PERSIAPAN LKS

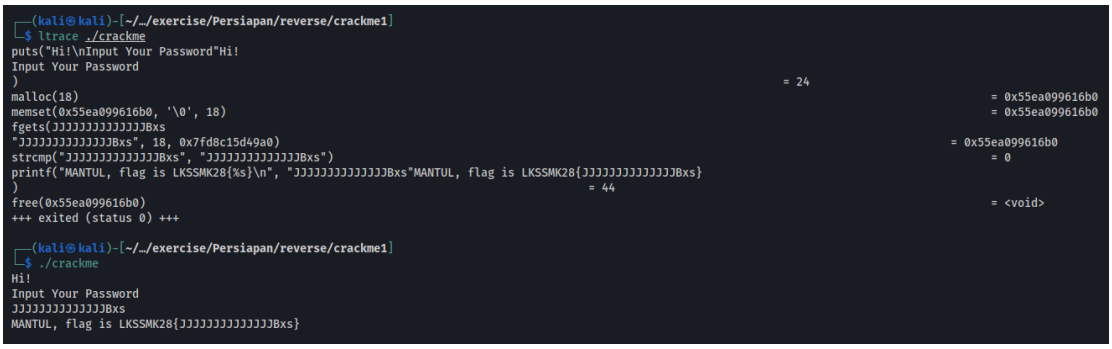
REJA REVALDY F.

COMPLETED

- Crackme1
- Petiharta
- Reverse1
- Reverse2
- Whoami

## Crackme1

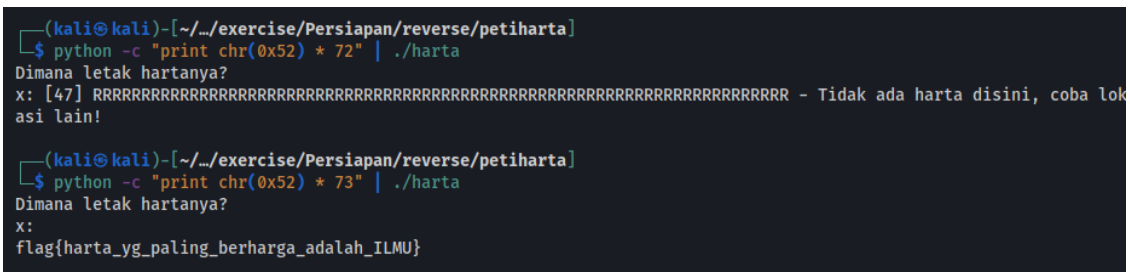
1. Diberikan sebuah program dan kita harus menginputkan sebuah password, lalu saya langsung saja menggunakan ltrace dan menemukan strcmp inputan kita dibandingkan dengan sebuah string “JJJJJJJJJJJJJBxs”, lalu saya langsung saja coba inputkan string tersebut dan menemukan flagnya




**Flag = LKSSMK28{JJJJJJJJJJJJJBxs}**

## Petiharta

1. Diberikan sebuah program yang berisikan pencarian harta, lalu saya coba menjalankan program strings untuk melihat library c yang dipakai disini saya menemukan gets yang dimana gets ini rentan di buffer overflow, lalu saya coba melakukan buffer overflow menggunakan python

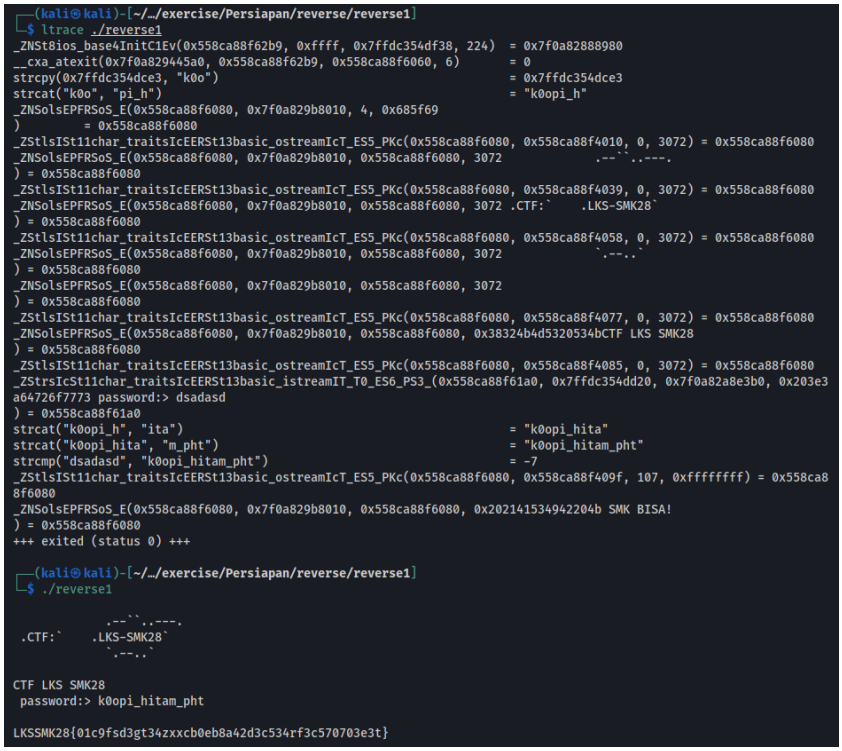


2. Disini ditemukan bahwa program akan terjadi buffer overflow setelah inputan ke 72 lalu saya coba inputkan 73 string dan string untuk flag nya muncul

