Advanced Password Recovery

Password-cracking programs should be used to get you, your friends or anyone else who asks for your help, out of a tight situation. For example, you may have forgotten your password and have been locked out of your own files or programs. I strongly disagree with using such programs to obtain passwords that are not for you to obtain, particularly if you are NOT doing it just to prove to your friends what a "l33t hax0r" you are. This is illegal and, more importantly from my point of view, immoral.

Many password-cracking programs work well, but quite a few of them do not. The bottom line is that it is difficult to find a decent password cracker with good features and a nice user-friendly GUI (Graphical User Interface). This fact frustrated many, including myself, but some time ago I found a number of password-crackers which I consider the best I've seen. They are a group of password crackers by Elcomsoft, available at http://www.elcomsoft.com/prs.html.

The password-crackers available at the location mentioned above are shareware, which means they require a certain amount of money to purchase a S/N (Serial Number). The limitations placed upon the shareware versions are enough to prevent you from doing any serious cracking (the limitations are mentioned at the download site). This can help keep some of the malicious "hackers" from obtaining other people's passwords, but in today's Internet society it is surprisingly easy to obtain serial numbers and program cracks for free.

At the above web site, there are password-crackers for many of the password-protected programs or files found on your normal PC, running M/S Windows. One of the best is AZPR (Advanced Zip Password Recovery) which cracks WinZip passwords. Another great one is AO2000PR (Advanced Office 2000 Password Recovery) which cracks virtually any password you may run into, while going through M/S Office files (M/S Office 97 included). AIMPR (Advanced Instant Messengers Password Recovery) is a program capable of obtaining the passwords of 17, different “Instant Messenger” programs on a local computer, in just a few milliseconds. I'll start by explaining every feature of AZPR below, and will fill in any blanks encountered on the others.

AZPR v2.0

ZIP password-encrypted file: Pretty simple. Just click browse and select the file you want cracked. Or you can type it in.
Password length options: Select the minimum and maximum password length you want it to search for. For instance, if you know the password is under 7 digits, you'll put minimum to 1 and maximum to 7.
Type of attack: Select the attack you would like it to perform. Dictionary will enter every word in a wordlist, and if the password is included in that list, you've got it. Brute-Force will try various combinations of letters, depending on what you set in the Brute-Force range options. I would recommend trying the dictionary attack first, as it takes much less time than Brute-Force. If you're in luck, you've saved time. If you're not, at least you tried.
AutoSave: Selecting this and choosing the time period to elapse between autosaves has the program save its state. For instance, if you set it to 3 minutes, it'll save it's state every 3 minutes, so if it has a problem and closes or you close it in a hurry, the next time you crack the same file you'll start from the state it was in since the last save.
Priority Options: You can select between Normal and High. If you're planning to use other programs at the same time and you're not in a real hurry then Normal is for you. But if you're just going to leave it go while you're at school or work or sleeping or whatever, then you should use High. What happens is that High uses more memory, so it cracks faster, but it slows down all other applications.
Brute-Force range options: Here you can enter what digits the program is to look for. Let's say if you know that the password was all in small letters, then you'll select "All small". If it also included numbers, then you'll select "All Digits" and so on. You can select "All Printable", which combines all the other options. You can also use "Custom Charset" if you know what letters are used in the password. Let's say you know that the password is made up only by the letters g, a, l, h, and d, then you'll set the Charset to those letters. "Start from password" helps if you know the first letter or the password. For instance, if you know it started with "h", had 6 digits and all the letters were small, then you can type in "haaaaa".

Dictionary File: If you'll use the Dictionary recovery method, then you'll have to specify which dictionary file to use (*.dic). There is such a file in the installation directory of AZPR, and it's called english.dic. This is the best dictionary file. It has almost every word you can run into in the English language. You can also have it try to capitalize the first letter of each word, or try to capitalize all the letters.
Start: Take a wild guess. If it's correct, you win a laundry machine (you're paying for it though).
Stop: Same as above.
Read setup: You will load a setup previously saved, and you'll have the same settings as they were when it was saved.
Save setup: Save the current settings.
Register: You can ask for 50-50 if you want…
Quit: Hmmm…I wonder…

AO2000PR v1.02

New/Open Project: You can save the state the program is in and load it later.
Start/Stop recovery: What it says.
IE Symbol: Clicking on that will get you the "IE Content Advisor" password, if it exists.
Encrypted Office 97 document: Open the file you want cracked.
Type of attack: You can choose from brute-force, brute-force with mask and dictionary attack. Brute-force and dictionary are explained in AZPR. Brute-force with mask will be explained further down.
Brute-force: Password length and range options are explained in AZPR. Now, masking is used if you know parts of the password. Let's say you know the password has seven digits, the first letter is "h", the forth is "8" and the last is "y". You'll leave the "starting password" field blank, and in "mask" you'll type in "h??8??y". The "?"s are the masks. You can use another mask, such as "#" whereas the entry would be "h##8##y", but you'll have to change it in the "Options" tab.
Dictionary: Most of this has already been covered in AZPR. "Mutations" will try 10 combinations of each word in the dictionary using upper and lower case.
Auto-save: It's been covered in AZPR.
Options: In priority options, "background" is AO2000PR's version of "Normal". You can set the program to log your activity, and you can clear the history. "Make backup before file changing" makes a "bak" file of a Microsoft Access database if you change the password. You can set the mask symbol, and you can set how often you want the progress bar (down below) to be updated.
Benchmark: This will calculate how many passwords your computer can enter each second.

AIMPR v1.21

Select Messenger: Click on that folder icon and select the IM (Instant Messenger) that you want. If it's on that computer, you'll have the password in a matter of seconds. That's all there is to it, actually.

Well, that's all for today. You can download all these at the location I mentioned previously, and if you do, be nice, be careful and be smart.

Galahad