

Buffer Overflow

Part 1

Stack level 0, frame at 0x7fff5fbffb60:

rip = 0x100000db6 in senior (examine_stack.c:9); saved rip = 0x100000e02
called by frame at 0x7fff5fbffb80
source language c.
Arglist at 0x7fff5fbffb50, args: a=2012, b=2
Locals at 0x7fff5fbffb50, Previous frame's sp is 0x7fff5fbffb60
Saved registers:
rbp at 0x7fff5fbffb50, rip at 0x7fff5fbffb58
cougars = 30000

Stack level 1, frame at 0x7fff5fbffb80:

rip = 0x100000e02 in junior (examine_stack.c:16); saved rip = 0x100000e53
called by frame at 0x7fff5fbffbd0, caller of frame at 0x7fff5fbffb60
source language c.
Arglist at 0x7fff5fbffb90, args: x=2012, y=0x7fff5fbffbb2
Locals at 0x7fff5fbffb90, Previous frame's sp is 0x7fff5fbffb80
Saved registers:
rbp at 0x7fff5fbffb90, rip at 0x7fff5fbffb98
name = "cougars\000\000"

Stack level 2, frame at 0x7fff5fbffbd0:

rip = 0x100000e53 in sophomore (examine_stack.c:23); saved rip = 0x100000ed4
called by frame at 0x7fff5fbffc30, caller of frame at 0x7fff5fbffb80
source language c.
Arglist at 0x7fff5fbffbc0, args: a=37, b=2012
Locals at 0x7fff5fbffbc0, Previous frame's sp is 0x7fff5fbffbd0
Saved registers:
rbp at 0x7fff5fbffbc0, rip at 0x7fff5fbffbc8
tiny = 8

Stack level 3, frame at 0x7fff5fbffc30:

rip = 0x100000ed4 in freshman (examine_stack.c:29); saved rip = 0x100000f32
called by frame at 0x7fff5fbffc60, caller of frame at 0x7fff5fbffbd0
source language c.
Arglist at 0x7fff5fbffc20, args: a=12, b=25, c=2012
Locals at 0x7fff5fbffc20, Previous frame's sp is 0x7fff5fbffc30
Saved registers:
rbp at 0x7fff5fbffc20, rip at 0x7fff5fbffc28
housing = "Helaman Halls", '\000' <repeats 16 times>

Stack level 4, frame at 0x7fff5fbffc60:

rip = 0x100000f32 in main (examine_stack.c:41); saved rip = 0x7fff864265ad
caller of frame at 0x7fff5fbffc30
source language c.
Arglist at 0x7fff5fbffc50, args:
Locals at 0x7fff5fbffc50, Previous frame's sp is 0x7fff5fbffc60

Saved registers:

