The method of Crack Passwords

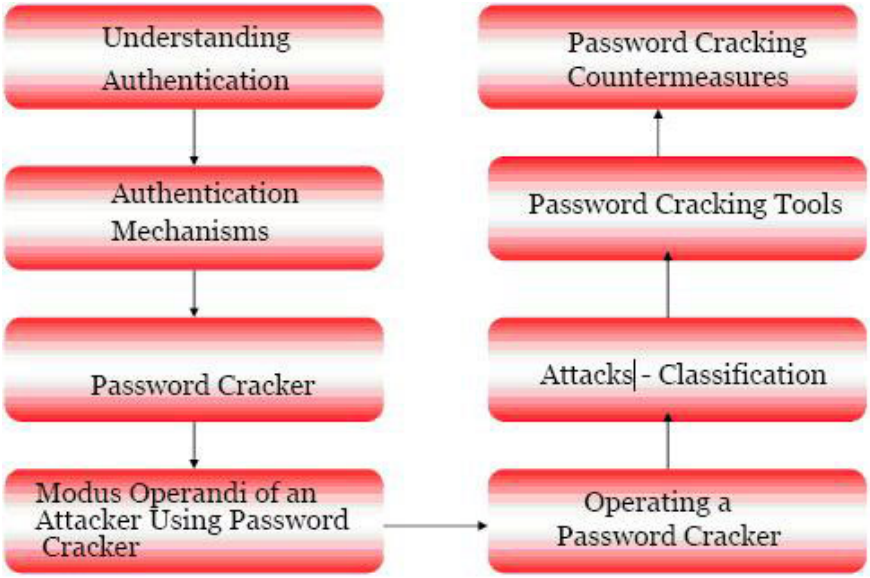
In this article, I present to you an overview of the authentication methods, the ways to password break and the Tools used to break the password. From there you will know how to protect yourself against attacks.

Username and Password are the most sensitive issues in a computer, a small network to the Internet. It is also an authentication method that is used a lot in computer systems and websites. However, this authentication method still exists vulnerabilities and is likely to be broken.

In this article, I present to you an overview of the authentication methods, the ways **to password break** and the Tools used to break the password. We also give you advice on how to set a secure password, from which you will know how to create strong passwords and protect yourself from attacks.

Main content in the lesson

Steps to take in the password attack process:



1. Authentication - Authentication

Authentication is a user identification process. In computer networks, authentication mainly uses LoginID (Username) and Password. Knowing the password of an account is essential for authentication, but the Password can be lost, stolen, altered and destroyed, which leads to a security risk for the system.

Besides passwords there are many ways to authenticate users, we will go into the specifics in the next section.

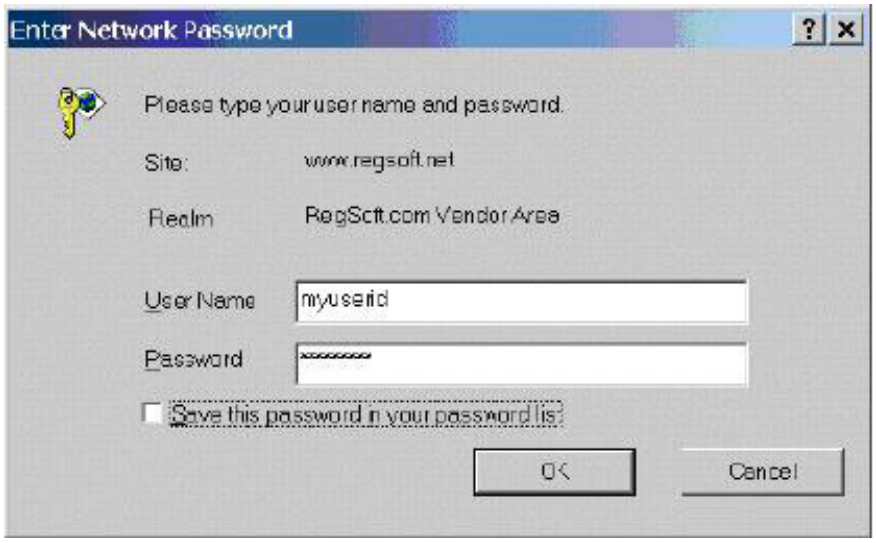
2. Authentication methods

1. Most authentication methods are based on:
    1. What you know (Password Username)
    2. What you have (Smart Card, Certificate)
    3. What are you (Biometrics)

1. HTTP Authentication - Authentication on the WEB.
    1. Basic Authentication
    2. Digest Authentication
2. Combined with Windows NTLM authentication method
3. Negotiate Authentication - Authentication agreement
4. Certificate-based authentication.
5. Authentication is based on Forms
6. Authentication relies on RSA Secure Token
7. Biometric-based authentication (fingerprint, face, iris authentication).

