Reverse & Cracking

Crack : Crack-1

1 . Identify the file

At first, we identify the type of the file with the command file.

```
rahmonex@Cyclop-os:~/Documents/Git/EFREI-M1-Ethical-Hacking/Reverse & Cracking/Level 1$ file crackme-1
crackme-1: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/
ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=7c4a00c885d8366b26a21d16386b3d33991556c7, not stri
pped
```

File type : ELF 64-bit LSB pie executable

2 . Basic Analysing

At first we retrieve the human readable strings in the document using the command :

'strings crackme-1'

```
__gmon_start__
_ITM_registerTMCloneTable
u3UH
[]A\A]A^A_
[input]:
Correct flag! :-) You're getting good at that!
Incorrect flag... :'(
;*3$"
Free-fL4g!ForTheLULZ
4ma2inz-F1ag!x86FTW
d0Ubtfu1-fLaG?Srsly
Real_F1AG!OrNot...
1nTeRESTING_flag!BobIsHere
l4st_bUt_Not_1east_f!ag|??
GCC: (GNU) 8.2.1 20180831
```

We can see some Flags here that we can test (since they are not a lot of them we ca ntest one by one)

3 . Executing the file

As usual we need to transform the file to executable and we run it with the following commands :

```
rahmonex@Cyclop-os:~/Documents/Git/EFREI-M1-Ethical-Hacking/Reverse & Cracking/L
evel 1$ chmod +x crackme-1
rahmonex@Cyclop-os:~/Documents/Git/EFREI-M1-Ethical-Hacking/Reverse & Cracking/L
evel 1$ ./crackme-1
[input]:
```

4 . Testing the flags

And now, we proceed with testing the Flags found :

```
rahmonex@Cyclop-os:~/Documents/Git/EFREI-M1-Ethical-Hacking/Reverse & Cracking/Level 1$ ./crackme-1
[input]: Free-fL4g!ForTheLULZ
Incorrect flag... :'(
rahmonex@Cyclop-os:~/Documents/Git/EFREI-M1-Ethical-Hacking/Reverse & Cracking/Level 1$ ./crackme-1
[input]: 4ma2inz-F1ag!x86FTW
Incorrect flag... :'(
rahmonex@Cyclop-os:~/Documents/Git/EFREI-M1-Ethical-Hacking/Reverse & Cracking/Level 1$ ./crackme-1
[input]: d0Ubtfu1-fLaG?Srsly
Correct flag! :-) You're getting good at that!
```

So the Flag is :

d0Ubtfu1-fLaG?Srsly