## **CONTRIBUTORS BIOGRAPHY**

****

Hello! I'm Karthikaa. R, a dedicated third-year student pursuing a B.Tech in Computer Science and Engineering with a specialization in cybersecurity at B.S. Abdur Rahman Crescent Institute of Science and Technology.

My academic journey has been centered around cybersecurity, and I'm deeply passionate about exploring its diverse aspects. I actively engage in courses and projects to deepen my expertise in cybersecurity. Additionally, I am committed to staying updated with the latest developments and trends in the field through full immersion in cybersecurity.

Outside of academics, I've participated in several hackathons where I've had the opportunity to apply my skills in practical settings. I have knowledge in several programming languages such as Python and Java, and I am familiar with fields like web development and machine learning. Furthermore, I've conducted workshops on “Artificial Intelligence for pharma”, aiming to share my knowledge and passion with fellow enthusiasts.

Connect with me on LinkedIn: [www.linkedin.com/in/karthikaa-ravikumar](http://www.linkedin.com/in/karthikaa-ravikumar)

## 

Hey there! I'm Dharanidharan, currently in my third year of B.Tech at B.S. Abdur Rahman Crescent Institute of Science and Technology, specializing in cybersecurity.

My coursework in ethical hacking, networking, and programming has ignited my passion for cybersecurity. During a cybersecurity internship focusing on penetration testing, I gained invaluable insights and knowledge in the field.

Proficient in programming languages like Python, Java, and C++, I thrive on tackling new challenges. Hands-on experience with cybersecurity tools such as Wireshark and Metasploit has deepened my understanding of cybersecurity principles. Beyond academics, I've actively participated in various projects and events, driven by my enthusiasm for cybersecurity.

Reach me on LinkedIn: [www.linkedin.com/in/dharanidharan-v-272426237](http://www.linkedin.com/in/dharanidharan-v-272426237)

## **CTF Report**

**Full Name: Karthikaa. R & Dharanidharan. V**  
**Program: HCS - Penetration Testing 1-Month Internship**  
**Date: 15/03/24**

**Category: OSINT (Open-Source Intelligence)**

**Description:** Open-source intelligence, also known as OSINT, refers to the gathering of information from publicly available sources, such as social media, company websites, and news articles.

**Challenge Overview:** Steven's artistic revival under the alias "ArtisticSteven" has piqued the interest of a group of friends. The task is to find the platforms where Steven may be secretly posting his artworks, including an art community, a gallery, and a social media platform.

**Steps for Finding the Flag:**

1. **Initial Reconnaissance:** Begin by searching for Steven's online presence using the alias "ArtisticSteven." Explore various online art communities, galleries, and social media platforms where artists typically share their work.
2. **Art Community Search:** Found Steven's presence on art communities like DeviantArt, where artists often showcase their creations. Looked for any artworks or profiles associated with the alias "ArtisticSteven”.
3. **Gallery Exploration:** Next, on exploring Steven’s galleries we got a link in one of his artworks.
4. **Flag Retrieval:** By exploring the link, which redirects to a spotify playlist where the flag is available in the form of Songs name.

**Flag:** flag{This\_feeling\_Makes\_you\_fly\_Higher\_than\_heaven\_Till\_forever\_falls\_apart}

**Category: OSINT (Open-Source Intelligence)**

**Description:** Open-source intelligence, also known as OSINT, refers to the gathering of information from publicly available sources, such as social media, company websites, and news articles.

**Challenge Overview:** The target individual, known as "LinuxKiller69," is a tech-savvy person who occasionally checks his social media accounts. The goal is to locate other platforms where "LinuxKiller69" has accounts and analyze any tech-related content or discussions associated with him.

