“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 contranenyes 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 diverosos mètodes per trobar les contrasenyes.

En resultat s’han trobat un total de 50 contrasenyes entre els 2 fitxers. (Veure fitxer hashcat.potfile adjunt). No son gaires però els he extret amb els métodes que m’han permes acabar en un temps raonable.

Totes les proves i el document resultat s’han realitzat fins el dia 3/12 que és quan suposava que s’acabava l’activitat. A partir d’aquell dia vam intercanviar formes d’extreure contrasenyes i per aixó no vaig creure oportú provar de nou amb el periode extra.

Métodes 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 diferentes técniques 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 métode 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 caràcteristiques dels fitxers shadow.

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

La majoria de diccionaris provats son de:

- github SecLists: https://github.com/danielmiessler/SecLists/tree/master/Passwords

- SkullSecurity: https://wiki.skullsecurity.org/Passwords

Alguns dels diccionaris usats son els que contenen més registres de les pagines mencionades.

Per exemple:

- rockyou
- darkweb2017-top10000
- xato-net-10-million-passwords-1000000
- unkown-azul
- UserPassCombo-Jay
- 000webhost
- Spanish

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 métode també s'han aconseguit bastants resultats dels totals aconesguits.

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 métode s'ha trobat 1 o 2 resultats. Gens significatiu pero no he pogut provar amb mes combinatoria.

Diccionaris + Força bruta

S'ha provat d'executar la comanda amb parametres de combinacio 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 digits en diferents posisions. Podem veure un petit script al fitxer hashcat/hashcat-noms-comb.sh.

Amb aquests métode s’han aconseguit uns 7 o 8 resultats.