Information Assurance: Homework 5

Not graded

1. A system allows the user to choose a password with a length of one to ten characters inclusive. Assume that 15,000 passwords can be tested per second. The system administrators want to expire passwords once they have a probability of 0.10 of being guessed. Determine the expected time to meet this probability under each of the following conditions.
    a. Password characters must be digits ("0" through "9").
    b. Password characters may be capital letters ("A" through "Z") and numerics ("0" through "9").
    c. 12 bits of salt are added for both a and b.

2. Try running the John the Ripper password cracking program http://www.openwall.com/john/. You should be able to install it local to your environment for an unprivileged account. Obtain a password file from http://www.cs.uiuc.edu/class/fa07/cs461/class07-passwd This file contains nine accounts with passwords from a linux system. At least one password should be cracked very easily. If you have access to a private system, try running the program for a while longer to see if you get more passwords cracked. Submit the account names and passwords that you crack. As long as you get the quickly cracked passwords, you will get full credit.

3. An organization implements a biometric authentication system. All employees register their fingerprints, and the organization stores the resulting templates on a central server. Eve hacks the server and gains access to the template. What harm can occur from this breech? How does it compare to hacked passwords?