Azerbaijan Cybersecurity Center | QuantumCTF

CAPSTONE PROJECT REPORT

CAPTURE THE FLAG POWERED BY CYWARIA

Prepared by :
GROUP_1

Prepared for :
Azerbaijan Cybersecurity Center

cywariactf@gmail.com

Table of Contents

Table of Contents 2

Table of Contents

1.0 Executive Summary 3
1.1 Projective Objectives 4
1.2 Scope and introduction to CTF 4
1.3 Easy Level Challenge Description 5
1.4 Medium Challenge Description 6
1.5 Hard Level Challenge Description 6
2.0 Literature review and reference to sources used 8
3.0 Project Plan Reflection 8
3.1 Time Management and obstancles 9
3.2 Areas for Improvement 9
4.0 Personal Reflection 10
4.1 Technical Learning and Tools 10
4.2 Methodology and Process 10
4.3 Areas for Improvement 10
5.0 Practical Application and Future Directions 11
6.0 Objectives of Project 12
7.0 Pie Chart format of Quantum Challenges 12

1.0 Project Introduction

Executive Summary

This reports present the final Capstone Project which contains the steps of CTF challenge which is called QuantumCTF and was prepared on Cywaria. This report details the experience and outcomes of the Cywaria Capture The Flag (CTF) competition, which featured 18 challenges centered around the creation and implementation of shellcode. The primary objective of the competition was to develop practical skills to solve the challenges and find the flags to cross the next step , a critical component in cybersecurity for executing arbitrary commands on target systems. Participants engaged in a series of challenges designed to test their understanding of shellcode generation, memory management, and some techniques across various architectures and operating systems. Each challenge presented unique scenarios, from basic buffer overflows to advanced exploitation techniques. Cywaria CTF provided a valuable platform for honing skills in shellcode development, fostering innovation in find the flag techniques which required the logic and promoting knowledge sharing among cybersecurity enthusiasts. The insights gained from this experience are crucial for advancing both individual proficiency and collective capabilities in defending against and mitigating cyber threats.

SME Technical Report on Cywaria CTF Challenges

This SME technical report delves into the intricacies of the Cywaria Capture The Flag (CTF) challenges, specifically focusing on the development and implementation of shellcode across 14 distinct scenarios and in easy , medium and hard levels. The report synthesizes findings from participants' approaches to ctf and find the all flags to finish the challenges.

Key insights from the report highlight the varied strategies employed by participants to address challenges ranging from basic buffer overflows to advanced memory exploitation techniques. The analysis underscores the importance of real-world applicability and practical skill development in cybersecurity education and training environments. CTF challenges often involve using various tools in the terminal to find the flag, making the process more challenging and intellectually stimulating. This approach not only tests technical skills but also encourages participants to think deeply and logically.

1.1 Project Objectives

Difficulty Level	Description and explanation of steps
Easy	These challenges are designed to introduce participants to fundamental concepts in cybersecurity, including file analysis, steganography, basic cryptography, and data manipulation techniques. They serve as a foundational step in developing skills necessary for more advanced cybersecurity challenges.
Medium	The medium part of the ***QuantumCTF*** challenge is designed to provide participants with a moderately complex yet engaging series of tasks. These tasks focus on key cybersecurity skills including brute force attacks, encoding techniques, and navigating maze-like directory structures. Each task builds on foundational knowledge and requires practical application of various tools and methodologies.
High	The ***QuantumCTF*** hard part is a comprehensive test of participants' technical capabilities, from steganography and directory traversal to archive extraction, HTML analysis, and brute-force attacks. Each step builds upon the previous one, culminating in a satisfying and rewarding experience for those who successfully navigate the challenge.

1.2 Scope and Introduction CTF

Capture the Flag (CTF) competitions are a popular and engaging way to develop and test cybersecurity skills in a simulated environment. Due to That we decide to eploy our CTF into the Cywaria platform. These events are designed to mimic real-world scenarios and challenges that cybersecurity professionals encounter in their daily work. CTFs are commonly used in educational settings, corporate training programs, and competitive events to foster learning, teamwork, and practical experience in the field of cybersecurity.

