Lab Exercise 1 – Introduction to Password Cracking

Objectives

In this lab exercise you will complete the following tasks:

- Learn the fundamentals of password storing, encrypting and cracking.
- Use a commercial password auditor to crack a password protected MS Office file.
- Use the professional security tool LC4 to crack as many passwords in a captured SAM file as you can.

Visual Objective

Introduction

Password cracking is a term used to describe the penetration of a network, system, or resource with or without the use of tools to unlock a resource that has been secured with a password. Password cracking tools may seem like powerful decryptors, but in reality are little more than fast, sophisticated guessing machines.

Types of password breaking

- **Dictionary attack**

A simple *dictionary* attack is usually the fastest way to break into a machine. A dictionary file (a text file full of dictionary words) is loaded into a cracking application, which is run against user accounts located by the application.

- **Brute force attack**

A *brute force* attack is a very powerful form of attack, though it may often take a long time to work depending on the complexity of the password. The program will begin trying any and every combination of numbers and letters and running them against the hashed passwords. Passwords that are composed of random letters numbers and characters are most vulnerable to this type of attack.

- **Hybrid attack**

Another well-known form of attack is the *hybrid* attack. A hybrid attack will add numbers or symbols to the search words to successfully crack a password. Many people change their passwords by simply adding a number to the end of their current password. Therefore, this type of attack is the most versatile, while it takes longer then a standard dictionary attack it does not take as long as a brute force attack.

Cracking Process

Since a brute force attack is the most time consuming and is not likely to break any passwords that are not composed of random characters, the best plan is to use techniques that are computationally efficient compared to untargeted and unspecific techniques. By applying what is known about how users select passwords, an intruder can tremendously increase the odds in their favor of finding passwords. With the right techniques, some poor passwords can be cracked in under a second.

The real power of dictionary attacks come from understanding the ways in which most people vary names and dictionary words when attempting to create a password. By applying all the common transformations to every word in the electronic list and encrypting each result the number tested passwords multiplies rapidly. Cracking tools can often detect "clever" ways of manipulating words to hide their origin. For example, such cracking programs often subject each word to a list of rules. A *rule* could be anything, any manner in which a word might appear. Typical rules might include

- Alternate upper- and lowercase lettering.
- Spell the word forward and then backward, and then fuse the two results (for example: cannac).
- Add the number 1 to the beginning and/or end of each word.

Naturally, the more rules one applies to the words, the longer the cracking process takes. However, more rules also guarantee a higher likelihood of success.

Task 1 – Microsoft Office Password Recovery

Many applications require you to establish an ID and password that may be saved and automatically substituted for future authentication. The password will usually appear on the screen as a series of asterisks. This is fine as long as your system remembers the password for you but what if it "forgets" or you need it for use on another system. Fortunately, many utilities have been written to recover such passwords. In this task, you will use OfficeKey to recover the password for a MS word document.

Step 1: Find the folder "Lab1" on your desktop, and open it.
You will find OfficeKey and a MS document in the folder.

Step 2: Open the Office Key – Password Recovery tool

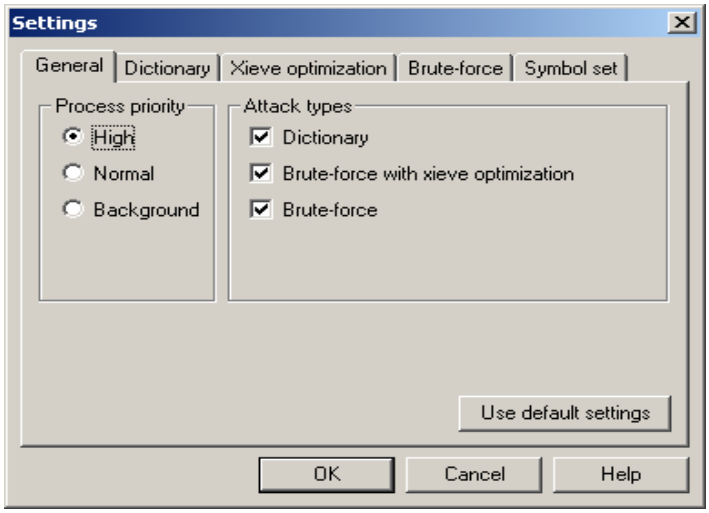
Step 3: Press the "Recover" button in the upper left corner, or select File → Recover

