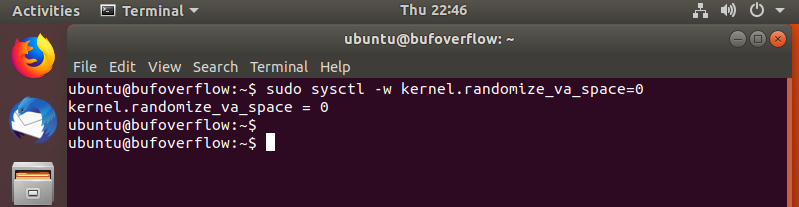
# 2, Thuc Hanh

## Lab1

sudo sysctl -w kernel.randomize\_va\_space=0

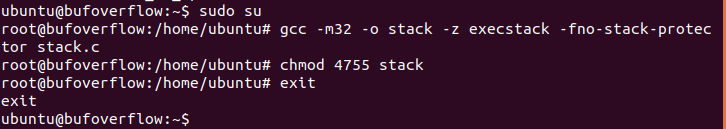


$ sudo su

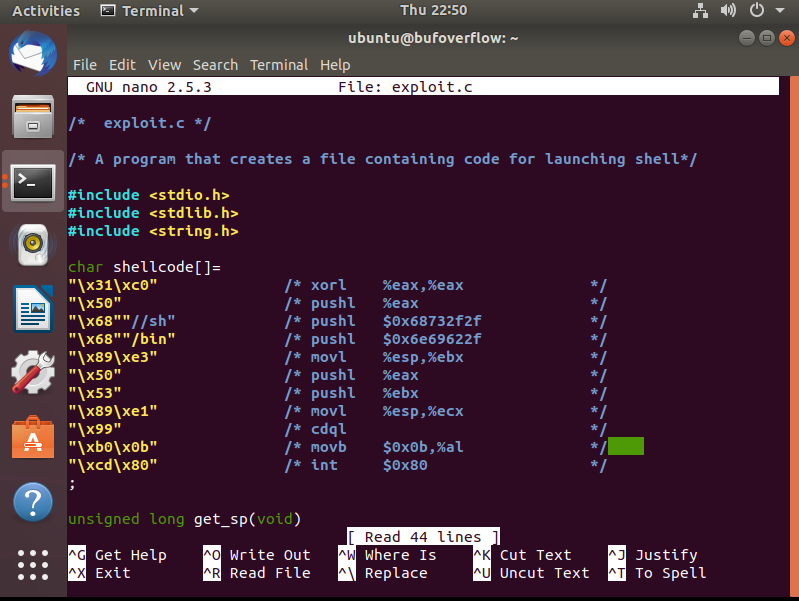
# gcc -m32 -o stack -z execstack -fno-stack-protector stack.c

