Homework 5

Due: December 6, 2024 **Points:** 100

1. (*30 points*) Why are attack trees constructed using a breadth-first search rather than a depth-first search?

2. (*30 points*) Why should the administrator (or the superuser) account never be locked regardless of how many incorrect login attempts are made? What should be done instead to alert the staff to the attempted intrusion, and how could the chances of such an attack succeeding be minimized?

3. (*40 points*) A company called the Drib has hired the computer security firm of Dewey, Cheatham, and Howe to audit their networks. The analyst from DC&H arrives and produces a floppy disk. They state that the disk is to be loaded onto a system on the internal network. They will then run the program. It will scan the Drib's networks and send the information to DC&H's headquarters in Upper Bottom. There, DC&H analysts will determine whether the Drib's security is acceptable, and will recommend changes.

   (a) The analyst informs the Drib that the program works by sending the data to DC&H's headquarters over the Internet using a proprietary protocol. They request that the firewalls be opened to allow communications to remote hosts with destination port 3260. The audit department manager, who was told to hire DC&H by the Drib's CEO, is nervous. Should his security expert recommend that the communication be allowed, or not? Why?

   (b) The analyst is asked exactly what the program does. They assures the Drib that it does nothing harmful. Given that they are so vague, the Drib security officers want to find out more information. Suggest three or four questions that they should ask to obtain the information they seek.

   (c) The analyst admits that their answers are based on what the DC&H auditors have told them. When asked for the source code of the program on the floppy, they state that it is proprietary and cannot be released. What could the Drib's officers do to assure themselves that the program is not harmful?

   (d) Based on the actions of the analyst, and assuming that finances are not a consideration, would you hire DC&H to analyze your network security? Why or why not?