CTF Report

Full Name: Muhammad Bokhtiar Uddin
Program: HCS - Penetration Testing 1-Month Internship
Date: 15-03-2024

Category: OSINT (Operation Alias)

Description: Our job is to discover the platform where Steven covertly distributes his artworks by following the trail of his previous moniker, "ArtisticSteven," and examining numerous online art forums, galleries, and social media platforms.

Challenge Overview: Open-Source Intelligence (OSINT) tasks require collecting information from publicly accessible sources in order to solve a puzzle or discover hidden information.

Steps for Finding the Flag:

1. **Initial Research:** Look for Steven's former moniker, "ArtisticSteven," throughout many internet venues, such as art groups, galleries, and social media.
2. **Platform Exploration:** Explore the profiles and posts related with the moniker "ArtisticSteven" to discover hints or connections to his hidden art platform.
3. **Link Analysis:** Analyze any links or references found in the profiles or posts associated with "ArtisticSteven" to discover his secret art platform
4. **Flag Retrieval:** Once you find the platform where Steven publishes his artworks, retrieve the flag from there.

Flag:
flag{this_feeling_makes_you_fly_higher_than_heaven_Till_forever_falls_apart}

Category: OSINT (Social Hunt)

Description: One of my tech-savvy friends often comments that using Linux these days is like attempting to kindle a fire with stones. We regularly tease him by saying, 'One day, you'll be renowned as the LinuxKiller and use the internet alias 'LinuxKiller69'. Despite not being a regular social media user, he periodically checks his account, which has the platform's mascot, 'Snoo'. We're intrigued about where else he's made accounts and what tech-related opinions he shares there.
Challenge Overview: The task entails obtaining information on the target individual's online presence, with an emphasis on their social media accounts and online activities linked to technology.

Steps for Finding the Flag:

1. **Reddit Profile:** Check the user profile on Reddit for 'LinuxKiller69' to gather information about their activity.
2. **Username Search:** Use a username search tool to look for other online accounts associated with the username 'LinuxKiller69'.
3. **Instagram Account:** Find and analyze the Instagram account 'LinuxKiller69' for additional information.
4. **Extract Flag:** Look for the flag in the discovered online accounts or posts related to technology.

Flag: flag{cr0ss_pl4tf0rm}

Category: OSINT (Tr4ck)

Description: We uncovered a criminal's flash drive, which included three photographs of several places. Perhaps the offender is hiding in one of these villages. Can you help us find out where they are?
Challenge Overview: Open-Source Intelligence (OSINT) tasks require collecting information from publicly accessible sources in order to solve a problem or discover hidden information.

Steps for Finding the Flag:

1. **Image Analysis:** Open the three images found on the flash drive and examine them closely.
2. **Location Identification:** Use visual clues in the images to identify the locations of the villages depicted.
3. **Flag Creation:** Combine the names of the villages to create the flag in the specified format.
4. **Flag Retrieval:** Submit the flag once you have correctly identified all three village locations.

Flag: flag{Llanfairpwllgwyngyll_monsanto_chefchaouen}

Category: OSINT (Lost)

Description: Nami discovered a lost smartphone on his journey to the United States, but he is unable to determine who owns it. Can you help him discover the owner and contact them? Steps to Find the Flag:
Challenge Overview: Open Source Intelligence (OSINT) tasks require collecting information from publicly accessible sources in order to solve a puzzle or discover hidden information.

Steps for Finding the Flag:

1. **Smartphone Examination:** Examine the smartphone to gather any information that may help identify the owner.
2. **Online Search:** Use the information found on the smartphone to search for the owner's identity online.
3. **Contact Information:** Locate the owner's contact information, such as an email address or phone number.
4. **Flag Creation:** Format the owner's name into the specified flag format.
5. **Flag Retrieval:** SSubmit the flag once you have successfully identified the owner and their contact information.

Flag: flag{johnsen.tia@razerzone.com}

Category: Cryptography (Cipher Quest)

Description: Imagine yourself as an intrepid cryptographer who comes upon a.txt file that looks to contain a secret. Your mission is to unlock this cryptic file and reveal the secret message within. This message's nature is veiled in mystery, and deciphering it will need your analytical and cryptographic talents.

Challenge Overview: Cryptography problems include decoding encoded or encrypted signals to expose hidden information.

Steps for Finding the Flag:

1. **File Conversion:** Convert the contents of the bin.txt file into an image format.
2. **Image Analysis:** Examine the image for any hidden messages or clues.
3. **Flag Extraction:** If you find a hidden message in the image, extract it.
4. **Flag Formatting:** Format the extracted message into the specified flag format.
5. **Flag Retrieval:** Submit the flag once you have successfully extracted and formatted the message.

Flag: flag{crypt1c_1mp0st3r}

Category: Cryptography (FeatherDust)

Description: Decode it to see the flag! This encryption employs URL-safe encoding, AES with CBC. That's enough information, right?

Challenge Overview: Cryptography tasks require decoding encoded or encrypted signals in order to expose concealed information.

Steps for Finding the Flag:

1. **Encryption Method Identification:** Identify the encryption method used, which is AES with CBC mode and URL safe encoding.
2. **Decryption Tool Selection:** Use a suitable tool or website that supports AES decryption with CBC mode and URL safe encoding.
3. **Decryption Process:** Input the encrypted text and the decryption key into the chosen tool to decipher the message.
4. **Flag Extraction:** Extract the decrypted message to reveal the flag.
5. **Flag Formatting:** Format the extracted message into the specified flag format.
6. **Flag Retrieval:** Submit the flag once you have successfully decrypted and formatted the message.

