Password Cracking

For lab 8 you will examine password cracking.

**Password strength is the measure of a password’s efficiency to resist password cracking attacks**. The strength of a password is determined by;

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

Let’s now look at a practical example. We will use three passwords namely

*1. password*

*2. password1*

*3. #password1$*

For this example, we will use the password strength indicator of Cpanel when creating passwords. The images below show the password strengths of each of the above-listed passwords.

<https://cpanel.net/>

This is a trial service and will work for you to look at the passwords.

The higher the strength number, better the password.

Let’s suppose that we have to store our above passwords using md5 encryption.

We will use an online [md5 hash generator](https://www.md5hashgenerator.com/) to convert our passwords into md5 hashes. Link here <https://www.md5hashgenerator.com/>

The table below shows the password hashes.

|  |  |  |
| --- | --- | --- |
| **Password** | **MD5 Hash** | **Cpanel Strength Indicator** |
| password | 5f4dcc3b5aa765d61d8327deb882cf99 | 1 |
| password1 | 7c6a180b36896a0a8c02787eeafb0e4c | 28 |
| #password1$ | 29e08fb7103c327d68327f23d8d9256c | 60 |

We will now use <http://www.md5this.com/> to crack the above hashes. The images below show the password cracking results for the above passwords.

<https://www.guru99.com/images/EthicalHacking/Password_cracking1.png>

<https://www.guru99.com/images/EthicalHacking/Password_cracking2.png>

<https://www.guru99.com/images/EthicalHacking/Password_cracking3.png>

As you can see from the above results, we managed to crack the first and second passwords that had lower strength numbers. We didn’t manage to crack the third password which was longer, complex and unpredictable. It had a higher strength number.

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.
* **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 a 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.

***Spidering sample dictionary attack wordlist***

1976 <founder birth year>

smith jones <founder name>

acme <company name/initials>

built|to|last <words in company vision/mission>

golfing|chess|soccer <founders hobbies  
  
Examine the available software for Kali Linux.

**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 to wordlist to crack passwords. The program is free, but the word list has to be bought. It has free alternative word lists that you can use. Visit the product website <https://www.openwall.com/john/> for more information and how to use it.

**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.softpedia.com/get/Security/Decrypting-Decoding/Cain-and-Abel.shtml> for more information and how to use it.

**Ophcrack**

Ophcrack is a cross-platform Windows password cracker that uses rainbow tables to crack passwords. It runs on Windows,[Linux](https://www.guru99.com/unix-linux-tutorial.html)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.

In this practical scenario, we are going to **crack 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. You will need to download the dictionary attack wordlist here [10k-Most-Common.zip](https://goo.gl/W46b80).

For your exercise, create a few accounts on both Linux and Windows VMs. Using the most common passwords, use Cane and Abel to attempts cracks on the passwords of varying size and difficulty. Also, think about changing the common passwords to see the difference in time. Record your finding