Homework 3

Due: November 5, 2025 **Points:** 100

Short Answer

Answer these questions in one or two sentences.

1. (*5 points*) What probability distribution of passwords maximizes the expected time to guess a password?
2. (*5 points*) Define the confinement problem.
3. (*5 points*) What is a buffer overflow?

Longer Answer

You can use more than 1 or 2 sentences to answer these. Remember to write clearly (if you need help, go to the Writing Center on campus) and *justify your answers*!

4. (*20 points*) Classify the following vulnerabilities using the RISOS model. Assume that the classification is for the implementation level. Justify your answer.
   (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 *heartbleed* bug occurred in an implementation of OpenSSL. A client would send a keepalive message to the server, which would echo the data of the packet back to the client. The length of the packet (including the data) was in the packet header. The first few bytes of the data also contained the length of the data, and OpenSSL used the latter to determine how big the data was. The problem was that one could give a data size of 1000 when only 5 bytes of data were present. OpenSSL would then return 1000 bytes from the input queue, revealing what information was in the buffer at those 995 bytes. (See https://xkcd.com/1354/ for an amusing description of this bug.)
   (d) The failure of the Burroughs system to detect offline changes to files (see Section 24.2.7).
5. (*15 points*) The Mysterious Mortgage Company announced it has upgraded the authentication required of its website users to two-factor authentication. Amy, a mortgagee, wants to log into her account on the web site. She enters her login name and password. Instead of showing her a screen with her account information, the next screen asked her to re-enter her login name and password. After she does so, she is then given the account page. Is this two-factor authentication? Why or why not?
6. (*20 points*) In the Janus system, when the framework disallows a system call, the error code **EINTR** (interrupted system call) is returned.
   (a) When some programs have read or write system calls terminated with this error, they retry the calls. What problems might this create?
   (b) Why did the developers of Janus not devise a new error code (say, **EJAN**) to indicate an unauthorized system call?
7. (*30 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?