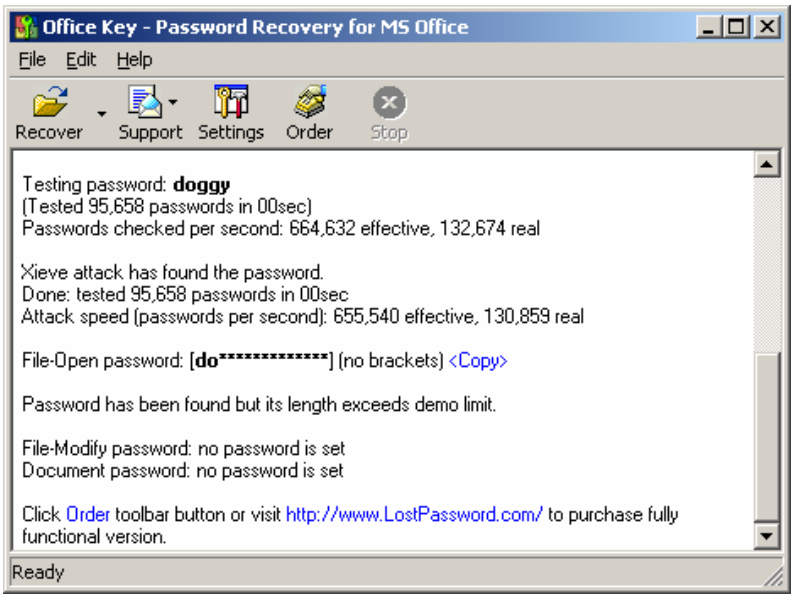
Step 4: Choose the password protected MS Office File you have saved to the Desktop.

Step 5: After running the first password auditing session, check to see if Office key has cracked the password. If the password has not been cracked press the Settings button on the upper tool bar.

Step 6: Once in the Settings menu you will be able to modify the search parameters and customize a more targeted search.

(Note: only the first two letters of the password will be displayed in the demo version. Scroll up and you should be able to see the last password tried.)





Step 7: Repeat steps 3 and 4 until the password has been cracked and opens the MS Office File.

Step 8: Write down the contents of the MS word document and the password into your lab report and submit it to your TA.

Task 2 – Password Auditing (Windows platform):

The purpose of this task is to familiarize you with act of password cracking/recovery. Password cracking software uses a variety of approaches, including intelligent guessing, dictionary attacks and automation that tries every possible combination of characters. Given enough time the automated method can crack any password, but more effective passwords will last months before breaking.

