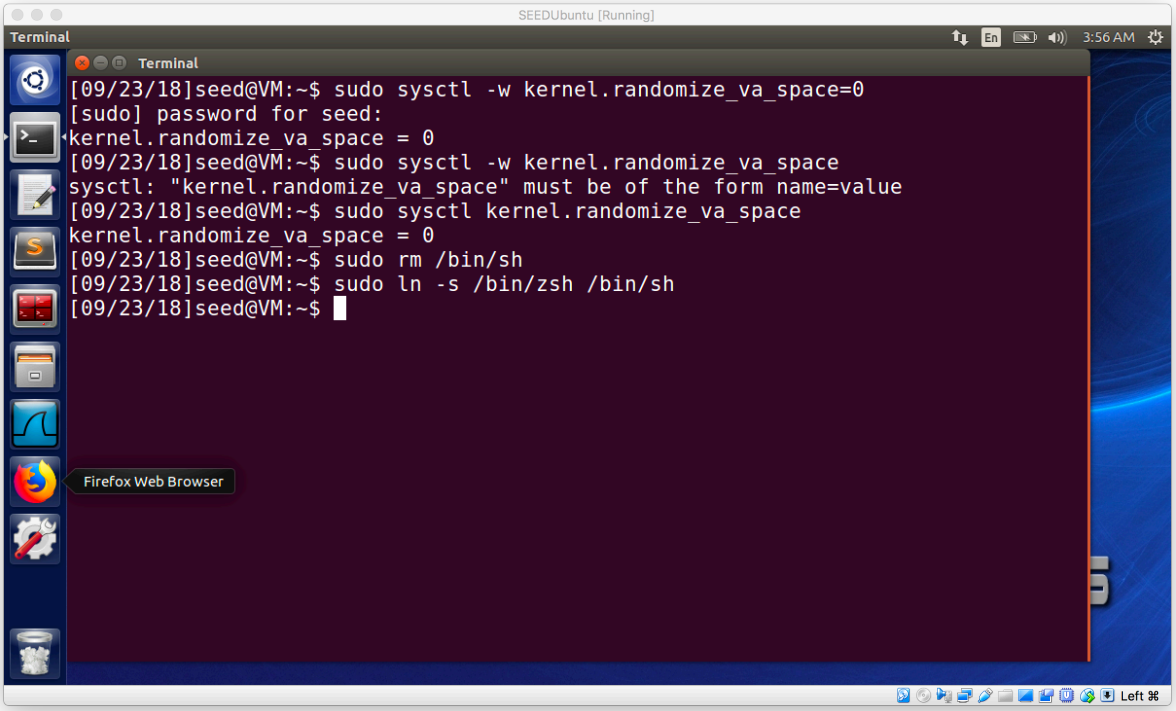
LAB #3
BUFFER OVERFLOW

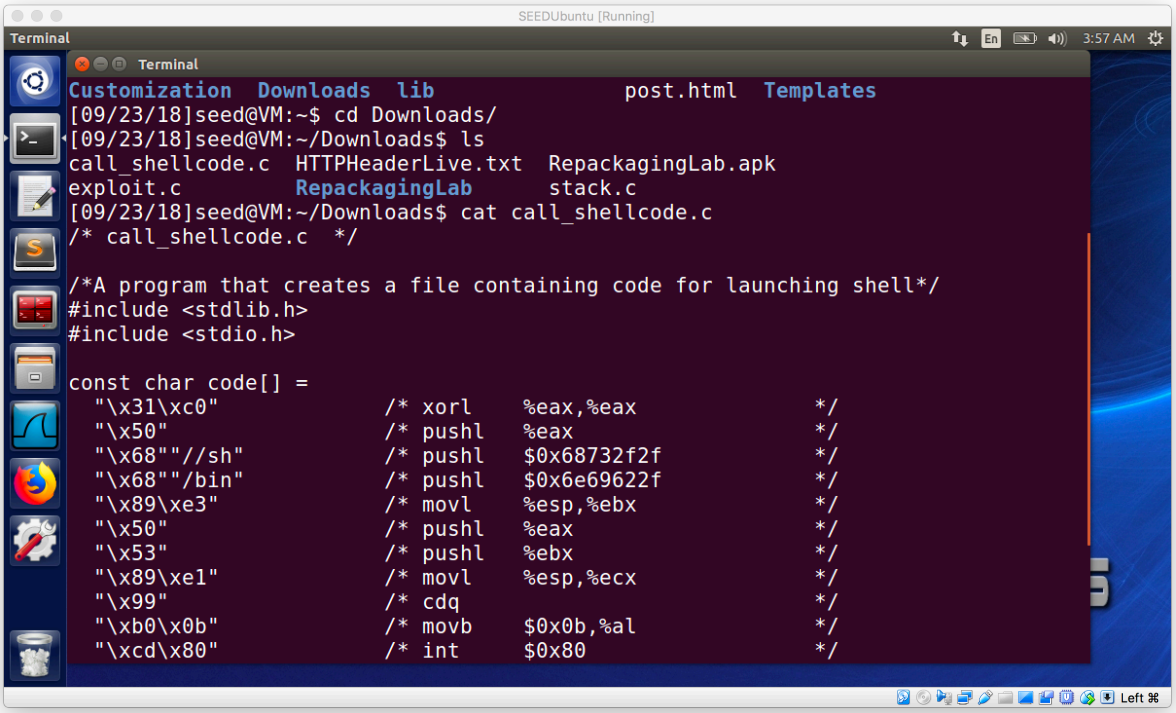
Name: Adithya Karthikeyan
SJSU ID: 011991941

