[ANGRy]

Tono diberikan sebuah program oleh temannya. Tetapi, program itu diproteksi oleh sebuah password. Tono tidak diberi tahu password nya. Setelah berhari-hari mencoba password yang benar, Tono pun marah. Tolong bantu Tono untuk mencari tahu password nya. Format flag : BeeFest{“passwordnya”}

Write-Up

Pada soal kali ini kita diberikan sebuah file elf, 64 bit stripped.

```
sscape@ubuntu:~/Desktop/test_soal$ file ANGRy
ANGRy: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked,
interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=5e7
0f9dd2408b563f722fcc9ac31e8f858d5b8d9, stripped
```

File ini akan meminta password ketika dijalankan, yang kemudian password tersebut adalah flag nya.

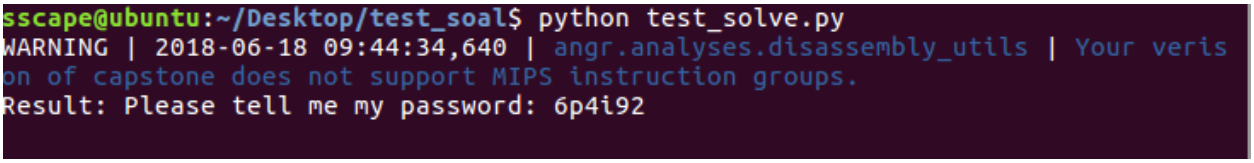
```
sscape@ubuntu:~/Desktop/test_soal$ ./ANGRy
Please tell me my password: uwotm8
That's not it! Try again.
```

Agar lebih mudah, kali ini saya akan menggunakan angr untuk mendapatkan password nya.

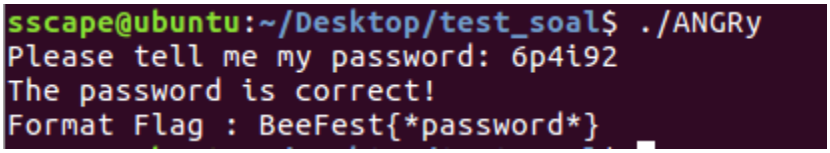
```
#!/usr/bin/env python
import angr

project = angr.Project("./ANGRy", auto_load_libs=False)
@project.hook(0x4009b2)
def print_flag(state):
    print "Result: {0}\n".format(state.posix.dump_fd(0))
    project.terminate_execution()

project.execute()
```

@project.hook diisi dengan alamat success program

Lalu, setelah script dijalankan



Kita tinggal input saja pada program tersebut



BeeFest{6p4i92}