Practical No. 8

Aim : Study and demonstrate system hacking and write a report.

a. How to crack a password?

b. How to use Ophcrack to Crack Passwords

Theory :

What is password cracking?

Password cracking is the process of using an application program to identify an unknown or forgotten password to a computer or network resource. It can also be used to help a threat actor obtain unauthorized access to resources.

With the information malicious actors gain using password cracking, they can undertake a range of criminal activities. Those include stealing banking credentials or using the information for identity theft and fraud.

A password cracker recovers passwords using various techniques. The process can involve comparing a list of words to guess passwords or the use of an algorithm to repeatedly guess the password.

What does a password cracking attack look like?

The general process a password cracker follows involves these four steps:

Steal a password via some nefarious means. That password has likely been encrypted before being stored using a hash Hashes are mathematical functions that change arbitrary-length inputs into an encrypted fixed-length output.

Choose a cracking methodology, such as a brute-force or dictionary attack, and select a cracking tool.

Prepare the password hashes for the cracking program. This is done by providing an input to the hash function to create a hash that can be authenticated.

Run the cracking tool.

A password cracker may also be able to identify encrypted passwords. After retrieving the password from the computer's memory, the program may be able to decrypt it. Or, by using the same algorithm as the system program, the password cracker creates an encrypted version of the password that matches the original.

What are password cracking techniques?

Password crackers use two primary methods to identify correct passwords: brute-force and dictionary attacks. However, there are plenty of other password cracking methods, including the following:

Brute force. This attack runs through combinations of characters of a predetermined length until it finds the combination that matches the password.

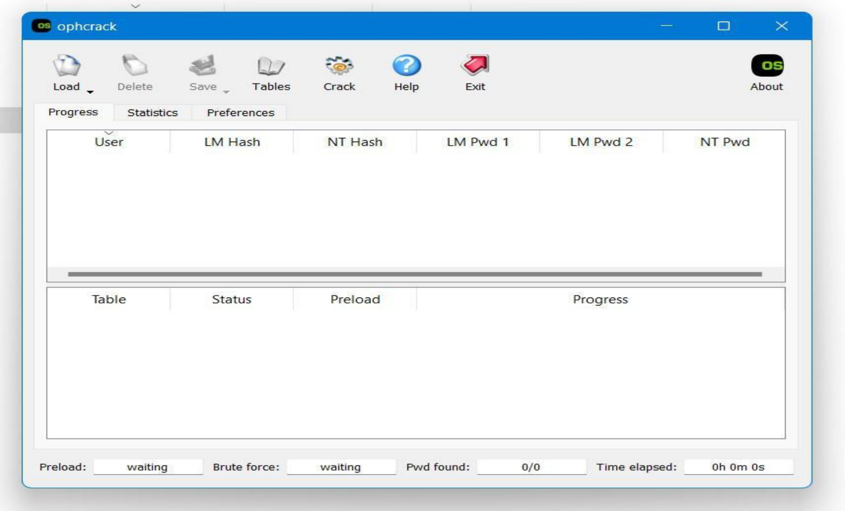
Dictionary search. Here, a password cracker searches each word in the dictionary for the correct password. Password dictionaries exist for a variety of topics and combinations of topics, including politics, movies and music groups.

Phishing. These attacks are used to gain access to user passwords without the use of a password cracking tool. Instead, a user is fooled into clicking on an email attachment. From here, the attachment could install malware or prompt the user to use their email to sign into a false version of a website, revealing their password.

Malware. Similar to phishing, using malware is another method of gaining unauthored access to passwords without the use of a password cracking tool. Malware such as keyloggers, which track keystrokes, or screen scrapers, which take screenshots, are used instead.

Guessing. An attacker may be able to guess a password without the use of tools. If the threat actor has enough information about the victim or the victim is using a common enough password, they may be able to come up with the correct characters.
Some password cracking programs may use hybrid attack methodologies where they search for combinations of dictionary entries and numbers or special characters. For example, a password cracker may search for ants01, ants02, ants03, etc. This can be helpful when users have been advised to include a number in their password.

How to use Ophcrack to Crack Passwords?
Ophcrack is a free, open-source tool that can be used to recover lost Windows passwords. It works by using pre-computed tables to crack password hashes, allowing users to recover their forgotten passwords quickly and easily. In this article, we will take a look at how to use Ophcrack for Windows password recovery, with step-by-step instructions and examples.
Before we begin, it's important to note that Ophcrack is only able to recover passwords for local Windows accounts, and not for Microsoft accounts. If you are using a Microsoft account to sign in to your Windows computer, you will need to reset your password through the Microsoft account website.



Preload: waiting Brute force: waiting Pwd found: 0/0 Time elapsed: 0h 0m 0s

With that said, let's take a look at **how to use Ophcrack for Windows password recovery.**
Step 1: Download and Install Ophcrack

- The first step in using Ophcrack for Windows password recovery is to download and install the tool. You can download the latest version of Ophcrack from the official website at https://ophcrack.github.io/.
- Once the download is complete, run the installer and follow the prompts to install Ophcrack on your computer.

Step 2: Create a Bootable Ophcrack USB or CD

- Next, you will need to create a bootable Ophcrack USB or CD. This will allow you to boot your computer from the Ophcrack USB or CD, allowing you to access the Ophcrack software and recover your lost password.
- To create a bootable Ophcrack USB, you will need a USB drive with at least 1 GB of storage space and a tool such as Rufus to create the bootable USB.
- To create a bootable Ophcrack CD, you will need a blank CD and a tool such as ImgBurn to create the bootable CD.
- Once you have your bootable Ophcrack USB or CD ready, move on to the next step.

Step 3: Boot Your Computer from the Ophcrack USB or CD

- With your bootable Ophcrack USB or CD ready, it's time to boot your computer from it. To do this, you will need to enter your computer's BIOS or UEFI settings and change the boot order.
- The exact steps for entering the BIOS or UEFI settings and changing the boot order will vary depending on your computer's make and model. In general, you will need to press a key (such as F2 or Del) during the boot process to enter the BIOS or UEFI settings, and then navigate to the "Boot" or "Boot Order" settings and change the order so that the Ophcrack USB or CD is first in the list.
- Once you have changed the boot order, save your changes and exit the BIOS or UEFI settings. Your computer should now boot from the Ophcrack USB or CD.

Step 4: Use Ophcrack to Recover Your Lost Password

- With your computer booted from the Ophcrack USB or CD, you can now use the Ophcrack software to recover your lost password.
- Upon booting, Ophcrack will automatically detect all of the user accounts on your computer and display them in a list. Simply select the user account for which you want to recover the password, and Ophcrack will begin the cracking process.
- Depending on the complexity of the password, the cracking process may take some time. Ophcrack will use the pre-computed tables to try different password combinations and crack the password hash. Once the password has been recovered, it will be displayed on the screen.

Conclusion : In this practical we studied how the passwords are cracked using system hacking and how to use Ophcrack to crack the password of windows system.