Chapter 4 Password Storage

Using Hashes to Store Passwords

A common usage scenario for hashes is to encode passwords for storing in a database. With the advent of modern processors and graphical processing units (GPUs), it is not recommended you take this approach as hashes can be brute force attacked or attacked by using rainbow tables.

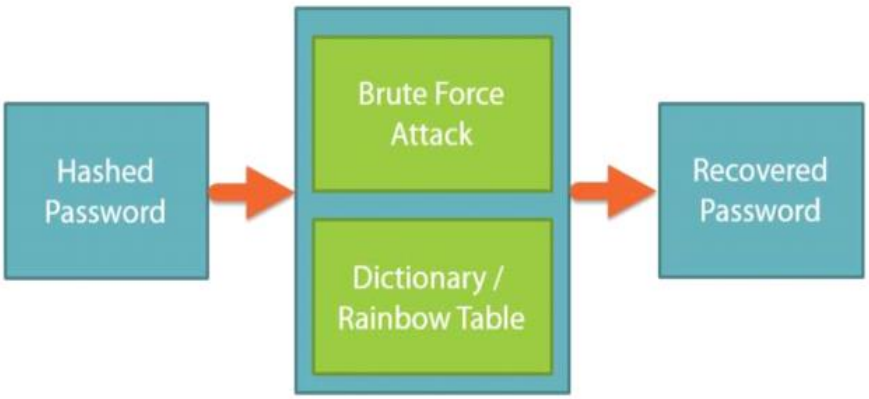

Figure 6: Hashed passwords can be brute force attacked or attacked using rainbow tables

A better approach is to increase the entropy of the password being attacked by making the password harder to recover. This can be done by adding a salt onto the password before hashing.

Note: A rainbow table contains precomputed hashes for different combinations of messages. These tables are used to determine the original plaintext from an already computed hash value. Rainbow tables can be many gigabytes in size and they greatly speed up attacks to recover the original value of a hash.