Hashcat

Rafael Tamayo Luisce A01421337

¿Que es?

- Hashcat, es una herramienta que nos permite obtener contraseñas a partir del hash de las mismas.
- Una pequeña ayuda que nos facilitará el trabajo cuando nos encontremos con una base de datos o un archivo que contenga credenciales de usuarios cifradas.
- Versiones disponibles para Linux, OS X, Windows.

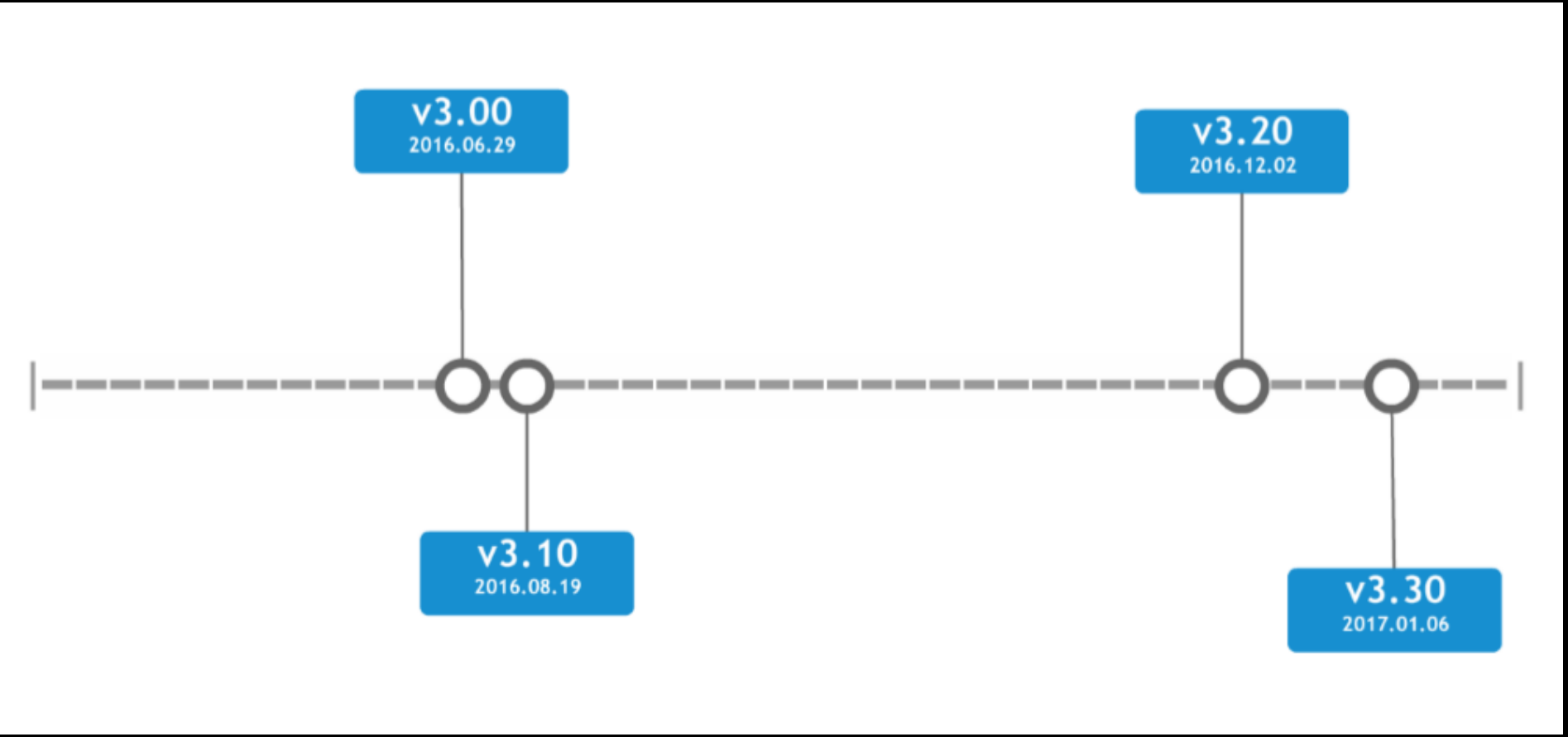
¿Que es?

