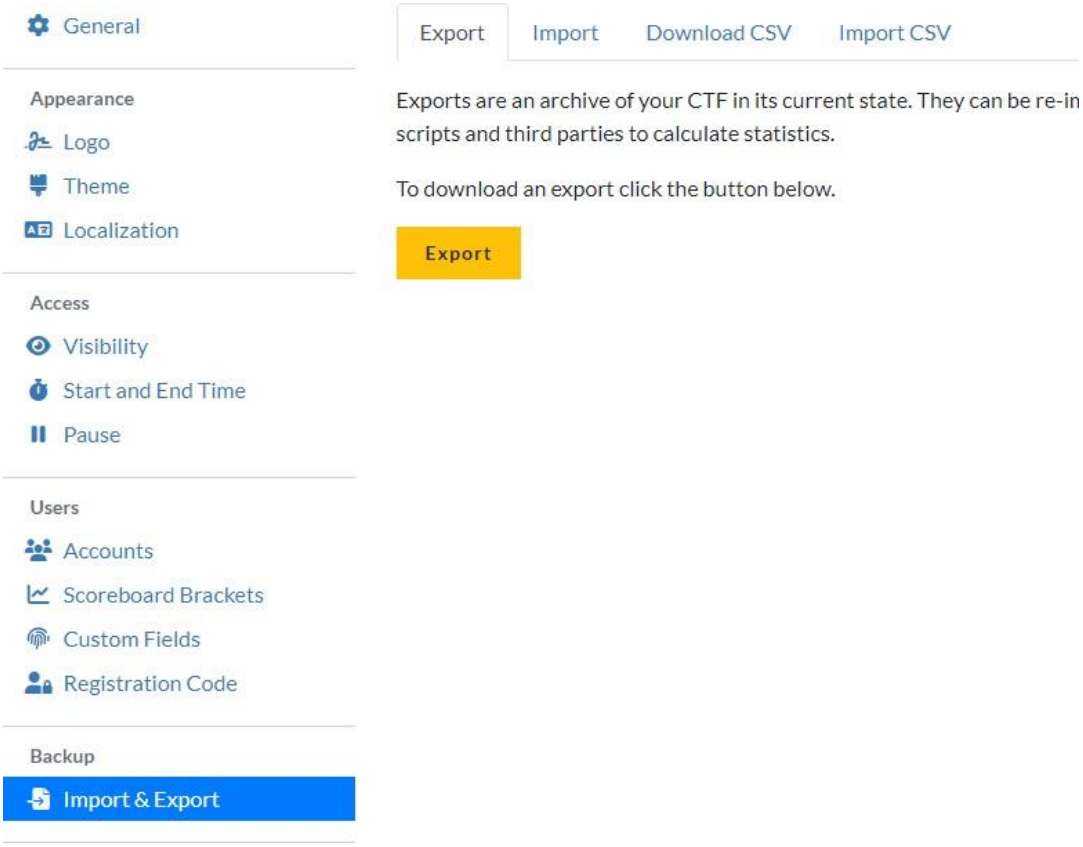


Figure 5.4.2.3: Exporting the CTFd

On the GCP VM instance, same as in 5.2.3 CTFd Platform Installation. The brief commands will be shown below:

- sudo su
- sudo apt update
- apt install docker
- apt -y install docker-compose
- git clone https://github.com/CTFd/CTFd.git
- cd ~/CTFd
- docker-compose up

After that, copy the IP address as shown in the VM instance and paste it on the browser and go to the “ADMIN PANEL”.

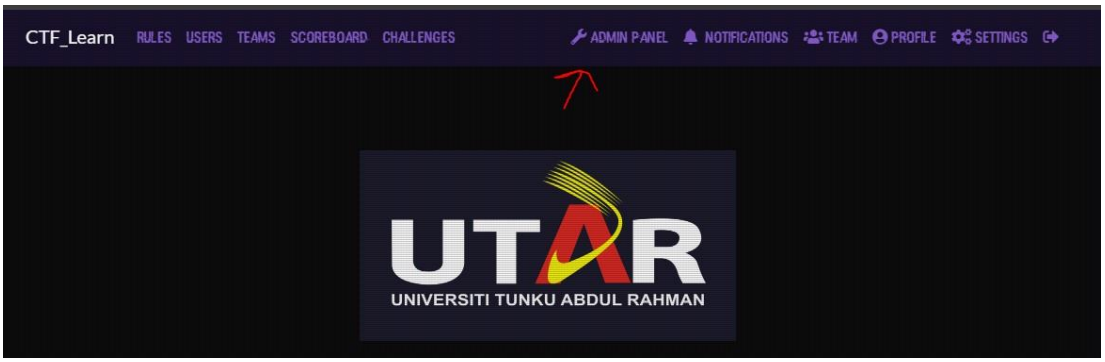


Figure 5.4.2.4: Click on ADMIN PANEL

Click on the “Config” tab.

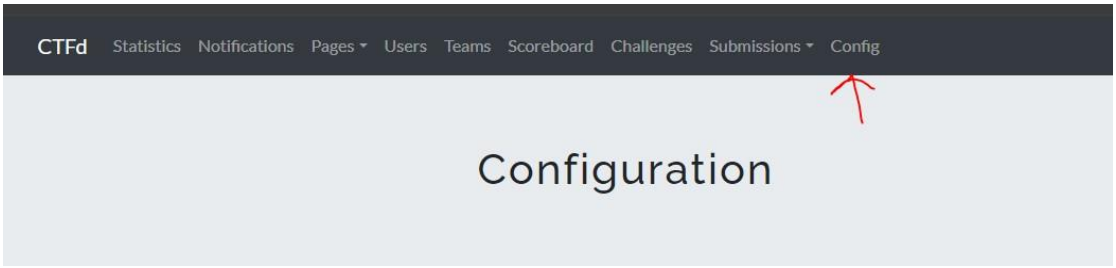


Figure 5.4.2.5: Click on Config

Scroll down onto “Backup” and click on the “Import & Export” settings. Then, click on the “Import” tab to import the “zip” file that we have exported.

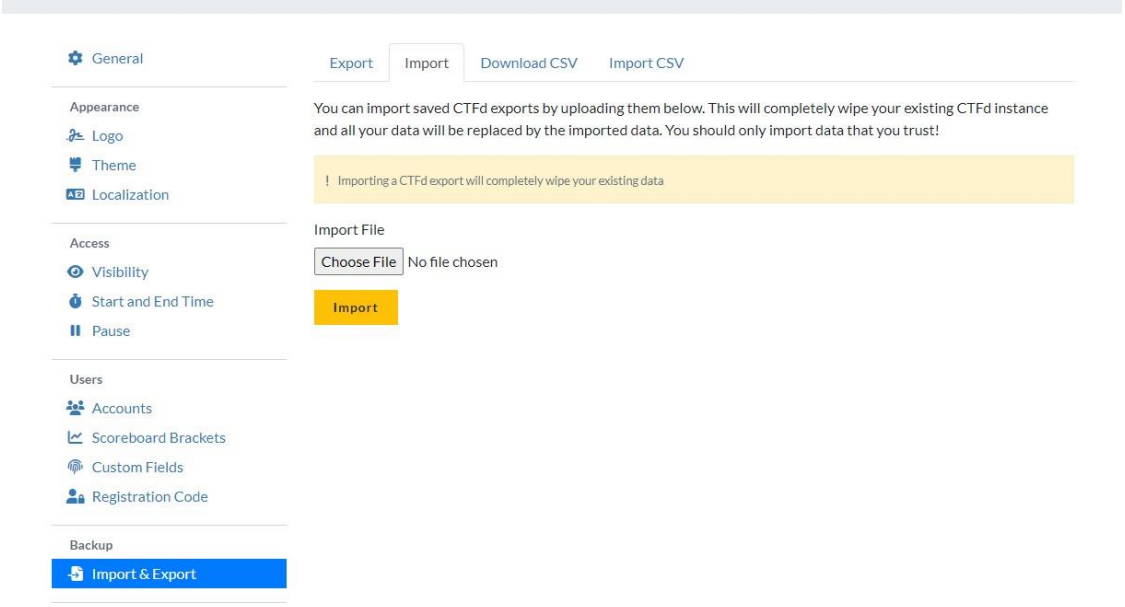


Figure 5.4.2.6: Importing the CTFd to GCP

5.5 Creation and Hosting PWN Challenges via Docker in GCP

5.5.1 Docker Overview

According to [15], Docker is an open platform for developing, shipping and running applications. It enables developers to package an application with all its dependencies into a standardized unit called a container. This container includes everything the software needs to run, such as the code, runtime, system tools, libraries, and settings. By encapsulating applications in containers, Docker ensures that the software will behave the same way, regardless of where it is executed, whether on a developer's local machine, a test environment, or in production.

The primary advantage of Docker is its ability to simplify the development lifecycle by enabling developers to work in standardized environments using local containers. These containers are lightweight and portable, making it easy to move applications between different environments or cloud services. Docker's architecture allows for efficient resource usage, as multiple containers can run on the same machine without the overhead of traditional virtual machines. This approach not only streamlines application development and deployment but also enhances scalability, as containers can be easily scaled up or down based on demand. Overall, Docker provides a consistent, isolated environment for application execution, leading to more predictable and reliable deployments.

5.5.2 Why Docker for PWN Challenges

As aforementioned, Docker is an invaluable tool for creating, deploying and managing PWN challenges in CTF environment due to its ability to provide isolated and consistent environments. Each PWN challenge can be encapsulated within its own Docker container, which includes all necessary dependencies, libraries and system configurations. This isolation ensures that the challenge runs consistently across different machines and environments, addressing the common issue where a challenge might behave differently on another system. For PWN challenges, which often rely on specific system setups or older software versions, the ability for Docker to encapsulate and reproduce these environments is particularly important.

Security is another significant advantage that Docker brings to PWN challenge creation. Since these challenges involve exploiting vulnerabilities by design, there is an inherent risk that an exploit could affect the system it's running on. Docker mitigates this risk by isolating each challenge within its own container. If a participant successfully exploits a challenge, the effects are confined to that container, protecting the host system and other challenges from any potential damage. This containerization not only ensures the security of the CTF infrastructure but also allows organizers to confidently deploy even the most vulnerable challenges.

Deploying PWN challenges in a CTF environment is also made easier with Docker. Once a challenge is developed and tested within a Docker container, it can be easily packaged as a Docker image and deployed across various servers with minimal setup. This streamlined deployment process is particularly beneficial during a CTF environment, where challenges need to be deployed quickly and reliably. Docker’s portability ensures that the exact environment used during development is replicated during the competition, minimizing the chances of unforeseen issues.

Moreover, Docker’s lightweight nature allows for efficient use of server resources. Unlike traditional virtual machines, Docker containers require fewer resources, enabling CTF organizers to run multiple challenges on a single server without significant overhead. This efficiency is especially important in large-scale competitions

where server capacity might be limited, and the ability to scale up challenge instances quickly can enhance the participant experience.

Finally, Docker's integration with continuous integration and deployment pipelines facilitates automated builds and testing of PWN challenges. Developers can create, test, and refine challenges locally using Docker, then automate the deployment process to ensure that the challenges are deployed exactly as intended. This automation reduces the likelihood of errors and ensures that challenges are thoroughly tested before being made available to participants, resulting in a smoother and more reliable competition experience.

In summary, Docker enhances the creation, deployment, and management of PWN challenges in CTF competitions by providing a secure, consistent, and efficient environment. It allows challenge creators to focus on designing complex and engaging challenges without worrying about deployment issues, while also giving organizers the tools to manage and scale the competition effectively.

5.5.3 PWN Challenge Creation

When deploying a PWN challenge for the first time, you may encounter an issue where the program fails to produce output unless user input is received first. This is due to the need for explicit buffer settings. To address this, ensure that you configure the buffer settings as demonstrated in the code below:

```
void init() {
   setbuf(stdin, 0);
   setbuf(stdout, 0);
   setbuf(stderr, 0);
}
```

Example source code is shown below, remember to call the init() in the main function and also create a flag.txt file:

```
#include  <stdio.h>
#include <stdlib.h>
#include <string.h>

void init() {
   setbuf(stdin, 0);
   setbuf(stdout, 0);
   setbuf(stderr, 0);
}

int main() {
   char buffer[16];
   int admin = 0;
   char flag[64];

   init();

   printf("Enter the password: ");
```

```
    gets(buffer);

    if(strcmp(buffer, "strongpassword") == 0) {
        printf("Access Granted! You've bypassed the password check.\n");
    } else {
        printf("Access Denied. Incorrect password.\n");
    }

    if(admin) {
        printf("Successfully logged in as admin.\n");
        fgets(flag, 64, fopen("flag.txt", "r"));
        puts(flag);
    }

    else {
        printf("Unsuccessful log in as admin.\n");
    }

    return 0;
}
```

After that, we can compile the program via “gcc”. According to [16], GCC (GNU Compiler Collection) is a robust and widely-used open-source compiler system that supports various programming languages, including C, C++, and Fortran. Originally developed by the Free Software Foundation (FSF), GCC is a cornerstone tool in the Unix and Linux ecosystems, providing developers with the ability to compile source code into executable programs. It plays a critical role in software development, enabling the translation of high-level programming languages into machine code that can be executed by a computer’s hardware.

GCC is not just a single compiler but a collection of compilers for different languages, all unified under a common framework. It includes a range of tools and features such as pre-processing, compiling, assembling, and linking. This versatility allows

developers to manage the entire build process of software projects within a single toolchain. Moreover, GCC is highly configurable and can be used across a variety of platforms, making it an essential tool for developers who need to create portable and efficient code. Its open-source nature has led to its widespread adoption and continuous improvement by the global development community.

A simple example will be:

- gcc test.c

However, when designing a pwn challenge for a CTF, we may need to evaluate its security protections to determine which ones should be disabled to craft an effective challenge. According to https://www.duo.uio.no/bitstream/handle/10852/79729/1/Master-Thesis---Detecting-Buffer-Overflows-using-Python---Ingeborg-Ytrehus.pdf, such protections are:

1) Stack Canaries

A stack canary is a protective measure placed between a buffer and the adjacent memory. These canaries function similarly to the canaries used in coal mines to monitor air quality. If the canary's value changes, it signals potential data corruption after the buffer (such as registry values in stack-based buffer overflows), akin to how a dead canary would warn miners of danger. If the stack canary's integrity is compromised, the program will terminate to prevent an attacker from exploiting the stack.

2) Non-Executable Stack (NX) or Heap

NX protection is to separate memory into regions designated for either code or data, ensuring that memory regions containing data are non-executable thus preventing the execution of shellcode if it is written to the buffer. This approach ensures that any memory that can be manipulated by the user cannot be executed. However, attackers can still bypass this protection, for example, by re-enabling stack execution during runtime.

3) Relocation Read-Only (RELRO)

RELRO (Relocation Read-Only) is a technique that marks the Global Offset Table (GOT) as read-only. RELRO can be implemented either partially or fully. Full RELRO makes the entire GOT read-only, preventing attacks where the address of a function in the GOT is overwritten with a different function address or ROP gadget. Full RELRO is, therefore, the most effective method for hardening ELF (Extensible Linking Format) binaries, though it may increase the program's startup time since the linker must create all GOT entries before the main function begins. With either full or partial RELRO, any attempt to overwrite a GOT entry will cause a segmentation fault. Partial RELRO ensures the GOT is placed before the BSS segment, eliminating the risk of overflowing variables into GOT entries during runtime. Partial RELRO is typically the default setting in Linux distributions.

4) Address Space Layout Randomization (ASLR)

Randomizing the memory layout so that the heap, stack, and libraries do not start at fixed addresses can make it more difficult for attackers to locate the addresses of functions, gadgets, and the buffer being overflowed.

5) Position Independent Executable (PIE)

Enabling PIE for a binary ensures that the binary and its dependencies are loaded into randomized locations within virtual memory each time the application runs. As a result, memory addresses will differ with each execution. When both PIE and ASLR are enabled, the memory layout of the program becomes highly variable, making it more challenging to carry out attacks against the program.

