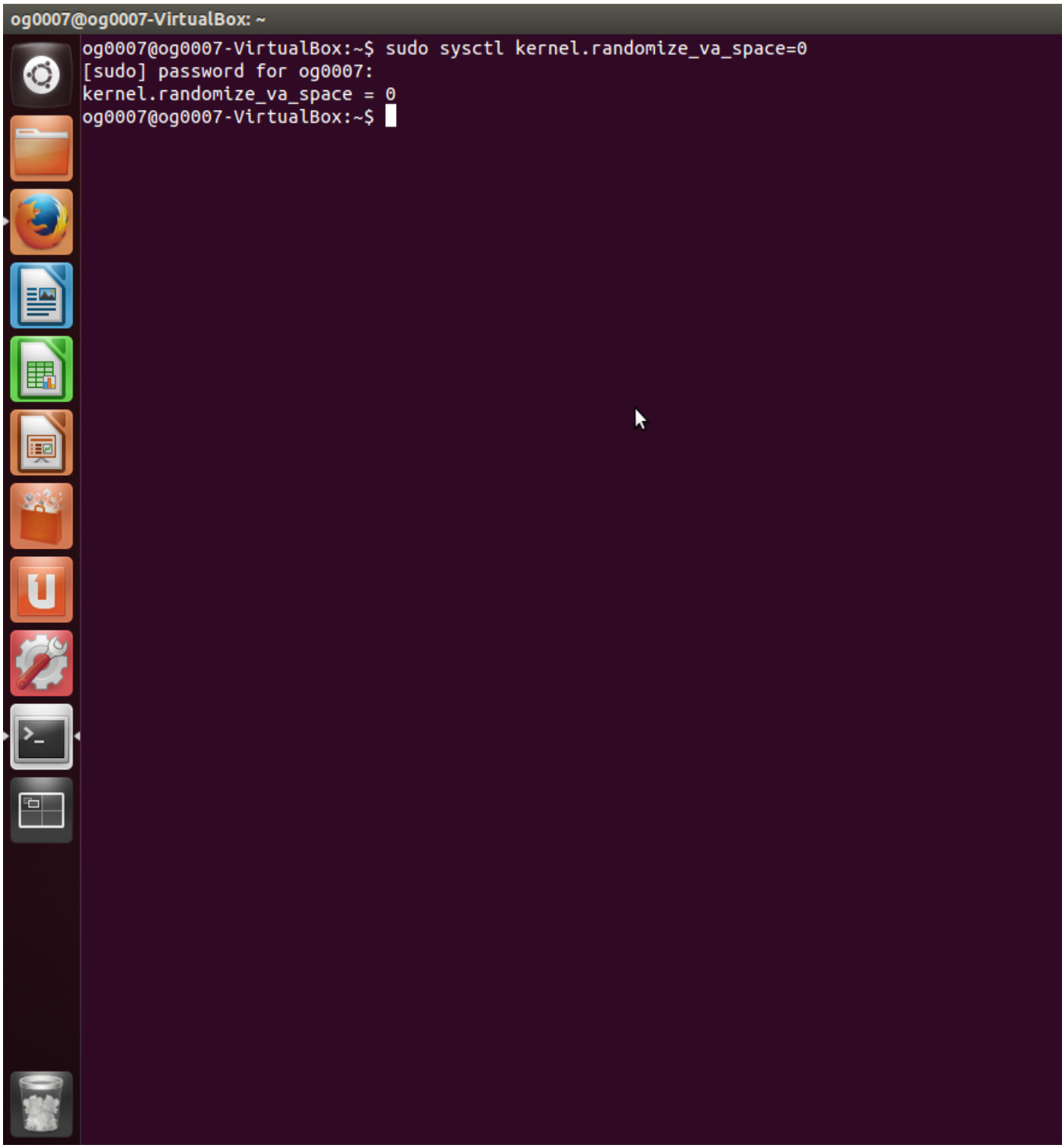
Return to libc Attack

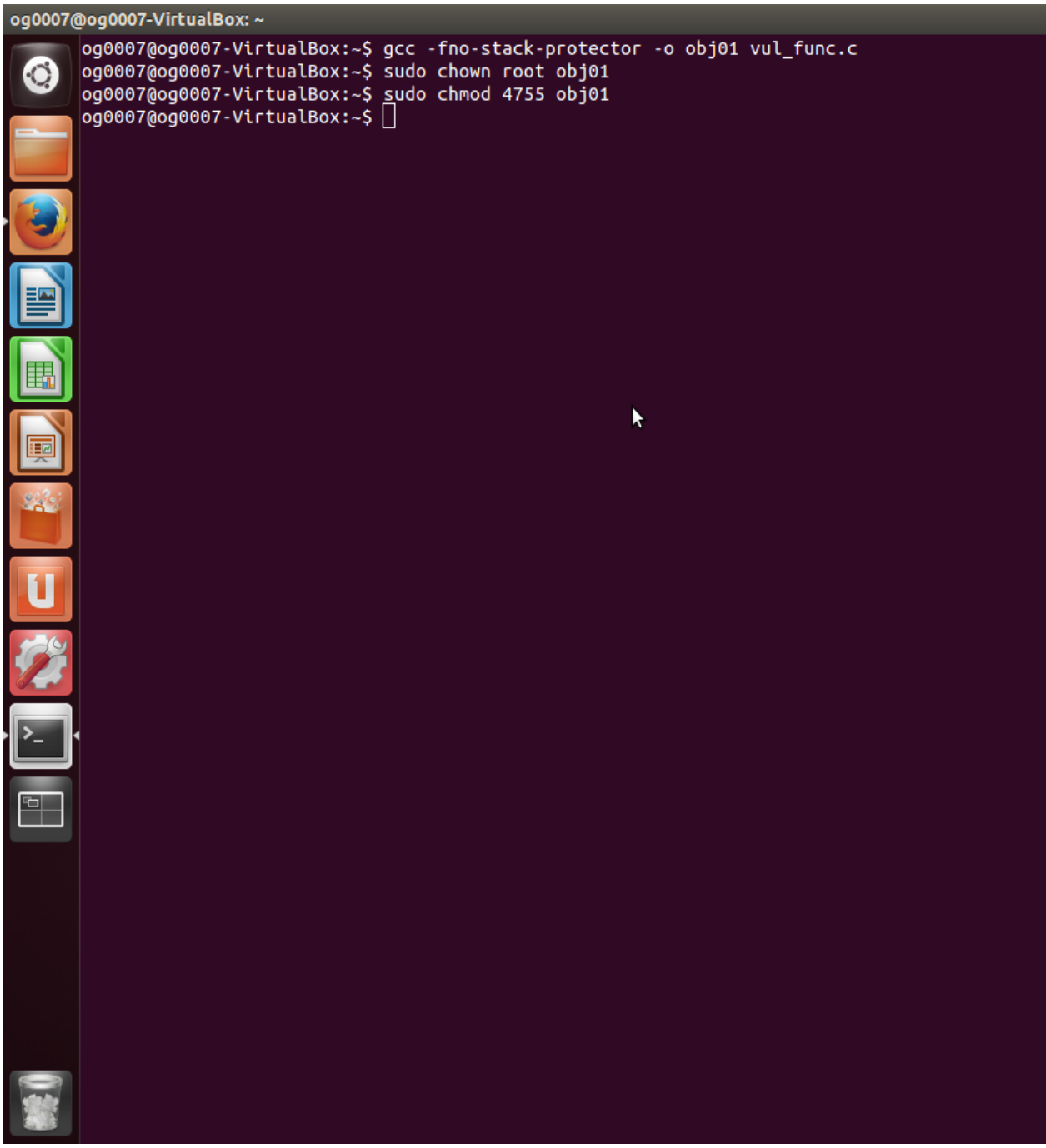
By LAKSHAY GARG

Thapar Institute of Engineering and Technolgy , Patiala

