



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE



Internet Security (IS)

Lab – Cracking Windows 7 Passwords
Using Dictionary Attack

Faculty of Architecture, Computing & Engineering
School of Applied Computing
Mount Pleasant Campus
Swansea
SA1 6ED

Cracking Windows 7 Passwords Using Dictionary Attack

Information is a valuable resource. It needs to be accessed and shared with legitimate people. Towards that end, access to information is usually protected via the use of authentication systems. **Password cracking is the process of attempting to gain un-authorized access to restricted systems using common passwords or algorithms that guess passwords.**

In this article, we will introduce you to the common password cracking techniques and the counter measures you can implement to protect systems against such attacks.

Topics covered in this tutorial

- What is password cracking?
- What is password strength?
- Password cracking techniques
- Password Cracking Tools
- Password Cracking Counter Measures
- Hacking Assignment: Hack Now!

What is password cracking?

Password cracking is the art of obtaining the correct password that gives access to a system protected by an authentication method. Password cracking employs a number of techniques to achieve its goals. The cracking process can involve either comparing stored passwords against word list or using algorithms to generate passwords that match.



Figure 1: Definition of password cracking.

What is password strength?

Password strength is the measure of a password's efficiency to resist password cracking attacks. The strength of a password is determined by the following factors:

- **Length:** the number of characters the password contains.
- **Complexity:** does it use a combination of letters, numbers and symbols?
- **Unpredictability:** is it something that can be guessed easily by an attacker?

Let's now look at a practical example. We will use four passwords examples as follows:

1. *password*
2. *password1*
3. *#password1\$*
4. *#p&55w0rd1\$*

Using an online resource called Password Meter (<http://www.passwordmeter.com/>), we will try to test the strengths of the above four passwords as shown below:

Test Your Password		Minimum Requirements
Password:	password	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	8%	
Complexity:	Very Weak	

Figure 2: Strength of password “password”.

Test Your Password		Minimum Requirements
Password:	password1	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	26%	
Complexity:	Weak	

Figure 3: Password “password1”.

Note from Figures 1 – 4, as the password complexity increases, the strength of the password also increases. The stronger the password, the more difficult it becomes to crack.

Test Your Password		Minimum Requirements
Password:	#password1\$	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	66%	
Complexity:	Strong	

Figure 4: Strength of Password “#password1\$”

Test Your Password		Minimum Requirements
Password:	#p&55w0rd1\$	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Figure 5: Strength of Password “#p&55w0rd1\$”

Password cracking techniques

There are a number of **techniques that can be used to crack passwords**. We will describe the most commonly used ones below;

- **Dictionary attack**– This method involves the use of a wordlist to compare against user passwords. This is the method you will be using in this laboratory exercise.
- **Brute force attack**– This method is similar to the dictionary attack. Brute force attacks use algorithms that combine alpha-numeric characters and symbols to come up with passwords for the attack. For example, a password of the value “password” can also be tried as p@\$word using the brute force attack.
- **Rainbow table attack**– This method uses pre-computed hashes. Let’s assume that we have database which stores passwords as md5 hashes. We can create another database that has md5 hashes of commonly used passwords. We can then compare the password hash we have against the stored hashes in the database. If a match is found then we have the password.
- **Guess**– As the name suggests, this method involves guessing. Passwords such as qwerty, password, admin etc. are commonly used or set as default passwords. If they have not been changed or if the user is careless when selecting passwords, then they can be easily compromised.
- **Spidering**– Most organizations use passwords that contain company information. This information can be found on company websites, social media such as facebook, twitter

etc. Spidering gathers information from these sources to come up with word lists. The word list is then used to perform dictionary and brute force attacks.

Password Cracking Tools

These are software programs that are used to crack user passwords. We already looked at a similar tool in the above example on password strengths. The website www.md5this.com uses a rainbow table to crack passwords. We will now look at some of the commonly used tools

1. John the Ripper

John the Ripper uses the command prompt to crack passwords. This makes it suitable for advanced users who are comfortable working with commands. It uses a wordlist to crack passwords. The program is free but the word list has to be bought. It has free alternative wordlists that you can use. Visit the product website <http://www.openwall.com/john/> for more information and how to use it.