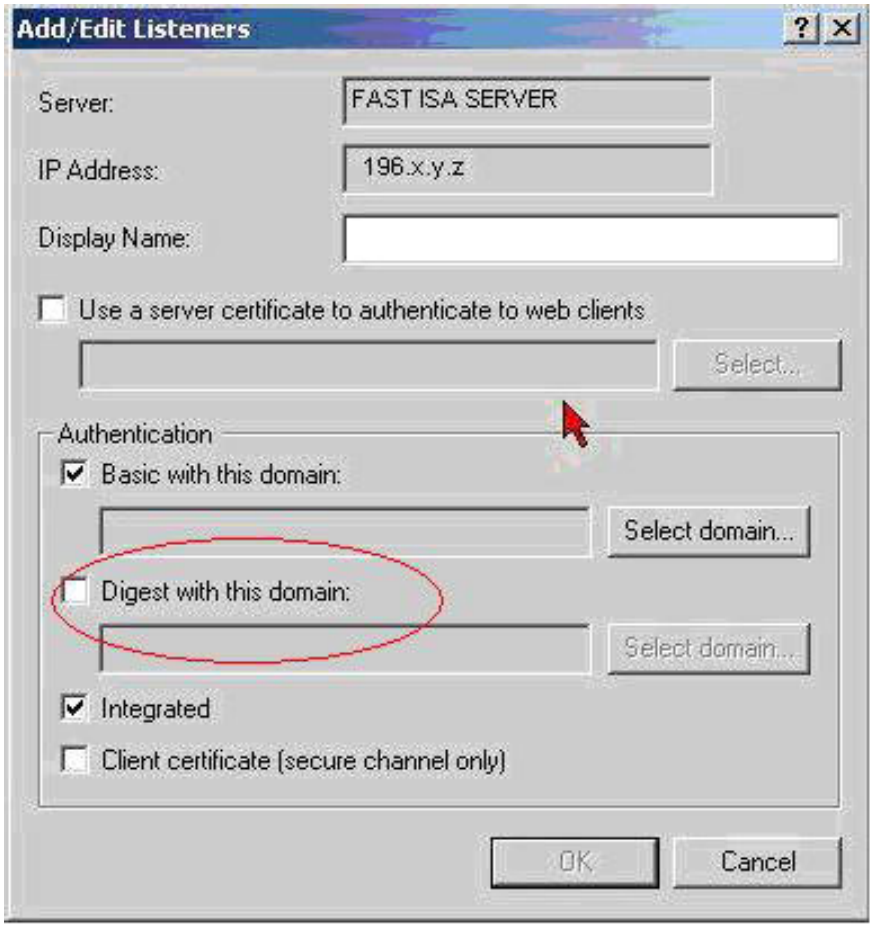
2. 1. HTTP Authentications

a. Basic Authentication



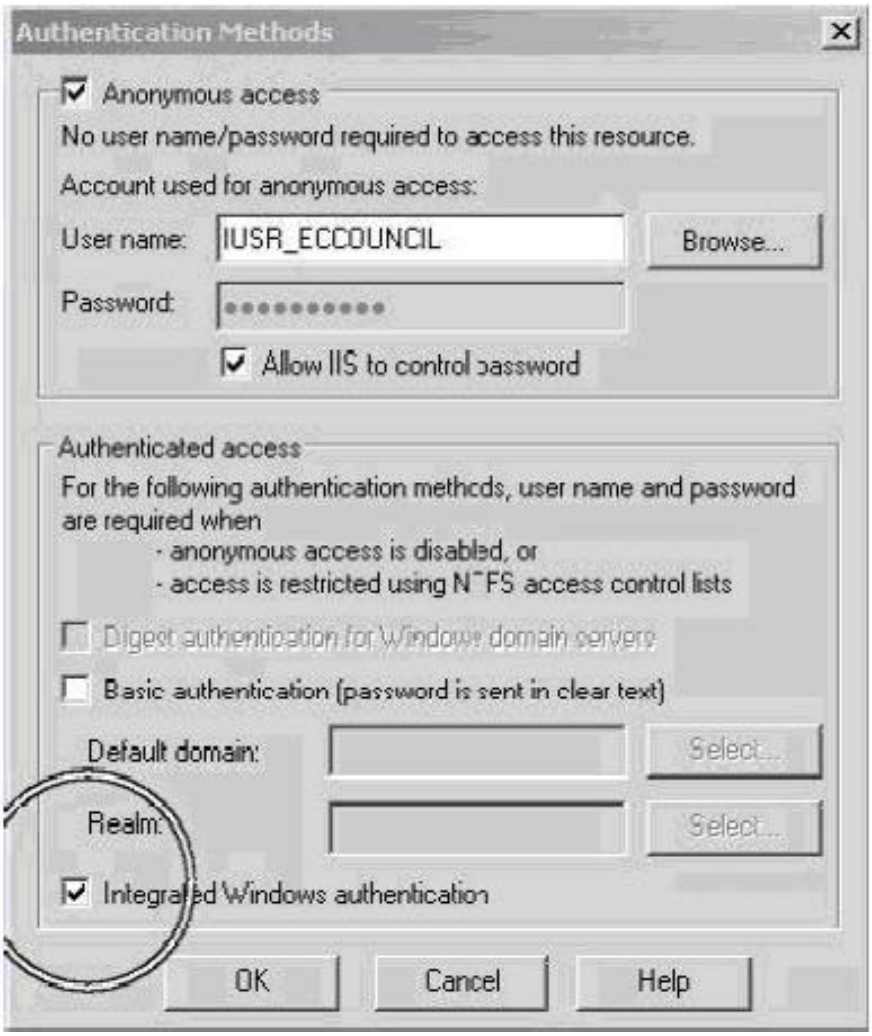
1. Is a universal authentication method available on the Web application platform.
2. It will appear when the Client requests information to be authenticated.
3. Limit protocols, allowing attackers to exploit.
4. Use SSL to encrypt the Username Password data to transfer between Client and Server.

b. Digest Authentication



1. Designed to enhance security more than Basic Authentication method
2. Based on Challenge-Response authentication platform
3. Advanced security than Basic Authentication method, the system will encrypt Usernaem Password before transferring on the network.

2.2. Combined with Windows NTLM authentication method



1. Use NT LAN Manager (NTLM) authentication technology for HTTP
2. Only works with IE and on the Web server platform that is IIS.
3. Combined with Windows authentication, it is suitable for corporate local area environments
4. It is an authentication method that does not have to transmit any information about the Username password on the network.

