

---

## “Trencar” contrasenyes amb hashcat

**Autor:** Francesc Xavier Bullich Parra

Dins del directori files hi han 2 fitxers shadow amb els hashos de diferents sistemes.

La idea es trobar les contrasenyes relacionades amb aquests hashos. No intentant trencar el hash sino provar diferents combinacions per intentar reproduir el mateix hash.

S'utilitza el software hashcat que permet generar diferents combinacions de hashos a partir de contrasenyes.

En aquesta pràctica s'han utilitzat diversos mètodes per trobar les contrasenyes.

En resultat s'han trobat un total de 45 contrasenyes entre els 2 fitxers. (Veure fitxer hashcat.potfile adjunt). No son gaires però els he extret amb els mètodes que m'han permetes acabar en un temps raonable

### Mètodes Utilitzats

Primer de tot s'han extret els hashos dels fitxers shadow1 i shadow2 als fitxers adjunts has1.txt i hash2.txt respectivament. Posteriorment s'han aplicat diferents tècniques per trobar les contrasenyes.

### Diccionaris

S'ha provat d'executar la comanda més simple utilitzant només diccionaris.

```
./haschat64.exe -a 0 -m 500 "fitxer hash" "fitxer diccionari" -O
```

Aquest mètode s'ha provat amb tots (o gariabe tots) els fitxers proporcionats amb el material original. A més he buscat alguns diccionaris amb les contrasenyes que s'han anat publicant per internet. Molts d'ells contenen paraules en anglès pel que pot ser que no siguin els més adequats donades les característiques dels fitxers shadow.

Amb aquesta tècnica s'han aconseguit bastants resultats en els 2 fitxers. Sobretot amb els diccionaris extra.

Els diccionaris extra que m'he descarregat es troben al directori files/provats.

### Combinatoria

S'ha provat d'executar la comanda amb parametres combinatoris.

---

```
./haschat64.exe -a 1 -m 500 "fitxer hash" "fitxer diccionari" "fitxer diccionari" -O
```

En aquest cas s'han provat algunes combinacions dels fitxers de noms i altres amb el fitxer anys. Es pot veure un petit script en bash que va provant diferents combinacions (hashcat/hascat-noms.sh)

Amb aquest mètode també s'han aconseguit bastants resultats dels totals aconseguits.

### **Força bruta**

S'ha provat d'executar la comanda amb parametres de força bruta.

```
./haschat64.exe -a 3 -m 500 "fitxer hash" ?a?a?a?a -O
```

S'han provat algunes combinacions de fins a 4 caràcters alfanumerics ja que més enllà el temps a dedicar era massa gran.

Amb aquest mètode s'ha trobat 1 o 2 resultats. Gens significatiu però no he pogut provar amb més combinatoria.

### **Diccionaris + Força bruta**

S'ha provat d'executar la comanda amb parametres de combinació de diccionari + força bruta.

```
./haschat64.exe -a 6 -m 500 "fitxer hash" ?d?d -O
```

S'han provat algunes combinacions de fins a dels fitxers de noms i 2 dígits en diferents posicions. Podem veure un petit script al fitxer hashcat/hashcat-noms-comb.sh.

Aquest ha estat un mètode d'última hora a veure si podia treure alguna contrasenya més i en el moment de fer l'informa encara no s'ha trobat cap contrasenya.