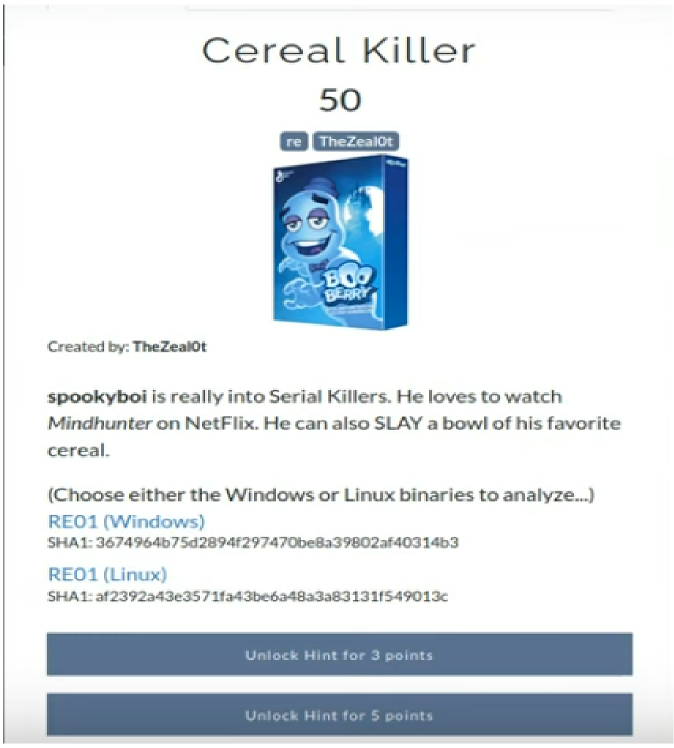
DeadFace CTF Writeup

Reverse Engineering:

1.Cereal Killer 1



Cereal Killer

50

Created by: TheZeal0t

spookyboi is really into Serial Killers. He loves to watch *Mindhunter* on NetFlix. He can also SLAY a bowl of his favorite cereal.

(Choose either the Windows or Linux binaries to analyze...)

RE01 (Windows)

SHA1: 3674964b75d2894f297470be8a39802af40314b3

RE01 (Linux)

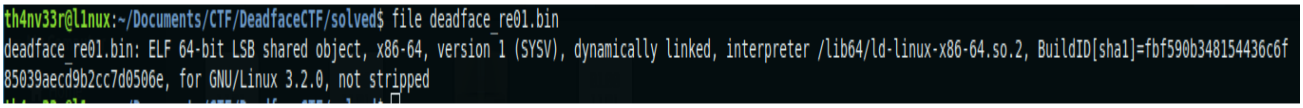
SHA1: af2392a43e3571fa43be6a48a3a83131f549013c

Walkthrough:

Step1: Downloaded the file which was given on the challenge

Step2: Checking the file type using the file command

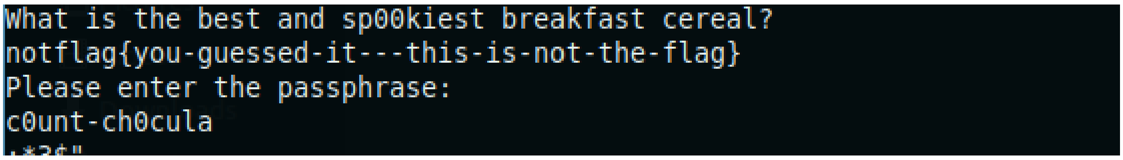
file deadface_re01.bin



```
th4nv33r@l1nux:~/Documents/CTF/DeadfaceCTF/solved$ file deadface_re01.bin
deadface_re01.bin: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=fbf590b348154436c6f
85039aecd9b2cc7d0506e, for GNU/Linux 3.2.0, not stripped
```

The file is a ELF type binary file

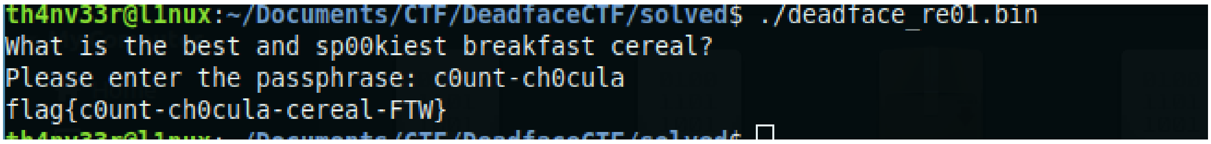
Step3: Now checking the strings of the file so i found something weird on the strings



```
What is the best and sp00kiest breakfast cereal?
notflag{you-guessed-it---this-is-not-the-flag}
Please enter the passphrase:
c0unt-ch0cula
.*3$"
```

