**Capture The Flag (CTF) Write-Up**

This document describes the techniques and tools utilized to solve various challenges in the CTF. Each section includes step-by-step solutions and automation techniques used.

1. Miscellaneous Challenges
   1. Welcome

This challenge served as an easy introduction to the event. The first flag was found in the pinned messages of the announcement channel on Discord, showcasing the importance of thoroughly exploring

communication platforms.

* 1. The Great Login Heist

Analyzed a provided .pcap file in Wireshark to locate HTTP POST requests. Within these, plain text login credentials were extracted, leading to the discovery of the flag.

Steps:

* Open the .pcap file in Wireshark.
* Apply filter: http.request.method == "POST".
* Inspect packet details to retrieve credentials.
  1. Silent Courier

Extracted a ZIP file from network traffic and cracked its password using a wordlist with Hashcat. The ZIP contained the flag.

Steps:

* Identify and download the ZIP from HTTP traffic in Wireshark.
* Use a password-cracking tool to unlock the file.
* Extract and locate the flag.
  1. Play with QR
* All the images had the same md5sum expect one.
* So I calculated the md5sum of all the images and using grep -v, I got the unique image.
* Using zbar-tools, I got the information from the qrcode

2.1 Weak:

* Figured the weak password is 12345678

2.2 Locate the bridge:

* Went to what3words.com
* Searched for connecting bridge REC and got the words

2.3 Find the lab:

* Went to what3words.com
* Searched for Idea lab REC and got the words

2.4 Magnetic Epicenter:

* Searched for place close to equator
* Got the place and went to what3words

2.5 Find the ranch:

* Searched with google images and went with the first result

2.6 Cyber sentinels hunt:

* Going to ctf.cybersentinels.xyz and scrolling to the bottom, we can see the social media pages.
* Got the hidden flags from discord, linkedin and Instagram.

3.1 Pixel Secrets:

* Had a pic file and passlist.
* Used stegcracker and found the right password.

3.2 Idoor:

* In the URL, we can see that the number 20 is hashed with SHA256.
* So I figured to bruteforce the right number using python script.
* Turns out the right number is 0.

4.1 Decode the Hex value:

* A hex value is given.
* Going to rapid tables, We can get the value

4.2 Route 47:

* Assuming ROT47, I cracked the flag.

4.3 Rail Conductor’s secret:

* The word ‘rail’ reminded me of rail cipher.
* So I went to dcode.fr and cracked it

4.4 Byte Buster:

* The given is a brainf\*ck code.
* Going to a online compiler, we can get the flag

5.1 Feedback:

* Filling the feedback form, we can get the flag.

6.1 Decrypting the Ransom: Malicious DOCM Analysis

* The File extension .docm refers to the macros used.
* To decode that, I used olevba and from the vba code, I got a base64 value
* Using base64 -d, I got the flag.

6.2 EDIT:

* Given is a corrupted .png image
* Seeing its magic number is changed, I reverted it back and got the flag from the photo.

7.1 Enigma Unveiled

* Using ghidra, we can reverse engineer the binary and get the flag.