RESEARCH PAPER DRAFT

Topic : An implementation and evaluation of pdf password cracking using John The Ripper and Crunch.

Introduction

John the Ripper is a free and Open Source software, distributed primarily in source code form. If you would rather use a commercial product, please consider John the Ripper Pro, which is distributed primarily in the form of "native" packages for the target operating systems and in general is meant to be easier to install and use while delivering optimal performance. Using this tools we can generate wordlists and find the password of the password protected pdf files. John the Ripper is a password security auditing and password recovery tool available for many operating systems

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

John The Ripper : John the Ripper (JtR) is one of the hacking tools the Varonis IR Team used in the first Live Cyber Attack demo, and one of the most popular password cracking programs out there. It supports several common encryption technologies out-of-the-box for UNIX and Windows-based systems. (ed. Mac is UNIX based). It autodetects the encryption on the hashed data and compares it against a large plain-text file that contains popular passwords, hashing each password, and then stopping it when it finds a match. Simple.

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

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

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

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

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,.

Summary

John the Ripper is an open source tool, and it can be used for finding the password hash of the pdf file and using that hash value we can find the password of the protected pdf. Crunch is and pre-requisite tool for using John th Ripper, 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 combination