Protection Mechanisms for ELF Files During Compilation:

- **NX:** -z execstack / -z noexecstack (Disable / Enable)
- **Canary:** -fno-stack-protector / -fstack-protector / -fstack-protector-all (Disable / Enable / Fully Enable)
- **PIE:** -no-pie / -pie (Disable / Enable)
- **RELRO:** -z now / -z lazy / -z norelro (Fully Enable / Partially Enable / Disable)

For example, if we want to create the challenge to have NX disabled, canary disabled and PIE disabled, we can type the following:

- gcc -z execstack -fno-stack-protector -no-pie -g pwn_level3.c -o test

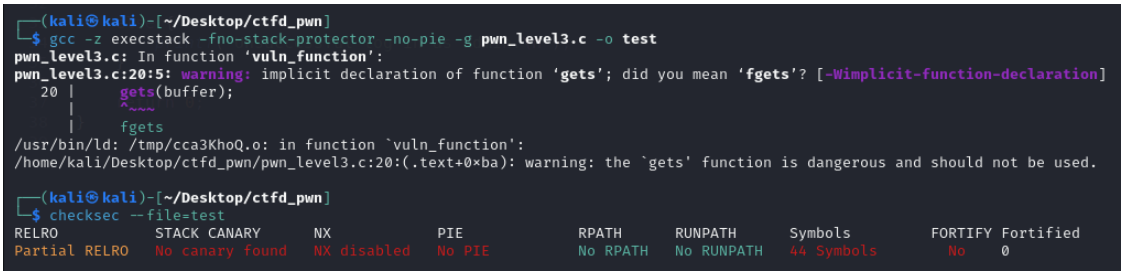


Figure 5.5.3.1: Checksec Protections

Hence, when we run checksec on the file as shown in Figure 5.5.3.1, we can see that all those protections are disabled.

If we want the file to be 32 bit, we can add -m32 onto the terminal:

- gcc -m32 -z execstack -fno-stack-protector -no-pie -g pwn_level3.c -o pwn_level3_32

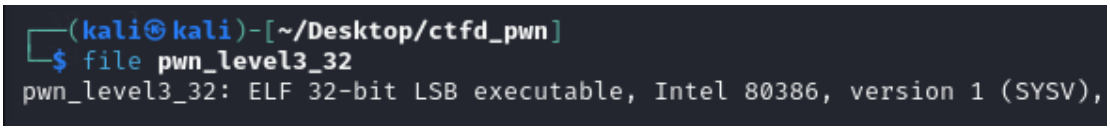


Figure 5.5.3.2: Changing ELF File to 32-bit

5.5.4 Hosting PWN Challenge via Docker in GCP

In this section, you may create a separate VM instance to host the pwn challenge. Using ctf_xinetd in conjunction with Docker, we can create a robust environment for our CTF environment to ensure that each challenge runs smoothly and securely. The ctf_xinetd is a docker repository to deploy CTF challenges. The link for the github repository is https://github.com/Eadom/ctf_xinetd/tree/master.

The first step is to clone the ctf_xinetd project from GitHub. This project is a pre-configured service template that helps set up a secure environment for hosting CTF challenges. The ctf_xinetd template is particularly useful for managing challenges that need to handle multiple simultaneous connections.

- git clone https://github.com/Eadom/ctf_xinetd.git
- cd ctf_xinetd/

We can also change the folder name from ctf_xinetd to other folder as shown below.

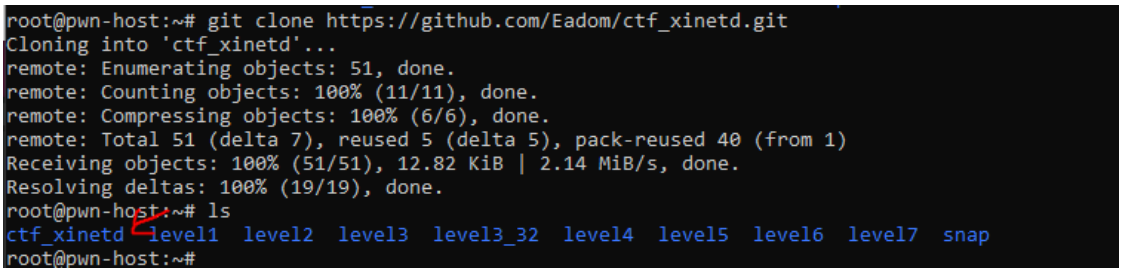


Figure 5.5.4.1: Changing folder name

Inside the ctf_xinted, the files that we need to note is ‘Dockerfile’, ‘ctf.xinetd’ and the ‘bin’ folder.

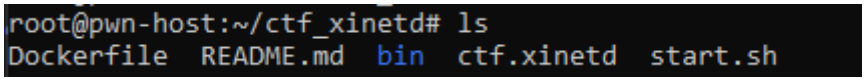


Figure 5.5.4.2: Files inside ctf_xinetd

First, we need to configure the Dockerfile, we need to change the ubuntu version to match the VM instance that we have created.

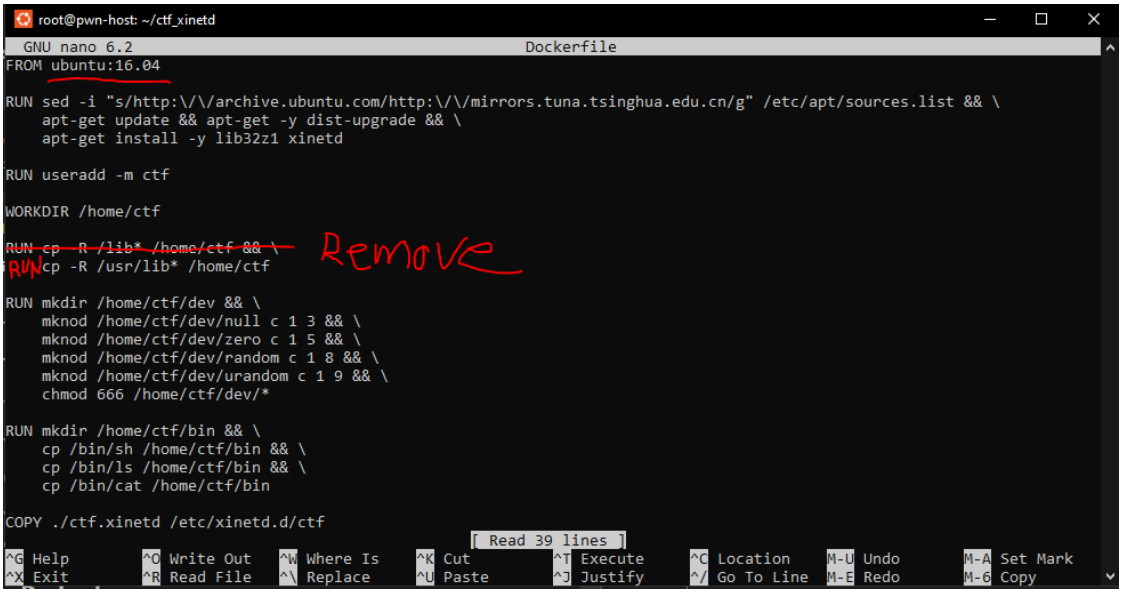


Figure 5.5.4.3: Configuring Dockerfile

We may also need to change the flag file, if you have set the flag file to “flag.txt”. After that, we may modify the port number to expose the port in Docker.

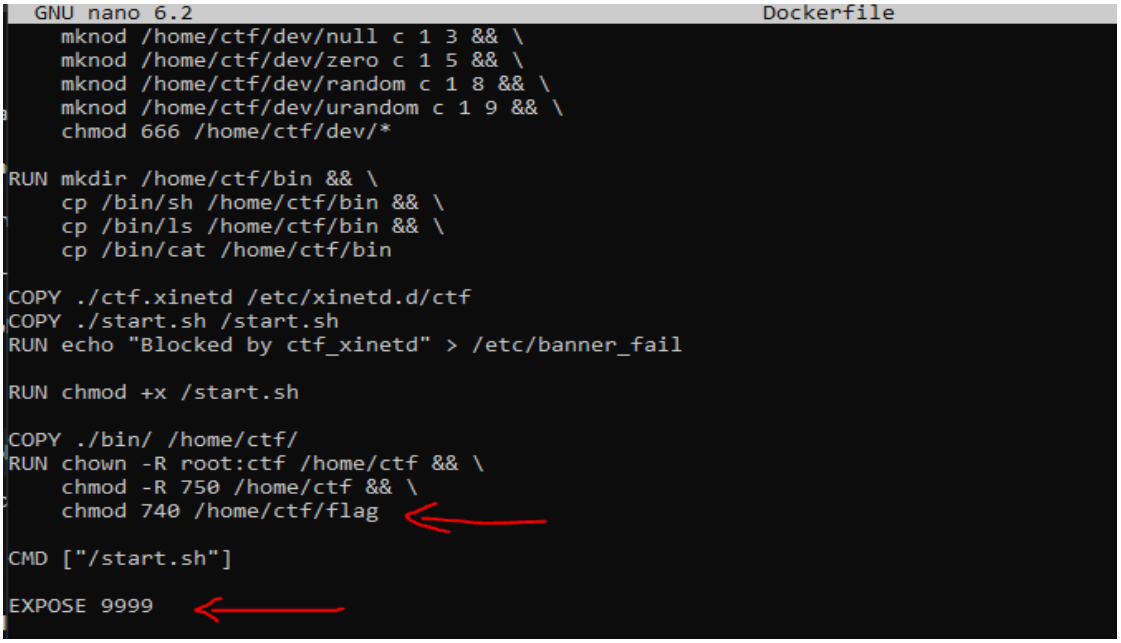


Figure 5.5.4.4: Changing flag file and port number

The Dockerfile after we have successfully modified.

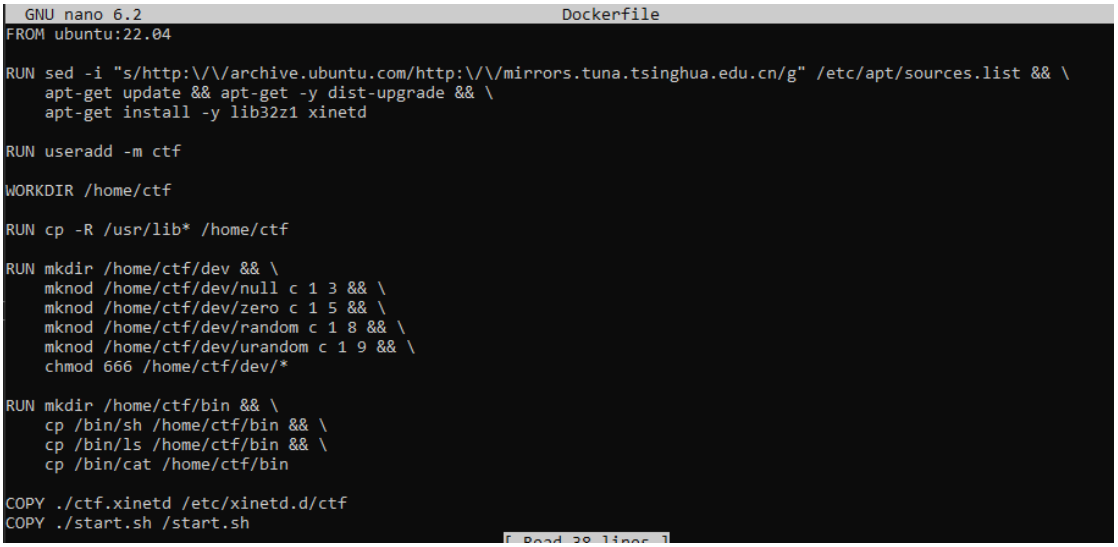


Figure 5.5.4.5: Result of the successful configuration

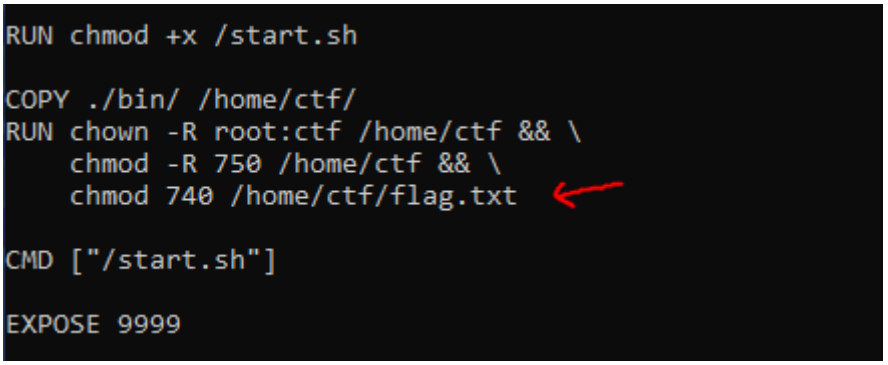


Figure 5.5.4.6: Result of the flag file name

The reason we need to remove the “RUN cp -R /lib* /home/ctf && \” is because the Ubuntu version being used is higher than 18.04 and the command is the old one hence we need to remove it.

If we do not remove it, this issue will come out:

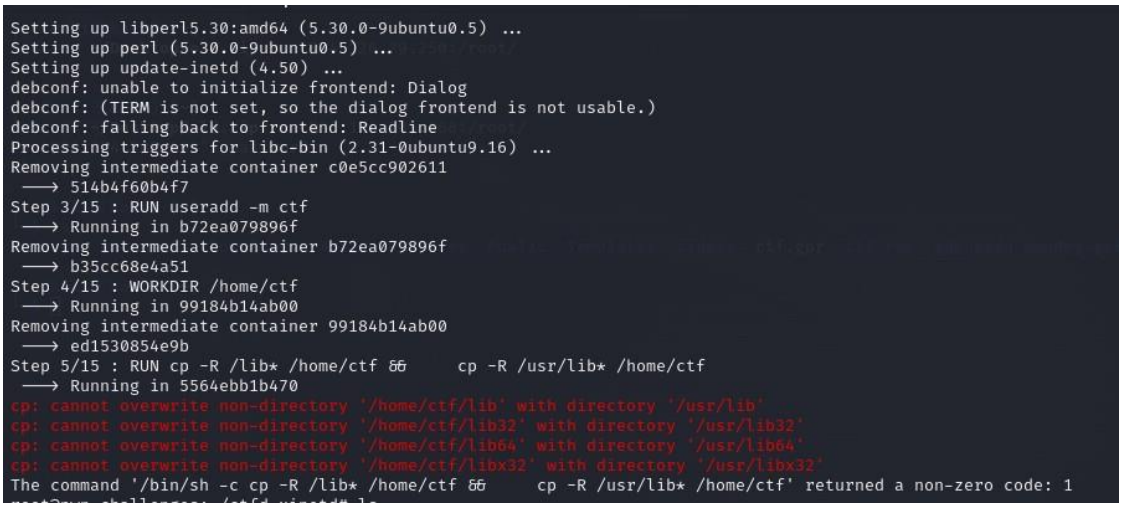


Figure 5.5.4.7: Ubuntu version error

After that, we need to configure the “ctf.xinetd” file. The ctf.xinetd file controls how the service behaves including network settings, security options and how to start the challenge binary.

Important Fields:

- port: Set this to the port number on which your challenge should run.
- server_args: Modify this to point to your challenge binary.
- user: Set to root or another user, depending on your requirements.
- server: Set this to the path of your challenge binary (e.g., ./helloworld).

