**What is Password Cracking?**

Password cracking is the process of guessing or recovering a password from stored locations or from data transmission system. It is used to get a password for unauthorized access or to recover a forgotten password. In penetration testing, it is used to check the security of an application.

In recent years, computer programmers have been trying to create algorithms for password cracking in less time. Most of the password cracking tools try to login with every possible combination of words. If login is successful, it means the password was found. If the password is strong enough with a combination of numbers, characters and special characters, this cracking method may take hours to weeks or months. A few password cracking tools use a dictionary that contains passwords. These tools are totally dependent on the dictionary, so success rate is lower.

In the past few years, programmers have developed many password cracking tools. Every tool has its own advantages and disadvantages. In this post, we are covering a few of the most popular password cracking tools.

**1. Brutus**

Brutus is one of the most popular remote online password cracking tools. It claims to be the fastest and most flexible password cracking tool. This tool is free and is only available for Windows systems. It was released back in October 2000.

It supports HTTP (Basic Authentication), HTTP (HTML Form/CGI), POP3, FTP, SMB, Telnet and other types such as IMAP, NNTP, NetBus, etc. You can also create your own authentication types. This tool also supports multi-stage authentication engines and is able to connect 60 simultaneous targets. It also has resume and load options. So, you can pause the attack process any time and then resume whenever you want to resume.

This tool has not been updated for many years. Still, it can be useful for you.

**2. RainbowCrack**

RainbowCrack is a hash cracker tool that uses a large-scale time-memory trade off process for faster password cracking than traditional brute force tools. Time-memory trade off is a computational process in which all plain text and hash pairs are calculated by using a selected hash algorithm. After computation, results are stored in the rainbow table. This process is very time consuming. But, once the table is ready, it can crack a password must faster than brute force tools.

You also do not need to generate rainbow tablets by yourselves. Developers of RainbowCrack have also generated LM rainbow tables, NTLM rainbow tables, MD5 rainbow tables and Sha1 rainbow tables. Like RainbowCrack, these tables are also available for free. You can download these tables and use for your password cracking processes.

Download Rainbow tables here: <http://project-rainbowcrack.com/table.htm>

A few paid rainbow tables are also available, which you can buy from here: <http://project-rainbowcrack.com/buy.php>

This tool is available for both Windows and Linux systems.

Download Rainbow crack here: <http://project-rainbowcrack.com/>

**3. Wfuzz**

Wfuzz is another web application password cracking tool that tries to crack passwords with brute forcing. It can also be used to find hidden resources like directories, servlets and scripts. This tool can also identify different kind of injections including SQL Injection, XSS Injection, LDAP Injection, etc in Web applications.

**Key features of Wfuzz password cracking tool:**

* Capability of injection via multiple points with multiple dictionary
* Output in colored HTML
* Post, headers and authentication data brute forcing
* Proxy and SOCK Support, Multiple Proxy Support
* Multi Threading
* Brute force HTTP Password
* POST and GET Brute forcing
* Time delay between requests
* Cookies fuzzing

**4. Cain and Abel**

Cain and Abel is a well-known password cracking tool that is capable of handling a variety of tasks. The most notable thing is that the tool is only available for Windows platforms. It can work as sniffer in the network, cracking encrypted passwords using the dictionary attack, recording VoIP conversations, brute force attacks, cryptanalysis attacks, revealing password boxes, uncovering cached passwords, decoding scrambled passwords, and analyzing routing protocols.

Cain and Abel does not exploit any vulnerability or bugs. It only covers security weakness of protocols to grab the password. This tool was developed for network administrators, security professionals, forensics staff, and penetration testers.

Download here: <http://www.oxid.it/ca_um/>

**5. John the Ripper**

John the Ripper is another well-known free open source password cracking tool for Linux, Unix and Mac OS X. A Windows version is also available. This tool can detect weak passwords. A pro version of the tool is also available, which offers better features and native packages for target operating systems. You can also download Openwall GNU/\*/Linux that comes with John the Ripper.