**Steps for Finding the Flag:**

1. **Reddit Search:** Begin by searching for the username "LinuxKiller69" on Reddit, a popular social media platform known for its mascot, "Snoo." Look for any posts or comments made by "LinuxKiller69" that may provide insights into his tech-related interests or thoughts.
2. **Exploration of Reddit Content:** Analyze the content associated with the "LinuxKiller69" account on Reddit, focusing on topics such as spam email and Bitcoin-related discussions. Look for any patterns or recurring themes in the posts or comments that may reveal additional information about the individual's interests or activities.
3. **Search for Other Social Media Platforms**: Expand the search to other social media platforms, such as Instagram, where accounts under the username "LinuxKiller69" may exist. Look for profiles or posts associated with this username and examine any tech-related content, or discussions shared by the individual.
4. **Investigate Instagram Profile:** Explore the Instagram profile associated with the username "LinuxKiller69" and analyze any information or posts available. Zoom in on any details or text present in the profile description or images to uncover additional clues or insights.
5. **Inspect Image Source:** Inspect the source of the images on the Instagram profile to access the full image and view any hidden text or details that may provide further information about the individual's tech-related thoughts or activities.
6. **Flag Retrieval:** While inspecting the profile of his Instagram account the flag is retrieved.

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

**Category: OSINT (Open-Source Intelligence)**

**Description:** Open-source intelligence, also known as OSINT, refers to the gathering of information from publicly available sources, such as social media, company websites, and news articles.

**Challenge Overview:** The sudden termination of @Recently1289445, a dedicated employee at a tech startup, prompted an investigation into the circumstances surrounding their dismissal. With no explanation provided, the focus shifted towards identifying the elusive owner of the company.

**Steps for Finding the Flag:**

1. **Reconnaissance:** Initiated the investigation by employing the Recon tool to gather insights into @Recently1289445's online presence. I discovered @Recently1289445's Twitter account, where two pictures with the caption "I miss Europe" and an office were found, hinting at potential clues regarding the termination and the company's owner.
2. **Twitter Analysis:** Through further analysis of @Recently1289445's Twitter account, identified the office in the pictures as belonging to a company named "Nintendo." This discovery prompted a search for the owner of "Nintendo," which was crucial in understanding the circumstances behind @Recently1289445's termination.
3. **President Search:** Utilizing information from Twitter, conducted a search for the presidents of "Nintendo" to uncover potential links to the tech startup. Discovered a total of eight past presidents of "Nintendo," including the elusive owner.
4. **Flag Retrieval:** Upon attempting to put the flag with each president's name, it was found that only the name "Hiroshi Yamauchi" worked. This discovery confirmed his status as the owner of the tech startup, leading to the retrieval of the flag

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

**Category: OSINT (Open-Source Intelligence)**

**Description:** Open-source intelligence, also known as OSINT, refers to the gathering of information from publicly available sources, such as social media, company websites, and news articles.

**Challenge Overview:** The investigation begins with the discovery of a flash drive belonging to a criminal, containing images of three different villages. The goal is to analyze the images and identify the names of the villages where the criminal may be hiding. The flag will be in the format flag{village1\_village2\_village3}, with the names of the villages separated by underscores and all in lowercase.

**Steps for Finding the Flag:**

1. **Image Analysis:** Start by examining the images of the villages provided on the flash drive. Look for any distinctive landmarks, signs, or geographical features that may help identify the locations.
2. **Reverse Image Search:** Use reverse image search tools or services like Google Images to upload the images and search for similar or identical images online. Analyze the search results to see if any matches provide information about the villages depicted in the images.
3. **Source Code Inspection:** If the images are sourced from a website or online platform, inspect the source code of the webpage to extract any metadata or information embedded within the images. Look for clues or hints about the villages' names or locations.
4. **Flag Retrieval:** Upon identifying the names of the villages depicted in the images, arrange them in lowercase and separate them with underscores to form the flag format flag{village1\_village2\_village3}.

**Flag:** flag{llanfairpwllgwyngyll\_monsanto\_chefchaouen}

**Category: OSINT (Open-Source Intelligence)**

**Description:** Open-source intelligence, also known as OSINT, refers to the gathering of information from publicly available sources, such as social media, company websites, and news articles.

**Challenge Overview:** Nami encountered a lost smartphone during his trip to the US but struggles to identify its rightful owner. The challenge is to assist him in locating the owner and establishing contact.

