CTF Report

Full Name: G M Sohanur Rahman
Program: HCS - Penetration Testing 1-Month Internship
Date: 15 March, 2024

---

1. Category: OSINT(Operation Alias)

Description: OSINT (Open Source Intelligence) in Capture The Flag (CTF) competitions involves gathering information from publicly available sources to solve challenges. This can include analyzing websites, social media profiles, public databases, and more to find clues or hidden flags. Participants use OSINT techniques to extract relevant information and often combine it with other skills like cryptography, steganography, and reverse engineering to progress in the CTF.

Challenge Overview: My friends and I are intrigued by Steven's artistic resurgence and are searching for the platform where he anonymously shares his new artwork under the pseudonym "ArtisticSteven." Can you help us find it?

Steps for Finding the Flag:

1. **Initial Reconnaissance:** Start by analyzing his username "ArtisticSteven". After searching his username we found some links we needed to explore. As it is art related we will go for Devianart. We can see a picture.
2. **Exploitation:** Let's analyze the picture deeply so that we don't miss anything. At the end of the bottom right corner we can see a Spotify Link. After trying to open the link we can see it saying the link is invalid. Now we try to remove "-" from the link and let's see if it is working or not. Boom! Now it is working.
3. **Flag Retrieval:** Once the link is working we can see the flag in the playlist.

Flag:
flag{This_Feeling_Makes_You_Fly_Higher_Than_Heaven_Till_Forever_Falls_Apart}

2. Category: OSINT(Social Hunt)

Description: OSINT (Open Source Intelligence) in Capture The Flag (CTF) competitions involves gathering information from publicly available sources to solve challenges. This can include analyzing websites, social media profiles, public databases, and more to find clues or hidden flags. Participants use OSINT techniques to extract relevant information and often combine it with other skills like cryptography, steganography, and reverse engineering to progress in the CTF.

Challenge Overview: My tech-savvy friend mocks Linux, calling it outdated, and we joke about him becoming 'LinuxKiller69' online. Despite rarely using social media, he occasionally checks his account, recognized by the 'Snoo' mascot. We're curious about his other online accounts and tech-related posts.

Steps for Finding the Flag:

1. **Initial Reconnaissance:** Start by analyzing the Social Media as it is social media related. We went to Facebook, Twitter, Reddit but found nothing by his Username except Instagram. We found a private Instagram profile with Profile Photo. Let's explore the picture.
2. **Exploitation:** Once we can see the profile is Private. We need to use a third part website to download his Displayed Photo to explore.
3. **Flag Retrieval:** Once we have successfully downloaded the picture we can see the flag below.

Flag: flag{cr0ss_pl4tf0rm}

3. Category: OSINT(OWn3r0

Description: OSINT (Open Source Intelligence) in Capture The Flag (CTF) competitions involves gathering information from publicly available sources to solve challenges. This can include analyzing websites, social media profiles, public databases, and more to find clues or hidden flags. Participants use OSINT techniques to extract relevant information and often combine it with other skills like cryptography, steganography, and reverse engineering to progress in the CTF.

Challenge Overview: Your loyal friend at a tech startup was suddenly terminated without explanation, leaving both of you curious about the mysterious company owner.

Steps for Finding the Flag:

4. **Initial Reconnaissance:** Start by analyzing the username given ***@Recently1289445***. We explore social media. In Twitter we can see his profile which has two pictures of his old company and its area. We can see the company building picture in the second photo. We can explore it.
5. **Exploitation:** Once we get the picture we do reverse engineering on it. After using Google Lens, we can see the picture with the name of the building *Campus Tower*,*Corporate office in Frankfurt*, *Germany*. Now we try to find the Startup Tech Company which we found there is a company named **Nintendo.**
6. **Flag Retrieval:** Once the company name is found we can now get the owner *Hiroshi Yamauchi.*

Flag: flag{Hiroshi_Yamauchi}

4. OSINT(Tr4ck)

Description: OSINT (Open Source Intelligence) in Capture The Flag (CTF) competitions involves gathering information from publicly available sources to solve challenges. This can include analyzing websites, social media profiles, public databases, and more to find clues or hidden flags. Participants use OSINT techniques to extract relevant information and often combine it with other skills like cryptography, steganography, and reverse engineering to progress in the CTF.

Challenge Overview: We found a flash drive with three village images that might be linked to a criminal's hideout. Can you help us locate them?