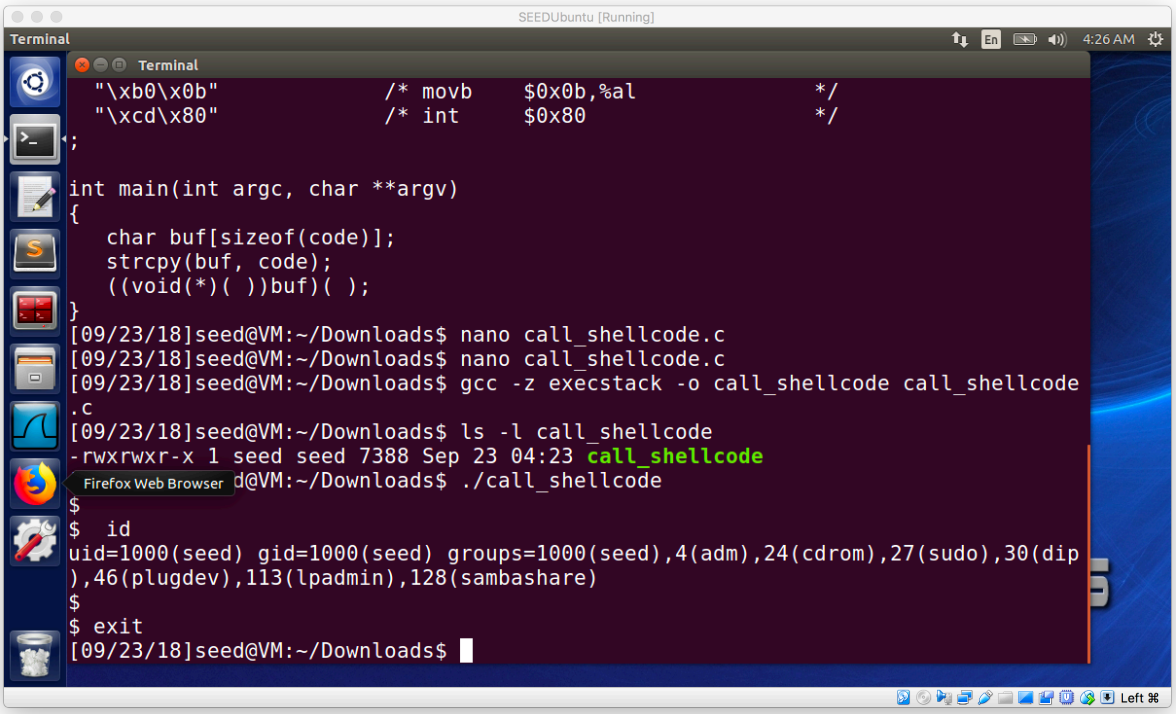
TASK 1: Running Shellcode

1) First we turn off address randomization. We check the randomization status then. We also change the default shell. The screenshot is attached below.

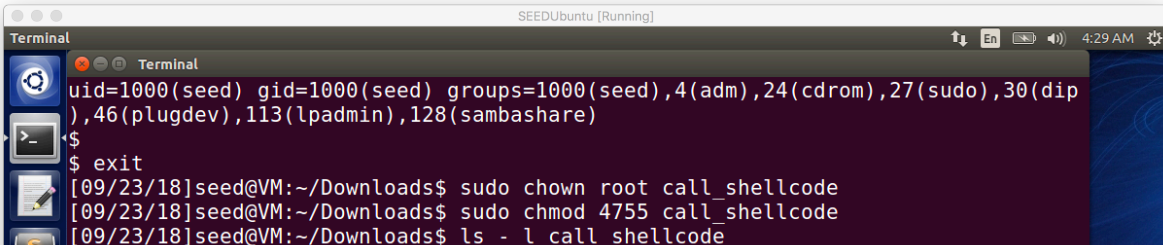


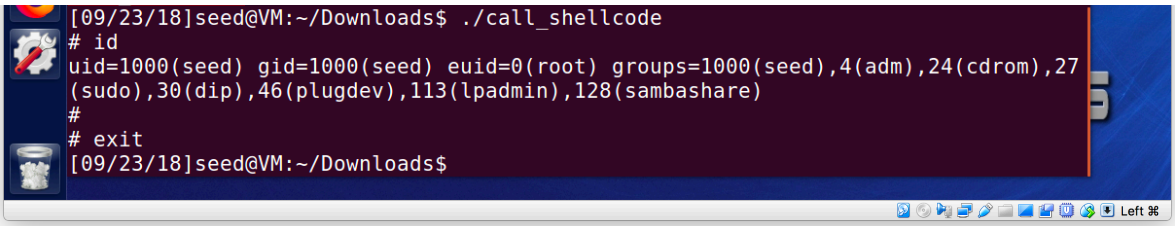
2) We then compile and run the provided shellcode.



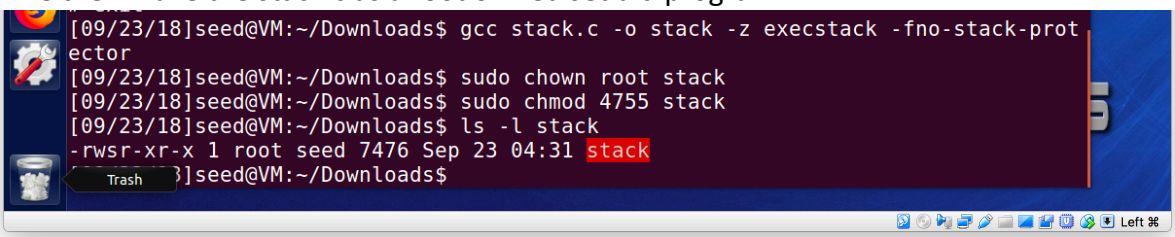


3) We then make the shell code as root owned set uid program and run it.