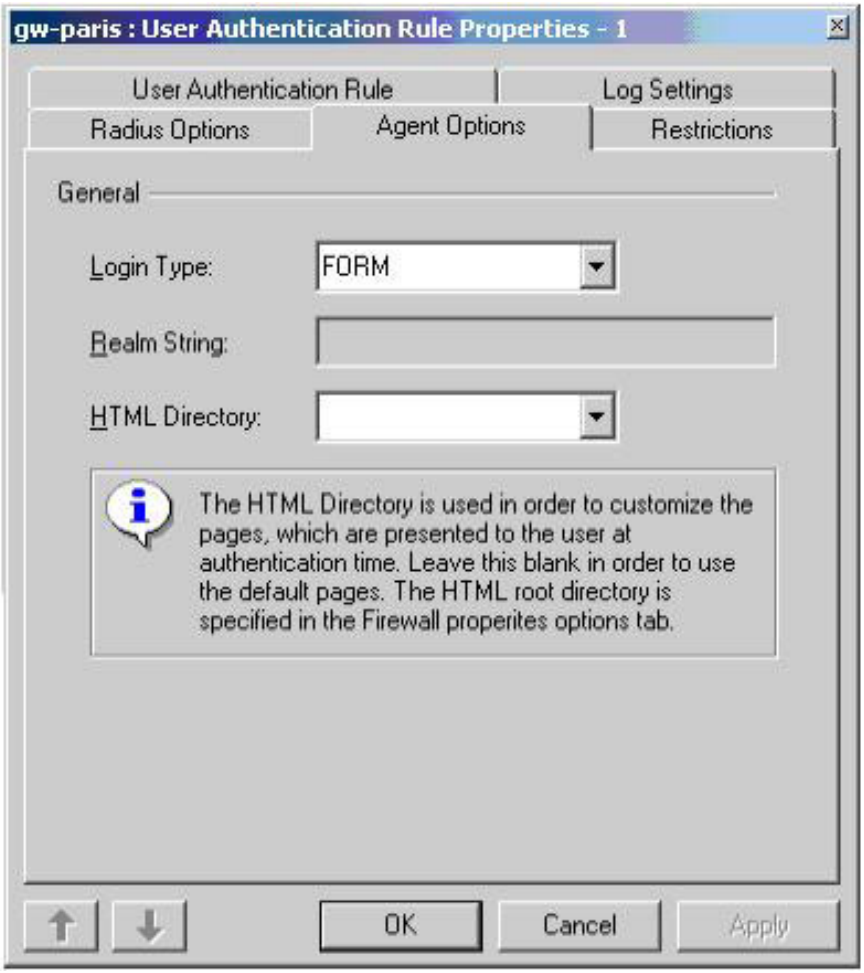
2.3. Validate Negotiate

1. This is an extended authentication method for NTLM Authentication
2. Provide authentication based on Kerberos platform
3. Use the negotiation process to determine the level of security used.
4. It is configured and used not only for local area networks.

2.4. Certificate-based authentication

1. Use Public Key to encrypt and digital Certificate to authenticate users.
2. It is of interest and incorporates two-factor authentication. When a user knows the Username Password he or she must provide a Certificate to be authenticated.
3. Users can be stolen Certtificate.
4. Many software now support digital certificate authentication.

2.5. Authentication relies on Forms-Based



1. It is not supported on HTTP and SSL platforms
   It is a premium option for authentication using a Form, and is often integrated in HTML format.
   Is a very popular authentication method on the Internet.

2.6. RSA SecurID Token authentication method

1. The SecureID authentication method uses a "token - Ticket, card." Having a hardware device will generate authentication codes every 60 seconds and use a Card to decode the key.
2. A user who performs the authentication and network resources will have to enter the PIN and display number for the SecureID for each time.

2.7. Biometrics Authentications

1. An authentication system based on biometrics will have devices that identify users based on biological factors such as fingerprints, eyes, face, hands .
2. This is an authentication method with very high security and convenient for users not to remember the password or bring a Card.

3. How to have a secure password

We've got a very detailed article about creating secure passwords with a lot of methods and tips so you can create a strong password to protect your data. Below are the basic notes when setting a password.

1. Apply a minimum password length policy of 8 and preferably 15
2. Special characters, numbers, uppercase and lowercase letters are required in a password
3. Do not use any keywords in English dictionary or other countries
4. Do not use the same Password as a Username, and must change often
5. Choose a password that is easy to use that others can hardly guess.

4. Recommendations to set another password

1. Never just put a special character after an example keyword: Don't set a password: vnexperts1
2. Never use a pair of words together to get a Password such as: vnevne
3. Do not set the Password easily
4. Do not set a password too short
5. Do not set a Password that frequently typed as: asdf; lkj
6. Change your password at least once a month - Change it immediately when your password is discovered by someone else.
7. Never store a Password on your computer - many people who have a habit of going to websites and saving their passwords are not as secure because the encryption on the computer is easily decrypted.
8. The passwords in Windows saved to .pwl files are not secure.
9. Don't tell others your password.
10. Do not send mail and avoid placing identical passwords on many applications
11. Do not write your Password to make it easy to remember.
12. When typing Password be careful with the types of Keyloggers and thieves.

5. Which methods do hackers take your password?

1. See you type the password
2. Find out if you have written your password on paper
3. Guess passwords based on familiar numbers like: 123456, 654321 .
4. Using Brute Force attack method: This is a method of synthesizing characters in turn to find the password, try and wrong continuously until the correct password is found.
5. Using Dictionary Attack attack method: This attack method finds the password in a previously generated dictionary.
6. How to create a hard password:
    1. For example, my password was originally set to: yeuemnhieu
    2. Now I capitalize the letter Y and the U into: YeUemnhieU
    3. The letter E in the alphabet stands for 5 of my password: Y5U5mnhi5U
    4. My i changed into! password into Y5U5mnh! 5U
    5. My password is full of 10 characters with numbers, with flowers, usually, with special characters.

6. Delete the saved password in Windows XP

Enter the run: **Rundll32.exe Keymgr.dll, KRShowKeyMgr** , will display the website listing list and you should delete all the saved passwords in the system.

