Lab 03: Buffer Overflows

Goals

- Identify vulnerabilities of a specified type in an application
- Remediate identified vulnerabilities using specified method

Notes

The lab is available in the Learn org of Dakota State University's Information Assurance Lab within the vApp <username>_CSC234_Zwach_Base. It's accessible at https://ialab.dsu.edu. You can start the vApp by double clicking on it and then clicking the play button in the Flash client or clicking Actions and Start in the HTML5 client.

The code that comprises the entire application (nums.c) is available within the /home/student/course_files/_assignments/buffer_overflow directory. Make your changes there using a text editor of your choosing. Compile using gcc. Remember, you can permanently revert your changes to the codebase at any time with the command `revertall`.

The username is **student** and the password is **Password1!**.

Discovery

This program has several flaws including some which could result in overflow of a memory buffer. Identify changes you'd make and why.

1. Review the source code for the application of interest (nums.c).
    a. Provide screenshots of vulnerable or otherwise flawed code segments.
    b. Explain each issue in your own words.
2. Compile and run the program
    a. Provide a screenshot demonstrating each of the vulnerabilities using a method of your choice (causing a segmentation fault or other result is good enough, it's not necessary to gain control of EIP/RIP)

Remediation

After confirming the vulnerability, use your knowledge and available resources to modify the source to follow best practices and avoid integer overflows.

3. Modify the source code to gracefully handle overflows and remove any other flaws.
    a. Document your resulting source code with a screenshot
4. Test your changes
    a. Are your attempts at entering further oversized input successful? Why or why not?
    b. Provide screenshots documenting proper handling of invalid / oversized input.

Scoring

The rubric will be published at scoring time. Each portion of the assignment has the following points assigned.

Section	Points
1	6
2	2
3	6
4	6
Total	**20**