Ataque LOOKUP TABLE

D1

-Las lookup tables son un conjunto de contraseñas asociadas a su hash correspondiente.

- Es una técnica de TMTO (Time-Memory tradeoff o compensación de tiempo-memoria) para consumir menos recursos de CPU.

-Es otra manera de hacer un ataque de fuerza bruta, solo que esta vez se obtienen los valores primero, luego se almacenan y se hacen consultas. Es un intercambio de memoria y tiempo de cómputo.

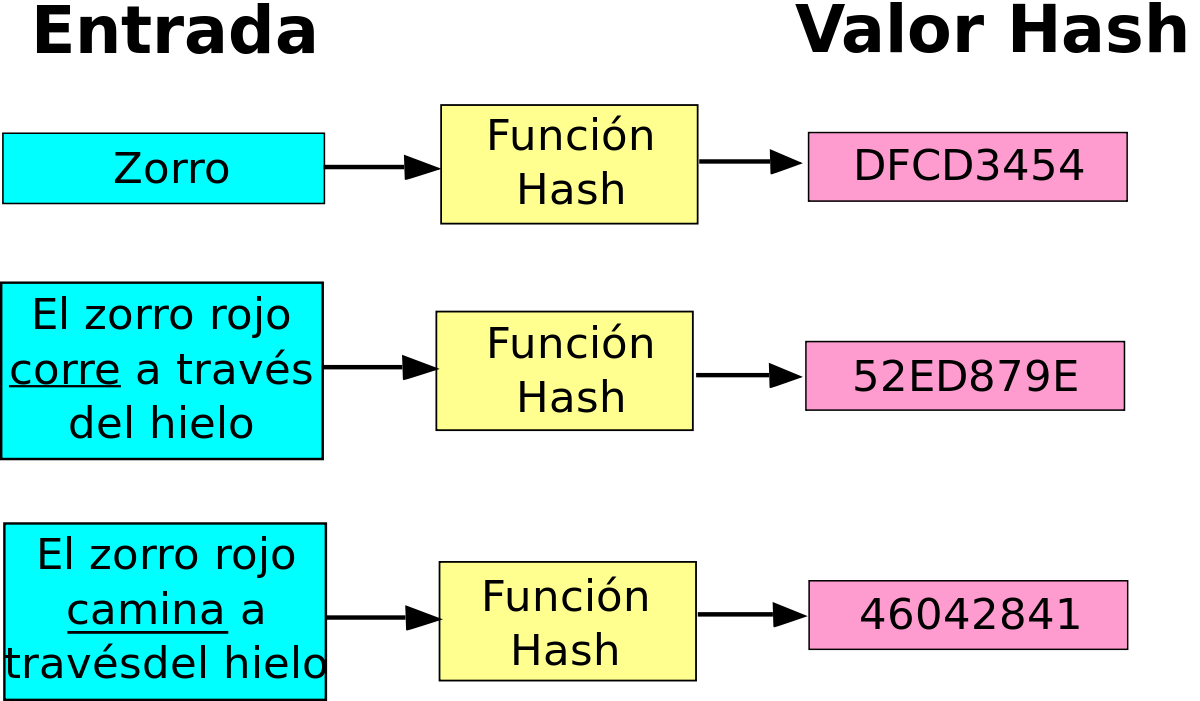
-Son técnicas que permiten que el tiempo de cómputo se reduzca a cambio del uso de memoria.

Estas tablas son rápidas en tiempo, pero pesadas en memoria, por eso las lookup tables se preparan antes para llegar a poder ser capaces de obtener la contraseña de varios hashes, siempre y cuando la contraseña se encuentre entre el conjunto de inputs escogidos

D2

- hash: función criptográfica -> es un algoritmo matemático que transforma cualquier bloque de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

Entonces la función hash recibe el input del dominio del texto que son las contraseñas.



D3

Otra versión de las lookup table son las reverse lookup table:

-Las reverse lookup table se basan al igual que las lookup table en pre computar un conjunto de valores hash. La diferencia principal entre las dos técnicas es el método de búsqueda, en el caso de las reverse lookup table se escoge el hash del que se quiere obtener el valor inicial y la búsqueda en la tabla se hace buscando ese hash, en vez de ir buscando fila a fila de forma secuencial en la tabla.

- Entonces mediante reverse lookup table y lookup table se pueden realizar ataques a los hash, para obtener el valor original de la contraseña.

D4

Problemas con contraseñas que facilitan ataques de lookup table:

-Cuando la mayoría de las contraseñas son similares, o a más de una persona se le ha ocurrido, por tanto, son susceptibles a distintos ataques.

-Conjuntos de contraseñas ya han sido comprometidas y aun así dentro de ese conjunto pueden encontrarse contraseñas que un usuario utilice actualmente.

Hash:

<https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/>

inf lookup table

<https://core.ac.uk/download/pdf/288501963.pdf>