- El 4 de Diciembre del 2015 , Jens 'Atom' Steube, creador de la herramienta, anuncio la apertura del codigo de Hashcat a la comunidad de software libre a través de un hash MD5 que publico en Twitter, craqueado como “hashcat Fuente abierta”

¿Que es?

- Provee versiones tanto por línea de comandos, como así también a través de una GUI bastante completa.
- Aunque antes de la aparición de Hashcat ya existían diferentes tipos de software (como "PasswordsPro" o "John the Ripper") que cumplían la misma función, esta herramienta se diferencia principalmente en que nos permite hacer “multiprocesamiento".
- Tiene soporte multihilo, soporta muchos algoritmos (más de 50) y permite utilizar técnicas avanzadas utilizando reglas o tablas de permutación, entre otros.

Versiones.



Jens Steube (atom)

- Jens Steube, aka atom, es un desarrollador de software Alemán
- Un renombrado experto en el “craqueo” de contraseñas.
- Se le conoce por ser el desarrollador principal de Hashcat.
- El y su equipo fueron el primer lugar de “Crack Me If You Can” 2010 y 2012 y Hash Runner 2012.
- Algunos dicen que esta convencido que Star Wars fue un documental.

Tipos de Ataques

- Brute-Force attack
- Combinator attack
- Dictionary attack
- Fingerprint attack
- Hybrid attack
- Mask attack
- Permutation attack
- Rule-based attack
- Table-Lookup attack
- Toggle-Case attack
- PRINCE attack

Rules

- ?l is all lower case letters from a to z
- ?u is all upper case letters from a to z
- ?d is all digits from 0-9
- ?s is all special characters on a standard keyboard
- ?D is all 8-bit characters from the German alphabet
- ?F is all 8-bit characters from the French alphabet
- ?R is all 8-bit characters from the Russian alphabet

Rules

- **-n 2** - Vamos a utilizar 2 cores de nuestra CPU.
- **-a 3** - Modo fuerza bruta.
- **-m 400** - Tipo de hash: phpass, MD5(WordPress), MD5(phpBB3).
- **-o wp.pass** - Fichero de salida.
- **wordpress.hash** - Fichero que contiene los hash a descifrar.
- **?l?l?l?l?l?l?l** - Máscara, hasta 7 caracteres en minúsculas.

Rules

- C= make the first letter of each word in the wordlist lowercase and makes the rest of the letters uPPERCASE
- t = tOgGLe cAsE fOr AlL wORdS
- TN = tOgGLe cAsE for character position N, where N = the letter N spaces from left starting position
- r = reverse each word in wordlist (so it is sdrawkcab - backwards)
- f = duplicates each word in wordlist in reverse fashionnoihsaf
- [= deletes the first character of each word in wordlist
-] = deletes the last character of each word in wordlist
- zN = duplicates the first character of each word in wordlist N times

```
$ ./hashcat-cli64.bin examples/A0.M0.hash examples/A0.M0.word
Initializing hashcat v0.47 by atom with 8 threads and 32mb segment-size...
Added hashes from file examples/A0.M0.hash: 102 (1 salts)
NOTE: press enter for status-screen
--- Output Omitted ---
All hashes have been recovered
Input.Mode: Dict (examples/A0.M0.word)
Index.....: 1/1 (segment), 102 (words), 2769 (bytes)
Recovered.: 102/102 hashes, 1/1 salts
Speed/sec.: - plains, - words
Progress..: 102/102 (100.00%)
Running...: --:--:--:--
Estimated.: --:--:--:--
Started: Tue Dec 10 18:07:54 2013
Stopped: Tue Dec 10 18:07:54 2013
```