Password cracking is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password.
Most passwords can be cracked by using following techniques :

1) Hashing :- Here we will refer to the one way function (which may be either an encryption function or cryptographic hash) employed as a hash and its output as a hashed password.
If a system uses a reversible function to obscure stored passwords, exploiting that weakness can recover even 'well-chosen' passwords.
One example is the LM hash that Microsoft Windows uses by default to store user passwords that are less than 15 characters in length.
LM hash breaks the password into two 7-character fields which are then hashed separately, allowing each half to be attacked separately.

Hash functions like SHA-512, SHA-1, and MD5 are considered impossible to invert when used correctly.

2) Guessing :- Many passwords can be guessed either by humans or by sophisticated cracking programs armed with dictionaries (dictionary based) and the user's personal information.

Not surprisingly, many users choose weak passwords, usually one related to themselves in some way. Repeated research over some 40 years has demonstrated that around 40% of user-chosen passwords are readily guessable by programs. Examples of insecure choices include:

* blank (none)
* the word "password", "passcode", "admin" and their derivatives
* the user's name or login name
* the name of their significant other or another person (loved one)
* their birthplace or date of birth
* a pet's name
* a dictionary word in any language
* automobile licence plate number
* a row of letters from a standard keyboard layout (eg, the qwerty keyboard -- qwerty itself, asdf, or qwertyuiop)
* a simple modification of one of the preceding, such as suffixing a digit or reversing the order of the letters.
and so on....

In one survery of MySpace passwords which had been phished, 3.8 percent of passwords were a single word found in a dictionary, and another 12 percent were a word plus a final digit; two-thirds of the time that digit was.
A password containing both uppercase & lowercase characters, numbers and special characters too; is a strong password and can never be guessed.

Check Your Password Strength

3) Default Passwords :- A moderately high number of local and online applications have inbuilt default passwords that have been configured by programmers during development stages of software. There are lots of applications running on the internet on which default passwords are enabled. So, it is quite easy for an attacker to enter default password and gain access to sensitive information. A list containing default passwords of some of the most popular applications is available on the internet.
Always disable or change the applications' (both online and offline) default username-password pairs.

4) Brute Force :- If all other techniques failed, then attackers uses brute force password cracking technique. Here an automatic tool is used which tries all possible combinations of available keys on the keyboard. As soon as correct password is reached it displays on the screen.This techniques takes extremely long time to complete, but password will surely cracked.

Long is the password, large is the time taken to brute force it.

5) Phishing :- This is the most effective and easily executable password cracking technique which is generally used to crack the passwords of e-mail accounts, and all those accounts where secret information or sensitive personal information is stored by user such as social networking websites, matrimonial websites, etc.
Phishing is a technique in which the attacker creates the fake login screen and send it to the victim, hoping that the victim gets fooled into entering the account username and password. As soon as victim click on "enter" or "login" login button this information reaches to the attacker using scripts or online form processors while the user(victim) is redirected to home page of e-mail service provider.
Never give reply to the messages which are demanding for your username-password, urging to be e-mail service provider.

It is possible to try to obtain the passwords through other different methods, such as social engineering, wiretapping, keystroke logging, login spoofing, dumpster diving, phishing, shoulder surfing, timing attack, acoustic cryptanalysis, using a Trojan Horse or virus, identity management system attacks (such as abuse of Self-service password reset) and compromising host security.
However, cracking usually designates a guessing attack.

//////////*1000+ HACKING TRICKS & TUTORIALS - ebook By Mukesh Bhardwaj Blogger - Paid Version - only @ TekGyd | itechhacks | Mukeshtricks4u*///////

