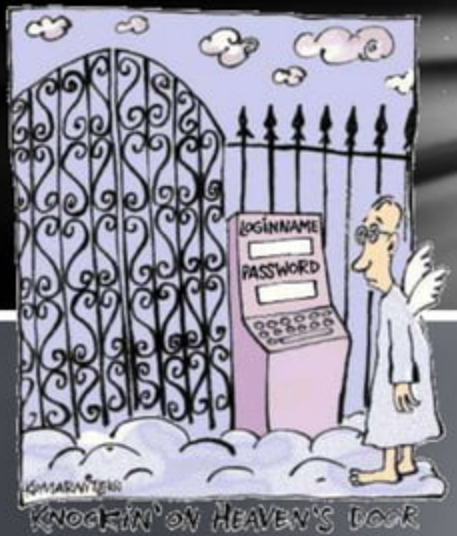
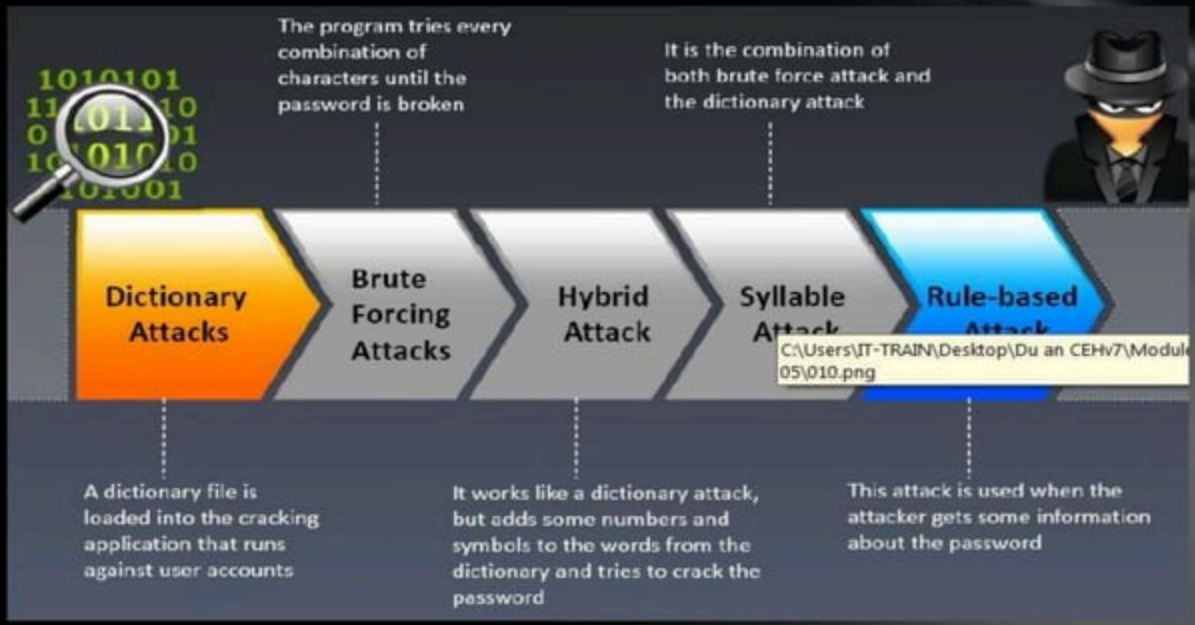
PASSWORD CRAKING TECHNIQUES



