macKrack
1.5.1

Release Date: 2005-09-22

email:
braden127@myrealbox.com

Summary:

MacKrack is freeware. It is a password hash brute forcer, supporting the Crypt, MD5 and SHA-1 algorithms, as well as brute forcing password-protected .dmg image files. It also now supports salted SHA-1, as implemented in OS 10.4 password hashes. It has two modes: dictionary and keyspace brute force. The brute force mode supports the lowercase alphabet, entire alphabet, and alphanumeric cracking, with a variable maximum and minimum password length of 1-10 characters.

To see an example password file and wordlist macKrack will crack, look at the very small sample wordlist and MD5 password file. The sample dictionary is not intended for practical use, since it is only 6k.

Looking for a good wordlist/dictionary?
Check out the extensive collection at
http://packetstormsecurity.nl/Crackers/wordlists/

Version History:
v1.5.1
• Fixed append characters and increased to 4
• Fixed numerous crashes (pressing cancel and incorrectly reading dictionary).

v1.5
• Added support for salted SHA1 hashes (used by OS 10.4).
• Added OS 10.4 hash extraction.

v1.4.3
• Rewrote DMG cracking to be much faster, resulting in a ridiculous speed increase (about 15 times faster).
• Fixed various bugs reported by beta testers. Thanks to mac-attack, Kyle, and ___ for the bug reports.
• Fixed bug in regular hash cracking that results in significant performance boost.
• Added performance stats at end of cracking session.

v1.4

• Rewrote DMG cracking to directly connect to DiskImages framework instead of forking hdiutil (50% speed increase)

v1.3
• Added entirely new support for .dmg files
• Added a function to print the current Open Firmware security password in the Passwd utility section.
• Added cool append fuction that will append up to 3 characters (digits or ascii non-letter characters to the end of dictionary words)
• Added support for other characters in Keyspace mode instead of limiting to only 3 options
• Added Estimated Time Remaining to cracking
• Innumerable under-the-hood changes to increase speed and stability and found and fixed some memory leaks I had not caught

v1.22
• Base 64 decoding as well as encoding for the algorithms that can be brute forced
• Dictionary Concatentation: lump together several smaller dictionaries)
• Dictionary Permutation: permute each word in a dictionary up to 20 times, creating a dictionary 20 times larger than the original.
• Mac OS X Password extraction: extract your Mac's passwd information from the netinfo database. This will not extract the root password. This feature makes it very easy to brute force all the user accounts on a Mac.
• Speed optimization over version 1.1.
• Version 1.22 seriously optimizes speed over previous.

Information:
DMG brute-forcing: Still slow. I hope to reverse engineer the framework further to improve speed at some point.

Append: For example, if you select 3 digits, it will try everything from the original word in the dictionary to wordxxx where the x's are all possible combinations of digits or characters. Keep in mind that if you have a dictionary of one thousand words, appending up to 3 digits will be about 10*10*10+10*10+10=1110 times slower. But at least it's faster than a brute force. It's sort of a combination of a dictionary attack and a brute force, and is often effective (who hasn't used passwords that are just dictionary words followed by a couple digits...).

Session files: Quitting while cracking or paused will cause macKrack to prompt you to save a session file. It isn't recommended for you to edit this session file, but I couldn't stop you if I tried. SECURITY NOTICE: Passwords already cracked are saved in CLEARTEXT in session files. If this is a security concern for you, you should encrypt it between cracking. All older session files are not compatible with version 1.3.

Password extraction feature: If you're having a problem with it, just restart the application and press it again, but this shouldn't be an issue. 10.2 passwords must be cracked using the Crypt algorithm, while 10.3 hashes need to be cracked with the SHA1 algorithm. Oh yeah, and I mention that 10.2 passwords might exist on 10.3 systems. To elaborate, if you update your system from 10.2 to 10.3, you'll still have the old 10.2 passwords. Email me with any questions/comments regarding this feature.

Context:
Salted SHA1 hashes are 48 characters where the first 8 characters make up a 32 bit salt value. They are used for the first time in OS 10.4 Tiger hashes. Thanks to Androto for helping me figure this out.

The MD5 algorithm is often used in web applications to hide passwords in transit, or to store passwords in some databases. However, more modern web applications combine MD5 hashing with other techniques to make their security unbreakable, such as salts, or a challenge mechanism. This application will NOT crack hashes made using these advanced measures, only standard MD5 hashes. MD5 hashes must be 32 characters long.

SHA-1 hashes are also used sometimes to encrypt passwords. For some reason this hash isn't constant when there are more than about 60 characters in the string. But, if you're using this to crack passwords, that shouldn't be a concern. SHA-1 hashes are 40 characters long.

Crypt hashes are used commonly to encrypt passwords on Unix-based operating systems, such as the Mac you're using. Crypt hashes are 13 characters long, the first two characters being the salt used to encrypt the password, and the remaining 11 being the encryption.

Base64 is very often used in transit by website deployments to obfuscate a password, but since it's not actually encryption, it's trivial to decode. This is a useful tool for network snoopers. It is not intended to decode base64 encoded files.

Password Files:
Password files can either be a list of passwords, or Unix-style password files. Unix-style password files consist of lines of the following format:
username:password:other stuff mackrack doesn't care about

Email me with questions/comments/bug reports.
-Braden