Steps for Finding the Flag:

7. **Initial Reconnaissance:** Start by analyzing the three pictures of the village that is given. We will analyze via Google Image search.
8. **Exploitation:** Once we have searched each picture individually we got the name of the three villages.
9. **Flag Retrieval:** Once the village name is ready we will put them sequentially in the flag.

Flag: Flag{llanfairpwllgwyngyll_monsanto_chefchaouen}

5. OSINT(Lost)

Description: OSINT (Open Source Intelligence) in Capture The Flag (CTF) competitions involves gathering information from publicly available sources to solve challenges. This can include analyzing websites, social media profiles, public databases, and more to find clues or hidden flags. Participants use OSINT techniques to extract relevant information and often combine it with other skills like cryptography, steganography, and reverse engineering to progress in the CTF.

Challenge Overview: Nami found a lost smartphone in the US and needs help locating its owner. Can you help him find a way to contact them?

Steps for Finding the Flag:

10. **Initial Reconnaissance:** Start by analyzing the picture given with the SmartPhone details. We can see the FCC ID in the picture. Now we have searched through the ID and found some details about the device.
11. **Exploitation:** Once we have found the details we keep searching for the owner details and we find email addresses of the owner.
12. **Flag Retrieval:** Once we have found the email addresses of the owner we will put the email in the flag.

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

6. Category: Cryptography(Cipher Quest)

Description: Cryptography involves decoding or encoding messages to uncover hidden information or flags. Participants use various cryptographic techniques such as Caesar ciphers, XOR operations, and RSA encryption to solve challenges and progress in the competition.

Challenge Overview: Imagine you're a skilled cryptographer faced with a mysterious .txt file containing a hidden message. Your challenge is to decrypt this file using your analytical and cryptographic abilities to reveal its concealed content.

Steps for Finding the Flag:

1. **Initial Reconnaissance:** Start by analyzing the given bin.txt file which is full of Binary Code. Now, we will head over to CyberChef to analyze those codes. After putting the codes we can see the output instantly in the CyberChef. If we look closely we can see there is PNG to render in the output and we will download it to analyze.
2. **Exploitation:** Once we have the image we will try to find the flag from it. Once we have zoomed the image we can see something in the bottom half which is our flag.
3. **Flag Retrieval:** Once the flag is discovered we will write it down and put it on the box and submit.

Flag: flag{crypt1c_1mp0st3r}

7. Category: Cryptography(FeatherDust)

Description: Cryptography involves decoding or encoding messages to uncover hidden information or flags. Participants use various cryptographic techniques such as Caesar ciphers, XOR operations, and RSA encryption to solve challenges and progress in the competition.

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

Steps for Finding the Flag:

1. **Initial Reconnaissance:** Start by analyzing the given file. After opening the file we can see some codes to understand and decode. We have analyzed those codes and found that we need to use Fernet Decoder to find the actual text/flag.
2. **Exploitation:** Once we have put those code to the decoder we can be able to see the flag.
3. **Flag Retrieval:** Once the flag is discovered, capture and document it for submission.

Flag: flag{f3rn3t_3ncrypt1on_@r3_s1m1lar_t0_b@s3}

8. Category: Cryptography(RulerOfTheWorld)

Description: Cryptography involves decoding or encoding messages to uncover hidden information or flags. Participants use various cryptographic techniques such as Caesar ciphers, XOR operations, and RSA encryption to solve challenges and progress in the competition.

Challenge Overview: Mr. Bob sent a file with a hidden secret, hinting at a non-binary code and warning that two people are needed to unlock it.

Steps for Finding the Flag:

1. **Initial Reconnaissance:** Start by analyzing the file given and we can see some binary code in the file. Lets research about the code and we have found that we need Baudot-Decoder to find the text.
2. **Exploitation:** Once we put those binary code to the decoder it has given us some texts. Let's try to find if there is anything in the text. After carefully analyzing the text we have found the flag there.
3. **Flag Retrieval:** Once the flag is discovered, capture and document it for submission.

Note: Modify the above steps for different challenges

Flag: flag{NOTAREGULARBINARY}

9. Category: Network Forensics(Shadow Web)

Description: Network Forensics in Capture The Flag (CTF) competitions involves analyzing network data (like packet captures) to identify and solve security challenges. Participants look for clues hidden in network traffic, including encrypted messages, anomalies, or specific patterns, to find flags (secret codes) proving their skill in understanding and exploiting network vulnerabilities or behaviors.

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 the Web. Try to find these secrets that are scattered to get a flag.