Flag: flag{f3rn3t_3ncrypt1on_@r3_s1m1lar_t0_b@s3}

Category: Cryptography (RulerOfTheWorld)

Description: Mr. Bob provided us this file and instructed us to recover the secret. He also claimed that following these electrical impulses would lead you to your goal. Focus on the formation! It's not binary, so don't fall into the trap! Because this involves two people, both are required; one will not suffice.

Challenge Overview: Cryptography tasks require decoding encoded or encrypted signals in order to expose concealed information.

Steps for Finding the Flag:

1. **File Analysis** Examine the file provided by Mr. Bob to understand its contents and format.
2. **Baudot Code Recognition:** Recognize the use of Baudot code in the file and understand its significance.
3. **Decryption Tool Selection:** Ise a suitable tool or website that supports Baudot code decryption.
4. **Decryption Process:** nput the Baudot code from the file into the chosen tool to decipher the message.
5. **Flag Retrieval:** Submit the flag once you have successfully extracted and formatted the message.

Flag: flag{NOTAREGULARBINARY}

Category: Network Forensics(Shadow Web)

Description: Uncover hidden data inside the complex network of protocols. This MULTIverse of packets has some Form Data, which may disclose the Web's secrets. To get a flag, search for the dispersed secrets.
Challenge Overview: Network forensics issues entail examining network traffic to discover hidden data or secrets.

Steps for Finding the Flag:

1. **Capture Analysis:** Open the provided capture file in a network analysis tool like Wireshark to examine the network traffic.
2. **Protocol Examination:** Analyze the different protocols used in the network traffic to identify any Form Data or hidden information.
3. **Data Decryption:** If the data is encrypted, use the appropriate decryption techniques to decrypt it.
4. **Flag Extraction:** Extract the decrypted data or secret information to reveal the flag.
5. **Flag Formatting:** Format the extracted flag into the specified flag format.
6. **Flag Retrieval:** Submit the flag once you have successfully decrypted and formatted the secret data.

Flag: flag{mult1pl3p4rtsc0nfus3s}

Category: Network Forensics (Mystic Connections)

Description: Are you ready to uncover the hidden mysteries of network communication and demonstrate your expertise via crisp analysis? Improve your analytical skills to uncover the hidden truth. Fact: Data can be found anywhere.

Challenge Overview: Network forensics issues entail examining network traffic to discover hidden data or secrets.

Steps for Finding the Flag:

1. **Capture Analysis:** Open the provided capture file in a network analysis tool like Wireshark to examine the network traffic.
2. **Protocol Filtering:** Filter the traffic to focus on ARP packets.
3. **Packet Reordering:** Reorder the ARP packets based on their sequence numbers or timestamps.
4. **Data Extraction:** Extract the data from each ARP packet, starting from packet number 18, and concatenate it.
5. **Flag Formatting:** Format the extracted flag into the specified flag format.
6. **Flag Retrieval:** Submit the flag once you have successfully extracted and formatted the hidden secret.

Flag: flag {ARP_b31ng_s1mpl3}

Category: Reverse Engineering (DecryptQuest)

Description: One day, one of Samarth's imaginary pals, Arjun, inexplicably sends him a text file claiming to contain encrypted secret material that cannot be decoded! Arjun offers a $1,000,000 incentive if Samarth can extract the information. Arjun, on the other hand, adores mischief and tries to fool Samarth by filling the file with unnecessary data. Would you help Samarth access this top-secret information? He promises to divide the prize with you if you succeed!

Challenge Overview: The task is to decode a text file containing encrypted secret data. The file is filled with extraneous data to confuse the decoder. The purpose is to extract the required information and locate the flag.

Steps for Finding the Flag:

1. **Decrypting the File:** Analyze the encrypted text in the file and decrypt it using the appropriate method.
2. **Decoding the Java Code:** Once decrypted, the file contains Java code. Translate the Java code to Python.
3. **Writing the Python Script:** Use the translated Java code to write a Python script that can decrypt the data correctly.
4. **Running the Script:** Execute the Python script to decrypt the data and extract the flag.

Flag: flag{hjwilj111970djs}

Category: Reverse Engineering (4pP)

Description: At the age of nine, a young coding genius developed a basic app for a school assignment. The app's objective was to handle many parts of a "School," however it was quite basic. However, the genius left a concealed message that only experienced hackers could decipher. Your objective is to locate the message.
Challenge Overview: The assignment is evaluating three files related with a tiny program developed by a teenage coding genius. The aim is to find a secret message left by the genius among the files.

Steps for Finding the Flag:

1. **File Analysis:** Open and analyze each of the three files associated with the app.
2. **String Extraction:** Use the “strings” command to extract printable strings from each file.
3. **Search for Flag:** Look through the extracted strings for any message that could be the hidden flag left by the prodigy.

Flag: flag{M1T_4PP_1NV3NT0R_bf0285c53}

Category: Phishing (Phish Guard)

Description: Aren't spam emails the worst? I could miss something vital!! Like this email from Amazon. I don't remember making a payment for a Samsung TV, but this may have been me.
Challenge Overview: The task is to analyze a three-page DOCX file. One page seems to be written, while the rest remain blank. The aim is to uncover a secret message within the apparently empty pages.

Steps for Finding the Flag:

1.DOCX Analysis: Open and analyze the DOCX file to understand its contents.

2. Copy Whitespace: Copy the whitespace from the seemingly empty pages of the DOCX file.

3. Whitespace Compiler: Use a whitespace compiler to compile the copied whitespace.

4. Extract Flag: Look for the hidden message within the compiled whitespace to find the flag.

Flag: Flag{D0n't_g3t_ph1sh3d}