RESEARCH PAPER DRAFT

Topic : An implementation and its evaluation of password cracking tool – Fcrackzip and Crunch.

Introduction

Fcrackzip is a fast password cracker partly written in assembler. It is able to crack password protected zip files with brute force or dictionary-based attacks, optionally testing with unzip its results. Fcrackzip searches each zip file given for encrypted files and tries to guess the password. All files must be encrypted with the same password, the more files you provide, the better. Have you ever mis-typed a password for unzip? Unzip reacted pretty fast with ´incorrect password´, without decrypting the whole file. While the encryption algorithm used by zip is relatively secure, PK made cracking easy by providing hooks for very fast password-checking, directly in the zip file. Crunch is a wordlist generator. It's a password attack tool in Kali Linux. It is mainly used for Dictionary Attack. Here you can specify a standard character set or number or symbols. It can generate all possible combinations and permutations.

Tools Involved in Research

Fcrackzip : Fcrackzip is a fast password cracker partly written in assembler. It is able to crack password protected zip files with brute force or dictionary-based attacks, optionally testing with unzip its results. Fcrackzip searches each zip file given for encrypted files and tries to guess the password. All files must be encrypted with the same password, the more files you provide, the better. Have you ever mis-typed a password for unzip? Unzip reacted pretty fast with ´incorrect password´, without decrypting the whole file. While the encryption algorithm used by zip is relatively secure, PK made cracking easy by providing hooks for very fast password-checking, directly in the zip file.

Crunch : Crunch is a wordlist generating tool that comes pre-installed with Kali Linux. It is used to generate custom keywords based on wordlists. It generates a wordlist with permutation and combination. We could use some specific patterns and symbols to generate a wordlist. Wordlists are a key part of brute force password attacks. For those readers that aren't familiar, a brute force

password attack is an attack in which an attacker uses a script to repeatedly attempt to log into an account until they receive a positive result. Brute force attacks are fairly overt and can cause a properly configured server to lock out an attacker or their IP. This is the point of testing the security of log in systems this way. Your server should ban attackers that attempt these attacks, and should report the increased traffic. Kali Linux comes with a powerful tool for creating wordlists of any length. It's a simple command line utility called Crunch. It has simple syntax and can easily be adjusted to suit your needs. Beware, though, these lists can be very large and can easily fill an entire hard drive.

Parameters Used for Finding Password

Rate of Process : The time taken to find the password will depend on the wordlist, if dictionary attack is used and in bruteforce attack the time depends on the password length,.

Wordlist : The file used as a dictionary for matching all the words in the dictionary with the password protected pdf file.

Metadata : The hash value of the password protected file is stored in the metadata of the pdf file.

Hash : The hash value of the password is find using the john the ripper tool.

Summary

Fcarckzip is an open source tool, and it can be used for finding the password hash of the zip file and using that hash value we can find the password of the protected zip file. Crunch is and pre-requisite tool for using Fcrackzip, using this tool we can create different types of dictionary file for attacking using dictionary attack. The another attack possible is bruteforce attack and it will take more time compared to dictionary attack because it uses all the password combinations to find the password of the zip file.