¿CUAL ES EL ÚNICO RESULTADO QUE NO CONTIENE NÚMEROS?

1. El nombre del archivo.txt está relacionado con una función de hash criptográfica en particular.

2. John The Ripper permite seleccionar el tipo de función criptográfica. Es aconsejable utilizar el comando john --help para más información.

3. Seleccionando un diccionario, como rockyou, se agiliza el proceso de john.

Nota

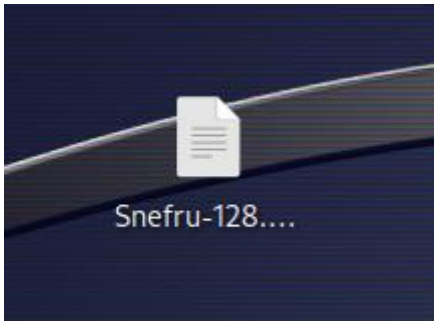
Con el programa John the Ripper, un diccionario, (en este caso utilizaremos “rockyou”) y el formato de los hashes podemos obtener resultados.

Referencias

Las tablas arcoíris o tablas Rainbow son tablas de consulta que ofrecen un compromiso espacio-tiempo para obtener claves en texto simple a partir del resultado de una función de hash. Cualquier sistema informático que requiera una autenticación por contraseña debe contener una base de datos de contraseñas, ya sea ordenada o en texto plano, y existen diversos métodos para el almacenamiento de dichas contraseñas. Debido a que las tablas son vulnerables al robo, el almacenamiento de la contraseña en texto llano es peligroso. Por lo tanto, la mayoría de las bases de datos almacenan un hash criptográfico de la contraseña del usuario en la base de datos. En un entorno así, nadie, incluyendo la propia autenticación de sistema puede determinar cuál es la contraseña del usuario simplemente observando el valor almacenado en la base de datos. En cambio, cuando un usuario introduce su contraseña para autenticarse, se calcula el hash de la contraseña introducida y se compara con el valor almacenado para ese usuario (que fue hash antes de ser almacenado). Si los dos valores hash coinciden, se concede el acceso. Una persona que tenga acceso a la tabla de contraseñas no puede simplemente copiar la entrada de la base de datos del usuario para obtener acceso (utilizar el hash como una contraseña sería, por supuesto, un error ya que el sistema de autenticación haría un hash por segunda vez, produciendo un resultado que no coincide con el valor almacenado). Con el fin de obtener la contraseña de un usuario, hay que encontrar una contraseña que produce el mismo valor hash. Las tablas arcoíris son una herramienta que se ha desarrollado en un esfuerzo por obtener una contraseña mirando solamente a un valor hash. Las tablas de arcoíris no siempre son necesarias, ya que existen métodos más simples de reversión de hash disponible. Como ataques de fuerza bruta y ataques de diccionario que son los métodos más simples disponibles, sin embargo, estos no son adecuados para sistemas que utilizan contraseñas largas, debido a la dificultad de almacenar todas las opciones disponibles. Para abordar esta cuestión de la escala, se generaron tablas de búsqueda inversa que almacena sólo una pequeña selección de los hashes que cuando se invierte podría generar contraseñas de cadenas largas de texto. Aunque la búsqueda inversa de un hash en una tabla encadenada llevará más tiempo de cálculo, el tiempo de búsqueda en la tabla en sí misma puede ser mucho menor, por lo que los hashes

de las contraseñas más largas se pueden almacenar. Las tablas arcoíris son un refinamiento de esta técnica de encadenamiento y proporcionan una solución a un problema llamado «colisiones en cadena».

Primero descargamos el archivo a desencriptar:



Vemos su contenido:

```
1 15b38e865ee1ddefda955939d0bd5c8e
2 337605c06242c094d64de46e2926fbc6
3 7548af65aca74df277e75a966fb68c23
4 10d0a3f80aa1216d13643e26046c164a
5 416c46988325682c379a0998412f39ea
6 74c3fe91c70fbae5eb2bd35e1825da19
7 8b15f1947bd0eb53ebc682a38de89ef1
```

Después utilizando John the Ripper desciframos el archivo:

```
┌──(root㉿kali)-[~/Downloads]
└─# john --format=SNEFRU-128  --wordlist=rockyou.txt Snefru-128.txt
Using default input encoding: UTF-8
huckleberry      (?)
0000099999       (?)
MTBC4549879      (?)
MSrL323628       (?)
9813485*ana      (?)
young_mike32@yahoo.com (?)
Using default input encoding: UTF-8
Loaded 7 password hashes with no different salts (Snefru-128 [32/64])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
```

Obteniendo así las contraseñas cifradas con SNEFRU-128

Nos fijamos en la lista de contraseñas obtenidas y concluimos que la única que no posee números es “huckleberry”.