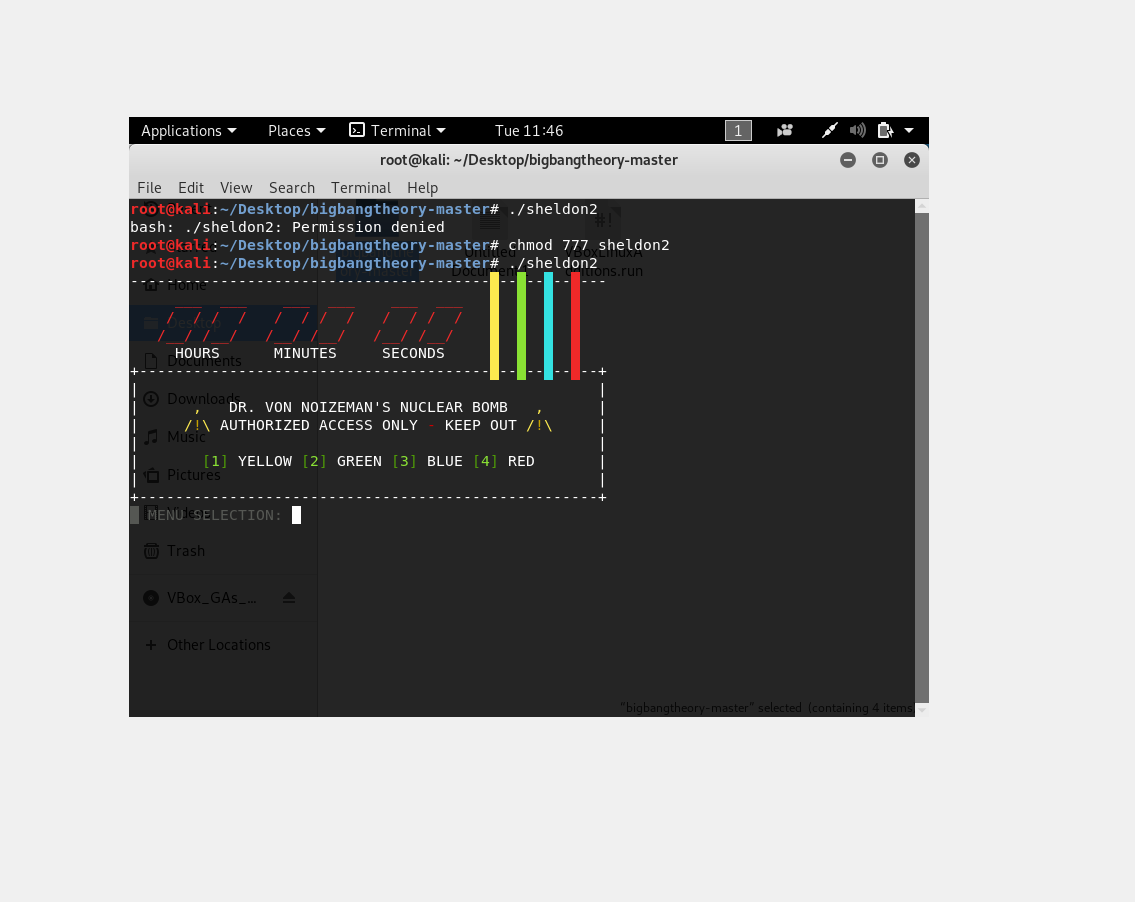


[**Offensive Hacking Tractical And Stratagic**](https://courseweb.sliit.lk/course/view.php?id=3250)