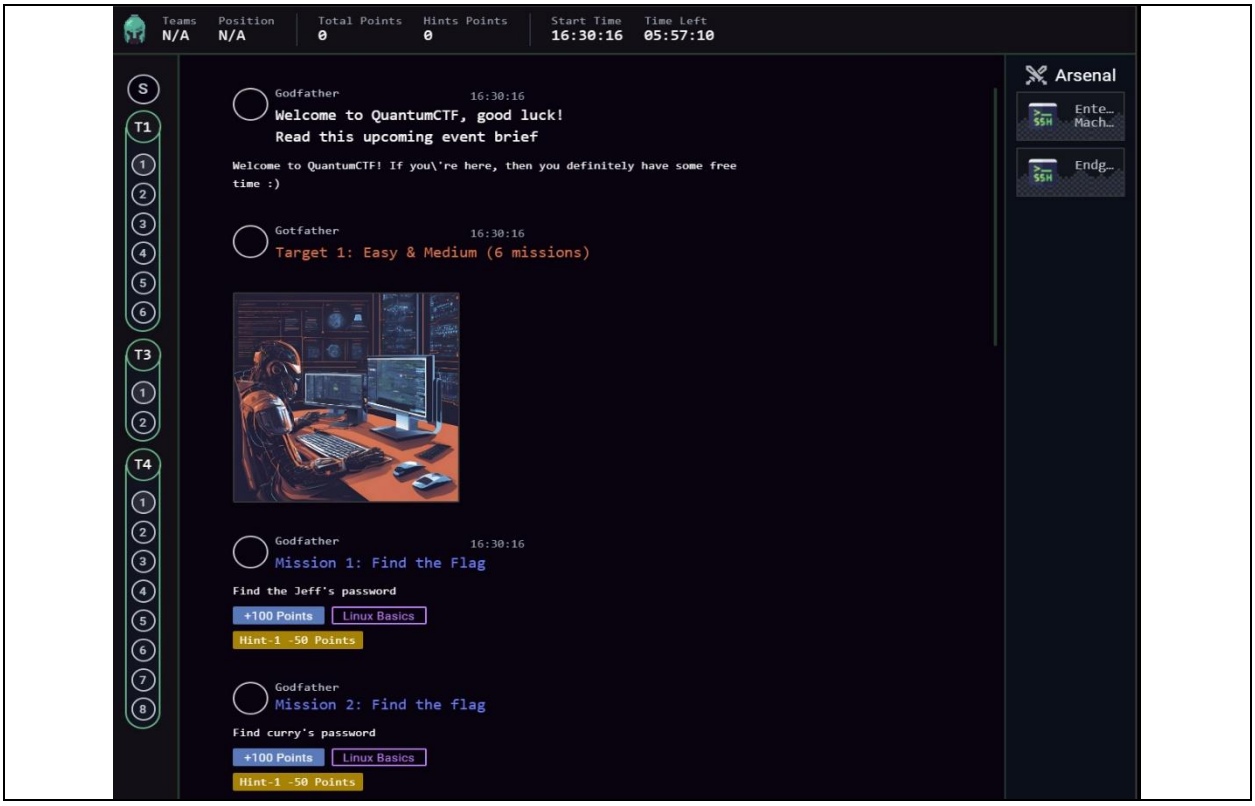
Scope of the CTF

The scope of this CTF competition encompasses a diverse range of cybersecurity challenges designed to test participants' skills in multiple areas. These challenges are crafted to simulate real-world security issues and scenarios, providing a comprehensive learning experience. The specific areas covered in this CTF include:

According to that we decided to add some challenges such as we will talk about them which will be more comprehensively . And all Tiers' theme will be displayed at the below

1.3 Easy Level Challenges Explanation Comprehensively

- **CTF Archive:** Participants are tasked with extracting hidden flags or information from archived files (e.g., ZIP, RAR) using basic file extraction techniques
- **Find Obfuscated Name:** Participants need to identify and decode obfuscated names or strings within files or source code. This challenge focuses on basic understanding of obfuscation techniques.
- **Maze:** In this challenge, participants navigate through a virtual maze to find and extract the hidden flag located at the endpoint of the maze.
- **Sort, Find Unique, Encoded Text, and Decode:** This challenge involves sorting data, finding unique elements, identifying encoded text (e.g., base64 encoded), and decoding it to reveal hidden information or flags.
- **Steganography (Steggide):** This challenge involves uncovering hidden messages or flags embedded within images, audio files, or other media using basic steganography tools and techniques.
- **File Exiftool (exifttol):** Participants use the ExifTool utility to extract metadata from files, focusing on understanding file attributes and hidden information stored within file headers.



