A logo with a symbol and text

Description automatically generatedRazorHack 2024

Writeup

“S-57x21-22 Await Further Instructions...?”

>Homer has kinda been acting weird lately. Someone put images up around the place of him hiding in a bush?

>Not sure what that's about but can you look into it?

>Best,

Shane Barnabas

CIO, RazorPower Co.

In this challenge participants had to first find this image of Homer which was stuck on several walls on both the 1st and 2nd floor of the building. Then if they turned it back it would show you the flag, flag{mmmdonuts}.

Once you submit that flag you see two new challenges unlocked, “What is Homer Hiding? and “CHAZ is Missing??”.

A logo with a symbol and text

Description automatically generatedRazorHack 2024

Writeup

“What is Homer Hiding?”

Homer has been acting sus all day, what's that about?

Author: Parker Darby (Pranav Mahesh)

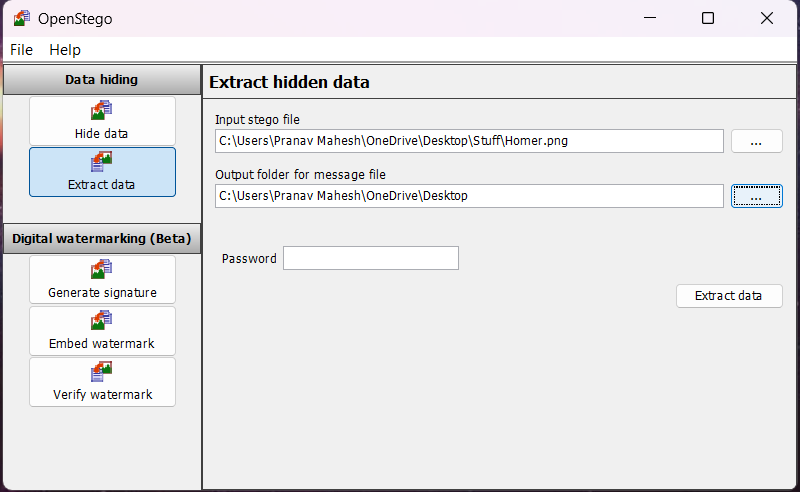
1. In this challenge participants were initially provided with just this image to download and use to find the flag. (Given it was a .png file it is a good tip to check which types of tools are compatible to use for extracting.)

In this case I used OpenStego, which is a free tool to download from the internet.

Cartoon a cartoon of a person in a green wall

Description automatically generated

1. Once you download it and run it you will see this screen, which shows you how to extract/hide files within a media file as well as gives you the option to add a password for it.



1. I clicked on Extract Data
2. Click on the 3 dots next to Input Stego file where we choose the image given to us then click on the 3 dots next to Output folder and choose where you want the contents pasted.
3. Typically, you might be given a password or rather have to find one, but in this case, I didn’t hide it using one hence we leave that box empty.
4. Once you follow the instructions, you find a zipped folder called “HomerMessage.zip” containing a text file and an mp3 file which gets pasted where you set your output folder, which in my case is Desktop.

A screen shot of a message

Description automatically generated

1. Once you extract the zipped folder, you will realize that the mp3 file is encrypted using an AES encryption. And the key is given to you in the .txt file but hidden using Caesar Cipher.

A black background with white text

Description automatically generated

1. To decrypt the cipher, there isn’t any particular website or tool so you can just search “Caesar Cipher decrypter” and use one of them. Once you decrypt it the text says, “to start press a”.

In this hint I said, “Don’t take it literally” because a lot of people were under the assumption that there was a physical button called “a”, when in reality I was trying to quote Simpsons but didn’t account for AES encryption being a 16-bit encryption hence had to cut it short.

1. After you get the hidden text, the way you decrypt the mp3 file is by creating a python script.

Code Breakdown:

A screenshot of a computer program

Description automatically generated

1. Imports:

* AES from Crypto.Cipher for the AES decryption.
* unpad from Crypto.Util.Padding to remove padding after decryption.

1. **Key Derivation** (derive\_key function):

* Convert the decryption phrase (e.g., "to start press a") into a 16-byte key.
* If the phrase is less than 16 bytes, it adds space; if it’s more, it truncates it to 16 bytes.

1. **Decrypting the Audio File** (decrypt\_audio\_file function):

* **Step 1**: Open the encrypted audio file in binary mode ('rb').
* **Step 2**: Skip reading the IV from the file because it’s derived from the phrase itself.
* **Step 3**: Create an AES cipher object in CBC mode with the phrase as both the key and IV.
* **Step 4**: Decrypt the encrypted audio data and remove padding using unpad.
* **Step 5**: Save the decrypted audio data to a new file, making it ready for playback.

1. **Usage**:

* Call derive\_key to convert the decryption phrase into a 16-byte key.
* Use decrypt\_audio\_file to decrypt the file with this derived key and save the result as the decrypted audio file.

1. Finally, you get the decrypted audio file which when you play would say, “The flag is h o m e r w I l l s a v e” as in flag{homerwillsaveus}