2. Cain & Abel

Cain & Abel runs on windows. It is used to recover passwords for user accounts, recovery of Microsoft Access passwords; networking sniffing etc. Unlike John the ripper, Cain & Abel uses a graphic user interface. It is very common among newbies and script kiddies because of its simplicity of use. Visit the product website <http://www.oxid.it/cain.html> for more information and how to use it.

3. Ophcrack

Ophcrack is a cross platform windows password cracker that uses rainbow tables to crack passwords. It runs on windows, Linux and Mac OS. It also has a module for brute force attacks among other features. Visit the product website <http://ophcrack.sourceforge.net/> for more information and how to use it.

Password Cracking Counter Measures

- An organization can use the following methods to reduce the chances of the passwords been cracked
- Avoid short and easily predictable passwords
- Avoid using passwords with predictable patterns such as 11552266.
- Passwords stored in the database must always be encrypted. For md5 encryptions, its better to salt the password hashes before storing them. Salting involves adding some word to the provided password before creating the hash.
- Most registration system have password strength indicators, organizations must adopt policies that favor high password strength numbers.

Hacking Activity: Cracking Windows7 Passwords

In this practical scenario, we are going to **crack a windows account with a simple password**. **Windows uses NTLM hashes to encrypt passwords**. We will use the NTLM cracker tool in Cain and Abel to do that.

Cain and Abel cracker can be used to crack passwords using;

- Dictionary attack
- Brute force
- Cryptanalysis

We will use the dictionary attack in this example. Your Module Tutor or lab assistant will provide you with a dictionary list of over 2 million passwords.

For this demonstration, we have created an account called Accounts with the password qwerty on windows 7. Your Module Tutor would have created one or two accounts in your lab machine. It is the passwords for these accounts that you will be harvesting using Cain and Abel.



Figure 6: Test Account.

Password cracking steps

- Remove any DVD from you machine and login to the computer from Windows 7 Operating System (NOT Linux).
- Open the **Cain and Abel application and** you will get the following main screen.