Steps for Finding the Flag:

1. **Initial Reconnaissance:** Start by analyzing the pcapng file given. We will put the file in the Wireshark and analyze. We can see many packets are visible like HTTP,TCP and ARP. TCP stream gives us hints that "Always look for small clues". Now, looking at HTTP packets we can see POST request packets containing multiple/form-data header in it. We can see letters in each packet between data. Now from every request we will collect those characters and arrange them to decode.
2. **Exploitation:** Once we have found all the characters we can see it needs a base64 decoder to decode it. After decoding we have found the flag.
3. **Flag Retrieval:** Once the flag is discovered, capture and document it for submission.

Flag: flag{mult1pl3p4rtsc0nfus3s}

10. Category: Network Forensics(Mystic Connections)

Description: Network Forensics in Capture The Flag (CTF) competitions involves analyzing network data (like packet captures) to identify and solve security challenges. Participants look for clues hidden in network traffic, including encrypted messages, anomalies, or specific patterns, to find flags (secret codes) proving their skill in understanding and exploiting network vulnerabilities or behaviors.

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.

Steps for Finding the Flag:

1. **Initial Reconnaissance:** Start by analyzing the file given and we can see there are some packets in after putting the file in the WireShark. In description ARP have been highlighted. So we will look for ARP packets and analyze them. If we check ARP packets we can see there is a word in every packet and certain time frame.
2. **Exploitation:** Once we have found this info we will try to arrange the time frame in descending order so that we can see the possible flag. After rearranging all of the flag from the packets we got the flag.
3. **Flag Retrieval:** Once the flag is discovered, capture and document it for submission.

Flag: flag{ARP_b31ng_s1mpl3}

11. Category: Reverse Engineering(Decrypt Quest)

Description: Network forensics involves analyzing network traffic data to uncover evidence of cyberattacks and identify compromised systems. It helps reconstruct events, determine attack vectors, and assess the impact on the network infrastructure.

Challenge Overview: Samarth's friend Arjun gives him an encrypted text file with a promise of a $1,000,000 reward if Samarth can decode it. However, Arjun has added a lot of irrelevant data to trick Samarth. Can I help Samarth unlock the secret information and potentially share in the reward?

Steps for Finding the Flag:

1. **Initial Reconnaissance:** Start by unzipping the file given and we have found some encoded text which needed to be decoded. We have found that it is base64 encoding. So, let's decode it and we have found a Java code and Key.txt after decoding. Now, we needed to modify the for loop to get the flag.
2. **Exploitation:** Once we have modified the code and we run. After that we can see a huge flag list in the output. Now, we need to see Key.txt. There we can see we have some clue like Unix Epoch Time. After searching we can see the time is 1970. Now, we will search 1970 in the flag list. Boom! We have got the flag.
3. **Flag Retrieval:** Once the flag is discovered, capture and document it for submission.

Flag: flag{hjwilj111970djs}

12. Category: Reverse Engineering(4pP)

Description: Network forensics in CTF involves analyzing network traffic data to uncover evidence of cyberattacks and identify compromised systems. It helps reconstruct events, determine attack vectors, and assess the impact on the network infrastructure.

Challenge Overview: A 9-year-old coding prodigy created a basic school app with a hidden message for seasoned hackers to discover. Can you find the message?

Steps for Finding the Flag:

1. **Initial Reconnaissance:** Start by extracting the given file in a Kali Linux machine. Let's analyze the file and check what's in it.
2. **Exploitation:** Once we have extracted the file we can see there is some source code. Let's explore more. Now, move on to the SRC then there is the App inventor folder→ ai_23saahilt →CTF→ Screen1.bky. After opening that file we need to focus on code and boom we have found the flag.
3. **Flag Retrieval:** Once the flag is discovered, capture and document it for submission.

Flag: flag{M1T_4PP_1NV3NT0R_bf0285c53}

13. Category: Phishing(Phish Guard)

Description: Phishing is a cyber attack where attackers trick people into revealing sensitive information by impersonating trustworthy entities through deceptive emails, messages, or websites.

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. **Initial Reconnaissance:** Start by analyzing the .docx file given. After opening the file we can see some info in the first page but if you can notice clearly it has three pages. But we can see the rest of the pages are blank. So, there must be something else. As there are white spaces, we move on to search *Whitespace decoders*.
2. **Exploitation:** Once we have put the whitespace in the decoder we have found the flag.
3. **Flag Retrieval:** Once the flag is discovered, capture and document it for submission.

Flag: flag{D0n't_g3t_ph1sh3d}