**Full Name:**

**1813\_AYUSH PARKARA**

CTF Report

**Program: HCS - Penetration Testing 1-Month Internship Date: 15/03/2024.**

# Category: {OSINT} Description: Operation Alias Challenge Overview:

Fascinated by Steven's artistic revival, my group of friends and I set out on a search to uncover the platform where he secretly publishes his newfound artworks. Remembering his old nickname "**ArtisticSteven**," we explored various online art communities, galleries, and social media platforms where he might have rekindled his creative flame. Can you help us?

# Steps for Finding the Flag:

1. **Initial Reconnaissance:** I started by Searching for username **ArtisticSteven.**
2. I searched different platforms like Instagram, reddit, deviantart and 1 more.
3. I found this profile [**https://www.deviantart.com/artisticsteven**](https://www.deviantart.com/artisticsteven)And on zooming to the profile picture. Inside a profile picture I got the link to spotify inside image.
4. This is the link provided.
5. ( https://open.spotify.com/playlist/3m7waCqC2YaQ544MDqNdyS)
6. After accessing thse website, I found that the playlist of the songs is the real flag.

**Flag:** flag{This\_Feeling\_Makes\_You\_Fly\_Higher\_Than\_Heaven\_Till\_Forever\_Falls\_Apart}

# Category: {OSINT} Description: Social Hunt Challenge Overview:

One of my tech-savvy friends constantly claims that using Linux these days is akin to trying to light a fire with stones. We often tease him by saying, 'One day, you'll be the one known as the LinuxKiller and go by the online persona of '**LinuxKiller69**' on google. Despite not being a frequent social media user, he occasionally checks his account, where the platform's mascot is 'Snoo'. We're curious to know where else he has created accounts and what tech-related thoughts he's sharing there.

# Steps for Finding the Flag:

1. I started by Searching for username **LinuxKiller69** on Instagram, and facebook.
2. I found the flag in profile picture.
3. But it is not accessible directly from the browser
4. So we need to use an Instagram dp downloader and with the help of that I was able to download the picture and get the flag.

**Flag:** flag{cr0ss\_pl4tf0rm}

# Category: {OSINT} Description: Own3r Challenge Overview:

Your friend had been working at a tech startup known for several years. He was a dedicated and loyal employee, always striving to make a positive impact within the company. However, as often happens in the corporate world, there were rumors of internal conflicts and unexplained decisions within the organization. One fateful day, your friend was called into the HR office, and just like that, he was handed a pink slip. The reason for his sudden termination was shrouded in mystery. No explanations, no warnings, just an abrupt end to his career. Your friend felt betrayed, and you both were left with a burning curiosity about the company owner, who remained a shadowy figure behind the scenes.

Friend's Username: @Recently1289445

Flag Format : flag{Name\_of\_Owner}

# Steps for Finding the Flag:

1. First of all I tried searching each and every social media.
2. I searched in Instagram, twitter, reddit, and linkedin.
3. I found the account in twitter and it is not available directly.
4. We need to login first to see the page.
5. So I used nitter to bypass the login process and saw 2 images posted there.
6. One image was of restaurant and another was of a commercial building.
7. So I founded the owner of the building and year it was build.
8. There I found the name of owner and got the flag.

**Flag:** flag{Nitendo\_Yamauchi}

# Category: {OSINT} Description: Tr4ck Challenge Overview:

We've discovered a flash drive belonging to a criminal, which contains three images of various villages. It's possible that the criminal is hiding in one of these villages. Can you help us find their whereabouts?

Flag Format : flag{village1\_village2\_village3}

# Steps for Finding the Flag:

1. I started by Searching each village picture using google lens
2. I found the flag on from different blogs I visited.

**Flag:** flag{Llanfairpwllgwyngyll\_Monsanto\_Chefchaouen}

**Category: {OSINT}**

**Description: Lost**

**Challenge Overview:**

Nami found a lost smartphone on his trip to US , but he is not able to figure out the real owner of the device. Can you help him locate the owner and find a way to contact him?

Flag format:- flag{Owner’s contact}

# Steps for Finding the Flag:

1. I searched for FCC ID I found on the picture.
2. In FCC ID database **https://fcc.report/FCC-ID/RWO-RZ350259** the request was not getting redirected.
3. So I used another site to get the fcc id details https://fccid.io/RWO-RZ350259.
4. there I was able to see the email of the person who was the owner.

**Flag:** flag{[johnsen.tia@razerzone.com](mailto:johnsen.tia@razerzone.com)}

**Category: { Cryptography}**

**Description: Cipher Quest**

**Challenge Overview:**

Picture yourself as an intrepid cryptographer, coming across a .txt file that appears to hold a secret. Your task is to unlock this enigmatic file and unveil the hidden message concealed within. The nature of this message is shrouded in mystery, and you'll need to rely on your analytical and cryptographic skills to decipher it. flag format: flag{HCS\_HCS}

# Steps for Finding the Flag:

1. After downloading the file and read the challenge description, I knew that the binary code needs to be converted to an image file.
2. By using this online tool (<https://capitalizemytitle.com/binary-to-image-converter/> ), I was able to see the flag in generated image.