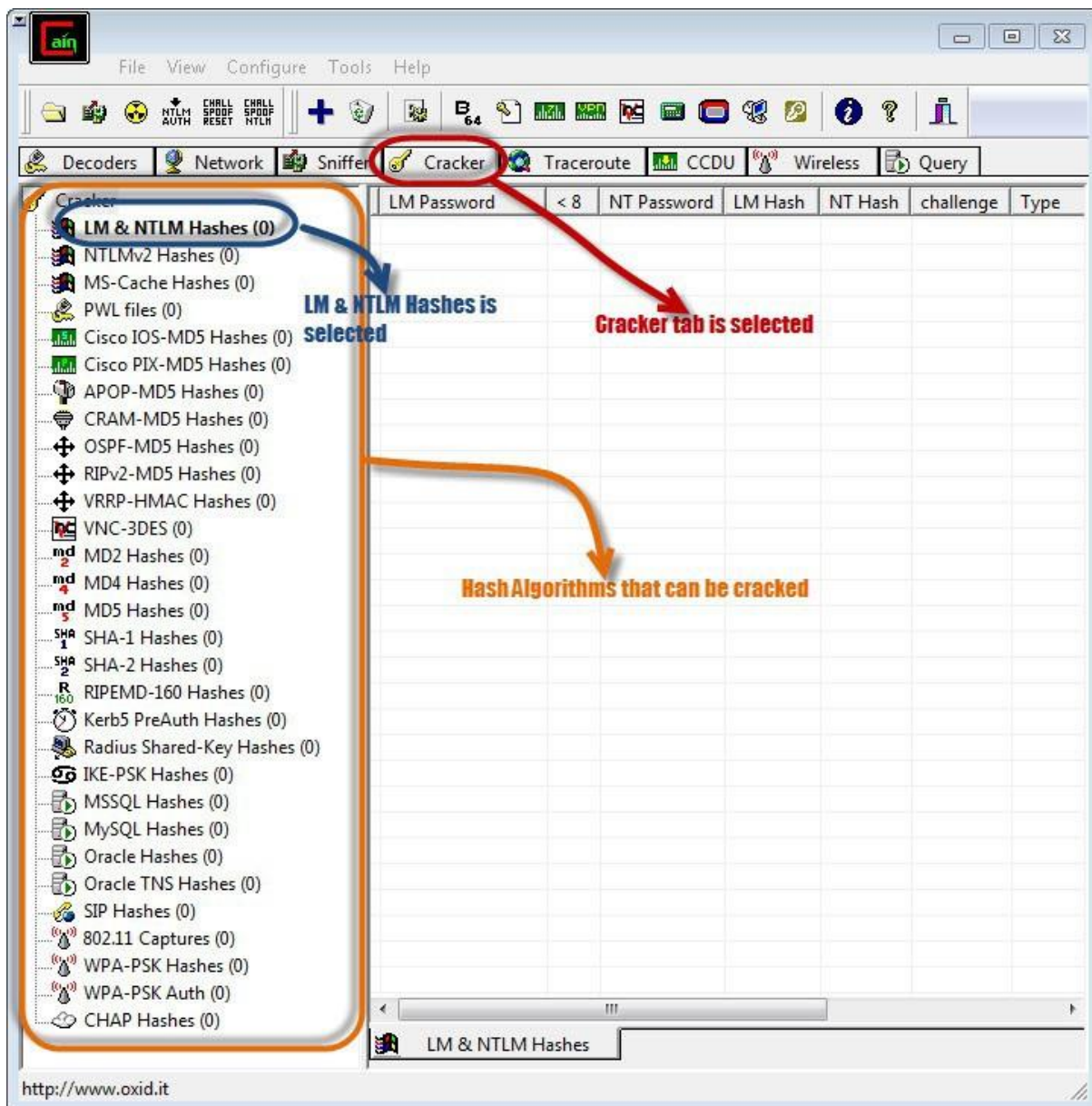


Figure 7: Cain and Abel main Application.

- Make sure the cracker tab is selected as shown above
- Click on the add button on the toolbar.

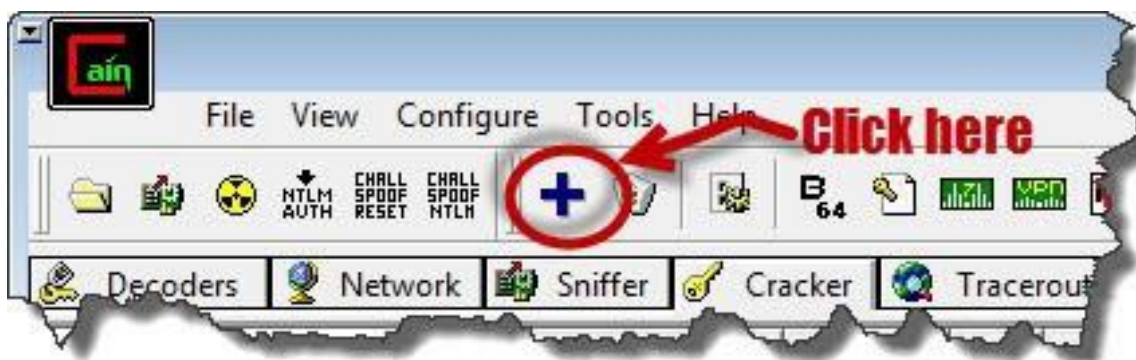


Figure 8: Clicking the “Add” button.

- The following dialog window will appear



Figure 9: Importing Local Users.

- The local user accounts will be displayed as follows. Note the results shown will be of the user accounts on your local machine.

