Homework 3

Due: November 11, 2022 **Points:** 100

1. (*20 points*) Consider the rule of transitive confinement. Suppose a process needs to execute a subprocess in such a way that the child can access exactly two files, one only for reading and one only for writing.
   (a) Could capabilities be used to implement this? If so, how?
   (b) Could access control lists implement this? If so, how?

2. (*40 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 (see Section 24.2.9).
   (b) The failure to handle the **IFS** shell variable by *loadmodule* (see Section 24.2.9).
   (c) The failure to select an *Administrator* password that was difficult to guess (see Section 24.2.10).
   (d) The failure of the Burroughs system to detect offline changes to files (see Section 24.2.7).

3. (*20 points*) An attacker breaks into a Web server running on a Windows Server 2022. Because of the ease with which he broke in, he concludes that the Windows Server 2022 is an operating system with very poor security features. Is his conclusion reasonable? Why or why not?

4. (*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?