Homework 4

Due: November 22, 2023 **Points:** 100

1. (*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).

2. (*20 points*) A computer system provides protection using the Bell-LaPadula policy. How would a virus spread if:

   (a) the virus were placed on the system at system low (the compartment that all other compartments dominate)?

   (b) the virus were placed on the system at system high (the compartment that dominates all other compartments)?

3. (*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?

4. (*20 points*) As encryption conceals the contents of network messages, the ability of intrusion detection systems to read those packets decreases. Some have speculated that *all* intrusion detection will become host-based once all network packets have been encrypted. Do you agree? Justify your answer. In particular, if you agree, explain why no information of value can be gleaned from the network; if you disagree, describe the information of interest.