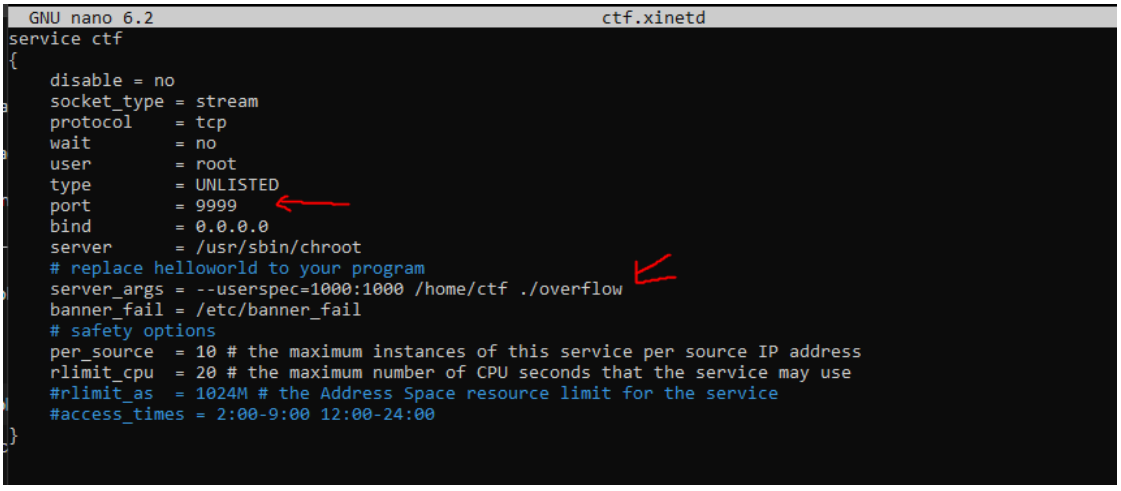


Figure 5.5.4.8: Configuring ctf_xinetd file

Next, we need to go to the “bin” folder and drop the binary into the folder. Remember to modify and rename the “flag” file. In my case, I will rename it to “flag.txt” because in the challenge source code, I wrote it as open “flag.txt” to open the flag upon successfully exploiting the challenge.

To easily transfer the challenge file to the GCP VM instance, we can use the following commands:

- scp ~/Desktop/ctfd_pwn/pwn_level1_64bit root@35.198.248.246:/root/ctf_xinetd/bin
- rm helloworld
- mv flag flag.txt
- echo “test_flag” > flag.txt
- cat flag.txt

```
┌──(kali㉿kali)-[~/Desktop/ctfd_pwn]
└─$ scp ~/Desktop/ctfd_pwn/pwn_level1_64bit root@35.198.248.246:/root/ctf_xinetd/bin
root@35.198.248.246's password:
pwn_level1_64bit
```

Figure 5.5.4.9: Transferring file

```
root@pwn-host:~/ctf_xinetd/bin# ls
flag  helloworld  pwn_level1_64bit
root@pwn-host:~/ctf_xinetd/bin# rm helloworld
root@pwn-host:~/ctf_xinetd/bin# mv flag flag.txt
root@pwn-host:~/ctf_xinetd/bin# echo "test_flag" > flag.txt
root@pwn-host:~/ctf_xinetd/bin# ls
flag.txt  pwn_level1_64bit
root@pwn-host:~/ctf_xinetd/bin# cat flag.txt
test_flag
root@pwn-host:~/ctf_xinetd/bin#
```

Figure 5.5.4.10: Successfully transferring file

Note: you may also need to change the binary permissions. Chmod +750 <filename> would be sufficient.

Once everything is configured, we can proceed to build the Docker Image via command shown below. Note: Do not forget about the "." at the end of the command and you need to execute it inside the "ctf_xinetd" folder or whatever folder you named it:

- docker build -t "pwn_level1" .

This command will create a Docker image named "pwn_level1". You may rename it to your liking.

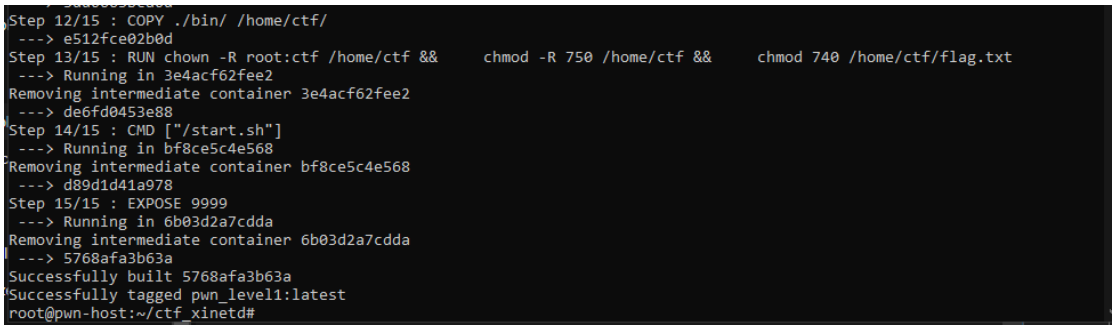


Figure 5.5.4.11: Building docker image

To confirm that you have successfully created the image, we can type the command:

- docker image ls

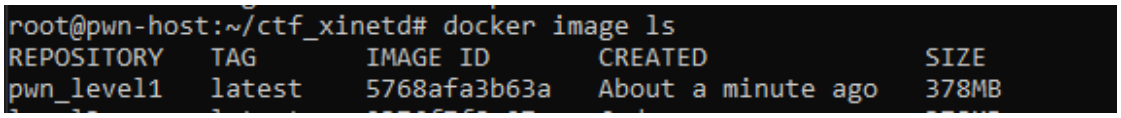


Figure 5.5.4.12: Confirming docker image has been created

To remove the docker image, you may type the following:

- docker image remove <REPOSITORY>

After building the image, you can launch the challenge in a Docker container. This will bind the challenge to a specific port and make it accessible to players.

- docker run -d -p 0.0.0.0:9000:9999 -h “pwn_level1” --name="pwn_level1 " pwn_level1

The explanation of the command is shown below:

1. **docker run**:

- This is the basic command to create and start a new container from a Docker image. When you run this command, Docker will start a new container based on the specified image.

2. **-d:**

- This flag tells Docker to run the container in "detached" mode, meaning it runs in the background. You won't see the container's output in your terminal, and your terminal will be free to use for other commands.

3. **-p 0.0.0.0:9000:9999:**

- This option maps a port on your host machine to a port inside the Docker container.
- 0.0.0.0:9000: Specifies that the container's port should be accessible on all network interfaces (0.0.0.0) of the host machine, using port 9000. This means that any IP address associated with your host machine can be used to access the service running on port 9000.
- 9999: This is the port inside the Docker container where the service is listening. So, any traffic sent to 10000 on the host machine will be forwarded to 9999 inside the container.

4. **-h "pwn_level1":**

- Sets the hostname of the Docker container to "pwn_level1". The hostname is an internal identifier for the container and can be used within the container itself or by other containers when communicating with it.

5. **--name="pwn_level1":**

- This option assigns a name to the running container, in this case, "pwn_level1". Naming containers makes them easier to manage since you can refer to them by name in other Docker commands (like docker stop pwn_level1, docker logs pwn_level1, etc.).

6. **pwn_level1 (at the end):**

- This is the name of the Docker image from which to create the container. Docker will look for an image named "pwn_level1" (as created earlier using the docker build command) and use it as the base for the new container.

```
root@pwn-host:~/ctf_xinetd# docker run -d -p 0.0.0.0:9000:9999 -h "pwn_level1" --name="pwn_level1" pwn_level1
1f37f49ef3f1ed04d2e84ca4cf440f86c685911460cae743e219ff939dae76db
```

Figure 5.5.4.13: Launching challenge via Docker container

Now, the challenge is accessible on port 9000 on the VM instance. If you have multiple challenge, you may use the same commands and host it on other ports.

To view running containers, you may type the following:

- docker ps -a

```
root@pwn-host:~/ctf_xinetd# docker ps -a
CONTAINER ID   IMAGE         COMMAND       CREATED         STATUS                     PORTS                    NAMES
1f37f49ef3f1   pwn_level1    "/start.sh"   3 seconds ago   Up 3 seconds               0.0.0.0:9000->9999/tcp   pwn_level1
25201a9649b6   level3        "/start.sh"   6 days ago      Exited (137) 6 days ago                             level3
472034ea1be7   level7        "/start.sh"   6 days ago      Exited (137) 6 days ago                             level7
e4b8ee095273   level6        "/start.sh"   6 days ago      Exited (137) 6 days ago                             level6
2488bae8f6ed   level5        "/start.sh"   6 days ago      Exited (137) 6 days ago                             level5
391353161edf   level4        "/start.sh"   6 days ago      Exited (137) 6 days ago                             level4
f82e23d32681   level3_32     "/start.sh"   6 days ago      Exited (137) 6 days ago                             level3_32
6b4f395bc053   level2        "/start.sh"   6 days ago      Exited (137) 6 days ago                             level2
c3183385ae0f   level1        "/start.sh"   6 days ago      Exited (137) 6 days ago                             level1
```

Figure 5.5.4.14: View all running containers

To start all the stopped containers, you may type the following:

- docker start $(docker ps -a -q -f status=exited)

```
root@pwn-host:~/ctf_xinetd# docker start $(docker ps -a -q -f status=exited)
25201a9649b6
472034ea1be7
e4b8ee095273
2488bae8f6ed
391353161edf
f82e23d32681
6b4f395bc053
c3183385ae0f
root@pwn-host:~/ctf_xinetd# docker ps -a
CONTAINER ID   IMAGE        COMMAND       CREATED         STATUS          PORTS                     NAMES
1f37f49ef3f1   pwn_level1   "/start.sh"   4 minutes ago   Up 4 minutes    0.0.0.0:9000->9999/tcp    pwn_level1
25201a9649b6   level3       "/start.sh"   6 days ago      Up 10 seconds   0.0.0.0:10002->9999/tcp   level3
472034ea1be7   level7       "/start.sh"   6 days ago      Up 9 seconds    0.0.0.0:10007->9999/tcp   level7
e4b8ee095273   level6       "/start.sh"   6 days ago      Up 8 seconds    0.0.0.0:10006->9999/tcp   level6
2488bae8f6ed   level5       "/start.sh"   6 days ago      Up 7 seconds    0.0.0.0:10005->9999/tcp   level5
391353161edf   level4       "/start.sh"   6 days ago      Up 7 seconds    0.0.0.0:10004->9999/tcp   level4
f82e23d32681   level3_32    "/start.sh"   6 days ago      Up 5 seconds    0.0.0.0:10003->9999/tcp   level3_32
6b4f395bc053   level2       "/start.sh"   6 days ago      Up 4 seconds    0.0.0.0:10001->9999/tcp   level2
c3183385ae0f   level1       "/start.sh"   6 days ago      Up 3 seconds    0.0.0.0:10000->9999/tcp   level1
root@pwn-host:~/ctf_xinetd#
```

Figure 5.5.4.15: Start all stopped containers

To stop all running containers, you may type the following:

- docker stop $(docker ps -a -q)

To restart all running containers, you may type the following:

- docker restart $(docker ps -a -q)

To remove the container, you may type the following:

- docker rm <CONTAINER ID>

If you need to capture network traffic for analysis or troubleshooting, you can use tcpdump. This tool captures and saves packets transmitted over the network, which can be useful for debugging and for capturing cheaters:

- tcpdump -w pwn.pcap -i eth0 port 10000

Explanation:

-w pwn.pcap: Saves the captured traffic to a file named pwn.pcap.

-i eth0: Specifies the network interface to capture traffic from.

port 10000: Captures only the traffic to/from port 10000.

5.6 Allow Access By Enabling Firewall

Next, enable the firewall so that outside connections are allowed to connect to your challenges. Click on the “three dot menu” and click on the “View network details” as shown in Figure 5.6.1 below:

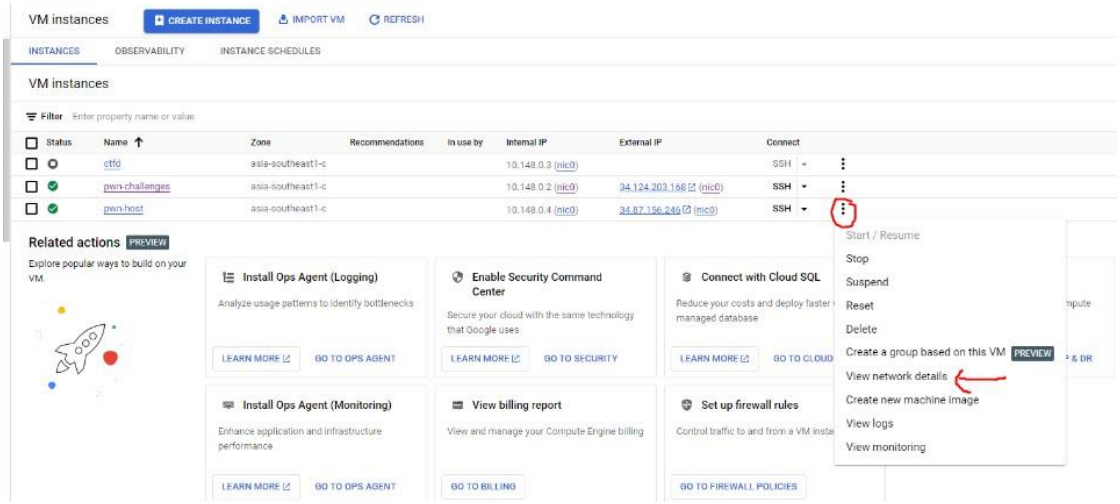


Figure 5.6.1: View network details

Click on the Firewall as shown in Figure 5.6.2 below:

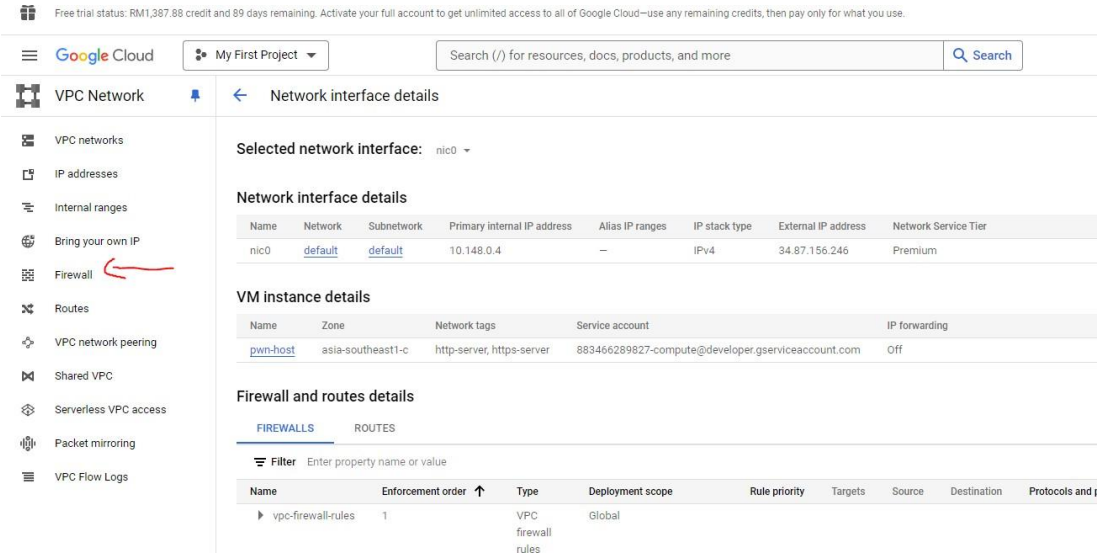


Figure 5.6.2: Go to firewall option

Next, click on the “Create Firewall Rule” tab in “Firewall policies” under the “Cloud NGFW”.