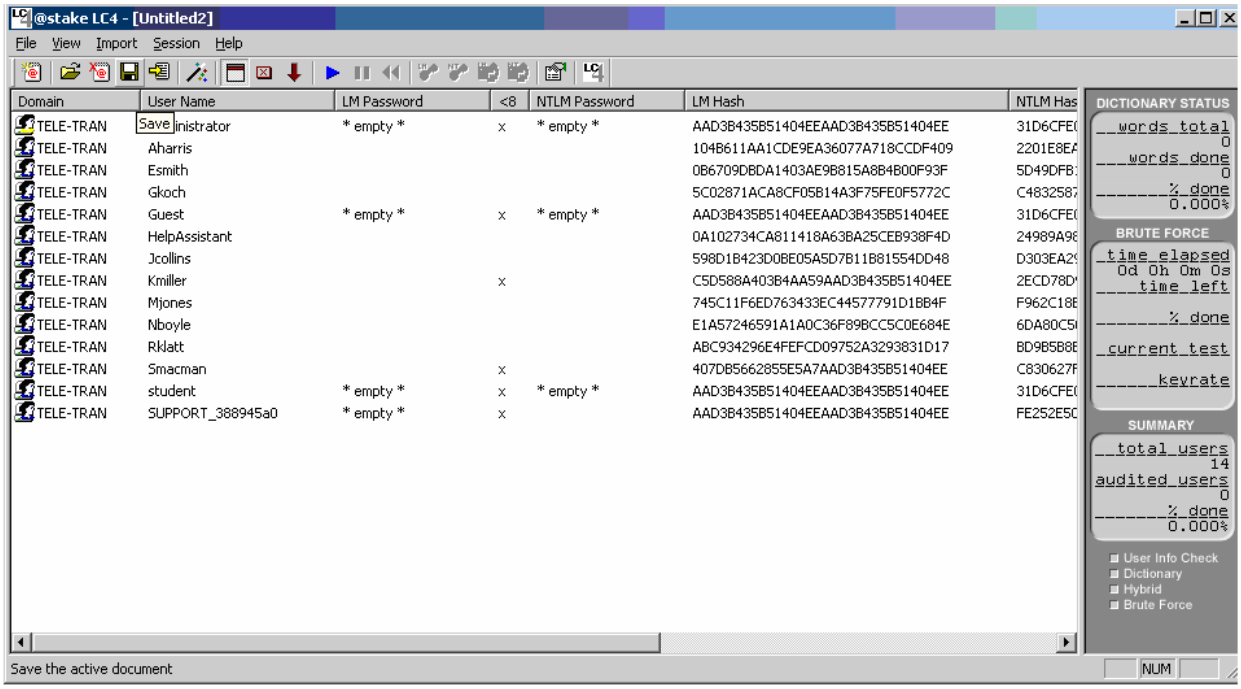
When a password is entered and saved on a computer it is encrypted, the encrypted password becomes a string of characters called a "hash" and is saved to a password file. A password cannot be reverse-decrypted. So a cracking program encrypts words and characters given to it (wordlist or randomly generated strings of characters) and compares the results with hashed passwords. If the hashes match then the password has successfully been guessed or "cracked". This process is usually performed offline against a captured password file so that being locked out of the account is not an issue, and guessing can go on continuously. Thus, revealing the passwords is simply a mater of CPU time and dictionary size

1. You obtain a *dictionary file*, which is no more than a flat file (plain text) list of words (commonly referred to as *wordlists*).

2. These words are fed through any number of programs that encrypt each word. Such encryption conforms to the DES standard.

3. Each resulting encrypted word is compared with the target password. If a match occurs, there is better than a 90 percent chance that the password was cracked.

Step 1: Go to Lab1 folder, and open LC4 to audit the passwords on your Windows system.
Select File → New Session
Select Import → Import from PWDUMP File (in the same folder)
Select the "Passwords" file that has been provided to you.



Note: The Windows password database is called the SAM. This Windows SAM password file was captured from a system running XP. In Windows XP, the SAM is SYSKEYED for additional security.

Objectives

This password file has been retrieved from a system that we must gain access to. To do this you must crack as many passwords as possible as quickly as possible. We have captured the user names and encrypted passwords for ten users. The user names follow a standard pattern of first initial and last name, but the passwords have no set standards. We do know that users of this system are encouraged to add numbers and other characters to the words they chose for passwords.