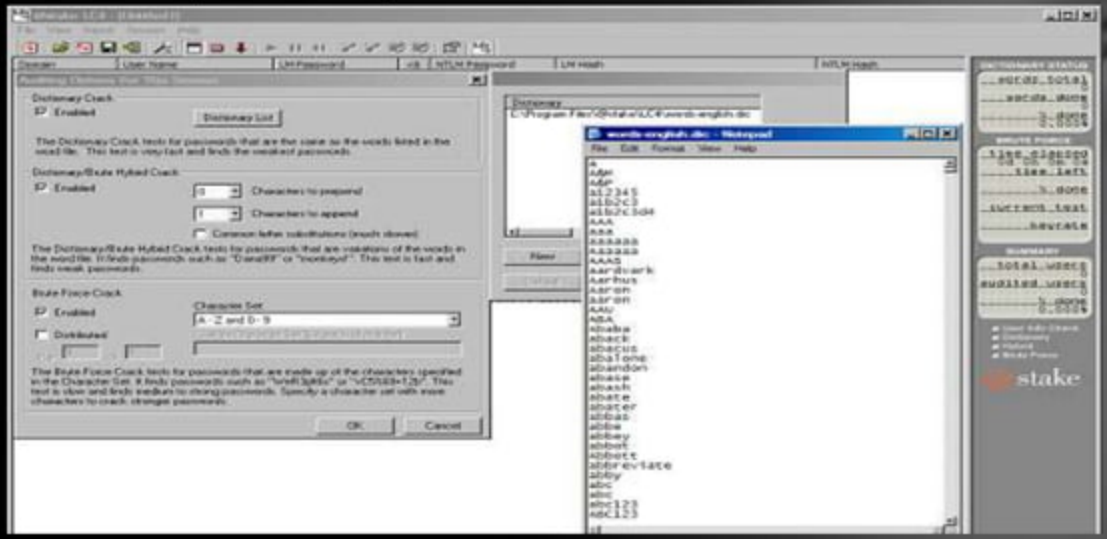
Password cracking is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password. Most passwords can be cracked by using following techniques :



Passwords

Dictionary Attack

- Attacker can compute H(word) for every word in a dictionary and see if the result is in the password file
- With 1,000,000-word dictionary and assuming 10 guesses per second, brute-force online attack takes 50,000 seconds (14 hours) on average
  This is very conservative; Offline attack is much faster!



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.

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.

* 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 license plate number

* a simple modification of one of the preceding, such as suffixing a digit or reversing the order of the letters. and so on....

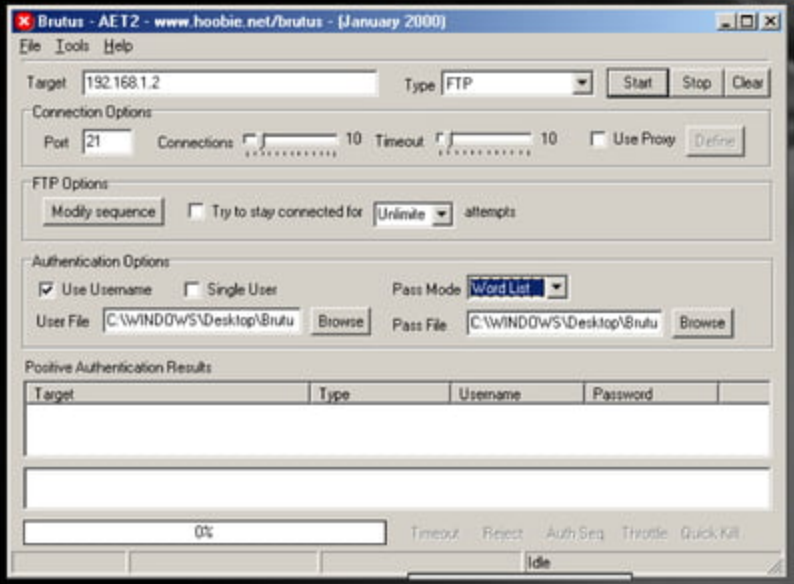
Default Passwords

- 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.

Brutus Password Cracker

- 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.

A Quick Look On Brutus Password Cracker



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.
- Never give reply to the messages which are demanding for your username-password, urging to be e-mail service provider.

