Unos cálculos ligeros estimativos sobre tiempos de crackeado de passwords hasheadas

¿ Cuánto tiempo es un billón de segundos ?

- - - - - - - - - - - - - -

Supongamos que podemos construir una password como máximo de 10 caracteres, utilizando solo letras sin distinguir mayúsculas de minúsculas (26 letras)

El número de combinaciones es 26 ** 10 (se llaman variaciones , no combinaciones)

(si fueran números decimales y tenemos 3 dígitos son 10 **3, 5 dígitos son 10 ** 5 , etc etc)

26**10 cuánto es ¿? Google dice --> 1.411671e+14

Si tenemos una máquina con un programa capaz de calcular hashes a una velocidad de

10 GH /s . - que no es una máquina especializada, las hay que llegan a 300 GH/s.

Sería capaz de calcular los hashes de las 26**10 combinaciones en . . . .

1.411671e+14 / 10 .000.000.000 -- > 14.116 segundos

(en realidad el tiempo medio para encontrar el hash sería la mitad, estadísticamente)

14116 / 3600 - - > 3,9 horas.

En menos de 4 horas se encuentra !!

Si consideramos el valor medio, en unas 2 horas se obtendría la password, no parece mucho tiempo, no ¿?

Ahora bien, si para cada prueba hay que calcular 3 hashes (el hash del hash del hash) entonces el tiempo se triplica y estaríamos hablando de un tiempo máximo de 12 horas o un tiempo medio de 6 horas. Tampoco me parece mucho.

Reforcemos el sistema . . .

Tenemos passwords de hasta 10 caracteres pero de un conjunto de letras (distinguiendo mayúsculas de minúsculas) más números (del 0 al 9, claro) más algunos signos especiales (pongamos 10 signos especiales) en total 72 caracteres para combinar.

Número de combinaciones 72**10 -- > 3.7439062e+18 (dice google)

3.7439062e+18 / 10.000.000.000 - - > 374.390.624 segundos (374 millones ¡!)

374390624 / 3600 - - > 103997 HORAS

103997 / 24 - - > 4333 DIAS ¡!!!

4333 / 365 - - > 11 AÑOS ¡!!!!!!! (y algunos meses)

Claro, podemos utilizar una máquina más potente . . . . 30 veces más potente (https://www.xataka.com/ordenadores/ocho-tarjetas-gtx-1080-conectadas-sirven-no-para-jugar-sino-para-crackear-contrasenas)

Entonces serían

3.7439062e+18 / 300.000.000.000 - - > 12479687 segundos

12479687 / 3600 -- > 3466 horas

3466 / 24 - - > 144 días

Hemos pasado de 11 años a unos 5 meses (así , redondeando) No está mal, no ¿?

Ahora bien, decíamos que estadísticamente una password se hackeará en un tiempo medio que será la mitad, es decir en 77 días (2 meses y medio) .

Tiempo medio: eso significa que a veces se encontrará antes y otras veces después , pero estadísticamente el promedio será ése.

Pero si decíamos que a veces hay que calcular para cada combinación hash x 3 (el hash del hash del hash) el tiempo se triplica.

Queda en unos 7 meses y 15 días.

7 meses y 15 días en una máquina muy potente trabajando sin parar ¡!!

¿ Qué creéis ?

¿Es un sistema robusto ? ¿ Es computacionalmente costoso ¿?

¿Y si montamos un sistema tipo SETI ?

¿Y si en vez de passwords hasta 10 caracteres usamos passwords hasta 20 o 30 caracteres ?

¿Sabéis como era la password de un ordenador que fue atacado por el virus cryptolocker ?

https://www.genbeta.com/seguridad/los-operadores-del-ransomware-teslacrypt-cierran-piden-perdon-y-dan-la-clave-de-desbloqueo