**Subject :** BIE 33003 – SOFTWARE ENGINEERING SECURITY

**Date :** Week 3

**Lab #2 :** Password Cracking (Brute Force Attack)

**Overview**

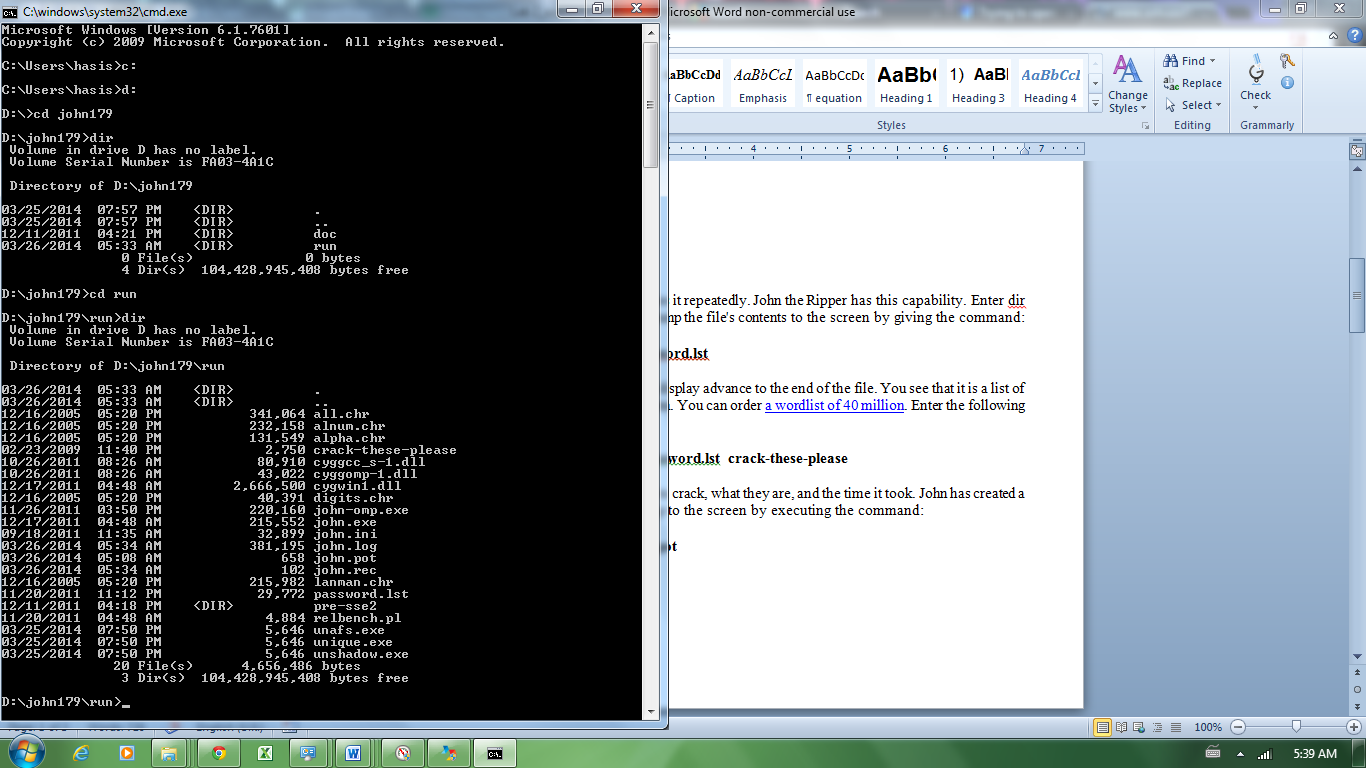
In this lab you will use a tool called "John the Ripper" to crack the passwords stored in a file. They were obtained from a Unix computer. Unix stores hashes of all its accounts' passwords in a single file. On old systems the file was /etc/passwd; on new ones it is /etc/shadow instead. The passwords themselves are never stored, but gaining their hashes is a matter of copying the containing file. Given the file, an attacker can try at his leisure to figure out what the original passwords were. That's what John the Ripper does. It has three techniques that you will use in this lab: dictionary attack, hybrid attack, and combination attack. There are John the Ripper versions for linux and Windows.

**Instructions:**

**1. Install needed software and files**

If John the Ripper is not already on the system, download it from [http://www.openwall.com/john/](http://www.openwall.com/john/p).Save the [file holding the passwords](http://www-scf.usc.edu/~csci530l/downloads/crack-these-please.zip) to your disk. Its name is "crack-these-please.zip". Save it to disk and place it in the same folder as the john the ripper. Unzip it, to yield a file named "crack-these-please". This file contains passwords for 50 users, with names crack01 through crack50. The passwords are various, some chosen to be simple and easy and others complex and hard.

1. open cmd terminal
2. Open the john the ripper directory
3. Example:



**2. Executing a dictionary attack**

John the Ripper is a command line tool.

A dictionary attack uses a word database, and tries it repeatedly. John the Ripper has this capability. Enter dir and see that there is a file called password.lst. Dump the file's contents to the screen by giving the command:

**C:\<john\_directory\_name>\run>more  password.lst**

Press the spacebar, or hold it down, to make the display advance to the end of the file. You see that it is a list of potential passwords. There are about 3000 of them. You can order [a wordlist of 40 million](http://www.openwall.com/wordlists/). Enter the following command to launch a dictionary attack:

**C:\<john\_directory\_name>\run>john -w:password.lst  crack-these-please**

Note how many of the 50 passwords it was able to crack, what they are, and the time it took. John has created a list of solved passwords called john.pot. Dump to the screen by executing the command:

**C:\<john\_directory\_name>\run>more john.pot**

You see the same passwords you did before. But previously they were displayed along with the users who own them, now with their hashed versions. The hashed versions were the input to John's process; it is they that got cracked.

**3. Executing a hybrid attack**

A hybrid attack checks for variations of a word or a combination of dictionary words. Launch a hybrid attack by executing:

**C:\<john\_directory\_name>\run>john  -w:password.lst   -rules  crack-these-please**

Note the passwords it was able to crack and the time it took. How many more passwords did the hybrid attack crack?

**4. Executing a combination attack**

In default usage John the Ripper executes dictionary, hybrid, and bruteforce attacks in combination. Launch a combination attack by executing:

**C:\<john\_directory\_name>\run>john   crack-these-please**

**The assignment:**

1. While john is working, examine the CPU utilization of your computer. Screen capture the CPU usage using resource monitor. Let John run long enough to do some more cracking. Note the time it took and how many additional passwords it was able to crack. Also note what the passwords are. The "simpler" ones should have been cracked in the earlier attempts, and these should be "less simple."
2. How many of the cracked passwords could be found in the dictionary?
3. How about a foreign language dictionary?
4. How many of the cracked passwords contain varied combinations of letters, symbols, numerals, and case?
5. Do the cracked passwords tend to be long or short?

Getting all the passwords could take forever, so if it is taking too long, you can hit CTRL-C to stop the run.

1. When applied to the file crack-these-please, how many of its 50 passwords were cracked at each phase:

    a. dictionary attack solved \_\_\_\_\_\_\_\_\_\_ of the passwords

    b. hybrid attack solved \_\_\_\_\_\_\_\_\_\_ of the passwords

    c. combination attack solved \_\_\_\_\_\_\_\_\_\_ of the passwords

    d.  \_\_\_\_\_\_\_\_\_\_ of the passwords were never solved within the time spent

1. The password-holding file is /etc/shadow for linux. Where are passwords stored for Windows Systems?

Submission: A softcopy of your solutions to be submitted to author in individual lab 2.