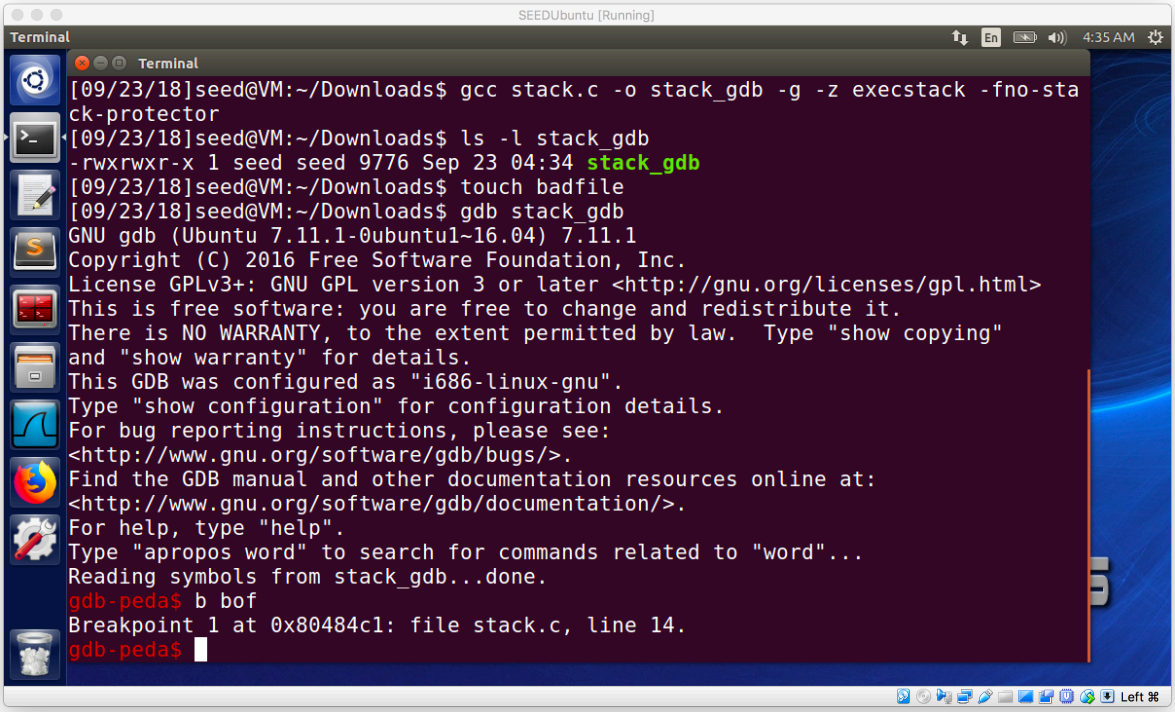


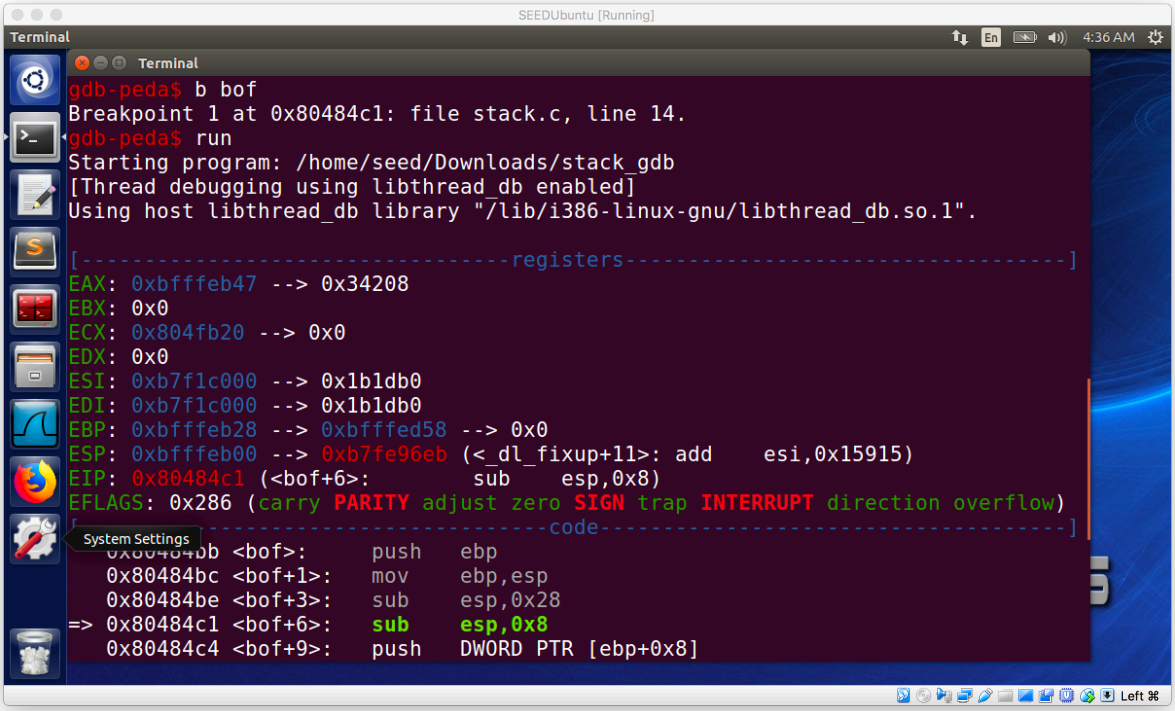
4) We then make the stack.c as a root owned set uid program

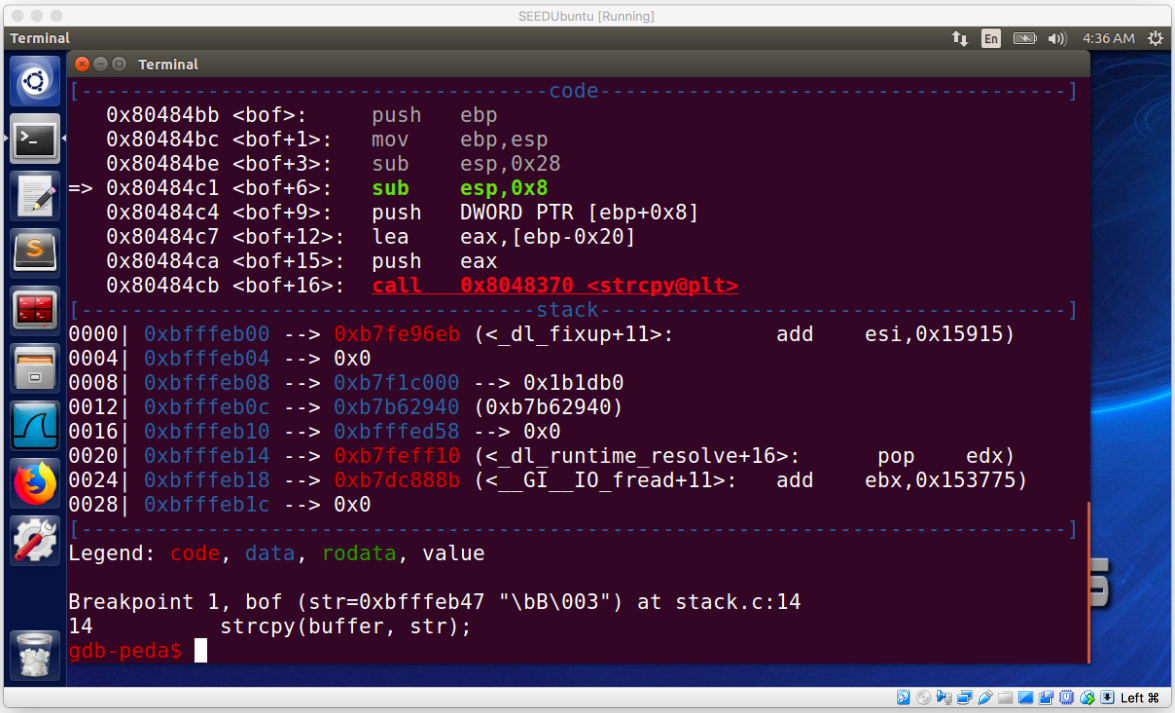


TASK 2: Exploit Buffer Overflow Vulnerability

1) We Create another executable for stack.c with debug flags. Debugged the program using gdb.

