A picture containing text

Description automatically generated

Pada soal nomor 1 diminta untuk mengoverflow input buffer sebanyak 72 byte lalu menuliskan return address yang diinginkan yaitu 0x401aa1. Oleh karena itu dengan menggunakan tool pipe yang diberikan pada praktikum orkom 3 saya memasukan input 72 byte serta 8 byte sisanya untuk alamat return

A screenshot of a computer

Description automatically generated with medium confidence

Saya hanya perlu memasukan input tersebut dengan bantuan kit hex2raw.py yang telah disediakan. Sehingga didapatkan flag dari fungsi

Text

Description automatically generated

Pada soal 2.0 terdapat 2 fungsi yang memberikan flag yang dipecah pada win\_stage\_1 dan win\_stage2. Oleh karena itu hanya perlu melakukan return ke kedua alamat tersebut satu persatu hingga didapatkan flag yang utuh. Namun karena pada soal ini tidak diberikan alamat dari kedua fungsi, maka dilakukan pengecekan dengan gdb terlebih dahulu.