SQL Injection

- Send a command to the DB
- Show the table of (userid, password)
- Or email me my password
  - If userid == 'x' OR 1 == 1

Passwords

Ten Common Mistakes

1. Leaving passwords blank or unchanged from default value.
2. Using the letters p-a-s-s-w-o-r-d as the password.
3. Using a favorite movie star name as the password.
4. Using a spouse's name as the password.
5. Using the same password for everything.
6. Writing passwords on post-it notes.
7. Pasting a list of passwords under the keyboard.
8. Storing all passwords in an Excel spreadsheet on a PDA or inserting passwords into a rolodex.
9. Writing all passwords in a personal diary/notebook.
10. Giving the password to someone who claims to be the system administrator.

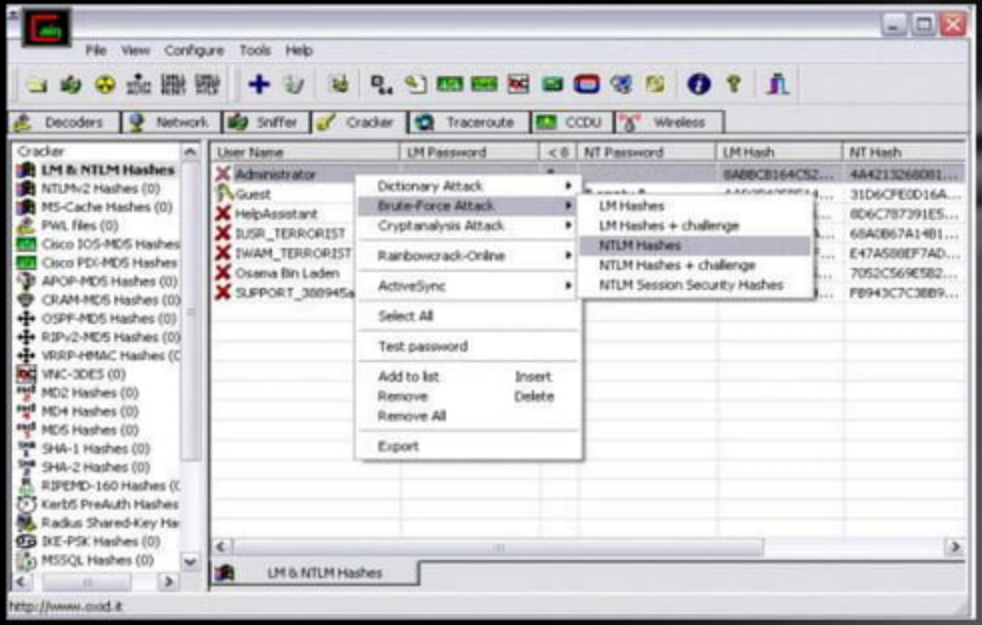
Password Cracking Tools

- The top 3 password crackers were:

1. Cain and Abel: The top password recovery tool for Windows.
2. John the Ripper: A powerful, flexible, and *fast* multi-platform password hash cracker.
3. THC Hydra: A Fast network authentication cracker which supports many different services.