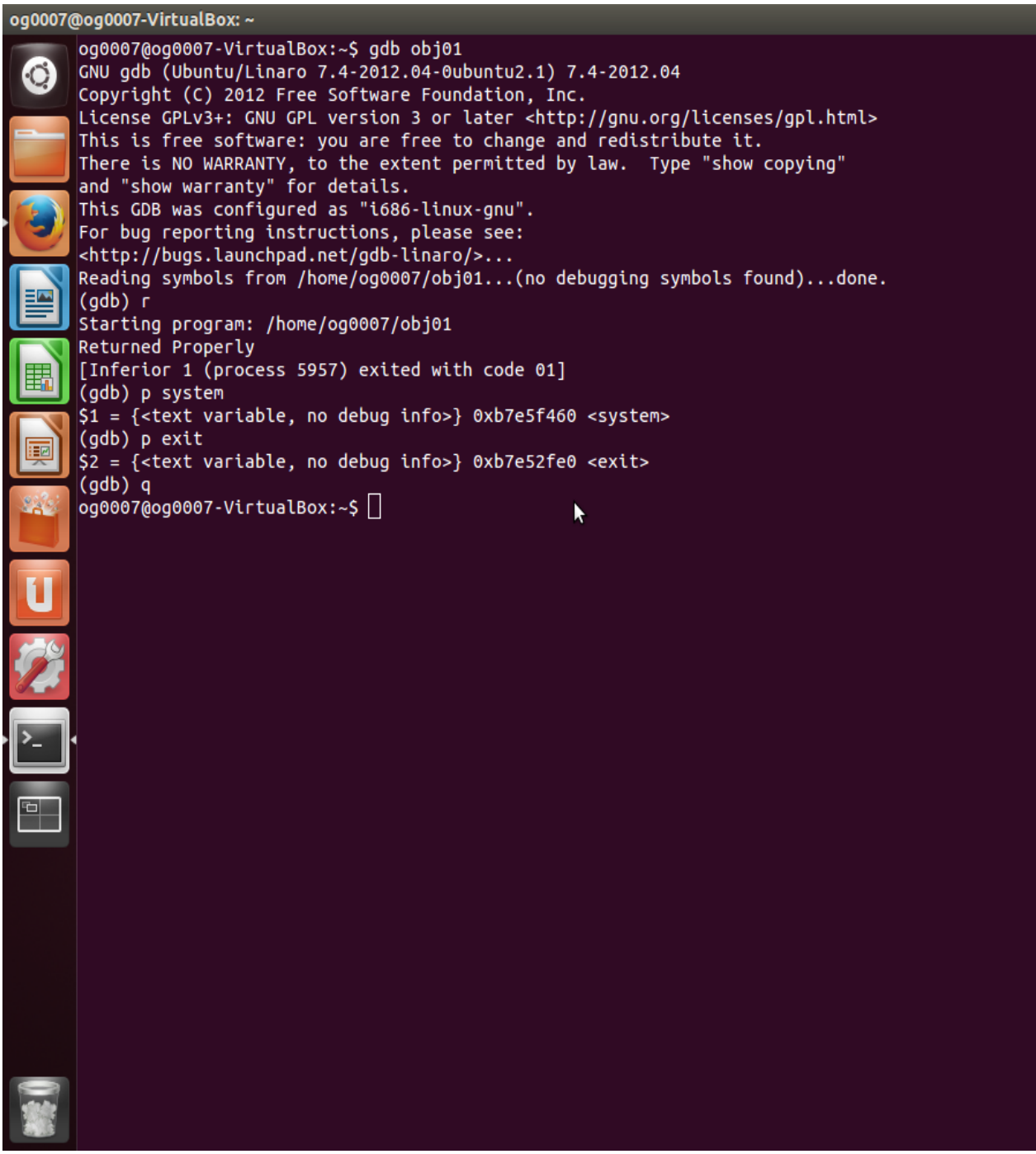
1. Switching off Address space layout randomization (ASLR = 0)



2. Compiling vul_func.c by making stack protector switch off (So as Buffer Overflow happens) and making obj01 (object file obtained by compiling vul_func.c) a root owned set-uid program.

