Buffer Overflow Exploit Lab

Tailang Cao u1480633

1. Test the code with random password, gives the wrong password message correctly

A black screen with white text

Description automatically generated

1. Test the code with the correct password, logged in successfully

A black background with white text

Description automatically generated

1. View the assembly code with otool -tV login

A screenshot of a computer program

Description automatically generated

1. The success function starts from address 0000000100003c6c
2. To make the attack successful, we should be able to make the function return to the success function instead of the main function by making the password the success address.
3. Write the password in little indian way hence backwards:

% python3 -c 'import sys; sys.stdout.buffer.write(b"a"\*24 + b"\x6c\x3c\x00\x00\x01\x00\x00\x00")' > password.txt

1. After multiple attempts the attack still wouldn’t work and the login function would still return in main. My guess is the address is incorrect or the way I write it in the password.txt cant direct it to success function.