Tutorial 1: Simple Dictionary Attack

1. Go to the pwcrack/1 directory
2. See problemMD5.txt
   1. We are instructed to find the passwords that match the MD5 hashes
3. We will be using hashcat with the rockyou.txt dictionary file

Process:

1. Create a hash list with the hashes
   1. Each hash must be separated by a new line
      1. Can be saved in a .txt file
2. A picture containing text

   Description generated with high confidenceCreating the hashcat instruction
   1. Hashcat has many attack modes, we will be dictionary mode which is mode 0
      1. This is denoted by the “-a” switch
      2. Other attack modes can be found with “hashcat --help”
   2. Hashcat defaults to MD5 hashes, so we don’t need to specify a hash mode
      1. This can be specified with the “-m” switch
      2. Other hash modes can be found with “hashcat --help”
   3. A dictionary attack command has the following syntax:
      1. Hashcat -a 0 -m <hash\_mode> <hash\_file> <dictionary\_file>
      2. A close up of a sign

         Description generated with high confidenceOurs: hashcat -a 0 md5.txt rockyou.txt
   4. A screenshot of text

      Description generated with very high confidenceThe output should look something like this:
   5. As you can see, it displays the hashes with their corresponding cracked passwords

Try on Your Own: The “problemSHA256.txt” file has a similar problem, only this time has SHA256 hashes. Use the rockyou.txt and hashcat to break the passwords.

\*Hint – Use the “-m” switch\*