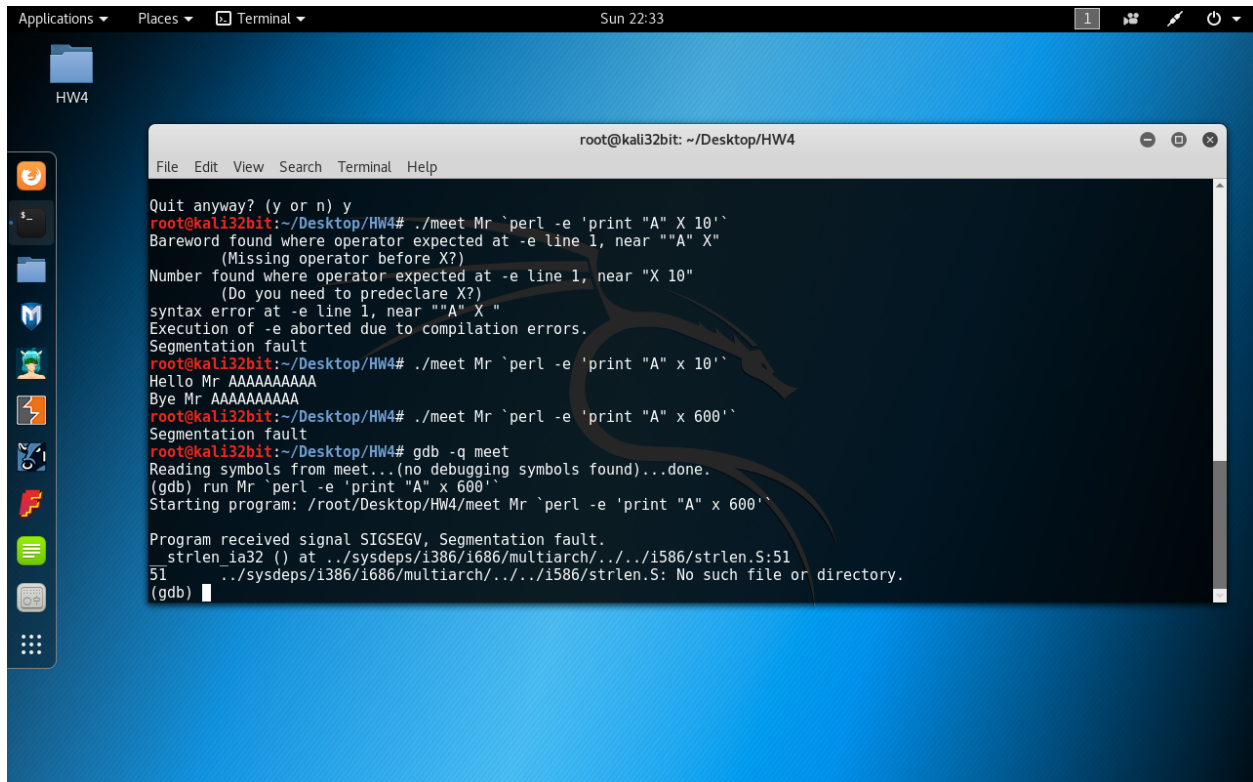


Michael Esposito  
Computer Network Defense  
HW4

1. Screenshot of current value of my “eip”



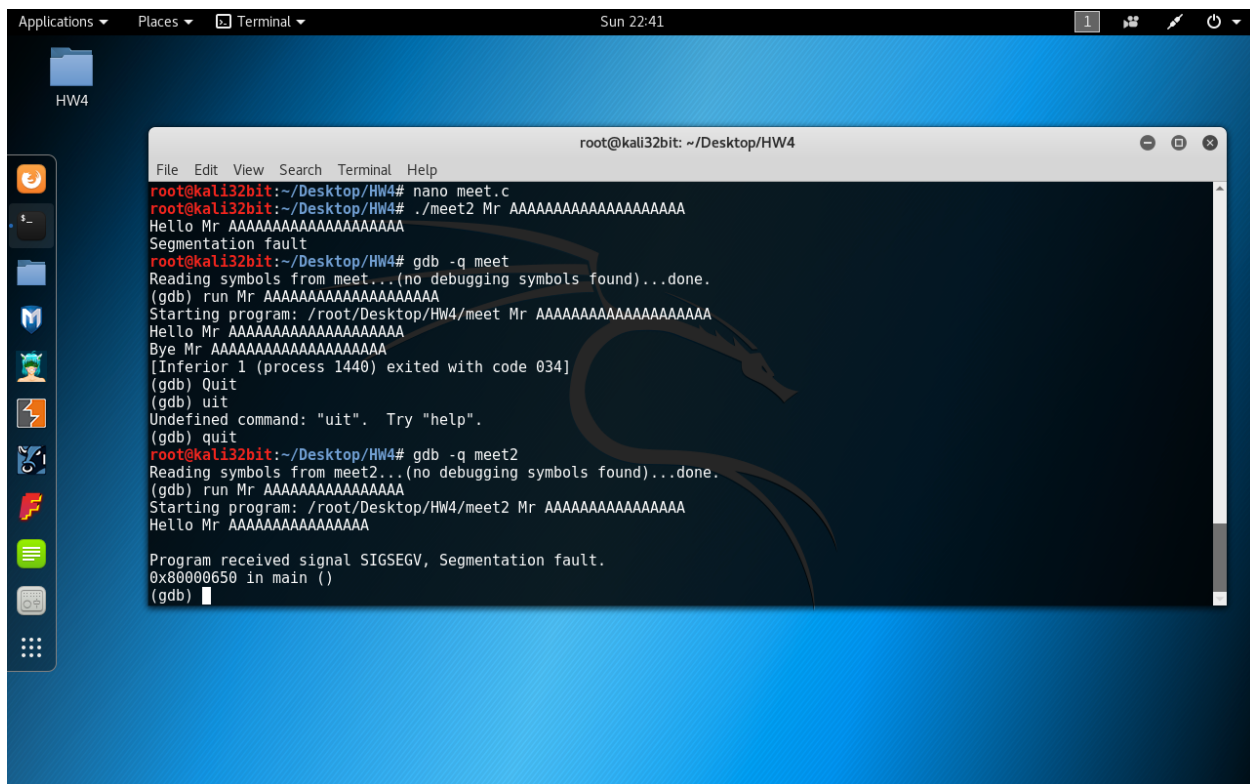
```
Applications ▾ Places ▾ Terminal ▾ Sun 22:33 1
HW4

root@kali32bit: ~/Desktop/HW4
File Edit View Search Terminal Help

Quit anyway? (y or n) y
root@kali32bit:~/Desktop/HW4# ./meet Mr `perl -e 'print "A" X 10`'
Bareword found where operator expected at -e line 1, near ""A" X"
(Missing operator before X?)
Number found where operator expected at -e line 1, near "X 10"
(Do you need to predeclare X?)
syntax error at -e line 1, near ""A" X "
Execution of -e aborted due to compilation errors.
Segmentation fault
root@kali32bit:~/Desktop/HW4# ./meet Mr `perl -e 'print "A" x 10`'
Hello Mr AAAAAAAAAA
Bye Mr AAAAAAAAAA
root@kali32bit:~/Desktop/HW4# ./meet Mr `perl -e 'print "A" x 600`'
Segmentation fault
root@kali32bit:~/Desktop/HW4# gdb -q meet
Reading symbols from meet...(no debugging symbols found)...done.
(gdb) run Mr `perl -e 'print "A" x 600`'
Starting program: /root/Desktop/HW4/meet Mr `perl -e 'print "A" x 600`'

Program received signal SIGSEGV, Segmentation fault.
strlen_ia32 () at ../sysdeps/i386/i686/multiarch/../../../../i586/strlen.S:51
51  ../sysdeps/i386/i686/multiarch/../../../../i586/strlen.S: No such file or directory.
(gdb)
```

This didn't give me an EIP value, so I modified meet.c. I replaced char name[400] with char name[10], that way I could type in a greater number of As manually without using perl. This generated the following output:



EIP = 0x80000650