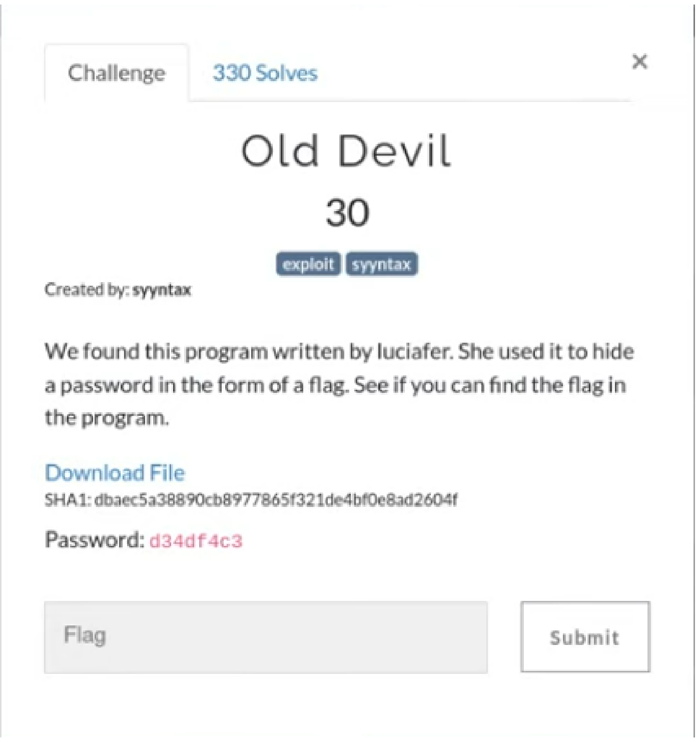
Deadface CTF Writeup

Binary Exploitation

1.Old Devil



Old Devil

30

Created by: syyntax

We found this program written by luciafer. She used it to hide a password in the form of a flag. See if you can find the flag in the program.

Download File

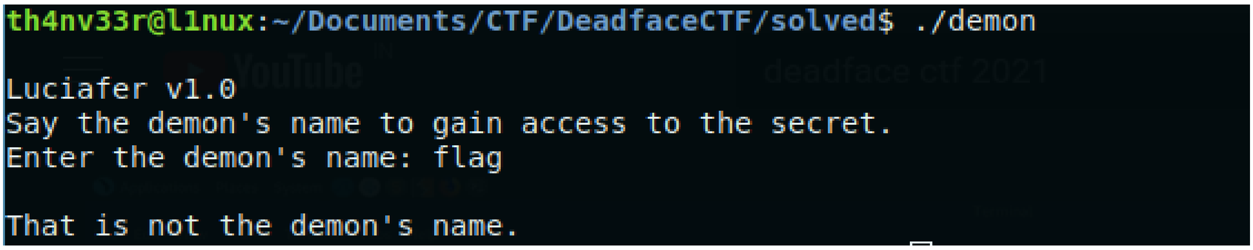
SHA1: dbaec5a38890cb8977865f321de4bf0e8ad2604f

Password: d34df4c3

Flag

Step 1: As usual checking the file type using **file** command
The file itself is a **ELF Binary** file means a Linux executable file

Step 2: Running the program it asks for a demon name to access the secret



```
th4nv33r@l1nux:~/Documents/CTF/DeadfaceCTF/solved$ ./demon

Luciafer v1.0
Say the demon's name to gain access to the secret.
Enter the demon's name: flag

That is not the demon's name.
```

Step 3:I checked for strings for any clues for this challenge,then i found they are using **strcmp**

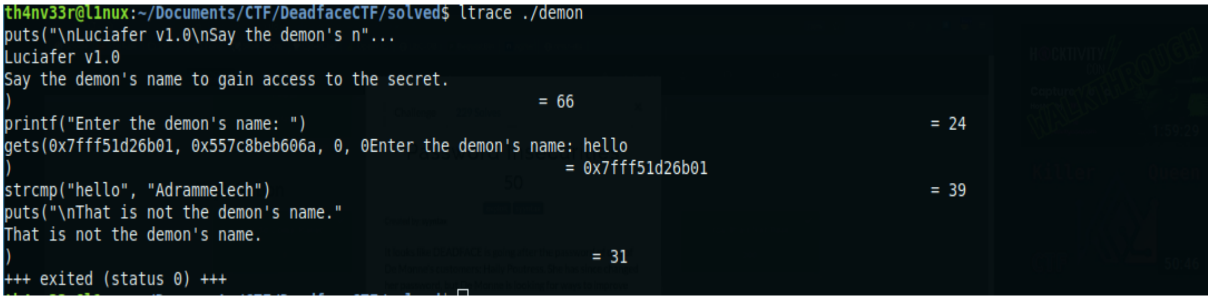
Note: The strcmp() Function in C. ... The strcmp() function is used to compare two strings two strings str1 and str2

Step 3: Then i tried to debug the program so far i used **ltrace**

Note: ltrace is a library call tracer and it is primarily used to trace calls made by programs to library functions.

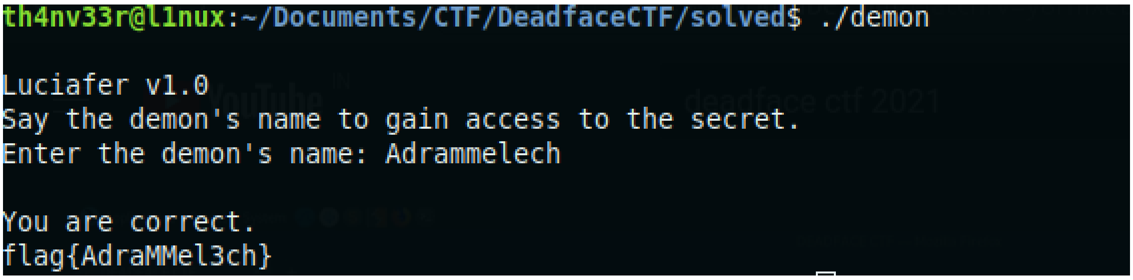
Step 4:passing hello as a string then i found the demon name

Adrammelech



```
th4nv33r@l1nux:~/Documents/CTF/DeadfaceCTF/solved$ ltrace ./demon
puts("\nLuciafer v1.0\nSay the demon's n"...
Luciafer v1.0
Say the demon's name to gain access to the secret.
)                                                            = 66
printf("Enter the demon's name: ")                                                                      = 24
gets(0x7fff51d26b01, 0x557c8beb606a, 0, 0Enter the demon's name: hello
)                                                               = 0x7fff51d26b01
strcmp("hello", "Adrammelech")                                                                          = 39
puts("\nThat is not the demon's name."
That is not the demon's name.
)                                                                  = 31
+++ exited (status 0) +++
```

Step 5: Prompting the name in the program Boooomm!!.Got the Flag :)



```
th4nv33r@l1nux:~/Documents/CTF/DeadfaceCTF/solved$ ./demon

Luciafer v1.0
Say the demon's name to gain access to the secret.
Enter the demon's name: Adrammelech

You are correct.
flag{AdraMMel3ch}
```

flag{AdraMMel3ch}