Cracking Zip Password Files

//////////*1000+ HACKING TRICKS & TUTORIALS - ebook By Mukesh Bhardwaj Blogger - Paid Version - only @ TekGyd | itechhacks | Mukeshtricks4u*///////

Tut On Cracking Zip Password Files..

What is FZC? FZC is a program that cracks zip files (zip is a method of compressing multiple files into one smaller file) that are password-protected (which means you're gonna need a password to open the zip file and extract files out of it). You can get it anywhere - just use a search engine such as altavista.com.

FZC uses multiple methods of cracking - bruteforce (guessing passwords systematically until the program gets it) or wordlist attacks (otherwise known as dictionary attacks. Instead of just guessing passwords systematically, the program takes passwords out of a "wordlist", which is a text file that contains possible passwords. You can get lots of wordlists at www.theargon.com.).

FZC can be used in order to achieve two different goals: you can either use it to recover a lost zip password which you used to remember but somehow forgot, or to crack zip passwords which you're not supposed to have. So like every tool, this one can be used for good and for evil.

The first thing I want to say is that reading this tutorial... is the easy way to learn how to use this program, but after reading this part of how to use the FZC you should go and check the texts that come with that program and read them all. You are also going to see the phrase "check name.txt" often in this text. These files should be in FZC's directory. They contain more information about FZC.

FZC is a good password recovery tool, because it's very fast and also support resuming so you don't have to keep the computer turned on until you get the password, like it used to be some years ago with older cracking programs. You would probably always get the password unless the password is longer than 32 chars (a char is a character, which can be anything - a number, a lowercase or undercase letter or a symbol such as ! or &) because 32 chars is the maximum value that FZC will accept, but it doesn't really matter, because in order to bruteforce a password with 32 chars you'll need to be at least immortal..heehhe.. to see the time that FZC takes with bruteforce just open the Bforce.txt file, which contains such information.

FZC supports brute-force attacks, as well as wordlist attacks. While brute-force attacks don't require you to have anything, wordlist attacks require you to have wordlists, which you can get from www.theargon.com. There are wordlists in various languages, various topics or just miscellaneous wordlists. The bigger the wordlist is, the more chances you have to crack the password.

Now that you have a good wordlist, just get FZC working on the locked zip file, grab a drink, lie down and wait... and wait... and wait...and have good thoughts like "In wordlist mode I'm gonna get the password in minutes" or something like this... you start doing all this and remember "Hey this guy started with all this bullshit and didn't say how I can start a wordlist attack!..." So please wait just a little more, read this tutorial 'till the end and you can do all this "bullshit".

We need to keep in mind that are some people might choose some really weird passwords (for example: 'e8t7@$^%*gfh), which are harder to crack and are certainly impossible to crack (unless you have some weird wordlist). If you have a bad luck and you got such a file, having a 200MB list won't help you anymore. Instead, you'll have to use a different type of attack. If you are a person that gives up at the first sign of failure, stop being like that or you won't get anywhere. What you need to do in such a situation is to put aside your sweet xxx MB's list and start using the Brute Force attack.

If you have some sort of a really fast and new computer and you're afraid that you won't be able to use your computer's power to the fullest because the zip cracker doesn't support this kind of technology, it's your lucky day! FZC has multiple settings for all sorts of hardware, and will automatically select the best method.

Now that we've gone through all the theoretical stuff, let's get to the actual commands.

Bruteforce

The command line you'll need to use for using brute force is:

fzc -mb -nzFile.zip -lChr Lenght -cType of chars

Now if you read the bforce.txt that comes with fzc you'll find the description of how works Chr Lenght and the Type of chars, but hey, I'm gonna explain this too. Why not, right?... (but remember look at the bforce.txt too)

For Chr Lenght you can use 4 kind of switches...

-> You can use range -> 4-6 :it would brute force from 4 Chr passwors to 6 chr passwords
-> You can use just one lenght -> 5 :it would just brute force using passwords with 5 chars
-> You can use also the all number -> 0 :it would start brute forcing from passwords with lenght 0 to lenght 32, even if you are crazy i don't think that you would do this.... if you are thinking in doing this get a live...
-> You can use the + sign with a number -> 3+ :in this case it would brute force from passwords with lenght 3 to passwords with 32 chars of lenght, almost like the last option...

For the Type of chars we have 5 switches they are:

-> a for using lowercase letters
-> A for using uppercase letters
-> ! for using simbols (check the Bforce.txt if you want to see what simbols)
-> s for using space
-> 1 for using numbers

Example:
If you want to find a password with lowercase and numbers by brute force you would just do something like:

fzc -mb -nzTest.zip -l4-7 -ca1

This would try all combinations from passwords with 4 chars of lenght till 7 chars, but just using numbers and lowercase.

*****
hint
*****

You should never start the first brute force attack to a file using all the chars switches, first just try lowercase, then uppercase, then uppercase with number then lowercase with numbers, just do like this because you can get lucky and find the password much faster, if this doesn't work just prepare your brain and start with a brute force that would take a lot of time. With a combination like lowercase, uppercase, special chars and numbers.

Wordlis

Like I said in the bottom and like you should be thinking now, the wordlist is the most powerfull mode in this

program. Using this mode, you can choose between 3 modes, where each one do some changes to the text that is in the wordlist, I'm not going to say what each mode does to the words, for knowing that just check the file wlist.txt, the only thing I'm going to tell you is that the best mode to get passwords is mode 3, but it takes longer time too.
To start a wordlist attak you'll do something like.

fzc -mwMode number -nzFile.zip -nwWordlist

Where:

Mode number is 1, 2 or 3 just check wlist.txt to see the changes in each mode.
File.zip is the filename and Wordlist is the name of the wordlist that you want to use. Remember that if the file or the wordlist isn't in the same directory of FZC you'll need to give the all path.

You can add other switches to that line like -fLine where you define in which line will FZC start reading, and the -lChar Length where it will just be read the words in that char length, the switche works like in bruteforce mode.
So if you something like

fzc -mw1 -nztest.zip -nwMywordlist.txt -f50 -l9+

FZC would just start reading at line 50 and would just read with length >= to 9.

Example:

If you want to crack a file called myfile.zip using the "theargonlistserver1.txt" wordlist, selecting mode 3, and you wanted FZC to start reading at line 50 you would do:

fzc -mw3 -nzmyfile.zip -nwtheargonlistserver1.txt -f50

Resuming

Other good feature in FZC is that FZC supports resuming. If you need to shutdown your computer and FZC is running you just need to press the ESC key, and fzc will stop. Now if you are using a brute force attack the current status will be saved in a file called resume.fzc but if you are using a wordlist it will say to you in what line it ended (you can find the line in the file fzc.log too).
To resume the bruteforce attack you just need to do:

fzc -mr

And the bruteforce attack will start from the place where it stopped when you pressed the ESC key.
But if you want to resume a wordlist attack you'll need to start a new wordlist attack, saying where it's gonna start. So if you ended the attack to the file.zip in line 100 using wordlist.txt in mode 3 to resume you'll type

fzc -mw3 -nzfile.zip -nwwordlist.txt -f100

Doing this FZC would start in line 100, since the others 99 lines where already checked in an earlier FZC

session.

Well, it looks like I covered most of what you need to know. I certainly hope it helped you... don't forget to read the files that come with the program