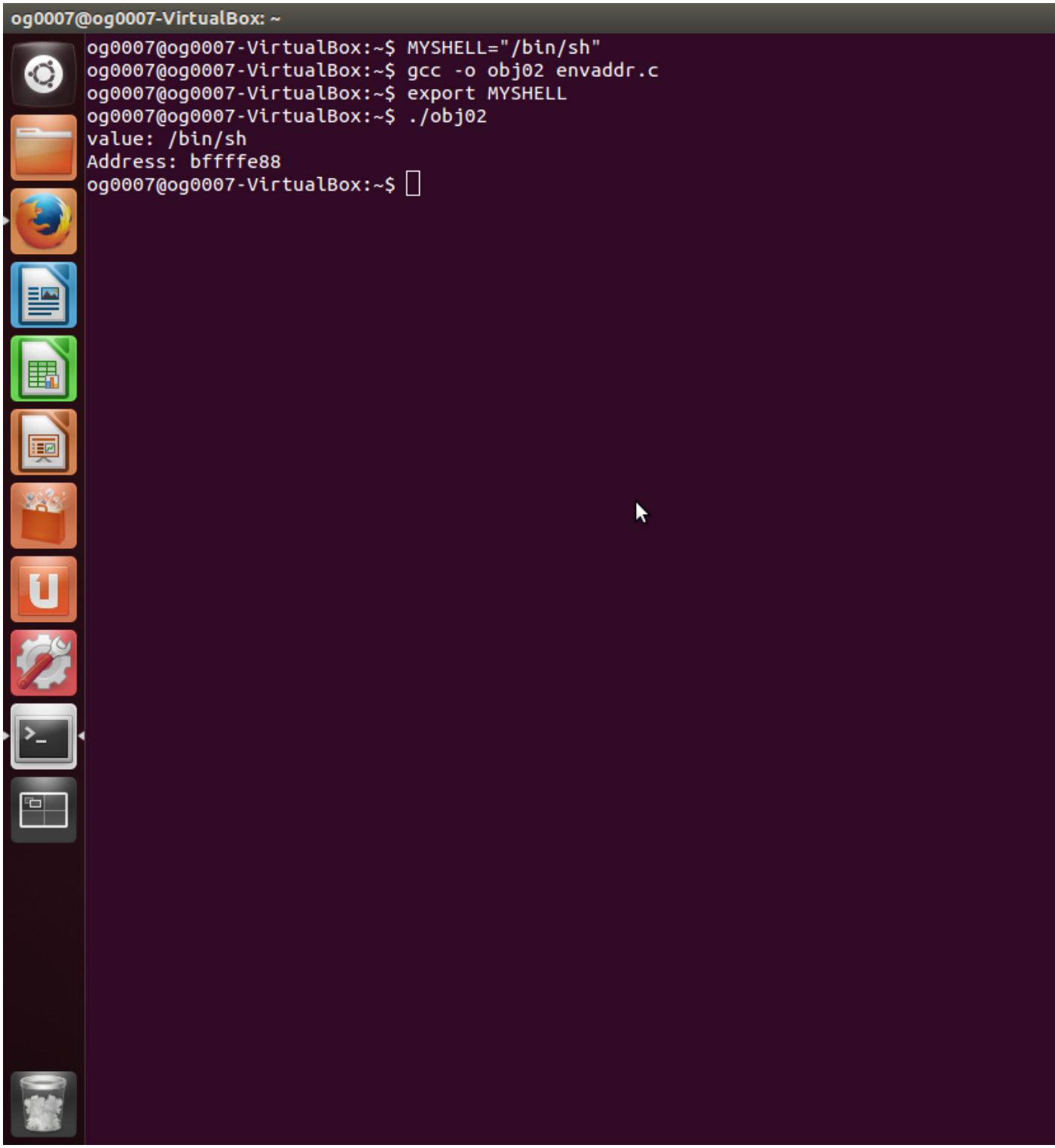


3. Debugging obj01 (object file of vul_func) to find address of system() function and exit() function

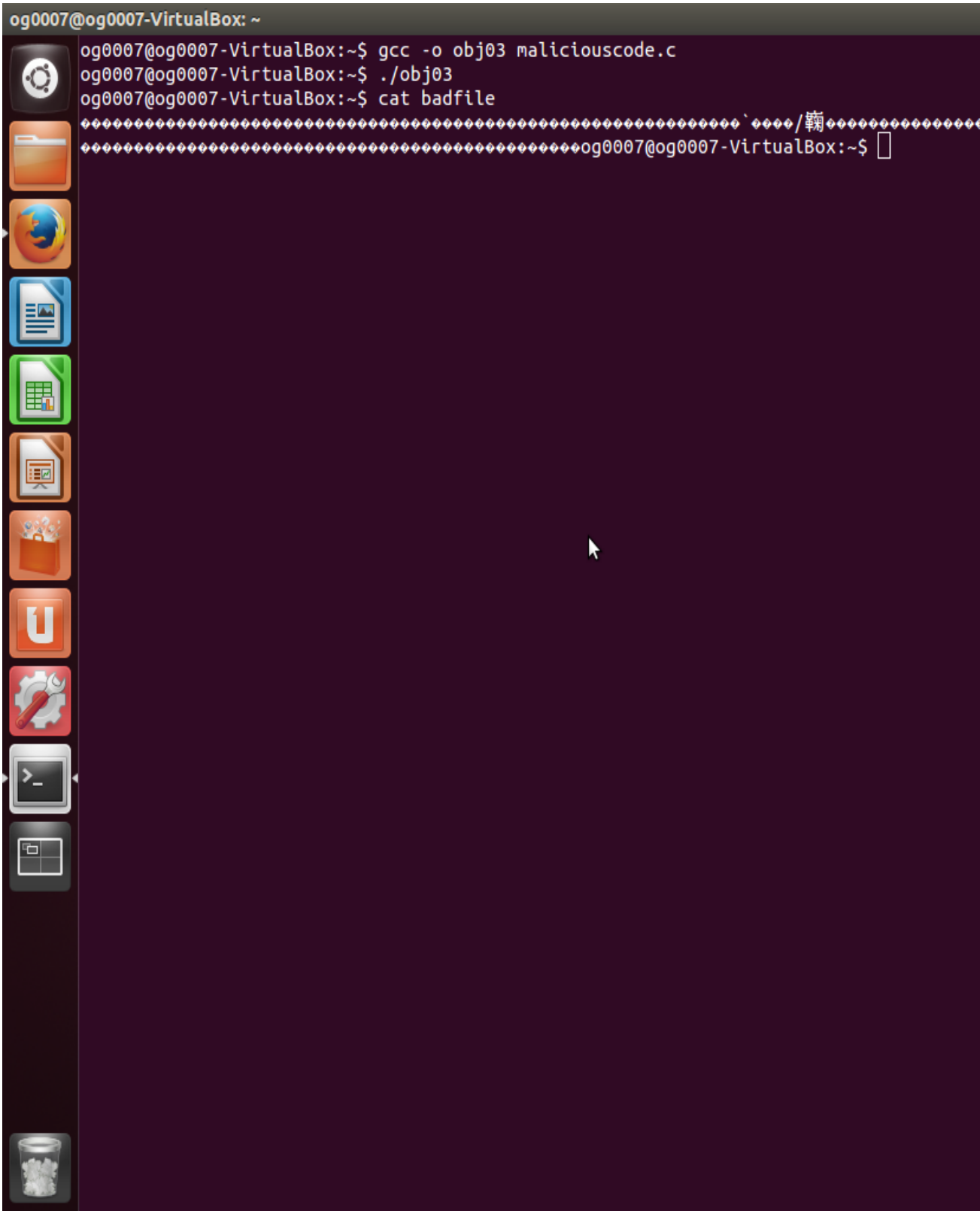


4. Exporting MYSHELL variable as environment variable and finding