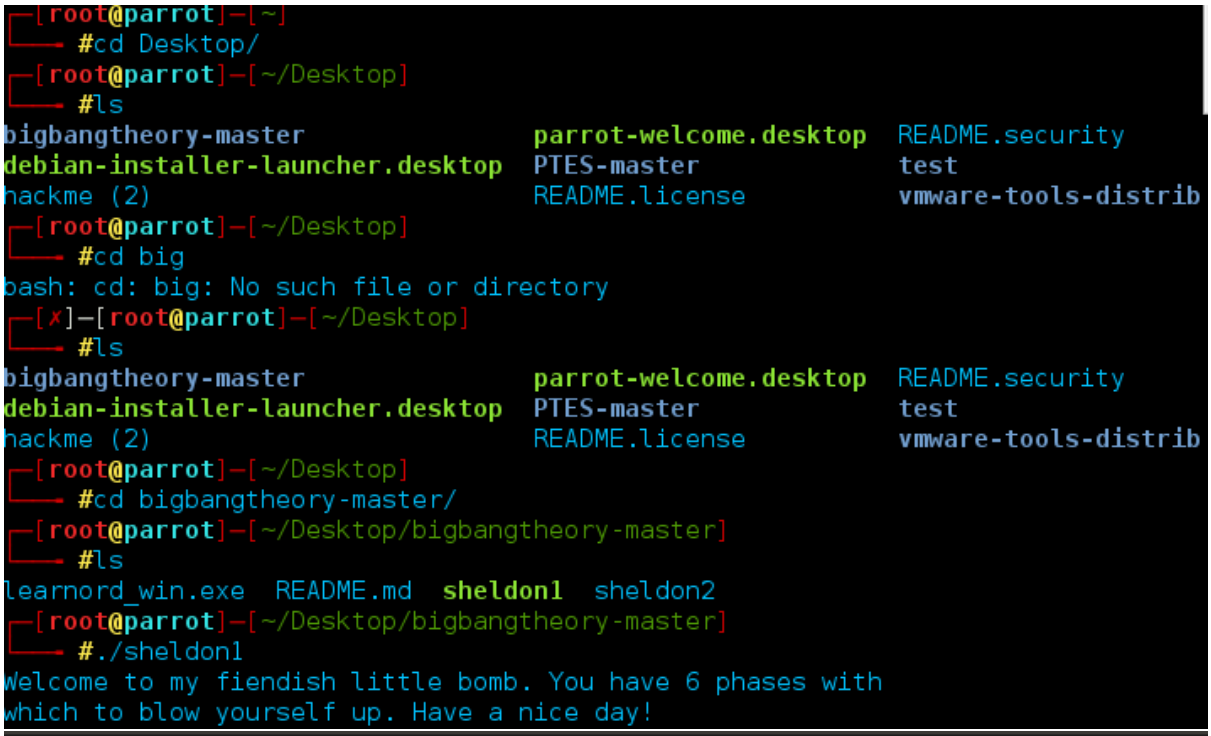
