Heslo by malo byt hešované a nie voľný text

Stranka hash generator spravy MD5 hash (32 znakov) a SHA1 hash (40 znakov)  
 hešované heslo je vysledok reťazca v pevnej dĺžke

Vygenerovat hash je jednoduhsie ako porovnavanie hashu

Rainbow tables

Crackstation net pouziva sa na porovnanie hashow z databazy a ak ho ma da vysledok neupraveny hash

Ak sa hashuje ma sa to robit so solou (salt)

Da akoby zakorenenu cast na zaciatok hashovaneho hesla

Vdaka tomuto koreniu (soly) aj ak maju viacery rovnake heslo tak to nevyzera rovnako ked to je zaheshovane

Cat /etc/shadow

tam si vieme pozriet zahashovane heslá na konci su casi kt. identifikuju kedy si pouzivatel naposledy upravoval heslo

za tim je kedy si musi zmenit heslo (za kolko dni)

ako tretie je kedy

ako stvrte je

predposledna vec je ze ked vyprsi heslo tak po kolkych dnoch sa deaktivuje ucet

posledne je ze po kolkych dnoch ucet prestane fungovat

Ale aj tieto tieto casy mozu identifikovat kedy sa nainstaloval linux alebo kedy bol naposledy spusteny neaky prikaz