**Flag:** flag{crypt1c\_1mp0st3r}

**Category: { Cryptography}**

**Description: FeatherDust**

**Challenge Overview:**

Decode it to get the flag! This encryption uses URL safe encoding, AES with CBC. Enough Info, right?

Flag format: flag{HCS\_HCS}

# Steps for Finding the Flag:

1. After downloading the file and read the challenge description, I knew that I need to decrypt the encrypted lines.
2. After some research work I was able to find out that the code was encrypted in fernet encoding.
3. So I used the fernet decoder([Fernet (Decode) (asecuritysite.com)](https://asecuritysite.com/encryption/ferdecode)).
4. In that the top most text was decrypted using the useme text as it was the key.

**Flag:** flag{f3rn3t\_3ncrypt1on\_@r3\_s1m1lar\_t0\_b@s3}

**Category: { Cryptography}**

**Description: RulerOfTheWorld**

**Challenge Overview:**

Mr. Bob sent us this file and asked us to retrieve the secret, he also mentioned that follow these electrical impulses, It will take you to the destination. Focus on the formation! It's !=Binary & Don't fall in the trap! Two persons are involved in this, so both are needed, a single one won't make it for you.

Flag format: flag{HCS}

# Steps for Finding the Flag:

1. After downloading the file and read the challenge description, I thought it was binary code, But it wasn’t. Then I came to find that It is baudot-code.
2. By using this online tool (<https://www.dcode.fr/baudot-code> ) I was able to decrypt the flag.

**Flag:** flag{NOTAREGULARBINARY}

**Category: { Network Forensics}**

**Description: Shadow Web**

**Challenge Overview:**

Unravel hidden data within the intricate landscape of protocols. This MULTIverse of packets contains some Form Data which can reveal the secrets of Web. Try to find this secrets that are scattered to get a flag.Flag format: flag{HCS}

# Steps for Finding the Flag:

1. Open and analyze pcapng file.
2. Reading the TCP stream gives us hint as "Always look for small clues in your way to find the answer. Clues can be scattered in 'multiple' locations."
3. Both Description and TCP stream give us hint like 'multiple'.Looking at HTTP packets these are POST request packets which contains multipart/form-data header in it.
4. Looking into data of these multipart/form-data and we can see a single letter in each packet in between the data.
5. Concatenating this letter gives us random string. S
6. This string appears to be base64 encoded, on decrypting it using cyberchef will give us flag.

**Flag:** flag{mult1pl3p4rtsc0nfus3s}

**Category: { Network Forensics}**

**Description: Mystic Connections**

**Challenge Overview:**

Are you ready to unravel the hidden secrets of network communication and showcase your prowess with your shARP analysis? shARPen your analysis skill to unhide the hidden secret. Fact: Data is everywhere to be found.

Flag format: flag{HCS\_HCS}

# Steps for Finding the Flag:

1. After downloading the file and reading the file description. I filter the packed as ARP
2. I order the packet based on time. And got the flag.

**Flag:** flag{ARP\_b31ng\_s1mpl3}

**Category: { Reverse Engineering}**

**Description: DecryptQuest**

**Challenge Overview:**

One day, one of Samarth’s imaginary friends, Arjun, mysteriously hands him a text file claiming it holds encrypted secret data impossible to decode! Arjun dangles a $1,000,000 reward if Samarth manages to extract the information. However, Arjun enjoys mischief and attempts to trick Samarth by flooding the file with loads of irrelevant data. Would you assist Samarth in unlocking this top-secret information? He pledges to split the reward with you if successful !!

Flag format: flag{HCS\_HCS}

# Steps for Finding the Flag:

1. After downloading the file, I uses cyberchef and got Java code that can make the flag.
2. In java code the were drive link so I accessed it and decrypt its content. Then I find the hint that says to use Unix Epoch Time.
3. Then I made some corrections to make the code simple.
4. I edited my code to search for 1970 value when looping and stop the running loop when it finds it.
5. After performing this I found the flag.

**Flag:** flag{hjwilj111970djs}

**Category: { Reverse Engineering}**

**Description: 4pP**

**Challenge Overview:**

At the age of 9, a young coding prodigy created a simple app for a school project. The app's purpose was to manage various aspects of an "School," although it was quite rudimentary. However, the prodigy left behind a hidden msg that only seasoned hackers could unravel. Your mission is to find the message**.**

# Steps for Finding the Flag:

1. After downloading the file, I extracted the whole file.
2. There I saw two folders and moved to the src folder.
3. Then I kept going on into the folders until I saw two files with the extension ‘ .scm’ and ‘.bky’.
4. Then I openend the screen1.bky file as I thought that it would be the ui and output file because the other file just had connections and all.
5. There I got the flag in between of the code.

**Flag:** flag{M1T\_4PP\_1NV3NT0R\_bf0285c53}

**Category: { Phishing }**

**Description: Phish Guard**

**Challenge Overview:**

Aren't spam emails just the worst? I could miss something important!! Like this one email from Amazon. I don't recall making a payment for a Samsung TV but this looks like it could've been me.

# Steps for Finding the Flag:

1. After opening the file. I found that it has 3 page long, with two blank pages.
2. I assumed it is whitespace-language. Then I searched for <https://www.dcode.fr/whitespace-language> online tool to give me a plain text.
3. After conversion, I got the flag

**Flag:** flag{D0n't\_g3t\_ph1sh3d}