7. Break the general password

About defining a Password Cracker is a program that can decrypt a password or can disable a password.

Password Cracker has two main methods: ***Brute Force*** and ***Dictionary Attack*** , and now there is a classic two-way password-breaking program on which to find the Password: ***Smart Table Recovery*** - speed response Find passwords very quickly.

Password Cracker can also be a program used to decrypt encrypted passwords, such as passwords saved in IE, Firefox, etc.

8. The goal of programs to find passwords

On Windows and Linux systems, there are two full accounts in that system: root and Administrator, and the attack target is to find the passwords of those two accounts.

When you find the Password of an account that has the right to administer an attacker, it has full control over the target computer.

The attacker can also use the Sniffer software to capture the Password Username packets transmitted in the network.

And the effect of losing administrative rights depends entirely on data and applications in the same way.

9. How Password Cracker works

To understand how a Password Cracker works, we need to understand how Password management programs work. Most Password management programs encrypt the Password in a certain way.

The password after being created and stored in the system will be encrypted, the system will contain the Key to decrypt the password. The Password Cracker software will try to get those cryptographic passages. After obtaining the passages on the victim's machine, they will proceed to decrypt the password using specific methods for each situation.

10. Types of Password Cracker

1. *Dictionary Attack:* Find passwords in a built-in dictionary file
2. *Brute Force Attack* : Find passwords by combining characters
3. *Hybird Attack* : Hybrid between the above two methods
4. *Smart Table Recovery Attack* : The smartest password search attack method based on data tables - About 700MB of text data.

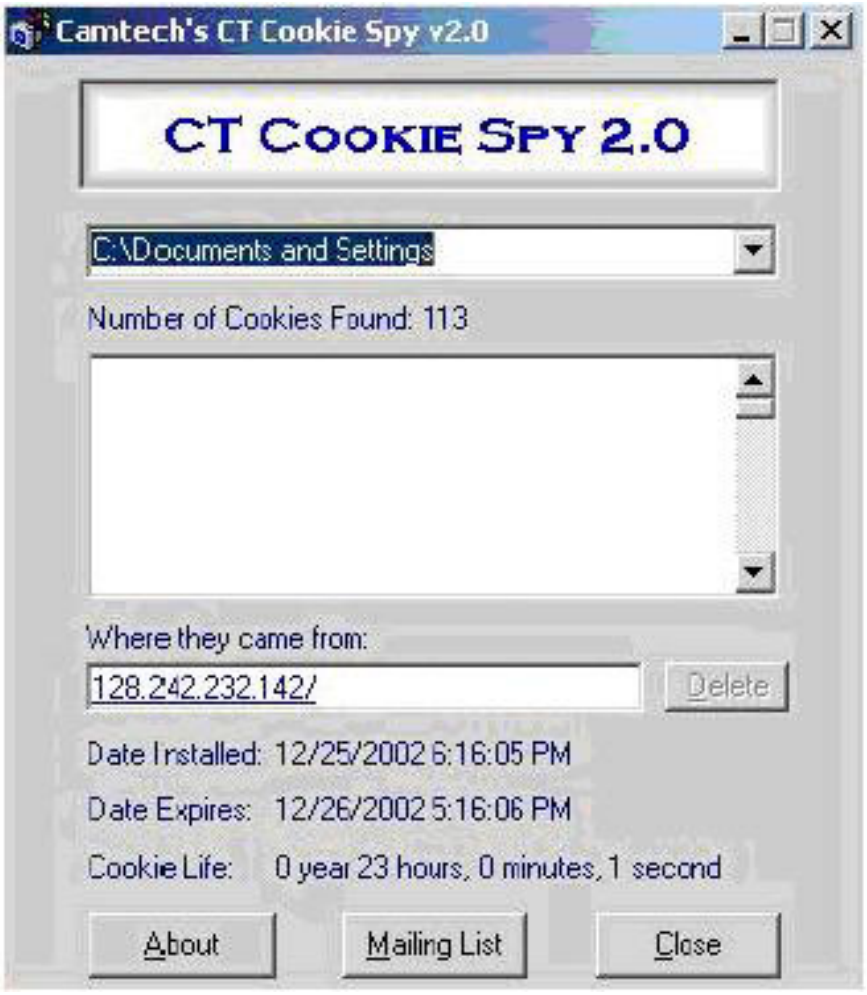
11. Find Password by simple method

There are 2 methods to find a simple password:

