Homework 5

Due: December 6, 2019 at 11:59pm **Points:** 100

Questions

Remember to justify your answers.

1. (*20 points*) StackGuard is a tool for detecting buffer overflows. It modifies the compiler to place a known (pseudo)random number (a *canary*) on the stack just before the return address when a function is called. Additional code is added so that, just before the function returns, it pops the canary and compares it to the value that was placed upon the stack. If the two differ, StackGuard asserts a buffer overflow has occurred, and invokes an error handler to terminate the program. How effective is this approach at stopping stack-based buffer overflows? Under what conditions might it fail?

2. (*20 points*) Assume that the Clark-Wilson model is implemented on a computer system. Could a computer virus that scrambled constrained data items be introduced into the system? Why or why not? Specifically, if not, identify the precise control that would prevent the virus from being introduced, and explain why it would prevent the virus from being introduced; if yes, identify the specific control or controls that would allow the virus to be introduced and explain why they fail to keep it out.

3. (*20 points*) Classify each of the following vulnerabilities using the PA model. Assume that the classification is for the implementation level. Remember to justify your answers.
   (a) The presence of the "wiz" command in the *sendmail* program.
   (b) The failure to handle the **IFS** shell variable by *loadmodule*.
   (c) The failure to select an Administrator password that was difficult to guess.
   (d) The failure of the Burroughs system to detect offline changes to files.

4. (*20 points*) An attacker breaks into a web server running on a Windows 10-based system. Because of the ease with which he broke in, he concludes that Windows 10 is an operating system with very poor security features. Is his conclusion reasonable? Why or why not?

5. (*20 points*) The story "Diabologic" by Eric Frank Russell presents an explorer making first contact with an alien race. That race thinks very logically. He proceeds to confound them.
   (a) Why can the newly-contacted race not cope with the explorer's tactics?
   (b) What key theme of this story relates to attacking or defending a computer system, and how does it do so?

Extra Credit

E1. (*20 points*) The year 2038 will pose a problem for most 32-bit UNIX and Linux systems because of the way time is represented. What specific aspect of the representation makes that year a problem? When during the year does the problem occur? Give a specific date and time. Show how you got it. What is the date with the same effect on a 64-bit system?
Hint: You will need to write a small program to find the specific date and time.