To err is human... to really foul up requires the root password.

0 1 3 6 10 15

6 966

52 4

beldog

6 1 4 5 3 2

\264\017@

"Curses, you've found the secret phase!"

"But finding it and solving it are quite different..."

CukoosEgg

zeus-1.vse.gmu.edu

zeus-1

0x604340

0x6042f0 <node1>: **701**

0x6042f4 <node1+4>: 1

0x6042f8 <node1+8>: 6308608

0x6042fc <node1+12>: 0

0x604300 <node2>: 270

0x604304 <node2+4>: 2

0x604308 <node2+8>: 6308624

0x60430c <node2+12>: 0

0x604310 <node3>: **353**

0x604314 <node3+4>: 3

0x604318 <node3+8>: 6308640

0x60431c <node3+12>: 0

0x604320 <node4>: **461**

0x604324 <node4+4>: 4

0x604328 <node4+8>: 6308656

0x60432c <node4+12>: 0

0x604330 <node5>: **435**

0x604334 <node5+4>: 5

0x604338 <node5+8>: 6308672

0x60433c <node5+12>: 0

0x604340 <node6>: **877**

(gdb) 6 1 4 5 3 2

11111111111111111111111111111111100000000010100

0000000000401728 <phase\_defused>:

401728: 48 83 ec 68 sub $0x68,%rsp

40172c: bf 01 00 00 00 mov $0x1,%edi

401731: e8 fa fe ff ff callq 401630 <send\_msg>

401736: 83 3d 5f 30 20 00 06 cmpl $0x6,0x20305f(%rip) # 60479c <num\_input\_strings>

40173d: 75 6d jne 4017ac <phase\_defused+0x84>

40173f: 4c 8d 44 24 10 lea 0x10(%rsp),%r8

401744: 48 8d 4c 24 08 lea 0x8(%rsp),%rcx

401749: 48 8d 54 24 0c lea 0xc(%rsp),%rdx

40174e: be 47 28 40 00 mov $0x402847,%esi

401753: bf b0 48 60 00 mov $0x6048b0,%edi

401758: b8 00 00 00 00 mov $0x0,%eax

40175d: e8 ce f4 ff ff callq 400c30 <\_\_isoc99\_sscanf@plt>

401762: 83 f8 03 cmp $0x3,%eax

401765: 75 31 jne 401798 <phase\_defused+0x70>

401767: be 50 28 40 00 mov $0x402850,%esi

40176c: 48 8d 7c 24 10 lea 0x10(%rsp),%rdi

401771: e8 ef fb ff ff callq 401365 <strings\_not\_equal>

401776: 85 c0 test %eax,%eax

401778: 75 1e jne 401798 <phase\_defused+0x70>

40177a: bf a8 26 40 00 mov $0x4026a8,%edi

40177f: e8 bc f3 ff ff callq 400b40 <puts@plt>

401784: bf d0 26 40 00 mov $0x4026d0,%edi

401789: e8 b2 f3 ff ff callq 400b40 <puts@plt>

40178e: b8 00 00 00 00 mov $0x0,%eax

401793: e8 98 fa ff ff callq 401230 <secret\_phase>

401798: bf 08 27 40 00 mov $0x402708,%edi

40179d: e8 9e f3 ff ff callq 400b40 <puts@plt>

4017a2: bf 38 27 40 00 mov $0x402738,%edi

4017a7: e8 94 f3 ff ff callq 400b40 <puts@plt>

4017ac: 48 83 c4 68 add $0x68,%rsp

4017b0: c3 retq

4017b1: 66 2e 0f 1f 84 00 00 nopw %cs:0x0(%rax,%rax,1)

4017b8: 00 00 00

4017bb: 0f 1f 44 00 00 nopl 0x0(%rax,%rax,1)