1.4 Medium Level Part Challenge Of the QuantumCTF

Encoding

In this task, participants must decode an encoded message to uncover hidden information. The message could be encoded using various techniques such as Base64, URL encoding, or hexadecimal. This task tests participants' ability to recognize and decode different types of encoding schemes.

- **Objective**: Decode the provided encoded message to reveal the hidden information.
- **Tools**: Encoding and decoding tools or scripts, such as `base64`, `urldecode`, or custom scripts.
- **Skills Tested**: Knowledge of encoding schemes, proficiency with decoding tools, and attention to detail.

Maze

The maze task involves navigating a complex, maze-like folder structure to locate a specific file. This task simulates real-world scenarios where sensitive information is buried within a convoluted directory system. Participants must use their directory traversal skills to efficiently find the target file.

- **Objective**: Navigate through the maze-like folder structure and locate the specified file.
- **Tools**: Command-line tools for directory traversal, such as `ls`, `cd`, and `find`.
- **Skills Tested**: Directory traversal techniques, problem-solving, and file system navigation.

The medium part of the QuantumCTF challenge is designed to provide participants with a balanced mix of tasks that require both theoretical knowledge and practical application. By completing these tasks, participants will enhance their understanding of brute force attacks, encoding techniques, and directory traversal, preparing them for more advanced challenges in the latter parts of the CTF.

1.5 Hard level part Challenges of the Quantum CTF

So there is also some tasks challenges in QuantumCTF and we would like to present these which are so difficult and let's talk about comprehensively about them.

Step 1: Steganography Inside HTML

- **Objective:** Identify hidden data within an HTML file.
- **Details:** Participants need to search for steganographic content embedded within an HTML file. The search begins in the `/usr/bin` directory, where the necessary

steganography tool. You can find it in the system of the `stegnow` tool and you can extract information from there. They can extract concealed information from the HTML.

Step 2: Maze Folder

- **Objective:** Navigate through a maze-like folder structure to find a specific file.
- **Details:** The target file is hidden deep within a folder that mimics a maze. Participants must efficiently traverse this complex directory structure to locate the file, which is essential for progressing to the next challenge.

Step 3: Nested Archive Extraction

- **Objective:** Unzip a deeply nested archive.
- **Details:** The file found in the maze folder is a multi-layered archive compressed using gunzip, bunzip2, and tar. Participants must correctly uncompress each layer in sequence to access the contents of the final archive. This step tests their proficiency with various compression tools and commands.

Step 4: Hidden Flag in HTML

- **Objective:** Discover a hidden flag within random HTML content.
- **Details:** Within the extracted files from the nested archive, there is an HTML file containing random content. Embedded in this content is a hidden flag that participants need to locate. This step requires careful analysis and attention to detail to uncover the concealed information.

Step 5: Brute Force with Wordlist from GitHub

- **Objective:** Use a wordlist to brute force a password or key.
- **Details:** Participants are provided with a wordlist hosted on GitHub, which they must download using the curl command. This wordlist is used to perform a brute-force attack, aiming to crack a password or key that grants access to the final piece of information or confirms completion of the challenge.

Step 6 : LockBox Folder

- Objective: There is a box and there is file inside them we should enter the file
- Details: Participants have Lockbox and for finding the flag we should write the script which open the box to enter the file and that time we can find the flag. According to that we should write in the right way format script to enter the box and catch the flag.

2.0 Literature review and reference to sources used

So in this project when we decide to write this ctf that time we absolutely utilize some tools and some sources to use that. Firstly, when we write that we decide to research some information what should we write shell code or add that.

The development of the QuantumCTF challenge was informed by extensive research from a variety of sources, including internet articles, and practical guides. This research provided the foundational knowledge necessary to create a comprehensive and challenging CTF experience.

Key Sources of our tasks challenge

- Various online resources, including articles on steganography tools and techniques, were consulted to understand the practical application of steganography in cybersecurity.
- Tutorials and articles on directory traversal attacks helped in designing the maze-like folder structure challenge. Due to that we decide to add that part to hard level challenges
- **Online HTML and Web Development Resources**: Various online tutorials and articles on HTML and web development techniques were consulted to enhance the challenge design.
- **Stegnow Tool Researcher**: The official documentation of the stegnow tool was used to understand its capabilities and how to integrate it into the challenge.
- **GitHub**: Resources on GitHub, including repositories with wordlists, were utilized to provide the necessary files for the brute force challenge.