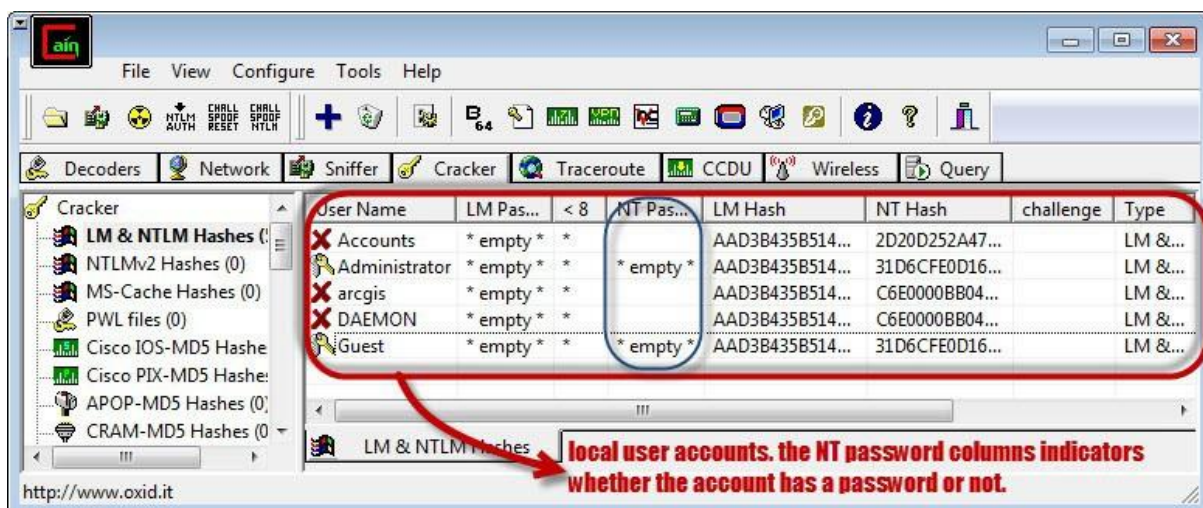


Figure 10: List of Local User Accounts.

- Right click on the account you want to crack. For this tutorial, we will use Accounts as the user account. Chose one of the accounts created by your Module Leader or lab assistant.

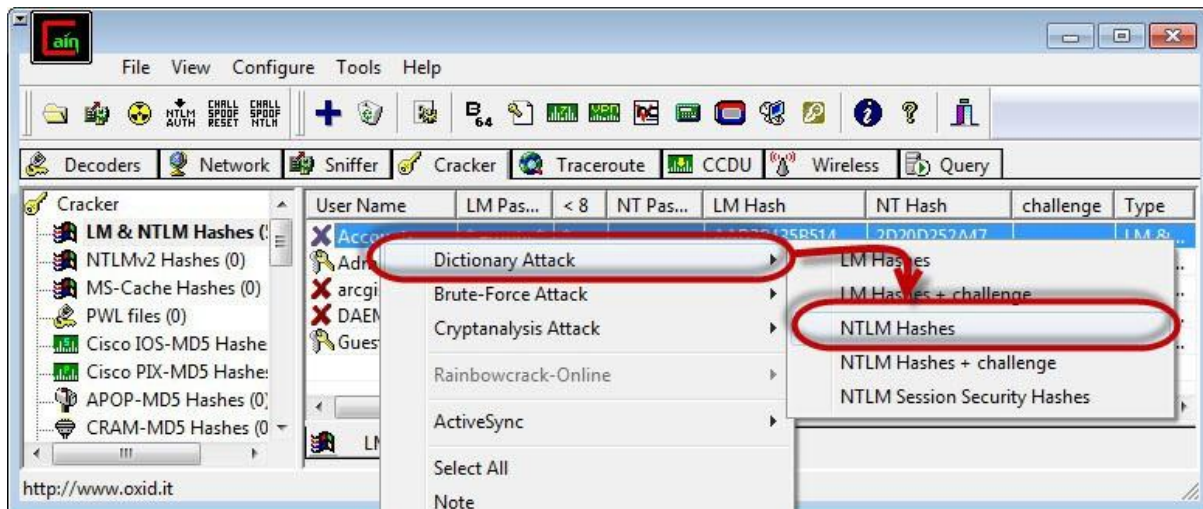


Figure 11: Selecting NTLM Hashes.

- The following screen will appear.

