Big Bank Theory

Sheldon1 phase_1

Twitter updates link https://twitter.com/Abishu14A/status/1237353060659331072?s=20

Execute the sheldon1

Change the access permission of sheldon1

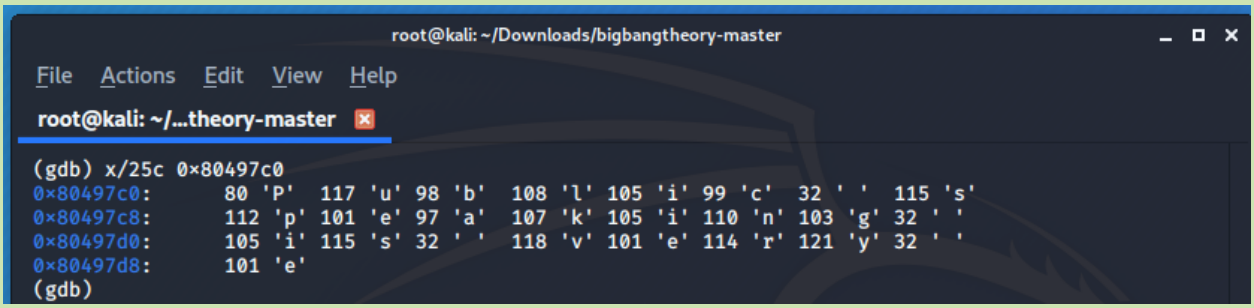
```
root@kali:~/Downloads/bigbangtheory-master# ./sheldon1
bash: ./sheldon1: Permission denied
root@kali:~/Downloads/bigbangtheory-master# chmod +x sheldon1
root@kali:~/Downloads/bigbangtheory-master# ./sheldon1
Welcome to my fiendish little bomb. You have 6 phases with
which to blow yourself up. Have a nice day!


gdb

BOOM!!!
The bomb has blown up.
root@kali:~/Downloads/bigbangtheory-master#
```

To find the call arguments in the disassembly of the sheldon1

Debugging start with **q** option

```
root@kali: ~/Downloads/bigbangtheory-master
File  Actions  Edit  View  Help
root@kali: ~/...theory-master
root@kali:~/Downloads/bigbangtheory-master# gdb -q sheldon1
Reading symbols from sheldon1...
(gdb) list
22      bomb.c: No such file or directory.
(gdb) disassemble phase_1
Dump of assembler code for function phase_1:
   0x08048b20 <+0>:     push   %ebp
   0x08048b21 <+1>:     mov    %esp,%ebp
   0x08048b23 <+3>:     sub    $0x8,%esp
   0x08048b26 <+6>:     mov    0x8(%ebp),%eax
   0x08048b29 <+9>:     add    $0xfffffff8,%esp
   0x08048b2c <+12>:    push   $0x80497c0
   0x08048b31 <+17>:    push   %eax
   0x08048b32 <+18>:    call   0x8049030 <strings_not_equal>
   0x08048b37 <+23>:    add    $0x10,%esp
   0x08048b3a <+26>:    test   %eax,%eax
   0x08048b3c <+28>:    je     0x8048b43 <phase_1+35>
   0x08048b3e <+30>:    call   0x80494fc <explode_bomb>
   0x08048b43 <+35>:    mov    %ebp,%esp
   0x08048b45 <+37>:    pop    %ebp
   0x08048b46 <+38>:    ret
End of assembler dump.
```

Debugging output shows that reversing value is stored in 0x80497c0



Sheldon1 Phase_1 completed