1. Guess the password
2. Replace the URL

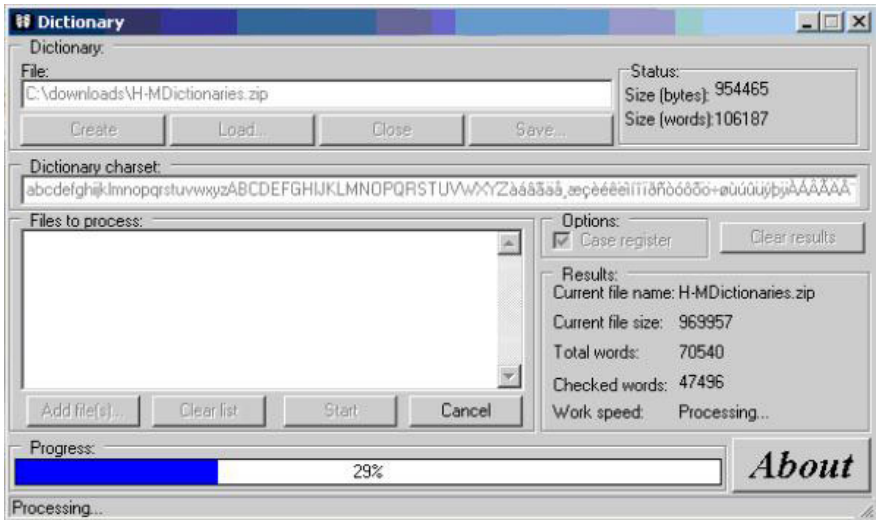
12. Find the Password by decrypting Cookies

1. With CT Spy cookie program 2.0
2. Trade Cookies store a lot of important information of users when accessing the Internet like Username and Password to access a Website.
3. With this software you can search for saved Cookies in the system and decrypt them to find the Password Username.



13. Attack Dictionary Attack

Create dictionary using software: Dictionary Maker



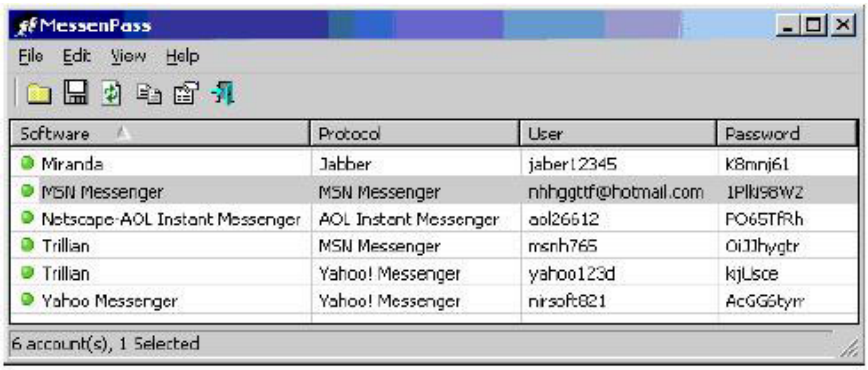
14. List of Tools Password Crackers

1. Lophtcrack - WebCracker
2. John The Ripper - Munga Bunga
3. Brutus - ReadCookies
4. Obiwan - SnadBoy
5. Authforce - WinSSLMiM
6. Hydra - RAR
7. Cain & Abel Gammaprog

Most of these tools are free and, if available, are completely cracked easily.

Most of them are capable of using all of these attacks, can Export Password Username from a Local or Remote system.

1. In my experience it is often used: Cain & Abel but this software is more powerful in decoding and Sniffer. Lophcrack probably cracked pretty quickly any password that is less than 10 characters long. My computer only needs about 1 hour to decrypt it.
2. John the Ripper is a password-breaker in Unix and uses DES and Extend DES encryption, MD5 also integrates many decryption methods.
3. Brutus is an Online program or Remote Password Cracker. Attack on a system like IIS, Windows server, ADSL Modem . They try a certain Username and Password one by one to attack the server
4. Obiwan overcomes Brutus's disadvantage of having a lag when using the wrong Username Password.
5. Authforce relies on HTTP Basic Authentication to support testing of Username Password to a certain site
6. MessenPass can extract most chat accounts like Yahoo, MSN .



1. Note that the YM 7 password version will never be saved on the Local machine, this software cannot be cracked.
2. Wireless WEP Key Password Spy is a decryption support tool to access a network system vWireless to set a password.

See also: How to check password strength