VAJA: Napadi na gesla

Namen

Namen vaje je predstavitev uporabe naprednega orodja za obnavljanje gesel Hashcat, s poudarkom na različnih tehnikah razbijanja gesel, vključno s slovarskimi napadi, napadi z maskami in napadi grobe sile. Cilj je okrepiti razumevanje kibernetske varnosti in pomena močnih gesel skozi praktično uporabo in analizo različnih strategij razbijanja gesel.

Uvod

V sodobnem digitalnem svetu, kjer so gesla ključna prva linija obrambe za zaščito naših osebnih in poslovnih podatkov, je razumevanje tehnik razbijanja gesel in orodij, ki se pri tem uporabljajo, bistvenega pomena za krepitev naše kibernetske varnosti. Razbijanje gesel ali "password cracking" je postopek dešifriranja ali pridobivanja gesla iz podatkov, shranjenih ali prenesenih v računalniški sistem. Ta proces se pogosto uporablja v etičnih hekerskih in forenzičnih preiskavah, da bi testirali in izboljšali varnostne postopke.

Med močnejša orodja za razbijanje gesel sodi Hashcat, napredno in hitro orodje za obnavljanje gesel, ki podpira številne algoritme šifriranja. Hashcat izkorišča moč procesorskih enot (CPU) in grafičnih procesorskih enot (GPU) za izvajanje različnih vrst napadov na gesla, vključno s slovarskimi napadi, napadi z masko, izčrpnimi napadi in hibridnimi napadi. Zmožnost izvajanja napadov z uporabo GPU omogoča Hashcatu, da opravlja razbijanje gesel z izjemno hitrostjo, kar razkriva šibkosti v uporabljenih geslih in omogoča uporabnikom, da izboljšajo svoje varnostne prakse.

Naloge:

1. Izbor gesel: Za začetek izberemo več gesel, ki predstavljajo različne stopnje zahtevnosti.
   - Geslo samo z malimi črkami (npr. ***varen***)
   - Geslo z malimi in velikimi črkami (npr. ***VarenDostop***)
   - Geslo z malimi, velikimi črkami in številkami (npr. ***Varen123***)
   - Geslo z malimi, velikimi črkami, številkami in posebnimi znaki (npr. ***Varen@123***)
2. Generiranje prstnih odtisov gesel:

Za vsako geslo izračunajte in v besedilno datoteko shranite prstne odtise zgostitvenih funkcij (MD5, SHA1, SHA2-256, SHA3-512).

Za izračun uporabite knjižnico OpenSSL v operacijskem sistemu Kali Linux. Ukaz za izračun vrednosti je:

```
echo -n "geslo" | openssl sha256
```

V teh ukazih, echo -n prepreči dodajanje nove vrstice na konec niza, ki bi lahko vplivala na izračunani hash. Uporaba cevi | prenaša izhod ukaza echo neposredno v OpenSSL, kjer se izračuna in izpiše želeni hash.

Če želite shraniti rezultat v datoteko lahko uporabite ukaz:

```
echo -n "geslo" | openssl sha256 >> datoteka.txt
```

3. Napad na gesla:

Za izvedbo napada na gesla z uporabo orodja Hashcat, sledite tem korakom. Hashcat je napredno orodje za obnavljanje gesel.

- Pri slovarskem napadu hashcat primerja vsako besedo iz slovarja (datoteko z možnimi gesli) s hashom ciljnega gesla.
- Pri napadu z maskami se uporablja, ko so na voljo informacije o strukturi gesla (npr. znano dolžino, uporabo določenih znakov), kjer Hashcat generira gesla na osnovi te maske.
- Pri napadu s kombinacijami hashcat kombinira besede iz dveh različnih slovarjev in preverja vsako kombinacijo.
- Brute force napad poskuša razbiti geslo s preizkušanjem vseh možnih kombinacij znakov določene dolžine

Za izvedbo napadov z uporabo Hashcata, uporabite naslednje ukaze, pri čemer zamenjajte potrebne parametre (npr. poti do datotek, vrste hashov) po potrebi.

Slovarski napad:

```
hashcat -m <hash-type> <hash-file> <wordlist> -o <output-file>
```

- <hash-type>: Številka, ki predstavlja tip hash algoritma (npr. 0 za MD5, 100 za SHA1).
- <hash-file>: Datoteka, ki vsebuje hash-e, ki jih želite razbiti.
- <wordlist>: Datoteka, ki vsebuje seznam možnih gesel (slovar).
- <output-file>: Datoteka, kamor se shranijo uspešno razbita gesla.

Napad z maskami:

```
hashcat -m <hash-type> <hash-file> -a 3 ?d?d?d?d?d -o <output-file>
```

- `-a 3` označuje napad z masko.
- `?d?d?d?d?d` je primer maske, ki predstavlja pet številk. Uporabite kombinacijo `?l` (male črke), `?u` (velike črke), `?d` (številke) in `?s` (posebni znaki) za definiranje maske.

Napad z grobo silo uporablja isto sintakso, kot napad z maskami, vendar z masko, ki pokriva večji nabor možnosti.

Splošni parametri:

- `-o`: Določa izhodno datoteko za shranjevanje razbitih gesel.
- `--force`: Uporabite, če želite prisiliti Hashcat, da nadaljuje kljub morebitnim opozorilom.
- `--status`: Prikaže status napredka med izvajanjem napada.

Za več informacij in napredne možnosti uporabite `hashcat --help` ali obiščite uradno dokumentacijo Hashcata.

4. Napad grobe sile

Izvedite napade z grobo silo na gesla, ki ste jih določili v prvi točki naloge. Pozorni bodite na čas razbijanja gesla in ga zapišite.

- Geslo samo z malimi črkami: _____
- Geslo z malimi in velikimi črkami: _____
- Geslo z malimi, velikimi črkami in številkami: _____
- Geslo z malimi, velikimi črkami, številkami in posebnimi znaki: _____

5. Napad s slovarjem

Kali vključuje osnovne sezname (wordlists | Kali Linux Tools), lahko pa prenesete lastni seznam iz željene spletne strani z ukazom:

```
wget https://raw.githubusercontent.com/andrazjelenc/Slovenian-wordlist/master/wordlist.txt
```

Poskusite razbiti različna gesla (npr. »***adminadmin***«). Ali je napad s slovarjem bolj uspešen kot napad grobe sile?

6. Pregled seznamov

Po končanem napadu s slovarjem je pomembno, da analizirate učinkovitost uporabljenih seznamov besed. Preglejte rezultate napada s slovarjem in ugotovite, katera gesla so bila uspešno razbita. Ocenite učinkovitost uporabljenega seznama glede na delež razbitih gesel od skupnega števila poskusov.