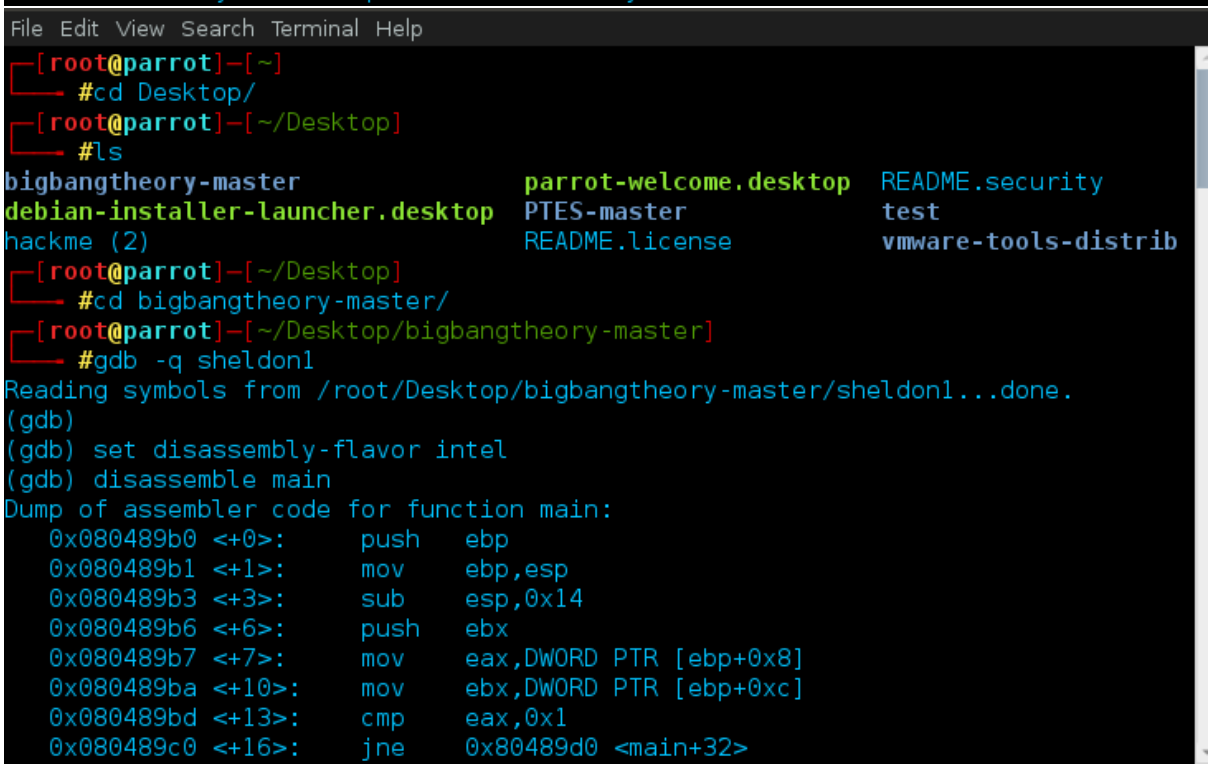
Applied Network Security

