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	Malé písmená	Veľké a malé písmená	Čísla, veľké a malé písmená	Čísla, veľké a malé písmená, symboly
4	Okamžite	Okamžite	3 sekundy	6 sekundy	9 sekúnd
5	Okamžite	4 sekundy	2 minúty	6 minút	10 minút
6	Okamžite	2 minúty	2 hodiny	6 hodín	12 hodín
7	4 sekundy	50 minút	4 dni	2 týždne	1 mesiac
8	37 sekúnd	22 hodín	8 mesiacov	3 roky	7 rokov
9	6 minút	3 týždne	33 rokov	161 rokov	479 rokov
10	1 hodina	2 roky	1 tis. rokov	9 tis. rokov	33 tis. rokov
11	10 hodín	44 rokov	89 tis. rokov	618 tis. rokov	2 mil. rokov
12	4 dni	1 tis. rokov	4 mil. rokov	38 mil. rokov	164 mil. rokov
13	1 mesiac	29 tis. rokov	241 mil. rokov	2 mld. rokov	11 mld. rokov
14	1 rok	766 tis. rokov	12 mld. rokov	147 mld. rokov	805 mld. rokov
15	12 rokov	19 mil. rokov	652 mld. rokov	9 bil. rokov	56 bil. rokov
16	119 rokov	517 mil. rokov	33 bil. rokov	566 bil. rokov	3 brd. rokov
17	1 tis. rokov	13 mld. rokov	1 brd. rokov	35 brd. rokov	276 brd. rokov
18	11 tis. rokov	350 mld. rokov	91 brd. rokov	2 trl. rokov	19 trl. rokov

Spolufinancovaný Európskou úniou

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberajú žiadnu zodpovednosť.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

www.cybercompetence.sk

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 apríli roku 2024 Hive Systems zverejnila zatiaľ najnovšiu tabuľku, ktorá berie do úvahy pokrok vo výpočtovom výkone súčasných prostriedkov IKT, ale aj v šifrovacích algoritmoch používaných pre haš funkciu. 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 roky ale výpočtový výkon násobne vzrástol, na druhej strane aj úroveň šifrovania pri generovaní haš reťazcov. A tak autori v roku 2024 použili novší typ grafickej karty RTX 4090 (12x), ktorej výpočtový výkon je navýšený z cca. 10 miliónov FLOPS na 82,6 milióna FLOPS. Takýto nárast vo výpočtovom výkone znamená aj výrazne kratšie časy potrebné na prelomenie hesiel, na druhej strane autori použili hašovaciu funkciu bcrypt (32 iterácií), ktorá je robustnejšia a v súčasnosti viac používaná ako MD5 a časy potrebné na prelomenie naopak podstatne navyšuje. 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, haš MD5) je útočník schopný prelomiť za menej ako 1 hodinu!

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 p4de.24xlarge za 40.96 USD za hodinu získate teoretický výkon vyše 36 miliónov haš reťazcov za sekundu.

ZNÁME OBMEDZENIA

- Snaha o prelomenie hesla uvedeným spôsobom predpokladá, že útočník má k dispozícii výber uniknutých haš reťazcov (podobne ako pri stránke HaveIbeenPwned).
- 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.
- V predošlých edíciách tabuľky sme medzi použité znaky v heslách rátali všetky znakové sady klávesnice QWERTY. Tento rok sme ale okrem základnej znakovej sady doplnili len tie znaky, ktoré sa štandardne používajú pri generovaní hesiel – „^*%$!&@#“ . Takéto riešenie ovplyvňuje len heslá v pravom stĺpci tabuľky. Inými slovami, generovanie hesiel sme obmedzili na nasledovné znakové sady:

Kódovanie	Alias	Znaková sada	Počet znakov
ASCII	Malé písmená	a-z	26
ASCII	Veľké písmená	A-Z	26
ASCII	Čísla	0-9	10
ASCII	Symboly A	^*%$!&@#	8

Obsah bol spracovaný na základe blogu Hivesystems

ISBN 978-80-69011-41-0
V 2.0 Sep 2024