SRP lab 6

Online and offline password guessing

U ovoj laboratorijskoj vježbi smo radili online i offline password guessing napade.

Prvo smo radili online password guessing attack.

Pomoću nmapa skenirali smo otvorene portove. Pokušali smo se s lokalne mašine spojiti na remote mašinu koristeći ssh.

```
ssh krizanac_stela@krizanacstela.local
```

Koristeći Hydru smo pokrenuli brute force napad a znali smo da lozinka ima između 4 i 6 slova i koriste se samo mala slova te smo postavili te uvjete tokom brute force napada.

```
hydra -l krizanac_stela -x 4:6:a krizanacstela.local -V -t 1 ssh
```

Zbog tih uvjeta znali smo da je moguće otprilike 26^6 kombinacija za lozinku i za testiranje pomoću brute force napada bi nam trebalo otprilike 3.5, 4 godine ako imamo 64 pokušaja u minuti što je neučinkovito/neisplativo i nema smisla i stoga smo koristili pre-computed dictionary napad

Nakon preuzimanja vlastitog challenge-a odnosno dictionary-a pokrenuli smo napad naredbom

```
hydra -l krizanac_stela -P dictionary/g3/dictionary_online.txt krizanacstela.local -V -t 4 ssh
```

Testirali smo samo 1000 određenih lozinki i uspješno smo pronašli odgovarajuću lozinku.

Nakon toga smo radili offline password guessing attack koristeći hashcat alat. U cilju nam je bilo pronaći lozinku nekog od usera na hostu pomoću hash vrijednosti koje smo imali. Hashirali smo sve moguće kombinacije slova i probali brute force napad koji je ponovno bio neisplativ pa smo radili dictionary napad.

```
hashcat --force -m 1800 -a 0 password_hash.txt dictionary/g3/dictionary_offline.txt --status --status-timer 10
```

Testirali smo ispravnost lozinke pokušajem logiranja na remote masinu kao odredeni korisnik.