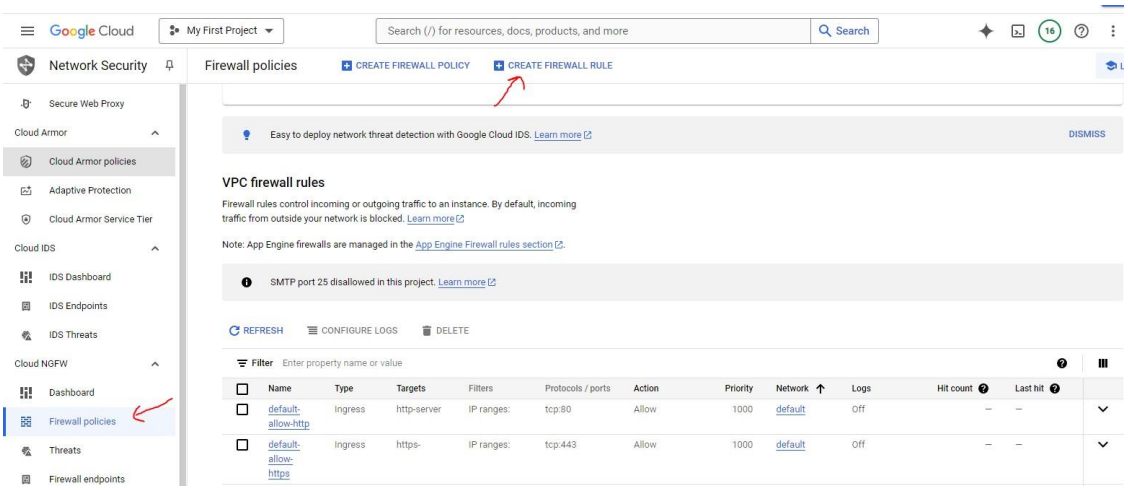


Figure 5.6.3: Create firewall rule

The most important setting is here as shown in Figure 5.6.4:

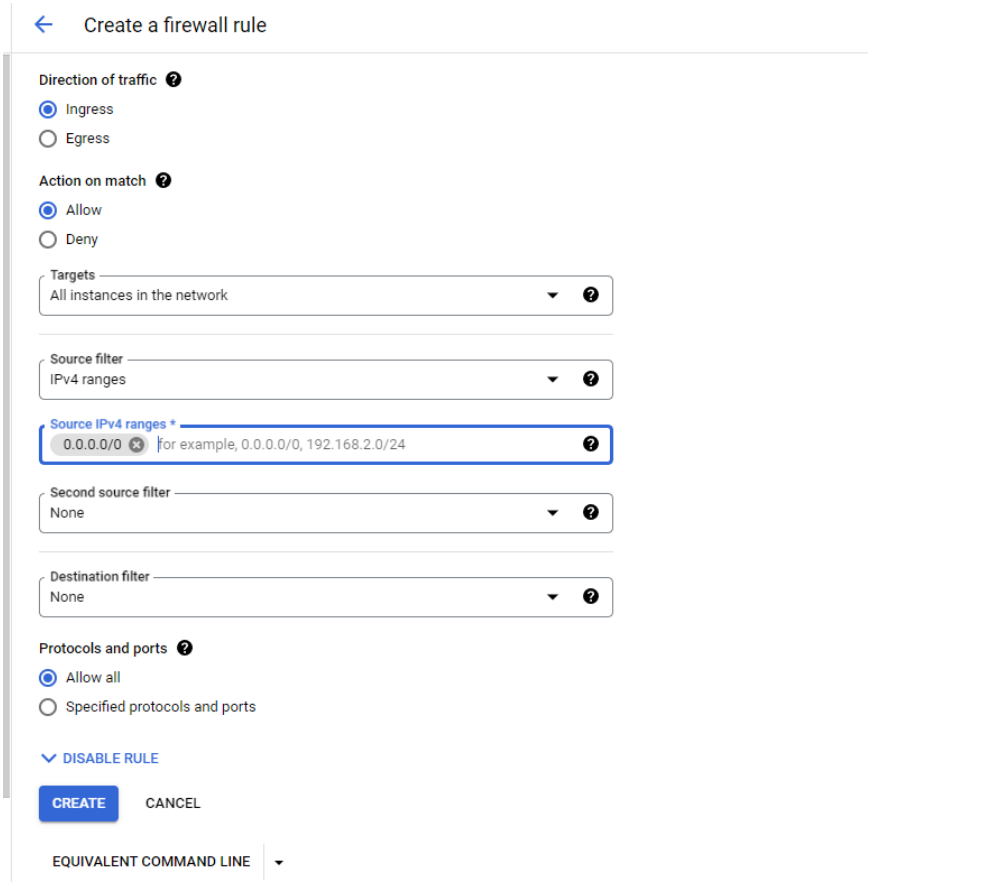


Figure 5.6.4: Allow all IP to access

5.7 Creating Static IP Address

To create a Static IP Address for the PWN or Boot2Root challenges, do the following as shown in Figure 5.7.1:

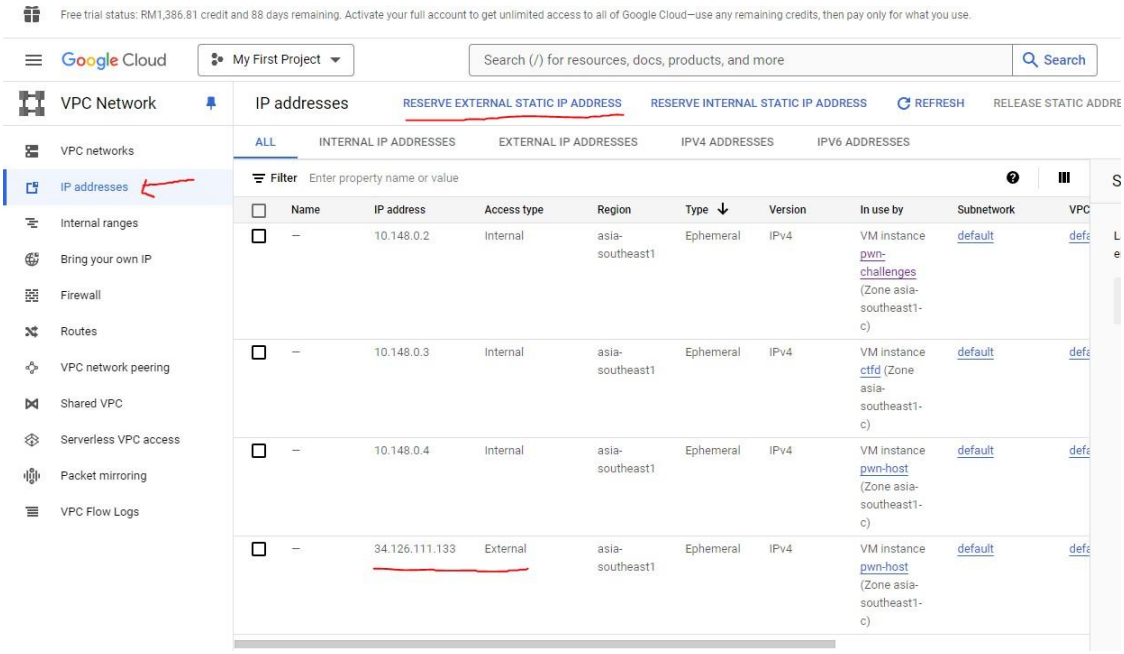


Figure 5.7.1: Reserving external static IP address

Set the name that you preferred and put the static IP to the attached VM instances as shown in Figure 5.7.2.

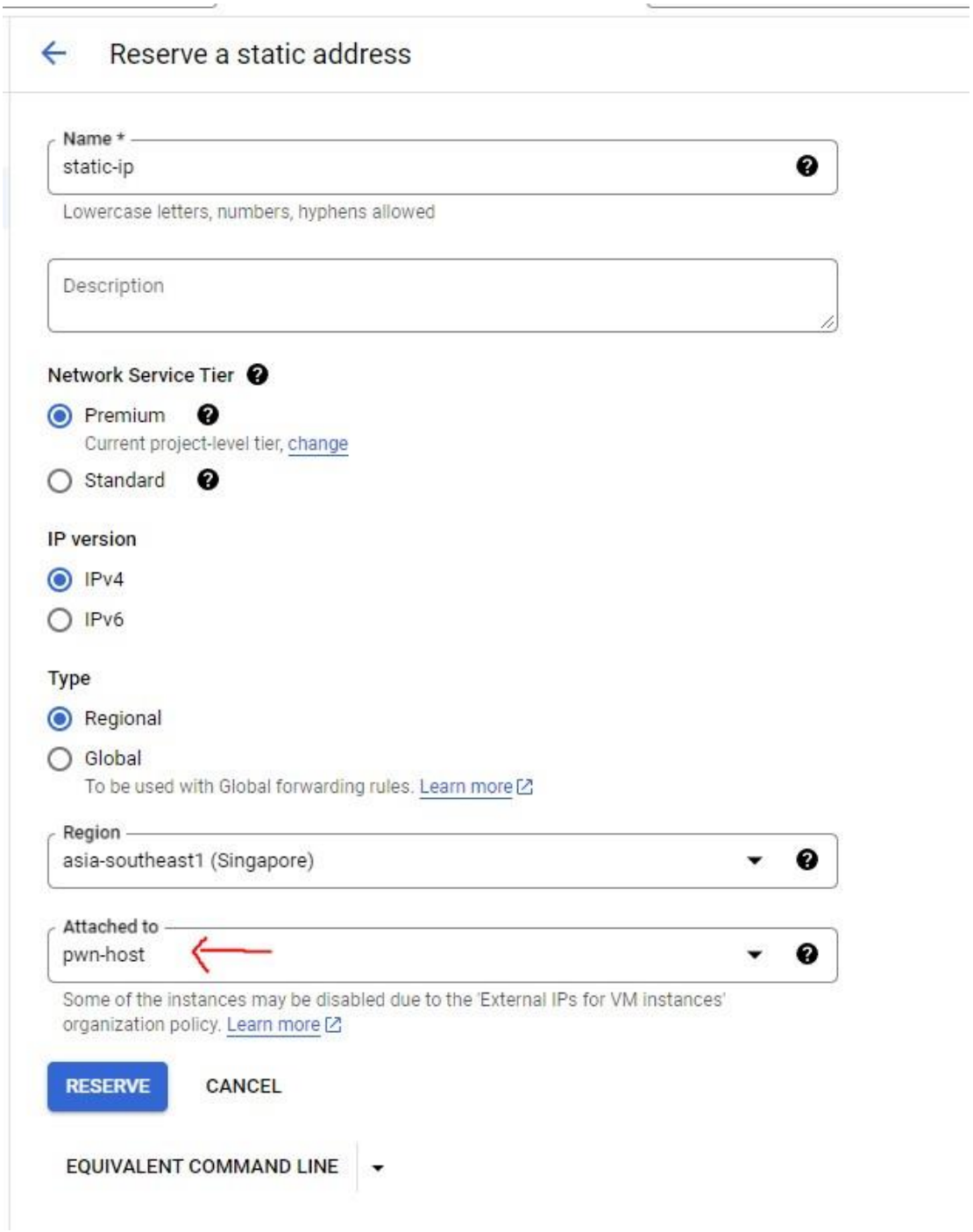


Figure 5.7.2: Attach to the VM instance

Now, we can double check to see whether it has been successfully applied or not.

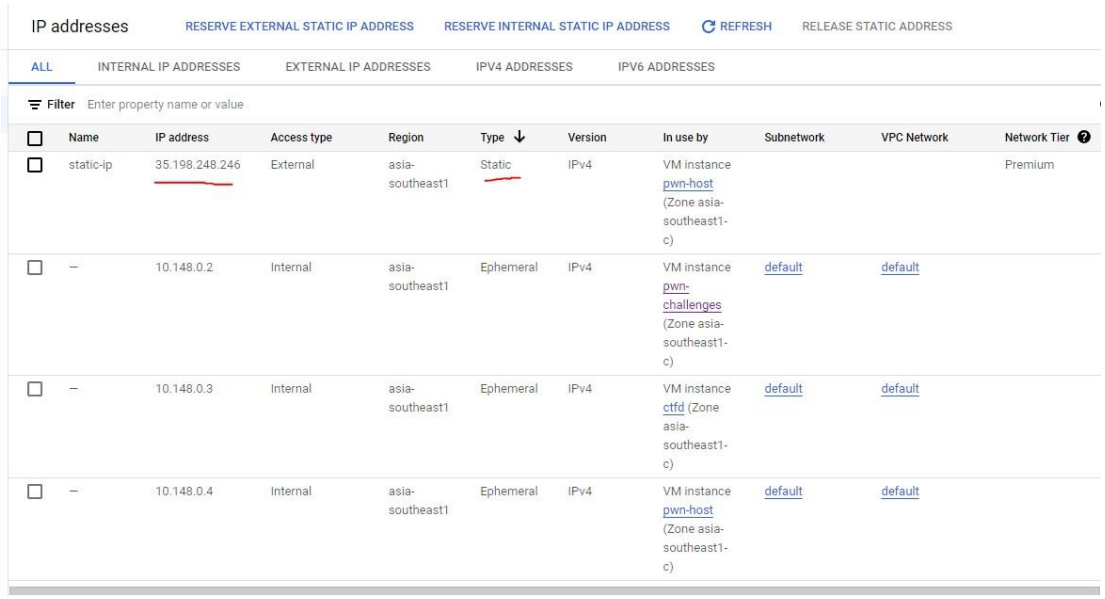


Figure 5.7.3: Double check on the static IP

So, now we do not need to change the challenge description every time we launch the instance.

Figure 5.7.4: Verifying IP address on VM instance

5.8 Important Configuration for Boot2Root Challenge in GCP

After successfully setting up the Boot2Root challenge in GCP, it is essential to ensure that users cannot delete important system files, even if they gain elevated privileges. To achieve this, we can utilize the chattr command to modify file attributes, effectively disabling the rm and rmdir commands, which are typically used to delete files and directories. By restricting these commands, even the root user will be prevented from executing file deletions.

- chattr -i /bin/rm
- chmod 000 /bin/rm
- chattr +i /bin/rm
- chmod 000 /bin/rmdir
- chattr +i /bin/rmdir

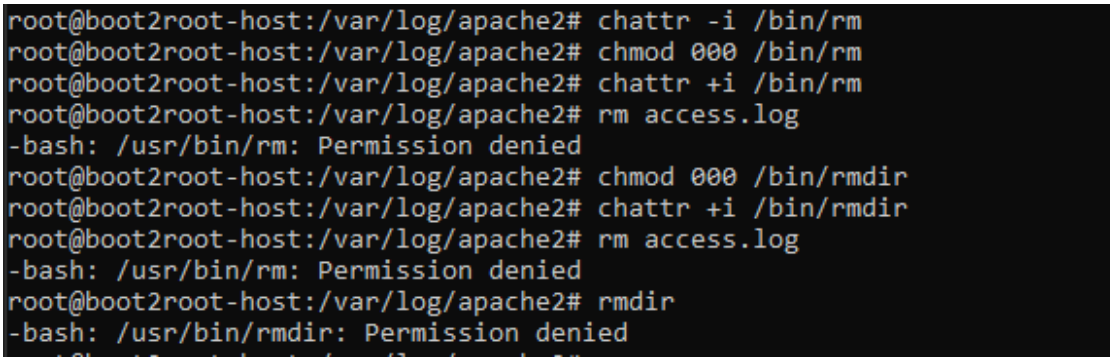


Figure 5.8.1: Commands to prevent accidental deletion

5.9 Implementation Issues and Challenges

Throughout the development phase, implementing a robust CTF educational platform entail navigating a multitude of complex challenges. Among the key challenges at the implementation stage is web page customization of the CTFd platform. It was very difficult to customize the platform in such a way that the rigid framework of the present templates and the advanced changes to them made it difficult to do better than that. These tasks require, in some cases, delving into the documentation of this platform, and even sometimes directly fiddling with the source code which risks the potential future integration issues with updates. Another substantial challenge was the creation of binary exploitation challenges, where it would not work on the remote connection and would need to do extensive research to solve the issue. Furthermore, striking a balance between crafting a challenge that was educational yet not overly contrived was the task at hand. The challenge needed to be realistic, therefore complex enough, for participants to have a real learning experience and approachable for participants with varying skill levels. Moreover, we also need to ensure the stability and security of these challenges as they posed its own set of problems as each submission could potentially affect the system's integrity.

CHAPTER 6
SYSTEM EVALUATION AND DISCUSSION

In this chapter, the system will be evaluated for testing purposes. Additionally, a discussion will be held to identify the challenges encountered and assess the extent to which the project's objectives have been met.

6.1 System Evaluation

There are 15 UTAR students participated in this testing. The participants were distributed across various programs: 9 from CN, 1 from CS, 1 from EN, 1 from IA, and 3 from MK. Based on the survey, when asked about their familiarity with the concept of cybersecurity on a scale of 1 to 5, with 1 being the least familiar and 5 being the most, most participants indicated a high level of familiarity. Specifically, **53.3%** of the respondents rated themselves as 5 (very familiar), and **26.7%** rated their familiarity as 4. On the other hand, **13.3%** rated their familiarity as 2, and **6.7%** rated it as 3, indicating a smaller group with lower familiarity. These results suggest that most of the respondents possess a strong understanding of cybersecurity concepts, but there remains a minority that may benefit from foundational training.