BIGBANG THEORY

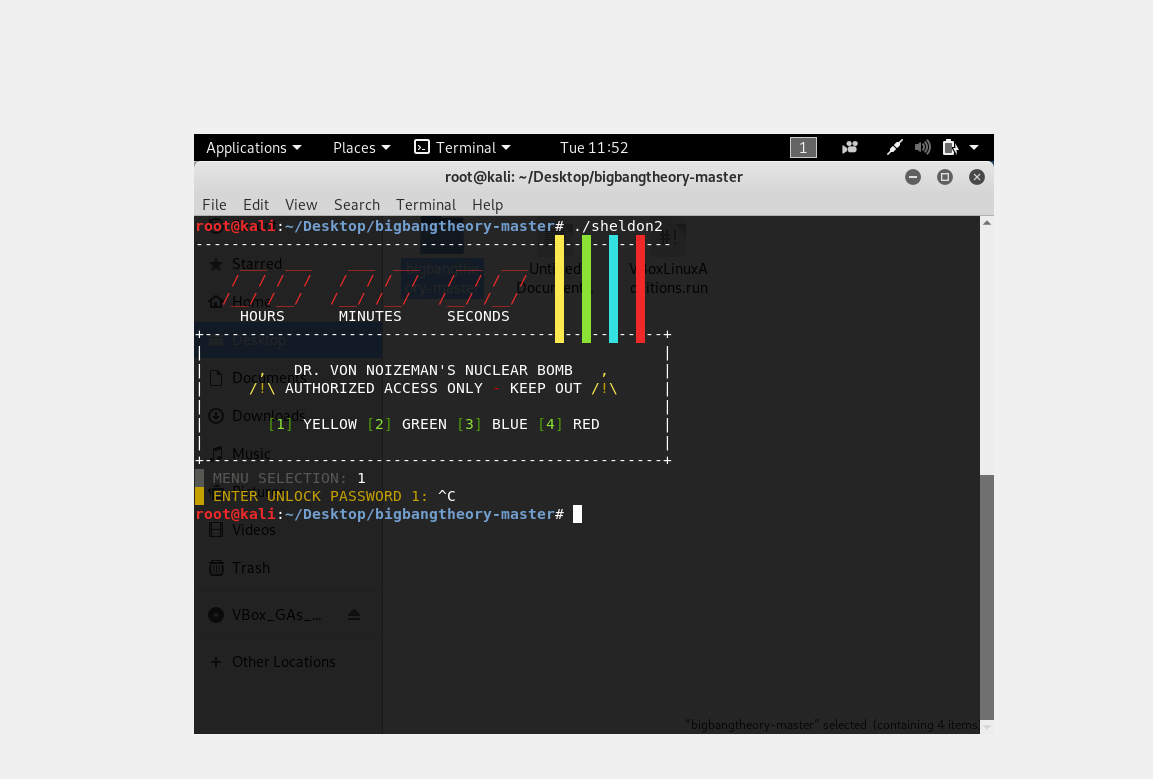
*I.L.Basnayake*

*IT16064164*



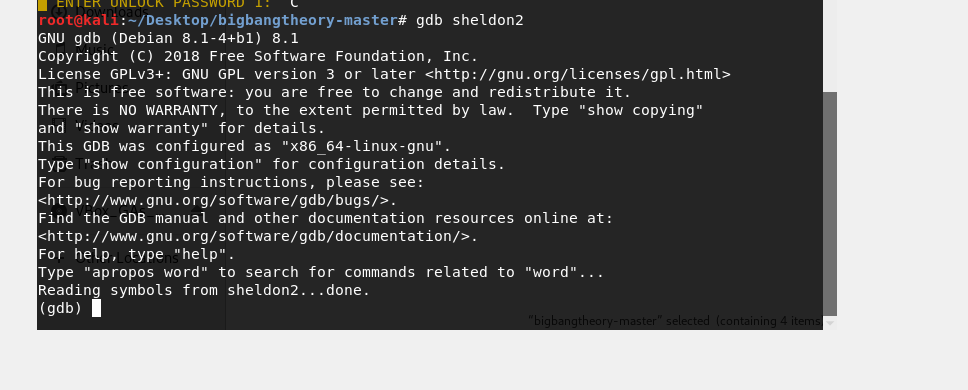
Here the execute permission to the file sheldon 2 . Run using the below command

