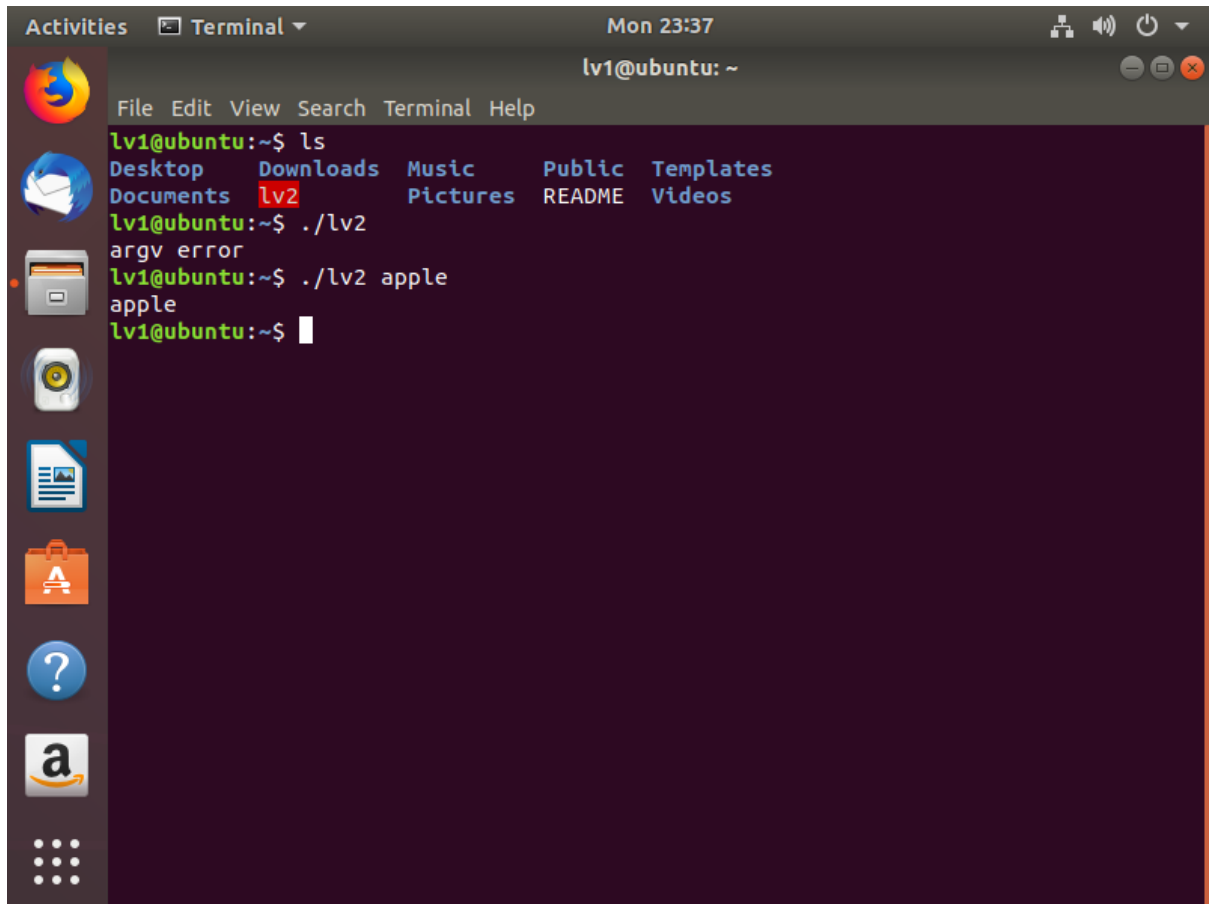


Wargame Write-up

유준혁

level1 -> level2



```
lv1@ubuntu:~$ ls
Desktop  Downloads  Music      Public    Templates
Documents lv2        Pictures   README    Videos

lv1@ubuntu:~$ ./lv2
argv error

lv1@ubuntu:~$ ./lv2 apple
apple

lv1@ubuntu:~$
```

lv2를 실행해 보았더니 lv1과 마찬가지로 argv에러가 뜬 것을 확인하였고 apple이라는 argv를 넣었더니 그대로 출력되었다.

```
Activities Terminal Mon 23:41 lv1@ubuntu: ~
File Edit View Search Terminal Help
▶ f 0 8048380 _start
Breakpoint *_start
pwndbg> pdisas main
▶ 0x8048430 <main>      push    ebp
0x8048431 <main+1>      mov     ebp, esp
0x8048433 <main+3>      sub     esp, 0x10
0x8048436 <main+6>      cmp     dword ptr [ebp + 8], 1
0x804843a <main+10>     jg      main+35 <0x8048453>

0x804843c <main+12>     push    0x80484d0
0x8048441 <main+17>     call   printf@plt <0x8048350>

0x8048446 <main+22>     add     esp, 4
0x8048449 <main+25>     push    0
0x804844b <main+27>     call   exit@plt <0x8048360>

0x8048450 <main+32>     add     esp, 4
pwndbg>
0x8048453 <main+35>     mov     eax, dword ptr [ebp + 0xc]
0x8048456 <main+38>     add     eax, 4
0x8048459 <main+41>     mov     edx, dword ptr [eax]
0x804845b <main+43>     push    edx
0x804845c <main+44>     lea     eax, [ebp - 0x10]
0x804845f <main+47>     push    eax
0x8048460 <main+48>     call   strcpy@plt <0x8048370>

0x8048465 <main+53>     add     esp, 8
0x8048468 <main+56>     lea     eax, [ebp - 0x10]
0x804846b <main+59>     push    eax
```

pwndbg로 디버깅을 해본 결과 16바이트의 공간이 할당되어 있음을 알 수 있다. (0x10)


```
Activities Terminal Tue 00:03 lv1@ubuntu: ~/yun
File Edit View Search Terminal Help
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
[ REGISTERS ]
EAX 0x19
EBX 0x0
ECX 0x0
EDX 0xf7fb7890 ← 0x0
EDI 0x0
ESI 0xf7fb6000 ← 0x1d7d6c
EBP 0x39393939 ('9999')
ESP 0xffffd1d0 ← 0x0
EIP 0x38383838 ('8888')
[ DISASM ]
Invalid address 0x38383838
[ STACK ]
00:0000 esp 0xffffd1d0 ← 0x0
01:0004 0xffffd1d4 → 0xffffd264 → 0xffffd41c ← './lv2'
02:0008 0xffffd1d8 → 0xffffd270 → 0xffffd43b ← 'CLUTTER_IM_MODULE=xim'
03:000c 0xffffd1dc → 0xffffd1f4 ← 0x0
04:0010 0xffffd1e0 ← 0x1
```

ESP레지스터의 주소가 0xffffd1d0임을 알 수 있다.