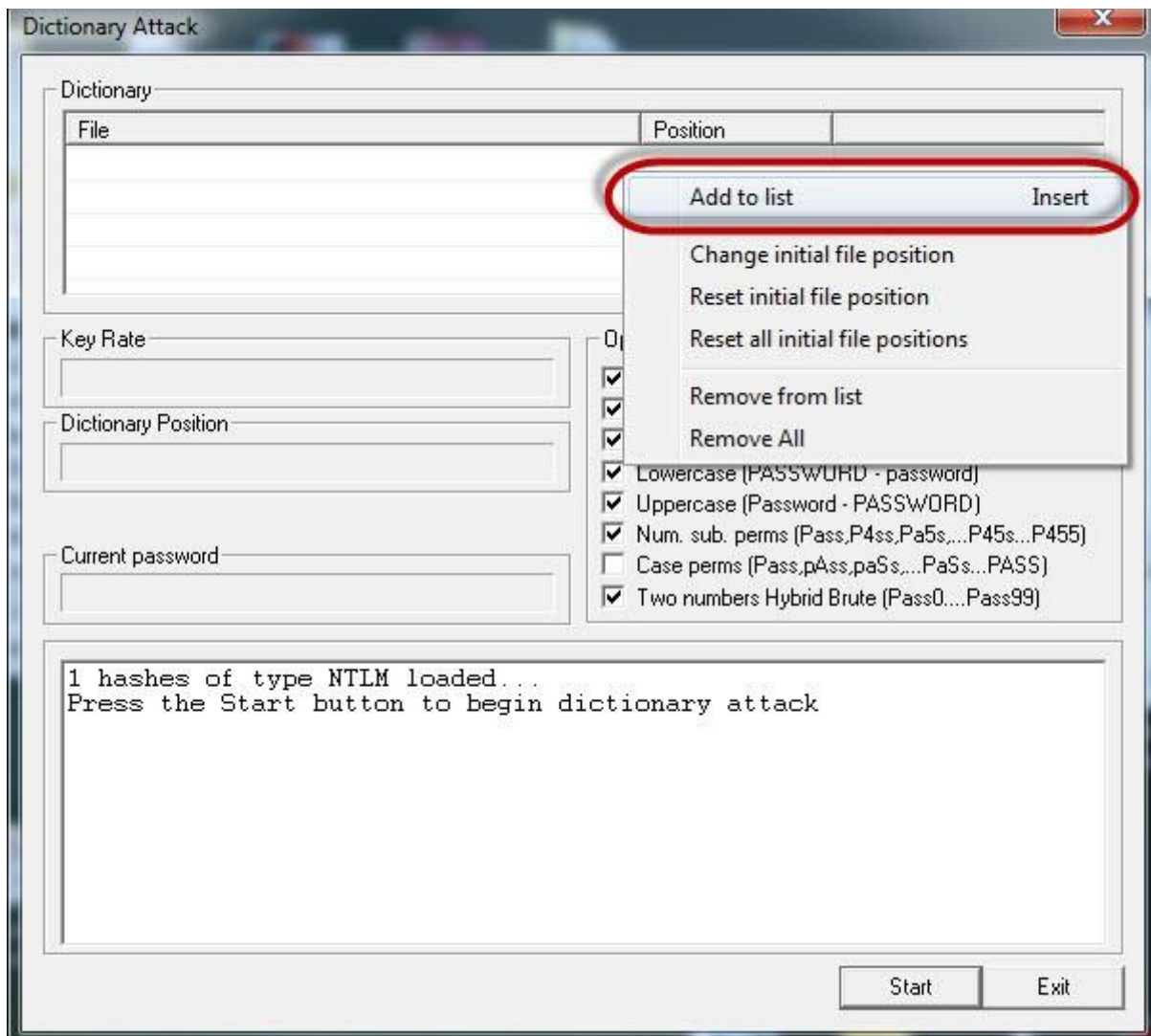


Figure 12: Inserting the Dictionary File (Passwords List.txt).

- Right click on the dictionary section and select Add to list menu as shown above
- Browse your computer and select the “Passwords List.txt” file given to you by your Module Leader or lab assistant.

