CRYPTO - Competition

Instal·la l'eina hashcat o demostra que la tens instal·lada i la seva versió 1
Quin tipus de hash hi ha al fitxer hashes.txt? 1
Cerca informació sobre el tipus de hash i descriu-me quant de vulnerable és 1
Com ho faries per petar hashos més ràpid que els demés? 2
Què vol dir que un hash col·lisiona? 3
Fes servir hashcat per petar el màxim de hashos que puguis 3

A continuació hi ha un fitxer de passwords d'una empresa real que va tancar les seves portes fa temps a la comarca de girona.

A partir del moment en què presento aquesta pràctica comença la competició.

Com puntuaré?

La puntuació serà vers el nombre de hashos que aconsegueixis, la intenció és fer un barem en funció dels resultats generals.

El que més hashos aconsegueixi tindrà la nota més alta.

Contestar les preguntes i passar el challenge amb el professor pot assegurar-te un 5 tot i no tenir cap hash aconseguit.

Instal·la l'eina hashcat o demostra que la tens instal·lada i la seva versió

```
hashcat --version
v5.1.0
```

Quin tipus de hash hi ha al fitxer hashes.txt?

Es tracta del tipus **md5crypt**, MD5 (Unix), Cisco-IOS 1 (MD5). Que correspon al hash-mode 500 del hashcat segons la seva documentació https://hashcat.net/wiki/doku.php?id=example_hashes.

Cerca informació sobre el tipus de hash i descriu-me quant de vulnerable és

md5crypt és un algoritme de xifrat vulnerable, no perquè l'algoritme criptogràfic sigui feble sinó perquè és molt ràpid d'utilitzar. És a dir, es poden provar moltes possibles contrasenyes en poc temps. A classe hem pogut provar moltes possibilitats fent servir les nostres GPU, amb altres tipus de hash més lents haguessim tardat molt més.

Podem fer servir el mode benchmark del hashcat per comprovar el hashrate del nostre hardware per cada tipus de hash. Amb això comprovem que els mil·lisegons en el md5crypt són molt més baixos, podrem provar moltes més possibilitats que amb els altres.

```
hashcat -b
-------------------------------------------------------------------------------

* Hash-Mode 500 (md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)) [Iterations
    : 1000]
-------------------------------------------------------------------------------


Speed.#2.........: 13138.6 MH/s (91.23ms) @ Accel:128 Loops:1024 Thr
    :256 Vec:1

----------------------
* Hash-Mode 100 (SHA1)
----------------------
Speed.#2.........:  4119.4 MH/s (72.74ms) @ Accel:128 Loops:1024 Thr:64
     Vec:1

---------------------------
* Hash-Mode 1400 (SHA2-256)
---------------------------
Speed.#2.........:  1697.6 MH/s (88.40ms) @ Accel:64 Loops:1024 Thr:64
    Vec:1
---------------------------
* Hash-Mode 1700 (SHA2-512)
---------------------------
Speed.#2.........:   447.2 MH/s (83.92ms) @ Accel:32 Loops:512 Thr:64
    Vec:1
```

```
hashcat -b -m 500

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

* Hash-Mode 500 (md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)) [Iterations
    : 1000]
-------------------------------------------------------------------------------


Speed.#2.........:  4933.9 kH/s (54.67ms) @ Accel:512 Loops:250 Thr:64
    Vec:1
```

Com ho faries per petar hashos més ràpid que els demés?

Aconseguir la millor de les targetes gràfiques i el millor dels diccionaris, així com la millor de les regles, per provar un nombre de hashes més gran que els altres en menor temps. És a dir, necessitaria el

hashrate més gran possible.

Per intentar ser més ràpid, tenint pistes sobre l'origen dels hashes, crearia un diccionari personalitzat i les regles més comunes. Això és el que he fet, sabent que tenia relació amb Girona i que la majoria de gent té contrasenyes febles, he creat un diccionari amb noms i cognoms catalans i espanyols, així com temes típics d'aquí com el futbol i les motos. He afegit regles típiques com són números al final de cada contrasenya (Peraira93, Marc19, Joel1995) i combinacions de minúscules i majúscules. A mesura que anava trobant contrasenyes anava veient més o menys de quin tipus són i anava creant les regles i el diccionari segons què trobava.

Què vol dir que un hash col·lisiona?

Una col·lisió de hash és quan dues entrades diferents donen el mateix resultat utilitzant la mateixa funció de hash, quan diferents entrades col·lisionen es diu que són sinònims.

Això passa perquè el conjunt de possibles hash és sempre més gran al nombre d'espais disponibles, el nombre de possibles entrades sempre serà més gran que el nombre de possibles entrades.

Fes servir hashcat per petar el màxim de hashos que puguis

S'han trobat un total de 180 resultats.

Algunes comandes fetes servir:

```
hashcat -d 1 -m 500 -a 0 -o cracked.txt hashes.txt -r material/joel.
    rule material/diccionaris/nombres_masculinos.txt  material/
    diccionaris/nombres_sin_acentos.txt material/diccionaris/
    nombres_variados_minusculas.txt material/diccionaris/
    noms_amb_accents.txt material/diccionaris/nombres_sin_acentos.txt
    material/diccionaris/noms_sense_accents.txt  -O
```

```
hashcat -d 1 -m 500 -a 0 -o cracked.txt hashes.txt material/cyclone.txt
     -O --force -w 3
```

```
hashcat -d 1 -m 500 -a 0 -o cracked.txt hashes.txt wordlists/
    el_diccionari_del_toni.txt -r rules/toni.rule -O
```