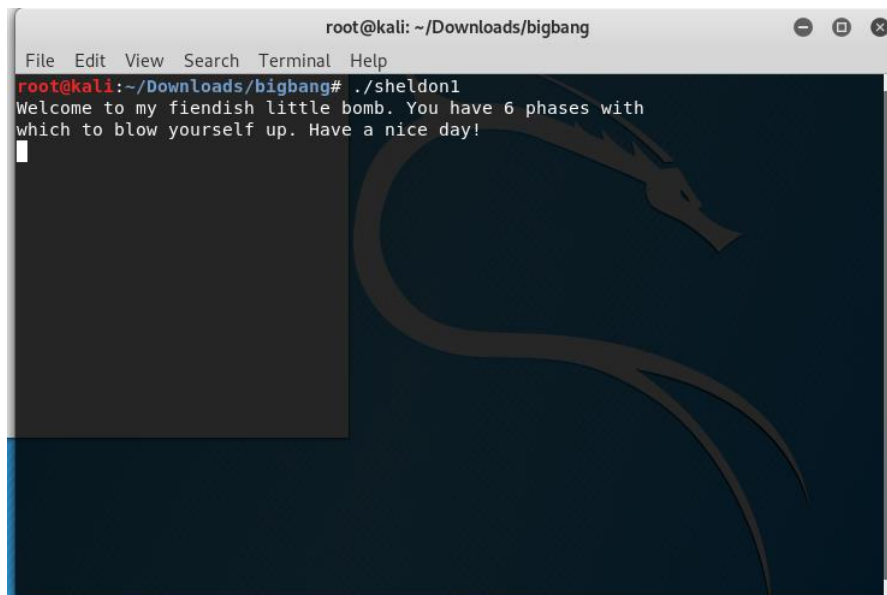


## Sheldon1



A terminal window titled "root@kali: ~/Downloads/bigbang" with a menu bar (File, Edit, View, Search, Terminal, Help) and standard window controls. The terminal shows the command `root@kali:~/Downloads/bigbang# ./sheldon1` being executed. The output is: "Welcome to my fiendish little bomb. You have 6 phases with which to blow yourself up. Have a nice day!". A large, faint, stylized dragon logo is visible in the background of the terminal window.

```
root@kali: ~/Downloads/bigbang
File Edit View Search Terminal Help
root@kali:~/Downloads/bigbang# ./sheldon1
Welcome to my fiendish little bomb. You have 6 phases with
which to blow yourself up. Have a nice day!
```

[illegible]

```

riper.cmcl.cs.cmu.edusockeye.cmcl.cs.cmu.edusheepshead.cmcl.cs.cmu.edushad.cmcl.cs.cmu.edusauger.cmcl.cs.cmu.educmcl.cs.cmu.edupaddlefish.cmcl.cs.cmu.edumuskie.cmcl.cs.cmu.eduminnow.cmcl.cs.cmu.eduinconnu.cmcl.cs.cmu.edugraydubuegill.cmcl.cs.cmu.edubass.cmcl.cs.cmu.eduSo you think you can stop the bomb with ctrl-c, do you?

```

Reading symbols from sheldon1...done.

(gdb) disass main

Dump of assembler code for function main:

```
0x080489b0 <+0>:    push    %ebp
0x080489b1 <+1>:    mov     %esp,%ebp
0x080489b3 <+3>:    sub     $0x14,%esp
0x080489b6 <+6>:    push    %ebx
0x080489b7 <+7>:    mov     0x8(%ebp),%eax
0x080489ba <+10>:   mov     0xc(%ebp),%ebx
0x080489bd <+13>:   cmp     $0x1,%eax
0x080489c0 <+16>:   jne     0x80489d0 <main+32>
0x080489c2 <+18>:   mov     0x804b648,%eax
0x080489c7 <+23>:   mov     %eax,0x804b664
0x080489cc <+28>:   jmp     0x8048a30 <main+128>
0x080489ce <+30>:   mov     %esi,%esi
0x080489d0 <+32>:   cmp     $0x2,%eax
0x080489d3 <+35>:   jne     0x8048a10 <main+96>
0x080489d5 <+37>:   add     $0xffffffff8,%esp
0x080489d8 <+40>:   push    $0x8049620
0x080489dd <+45>:   mov     0x4(%ebx),%eax
0x080489e0 <+48>:   push    %eax
0x080489e1 <+49>:   call    0x8048880 <fopen@plt>
0x080489e6 <+54>:   mov     %eax,0x804b664
0x080489eb <+59>:   add     $0x10,%esp
0x080489ee <+62>:   test    %eax,%eax
--Type <return> to continue, or q <return> to quit---r
0x080489f0 <+64>:   jne     0x8048a30 <main+128>
0x080489f2 <+66>:   add     $0xfffffffffc,%esp
0x080489f5 <+69>:   mov     0x4(%ebx),%eax
0x080489f8 <+72>:   push    %eax
0x080489f9 <+73>:   mov     (%ebx),%eax
0x080489fb <+75>:   push    %eax
0x080489fc <+76>:   push    $0x8049622
0x08048a01 <+81>:   call    0x8048810 <printf@plt>
0x08048a06 <+86>:   add     $0xffffffff4,%esp
0x08048a09 <+89>:   push    $0x8
0x08048a0b <+91>:   call    0x8048850 <exit@plt>
0x08048a10 <+96>:   add     $0xffffffff8,%esp
0x08048a13 <+99>:   mov     (%ebx),%eax
0x08048a15 <+101>:  push    %eax
0x08048a16 <+102>:  push    $0x804963f
0x08048a1b <+107>:  call    0x8048810 <printf@plt>
0x08048a20 <+112>:  add     $0xffffffff4,%esp
0x08048a23 <+115>:  push    $0x8
0x08048a25 <+117>:  call    0x8048850 <exit@plt>
0x08048a2a <+122>:  lea     0x0(%esi),%esi
0x08048a30 <+128>:  call    0x8049160 <initialize_bomb>
0x08048a35 <+133>:  add     $0xffffffff4,%esp
```

```

Reading symbols from sheldon1...done.
(gdb) break phase_1
Breakpoint 1 at 0x8048b26
(gdb) run
Starting program: /root/Downloads/bigbang/sheldon1
Welcome to my fiendish little bomb. You have 6 phases with
which to blow yourself up. Have a nice day!
test string

Breakpoint 1, 0x8048b26 in phase_1 ()
(gdb) p/x $eax
$1 = 0x804b680
(gdb) x /25c 0x804b680
0x804b680 <input_strings>: 116 't' 101 'e' 115 's' 116 't' 32 ' ' 115 's' 116 't' 114 'r'
0x804b688 <input_strings+8>: 105 'i' 110 'n' 103 'g' 0 '\000' 0 '\000' 0 '\000' 0 '\000' 0 '\000' 0 '\000' 0 '\000' 0 '\000'
0x804b690 <input_strings+16>: 0 '\000' 0 '\000' 0 '\000' 0 '\000' 0 '\000' 0 '\000' 0 '\000' 0 '\000' 0 '\000' 0 '\000'
0x804b698 <input_strings+24>: 0 '\000'
(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) asy
Undefined command: "asy". Try "help".
(gdb)

```

```

root@kali:~/Downloads/bigbang# ./sheldon1
Welcome to my fiendish little bomb. You have 6 phases with
which to blow yourself up. Have a nice day!
Public speaking is very easy.
Phase 1 defused. How about the next one?

```