l_2

Connor Taffe

April 1, 2016

1 Task 1

Task one is just to fill the proper line in in `exploit.c`:

```
/* You need to fill the buffer with appropriate contents here */
memcpy(buffer, shellcode, sizeof(shellcode));
```

The following three figures show me editing and running the programs.

2 Task 2

Address randomization has no effect on the stack addressed relative to the stack. The stack grows linearly regardless unless you are compiling with split stacks, which in such a small area like a frame, would not cause issues.

3 Task 3

Stack Guard causes the stack smashing to be detected at runtime.

Figure 1: Disabling memory layout randomization

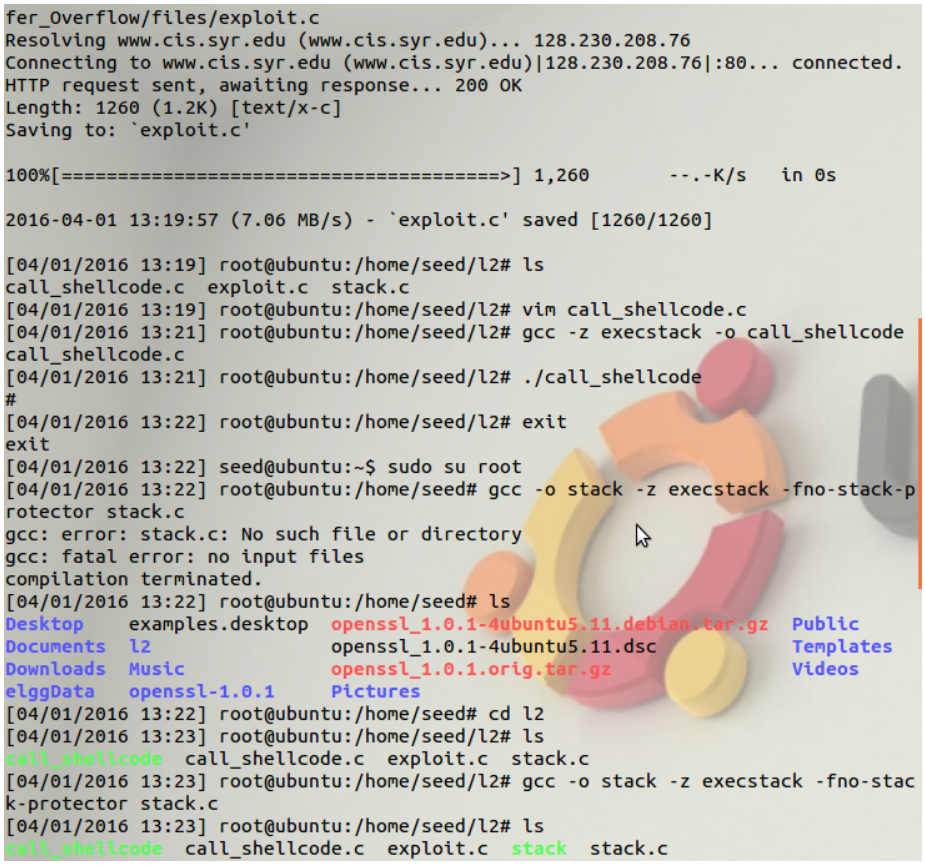

Figure 2: Running `call_shellcode.c`

Figure 3: Successfully running `exploit.c` and `stack.c`

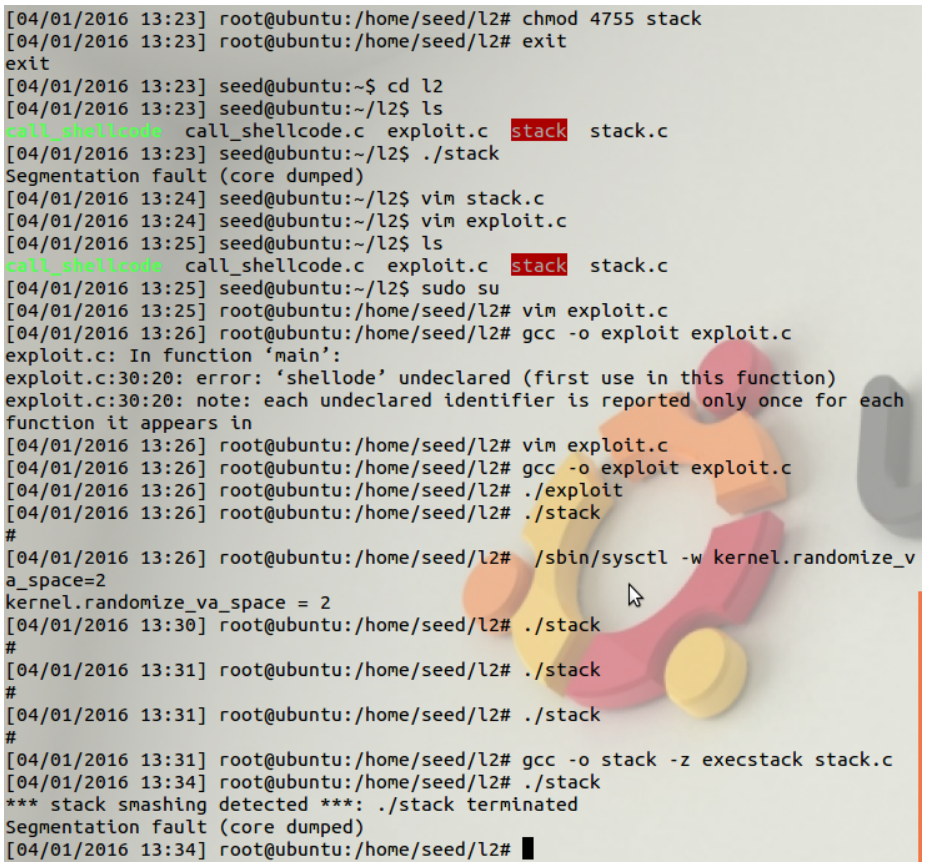

Figure 4: Turning on memory layout randomization, running program, compiling with stack smash detection, running program yet again