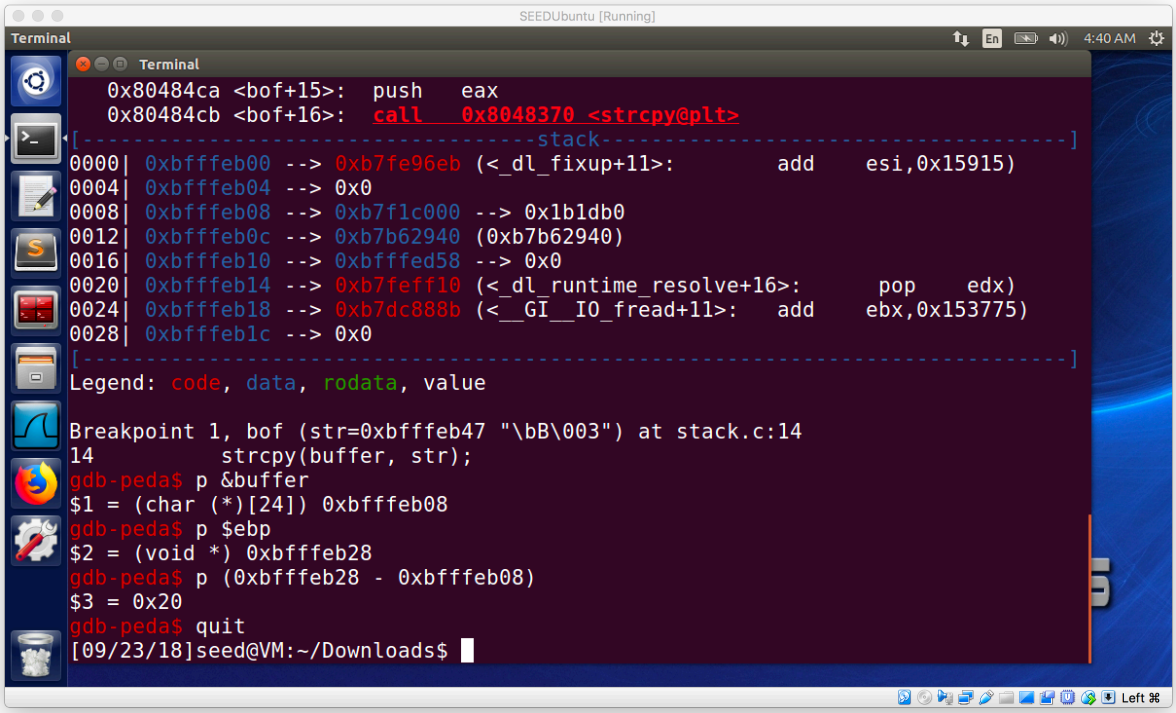




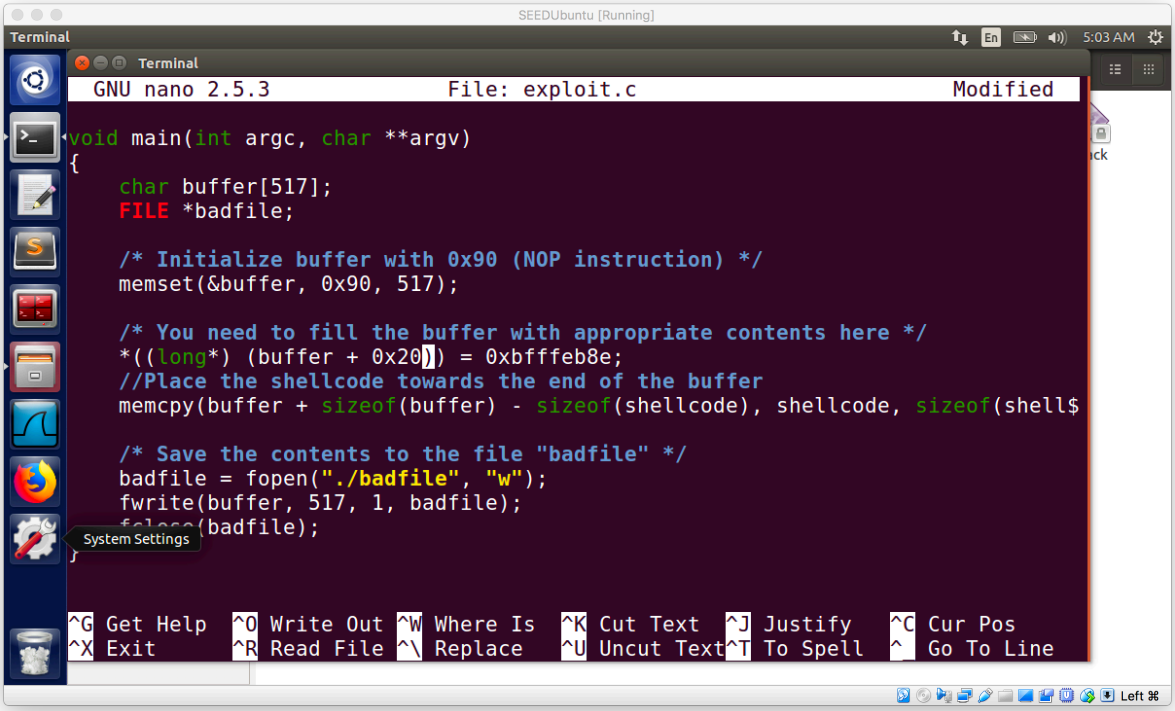


2) We then debug and print commands

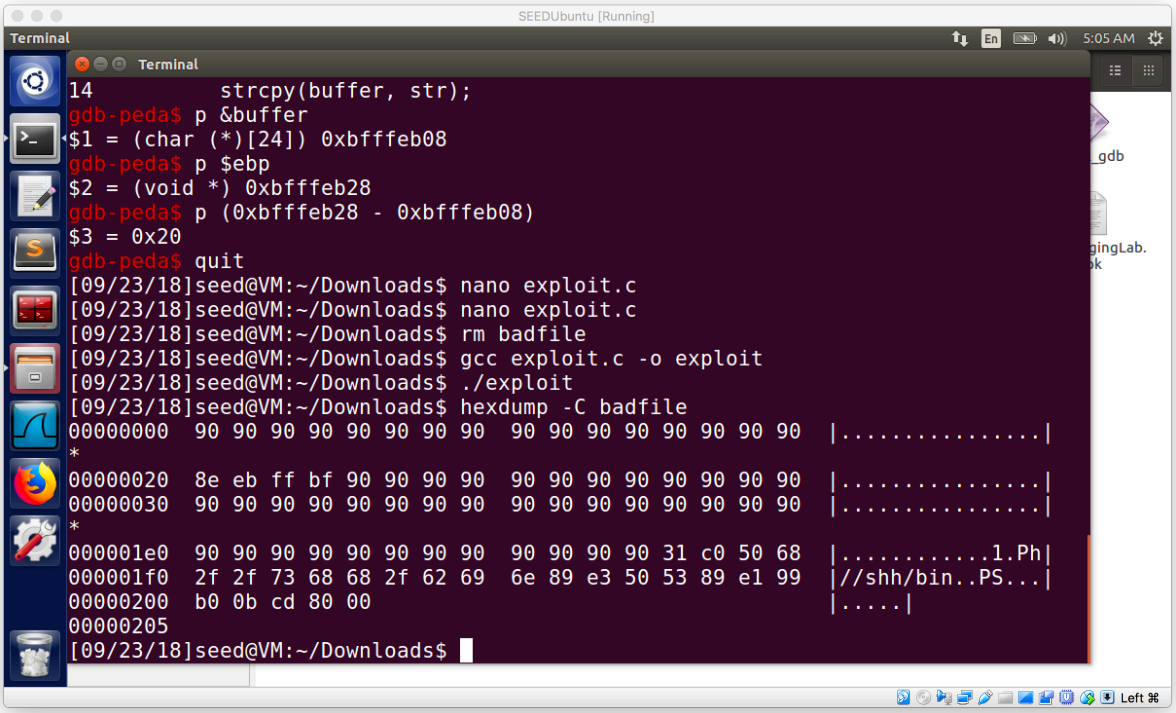
$ b bof
$ run
$ p &buffer
$ p $ebp
$ p ({address_of_ebp} - {address_of_buffer}) eg. p 0x20-0x10
$ quit



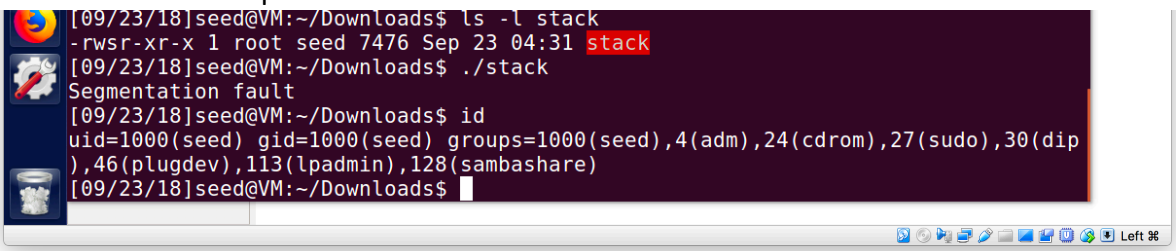
