Lab 4

1

```
0.000000 execve("./prob1", ["./prob1"], [/* 50 vars */]) = 0
0.000664 brk(NULL)           = 0x16f7000
0.000110 access("/etc/ld.so.nohwcap", F_OK) = -1 ENOENT (No such file or directory)
0.000113 access("/etc/ld.so.preload", R_OK) = -1 ENOENT (No such file or directory)
```

Open cache

```
0.000101 open("/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
0.000103 fstat(3, {st_mode=S_IFREG|0644, st_size=157041, ...}) = 0
0.000093 mmap(NULL, 157041, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7fbf55273000
```

Close cache

```
0.000086 close(3)            = 0
0.000091 access("/etc/ld.so.nohwcap", F_OK) = -1 ENOENT (No such file or directory)
```

Open lib

```
0.000145 open("/lib/x86_64-linux-gnu/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
```

Read lib

```
0.000095 read(3, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\t\2\0\0\0\0\0"..., 832) = 832
0.000090 fstat(3, {st_mode=S_IFREG|0755, st_size=1868984, ...}) = 0
0.000088 mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) =
0x7fbf552a7000
0.000103 mmap(NULL, 3971488, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) =
0x7fbf54cab000
0.000090 mprotect(0x7fbf54e6b000, 2097152, PROT_NONE) = 0
0.000092 mmap(0x7fbf5506b000, 24576, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE,
3, 0x1c0000) = 0x7fbf5506b000
0.000105 mmap(0x7fbf55071000, 14752, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS,
-1, 0) = 0x7fbf55071000
```

Close lib

```
0.000101 close(3)            = 0
0.000106 mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) =
0x7fbf552a6000
0.000092 mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) =
0x7fbf552a5000
0.000089 arch_prctl(ARCH_SET_FS, 0x7fbf552a6700) = 0
0.000200 mprotect(0x7fbf5506b000, 16384, PROT_READ) = 0
0.000087 mprotect(0x600000, 4096, PROT_READ) = 0
0.000089 mprotect(0x7fbf552a0000, 4096, PROT_READ) = 0
0.000085 munmap(0x7fbf55273000, 157041) = 0
0.000242 brk(NULL)           = 0x16f7000
0.000080 brk(0x1718000)      = 0x1718000
```

Open the input file in read-only mode

```
0.000091 open("input.txt", O_RDONLY) = 3
0.000098 fstat(3, {st_mode=S_IFREG|0664, st_size=33, ...}) = 0
```

Read is called and the entire file is read in

```
0.000094 read(3, "blah 1\nblah 10\nblah 100\nblah 100"..., 4096) = 33
0.000116 fstat(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 0), ...}) = 0
```

The first three lines of the file are printed

The fourth line of the file is not printed because it had EOF at the end of the line instead of newline

```
0.000090 write(1, "blah 1\n", 7) = 7
0.000119 write(1, "blah 10\n", 8) = 8
0.000092 write(1, "blah 100\n", 9) = 9
```

Read is called again but there is nothing more to read

```
0.000093 read(3, "", 4096)   = 0
```

The file is closed

```
0.000087 close(3)            = 0
0.000095 exit_group(0)       = ?
0.000148 +++ exited with 0 +++
```

2

The java strace is significantly longer because it has to load the entire Java Virtual Machine However, it eventually does basically the same thing. A read of the entire file, and then a series of write operations. Java prints all 4 lines though

3

a) The new write function shadows the actual write function

b) The goodbye call directly bypasses the blocked write() function and goes straight to the syscall that does the same thing
c) They are in the same place
d) Look in the 32 libraries to see where syscall is defined
e) Syscall might not be defined in the 32 bit libraries
f) Now syscall is defined to do nothing no matter how you compile it
g) Because syscall is now defined to actually do something, print the variable
h) Yes, functions can always shadow eachother

```
10748 execve("./a.out", ["./a.out"], [/* 55 vars */]) = 0
10748 brk(NULL)                         = 0x56878000
10748 access("/etc/ld.so.nohwcap", F_OK) = -1 ENOENT (No such file or directory)
10748 mmap2(NULL, 12288, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0xf7784000
10748 access("/etc/ld.so.preload", R_OK) = -1 ENOENT (No such file or directory)
10748 open("/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
10748 fstat64(3, {st_mode=S_IFREG|0644, st_size=298723, ...}) = 0
10748 mmap2(NULL, 298723, PROT_READ, MAP_PRIVATE, 3, 0) = 0xf773b000
10748 close(3)                          = 0
10748 access("/etc/ld.so.nohwcap", F_OK) = -1 ENOENT (No such file or directory)
10748 open("/lib/i386-linux-gnu/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
10748 read(3, "\177ELF\1\1\1\3\0\0\0\0\0\0\0\3\0\3\0\1\0\0\0\0\204\1\0004\0\0\0"..., 512) =
512
10748 fstat64(3, {st_mode=S_IFREG|0755, st_size=1787812, ...}) = 0
10748 mmap2(NULL, 1796604, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0xf7584000
10748 mmap2(0xf7735000, 12288, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3,
0x1b0000) = 0xf7735000
10748 mmap2(0xf7738000, 10748, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0)
= 0xf7738000
10748 close(3)                          = 0
10748 set_thread_area({entry_number:-1, base_addr:0xf77867c0, limit:1048575, seg_32bit:1,
contents:0, read_exec_only:0, limit_in_pages:1, seg_not_present:0, useable:1}) = 0
(entry_number:12)
10748 mprotect(0xf7735000, 8192, PROT_READ) = 0
10748 mprotect(0x565cb000, 4096, PROT_READ) = 0
10748 mprotect(0xf77ae000, 4096, PROT_READ) = 0
10748 munmap(0xf773b000, 298723)        = 0
10748 write(1, "goodbye\n", 8)          = 8
10748 --- SIGSEGV {si_signo=SIGSEGV, si_code=SEGV_MAPERR, si_addr=0xd} ---
10748 +++ killed by SIGSEGV +++
```

The first four lines of the assembly (the “mov”s) are loading in variables into memory, then the `int $0x80` is the call to the kernel, and that’s where the string is printed.