**CSE 410/518 Software Security**

**Instructor: Ziming Zhao
Homework – 8**

**We will enable ASLR on the CTF platform on 11/31/2023 8PM.**

[5 points] Task 1: Compare the disassembly of the **compute** function in ***aslr1\_nopiestatic\_32 , aslr1\_32, aslr1\_nopie\_32***. Explain how and why they are different. Take screenshots.

[5 points] Task 2: Execute ***aslr1\_nopiestatic\_32 , aslr1\_32, aslr1\_nopie\_32***. Briefly explain the outputs.

[10 points] Task 3: Exploit **aslr2\_32** and get the flag. The goal is to return to printfsecret. Take screenshots and briefly explain why your exploit work.

[10 points] Task 4: Compare the source code of **seccompallow** and **seccompdisallow,** which are the same file in lecture notes. Run both binaries with **strace** and compare the differences in the issued system calls.

[15 points] Task 5: Develop a **32-bit ascii shellcode** that reads the flag file and prints the flag in the terminal. Use **testerascii\_32** to test your shellcode and get the flag**.** You can use open and sendfile system calls (changing from the 32-bit version without zeros in the lecture notes). Attach your shellcode in your submission. Show screenshots to indicate the successful execution of your shellcode.

[20 bonus points] Task 6: Develop a **64-bit non-zero shellcode** that reads the flag file and prints the flag in the terminal. Use **testernozero\_64** to test your shellcode and get the flag**.** You can use open and sendfile system calls (changing from the 64-bit bit version with zero in the lecture notes). Attach your shellcode in your submission. Show screenshots to indicate the successful execution of your shellcode.