Bug Bounty Progress

Activity-1

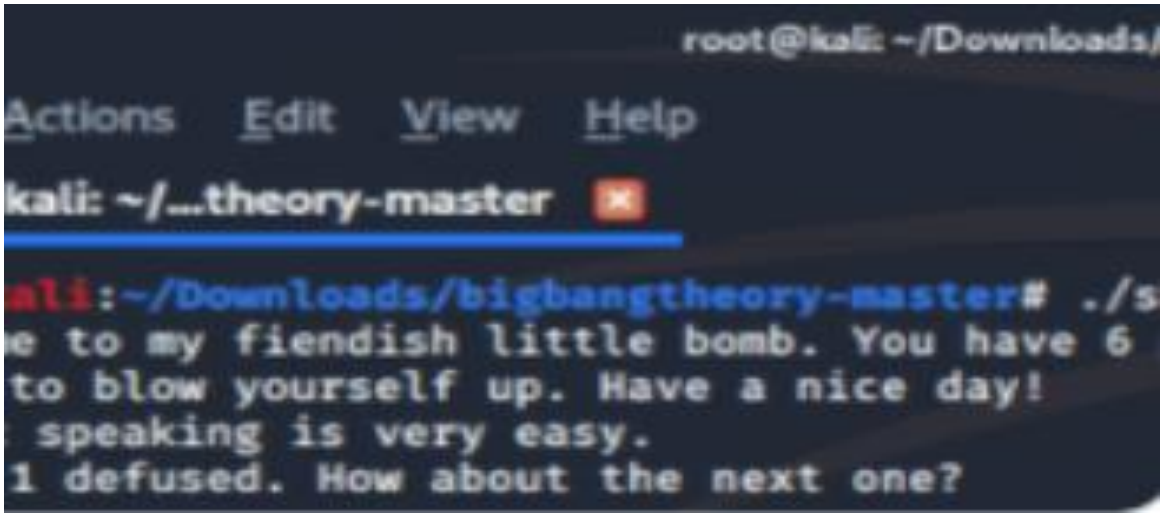
Sheldon1

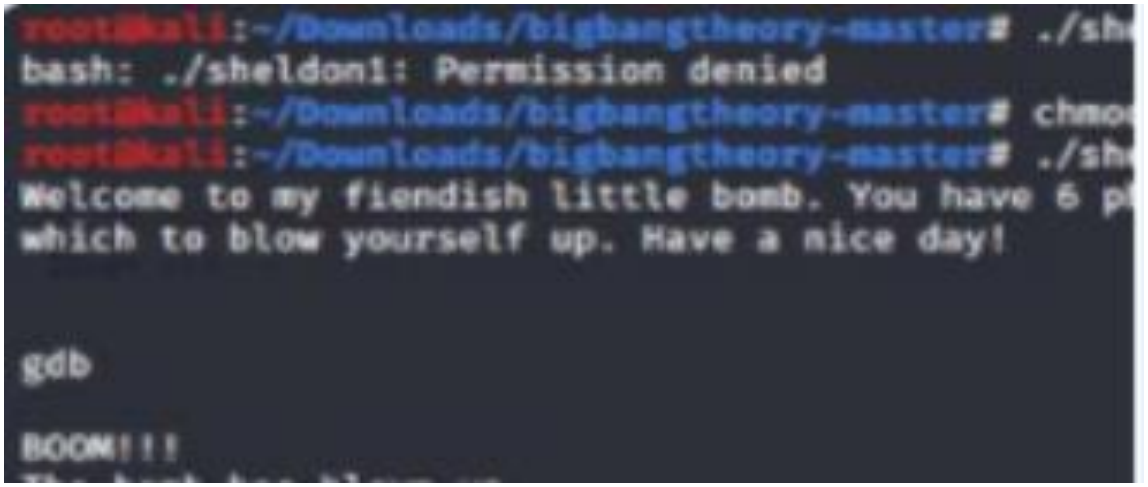

[root@parrot]-[~]
#cd Desktop/
[root@parrot]-[~/Desktop]
#ls
bigbangtheory-master
debian-installer-launcher.desktop
hackme (2)
parrot-welcome.desktop
PTES-master
README.license
README.security
test
vmware-tools-distrib
[root@parrot]-[~/Desktop]
#cd big
bash: cd: big: No such file or directory
[x]-[root@parrot]-[~/Desktop]
#ls
bigbangtheory-master
debian-installer-launcher.desktop
hackme (2)
parrot-welcome.desktop
PTES-master
README.license
README.security
test
vmware-tools-distrib
[root@parrot]-[~/Desktop]
#cd bigbangtheory-master/
[root@parrot]-[~/Desktop/bigbangtheory-master]
#ls
learnord_win.exe README.md sheldon1 sheldon2
[root@parrot]-[~/Desktop/bigbangtheory-master]
#./sheldon1
Welcome to my fiendish little bomb. You have 6 phases with
which to blow yourself up. Have a nice day!

