CTF Report

Full Name: Anumandla Dhanush
Program: HCS - Penetration Testing 1-Month Internship
Date: 15/03/2024

Category: OSINT

Description: OSINT, or Open Source Intelligence, is the process of gathering and analyzing publicly available information from open sources to extract actionable insights and intelligence

Challenge Overview: OSINT challenges involve navigating vast public data to extract actionable intelligence amidst misinformation and data obfuscation.

1.1 Operation Alias

Steps for Finding the Flag:

1. Go to Google search and type “intitle:ArtisticSteven”.
2. There you will get a link to DevianArt platform.
3. Open https://www.deviantart.com/artisticsteven
4. In the Home section, you will see a picture.
5. Click on the picture and zoom the picture.
6. There is a spotify link hidden at the bottom right of the image.
7. Open the link https://open.spotify.com/playlist/3m7waCqC2YaQ544MDqNdyS
8. You get the flag as the names of the songs.

Flag:

flag{ this_feeling_makes_you_fly_higher_than_heaven_till_forever_falls_apart}

1.2 Social Hunt

Steps for Finding the Flag:

1. Go to https://www.instagram.com/LinuxKiller69/
2. Then click on inspect.
3. Dive through profile picture in the inspector element.
4. There you will see the profile picture source.
5. Move the mouse pointer to the source link.
6. It shows the entire profile picture containing the flag.

Flag: flag{cr0ss_pl4tf0rm}

1.3 OWn3r

Steps for Finding the Flag:

1. Go to https://twitter.com/ and login.
2. Search for @Recently1289445, you will see a user with “My Friend Recently”. Click on it.
3. You will see two pictures in the post section.
4. Scan the pictures of buidings using google lens.
5. You will find that the images are campus of “Nintendo”.
6. Search the owner of Nintendo in google.
7. The flag is the name of the owner “hiroshi_yamauchi”

Flag:flag{hiroshi_yamauchi}

1.4 Tr4ck

Steps for Finding the Flag:

1. Download “villages.zip” and extract it.
2. You will see 3 images (1.png,2.png,3.png) of places in the extracted file.
3. By Search the images in google to find the names of the village.
4. The flag is the names of villages combined.

Flag: flag{llanfairpwllgwyngyll_monsanto_chefchaouen}

1.5 Lost

Steps for Finding the Flag:

1. Go Download “lost.png” and open it.
2. You will see the information of the lost phone.
3. Copy the “fcc id” from the image.
4. Go to https://fccid.io
5. Paste the fcc id and click on search.
6. You will get the information of the owner of the lost phone.
7. The flag is the owner’s email id.

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

Category: Cryptography

Description: Cryptography is the study and practice of secure communication techniques, encompassing encryption, decryption, and authentication, to protect data integrity and confidentiality, often involving the use of mathematical algorithms and keys for encoding and decoding messages.

Challenge Overview: Cryptography challenges entail deciphering encrypted messages or systems by applying cryptographic techniques and analysis, often involving breaking codes or uncovering hidden patterns to reveal sensitive information.

2.1 Cipher Quest

Steps for Finding the Flag:

1. Download the “bin.txt” file and copy the binary code.
2. Go to https://gchq.github.io/CyberChef/
3. Paste the binary code in the input section, select the Data Format: “From Binary” and drop it in the recipe section.
4. The binary code is converted to PNG, save the output as “file.png”.
5. Open the “file.png” you will see an avatar.
6. Zoom it a little and you will see the flag hidden in the body.
7. Go to https://www.gifgit.com/image/adjust-image-brightness and upload the “file.png” and increase the brightness.

8. The flag is clearly visible on the body of the avatar.

Flag: flag{crypt1c_1mp0st3r}

2.2 FeatherDust

Steps for Finding the Flag:

1. Go Download the "chall.file" which contain encrypted data with "key"(USEME).
2. The hint is given in the description of the challenge that the encryption used is URL safe encoding, AES with CBC.
3. This is known as Fernet Encryption Method. So we use Fernet Decoder.
4. Go to https://asecuritysite.com/tokens/ferdecode
5. In the Token, paste the encrypted data from "chall.file" and paste the key in the key input field. Click on Determine.
6. It gives the decode data as the flag itself.

Flag: flag{f3rn3t_3ncrypt1on_@r3_s1m1lar_t0_b@s3}

2.3 RulerOfTheWorld

Steps for Finding the Flag:

1. Go Download the "chall.file"
2. The data inside the "chall.file" looks like binary containing combinations 0's and 1's.
3. A hint is given in the description of the challenge. i.e., "It's !=Binary & Don't fall in the trap!" .
4. This means the data inside "chall.file" is not binary. Its Baudot code.
5. byGo to https://www.dcode.fr/baudot-code
6. Paste the data in the Baudot decoder and click on "Decode baudot code".
7. You will get a long set of results containing "FLAGNOTAREGULARBINARY" which is the intended flag.

Flag: flag{NOTAREGULARBINARY}

Category: Network Forensics

Description: Network forensics involves the analysis of network traffic and logs to uncover evidence of cyberattacks, intrusions, or malicious activities, aiding in the identification of perpetrators, understanding attack vectors, and enhancing cybersecurity defenses.