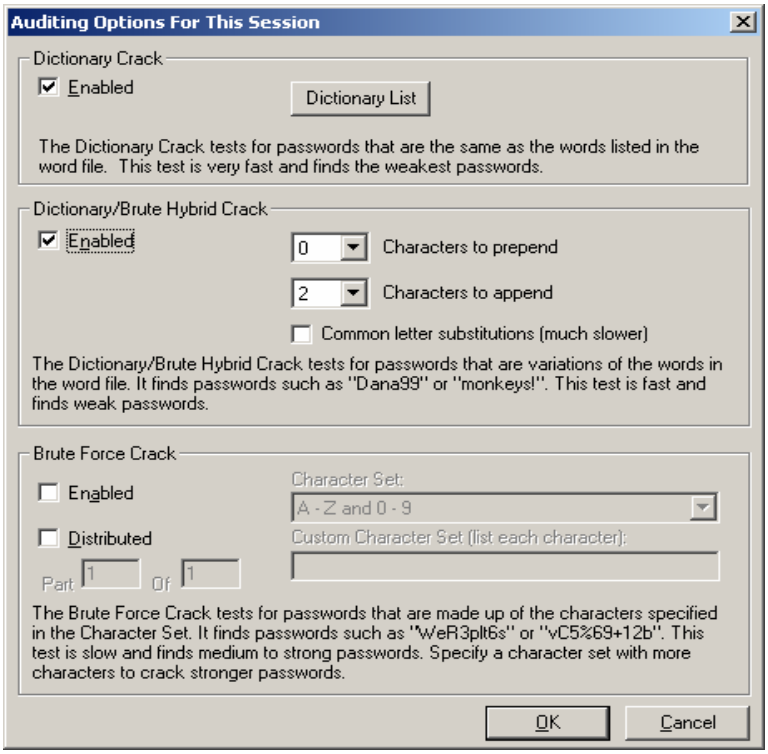
To aid you in cracking these passwords we have managed to collect some basic information about the users. This personal information may help you target your searches as to what the user's password may be.

Kmiller	Ken Miller is an avid fly fisher and his record number of catches is just under 30
Smacman	Steven MacMan has a fiancé who's name is 4 letters long and starts with a "K"
Gkoch	Gina Koch grew up with her German grandmother, who used to call her 'Little Precious' *
Mjones	Matt Jones was born in 1979. He compares himself to a Shakespearean character who was born via C section
Tgriffin	Tim Griffin loves funky '70's and '80s music. And songs about 'Love'
Rklatt	Ryan Klatt is a big Star Trek fan and has most likely chosen an obscure reference for his password *
Nboyle	Nancy Boyle is an a fan of the books of British writer Douglas Adams
Esmith	Edward Smith was very close to his grandfather who died in 1968. We know his grandfather's name was a less common name starting with 'L'
Jcollins	Jim Collins keeps a copy of the book "The Prince" *
Hharris	Alan Harris has a wife named Sue and a daughter named Megan Alan was married on May 3rd. His daughter was born on August 6th

- **May require additional compiled word lists, create your own or download online.**

Step 2: Select Session → Session Options

Use this menu to customize your password search. Here you can add different word list for Dictionary attacks, change Hybrid attack features. Keep in mind you are working with a short dead line and more in depth searches will take longer then you have. You must use the information given to you to target your search most specifically at more likely passwords.



Step 3: Select Session → Begin "Audit" or Press the blue play button on the upper toolbar to start the password search.

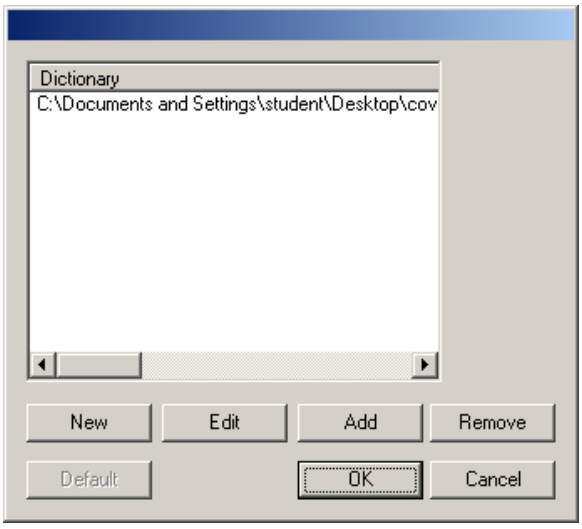
Step 4: After the first search has run check your progress. Have some of the passwords been cracked all the way though or have some only been partially cracked. Use what you've learned from this first search to target your next few searches. You will need to search the internet and use the information you have been given about each user to find words they may have used as their password.

Note: The question marks in the partially cracked passwords do not necessarily represent the number of remaining undiscovered characters.

Step 5: Add words to your wordlist
Session → Session Options
Press the 'Dictionary List' button in the Dictionary crack section. Here you can edit your current word list and add words by selecting the 'EDIT' button and entering each word on a new line. You can also add multiple dictionaries and wordlist.

