CS 5434 Assignment 1

Due Weds 11th Sep by 5pm in Upson 317

Summary

This exercise requires you to find a partner. Each of you will write your own program with vulnerabilities in. Then you will trade programs (in source code form) with your partner and find/exploit the vulnerabilities in their program. You should not collaborate on writing the program. You will then come together to explain and demonstrate your programs and how to exploit each other's programs to either me or the TA, who will question you to make sure you understand what you did.

If you end up without a partner, contact me and we will form a group of three who can exchange programs round-robin style.

Program

Your program, written in C, should take an ASCII text file containing English text (filename as a command line argument), and count how many times each word appears. It should output the words and the counts in sorted order on stdout. For example, if the input file was

foo foo bar foo gnu bar

It should output

foo 3
bar 2
gnu 1

Intentionally include in your program at least one buffer overflow vulnerability, and at least one system() vulnerability. The vulnerabilities should be exploitable by a malicious input text file.

Your program should compile and run on the Linux machines in 317 and you should have at least one multi-line text file which exhibits that it works correctly.

Exploitation Step 1

Take your partner's program, and develop an input text file that will exploit the system() vulnerability. Your file should include within it a shell script or similar,

and be able to run that script on the machine by exploiting the system() vulnerability.

Exploitation Step 2

Locate the buffer overflow in your partner's program, and develop a text file that demonstrates the ability to crash their program by overflowing the buffer.

Exploitation Step 3

Develop an exploit that will actually execute a shell command against the buffer overflow in your partner's program. For this purpose, it's permissible to turn off compiler/OS protections. You might want to examine these links for some hints:

http://stackoverflow.com/questions/2340259/how-to-turn-off-gcc-compiler-optimization-to-enable-buffer-overflow
http://paulmakowski.wordpress.com/2011/01/25/smashing-the-stack-in-2011/

Extra Credit (for those aiming for A+)

Develop an exploit against your partner's program that will work without turning off all the compiler/OS protections.

Notes

Again, it's permissible to discuss the assignment in general terms with your classmates, but you need to develop your own program and exploits, so that you have done your own work and can defend it in detail in our discussion.

If you believe that your partner's program is not actually vulnerable, it's permissible to go back to them and have them correct the issue, or clarify why they believe it is vulnerable.

Also, this is the first assignment and the first time this lab has been used for this class. Chances are excellent that we'll have a few teething problems with the lab. Please email or call me immediately if you run into any problems and I'll try to get them resolved promptly. If we have huge problems, I'll extend the deadline (but don't count on that unless I say ☺)