

Lab 5

Laboratorijska vježba 5 demonstrira ranjivost lozinki putem online i offline password guessing napada.

Online password guessing

Studenti na lokalnom serveru imaju Docker kontejner s jedinstvenom IP adresom i imenom.

Ne ograničava se broj pokušaja prijave korisnika.

Koristimo alat hydra koji oponaša ssh klijenta i testira sve moguće lozinke.

Lozinke su načinjene od 4 do 6 malih slova engleske abecede.

Približni keyspace je 26^6 .

Potreban je velik napor za provođenje napada. Poslužit ćemo se rječnikom koji sadrži lozinke i njihove hash vrijednosti i time smanjujemo vrijeme za otkrivanje lozinki.

lozinka je pronađena.

```
[ATTEMPT] target 10.0.15.0 - login "curak_sara" - pass "kajjnk" - 248 of 872 [child 1] (0/0)
[ATTEMPT] target 10.0.15.0 - login "curak_sara" - pass "kajnpk" - 249 of 872 [child 2] (0/0)
[ATTEMPT] target 10.0.15.0 - login "curak_sara" - pass "kajlzp" - 250 of 872 [child 3] (0/0)
[ATTEMPT] target 10.0.15.0 - login "curak_sara" - pass "kajlje" - 251 of 872 [child 0] (0/0)
[ATTEMPT] target 10.0.15.0 - login "curak_sara" - pass "kajgat" - 252 of 872 [child 1] (0/0)
[ATTEMPT] target 10.0.15.0 - login "curak_sara" - pass "kajatk" - 253 of 872 [child 2] (0/0)
[ATTEMPT] target 10.0.15.0 - login "curak_sara" - pass "kajlng" - 254 of 872 [child 3] (0/0)
[ATTEMPT] target 10.0.15.0 - login "curak_sara" - pass "dtttter" - 255 of 872 [child 0] (0/0)
[22][ssh] host: 10.0.15.0 login: curak_sara password: dtttter
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-12-20 16:43:13
student@DESKTOP-709BASR: /mnt/c/Users/A507$
```

Offline password guessing

Sada treba locirati hash vrijednosti lozinki spremljenih na virtualnm stroju.

Koristimo hashcat alat za provedbu napada.

Lozinka sadrži 6 malih slova engleske abecede.

Dobili smo priližno potrebno vrijeme za otkrivanje lozinke. Približno 26 dana, stoga ćemo se poslužiti predefiniranim rječnikom.

Kada hashcat otkrije lozinku, prikazat će je u outputu. Njenu ispravnost provjeravamo prijavom u korisnički profil na vlastitom virtualnom stroju.

Sara Ćurak

Računarstvo 120