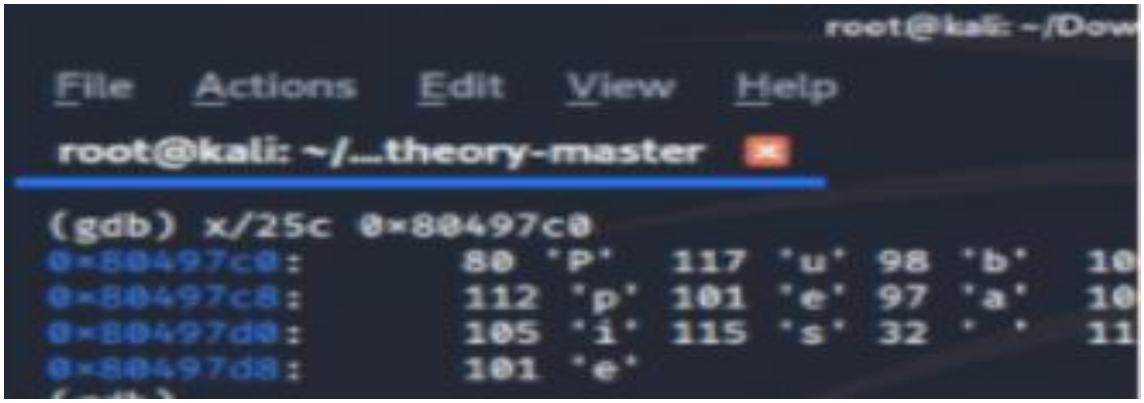

File Edit View Search Terminal Help
[root@parrot]-[~]
#cd Desktop/
[root@parrot]-[~/Desktop]
#ls
bigbangtheory-master
debian-installer-launcher.desktop
hackme (2)
parrot-welcome.desktop
PTES-master
README.license
README.security
test
vmware-tools-distrib
[root@parrot]-[~/Desktop]
#cd bigbangtheory-master/
[root@parrot]-[~/Desktop/bigbangtheory-master]
#gdb -q sheldon1
Reading symbols from /root/Desktop/bigbangtheory-master/sheldon1...done.
(gdb)
(gdb) set disassembly-flavor intel
(gdb) disassemble main
Dump of assembler code for function main:
0x080489b0 <+0>: push ebp
0x080489b1 <+1>: mov ebp,esp
0x080489b3 <+3>: sub esp,0x14
0x080489b6 <+6>: push ebx
0x080489b7 <+7>: mov eax,DWORD PTR [ebp+0x8]
0x080489ba <+10>: mov ebx,DWORD PTR [ebp+0xc]
0x080489bd <+13>: cmp eax,0x1
0x080489c0 <+16>: jne 0x80489d0 <main+32>

```
File  Edit  View  Search  Terminal  Help
   0x08048aa0 <+240>:   push   eax
   0x08048aa1 <+241>:   call   0x8048b98 <phase_3>
   0x08048aa6 <+246>:   call   0x804952c <phase_defused>
   0x08048aab <+251>:   add    esp,0xfffffff4
   0x08048aae <+254>:   push   0x804973f
   0x08048ab3 <+259>:   call   0x8048810 <printf@plt>
   0x08048ab8 <+264>:   add    esp,0x20
   0x08048abb <+267>:   call   0x80491fc <read_line>
   0x08048ac0 <+272>:   add    esp,0xfffffff4
   0x08048ac3 <+275>:   push   eax
   0x08048ac4 <+276>:   call   0x8048ce0 <phase_4>
   0x08048ac9 <+281>:   call   0x804952c <phase_defused>
   0x08048ace <+286>:   add    esp,0xfffffff4
   0x08048ad1 <+289>:   push   0x8049760
   0x08048ad6 <+294>:   call   0x8048810 <printf@plt>
   0x08048adb <+299>:   add    esp,0x20
   0x08048ade <+302>:   call   0x80491fc <read_line>
   0x08048ae3 <+307>:   add    esp,0xfffffff4
   0x08048ae6 <+310>:   push   eax
   0x08048ae7 <+311>:   call   0x8048d2c <phase_5>
   0x08048aec <+316>:   call   0x804952c <phase_defused>
---Type <return> to continue, or q <return> to quit---
   0x08048af1 <+321>:   add    esp,0xfffffff4
   0x08048af4 <+324>:   push   0x80497a0
```

```
File  Edit  View  Search  Terminal  Help
---Type <return> to continue, or q <return> to quit---
   0x08048af1 <+321>:   add    esp,0xfffffff4
   0x08048af4 <+324>:   push   0x80497a0
   0x08048af9 <+329>:   call   0x8048810 <printf@plt>
   0x08048afe <+334>:   add    esp,0x20
   0x08048b01 <+337>:   call   0x80491fc <read_line>
   0x08048b06 <+342>:   add    esp,0xfffffff4
   0x08048b09 <+345>:   push   eax
   0x08048b0a <+346>:   call   0x8048d98 <phase_6>
   0x08048b0f <+351>:   call   0x804952c <phase_defused>
   0x08048b14 <+356>:   xor    eax,eax
   0x08048b16 <+358>:   mov    ebx,DWORD PTR [ebp-0x18]
   0x08048b19 <+361>:   mov    esp,ebp
   0x08048b1b <+363>:   pop    ebp
   0x08048b1c <+364>:   ret
End of assembler dump.
(gdb) x/25c 0x80497c0
0x80497c0:      80 'P'  117 'u' 98 'b'  108 'l' 105 'i' 99 'c'  32 ' '  115 's'
0x80497c8:      112 'p' 101 'e' 97 'a'  107 'k' 105 'i' 110 'n' 103 'g' 32 ' '
0x80497d0:      105 'i' 115 's' 32 ' '  118 'v' 101 'e' 114 'r' 121 'y' 32 ' '
0x80497d8:      101 'e'
(gdb) break main
Breakpoint 1 at 0x80489b7: file bomb.c, line 36.
(gdb)
```