3) We then fill the code in the exploit.c
The edited code is shown in the attached screenshot below.



4) We then create the badfile. The attached sceenshot is shown below.

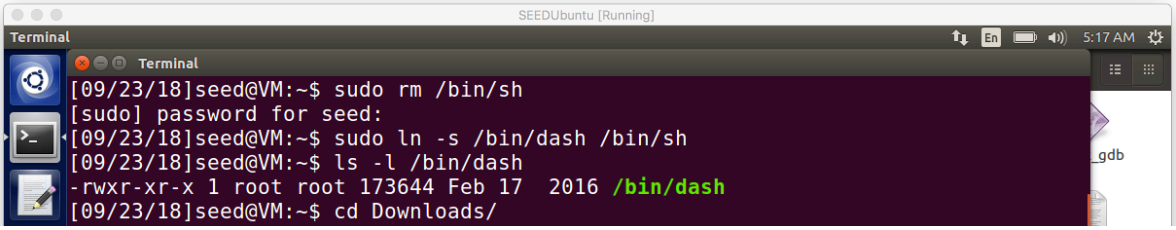


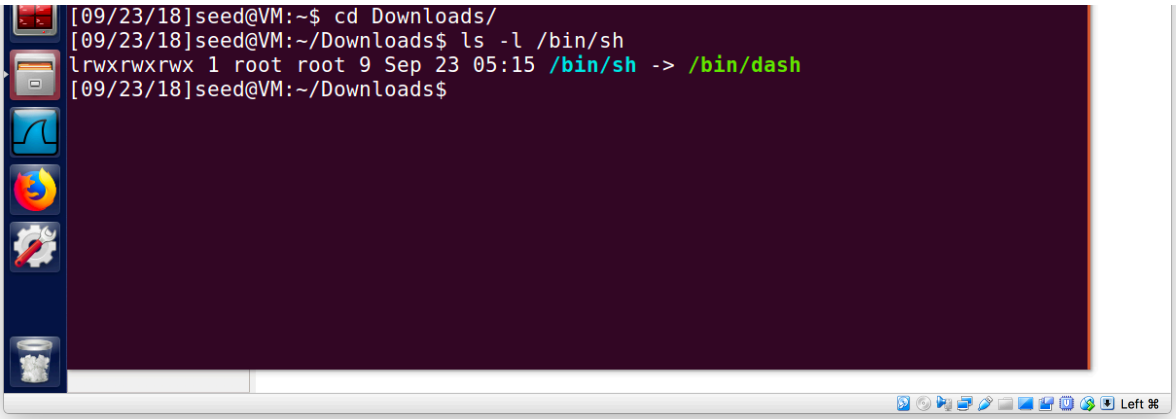
5) We then run the exploit.