**FLAG = palui{harta_yg_paling_berharga_adalah_ILMU}**

## Reverse1

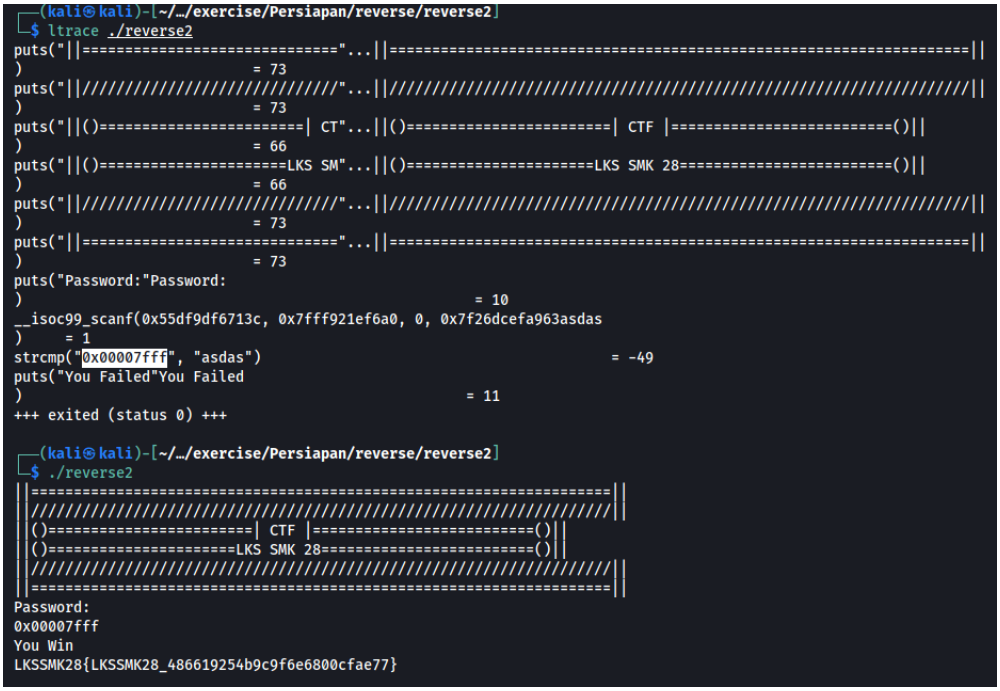
1. Disini kita diberikan sebuah program yang berisikan inputan untuk password lalu saya menggunakan cara yang sama dengan crackme1 dan saya mendapatkan flagnya




**FLAG = LKSSMK28{01c9fsd3gt34zxxcb0eb8a42d3c534rf3c570703e3t}**

Reverse2

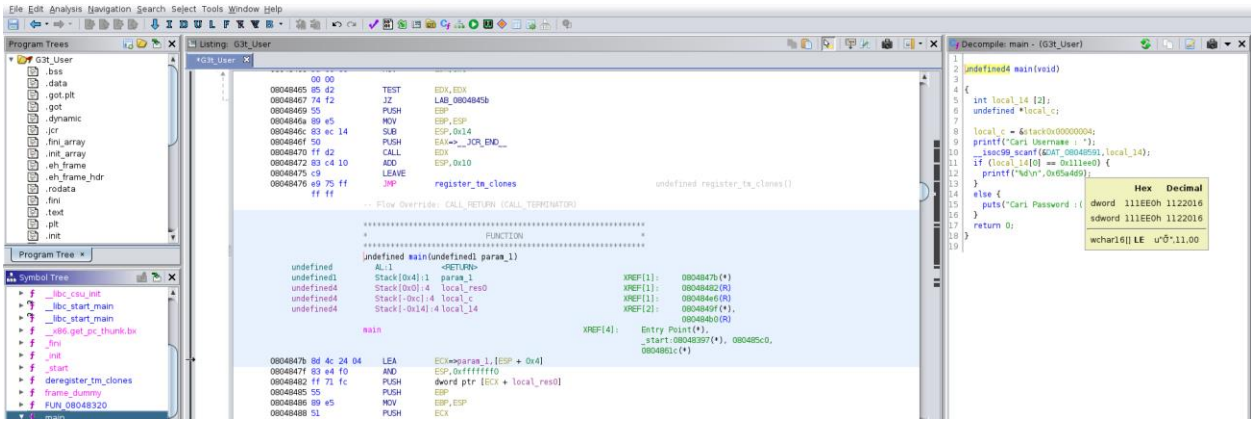
1. Disini kita diberikan sebuah program yang berisikan inputan untuk password lalu saya menggunakan cara yang sama dengan reverse1 dan saya mendapatkan flagnya



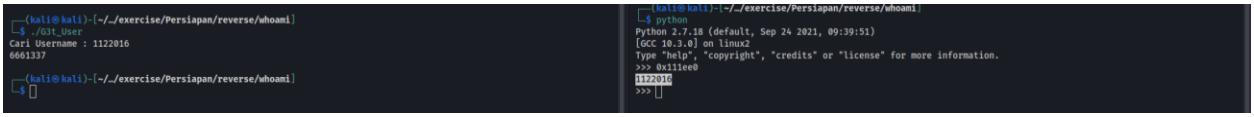

**FLAG = LKSSMK28{LKSSMK28_486619254b9c9f6e6800cfae77}**

Whoami

1. Diberikan sebuah program yang memiliki fungsi mencari username lalu memunculkan password, setelah saya menggunakan ltrace saya tidak menemukan apa apa lalu saya coba ghidra untuk melihat pseudo code program ini lalu saya menemukan kondisi dimana jika inputan kita sama dengan hex yang diberikan maka akan memunculkan password nya



2. Disini saya langsung coba masukan hex tersebut dan gagal lalu saya coba ubah ke decimal dan berhasil memunculkan password dari user tersebut



**FLAG = {1122016}**