rbp at 0x7fff5fbffc50, rip at 0x7fff5fbffc58

year = 2012

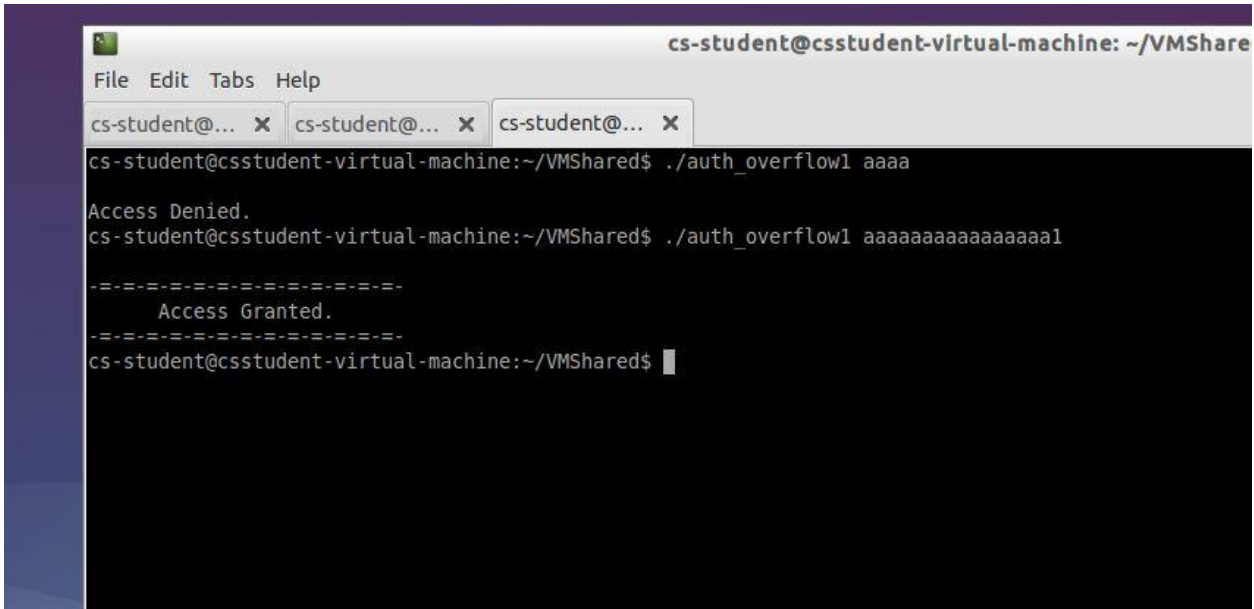
month = 12

day = 25

result = 0

Part 2

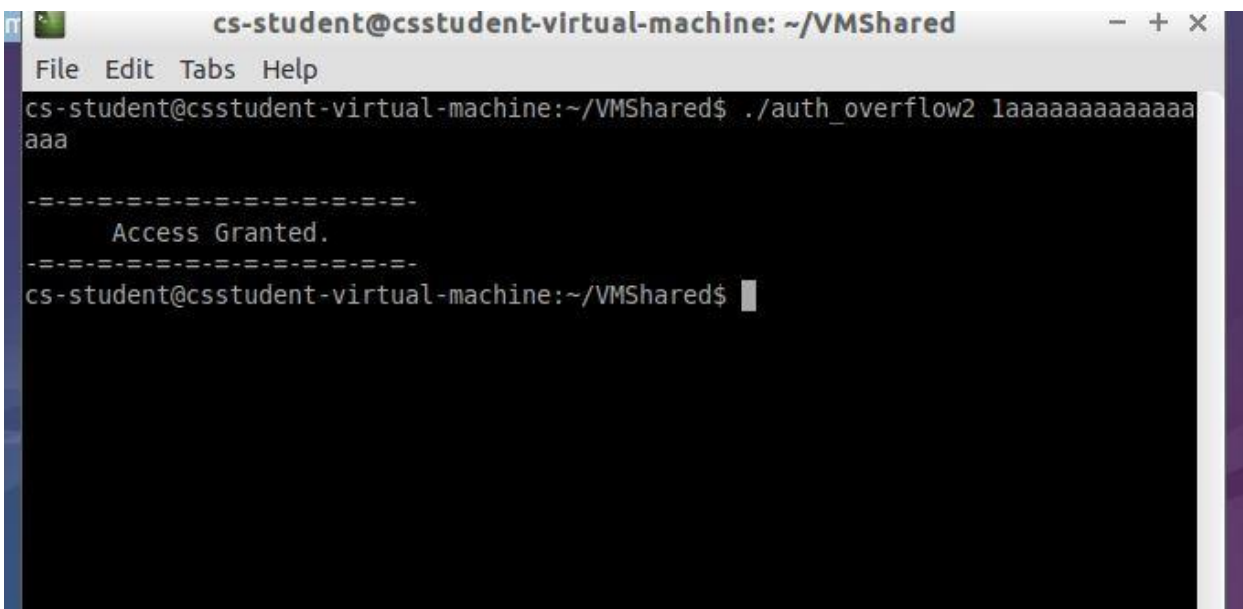
Part A



A terminal window titled "cs-student@csstudent-virtual-machine: ~/VMShare". The window has a menu bar with "File", "Edit", "Tabs", and "Help". There are three tabs, all labeled "cs-student@...". The terminal shows the following commands and output:

```
cs-student@csstudent-virtual-machine:~/VMShared$ ./auth_overflow1 aaaa
Access Denied.
cs-student@csstudent-virtual-machine:~/VMShared$ ./auth_overflow1 aaaaaaaaaaaaaaaaaa1
-----
Access Granted.
-----
cs-student@csstudent-virtual-machine:~/VMShared$
```

Part B



A terminal window titled "cs-student@csstudent-virtual-machine: ~/VMShared". The window has a menu bar with "File", "Edit", "Tabs", and "Help". The terminal shows the following commands and output:

```
cs-student@csstudent-virtual-machine:~/VMShared$ ./auth_overflow2 1aaaaaaaaaaaaa
aaa
-----
Access Granted.
-----
cs-student@csstudent-virtual-machine:~/VMShared$
```

Part C

```
Breakpoint 1, 0x08048573 in main (argc=2, argv=0xbffffef64) at auth_overflow3.c:23
23         if(check_authentication(argv[1])) {
(gdb) jump *0x0804857c
Continuing at 0x804857c.

-----
        Access Granted.
-----
[Inferior 1 (process 9746) exited with code 034]
(gdb) █
```

Part D

I was unable to get the shell code working on the command line to give access in the program. After so many tries and searching on Google I decided that I probably wasn't going to be able to get and so I am satisfied with getting all but the last part done.