CTF Report

Full Name: Rohit Kumar
Program: HCS - Penetration Testing 1-Month Internship
Date: 10-March-2025

Category: Web 2.0(The World)

Description: This is a typical process in Capture The Flag (CTF) challenges, where each step involves discovering hidden information, exploiting vulnerabilities, and retrieving a flag as proof of success.

Challenge Overview: Use **gobuster** to enumerate directories and find hidden files like /secret.txt. Decode the Base64 string found in /secret.txt. Retrieve the flag from the decoded string.

Steps for Finding the Flag:

1. **Directory Enumeration:** Explore directories and endpoints within the web application to uncover hidden pages or functionalities that may lead to the flag use tool: **gobuster** for endpoint and **/secret.txt** hidden files.
2. **Exploitation:** find base64 code in /secret.txt and decode it from this website, the is **RkxBR3tZMHVfaGF2M180eHBsMHJlRF90aDNfVzByTGQhfQ==**
3. **Flag Retrieval:** **https://www.base64decode.org/** decode the code , and find this flag **FLAG{Y0u_hav3_4xpl0reD_th3_W0rLd!}**

Note: Modify the above steps for different challenges

Flag: FLAG{Y0u_hav3_4xpl0reD_th3_W0rLd!}

Category: OSNIT (Snapshot Whispers)

Description: OSINT stands for **Open Source Intelligence**. It involves gathering information from publicly available sources to be used for intelligence purposes. This can include anything from social media profiles, publicly available documents,

websites, forums, and other open sources to identify potential threats, vulnerabilities, or track adversaries' movements.

Challenge Overview: In this OSNIT assignment, I used reverse image search to identify the photo as being taken from the Sydney Opera House. After conducting further research, I found the same image in a review by Jeffrey Seidman. This process demonstrated how open-source intelligence tools can help gather context and uncover hidden information from publicly available sources.

Steps for Finding the Flag:

1. **Initial Image Analysis:** I began by analyzing the image provided in the assignment. I noticed key features within the image that looked like a famous landmark.
2. **Reverse Image Search:** I used **Google's reverse image** search tool to find the origin of the image. The search results identified the image as a photograph taken from the **Sydney Opera House**.
3. **Researching the Sydney Opera House:** After identifying the Sydney Opera House, I decided to gather more information about it. I conducted a Google search using the terms “Sydney Opera House review.”
4. **Finding the Image in a Review:** While scrolling through the results on a review page about the Sydney Opera House, I came across the same image. The image was attributed to a review by **Jeffrey Seidman**.

Note: Modify the above steps for different challenges

Flag: flag{Jeffrey_Seidman}

Category: OSNIT (Time Machine)

Description: OSINT stands for **Open Source Intelligence**. It involves gathering information from publicly available sources to be used for intelligence purposes. This can include anything from social media profiles, publicly available documents, websites, forums, and other open sources to identify potential threats, vulnerabilities, or track adversaries' movements.

Challenge Overview: In this challenge, I followed a series of steps to uncover the flag. First, I clicked on a hint that revealed the term "Trojan Hunt." I then performed a Google search, explored several websites, and eventually found a link to archive.org. After accessing the archive, I downloaded a text file where I found the flag: flag{Tr0j3nHunt_t1m3_tr4v3l}

Steps for Finding the Flag:

1. **Clicking the Hint:** I started by clicking on the hint provided for the assignment, which revealed the name "Trojan Hunt".
2. **Google Search for "Trojan Hunt":** I performed a Google search using the term "Trojan Hunt" to find relevant websites and information.
3. **Exploring Websites:** After scrolling, I found a useful link that led me to **archive.org**, a digital archive platform.
4. **Accessing the Archive:** On the **archive.org** website, I clicked the download option, which led me to different file types.
5. **Opening the Text File:** I selected the text file and opened it to find the flag.

Note: Modify the above steps for different challenges

Flag: flag{Tr0j3nHunt_t1m3_tr4v3l}