We also research what should we add to our CTF and find some information what should be so perfect to add our Quantum Capture The Flag Challenge.

3.0 Project Plan Reflection

Reflecting on the QuantumCTF project, the experience was both deeply instructive and challenging. This section provides an overview of the personal insights gained, time management issues encountered, obstacles faced, and areas for improvement for future projects.

3.1 Time Management and Obstacles

Time management was a significant challenge throughout the project. Balancing the complexity of each task with the project's timeline required careful planning and frequent adjustments. Some specific issues included:

 Stegnow Tool and Steghide Integration: Unexpected difficulties in using the stegnow tool delayed progress. Debugging these issues took more time than anticipated, highlighting the need for a more flexible project schedule.

 Maze Folder Design and Hidden Flag in Content: Creating a sufficiently challenging maze-like folder structure proved to be more time-consuming than expected. This task required iterative testing and refinement, leading to delays in subsequent steps.

 Nested Archive Extraction: The intricacies of extracting multi-layered archives presented unforeseen obstacles. Each layer required precise commands and thorough understanding, which extended the planned timeline.

3.2 Areas for Improvement

Reflecting on the project's execution, several improvements can be made for future projects:

1. **Detailed Initial Planning**: More comprehensive initial planning, including detailed task breakdowns and time allocations, would improve overall time management. Regular progress reviews and adjustments can help stay on track.
2. **Buffer Time for Debugging**: Allocating buffer time for unexpected issues, especially for complex tasks like tool integration and nested archive extraction, would provide a safety net and reduce stress.

The QuantumCTF project was a profoundly educational experience that offered numerous insights into both technical skills and project management. Despite the time management challenges and obstacles faced, the project provided invaluable lessons that will inform future endeavors. By incorporating more detailed planning, allowing buffer time for unforeseen issues, enhancing testing procedures, and seeking collaborative feedback, future projects can be executed more smoothly and effectively. This reflection highlights the importance of continuous learning and adaptation in the ever-evolving field of cybersecurity.

4.0 Personal Reflection

The QuantumCTF project was a profoundly transformative experience, providing a wealth of learning opportunities across various technical and methodological aspects. Reflecting on the journey, several key areas of personal and professional development stand out.

4.1 Technical Learning and Tools

1. **Deepening Technical Knowledge**: The project demanded a thorough understanding of diverse cybersecurity techniques, from steganography and directory traversal to nested archive extraction and brute force attacks. Each task required detailed research and practical application, significantly deepening my technical knowledge and skills.
2. **Tool Profiency**: When we create this CTF that time we decided to research some tools and besides that we also utilize some tools during our 6-month lessons. According to that we decide to use `steghide` `exiftool` and other tools which was added to our CTF, all of these helps participants to get know the working of the tools in the CTF.

4.2 Methodology and Process

1. **Iterative Development**: Adopting an iterative approach to challenge development allowed for continuous testing and refinement. This methodology ensured that each component of the CTF challenge was rigorously tested and improved upon before final integration.
2. **Research and Resource Utilization**: Conducting thorough research using academic literature, online articles, and practical guides was crucial in designing robust and challenging tasks. This research process reinforced the importance of utilizing diverse resources to build a comprehensive knowledge base.

4.3 Areas for Improvement

1. **Enhanced Planning and Organization**: While the project was successful, more detailed initial planning would have mitigated some of the time management challenges encountered. In future projects, I plan to create more granular task breakdowns and allocate specific time blocks for each phase of the project, including buffer time for unexpected issues.
2. **Comprehensive Testing and Validation**: Ensuring more comprehensive testing and validation of each task and tool before full integration is an area for improvement. This includes conducting thorough unit tests and simulations to identify potential issues early in the development process.
3. **Feedback and Collaboration**: Engaging peers and mentors for feedback throughout the project could have provided valuable insights and alternative solutions to challenges faced. In future projects, I aim to seek collaborative input more proactively, leveraging diverse perspectives to enhance the quality and effectiveness of the final product.