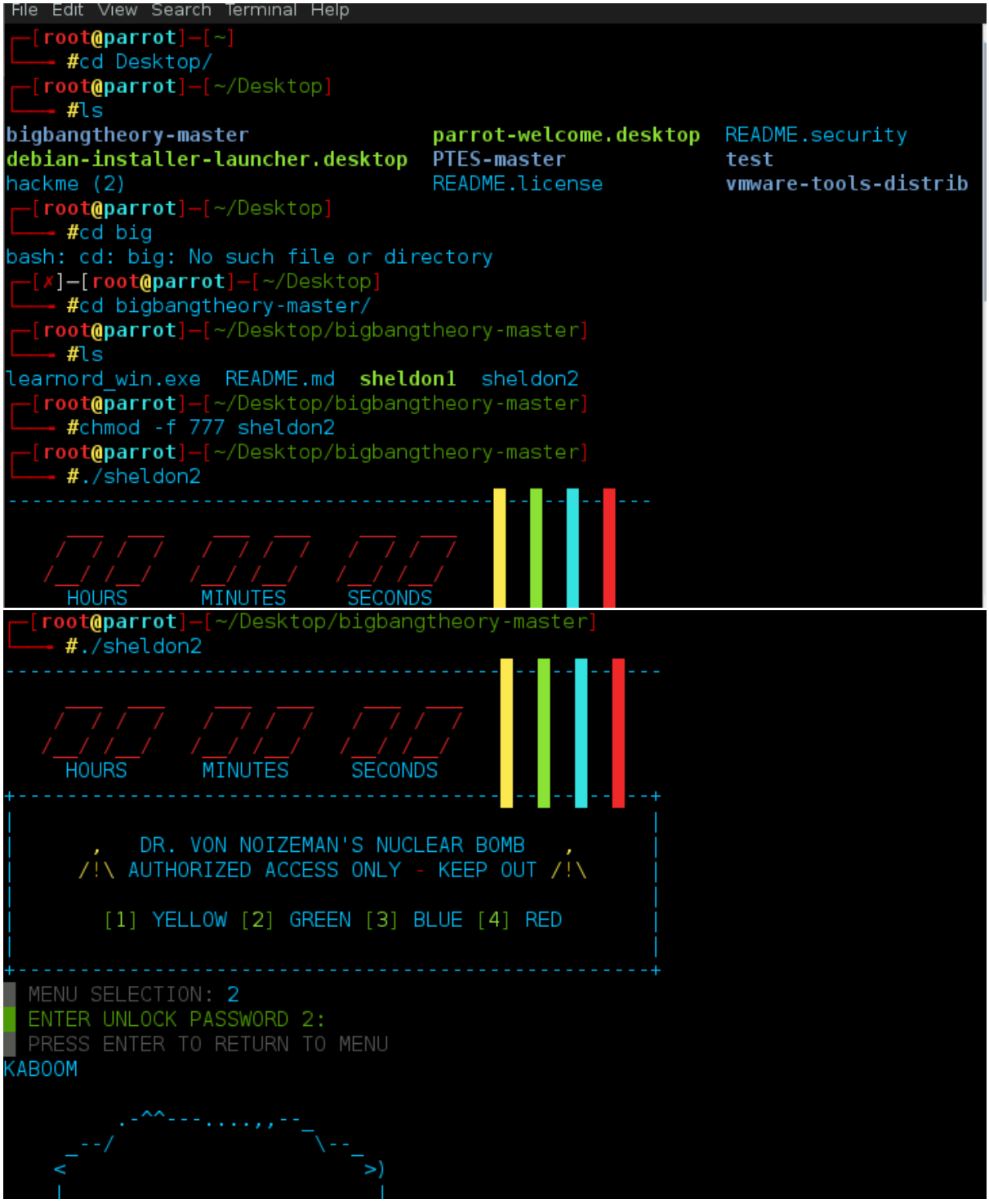

root@kali: ~/Downloads/
Actions Edit View Help
kali: ~/...theory-master
:~/Downloads/bigbangtheory-master# ./s
e to my fiendish little bomb. You have 6
to blow yourself up. Have a nice day!
speaking is very easy.
1 defused. How about the next one?