# chmod 4755 stack

# exit

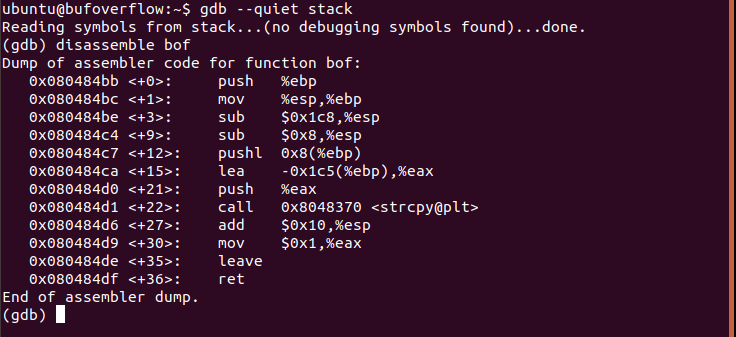


sudo nano exploit.c



gdb --quiet stack

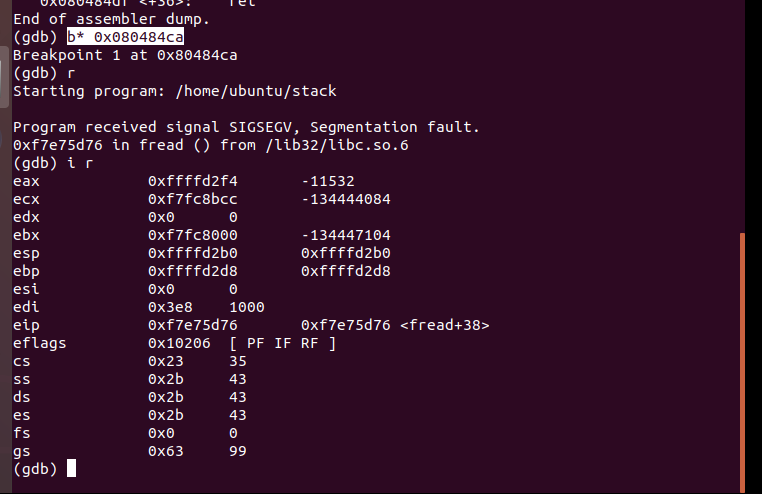
disassemble bof



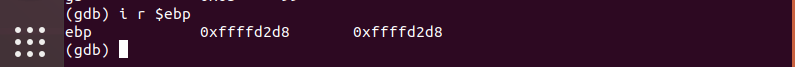
b\* 0x080484ca

r

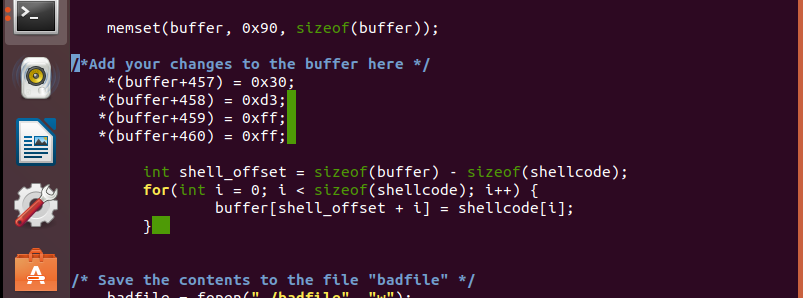
i r

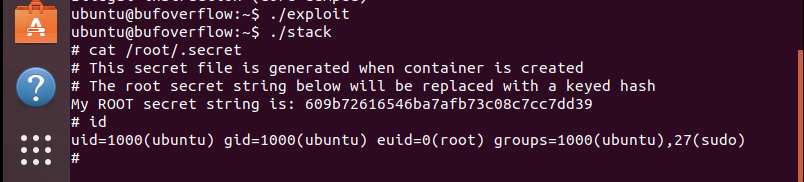


i r $ebp



sudo nano exploit.c

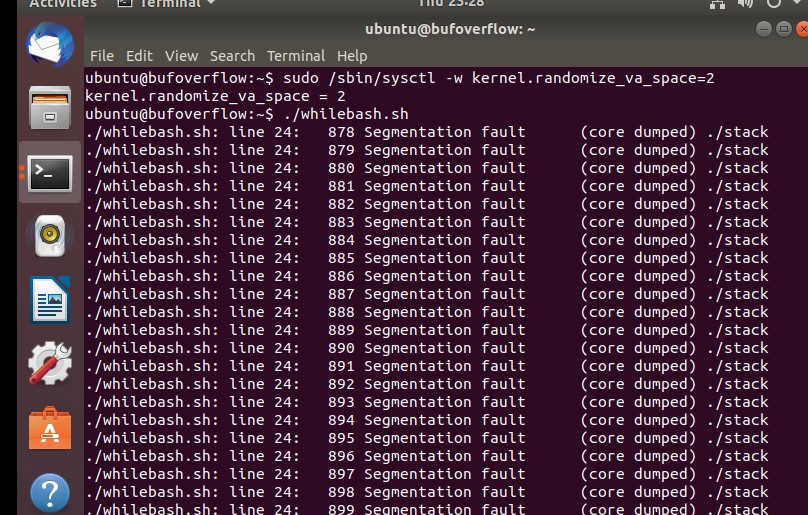




## Lab2

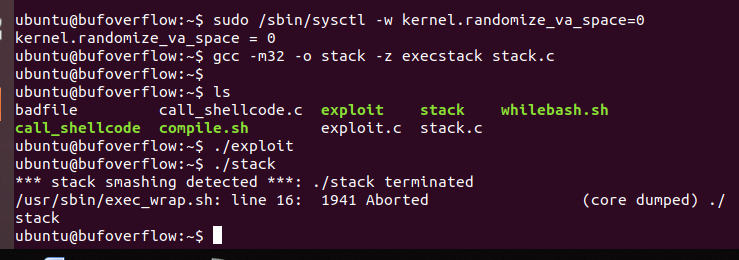
sudo /sbin/sysctl -w kernel.randomize\_va\_space=2

./whilebash.sh



sudo /sbin/sysctl -w kernel.randomize\_va\_space=0

gcc -m32 -o stack -z execstack stack.c



gcc -m32 -o stack -fno-stack-protector -z noexecstack stack.c

chmod 4755 stack