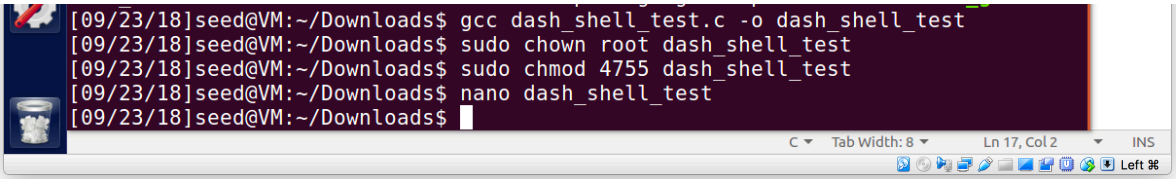
TASK 3 : Dropping Privelege by Bash

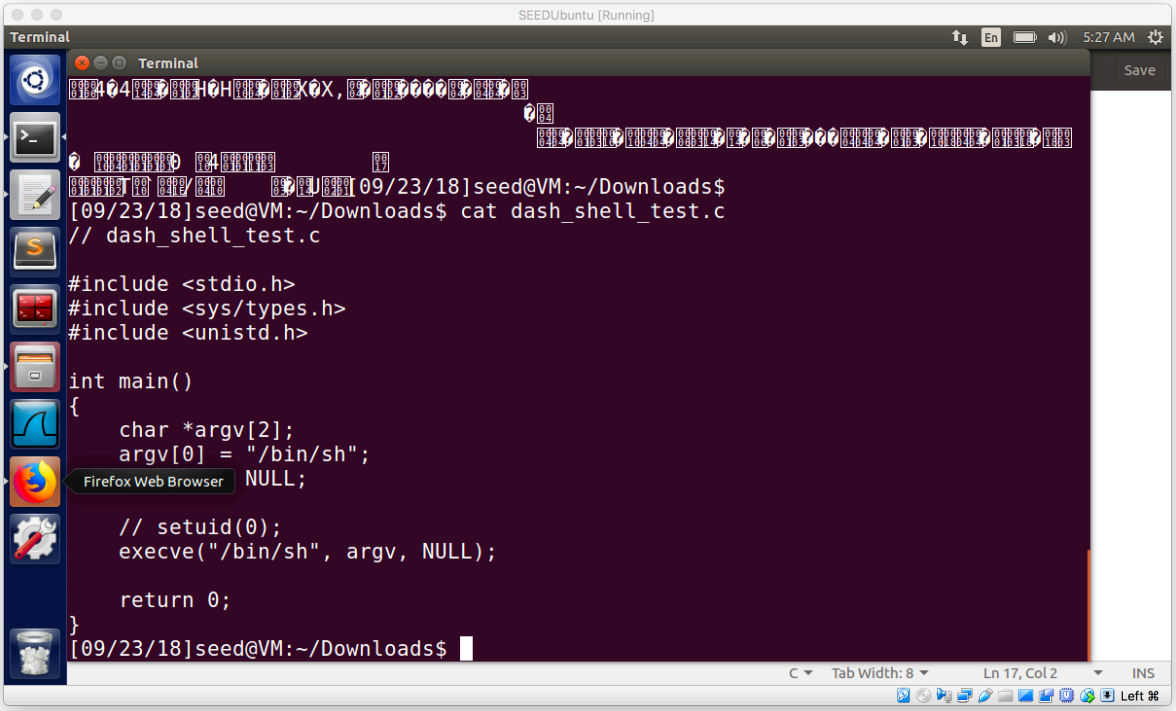
1) We first change the default shell.



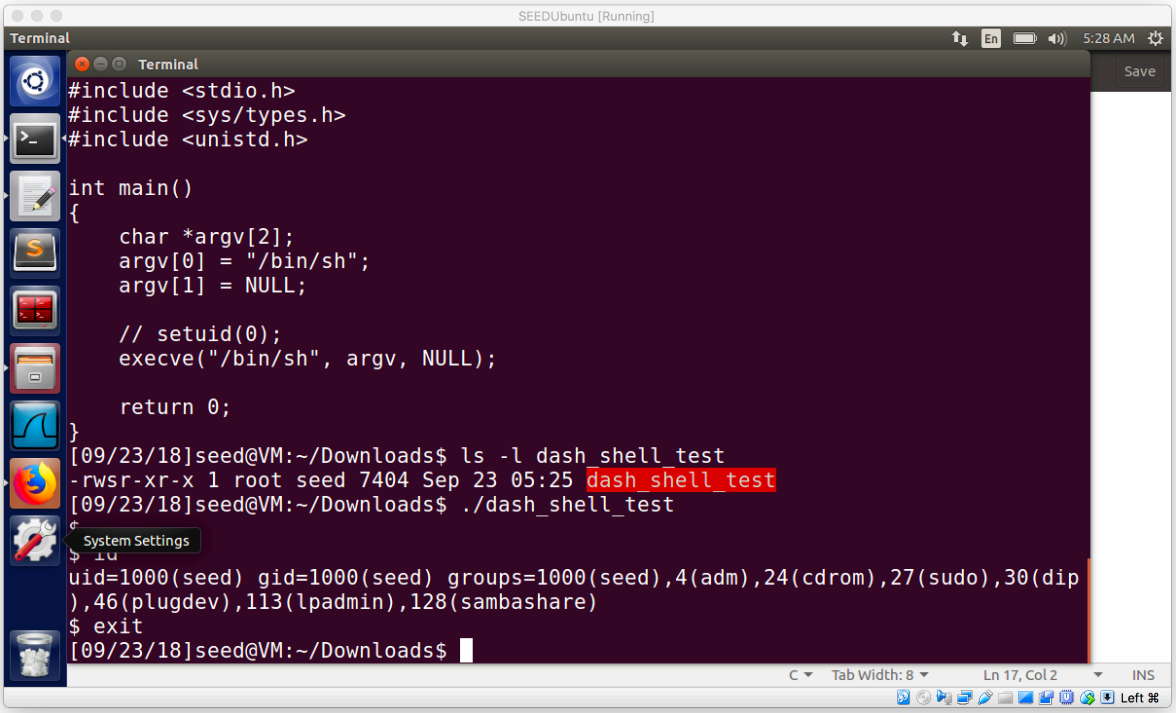


2) We then compile and run dash_shell_test.c





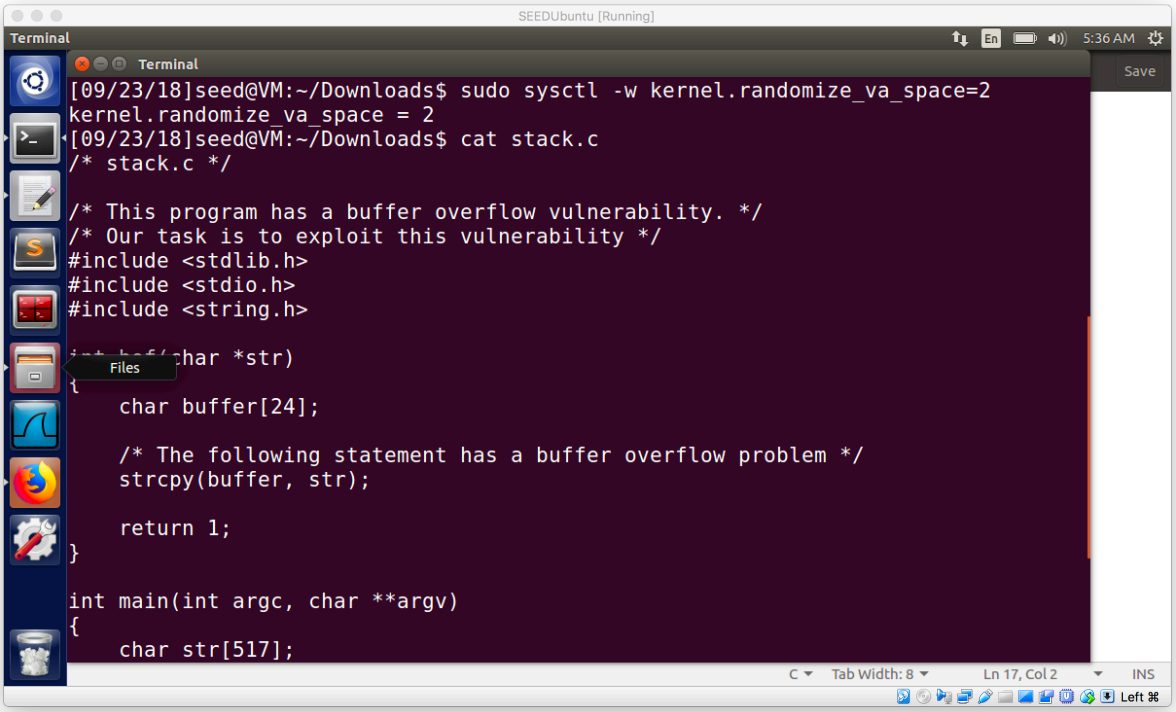
3) We finally compile and run call_shellcode_dash.c