:~/Downloads/bigbangtheory-master# ./sh
bash: ./sheldon1: Permission denied
:~/Downloads/bigbangtheory-master# chmo
:~/Downloads/bigbangtheory-master# ./sh
Welcome to my fiendish little bomb. You have 6 p
which to blow yourself up. Have a nice day!
gdb
BOOM!!!



Task-2

Sheldon-2


File Edit View Search Terminal Help
root@parrot ~
#cd Desktop/
root@parrot ~/Desktop
#ls
bigbangtheory-master
debian-installer-launcher.desktop
hackme (2)
parrot-welcome.desktop
PTES-master
README.license
README.security
test
vmware-tools-distrib
root@parrot ~/Desktop
#cd big
bash: cd: big: No such file or directory
root@parrot ~/Desktop
#cd bigbangtheory-master/
root@parrot ~/Desktop/bigbangtheory-master
#ls
learnord_win.exe README.md sheldon1 sheldon2
root@parrot ~/Desktop/bigbangtheory-master
#chmod -f 777 sheldon2
root@parrot ~/Desktop/bigbangtheory-master
#./sheldon2
HOURS
MINUTES
SECONDS
root@parrot ~/Desktop/bigbangtheory-master
#./sheldon2
HOURS
MINUTES
SECONDS
DR. VON NOIZEMAN'S NUCLEAR BOMB
AUTHORIZED ACCESS ONLY - KEEP OUT
[1] YELLOW [2] GREEN [3] BLUE [4] RED
MENU SELECTION: 2
ENTER UNLOCK PASSWORD 2:
PRESS ENTER TO RETURN TO MENU
KABOOM

```
┌─[root@parrot]─[~/Desktop]
└──╼ #cd bigbangtheory-master/
┌─[root@parrot]─[~/Desktop/bigbangtheory-master]
└──╼ #chmod -f 777 sheldon2
┌─[root@parrot]─[~/Desktop/bigbangtheory-master]
└──╼ #gdb sheldon2
GNU gdb (GDB) 7.4.1-debian
Copyright (C) 2012 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>...
Reading symbols from /root/Desktop/bigbangtheory-master/sheldon2...done.
(gdb)
(gdb) set disassembly-flavor intel
(gdb) disassemble main
Dump of assembler code for function main:
   0x080494ca <+0>:     lea    ecx,[esp+0x4]
   0x080494ce <+4>:     and    esp,0xfffffff0
   0x080494d1 <+7>:     push   DWORD PTR [ecx-0x4]
   0x080494d4 <+10>:    push   ebp
```

```
   0x08049670 <+422>:   lea    eax,[ebp-0x1c]
   0x08049673 <+425>:   mov    DWORD PTR [esp],eax
   0x08049676 <+428>:   call   0x8048764 <strcasecmp@plt>
   0x0804967b <+433>:   test   eax,eax
   0x0804967d <+435>:   jne    0x804968d <main+451>
   0x0804967f <+437>:   mov    DWORD PTR [esp],0xa
   0x08049686 <+444>:   call   0x8048754 <raise@plt>
   0x0804968b <+449>:   jmp    0x80496ab <main+481>
   0x0804968d <+451>:   movzx  eax,BYTE PTR [ebp-0x1c]
   0x08049691 <+455>:   cmp    al,0xa
   0x08049693 <+457>:   jne    0x80496a1 <main+471>
   0x08049695 <+459>:   mov    DWORD PTR [ebp-0x24],0x0
---Type <return> to continue, or q <return> to quit---q
Quit
(gdb) x/4 0x0804961c
0x804961c <main+338>:   69485767        134521207       -1981528691     9044060
0
(gdb) break point
Function "point" not defined.
Make breakpoint pending on future shared library load? (y or [n]) y

Breakpoint 1 (point) pending.
(gdb)
Function "point" not defined.
```