HACK LIKE A PRO

How to Crack Passwords, Part 1 (Principles & Technologies)

BY OCCUPYTHEWEB 07/18/2014 11:44 PM 05/27/2016 12:45 AM PASSWORD CRACKING

Welcome back, my neophyte hackers!

I have already done a few tutorials on password cracking, including ones for **Linux** and **Windows**, **WEP** and **WPA2**, and even online passwords using **THC Hydra**. Now, I thought it might be worthwhile to begin a series on password cracking in general. Password cracking is both an art and a science, and I hope to show you the many ways and subtleties involved.

We will start with the basic principles of password cracking that are essential to ALL password cracking techniques, followed by some of the tools and technologies used. Then, one by one, I will show you how to use those principles and technologies effectively to crack or capture the various types of passwords out there.

The Importance & Methods of Password Cracking

Passwords are the most widely used form of authentication throughout the world. A username and password are used on computer systems, bank accounts, ATMs, and more. The ability to crack passwords is an essential skill to both the hacker and the **forensic investigator**, the latter needing to hack passwords for accessing the suspect's system, hard drive, email account, etc.

Although some passwords are very easy to crack, some are very difficult. In those cases, the hacker or forensic investigator can either employ greater computing resources (a botnet, supercomputer, GPU, ASIC, etc.), or they can look to obtain the password in other ways.

These ways might include insecure storage. In addition, sometimes you don't need a password to access password-protected resources. For instance, if you can replay a cookie, session ID, a Kerberos ticket, an authenticated session, or other resource that authenticates the user after the password authentication process, you can access the password protected resource without ever knowing the password.

Sometimes these attacks can be much easier than cracking a complex and long password. I will do a tutorial on various replay attacks in the near future (look out specifically for my upcoming article on stealing the Facebook cookie to access someone's Facebook account).

Now, let's start with the basics.

Step 1

Password Storage

In general, passwords are not stored in clear text. As a rule, passwords are stored as hashes. Hashes are one-way encryption that are unique for a given input. These systems very often use MD5 or SHA1 to hash the passwords.

In the Windows operating system, passwords on the local system are stored in the *SAM* file, while Linux stores them in the */etc/shadow* file. These files are accessible only by someone with root/sysadmin privileges. In both cases, you can use a service or file that has root/sysadmin privileges to grab the password file (e.g. DLL injection with samdump.dll in Windows).

Step 2

Types of Attacks

Dictionary

A dictionary attack is the simplest and fastest password cracking attack. To put it simply, it just runs through a dictionary of words trying each one of them to see if they work. Although such an approach would seem impractical to do manually, computers can do this very fast and run through millions of words in a few hours. This should usually be your first approach to attacking any password, and in some cases, it can prove successful in mere minutes.

Rainbow Table

Most modern systems now store passwords in a hash. This means that even if you can get to the area or file that stores the password, what you get is an encrypted password. One approach to cracking this encryption is to take dictionary file and hash each word and compare it to the hashed password. This is very time- and CPU-intensive. A faster approach is to take a table with all the words in the dictionary already hashed and compare the hash from the password file to your list of hashes. If there is a match, you now know the password.

Brute Force

Brute force is the most time consuming approach to password cracking. It should always be your last resort. Brute force password cracking attempts all possibilities of all the letters, number, special characters that might be combined for a password and attempts them. As you might expect, the more computing horsepower you have, the more successful you will be with this approach.

Hybrid

A hybrid password attack is one that uses a combination of dictionary words with special characters, numbers, etc. Often these hybrid attacks use a combination of dictionary words with numbers appending and prepending them, and replacing letters with numbers and special characters. For instance, a dictionary attack would look for the word "password", but a hybrid attack might look for "p@$$w0rd123".

Step 3

Commonly Used Passwords

As much as we think each of us is unique, we do show some common patterns of behavior within our species. One of those patterns is the words we choose for passwords. There are number of

wordlists that have been compiled of common passwords. In recent years, many systems have been cracked and passwords captured from millions of users. By using these already captured passwords, you are likely to find at least a few on the network you are trying to hack.

