AKÉ SILNÉ JE VAŠE HESLO?

JE VAŠE HESLO DOSTATOČNE ODOLNÉ VOČI KYBERNETICKÉMU ÚTOKU? V TABUĽKE SI MÔŽETE ĽAHKO OVERIŤ, ZA AKÝ ČAS VÁM HO DOKÁŽE ÚTOČNÍK PRELOMIŤ.

Počet znakov \ Typ znakov	Iba číslice	Veľké, alebo malé písmená	Kombinácia veľkých a malých písmen	Čísla, veľké a malé písmená	Čísla, veľké a malé písmená, symboly
4	Okamžite	Okamžite	Okamžite	Okamžite	Okamžite
5	Okamžite	Okamžite	Okamžite	Okamžite	Okamžite
6	Okamžite	Okamžite	Okamžite	Okamžite	Okamžite
7	Okamžite	Okamžite	2 sekundy	7 sekúnd	31 sekúnd
8	Okamžite	Okamžite	2 minúty	7 minút	39 minút
9	Okamžite	10 sekúnd	1 hodina	7 hodín	2 dni
10	Okamžite	4 minúty	3 dni	3 týždne	5 mesiacov
11	Okamžite	2 hodiny	5 mesiacov	3 roky	34 rokov
12	2 sekundy	2 dni	24 rokov	200 rokov	3 tis. rokov
13	19 sekúnd	2 mesiace	1 tis. rokov	12 tis. rokov	202 tis. rokov
14	3 minúty	4 roky	64 tis. rokov	750 tis. rokov	16 mil. rokov
15	32 minút	100 rokov	3 mil. rokov	46 mil. rokov	1 mld. rokov
16	5 hodín	3 tis. rokov	173 mil. rokov	3 mld. rokov	92 mld. rokov
17	2 dni	69 tis. rokov	9 mld. rokov	179 mld. rokov	7 tln. rokov
18	3 týždne	2 mil. rokov	467 mld. rokov	11 tln. rokov	438 tln. rokov

TABUĽKA HESIEL A JEJ PÔVOD

V roku 2020 spoločnosť **Hive Systems** prvýkrát zverejnila tabuľku, ktorá ukazuje aké odolné je vaše heslo voči prelomeniu hrubou silou na základe dĺžky hesla a rôznorodosti použitých znakov v hesle. Tabuľka sa čoskoro stala virálnou a zdieľali ju mnohé médiá, sociálne siete a vzdelávacie inštitúcie. V marci roku 2022 Hive Systems zverejnila aktualizovanú tabuľku, ktorá berie do úvahy pokrok vo výpočtovom výkone súčasných prostriedkov IKT. Originálnu verziu tabuľky nájdete na stránke **https://www.hivesystems.io/blog/are-your-passwords-in-the-green**

POUŽITÁ METODIKA

Pri výpočte času potrebnom na prelomenie hesla autori v roku 2018 postupovali rovnako ako postupujú bežní útočníci - pomocou MD5 hašovacej funkcie "Hashcat" na grafickej karte RTX 2020 GPU simulovali porovnávanie generovaných haš reťazcov voči jednotlivým typom hesiel, tiež hašovaných cez MD5. Výsledné časy potrebné na prelomenie daných kombinácií číslic a znakov zaniesli do tabuľky, ktorú pre názornosť rozdelili do 5 kategórií od okamžitého prelomenia hesla až po heslá, ktorých prelomenie touto technikou by trvalo viac ako 15 miliárd rokov.

Za posledné 4 roky ale výpočtový výkon násobne vzrástol. A tak autori v roku 2022 použili novší typ grafickej karty RTX 3090, ktorej výpočtový výkon je navýšený z cca. 10 miliónov FLOPS na 35,6 milióna FLOPS, čo znamená reálne generovanie takmer 70 miliónov haš reťazcov za sekundu. Takýto nárast o cca. 86% vo výpočtovom výkone znamená aj výrazne kratšie časy potrebné na prelomenie hesiel. Výsledky nájdete v tabuľke.

PRAKTICKÉ DOPADY

Stačí, ak útočník použije metodiku popísanú vyššie, na bežnej, aj keď výkonnej grafickej karte v štandardnom PC. Najbežnejšie používané heslá (8 znakov, mix číslic, veľkých a malých písmen a špeciálnych znakov) je útočník schopný prelomiť za menej ako 3 hodiny!

Podobne, ak použijete akokoľvek komplikované a dlhé heslo, ktoré sa bežne vyskytuje v hovorovej reči (fráza a pod.), alebo už skôr uniknuté heslo, k jeho prelomeniu prichádza okamžite.

INÉ METODIKY

Zatiaľ čo výskumníci v HiveSystems použili postup popísaný v metodike, je samozrejme možné na lámanie hesiel získať aj vyšší výpočtový výkon. Dá sa napríklad použiť viacero výkonných kariet naraz, alebo prenajať si ich. Najvýkonnejším z dostupných riešení je prenájom výpočtového výkonu v cloude.

Napríklad pri využití výpočtového klastra od Amazonu (8 NVIDIA A100 Tensor Core GPU) cez službu EC2 P4d za 32.77 USD za hodinu získate výkon vyše 523 triliónov haš reťazcov za sekundu, čo je približne 7,5 násobné zrýchlenie oproti metodike použitej v tabuľke. Podobné zrýchlenie ale získate aj použitím inej služby, ktorá ponúka 8 grafických kariet RTX 3090 naraz v cene len 3.20 USD za hodinu.

ZNÁME OBMEDZENIA

- Snaha o prelomenie hesla uvedeným spôsobom predpokladá, že útočník má k dispozícii výber uniknutých haš reťazcov (podobne ako pri stránke HavelbeenPwned)
- Predpokladaný útok nevyužíva funkcionalitu viacfaktorovej autentizácie
- Použitá metodika predpokladá náhodne generované heslá. Nenáhodné heslá je možné prelomiť oveľa rýchlejšie
- V prípade, že heslo už bolo v minulosti prelomené, časy uvedené v tabuľke sa na neho nevzťahujú. Prelomené heslá totiž útočníci kontrolujú ako prvé.
- Funkcia Hashcat používa 999 iterácií pre typ PBKDF2 SHA-256, čo je menej ako odporúča napr. NIST (najmenej 1.000 iterácií)
- Do výsledných časov nie je započítaný čas nutný na porovnanie generovaného hašu s hašom hesla, nakoľko tieto časy sú triviálne
- Autori medzi použité znakové sady zaradili okrem štandardných ASCI a UNICODE Latin znakov aj cyriliku (Unicode), takže v prípade znakov len z Latin sady bude prelomenie hesla ešte rýchlejšie

Obsah bol spracovaný na základe blogu Hivesystems