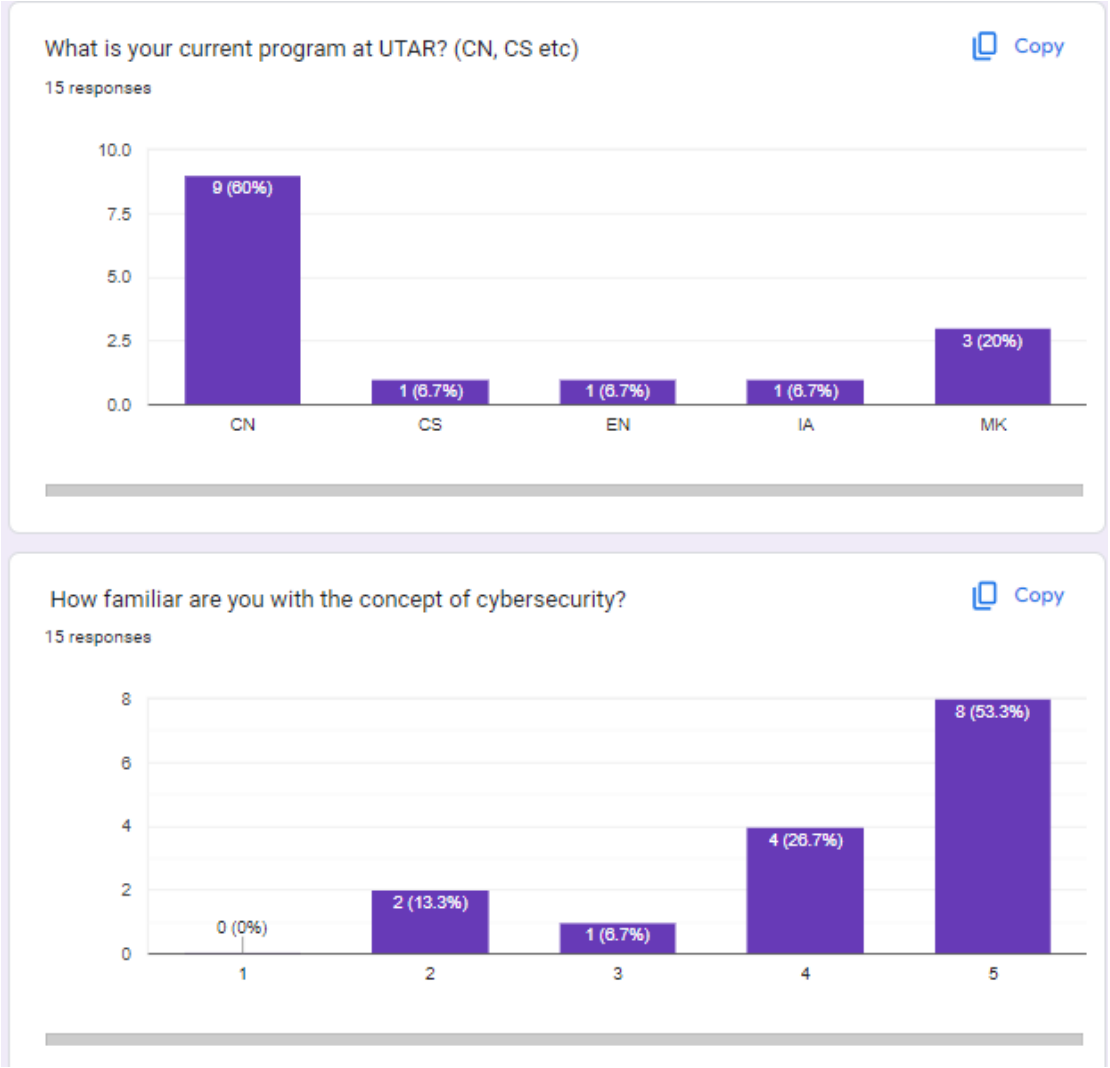


Figure 6.1.1: Questionnaire 1

In terms of the personal importance of cybersecurity, the survey revealed that almost all respondents consider it highly significant. **93.3%** of the participants rated cybersecurity as a 5 (very important) on a scale of 1 to 5, with only **6.7%** rating it as 4. There were no responses below 4, indicating a strong consensus that cybersecurity is a critical area of interest for these individuals. This high level of personal importance underscores the relevance of cybersecurity education to the participants' future career aspirations or academic focus.

Figure 6.1.2: Questionnaire 2

When asked whether they were familiar with Capture the Flag (CTF) competitions in the context of cybersecurity, the responses were more evenly split. **53.3%** of respondents indicated that they were aware of CTFs, while **48.7%** were unfamiliar with the concept. This suggests a notable gap in knowledge regarding CTF as an educational and practical tool for developing cybersecurity skills. Given the hands-on, practical nature of CTF challenges, incorporating more exposure to CTFs could significantly enhance the educational experience and help bridge the gap for those unfamiliar with this learning method.

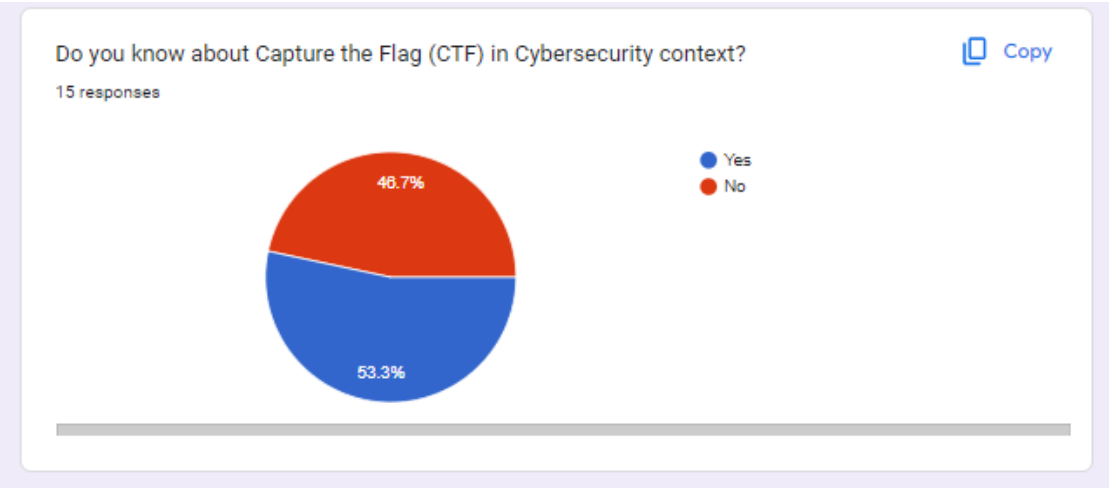


Figure 6.1.3: Questionnaire 3

The data shows that **73.3%** of the respondents have not participated in any CTF competitions before, while **26.7%** have. This indicates that there is a significant opportunity to introduce more students to CTF events, potentially improving engagement with cybersecurity learning through practical challenges. Despite limited participation, those who have been involved in CTFs highlighted key motivations for taking part. All respondents (100%) indicated that their primary motivation for participating in CTF challenges is to **learn new skills**, while **75%** also expressed interest in gaining **competition experience**. Notably, none of the respondents were driven by career opportunities, suggesting that their focus is more on the learning and experiential aspects of CTF competitions.

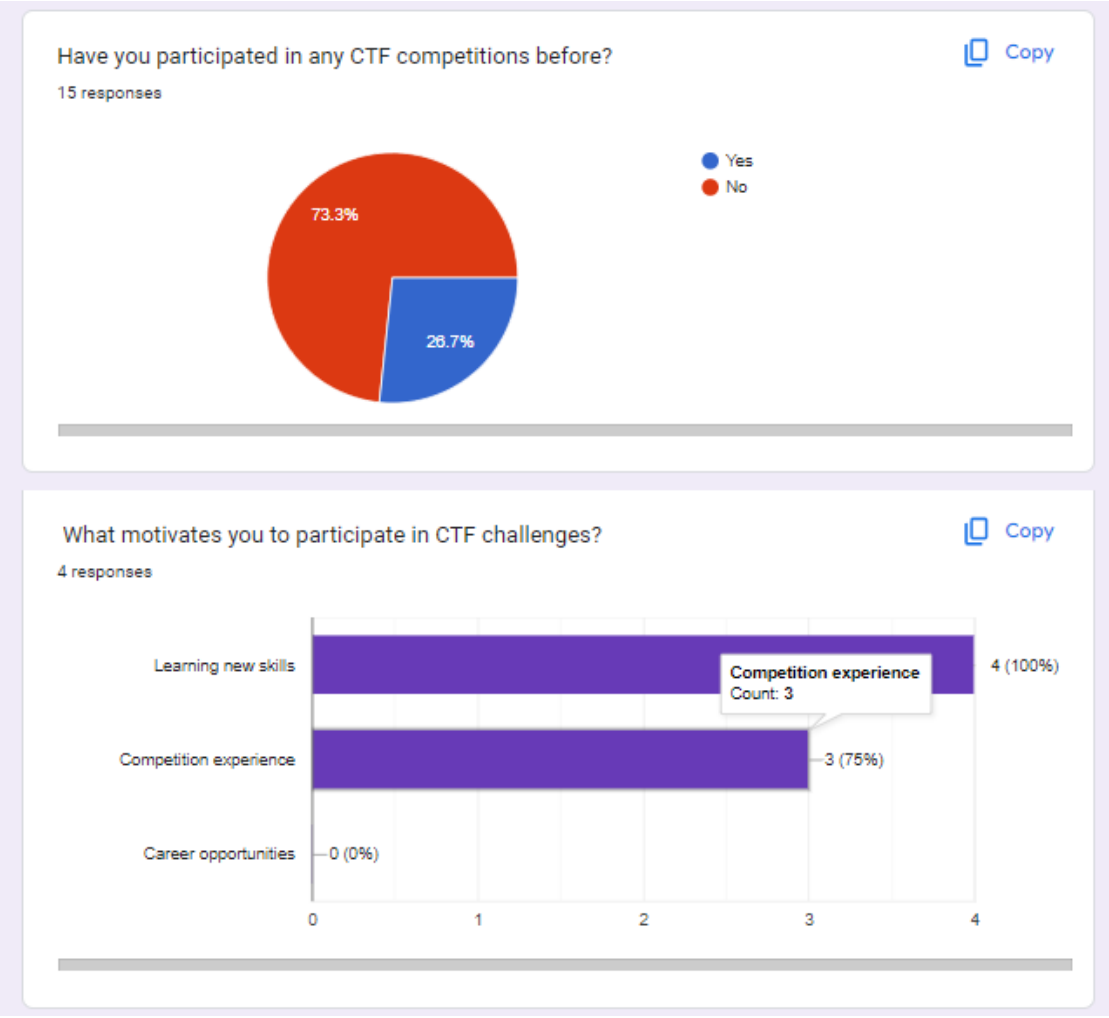


Figure 6.1.4: Questionnaire 4

Regarding the most challenging aspects of CTF competitions, the four responses provided a range of categories. Students found **Forensics**, **Cryptography**, **Binary Exploitation**, and **Reverse Engineering (PWN)** the most challenging categories. This indicates that students perceive difficulties in different technical areas of cybersecurity, highlighting the need for additional resources or focused training in these domains.

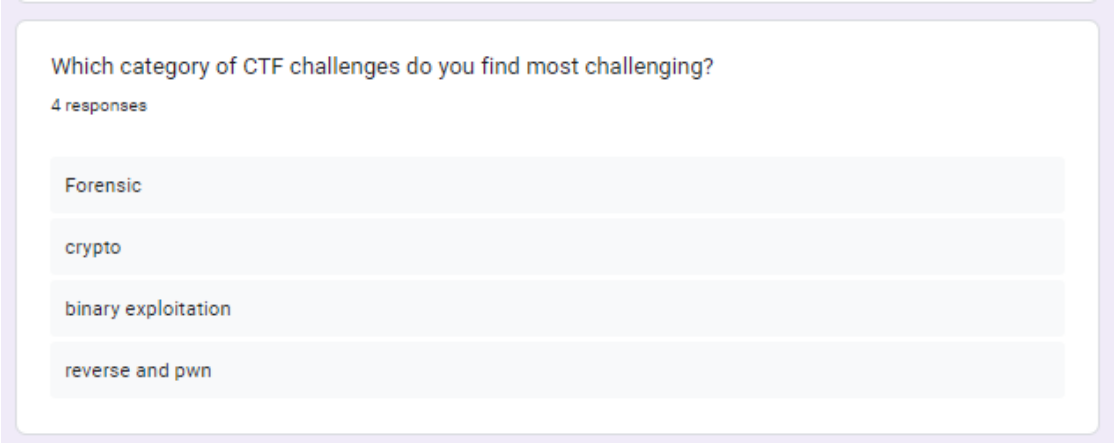


Figure 6.1.5: Questionnaire 5

Besides, students were asked how CTF challenges contribute to their understanding of cybersecurity concepts. Their responses emphasized the importance of hands-on learning. They noted that CTFs provide a better understanding through **practical work** and allow them to apply theoretical knowledge in real-world scenarios. Additionally, students valued the **hands-on experience** that CTF competitions offer and appreciated the opportunity to **practice and reinforce concepts**. Overall, CTF challenges are seen as a valuable tool for enhancing practical knowledge and bridging the gap between theory and application in cybersecurity education.

Figure 6.1.6: Questionnaire 6

When asked whether participants encountered any technical issues while using the UTAR CTF Guide platform, all 15 respondents unanimously reported no problems, with each answering "No." This is a positive indicator of the platform's reliability and user-friendliness, ensuring a smooth experience for users as they engage with CTF challenges and resources.

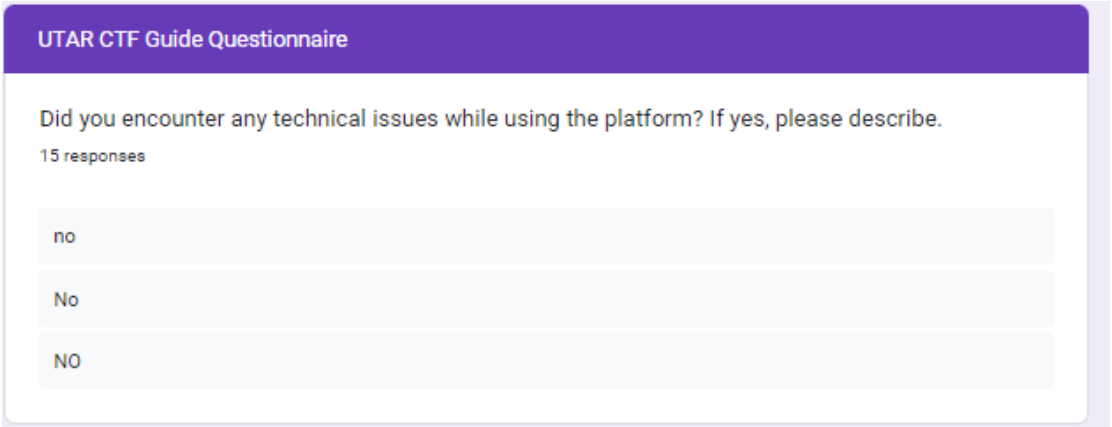


Figure 6.1.7: Questionnaire 7

All participants (100%) confirmed that they had used the guides and resources linked on the platform, demonstrating that users actively sought support and instructional materials to aid their understanding of CTF challenges. This highlights the importance of providing accessible, relevant resources as part of the learning experience. When asked how relevant and helpful they found the guides and resources, **60%** of respondents rated their usefulness as 4 out of 5, while **28.7%** rated them as 3 out of 5.

A smaller percentage (**6.7%**) rated the resources as 5 out of 5, indicating a high level of satisfaction with the materials. These results suggest that the guides were generally well-received and valuable, though there may still be room for enhancement to increase their helpfulness.