address of variable by envaddr.c program.

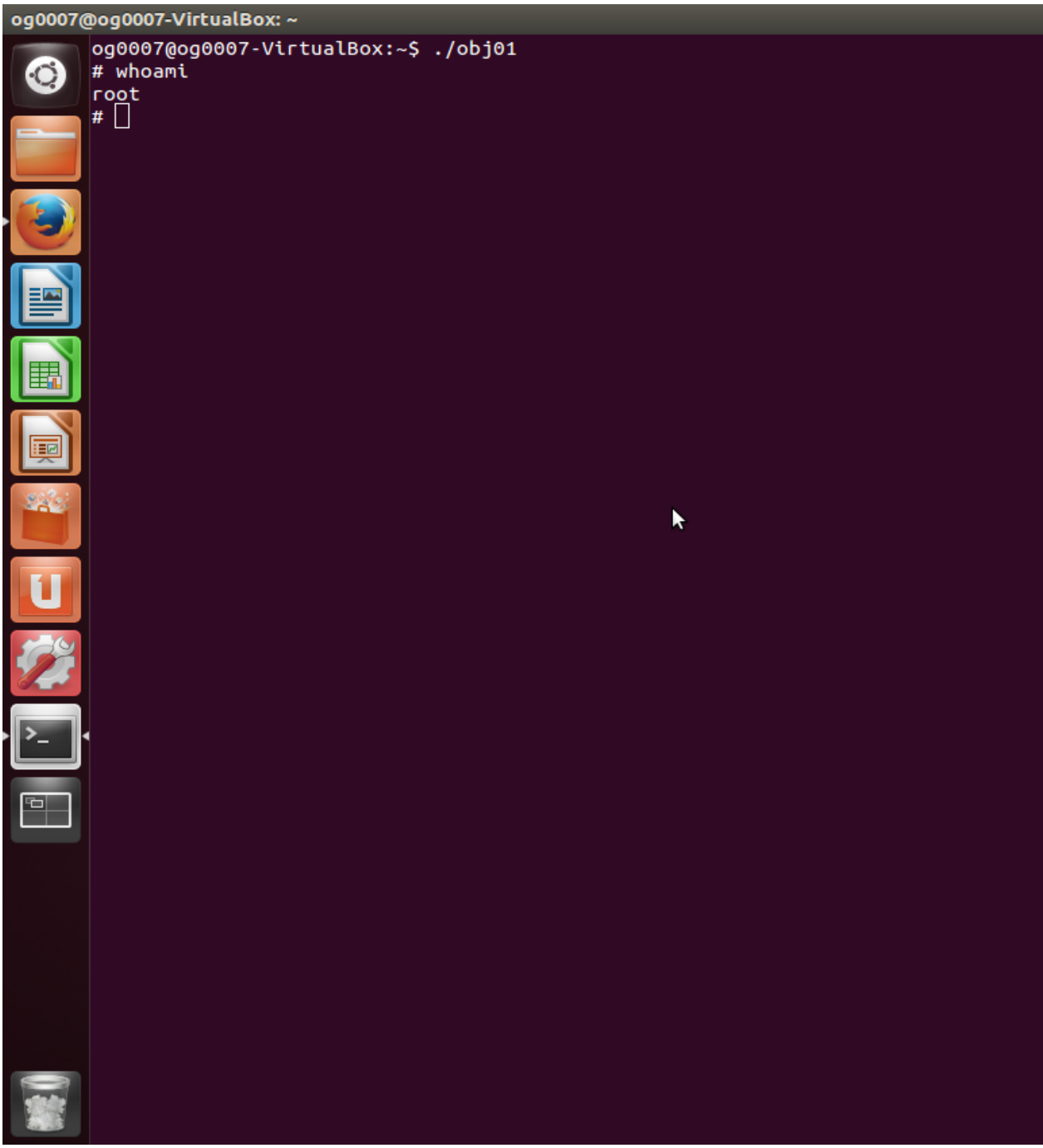
Note -> Length of name of the object file obtained in first program(obj01) and second program(obj02) must be same as changing length will changing address value. .



5. Compiling our maliciouscode.c so to make badfile.



6. I executed obj01 (object file of vul_func.c) and I got the root shell.
   Attack Performed.



Thanks to Dr. Maninder Singh
(HEAD C.I.T.M)

Thapar Institute of Engineering and Technology, Patiala