**Steps for Finding the Flag:**

1. **Reconnaissance:** Commenced the investigation by scrutinizing an image source containing the US's FCC ID "RWO-RZ350259" alongside the mobile name "Razer Phone 2" and model "RZ35-0259".
2. **Web Search - FCC ID Verification:** Executed a web search to authenticate the mobile details on the official website using the FCC ID, which yielded no fruitful results.
3. **General Web Search:** Broadened the search by exploring general search results using the FCC ID. After attempting various links, relevant details about the phone model were successfully retrieved.
4. **Owner Identification:** Encountered conflicting information about the owner, with details including the name "Johnsen Tia" and the email "Johnsen.tia@razerzone.com". Initially tried using the name as the flag without success. Realized the flag format required "owner.name
5. **Flag Retrieval:** In the final stage, attempted to use the email as the flag format, resulting in the successful retrieval of the flag.

**Flag:** flag{ Johnsen.tia@razerzone.com }

**Category: Cryptography**

**Description:** Cryptography is the study of secure communication techniques in the presence of adversaries. It encompasses methods such as encryption and decryption to protect sensitive information and ensure data integrity.

**Challenge Overview:** Participants are provided with an encrypted message and informed that it has been encoded using URL safe encoding and encrypted using AES in CBC mode. The goal is to decode the message and extract the flag, which will be in the format flag{HCS\_HCS}.

**Steps for Finding the Flag:**

1. **Understanding Encryption Scheme:** Start by researching and understanding the encryption scheme used in the challenge. This includes familiarizing oneself with URL safe encoding and the AES encryption algorithm in CBC mode.
2. **Initial Decryption Attempts:** Use online decryption tools or libraries to attempt to decrypt the encrypted message using the provided information. Try different combinations of decryption keys and modes to see if the message can be successfully decrypted.
3. **Research Alternative Decryption Methods:** If initial decryption attempts are unsuccessful, research alternative decryption methods or algorithms that may be compatible with the encryption scheme used. Look for cryptographic libraries or tools that support URL safe encoding and AES in CBC mode.
4. **Fernet Algorithm:** Consider using the Fernet algorithm, a symmetric encryption algorithm used in the Python cryptography library, which supports URL safe encoding and AES encryption in CBC mode. Explore tutorials or documentation on how to decrypt messages using the Fernet algorithm.
5. **Decryption Using Fernet Algorithm:** Implement or use existing tools that leverage the Fernet algorithm to decrypt the encrypted message. Provide the necessary parameters, including the encryption key, and attempt to decrypt the message to reveal the flag.
6. **Flag Retrieval:** Upon successful decryption, extract the flag from the decrypted message, which will be in the format flag{HCS\_HCS}.

**Flag:** flag{f3net\_3ncrypt1on\_@r3\_s1m1lar\_t0\_b@s3}

**Category: Cryptography**

**Description:** Cryptography is the study of secure communication techniques in the presence of adversaries. It encompasses methods such as encryption and decryption to protect sensitive information and ensure data integrity.

**Challenge Overview:** Mr. Bob sent us this file and asked us to retrieve the secret. He mentioned following electrical impulses and focusing on the formation. It's not binary, and we must avoid falling into traps. This task requires two persons for success.

**Steps for Finding the Flag:**

1. **Reconnaissance:** Began by examining the provided file containing a sequence of 0's and 1's. Tried copying segments and searching online, leading to websites where the binary sequences translated into text.
2. **Website Analysis:** Explored the websites discovered during reconnaissance, where inputting the binary sequences yielded readable text. Gathered all decoded text for further analysis.
3. **Decryption:** Decrypted the compiled text, uncovering a message with the phrase "flagnotaregularbinary" at the end. Initially tried using "flag{flag{notaregularbinary}" as the flag format without success
4. **Flag Retrieval:** Realized the flag format required avoiding the word "flag" and successfully retrieved the flag using "flag{notaregularbinary}".

**Flag:** flag{notaregularbinary}