There is a text on the string called **c0unt-ch0cula**

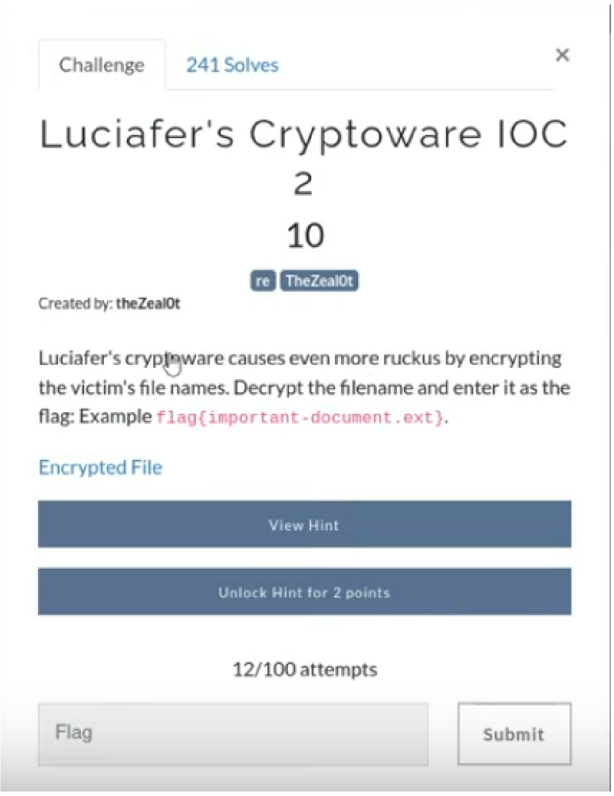
Step4: So i grabbed the text and tried to run the file it asks for a password then i pasted the text which i copied in the strings and boom….GOT THE FLAG



```
th4nv33r@linux:~/Documents/CTF/DeadfaceCTF/solved$ ./deadface_re01.bin
What is the best and sp00kiest breakfast cereal?
Please enter the passphrase: c0unt-ch0cula
flag{c0unt-ch0cula-cereal-FTW}
th4nv33r@linux:~/Documents/CTF/DeadfaceCTF/solved$
```

flag{c0unt-ch0cula-cereal-FTW}

2.Luciafer's Cryptoware IOC 2



Luciafer's Cryptoware IOC 2

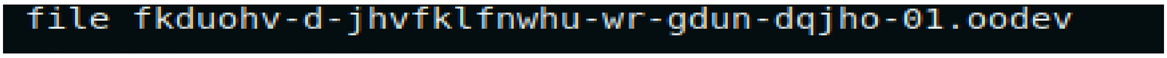
10

Created by: theZeal0t

Luciafer's cryptoware causes even more ruckus by encrypting the victim's file names. Decrypt the filename and enter it as the flag: Example flag{important-document.ext}.

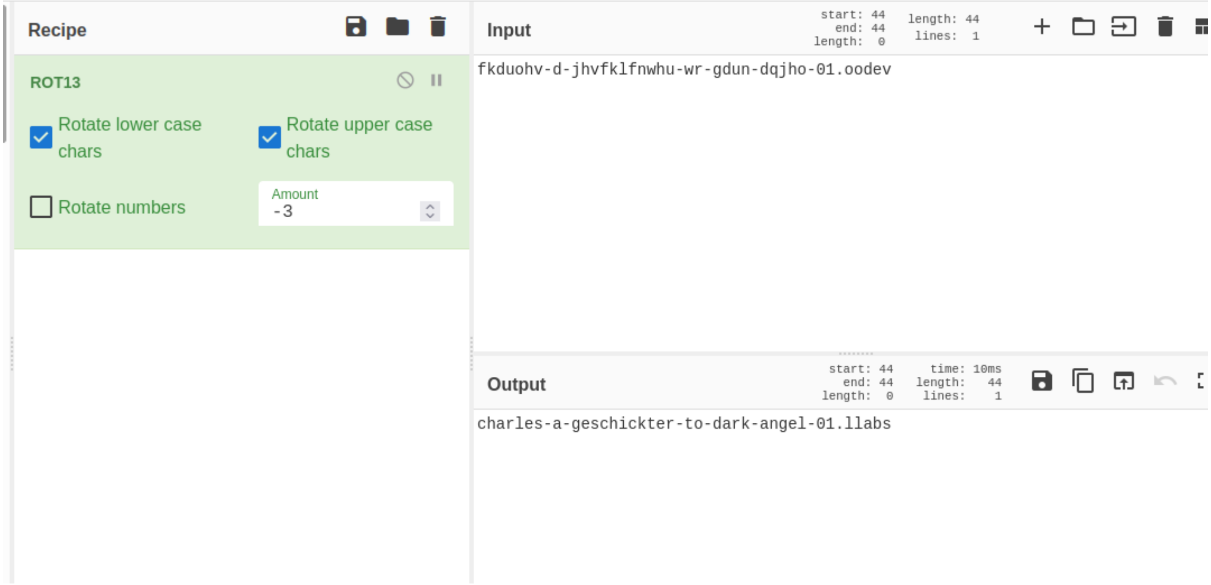
12/100 attempts

Step 1: Checking out the file type it has a kind of some weird file name



```
file fkduohv-d-jhvfklfnwhu-wr-gdun-dqjho-01.oodev
```

Step 2: Then i copied the file name and tried to decode the file name using https://gchq.github.io/CyberChef/
Selecting the **ROT13** Decoding in the Cyberchef



ROT13

☑ Rotate lower case chars ☑ Rotate upper case chars

□ Rotate numbers

Amount
-3

Input

```
start: 44   length: 44
  end: 44    lines: 1
length: 0
```

```
fkduohv-d-jhvfklfnwhu-wr-gdun-dqjho-01.oodev
```

Output

```
start: 44     time: 10ms
  end: 44   length:   44
length: 0    lines:    1
```

```
charles-a-geschickter-to-dark-angel-01.llabs
```

flag{charles-a-geschickter-to-dark-angel-01.labs}