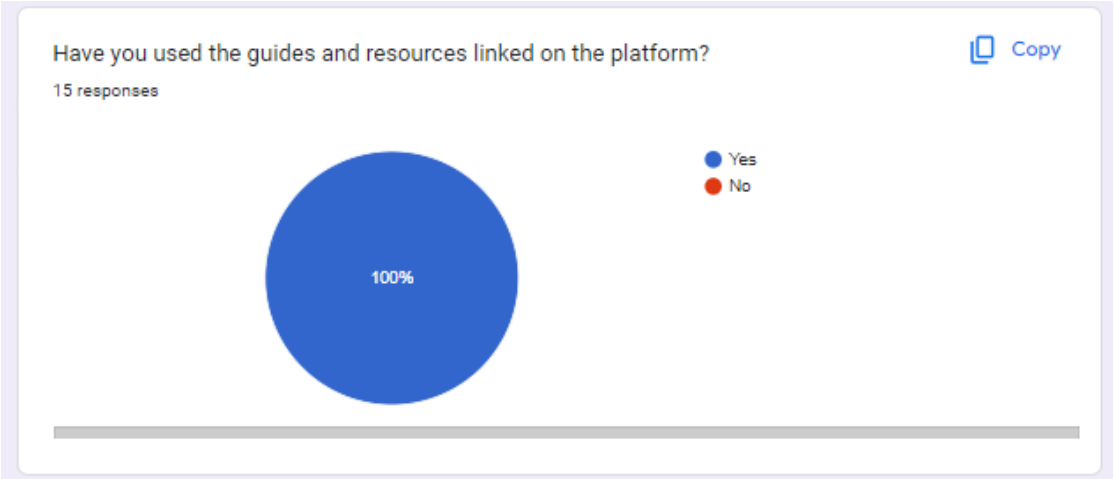


Figure 6.1.8: Questionnaire 8

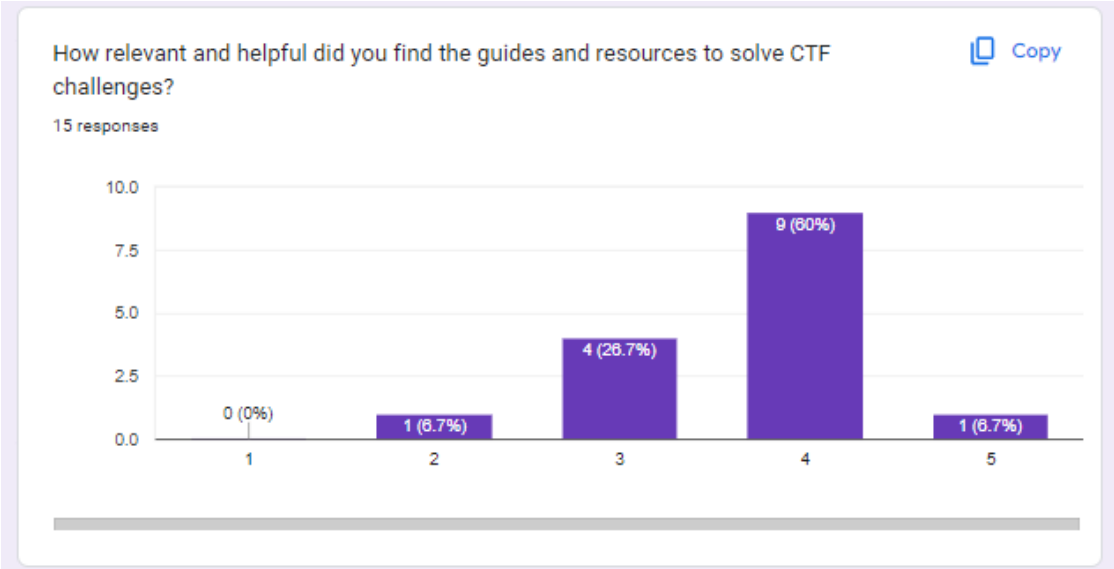


Figure 6.1.9: Questionnaire 9

Additionally, the survey asked about the participants' experience with external platforms like TryHackMe or PicoCTF, both popular for cybersecurity learning and CTF challenges. Once again, all respondents (100%) indicated that they had used these platforms.

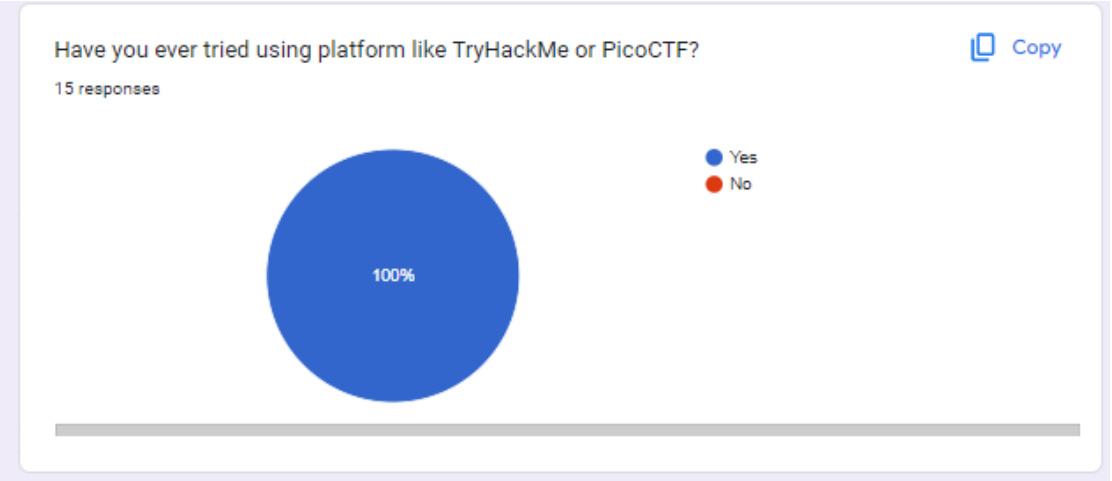


Figure 6.1.10: Questionnaire 10

When asked to compare the guides and resources on this platform with those on TryHackMe or PicoCTF, **60%** of respondents rated the resources as 4 out of 5 in terms of usefulness and ease of understanding, and **13.3%** rated them as 5 out of 5. However, **28.7%** rated the resources as 3 out of 5, indicating that while the majority found the resources helpful, there is room for improvement in making them more accessible or comprehensive compared to other platforms. These findings suggest that while the platform provides valuable resources, further enhancements could be made to match or exceed the quality of well-established platforms like TryHackMe or PicoCTF.

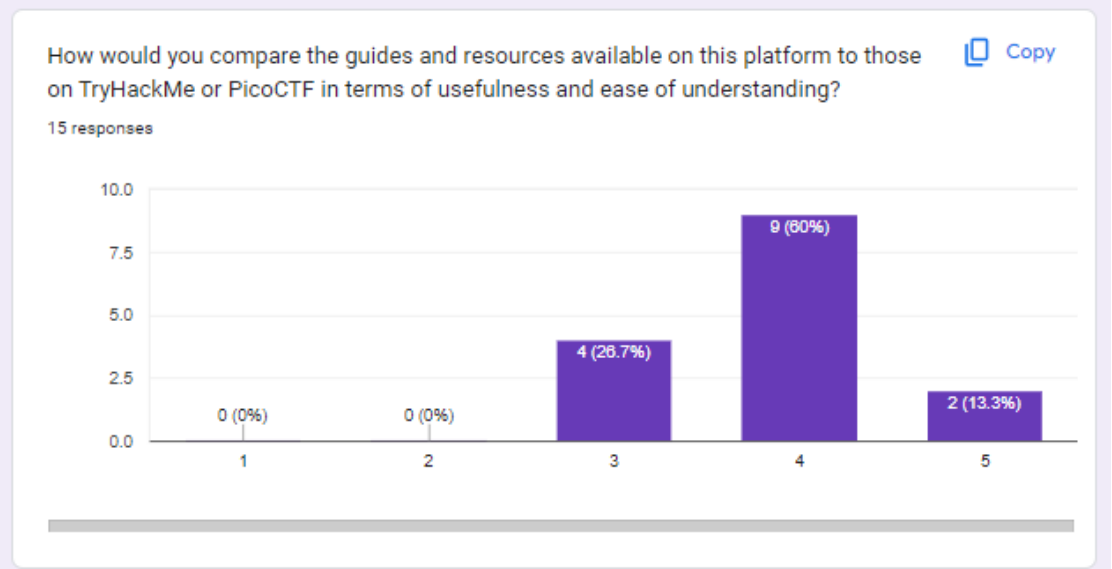


Figure 6.1.11: Questionnaire 11

Regarding the effectiveness of the platform in enhancing cybersecurity skills, **73.3%** of participants rated the platform's ability to improve their skills as 4 out of 5, while **28.7%** rated it as 5 out of 5. This high rating underscores the effectiveness of the platform in helping users develop practical cybersecurity competencies. There is clear evidence that participants feel their skills are being significantly enhanced through engagement with the platform and its challenges.

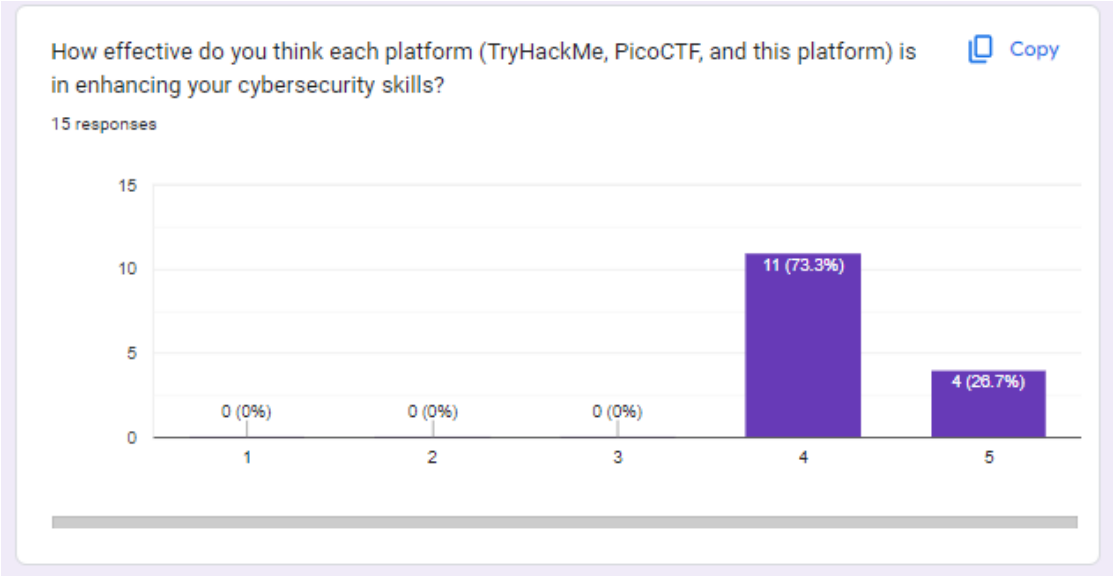


Figure 6.1.12: Questionnaire 12

In terms of the difficulty level of the challenges, most respondents (**60%**) rated the difficulty as 2 out of 5, suggesting that the challenges were perceived as somewhat easy. **13.3%** of participants rated the difficulty as 4, and another **6.7%** rated it as 5, indicating that a minority of participants found the challenges more demanding. These results suggest that while the platform offers a good entry point for beginners, more advanced or challenging tasks could be incorporated to better engage intermediate and advanced users.

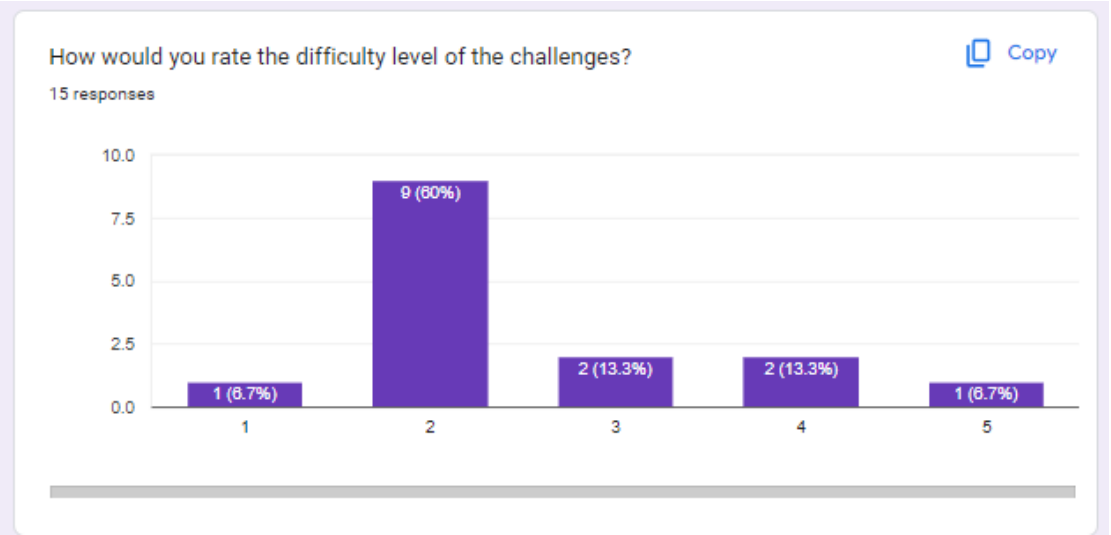


Figure 6.1.13: Questionnaire 13

Based on the feedback from participants regarding improvements to the guides and platform, several recurring themes have emerged. In summary, participants emphasized the need for web-related content and boot2root challenges to be improved and expanded, along with the introduction of harder cryptography challenges.

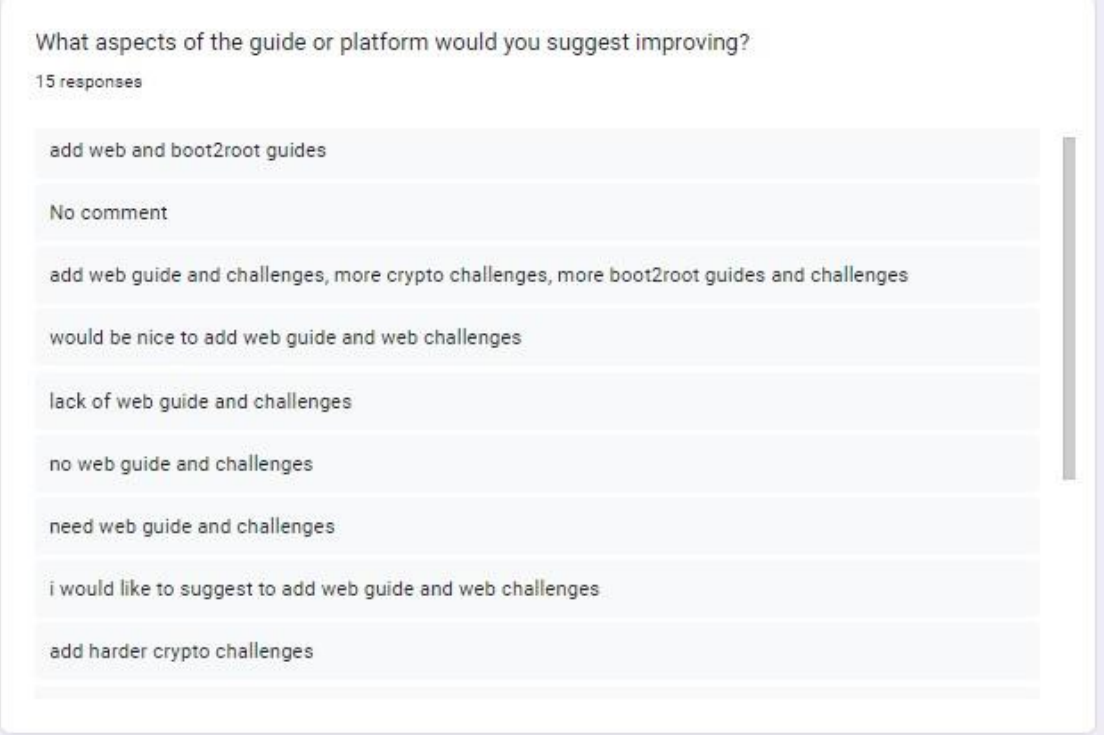


Figure 6.1.14: Questionnaire 14

6.2 Testing Setup and Result

In this section, test cases for each activity of the platform will be shown.