Step 4

Password Cracking Strategy

Many newbies, when they start cracking passwords, simply choose a tool and word list and then turn them loose. They are often disappointed with the results. Expert password crackers have a strategy. They don't expect to be able to crack every password, but with a well-developed strategy, they can crack most passwords in a very short amount of time.

The key to develop a successful strategy of password cracking is to use multiple iterations, going after the easiest passwords with the first iteration to the most difficult passwords using different techniques for each iteration.

Step 5

Password Cracking Software

John

John the Ripper is probably the world's best known password cracking tool. It is strictly command line and strictly for Linux. Its lack of a GUI makes a bit more challenging to use, but it is also why it is such a fast password cracker.

One of the beauties of this tool is its built in default password cracking strategy. First, attempts a dictionary attack and if that fails, it then attempts to use combined dictionary words, then tries a hybrid attack of dictionary words with special characters and numbers and only if all those fail will it resort to a brute force.

Ophcrack

Ophcrack is a free rainbow table-based password cracking tool for Windows. It is among the most popular Windows password cracking tools (Cain and Abel is probably the most popular; see below), but can also be used on Linux and Mac systems.

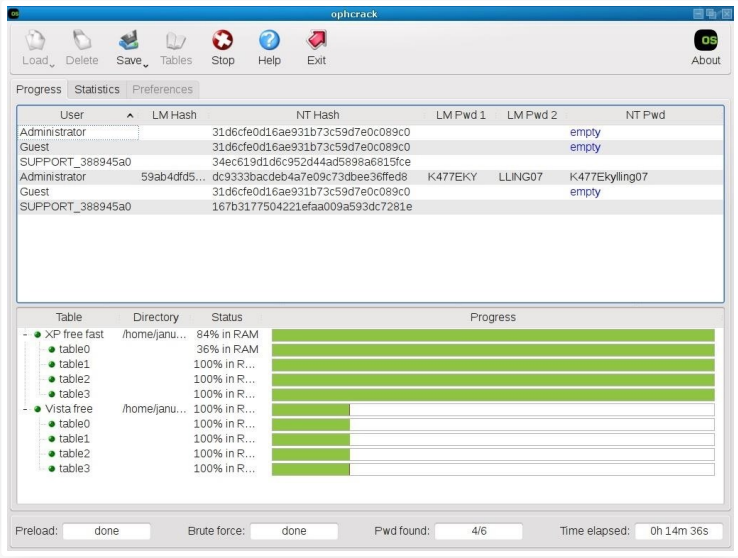
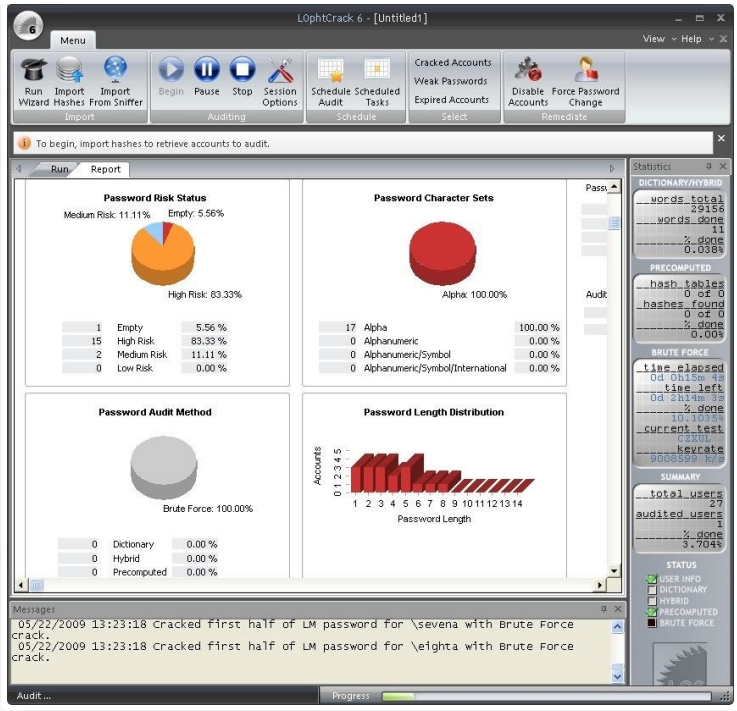


Image by Ysangkok/Wikimedia Commons

It cracks LM and NTLM (Windows) hashes. For cracking Windows XP, Vista and Windows 7, you can download free rainbow tables. You can download Ophcrack on SourceForge, and you can get some free and premium rainbow tables for Ophcrack here.