**./sheldon2**

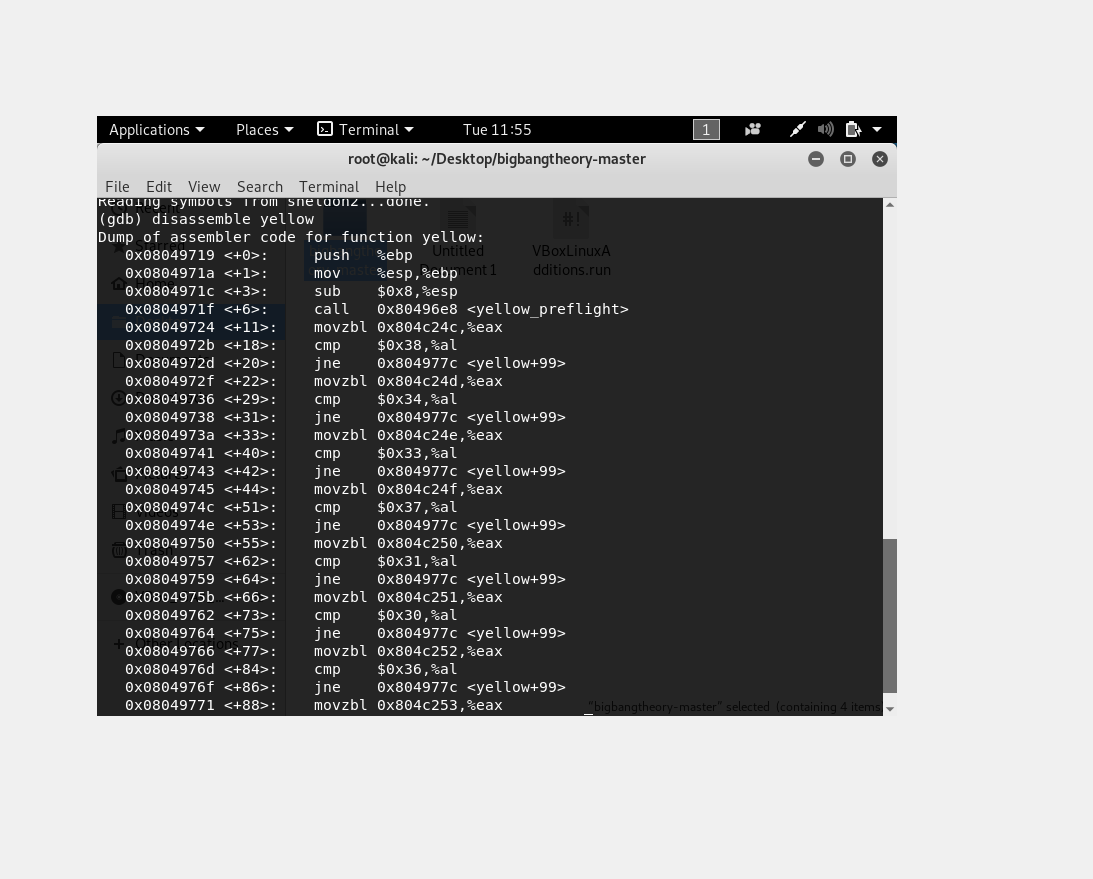


**Select Yellow for phase 1**

**MENU SELECTION: 1**



Use gdb with sheldon 2. Use gdb's disassemble command to get all available assembler code for function yellow in sheldon2. It reads in your input from stdin after selecting ‘yellow’ and compares it character for character with a “fixed” sequence. So Just convert all these 0x3Y values to ASCII and enter it as a password.



**The ASCII values:**

0x0804972b <+18>: cmp $0x38,%al =>> 8

0x08049736 <+29>: cmp $0x34,%al =>> 4

0x08049741 <+40>: cmp $0x33,%al =>> 3

0x0804974c <+51>: cmp $0x37,%al =>> 7

0x08049757 <+62>: cmp $0x31,%al =>> 1

0x08049762 <+73>: cmp $0x30,%al =>> 0

0x0804976d <+84>: cmp $0x36,%al =>> 6

