Password Cracking

Introduction

The use of strong passwords plays a crucial role in access control. It is tempting for the end user to select simple easy to remember passwords, or employ techniques such as appending an incrementing number to the end of their password. Unfortunately, passwords generated using such approaches are easy to crack.

Review the lecture notes on dictionary and brute force attacks. Skim read the background on dictionary attacks from the link below:

https://crackstation.net/hashing-security.htm

Task 1 – Online Password Cracker

Use the online password cracker (https://crackstation.net/) to crack each of the passwords below:

- c11083b4b0a7743af748c85d343dfee9fbb8b2576c05f3a7f0d632b0926aadfc
- 08eac03b80adc33dc7d8fbe44b7c7b05d3a2c511166bdb43fcb710b03ba919e7
- e4ba5cbd251c98e6cd1c23f126a3b81d8d8328abc95387229850952b3ef9f904
- 5206b8b8a996cf5320cb12ca91c7b790fba9f030408efe83ebb83548dc3007bd

Create some dummy passwords hashes of your own using the following command in the Linux terminal:

```
echo -n "password" | md5sum
```

Replace "password" with your dummy password, then paste the resulting hash value into the online password cracker, and see if it can crack your dummy password.

Increase the length and complexity of your dummy password, and repeat the process. Continue increasing the length and complexity until the password cannot be cracked. Reflect on why they is the case.

Task 2 – John the Ripper

John the Ripper is a password cracking recovery that can be used to recover passwords using brute force or dictionary techniques. For this lab session we will use the built-in dictionary. You may need to supply a more comprehensive dictionary when using this tool in the field.

Boot up your Metasploitable virtual machine and login.

1. Switch to root using the following command
    a. sudo su
2. The shadow file contains a list of user names, and hashed passwords. Copy the shadow file to the directory containing john the ripper using the following command
    a. `cp /etc/shadow /opt/john/run`
3. Switch to the directory containing john the ripper and the shadow file and view the contents of the file using the commands below:
    a. `cd /opt/john/run`
    b. `cat shadow`
4. Review the documentation on the /etc/shadow file from the link below, it explains the format of the data stored in the file.
    a. https://www.cyberciti.biz/faq/understanding-etcshadow-file/
5. Review the manual for John the Ripper to determine how it works, and what options are available:
    a. http://www.openwall.com/john/doc/OPTIONS.shtml
6. Crack the passwords using commands below:
    a. `./john shadow- --show`

Task 3 – Python Password Cracking

You have been provided with a dictionary file (Dictionary.txt), and a file containing two md5 hashed passwords (HashedPasswords.txt).

Use either md5sum to determine the passwords that match the hashes in HashedPasswords.txt

Consider the process you employed and write down the steps. e.g. opened the dictionary file, read the first line from the file, created a hash of the first line, etc.

Create a script that can crack the passwords stored in HashedPasswords.txt using the Dictionary.txt file.

To accomplish this task, you will need review the documentation below:

File open - https://docs.python.org/2/tutorial/inputoutput.html#reading-and-writing-files

Hashlib - https://docs.python.org/2/library/hashlib.html

Dictionary - https://docs.python.org/2/tutorial/datastructures.html#dictionaries

Rstrip - https://docs.python.org/2/library/string.html

An example script (ExampleCode.py) has been provided this demonstrates how to use each of the libraries above to develop you password cracker.

Extended Task - KeePass

http://keepass.info/

Download and setup KeePass on either your laptop or mobile phone (Available in App stores), setup a secure password wallet and reset any of your existing weak or duplicate passwords. Use KeePass to generate and store strong passwords.