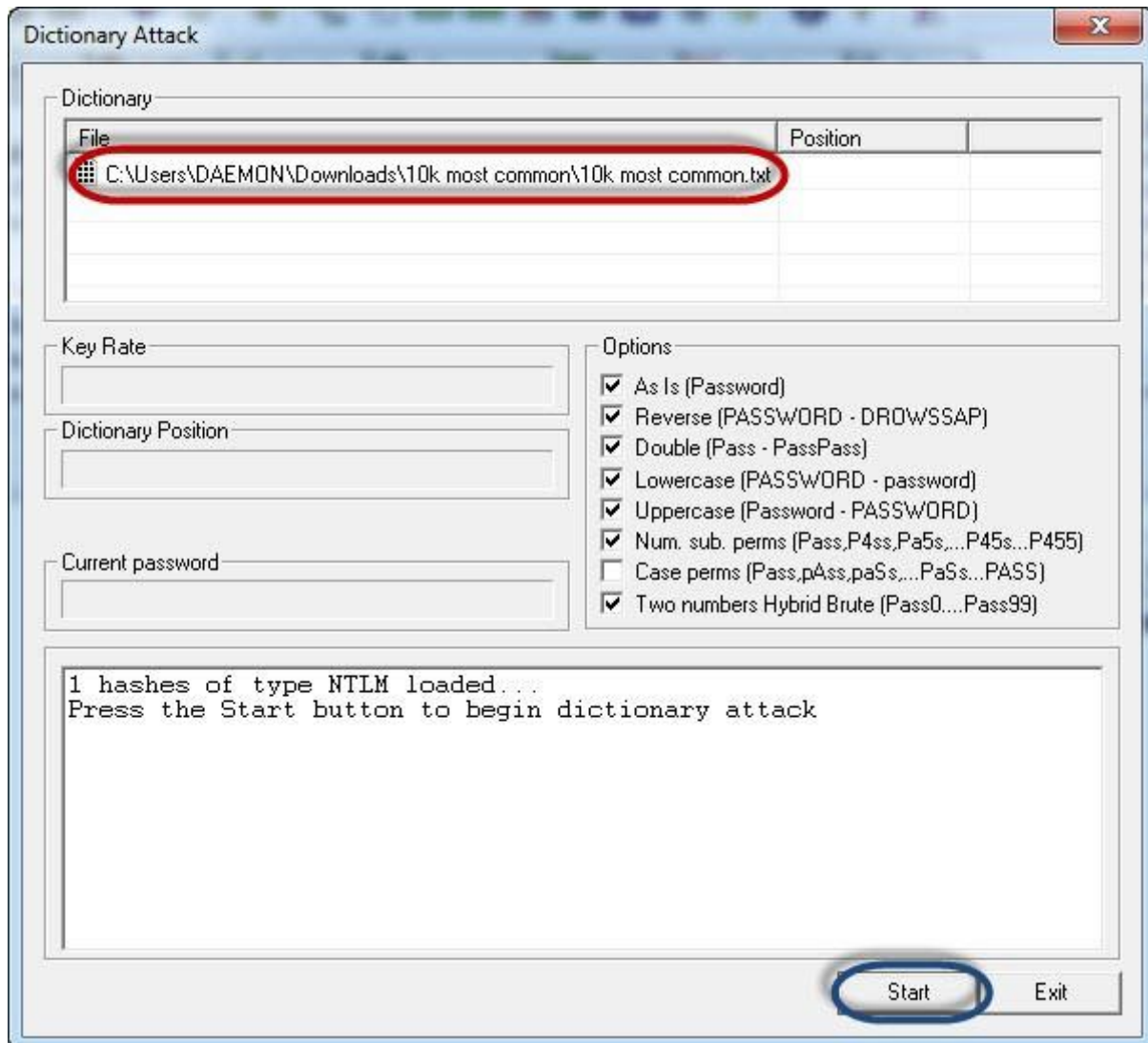


Figure 13: Inserting the Dictionary File (Passwords List.txt).

- Click on start button.
- If the user used a simple password like qwerty, then you should be able to get the following results.

