1. Password Dump: Yahoo

The Yahoo Password Dump contains a password.file dump. The password dump in this file was easy to understand and process to retrieve the maximum number of passwords from the list. It was in the format ‘`user_id:user_name:clear_passwd`’.

Working:

The passwords were clearly not hashed or in any other encrypted form. It was a matter of simple strip and split to retrieve just the password from the dump. Strip is used to remove any leading or trailing whitespaces whereas every line gets split into small strings when split at every ‘:’ (colon). Redundant data at the start of the dump file was removed. And thus, 1000 passwords were retrieved from the Yahoo Dump.

Attachments:

- yahoo.py
- yahoo_passwords.txt

2. Password Dump: LinkedIN

The LinkedIN Dump includes file SHA1.txt which is in a hashed format. It has 40 characters per line of password. One of the most common technique of hashing used for a 40 character long is SHA1. To crack these passwords, dictionary attack is used. In dictionary attack, a list of passwords is encrypted using a hashing algorithm (SHA1 is this case). Subsequently, every line in already encrypted file SHA1.txt is compared with the encrypted password list file to find matches.

Working:

Though there are lot of dictionaries and list of common passwords available online, an attempt of creating a new customized password list has been tried. It uses two help lists of ‘Commonly used English words’ and ‘Common First Names’ each containing few thousand words. The new password list comprises of various combinations of these words, numbers and few special characters selected randomly. Sometimes these words, numbers and characters are joined randomly (For example: word + number + character + number -> mary1!4) and sometimes they are sequentially joined (For example: word+character+number+number -> john@25). Few of the randomly generated passwords have first letter capitalized and few have all letters capitalized.

So, here not all possible combinations are generated like in Brute Force but few best password combinations are generated based on the recent trends of password formats. Thus, after few trail and error methods and appending the passwords on every run of the script, a few passwords were retreived with the help of the customized password list.

The custom passwords generated are still furthered modified just before converting to hash value by techniques like converting strings to Upper Case, Lower Case, First Letter Upper Case or randomly capitalizing letters in the password. Thus, the custom dictionary doesn’t increase in size because this action happens at runtime.

This helps to reach almost 1000 passwords with ypur very own customized password list.

Attachments:

- linkedin.py
- linkedin_passwords.txt
- password_customlist.py
  - → Generates: password_custom.txt

3. Password Dump: Formspring

In the Formspring Password Dump, each hashed password is a 64-character long hash. SHA256 is the hashing algorithm that deals with a 64-character long hash. It is that long because it includes something called as Salts. Salts are random strings generated for passwords that are appended to the passwords. The total string with the original password and salt is then encrypted to get a 64-character hash value. Salts help when there are same passwords for different people. But then salts when appended with different combinations give unique hash values.

Working:

The working of this script is same as that of the Linkedin script. Customized passwords are generated using the same method explained above.

Passwords generated through the custom generation method are appended with Salts. The script adds two random salts before the passwords from the custom list. The passwords are also modified with changes cases of the letters in the passwords. They are then hashed to get the final values to be compared with the Formspring Dump.

If a hash value matches, it is printed in the output file. Repetition was observed in the Dump file.

Attachments:

- formspring.py
- formspring_passwords.txt
- password_customlist.py
  - → Generates: password_custom.txt

4. Comparison of Techniques

- Password Cracking of Yahoo Dump was very easy and fast as compared to LinkedIN and Formspring.
- Formspring (SHA256) was much slower because computing took time because of additional salts.
- Generating customized passwords seem to be more efficient and intelligent than Brute Force method because of the randomness property used.
- More passwords can be cracked if the customized password list is larger and if more combinations are used.