L0phtCrack

L0phtCrack is an alternative to Ophcrack, and attempts to crack Windows passwords from hashes in the SAM file or the Active Directory (AD). It also uses dictionary and brute force attacks for generating and guessing passwords.



ıtCrack

mptly discontinued it in 2006. Later,
ssword cracking tool and re-released it in

rd cracking tool on the planet. Written strictly
luding NTLM, NTLMv2, MD5, wireless,
Oracle, MySQL, SQL Server, SHA1, SHA2, Cisco, VoIP, and many others.

Cain and Abel can crack passwords using a dictionary attack, rainbow attack, and brute force. One of its better features is the ability to select the password length and character set when attempting a brute force attack. And besides being an excellent password cracking tool, it is also a great ARP Poisoning and MiTM tool.

THC-Hydra

THC-Hydra is probably the most widely used online hacking tool. It is capable of cracking web form authentication, and when used in conjunction with other tools such as Tamper Data, it can be a powerful and effective tool for cracking nearly every type of online password authentication mechanism.

The initial help screen for Hydra.

Brutus

Brutus is an online password cracking tool that many consider the fastest online password cracker. It is free and available on both Linux and Windows, and it supports password cracking in HTTP (Basic Authentication), HTTP (HTML Form/CGI), POP3, FTP, SMB, Telnet, and other types such as IMAP, NNTP, NetBus, etc.

Brutus has not been updated in quite awhile, but it can still be useful and since it is open source, you can update it yourself. Brutus can be downloaded here.

Aircrack-Ng

In my humble opinion, **aircrack-ng** is undoubtedly the best all-around Wi-Fi hacking software available. It is capable of cracking both WEP and WPA2, and it is also capable of doing the following, among many other things.

1. Creating a Soft AP
2. Creating an Evil Twin
3. Creating a Rogue AP
4. Conducting a DOS attack against a Wi-Fi AP

It is only available for Linux and requires a bit of a learning curve to master, but you will be richly rewarded for the time spent learning it. In addition, to be most effective you will need to use an aircrack-ng compatible wireless card, so check their extensive list before buying your card. You can find more info on aircrack-ng over in my Wi-Fi hacking series.

Aircrack-ng is built into BackTrack and Kali and can be downloaded here.

Step 6

Password Cracking Hardware

Botnet

Password cracking is simply a function of brute force computing power. What one machine can do in one hour, two machines can do in a half hour. This same principle applies to using a network machines. Imagine what you can do if you could access a network of one million machines!

Some of the botnets available around the globe are more than a million machines strong and are available for rent to crack passwords. If you have a password that might take one year to crack with your single CPU, a million-machine botnet can cut that time to approximately 1 millionth the time, or 30 seconds!

GPU

GPUs, or graphical processing units, are much more powerful and faster than CPU for rendering graphics on your computer *and* for cracking passwords. We have a few tools built into Kali that are specially designed for using GPUs to crack passwords, namely cudahashcat, oclhashcat, and pyrit. Look for coming tutorials on using these tools and the GPU on your high-end video card to accelerate your password cracking.

ASIC

In recent years, some devices have been developed specifically for hardware cracking. These application-specific devices can crack passwords faster than over 100 CPUs working symmetrically.

(1) Bitfury boards by Black Arrow, (2) Butterfly Labs processor, (3) Inside the Butterfly Labs Monarch.
Images via Bitcoin Talk, CoinDesk, Gizmodo

Black Arrow Software and Butterfly Labs, among others, are now selling these devices for prices up to $1500 per.

That concludes our beginning lesson on the basics of general password cracking. Stay tuned for more lessons as we go more in-depth with specific examples of using some of the tools and methods we have just covered above.

- Follow Null Byte on Twitter, Flipboard, and YouTube
- Sign up for Null Byte's weekly newsletter

Cover image via Aurich Lawson/ArsTechnica