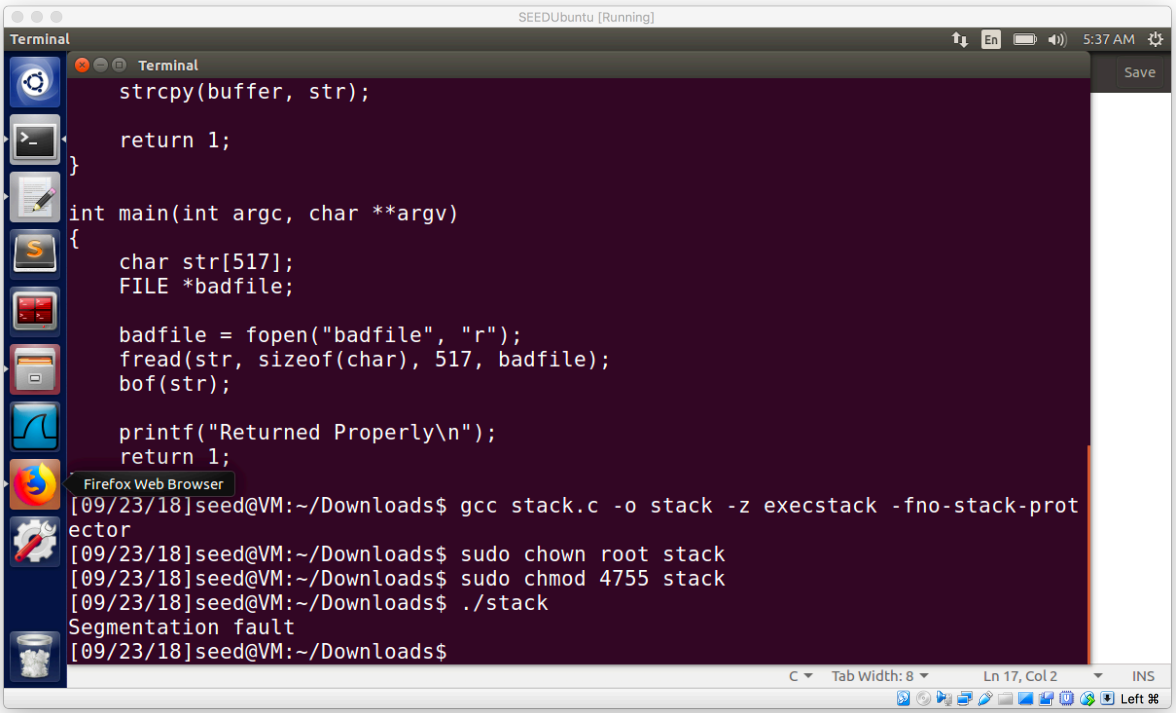
TASK 4 : ASLR (ADDRESS SPACE LAYOUT RANDOMIZATION)

1) We first Turn the countermeasure on by the following command:

$ sudo sysctl -w kernel.randomize_va_space=2

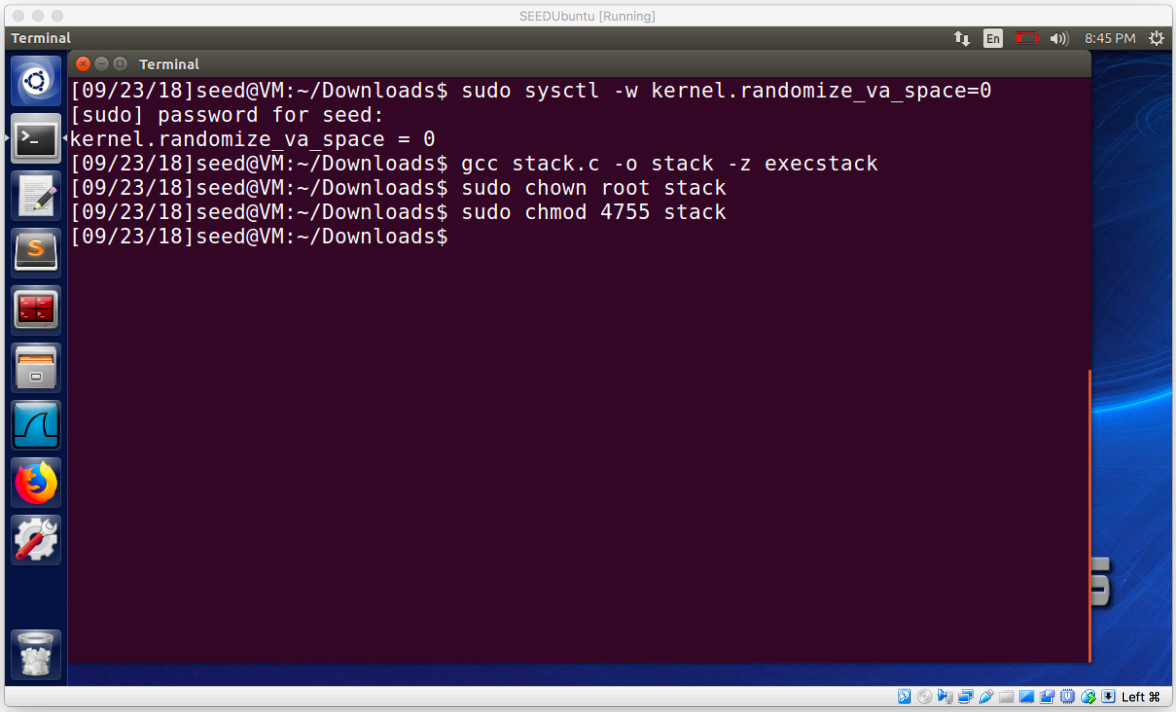


2) Finally, we then compile set-uid root version of stack.c

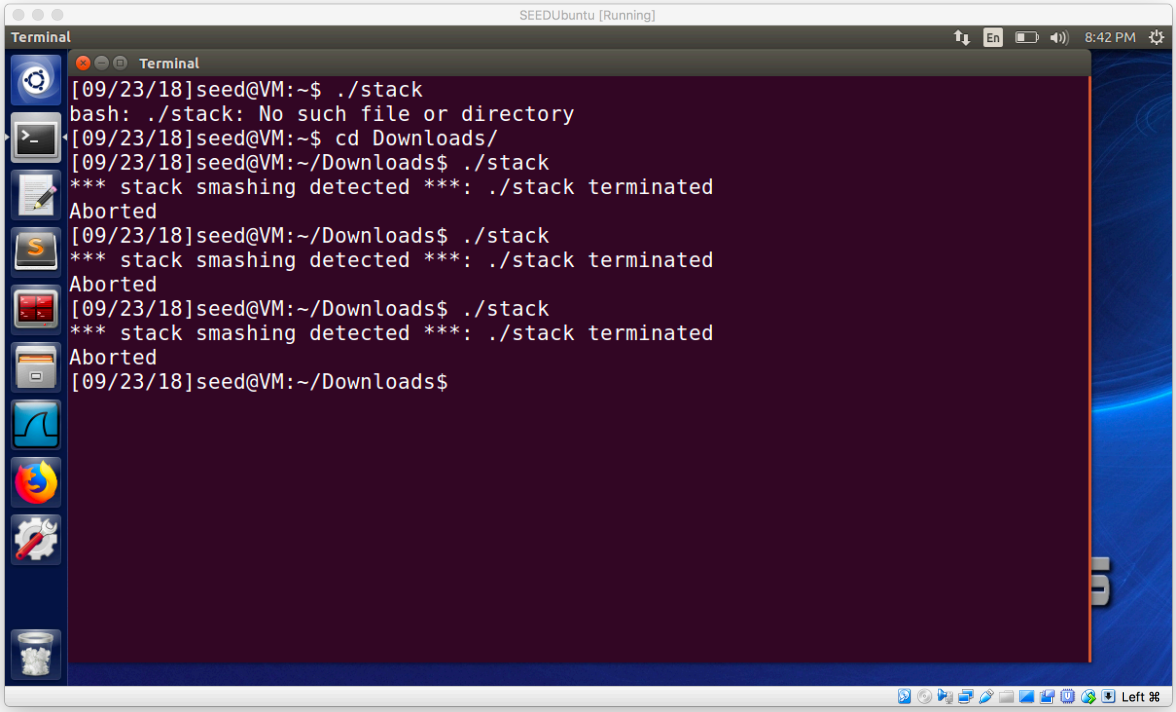


TASK 5 : STACKGUARD

1) We first turn off address randomization.

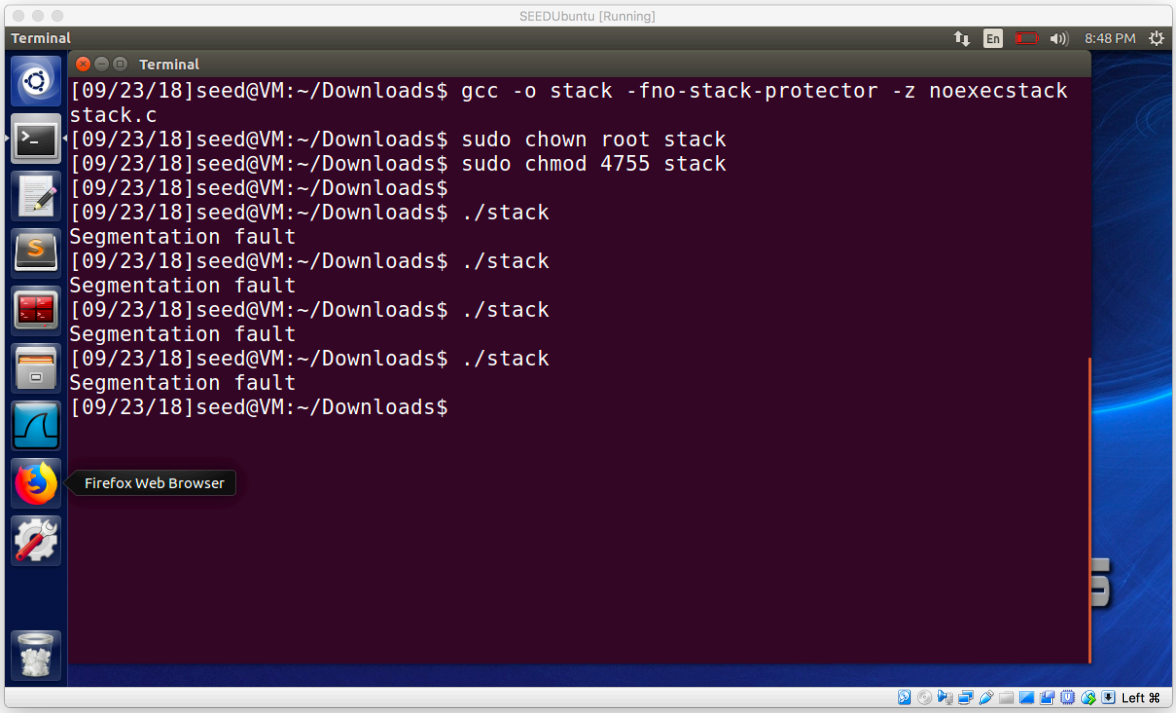


2) We then Compile set-uid root version of stack.c with StackGuard on. The attached screenshot is shown below.



TASK 6: NON EXECUTABLE STACK

1) WE Compile set-uid root version of stack.c with noexecstack option and run the exploit again. The screenshot is attached below.


SEEDUbuntu [Running]
Terminal
En
8:48 PM
Terminal
[09/23/18]seed@VM:~/Downloads$ gcc -o stack -fno-stack-protector -z noexecstack
stack.c
[09/23/18]seed@VM:~/Downloads$ sudo chown root stack
[09/23/18]seed@VM:~/Downloads$ sudo chmod 4755 stack
[09/23/18]seed@VM:~/Downloads$
[09/23/18]seed@VM:~/Downloads$ ./stack
Segmentation fault
[09/23/18]seed@VM:~/Downloads$ ./stack
Segmentation fault
[09/23/18]seed@VM:~/Downloads$ ./stack
Segmentation fault
[09/23/18]seed@VM:~/Downloads$ ./stack
Segmentation fault
[09/23/18]seed@VM:~/Downloads$
Firefox Web Browser
Left ⌘