**Password Cracking**

By: Matt Lazeroff

**Software:**

1. Hashcat – (Windows/Linux/Mac)
2. Ophcrack – (Windows/Linux/Mac)
3. Md5sum/sha256sum - (Linux/Available as web applications)

**Suggested Password Dictionaries:**

1. Rockyou.txt
2. Windows XP / Vista Tables (available at ophcrack.sourceforge.net)

**Basis:**

In modern systems involving password authentication, systems “hash” user passwords for storage, instead of saving plain-text passwords. Passwords are “hashed” using a cryptographic hash function which takes in the password as an input and outputs some data of a fixed size. Examples of these hash functions include MD5 and SHA256. These functions are designed to be one-way, in the sense that you can only go from an input to a hashed output, not vice-versa. While the ideal output for some input would be unique, depending on the hashing function, it may be possible to have two different inputs with the same outputted hash.

MD5 Hash Example:

Input – “kobRAkai”

Output – “159137bd1e0085ec925f5ac55d3fdedc”

The basis of password cracking is using hashing a wide-variety of inputs to generate a hash that matches the password you are trying to crack. There are various password cracking “attacks” that exist:

**Brute Force –** Iterating through every possible composition of characters. The slowest possible method. For an 8-character password that has only letters and numbers, the set of possible passwords would be 21,400,000,000,000,000 passwords - (

**Dictionary Attack –** Uses a list of passwords and individually hashes each one to see if it matches the password hash to be cracked.

**Hybrid Attack –** Uses variations on the passwords in a password dictionary

**Rainbow Table Attack -** A table that contains passwords and their hashes already computed. All that needs to be done is do a lookup with the password hash.

**Installing the Software:**

**1. Hashcat:**

* 1. **Linux:** sudo apt install hashcat
     1. If your distribution doesn’t have a package for hashcat, follow the instructions for Windows below. You will need to “chmod +x hashcat64.bin”. Then you can execute hashcat as ./hashcat64.bin
  2. **Windows:**

1. Download “hashcat binaries” from hashcat.net
2. Unzip the folder to a directory
3. Use Powershell to navigate to the directory you unzipped to

Example:

* + - * 1. Hashcat directory is on desktop
        2. Type in powershell terminal: cd C:\Users\<user\_name>\Desktop\hashcat-4.2.1\

1. To see if you were successful, type: “./hashcat64.exe --help”
   1. If the really long usage message appears you did it right

**2. Ophcrack:**

* 1. **Linux:** sudo apt install ophcrack
  2. **Windows:  
     1.** Download the Windows zip off ophcrack.sourceforge.net

**2.** Unzip into a directory

**3.** Enter the “x64” directory

**4.** Run ophcrack.exe