6.2.1 Connecting to CTFd

Table 6.2.1.1: Test case for connection to the platform

Test Case	Expected Result	Actual Result	Status (Pass/Failed)
Connecting to the CTFd Website via IP **34.87.51.217**	Successfully connected to the website.	Successfully connected to the website.	Pass

6.2.2 Register Activity on CTFd

Table 6.2.2.1: Test case for register activity

Test Case	Expected Result	Actual Result	Status (Pass/Failed)
During registration, intentionally leaving some of the fields empty	Show "Please fill out this field"	Show "Please fill out this field"	Pass
Sign up with invalid email address format (example: test)	Show "Please include an '@' in the email address. 'test' is missing an '@'	Show "Please include an '@' in the email address. 'test' is missing an '@'	Pass
Sign up with used email	Show "That email has already been used"	Show "That email has already been used"	Pass
Sign up with valid format	Redirect to "Team" and ask the user to "Join Team" or "Create Team"	Redirect to "Team" and ask the user to "Join Team" or "Create Team"	Pass

6.2.3 Login Activity on CTFd

Table 6.2.3.1: Test case for login activity

Test Case	Expected Result	Actual Result	Status (Pass/Failed)
Entering incorrect username or password	Show "Your username or password is incorrect"	Show "Your username or password is incorrect"	Pass
Entering correct credentials	Redirect to "Team" and ask the user to "Join Team" or "Create Team" if the user have not created or join a team.	Redirect to "Team" and ask the user to "Join Team" or "Create Team" if the user have not created or join a team.	Pass
Joining an existing team	Redirect to "Challenges" section	Redirect to "Challenges" section	Pass
Create a team	Redirect to "Challenges" section	Redirect to "Challenges" section	Pass

6.2.4 Main Activity on CTFd

Table 6.2.4.1: Test case for main activity

Test Case	Expected Result	Actual Result	Status (Pass/Failed)
User try downloading the challenge file	Successfully downloaded the challenge file	Successfully downloaded the challenge file	Pass
User enters wrong flag	Show “Incorrect”	Show “Incorrect”	Pass
User enters the correct flag	Show “Correct”	Show “Correct”	Pass
User try to solve the challenges that they already solved	Show “You already solved this”	Show “You already solved this”	Pass
User unlock hint	Prompt “Unlock Hint?” message box	Prompt “Unlock Hint?” message box	Pass
User press “No” during unlock hint	Redirect to the challenge that the user currently selected	Redirect to the challenge that the user currently selected	Pass
User press “Yes” during unlock hint	Show the hint	Show the hint	Pass
User click on the “Rules” link on the Main Page	Redirect to the rules of the platform	Redirect to the rules of the platform	Pass
User click on the “Learn” link on the Main Page	Redirect to the learning platform	Redirect to the learning platform	Pass

6.2.5 PWN Challenges on CTFd

Table 6.2.5.1: Test case for pwn challenges

Test Case	Expected Result	Actual Result	Status (Pass/Failed)
User accessing PWN challenges via netcat	Successfully connected	Successfully connected	Pass
User failed to exploit PWN challenges	Does not output the flag	Does not output the flag	Pass
User successfully solve and exploited the PWN challenges	Output the flag	Output the flag	Pass
User exit the remote connection	Successfully exited	Successfully exited	Pass

6.2.6 Boot2Root Challenges on CTFd

Table 6.2.6.1: Test case for boot2root challenge

Test Case	Expected Result	Actual Result	Status (Pass/Failed)
User accessing Boot2Root challenges via netcat	Successfully connected	Successfully connected	Pass
User can nmap and scan the port on the IP address in Boot2Root challenges	Show port 80, 8080 and port 22 running	Show port 80, 8080 and port 22 running	Pass
User can use the credentials for ctfplayer during ssh when solving Boot2Root challenges	Successfully connected as ctfplayer	Successfully connected as ctfplayer	Pass
User can view the log files to solve Boot2Root challenge	Show the flag	Show the flag	Pass
User exit the remote connection	Successfully exited	Successfully exited	Pass

6.2.7 Admin Activity on CTFd

Table 6.2.7.1: Test case for admin activity

Test Case	Expected Result	Actual Result	Status (Pass/Failed)
Admin create and add challenges	Successfully added the challenges	Successfully added the challenges	Pass
Admin delete user	Selected user will be deleted	Selected user will be deleted	Pass
Admin hide scoreboard	Successfully hide scoreboard	Successfully hide scoreboard	Pass
Admin modify the content of the platform	Successfully modifies the content of the platform	Successfully modifies the content of the platform	Pass
Admin add notification	Successfully added notifications	Successfully added notifications	Pass
Admin delete and modify challenges	Successfully delete and modify challenges	Successfully delete and modify challenges	Pass

6.3 Project Challenges

One of the main challenges encountered during the project was the difficulty in implementing remote connections via GCP. Establishing secure and reliable remote access required configuring firewalls, which often posed complications. The process involved setting up appropriate firewall rules to allow access while ensuring that the system remained secure, which proved to be time-consuming and complex, especially for those unfamiliar with GCP's networking configurations.

Additionally, another significant challenge was the difficulty in configuring GCP resources due to outdated or inconsistent documentation. Many GCP resources used in the project did not have up-to-date guides, making it harder to follow instructions and implement solutions efficiently.

Another challenge faced during the project was the difficulty in implementing dynamic flags to prevent and catch cheating in the CTF environment. Dynamic flag generation requires the system to generate unique flags for each participant or team in real-time, ensuring that no two flags are identical. This complexity adds an additional layer of security, but implementing this feature was technically challenging due to the need for precise synchronization between the flag generation system and the scoreboard. Furthermore, ensuring that flags could not be easily intercepted or shared among teams without detection required advanced monitoring mechanisms, which proved to be difficult to configure effectively.

6.4 Objective Evaluation

Table 6.4.1: Objective Evaluation

Objective	Evaluation	Conclusion
To propose and develop an educational framework that enhances the cybersecurity competencies of students at UTAR	The system provides students with a structured learning approach to develop and improve their cybersecurity skills	Achieved
To make cybersecurity learning accessible and engaging for students of all expertise levels	The survey indicates that even students without a background in IT were able to successfully solve some of the challenges	Achieved
To bridge the gap between theoretical knowledge and practical application by enabling students to apply learned concepts in real-world scenarios	The UTAR CTF Guide platform demonstrates that students were able to apply theoretical knowledge to solve challenges, reflecting real-world cybersecurity scenarios	Achieved

6.5 Concluding Remark

The development of the UTAR CTF Guide has effectively met its primary objectives by providing an essential tool that seamlessly integrates theoretical knowledge with practical cybersecurity skills. By incorporating recognized industry technologies and advanced educational methodologies, the platform not only enhances student engagement but also prepares them comprehensively for challenges they will encounter in the cybersecurity field.

This platform has proven its utility by offering features that simulate real-world cybersecurity scenarios to allow students to develop and refine their problem-solving and technical skills in a controlled environment. The implementation of Docker for secure and isolated challenge environments, alongside the scalable architecture provided by Google Cloud Platform ensures that the system remains both flexible and powerful. Furthermore, the continuous integration of programming tools and environments supports an iterative learning process, encouraging students to learn and adapt continuously.

CHAPTER 7

7.1 Conclusion

In conclusion, this project reflects a comprehensive effort to enhance cybersecurity education through the development of a tailored CTF guide for students at UTAR. This initiative not only delivered a dynamic educational platform by featuring a wide array of cybersecurity challenges but also addressed the gap between theoretical knowledge and practical application. The platform includes various levels of challenges, from basic to advanced, ensuring accessibility and continuous learning for all students irrespective of their initial expertise.

Throughout the development process, several key challenges were tackled, particularly in customizing the CTFd platform to suit specific educational goals and in crafting intricate challenges that simulate real-world cybersecurity scenarios. The resolution of these challenges highlighted the success of the project in creating a robust, user-friendly learning environment that fosters both skill development and deep engagement with cybersecurity practices. The impact of this project extends beyond immediate educational benefits by contributing valuable insights to the field of cybersecurity education and showcasing effective methods for integrating practical cybersecurity exercises into academic curricula. These contributions are anticipated to inspire further research and adoption of similar educational frameworks elsewhere which reinforcing the importance of hands-on experience in technical education.

The project is set to expand the scope of challenges and enhance the platform's features to keep pace with the latest cybersecurity developments. Future enhancements will focus on increasing the platform's adaptability and scalability to meet the emerging needs of a broader learner base. This development underscores the project's commitment to providing enduring value to UTAR students and the academic community at large which ultimately aiming to cultivate a well-informed and technically proficient generation of cybersecurity professionals.

7.2 Recommendation

Based on the survey, while the current CTFd learning platform is designed primarily for beginners, it is recommended to introduce a more diverse range of challenges to cater to intermediate and advanced users as well. By expanding the challenge difficulty levels, users can progressively build their skills, making the platform more appealing and beneficial for a wider audience.

One key recommendation is to add harder challenges across various categories, particularly in areas such as PWN, cryptography and reverse engineering. These advanced challenges would help students push their limits and apply the foundational skills they have gained from the beginner-level tasks. Introducing a tiered difficulty system will allow users to challenge themselves as they improve and keep them engaged with new learning opportunities.

In addition to this, it is recommended to integrate web-based challenges. Web security is an essential part of cybersecurity education, and adding challenges related to common vulnerabilities, such as SQL injection, cross-site scripting (XSS) and remote code execution, would provide valuable real-world scenarios. Coupling these challenges with a comprehensive web security guide will help users understand the intricacies of web attacks and defenses.

Another recommendation is to expand the platform's cryptography challenges. While there may already be some beginner-level tasks, adding more advanced cryptographic puzzles such as those involving public-key encryption, cryptanalysis or modern cryptographic algorithms will further develop the students' understanding of how encryption works and how it can be exploited in a controlled learning environment.

Including additional boot2root challenges is also highly recommended. These challenges provide full-system exploitation practice, where users start from basic user-level access and escalate their privileges to root. Such scenarios provide a practical, hands-on approach to learning about system vulnerabilities and are invaluable for those looking to enhance their ethical hacking skills.

Moreover, it would be recommended to implement the dynamic flags to prevent and catch cheating in CTF. This is to ensure no two flags are identical whenever participants are solving challenges that require remote connections.

Lastly, it would be beneficial to expand the educational resources. Adding a comprehensive web security guide and a complete reverse engineering guide would give students the necessary foundational knowledge to tackle the more challenging exercises.

REFERENCES

[1] V. Švábenský, P. Čeleda, J. Vykopal, and S. Brišáková, “Cybersecurity knowledge and skills taught in capture the flag challenges,” Computers & Security, vol. 102, p. 102154, Mar. 2021, doi: 10.1016/j.cose.2020.102154.

[2] L. McDaniel, E. Talvi and B. Hay, "Capture the Flag as Cyber Security Introduction," 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 2016, pp. 5479-5486, doi: 10.1109/HICSS.2016.677.

[3] I. Ortiz-Garces, R. Gutierrez, D. Guerra, S. Sanchez-Viteri, and W. Villegas-Ch., “Development of a Platform for Learning Cybersecurity Using Capturing the Flag Competitions,” *Electronics*, vol. 12, no. 7, p. 1753, Apr. 2023, doi: https://doi.org/10.3390/electronics12071753.

[4] A. H. A. Hanafi, H. Rokman, A. D. Ibrahim, Z.-A. Ibrahim, M. N. A. Zawawi, and F. A. Rahim, “A CTF-Based Approach in Cyber Security Education for Secondary School Students,” *electronic Journal of Computer Science and Information Technology*, vol. 7, no. 1, Oct. 2021, doi: https://doi.org/10.52650/ejcsit.v7i1.107.

[5] A. Mansurov, “A CTF-Based Approach in Information Security Education: An Extracurricular Activity in Teaching Students at Altai State University, Russia,” *Modern Applied Science*, vol. 10, no. 11, p. 159, Aug. 2016, doi: https://doi.org/10.5539/mas.v10n11p159.

[6] G. Costa, M. Lualdi, M. Ribaudo, and A. Valenza, “A NERD DOGMA,” Oct. 2020, doi: https://doi.org/10.1145/3368308.3415405.

[7] Q. Yan, W. Lai and Z. Wang, "Online Experiments Based on the CTF Model for Information Security MOOC Courses," *2021 16th International Conference on Computer Science & Education (ICCSE)*, Lancaster, United Kingdom, 2021, pp. 783-788, doi: 10.1109/ICCSE51940.2021.9569691.

[8] J. Werther, M. Zhivich, T. Leek, and Nickolai Zeldovich, “Experiences in cyber security education: the MIT Lincoln laboratory capture-the-flag exercise,” *USENIX Security Symposium*, pp. 12–12, Aug. 2011.

[9] P. Chapman and D. Brumley, “picoCTF: Teaching 10,000 High School Students to Hack Preliminary Report,” 2013. Accessed: Sep. 12, 2024. [Online]. Available: https://picoctf.org/pdfs/picoCTF_report_June_2013.pdf

[10] “TryHackMe,” *TryHackMe*. https://tryhackme.com/r/about

[11] “All About Hack The Box,” *Hack The Box*. https://www.hackthebox.com/about-us

[12] “SKR CTF,” *Skrctf.me*, 2018. https://skrctf.me/about#:~:text=We%20are%20CTF%20team%20from (accessed Sep. 12, 2024).

[13] D. Kuhn, C. Kim, and B. Lopuz, “Chapter 12: VirtualBox for Oracle,” in *Apress eBooks*, 2015, pp. 325–344. doi: 10.1007/978-1-4842-1254-7_12.

[14] R. Rohleder, “Hands-On Ghidra - A Tutorial about the Software Reverse Engineering Framework,” *SPRO’19: Proceedings of the 3rd ACM Workshop on Software Protection*, Nov. 2019, doi: 10.1145/3338503.3357725.

[15] “What is Docker?,” *Docker Documentation*, 2024. https://docs.docker.com/get-started/docker-overview/

[16] “CS107 Compiling C Programs with GCC,” *Stanford.edu*, 2024. https://web.stanford.edu/class/archive/cs/cs107/cs107.1202/resources/gcc (accessed Sep. 12, 2024).

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: 4, 1	**Study week no.: 8**
Student Name & ID: Ang Boon Keat 20ACB03822	
Supervisor: Puan Nor' Afifah Binti Sabri	
Project Title: A Comprehensive Capture The Flag Guide For UTAR Students	

1. WORK DONE

[Please write the details of the work done in the last fortnight.]

Show the overall progress on the project.

2. WORK TO BE DONE

Finalizing the development.

3. PROBLEMS ENCOUNTERED

No problem encountered.

4. SELF EVALUATION OF THE PROGRESS

Overall, the progress is going well.

Supervisor's signature

Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: 4, 1	**Study week no.: 10**
Student Name & ID: Ang Boon Keat 20ACB03822	
Supervisor: Puan Nor' Afifah Binti Sabri	
Project Title: A Comprehensive Capture The Flag Guide For UTAR Students	

1. WORK DONE

[Please write the details of the work done in the last fortnight.]

Completed the development on the project.

2. WORK TO BE DONE

Continue to finish the Chapter 3 and 5 of the report.

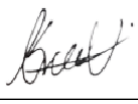
3. PROBLEMS ENCOUNTERED

No problem encountered.

4. SELF EVALUATION OF THE PROGRESS

Overall, the progress is going well.

Supervisor's signature



Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: 4, 1	**Study week no.: 11**
Student Name & ID: Ang Boon Keat 20ACB03822	
Supervisor: Puan Nor' Afifah Binti Sabri	
Project Title: A Comprehensive Capture The Flag Guide For UTAR Students	

1. WORK DONE

[Please write the details of the work done in the last fortnight.]

Completed Chapter 3 and 5 of the report.

2. WORK TO BE DONE

Continue to write chapter 6 of the report.