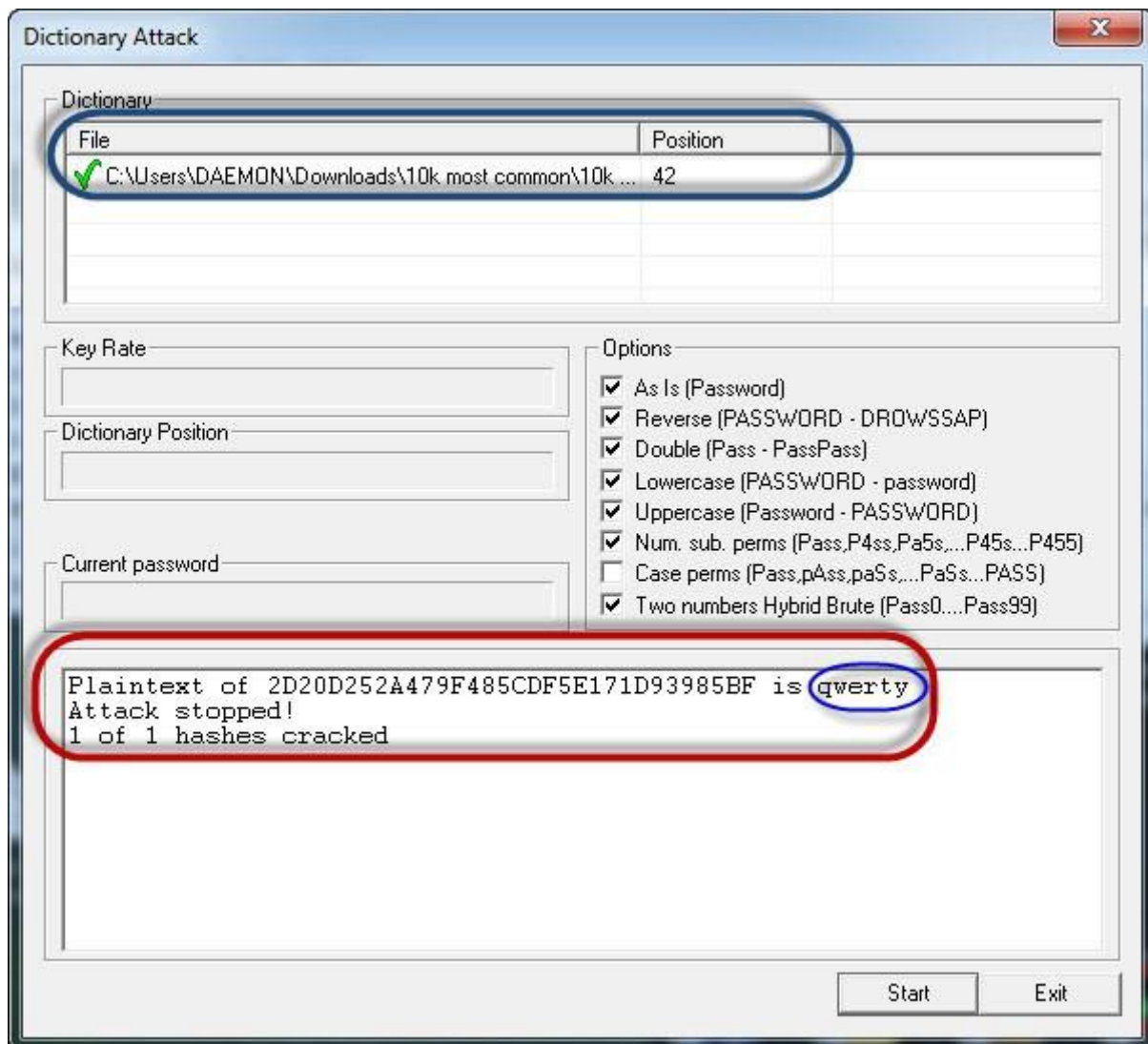


Figure 14: Windows7 password cracked.

Note: the time taken to crack the password depends on the password strength, password complexity, memory, and the processing power of your computer.

- If the password is not cracked using dictionary attack, you can try brute force or cryptanalysis attacks.

Summary

- Password cracking is the art of recovering stored or transmitted passwords.
- Password strength is determined by the length, complexity and unpredictability of a password value.
- Common password techniques include dictionary attacks, brute force, rainbow tables, spidering and cracking.
- Password cracking tools simplify the process of cracking passwords.

Credit: This Hacking Lab Exercise was adapted from Guru 99.