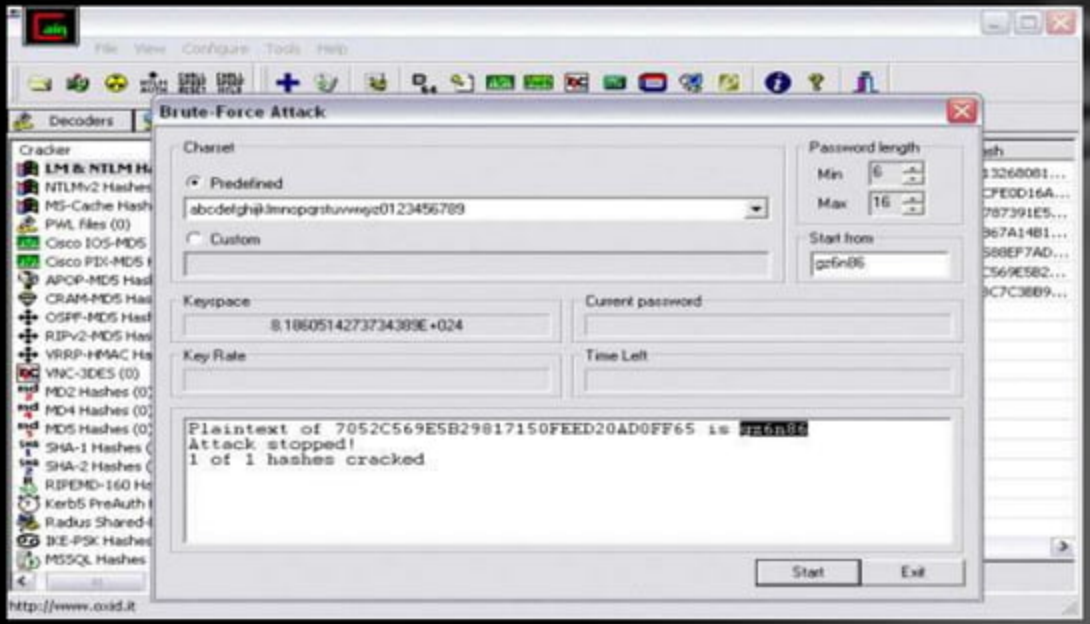
Window-XP Password Cracking

- Using Cain And Abel



Brute-Force

Using Cain And Abel



Cryptanalisys

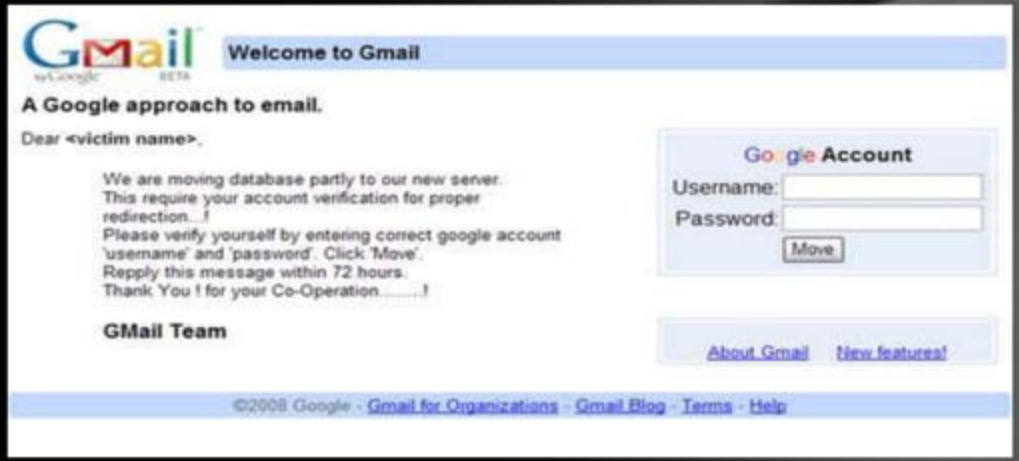
- Basically, Cryptanalisy converting encrypted messages to plain crypto-algorithm and/or key employed in This is the fastest technique of password Tables. A rainbow table is a file that is used to look known hash for an algorithm that does n Steps 1 to 4 i.e. up to importing hashes fro technique (i.e. brute-force).

- Here, select "cryptanalisys attack" then rainbow tables". Here we can choose either of tables. Click on "Add Table"
- Browse for the location of ra and click "open". 8) Select the loaded table and then click on "Start" button…
- On completion it will the exact password…

Cracking Gmail Account Password

- This method uses 'Social Engineering' rather than 'Phishing'.
- Follow the steps as given below :-

I. Create your own fake gmail login form using HTML, which may look as follow...



- We require a form processor to process this fake login form, i.e. to store the username and password entered by the victim. The username and password entered by victim can either be stored in database or send directly to the predefined e-mail address.
- This can be done in two ways-

i. Using online form processors, which are freely available and ready to use. eg. One of such form processor is provided by http://www.formmail.com .

ii. If you are having your own domain hosted on some server; know basics of ASP for processing HTML forms, you can create your own processor in ASP (eg. 'login.asp' page) .

- As soon as victim click on 'Move' button he/she get redirected to p webpage (eg. http://www.gmail.com), while his/her 'username' an get emailed to you by formmail.com .