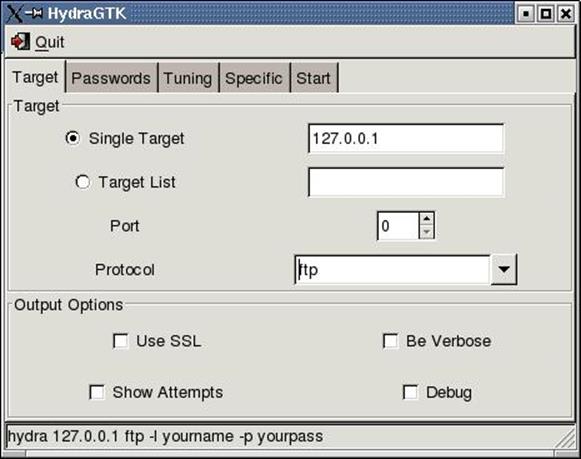
Download John the Ripper here: <http://www.openwall.com/john/>

**6. THC Hydra**

THC Hydra is a fast network logon password cracking tool. When it is compared with other similar tools, it shows why it is faster. New modules are easy to install in the tool. You can easily add modules and enhance the features. It is available for Windows, Linux, Free BSD, Solaris and OS X. This tool supports various network protocols. Currently it supports Asterisk, AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MYSQL, NCP, NNTP, Oracle Listener, Oracle SID, Oracle, PC-Anywhere, PCNFS, POP3, POSTGRES, RDP, Rexec, Rlogin, Rsh, SAP/R3, SIP, SMB, SMTP, SMTP Enum, SNMP, SOCKS5, SSH (v1 and v2), Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC and XMPP.

Download THC Hydra here: <https://www.thc.org/thc-hydra/>

If you are a developer, you can also contribute to the tool’s development.



**7. Medusa**

Medusa is also a password cracking tool similar to THC Hydra. It claims to be a speedy parallel, modular and login brute forcing tool. It supports HTTP, FTP, CVS, AFP, IMAP, MS SQL, MYSQL, NCP, NNTP, POP3, PostgreSQL, pcAnywhere, rlogin, SMB, rsh, SMTP, SNMP, SSH, SVN, VNC, VmAuthd and Telnet. While cracking the password, host, username and password can be flexible input while performing the attack.

Medusa is a command line tool, so you need to learn commands before using the tool. Efficiency of the tool depends on network connectivity. On a local system, it can test 2000 passwords per minute.

With this tool, you can also perform a parallel attack. Suppose you want to crack passwords of a few email accounts simultaneously. You can specify the username list along with the password list.

Read more about this here: <http://foofus.net/goons/jmk/medusa/medusa.html>

Download Medusa here: <http://www.foofus.net/jmk/tools/medusa-2.1.1.tar.gz>

**8. OphCrack**

OphCrack is a free rainbow-table based password cracking tool for Windows. It is the most popular Windows password cracking tool, but can also be used on Linux and Mac systems. It cracks LM and NTLM hashes. For cracking Windows XP, Vista and Windows 7, free rainbow-tables are also available.

A live CD of OphCrack is also available to simplify the cracking. One can use the Live CD of OphCrack to crack Windows-based passwords. This tool is available for free.

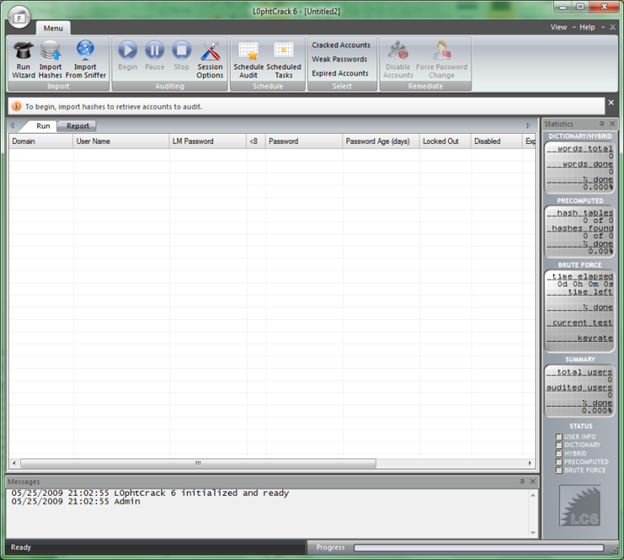
Download OphCrack here: <http://ophcrack.sourceforge.net/>

Download free and premium rainbow tables for OphCrack here: <http://ophcrack.sourceforge.net/tables.php>

**9. L0phtCrack**

L0phtCrack is an alternative to OphCrack. It attempts to crack Windows password from hashes. For cracking passwords, it uses Windows workstations, network servers, primary domain controllers, and Active Directory. It also uses dictionary and brute force attacking for generating and guessing passwords. It was acquired by Symantec and discontinued in 2006. Later L0pht developers again re-acquired it and launched L0phtCrack in 2009.