3. PROBLEMS ENCOUNTERED

No problem encountered.

4. SELF EVALUATION OF THE PROGRESS

Overall, the progress is going well.

Supervisor's signature

Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: 4, 1	**Study week no.: 12**
Student Name & ID: Ang Boon Keat 20ACB03822	
Supervisor: Puan Nor' Afifah Binti Sabri	
Project Title: A Comprehensive Capture The Flag Guide For UTAR Students	

1. WORK DONE

[Please write the details of the work done in the last fortnight.]

Completed half of the progress on Chapter 6.

2. WORK TO BE DONE

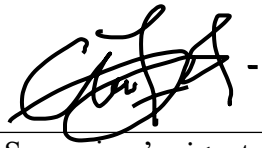
Find participants to test the project.

3. PROBLEMS ENCOUNTERED

No problem encountered.

4. SELF EVALUATION OF THE PROGRESS

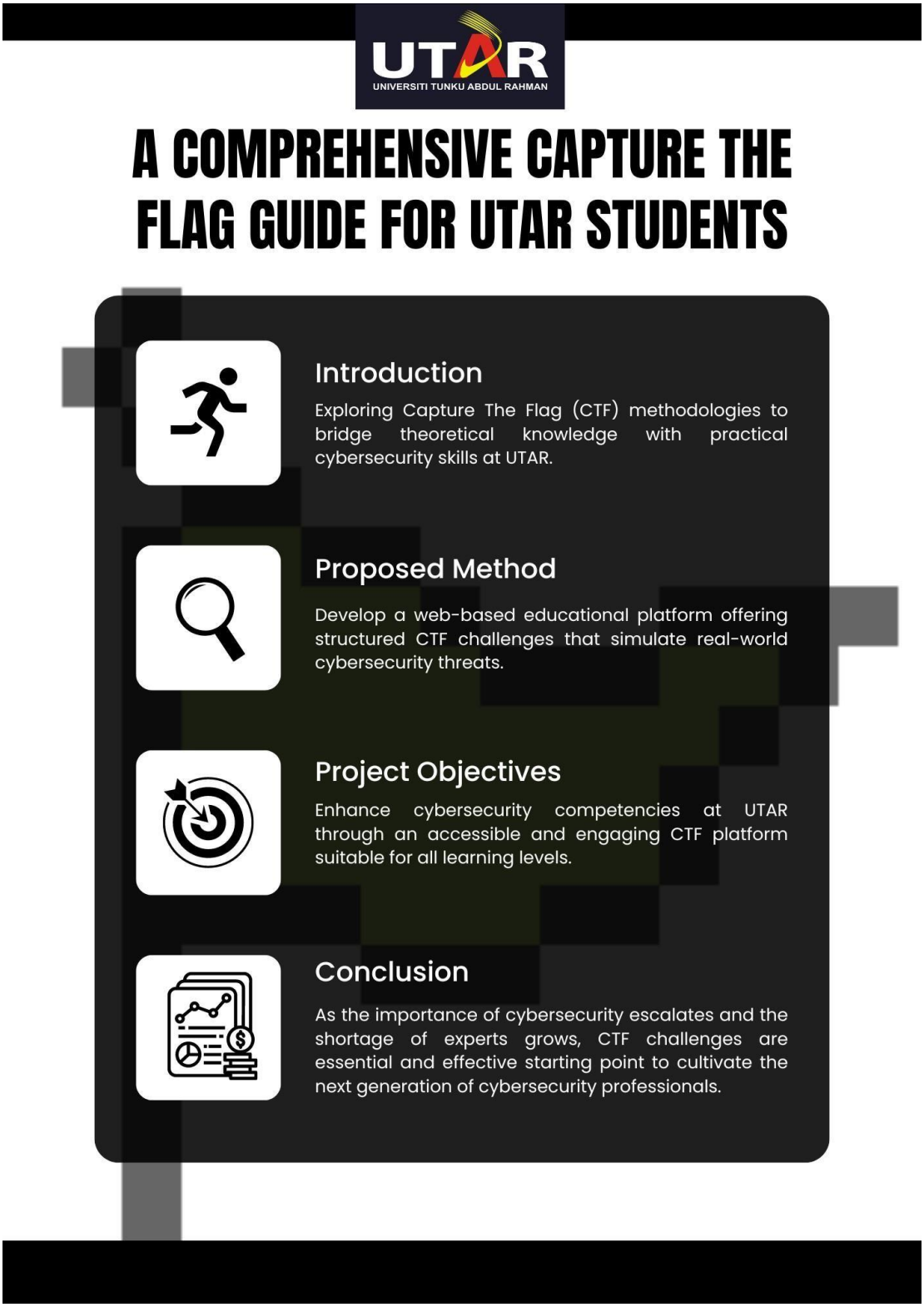
Overall, the progress is going well.



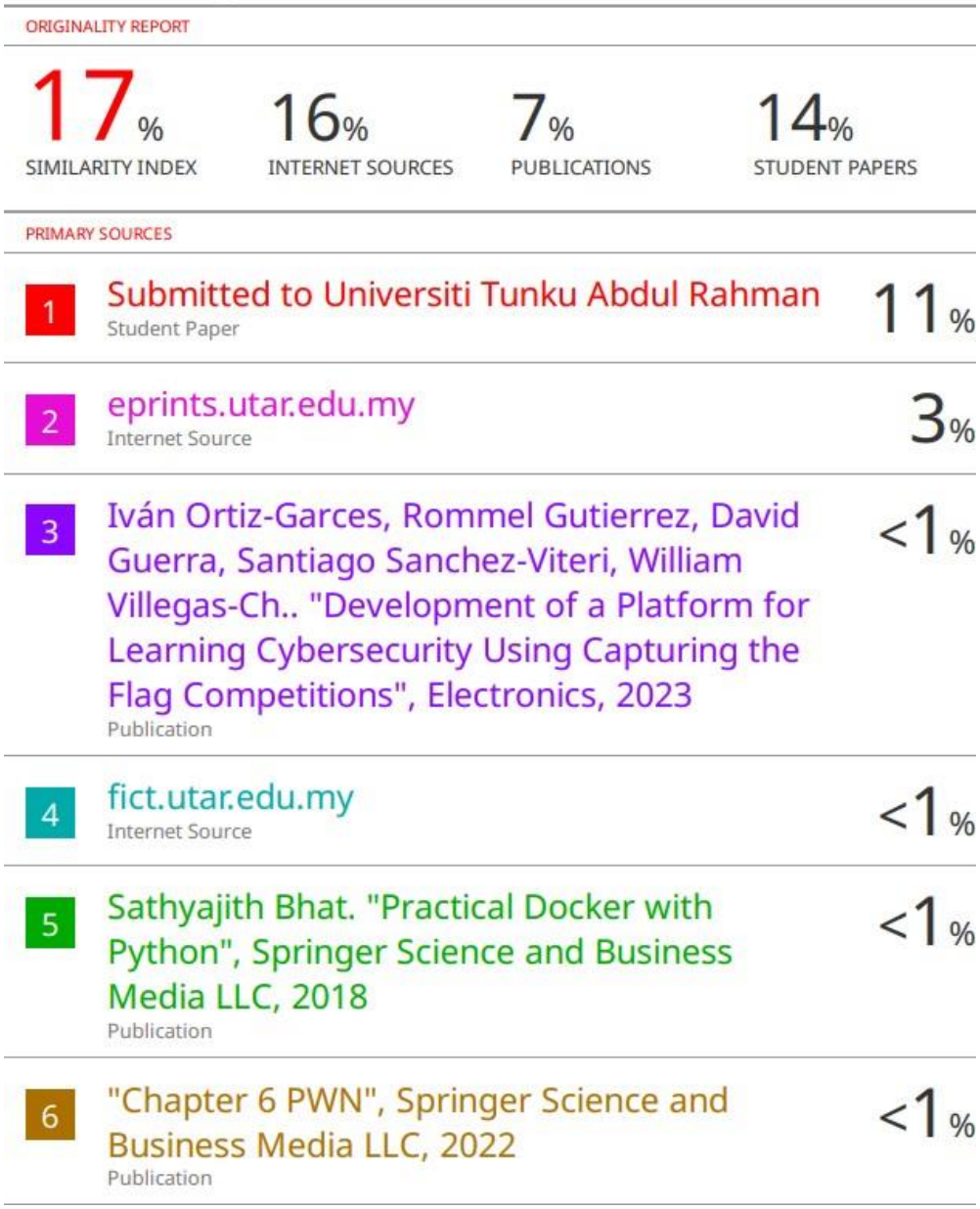
Supervisor's signature

Student's signature

POSTER


UTAR
UNIVERSITI TUNKU ABDUL RAHMAN
A COMPREHENSIVE CAPTURE THE FLAG GUIDE FOR UTAR STUDENTS
Introduction
Exploring Capture The Flag (CTF) methodologies to bridge theoretical knowledge with practical cybersecurity skills at UTAR.
Proposed Method
Develop a web-based educational platform offering structured CTF challenges that simulate real-world cybersecurity threats.
Project Objectives
Enhance cybersecurity competencies at UTAR through an accessible and engaging CTF platform suitable for all learning levels.
Conclusion
As the importance of cybersecurity escalates and the shortage of experts grows, CTF challenges are essential and effective starting point to cultivate the next generation of cybersecurity professionals.

PLAGIARISM CHECK RESULT



ORIGINALITY REPORT

17%	16%	7%	14%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universiti Tunku Abdul Rahman Student Paper	11%
2	eprints.utar.edu.my Internet Source	3%
3	Iván Ortiz-Garces, Rommel Gutierrez, David Guerra, Santiago Sanchez-Viteri, William Villegas-Ch.. "Development of a Platform for Learning Cybersecurity Using Capturing the Flag Competitions", Electronics, 2023 Publication	<1%
4	fict.utar.edu.my Internet Source	<1%
5	Sathyajith Bhat. "Practical Docker with Python", Springer Science and Business Media LLC, 2018 Publication	<1%
6	"Chapter 6 PWN", Springer Science and Business Media LLC, 2022 Publication	<1%

7	Julien Favreau, Julio Mercader. "Lithic Raw Material Characterisation at Olduvai Gorge, Tanzania", Open Science Framework, 2019 Publication	<1 %
8	Jonnathan Berrezueta-Guzman, Markus Paulsen, Stephan Krusche. "Plagiarism Detection and its Effect on the Learning Outcomes", EdArXiv, 2023 Publication	<1 %
9	Lee Chao. "Virtualization and Private Cloud withVMware Cloud Suite", Routledge, 2017 Publication	<1 %
10	Dzakwan Al Dzaky Bewasana, Muhammad Sofyan Arif Harumnanda, Dimas Febriyan Priambodo. "Securing Networks with Port Knocking: An Experimental Study on Ubuntu and Kali", 2023 3rd International Conference on Electronic and Electrical Engineering and Intelligent System (ICE3IS), 2023 Publication	<1 %
11	"Information Security Education. Information Security in Action", Springer Science and Business Media LLC, 2020 Publication	<1 %
12	Daniele Antonioli, Hamid Reza Ghaeini, Sridhar Adepu, Martin Ochoa, Nils Ole Tippenhauer. "Gamifying ICS Security Training	<1 %

	and Research", Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy - CPS '17, 2017 Publication	
13	Shimon Ifrah. "Getting Started with Containers in Google Cloud Platform", Springer Science and Business Media LLC, 2021 Publication	<1 %
14	Vinicius Ramos Apolinario. "Windows Containers for IT Pros", Springer Science and Business Media LLC, 2021 Publication	<1 %
15	Pawan Singh Mehra, Dhirendra Kumar Shukla. "Artificial Intelligence, Blockchain, Computing and Security - Volume 2", CRC Press, 2023 Publication	<1 %
16	R Geller. "Electron Cyclotron Resonance Ion Sources and ECR Plasmas", CRC Press, 2018 Publication	<1 %
17	"Corruption risks of Hungarian municipalities: Quantitative and Qualitative Analyses", Corvinus University of Budapest, 2023 Publication	<1 %
18	Fernando Hoces de la Guardia. "How Transparency and Reproducibility Can Increase Credibility in Policy Analysis: A Case	<1 %

Study of the Minimum Wage Policy Estimate", MetaArXiv, 2017
Publication

19	Frank Melendez, Nancy Diniz, Marcella Del Signore. "Data, Matter, Design - Strategies in Computational Design", Routledge, 2020 Publication	<1 %
20	Kopp, David M.. "Human Resource Development: Performance Through Learning, Second Edition", UAGC, 2023 Publication	<1 %
21	Zachary Romano, Jennifer Windsor, Mathew VanDerPol, Joel Coffman. "Election Security in the Cloud: A CTF Activity to Teach Cloud and Web Security", 2021 IEEE Frontiers in Education Conference (FIE), 2021 Publication	<1 %
22	Allen Tucker, Ralph Morelli, Chamindra de Silva. "Software Development - An Open Source Approach", CRC Press, 2019 Publication	<1 %
23	Giuseppe Mancia, Guido Grassi, Konstantinos P. Tsioufis, Anna F. Dominiczak, Enrico Agabiti Rosei. "Manual of Hypertension of the European Society of Hypertension", CRC Press, 2019 Publication	<1 %

PLAGIARISM CHECK RESULT

Form Title: Supervisor's Comments on Originality Report Generated by Turnitin for Submission of Final Year Project Report (for Undergraduate Programmes)			
Form Number: FM-IAD-005	Rev No.: 0	Effective Date:	Page No.: 1of 1

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

Full Name(s) of Candidate(s)	Ang Boon Keat
ID Number(s)	2003822
Programme / Course	CN
Title of Final Year Project	A Comprehensive Capture The Flag Guide For UTAR Students

Similarity	**Supervisor's Comments (Compulsory if parameters of originality exceed the limits approved by UTAR)**
Overall similarity index: 17 % **Similarity by source** Internet Sources: 16 % Publications: 7 % Student Papers: 14 %	Everything has been checked. All good.
Number of individual sources listed of more than 3% similarity: 2	Everything has been checked. All good.
Parameters of originality required, and limits approved by UTAR are as Follows: **(i) Overall similarity index is 20% and below, and** **(ii) Matching of individual sources listed must be less than 3% each, and** **(iii) Matching texts in continuous block must not exceed 8 words** ***Note: Parameters (i) – (ii) shall exclude quotes, bibliography and text matches which are less than 8 words.***	

Note: Supervisor/Candidate(s) is/are required to provide softcopy of full set of the originality report to Faculty/Institute

Based on the above results, I hereby declare that I am satisfied with the originality of the Final Year Project Report submitted by my student(s) as named above.

Signature of Supervisor

Name: Nor' Afifah Binti Sabri

Date: 12/9/2024

Signature of Co-Supervisor

Name: _____

Date: _____

FYP 2 CHECKLIST

UNIVERSITI TUNKU ABDUL RAHMAN

FACULTY OF INFORMATION & COMMUNICATION TECHNOLOGY (KAMPAR CAMPUS)

CHECKLIST FOR FYP1 THESIS SUBMISSION

Student ID	20ACB03822
Student Name	Ang Boon Keat
Supervisor Name	Puan Nor' Afifah Binti Sabri

TICK (√)	DOCUMENT ITEMS Your report must include all the items below. Put a tick on the left column after you have checked your report with respect to the corresponding item.
√	Title Page
√	Signed form of the Declaration of Originality
√	Acknowledgment
√	Abstract
√	Table of Contents
√	List of Figures (if applicable)
√	List of Tables (if applicable)
	List of Symbols (if applicable)
√	List of Abbreviations (if applicable)
√	Chapters / Content
√	Bibliography (or References)
√	All references in bibliography are cited in the thesis, especially in the chapter of literature review
√	Appendices (if applicable)
√	Poster
√	Signed Turnitin Report (Plagiarism Check Result – Form Number: FM-IAD-005)
√	I agree 5 marks will be deducted due to incorrect format, declare wrongly the ticked of these items, and/or any dispute happening for these items in this report.

*Include this form (checklist) in the thesis (Bind together as the last page)

I, the author, have checked and confirmed all the items listed in the table are included in my report.

(Signature of Student)
Date: 20/08/2024