Homework 3: implementing a 64-bit Buffer Overflow Exploit

Xin Liu

Florida State University
xliu15j@fsu.edu

CIS 5370 Computer Security
https://xinliulab.github.io/cis5370.html
January 29, 2025

Homework 3

Objective: In our course, we have used a 64-bit `stack.c` file to demonstrate stack-based vulnerabilities in a 64-bit environment. However, the textbook provides a 32-bit exploit script (`exploit.py`) that generates a malicious file (`badfile`) containing shellcode and a return address overwrite. Your task is to convert this 32-bit exploit into a 64-bit version.

Task:

1. Modify the exploit to work in a 64-bit Linux environment.
2. Consider differences between 32-bit and 64-bit registers.
3. Adjust the buffer overflow offset for the 64-bit architecture.
4. Run the exploit in your 64-bit Linux virtual machine.

Submission Requirements:

- Submit the modified 64-bit exploit code.
- Provide a report including:
  - Screenshots demonstrating the exploit execution (e.g., successfully gaining a shell).
  - Explanation of modifications and key differences from the 32-bit version.