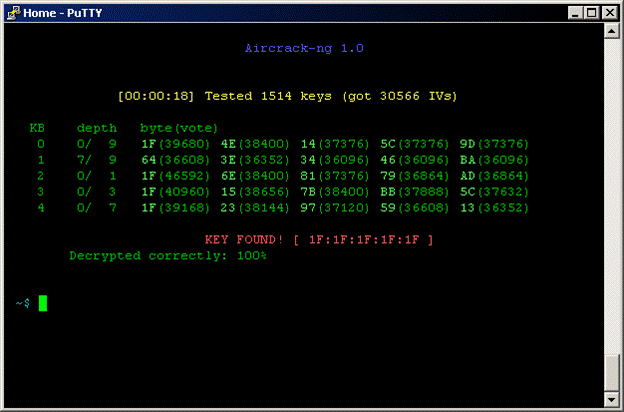
It also comes with a schedule routine audit feature. One can set daily, weekly or monthly audits, and it will start scanning on the scheduled time.



L0phtCrack: <http://www.l0phtcrack.com/>

**10. Aircrack-NG**

Aircrack-NG is a WiFi password cracking tool that can crack WEP or WPA passwords. It analyzes wireless encrypted packets and then tries to crack passwords via its cracking algorithm. It uses the FMS attack along with other useful attack techniques for cracking password. It is available for Linux and Windows systems. A live CD of Aircrack is also available.



If you want to use AirCrack NG for password cracking, read tutorials here: <http://www.aircrack-ng.org/doku.php?id=getting_started>

Download AirCrack-NG here: <http://www.aircrack-ng.org/>

**How to create a password that is hard to crack**

In this post, we have listed 10 password cracking tools. These tools try to crack passwords with different password cracking algorithms. Most of the password cracking tools are available for free. So, you should always try to have a strong password that is hard to crack by these password cracking tools. These are few tips you can try while creating a password.

**The longer the password, the harder it is to crack:** Password length is the most important factor. If you select a small password, password cracking tools can easily crack it by using few words combinations. A longer password will take a longer time in guessing. You’re your password at least 8 characters long.

**Always use a combination of characters, numbers and special characters**: This is another thing which makes passwords hard to crack. Password cracking tools try the combination of one by one. Have a combination of small characters, capital letters, and special characters. Suppose if you have only numbers in your password. Password cracking tools only need to guess numbers from 0-9. Here only length matters. But having a password combination of a-z, A-Z, 0-9 and other special characters with a good length will make it harder to crack. This kind of password sometimes takes weeks to crack.

**Variety in passwords:** One important thing you must always take care. Never use same password everywhere. Cyber criminals can steal passwords from one website and then try it on other websites too.

In case you are not sure about the strength of your password, you can check it from variety of online tools available for free.

**What to avoid while selecting your password**

There are a few things which were very common a few years back and still exist. Most of the password cracking tools start from there. Passwords that fall into this category are most easy to crack. These are the few password mistakes which you should avoid:

1. Never use a dictionary word
2. Avoid using your pet’s name, parent name, your phone number, driver’s license number or anything which is easy to guess.
3. Avoid using passwords with sequence or repeated characters: For Ex: 1111111, 12345678 or qwerty, asdfgh.

Avoid using passwords that fall in worst password list. Every year, data analysis companies publish the list of worst passwords of the year from analyzing the leaked password data.

**The**[**top 25 passwords on the 2017**](http://fortune.com/2017/12/19/the-25-most-used-hackable-passwords-2017-star-wars-freedom/)**list.**

1. 123456
2. Password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. letmein
8. 1234567
9. football
10. iloveyou
11. admin
12. welcome
13. monkey
14. login
15. abc123

**The top 11 worst passwords of 2012:**

1. password
2. 123456
3. 12345678
4. abc123
5. qwerty
6. monkey
7. letmein
8. dragon
9. 111111
10. baseball
11. iloveyou