5.0 Practical Application and Future Directions

1. **Real-World Application**: The skills and knowledge gained from this project are directly applicable to real-world cybersecurity scenarios. Understanding how to conceal and uncover information, navigate complex file structures, and perform brute force attacks are essential skills for both defensive and offensive security practices.
2. **Continuous Learning**: The ever-evolving field of cybersecurity demands continuous learning and adaptation. This project underscored the importance of staying current with emerging technologies and methodologies, and I am committed to ongoing professional development to stay ahead in this dynamic field.
3. **Future Projects**: For future CTF challenges and cybersecurity projects, I plan to implement the lessons learned from this experience. This includes more detailed planning, enhanced testing procedures, and proactive collaboration. By doing so, I aim to create even more robust and challenging projects that push the boundaries of my technical and creative abilities.

6.0 Objectives of Project

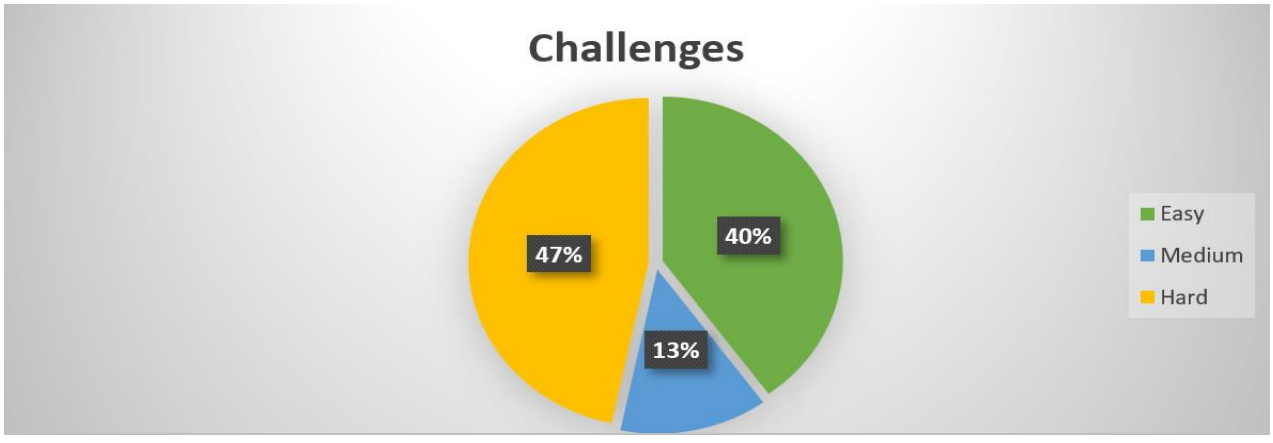
The primary objectives of this CTF competition are:

1. **Skill Development:**
    - To provide a platform for participants to practice and enhance their cybersecurity skills in a controlled, competitive environment.
2. **Knowledge Application:**
    - To allow participants to apply theoretical knowledge to practical challenges, bridging the gap between academic learning and real-world application.
3. **Team Collaboration:**
    - To foster teamwork and collaboration, as participants work together to solve complex problems and share knowledge.
4. **Industry Preparation:**
    - To prepare participants for real-world cybersecurity roles by exposing them to scenarios and challenges that mimic those encountered by professionals in the field.
5. **Innovation and Creativity:**
    - To encourage innovative thinking and creative problem-solving, as participants devise novel solutions to unique challenges.

By achieving these objectives, the CTF competition aims to contribute to the overall growth and development of the cybersecurity community, nurturing the next generation of skilled cybersecurity professionals.

7.0 The Pie Chart format of Our Quantum Project

In this pie chart we can see the percent of the challenges that time it will be more clear to understand the main steps of challenges comprehensively lets watch that which is displayed at the below



Azerbaijan Cybersecurity Center | QuantumCTF

Welcome to the QuantumCTF Report! This document provides a comprehensive overview of QuantumCTF, an interactive Capture The Flag (CTF) competition designed to enhance participants' cybersecurity skills. Hosted on the Cywaria platform, QuantumCTF challenges participants to navigate through a series of progressively complex tasks, retrieving hidden flags to advance to subsequent levels.

QuantumCTF has been created and presented by:

- Teymur Novruzov
- Maleyka Heybatova
- Vahab Poladzada
- Mahammad Seyidzada
- Mammad Samadov
- Ravan Panjaliyev

Prepared by : GROUP_1