Challenge Overview: Network forensics challenges entail dissecting network traffic captures to identify anomalies, detect intrusion attempts, and extract crucial evidence for investigating cyber incidents.

3.1 Shadow Web

Steps for Finding the Flag:

1. Download “capture.pcapng” file and open it with wireshark.
2. You will see all the packets with different protocols like TCP,HTTP,ARP.
3. Click on the TCP packet and follow tcp stream, there you will find the hint “Always look for small clues in your way to find the answer. Clues can be scattered in 'multiple' locations.”
4. Be As the hint says “multiple”, we will observe all the packets.
5. The HTTP packets in POST method contains multipart/form-data header
6. The data in the header contains single letter in each packet.
7. Collect these letters from every HTTP packets.
8. Upon combining we get “ZmxhZ3ttdWx0MXBsM3A0cnRzYzBuZnVzM3N9” which is Base64 encoded.
9. Go to https://www.base64decode.org/ and decode it
10. The decoded data is the flag.

Flag: flag{mult1pl3p4rtsc0nfus3s}

3.2 Mystic Connections

Steps for Finding the Flag:

1. Go Download “cature_2.pcapng” file and open it with wireshark.
2. Since the description of the challenge is pointing out to “ARP”.
3. Enter arp in the filter to view all the “ARP” packets.

4. Now arrange the ARP packets in descending order by clicking on the “Time” section.
5. As you check each packet, there is single value data at the end which is visible in the ASCII Dump.
6. Note down each value from the sequence of packets which reveals the flag.

Flag: flag{ARP_b31ng_s1mpl3}

Category: Reverse Engineering

Description: Reverse engineering involves dissecting software or hardware systems to understand their functionalities, inner workings, and design principles by analyzing code, binaries, or physical components, often employed to uncover vulnerabilities, create patches, or develop interoperable solutions.

Challenge Overview: Reverse engineering challenges require participants to deconstruct and analyze software or hardware components to uncover hidden functionalities, discover vulnerabilities, or extract sensitive information.

4.1 DecryptQuest

Steps for Finding the Flag:

1. Go Download the “Answer.zip” file and extract it.
2. Upon extraction, you will get “Answers.txt” file.
3. Open the Answers.txt file, the data inside is Base64 encoded.
4. So, Go to https://www.base64decode.org/ and paste the data.
5. The decoded data consists of some messages, java code and link to a google drive.
6. Copy the java code and run it. It asks to enter an integer.
7. Feeding random integers to the code generates flags.
8. Open the google drive link https://drive.google.com/file/d/1A6Eh_oCtEniOYq8bxwrujRuyT1SU_Q-b/view
9. The link opens the “kEY.txt” file containing data that is in “Brainfuck” language.
10. Copy the data, Go to https://www.splitbrain.org/_static/ook/ and paste the data. Then click on “Brainfuck to Text”.

11. The converted data is in Base64 format.
12. Copy the data in https://www.base64decode.org/ to decode it.
13. This gives the hint to find the correct flag, which is 'Roses are red, Violets are blue, If one wants to pick the correct flag, Then they should seek the Unix Epoch as a clue'.
14. Its referring the 'Unix Epoch' as the clue.
15. The clue refers to 'Unix computer systems measure time as the number of seconds that have passed since Thursday 1 January 1970 00:00:00 UT, a point in time known as the Unix epoch'.
16. Since the java code is generating random flags based on random integers, the correct flag contains "1970" in it.
17. So, update the java code which runs a For loop from 0 to 1106 to generate all the flags.
18. Filter the flag which contains 1970 in it. Which is the intended flag.

Flag: flag{hjwilj111970djs}

4.2 4pP

Steps for Finding the Flag:

1. Download the "CTF.aia" file.
2. The hint is given as 'App Inventor, a cloud based development tool used to create Android app from the Massachusetts Institute of Technology.'
3. We will use the online app inventor tool.
4. Go to https://appinventor.mit.edu/ and click on "Create Apps".
5. You will be directed to https://ai2.appinventor.mit.edu/
6. Click on 'Projects' and then select 'import project(.aia) from my computer'.
7. Upload the "CTF.aia" file and give it a name, then click on OK.
8. There is a 'Blocks' button at the right upper corner. Click on it.
9. Its shows the structure of the app in blocks revealing the flag.

Flag: flag{M1T_4PP_1NV3NT0R_bf0285c53}

Category: Phishing

Description: Phishing involves the use of deceptive tactics, often through emails, messages, or websites, to trick individuals into divulging sensitive information such as passwords, credit card details, or personal data, commonly used in cyberattacks to gain unauthorized access or commit identity theft.

Challenge Overview: Phishing challenges entail identifying and analyzing deceptive emails, messages, or websites to recognize malicious intent, detect potential threats, and implement strategies to mitigate risks.

5.1 Phish Guard

Steps for Finding the Flag:

1. Download the “amazon.docx” file and Open it.
2. The document contains 3 pages but the data is only visible in 1st page.
3. The rest of the lines contains invisible data(whitespaces). So copy it.
4. Go to https://ideone.com/l/whitespace and paste the data in the code.
5. Click on “Run”.
6. The data gets decoded and the flag is displayed in stdout.

Flag: Flag{D0n't_g3t_ph1sh3d}