Password Cracking

What is Password ?

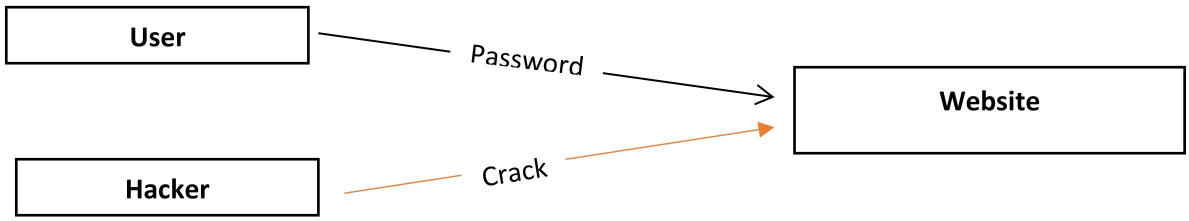
Password is a secret word or string of character value that must be allow to access a website, account, computer system or services.

What is Password Cracking ?

- Password Cracking is the method of extracting the password to gain authorized access to the target website or system.
- Password Cracking may be performed by social engineering attack or cracking through tempering the communication, or stealing the stored information.

How hacker hack password

This diagram shows you how hacker work, User access a website using password but hacker use crack password for access in a website.



Now first see how company store our password in database

Company basically use hashing algorithms to store our password in database, normally database look like table. There are many types hashing like MD5, MD6, SHA1, SHA2, SHA256, TIGER, and much more types of hashing, mostly company use MD5 hashing algorithms to store a password.

How look like MD5 hashing I use some word and change in MD5 hash

1. Password@123	d00f5d5217896fb7fd601412cb890830
2. I love you	e4f58a805a6e1fd0f6bef58c86f9ceb3
3. Om_shai_ram	d57e3d4f386de066c49887bd4e6bd274
4. 1928374650	5e980878408e8fdd35242a3c76d3d979
5. hac4er	7d6c34980ff9a213a38f7e77ee87fbe2

There is common password to use peoples and there MD5 hash values.

Example:

One website xyz.com and one person create an account then he fills some basic information like username, name, phone number, email id, password.

Website store this data in website database, now all basic information store in plain text remain password. Password store in hash values.

Note: Hashing only one way, we only encrypted password but we can’t decrypt that password using same method.

Types of Password Cracking

Now we discuss various types of password cracking method.

a. Non-Electronic (Social Engineering)
   Now we have one question how to social engineering help in password cracking see, Almost every type of attack contains some kind of social engineering. The classic email “phishing” and virus scam.
   For example: Attacker convince a user or victim to fill any phishing link, like attacker give some interesting offer(earn money without investing money, download least movies and web series, etc.) then victim fill that phishing link then attacker have user credentials like username, password.

b. Active Online Attacks: In this includes different techniques that directly interact with the target from cracking the password.
   a. Rainbow Table Attack: A rainbow table attack is a type of hacking wherein the perpetrator tries to use a rainbow hash table to crack the passwords stored in a database system.

   b. Dictionary Attack: A dictionary attack is a brute-force technique where attackers run through common words and phrases, such as those from a dictionary, to guess passwords.

   c. Brute Force Attack: A brute force attack, also known as an exhaustive search, is a cryptographic hack that relies on guessing possible combinations of a targeted password until the correct password is discovered. The longer the password, the more combinations that will need to be tested.

   These techniques depend up to your wordlist. If wordlist have that password then you crack either not.

c. Passive Online Attacks: They are performed without interacting the target.
   a. Sniffing:
      i. It is a process to monitor and capturing the packet through a network.
      ii. Sniffing is legal and illegal both.
      iii. It is part of passive attack.
      iv. Hacker use sniffing capture data packet contain sensitive information like username, email-id, password, account details, URLs, etc.

b. Man In the Middle Attack:
    i. This is same as Sniffing techniques.
    ii. It is a type of eavesdropping attack, where attackers interrupt an existing conversation or data transfer.

d. Default Password: An attacker using default password by searching through the official website of device manufacturer or thought online tools for scanning default password can attempt this type of attack. We use one website to find these types password: https://www.passwordsdatabase.com/

This method hacker cracks our password, now how to safe these thing

How to Safe

Now we discuss how to safe these methods.

1. Change default password.
2. Every months change your password.
3. Use complex password like Minimum 8 characters in length, Contains Uppercase Letters, Numbers, Symbols, Lowercase Letters, use this website for check password is strong or not http://www.passwordmeter.com/
4. If you have website and you store these type details (username, password, email-id, etc.) use salting algorithms, Salt Algorithms provide higher security.
   Note: Each company use own salt algorithm methods.

Reference

Google Articles and some YouTube videos