Goldman Sachs FinTech Engineering Virtual Experience Program by Forage  
  
Crack the leaked database task

MY LEARNINGS  
  
Skills acquired: Basics of cryptography, password cracking.  
Software used: Hashcat.  
  
Cryptography works on several attacks and several hash algorithms.  
When a user enters a password, its hashed value is saved in the database. This hashed value is of a fixed length depending on the hash function used. And everytime the password is entered, the same hash will be produced, it will be matched with the hash stored in the database corresponding to the username when the account was created. If the match is found, access is granted.  
In order to Crack passwords, if the database of encrypted hashes is available, methods are employed to generate a hash that matches with the encrypted hash. Usually, attacks can be  
1. Dictionary attacks- in this, a wordlist of some of the most popular and commonly used passwords in plain text is used. The 'rockyou.txt' is mostly used. This list was released when the database of the website Rockyou was compromised and passwords were revealed. Each word on the list is hashed in the algorithm chosen and matched with the hash to be decrypted.  
2. Brute force- every character, 26 upper case 26 lower case, 10 digits and 33 special characters are brute forced and every combination is tried, hashed and matched.  
3. Combination- a combination of two wordlists is made, hashed and matched.  
  
The hashed algorithms are-  
1. MD5- message digest. This hashing algorithms is weak and can be cracked easily. In the task I was assigned, all passwords were md5 and 13 out of 19 were broken in one go.  
2. SHA1 and SHA 2- better encryption algorithms. Less likely to be breached.  
  
In Hashcat, the attack mode is chosen, the hashed algorithm is chosen (-a 0 means dictionary attack. -m 0 means MD5 is used and -m 100 means SHA)  
Following this, the location of the file of hashes is to decrypted is mentioned and the location of the wordlist chosen is to be mentioned.  
In case there are rules as well, then following the location of the wordlist, mention -r and enter the rule. Most used is best64 rule.  
  
The decryption is performed and the value is revealed.