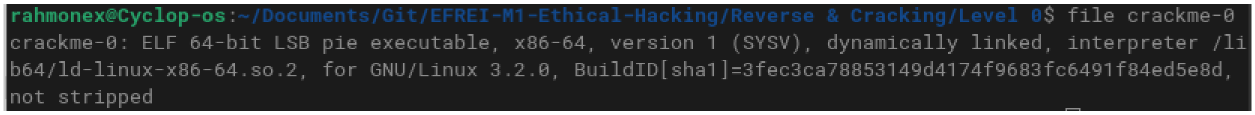
Bilel RAHMOUNI & Meriem NOUIRA

Reverse & Cracking

`Crack : Crack-0`

1 . Identify the file

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

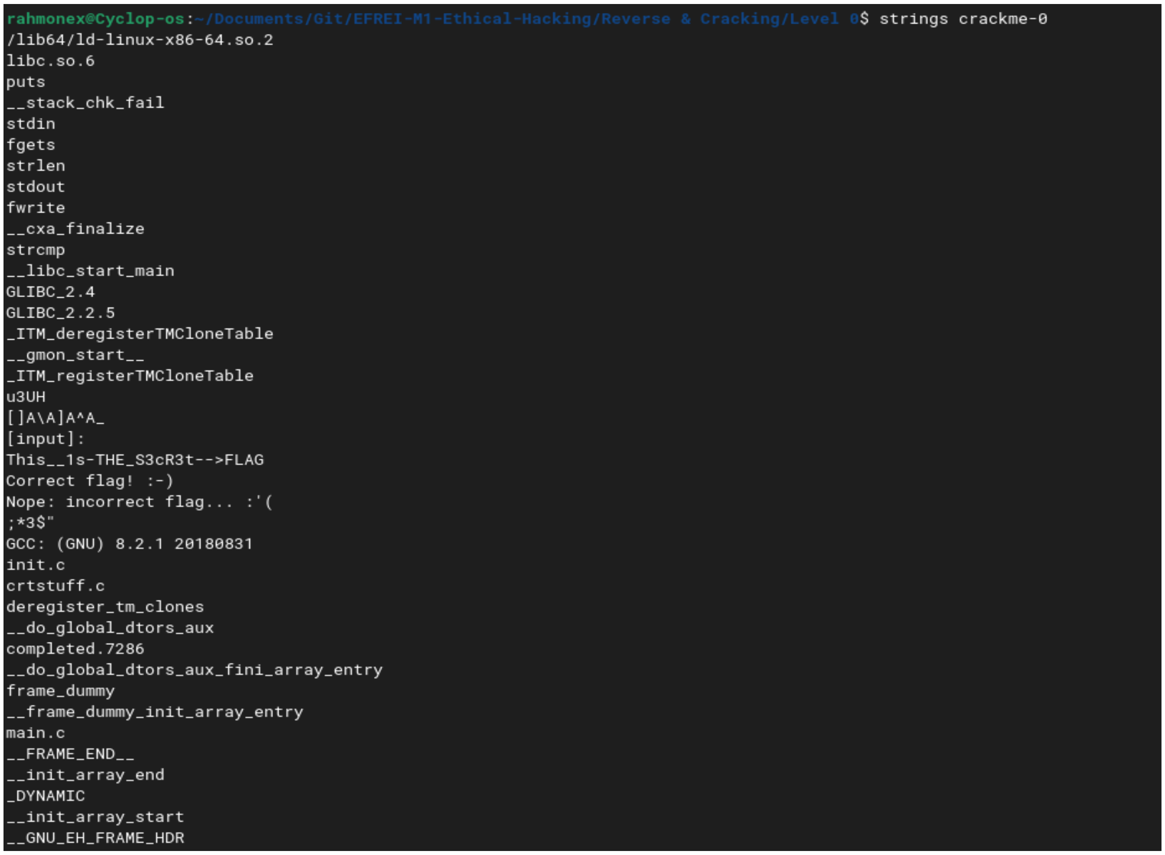


```
rahmonex@Cyclop-os:~/Documents/Git/EFREI-M1-Ethical-Hacking/Reverse & Cracking/Level 0$ file crackme-0
crackme-0: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /li
b64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=3fec3ca78853149d4174f9683fc6491f84ed5e8d,
not stripped
```

File type : ELF 64-bit LSB pie executable

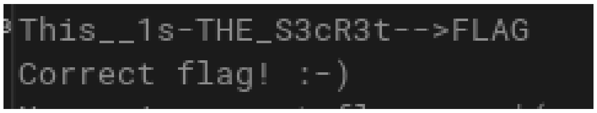
2 . Basic Analysis

After that we use the command “strings” to retrieve the group of words human readable in the document :



```
rahmonex@Cyclop-os:~/Documents/Git/EFREI-M1-Ethical-Hacking/Reverse & Cracking/Level 0$ strings crackme-0
/lib64/ld-linux-x86-64.so.2
libc.so.6
puts
__stack_chk_fail
stdin
fgets
strlen
stdout
fwrite
__cxa_finalize
strcmp
__libc_start_main
GLIBC_2.4
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u3UH
[]A\A]A^A_
[input]:
This__1s-THE_S3cR3t-->FLAG
Correct flag! :-)
Nope: incorrect flag... :'(
;*3$"
GCC: (GNU) 8.2.1 20180831
init.c
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.7286
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
main.c
__FRAME_END__
__init_array_end
_DYNAMIC
__init_array_start
__GNU_EH_FRAME_HDR
```

And we can see this output here :



```
This__1s-THE_S3cR3t-->FLAG
Correct flag! :-)
```

We can go with the hypothesis that the Flag is : **This__1s-THE_S3cR3t-->FLAG**

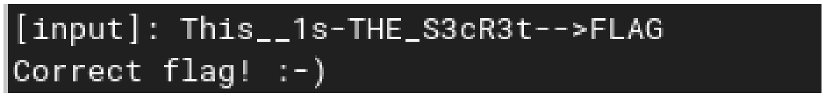
3 . Verify the response

In a first place, we transform the file in an executable file with the following command :

chmod +x crackme-0

And we execute :

./crackme-0



```
[input]: This__1s-THE_S3cR3t-->FLAG
Correct flag! :-)
```