**CY5770 Software Vulnerabilities and Security**

**Instructor: Ziming Zhao
Homework – 1**

**Submit your homework on Canvas.**

**Reading. Read the following materials.**

[ ] Reading Task 1: Read “x86 Assembly Guide” at Intel syntax https://www.cs.virginia.edu/~evans/cs216/guides/x86.html

[ ] Reading Task 2: Read “Guide to x86-64” at https://web.stanford.edu/class/cs107/guide/x86-64.html

[ ] Reading Task 3: Read “Setuid Program Example” at <https://www.gnu.org/software/libc/manual/html_node/Setuid-Program-Example.html>

[ ] Reading Task 4: Read blog “Anatomy of a Program in Memory” at <https://manybutfinite.com/post/anatomy-of-a-program-in-memory/>

[ ] Reading Task 5: Read the Chapter 0 “Operating system interfaces” in “xv6, a simple, Unix-like teaching operating system” <https://pdos.csail.mit.edu/6.828/2014/xv6/book-rev8.pdf>

**Hands-on Tasks.**

**Your username on http://cy5770-cacti.khoury.northeastern.edu: \_\_\_\_\_\_\_\_\_**

[0 point] Google and read NEU academic integrity policies.

[6 points] Task 1: Read the syllabus. Find the secret, which is in the format of “FLAG-XXXXXXXX”.

[6 points] Task 2: Register an account at **cy5770-cacti.khoury.northeastern.edu.** (1) Use the “cat” command to print the content in “/flag”. Explain the results and take a screenshot. (2) Run the **firstflag\_32** challenge, explain the results, submit the flag, take a screenshot.

[6 points] Task 3: Run any challenge, and list all the set-UID or set-GID (Google what set-GID is.) programs under /bin. Explain the commands you used and take a screenshot of the results.

[7 points] Task 4: Run the **add\_32** challenge. You can find the source code of add at the **/code/add** directory. Compile the C program with and without the **-save-temps** option. Note that the /code/add directory is not-writable. Explain the differences between compiling with and without -save-temps.

[7 points] Task 5: Run the **ladd\_32** challenge. Use the *objdump -M intel -d* command to disassemble the binary. Find the function **ladd** in the binary (Screenshot). Explain each instruction of this function. Please use the Intel syntax. Google the instruction if you do not understand its meaning.

[7 points] Task 6: Run the **ladd\_64** challenge. Use *objdump* to disassemble the binary. Find the function **ladd** in the binary (Screenshot). Explain each instruction of this function. Please use the Intel syntax. Google the instruction if you do not understand its meaning.

[6 points] Task 7: Read <https://www.gnu.org/software/libc/manual/html_node/Setuid-Program-Example.html>. Run the **rdsecret\_64** challenge. Explain the outputs. Submit the flag and take screenshots.