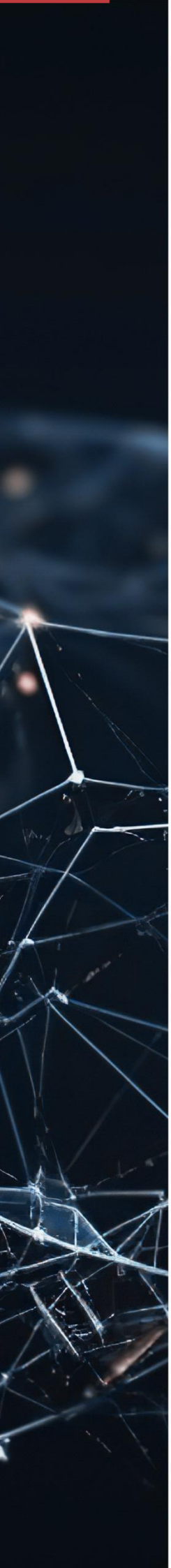

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Všeobecné informácie

Bruteforce

VJ CSIRT

Čo je to bruteforce útok

Jedná sa o typ útoku v rámci ktorého útočník využíva veľké množstvo pokusov o prihlásenie („háda“ prihlasovacie údaje). Takto dokáže útočník vyskúšať niekoľko desiatok tisíc prihlásení za sekundu. Takýto útok vieme následne rozdeliť do niekoľkých kategórií:

1. **Jednoduchý:** útočník nevyužíva žiadnu logiku „hádania“ prihlasovacích údajov a spolieha sa len na náhodu.
2. **Slovníkový:** útočník využíva slovníky (zoznamy) zväčša známych údajov
3. **Rainbow tables:** útočník využíva predvypočítané hodnoty na uhádnutie hashu prihlasovacích údajov
4. **Credential stuffing:** útočník využíva už jemu známe prihlasovacie údaje naprieč možným spektrom prihlasovacích portálov. Využíva sa tu fakt, že používatelia používajú rovnaké prihlasovacie údaje vo viacerých portáloch.

Indikátory bruteforce útoku vo Vašej infraštruktúre

☐ nezvyčajne veľké množstvo pokusov o prihlásenie pre 1 používateľa

☐ nezvyčajne veľké množstvo používateľov prihlasujúcich sa súčasne

☐ používateľské mená sa nezhodujú s politikou prihlasovacích údajov

☐ veľký počet prihlásení zamietnutý na úrovni MFA

☐ veľký počet zablokovaných účtov

Ochrana pred bruteforce útokom

Existuje množstvo spôsobov, akým zabrániť úspešnému prieniku do konta pomocou bruteforce útoku. Patrí medzi ne:

☐ Použitie zložitých, dostatočne dlhých hesiel (ideálne použitie passphrase)

☐ Použitie viacfaktorovej autentifikácie

☐ Obmedziť používanie rovnakých prihlasovacích údajov do viacerých portálov

☐ Vyhnúť sa používaniu známych uniknutých hesiel

☐ Vyhnúť sa zdieľaniu hesiel s inými ľuďmi

☐ Nenechávať heslo na viditeľnom mieste

☐ Použitie správcu hesiel

☐ Zavedenie bezpečnostných politík (lockout, minimálne nároky na heslo, životnosť hesla a pod.)

☐ Využitie whitelistov/blacklistov na povolenie prihlásenia

☐ Využitie geoblokácie