**CPS3498 Computers Security**

**Lab 5: Password Cracking**

**Description:**

Access control and authentication are the first line of defense for today’s computer security, especially for networked computer systems. The most common mechanism implemented for such defense is a pair of user ID and password. This is usually referred as the One-Factor Authentication. The users, including the administrator(s), of the computer system must logon to the system using the valid user ID and password that are stored in the computer system

The user account information (ID and password) is usually stored in a password file. If an attacker can get the account information, especially with administrator privilege, the attacker will be able to access and even to modify the computer system. One way to get the account information is to crack the password file. There are two steps to password cracking. The attacker needs to firstly access to the hash of the password that is stored on the computer. The second step is actually crack the password.

Although the cracking program does not know how to reverse the hash back to password, it does know the algorithm to create a hash from a password. Therefore, it can process any combination of characters and generate its hash, and then compares the captured hash with the one it generates. It the hashes match, then it has found the password. One popular way to generate hashes and search for passwords is with dictionary attack with a dictionary file. Another method of attack is a hybrid attack that uses other techniques in conjunction with a dictionary attack. Brute-force attack tries every possible combination of characters that may take days even months.

This lab uses tool called John the Ripper to crack passwords from a provided hash file. John the Ripper is a command line tool that does not run on Windows. You need to use the Command Prompt and change to proper directory to run the tool.

**Procedure:**

1. Long on to a PC with the administrator account, or an account that has administrator privilege.
2. Go to <http://www.openwall.com/john/>. Download John the Ripper **John179** and save it on your MS Windows, Mac, or other computer OS.
3. Extract john179w.zip that you downloaded to your C:\ drive. This should create a directory **john179** andtwo subdirectory **doc** and **run** in Windows PC. For Mac, it will create an additional subdirectory **src**.
4. Save the two password files: **passwd.des** and **passwd.md5** into c:\john179\run. For Mac, save them into ~/desktop/John179/run. You should also see a password list file password.lst that comes with John the Ripper in the same directory.
5. Start command prompt. At the command prompt, type **cd\** (For Mac**, cd ~/desktop**)to change your current directory to c:\. Type dir (For Mac, type **ls -al**) to see all of the directories of your c:\. Can you find the directory john179?
6. Type **cd john179\run** (For Mac, **cd ~/desktop/John179/run**) to change directory to where you can run John the Ripper.
   1. Type **dir pass\*.\*** (For Mac, **ls -pass\*.\***), how many password files do you see?
   2. Type **dir**, how many files do you see?
7. Type **john passwd.des** (For Mac, **./john passwd.des**). The tool will start to crack the password from the hash file passwd.des. How many passwords have the tool cracked for you? What is the account information (ID/password)? The cracking may take a while. If you want, you may stop the tool after running 30 mins by press Ctrl-C (Control C) at the Command Prompt.
8. Type **dir**, how many files do you see?
   1. Comparing with 6b, what are the files generated by running John the Ripper?
   2. Delete those files generated by John the Ripper.
9. Type **john passwd.md5**. The tool will start to crack the password from the hash file passwd.md5. How many passwords have the tool cracked for you? What is the account information (ID/password)? The cracking may take a while. If you want, you may stop the tool after running 30 mins by press Ctrl-C (Control C) at the Command Prompt.
10. Delete those files generated by John the Ripper.
11. Type **john –wordlist=password.lst –rules passwd.md5**. The tool will start to crack the password using a dictionary file password.lst from the hash file passwd.md5. How many passwords have the tool cracked for you? What is the account information (ID/password)? The cracking may take a while. If you want, you may stop the tool after running 30 mins by press Ctrl-C (Control C) at the Command Prompt.
12. Password cracking for PC: For PC users, the Ophcrack Windows password cracker is an open source (GPL license) program; it cracks Windows LM hashes using rainbow tables. It can be used for Windows password recovery. Search the Internet or download Ophcrack from <http://ophcrack.sourceforge.net/> to a CD or USB. For Mac OS, download DaveGrohl from <https://github.com/octomagon/davegrohl> and follow instructions (another reference at <http://www.hackmac.org/tutorials/crack-os-x-mountain-lion-passwords/>). Then reboot your PC from the tool to crack your own local password. NOTE : It is illegal cracking password from PC without owner’s consent.

**Notes and Suggestions:**

* Different computers may have different operating systems and hardware configurations. If you use your own computer for this lab, the above procedure may not be completely applicable. For example, you cannot follow the same procedure for MAC computer.
* Make sure that the computer is back to its original condition. Do not leave a computer in a non-functioning condition.

**Lab report:**

* Your report should include all information required to be noted in the procedure, any problems/issues you encountered during the lab and how did you resolve them.