Step 6: You may chose to conduct dictionary attacks with other wordlists. You can find additional wordlist to use here: ftp://ftp.cerias.purdue.edu/pub/dict

Note: To use a new word list in a search, first download the file to your desktop (you can download additional dic files from Internet). Then select Session → Session Options and press the 'Dictionary List' button in the Dictionary crack section. Press the 'ADD' button and select the new wordlist you have downloaded.



Step 7: Continue searching for possible passwords during the remainder of the lab. Repeating steps 3 and 4 each time you modify your search.

Step 8: Once you have cracked all the passwords in the file, write them down in your lab report or once the lab time has ended, submit the passwords you were able to crack.

Report to deliver:

The group report is to show what you did in the project. Please clearly state your results of this project. You are expected to hand in a report in the following formats:

- A cover page (including project title) with group name and group members
- A table of contents with page numbers
- Using double-spaced typing for convenient grading
- Hard copies only, Font size 12, Single column
- A bound or stapled document, with numbered pages

The report should have the following sections. Each section has multiple items. You need to write a report section by section that covers all required items. But you do not have to write the report item by item. Take screenshots if it is necessary.

Section I: Introduction:

You should have the following parts:

- Describe the goal and motivation of this project. In addition to what has been stated in the project instruction, please tell your own expectation in this project.
- Give an outline of this report, in which the content of each section needs to be briefly described.

Section II: Task 1

You should have the following parts:

- Briefly describe the functionality of OfficeKey.
- Briefly describe the strategy you used to find the password (like what attacks you used).

- The password and the contents of the MS word document

Section III: Task 2
You should have the following parts:
- Briefly describe the functionality of LC4.
- Describe the strategy you used to find each password (like what attacks, dics you used).
- List the passwords you have gotten.

Section IV: Questions
You should answer the following questions related to this project:
- What does SYSKEYED mean?
- Search the internet to find a program that could have been used to decrypt the SAM file and save it as a PWDUMP file for LC4 to crack. What is the name of the program you found and what does it do?
- If you weren't the administrator, how could you retrieve a copy of the SAM file? You'll have to do some reading/exploring to find out (hint: One way involves checking to see if the system has been secured after the backup process).
- Explain the differences between brute force, dictionary, and hybrid modes and what the relative advantages/disadvantages of each are?

Section IV: Experiment Log
This part should describe your activities in this project.
- Clearly state the responsibility of each group member. If possible, give a table to tell who did which task, who collected information of which device, who wrote which part of the report, who coordinated the group work activities, etc.
- Give a log of your group activity, such as what you did on which day, and how many people attend.

Grading Rubric

This project has a number of specific requirements. The requirement for each section is documented in the above project instruction "Report to deliver". Whether you will get credits depends on the following situations:
- You will get full credits on one item, if it is correctly reported as required and well written.
- You will get half credits on one item, if it is reported as required but there is something definitely wrong.
- You will not get any credit for one item, if it is not reported.

The credits for each section are in the following. Each item in one section has equal credits.
1. Section I: Introduction (5%):
Each item has 2.5 credits.
2. Section II: Task 1(10%):
Password and document content have 5 credits, other items have 5 credits.
3. Section III: Task 2 (55%):
Each password has 5 credits, other items have 5 credits.
4. Section IV: Questions (20%)
Each question has 5 credits.
5. Section IV: Experiment log (10%)

- If you are responsible for some parts of your group work, you get 10 credits. If you do nothing for your group work, you get 0.
- If you attend more than 90% of your group activities, you get 10 credits. If you attend between 70% and 90%, you get 7 credits. If you attend between 50% and 70%, you get 5. Otherwise, you get 0.

Note

This is a group project. Only hard copies of the report will be accepted. Be sure to include the names of all the teammates and email addresses in the report. The report should be turned in before class on the specified due date. Late grade will be deducted in case the submission is not made on time and prior permission is not obtained from the Dr Liu for submitting later than the specified due date.