NAJBEŽNEJŠIE TYPY ÚTOKOV NA HESLÁ

ÚTOK HRUBOU SILOU

Útok hrubou silou je typ prelomenia hesla, ktorý používa špeciálny počítačový program na generovanie a skúšanie čo najväčšieho množstva kombinácií znakov, kým nenájde správne heslo. Tento útok je veľmi časovo náročný a vyžaduje si vysoký výpočtový výkon, ale môže byť úspešný, ak má útočník dostatok času a zdrojov.

Príklad: Útočník sa pokúša prihlásiť do vášho bankového účtu tým, že postupne vyskúša všetky možné kombinácie písmen, čísiel a znakov, až kým sa mu nepodarí nájsť správne heslo.

SLOVNÍKOVÝ ÚTOK

Slovníkový útok používa zoznam slov (zvyčajne prevzatých z dostupných slovníkov) na generovanie a skúšanie možných hesiel. Tento útok môže byť úspešný, ak je heslom bežné slovo alebo fráza, ale je oveľa menej pravdepodobné, že útočník uspeje, ak je heslo náhodným reťazcom znakov.

Príklad: Útočník skúša heslá ako „heslo123", „admin" alebo „123456" v nádeji, že používateľ používa jednoduché heslo.

ÚTOK POMOCOU DÚHOVEJ TABUĽKY (RAINBOW TABLE ATTACK)

Útok pomocou dúhovej tabuľky je typ prelomenia hesla, ktorý používa vopred vypočítanú tabuľku hash hodnôt pre veľké množstvo hesiel. Keď má útočník k dispozícii hash hesla, porovnáva ho s hash hodnotami v dúhovej tabuľke, aby zistil pôvodné heslo.

Príklad: Útočník získa databázu hash hesiel a následne použije dúhovú tabuľku na odhalenie pôvodných hesiel používateľov.

ÚTOK POMOCOU SOCIÁLNEHO INŽINIERSTVA

Útok pomocou sociálneho inžinierstva spočíva v tom, že útočník manipulatívnymi technikami presvedčí používateľa, aby dobrovoľne prezradil svoje heslo alebo iné citlivé údaje. Tento druh útoku je úspešný najmä u ľudí, ktorí nie sú dostatočne informovaní o bezpečnostných rizikách.

Príklad: Útočník zavolá zamestnancovi spoločnosti a predstiera, že je pracovník z IT podpory, ktorý potrebuje heslo na vykonanie aktualizácie systému.

ÚTOK NAPLNENÍM POUŽÍVATEĽSKÝCH PRÁV (CREDENTIAL STUFFING ATTACK)

Tento druh útoku spočíva v tom, že útočník používa získané prihlasovacie údaje z predchádzajúcich únikov údajov na prihlásenie sa do iných online služieb, s predpokladom, že používatelia majú z pohodlnosti často rovnaké prihlasovacie údaje (používateľské mená a heslá) na viacerých platformách.

Príklad: Po úniku údajov z online obchodu útočník použije získané e-maily a heslá na prihlásenie do iných služieb, ako sú e-mailové účty alebo sociálne siete, ak si používateľ nezmenil heslo.

PHISHINGOVÝ ÚTOK

Phishing je technika, pri ktorej útočník získa citlivé údaje od používateľa (napríklad heslá alebo čísla platobných kariet) tým, že sa vydáva za dôveryhodný subjekt, typicky prostredníctvom e-mailov alebo SMS správ, ktoré obsahujú odkaz smerujúci na falošné webové stránky.

Príklad: Používateľ dostane e-mail, ktorý predstiera, že je od jeho banky, a po kliknutí na odkaz v e-maile je vyzvaný, aby zadal svoje prihlasovacie údaje. V skutočnosti ich však odovzdáva útočníkovi.

KEYLOGGING ÚTOK

Keylogger je softvér alebo hardvér, ktorý zaznamenáva každé stlačenie klávesnice. Útočník ho môže použiť na zachytávanie hesiel a iných citlivých informácií bez vedomia obete.

Príklad: Útočník nainštaluje keylogger na verejný počítač v knižnici alebo kaviarni a zaznamenáva heslá používateľov, ktorí sa na tomto zariadení prihlasujú.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

v 1.0. Október 2024

www.cybercompetence.sk