SRP Vježba 5

U prvom dijelu vježbe bavimo se Online Password Guessing-om. Postoje dvije metode, pogađanje i dictionary. Kod pogađanja testiramo sve permutacije zaporke dok kod Dictionary metode koristimo listu pred-definiranih čestih zaporki.

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

Ova komanda nam omogućuje uvid u otvorne portove za pojedino računalo na mreži. Koriste je sistemski administratori za nadzor mreže.

```
ssh prezime_ime@10.0.15.1
```

Ovom komandom otvaramo ssh vezu sa tim računalom na toj IP adresi i tim korisnikom. SSH je secure shell (remote). Za uspješnu uspostavu veze potrebna je zaporka.

```
hydra -l prezime_ime -x 4:6:a ip_adresa_zrtve -V -t 1 ssh
```

Hydra je alat za online pogađanje zaporki, kojoj kao parametre šaljemo IP adresu i korisničko ime žrtve na čije računalo se želimo prijaviti, duljinu zaporke i broj zahtjeva u sekundi, te protokol.

Kao što vidimo to bi moglo potrajati jako dugo, od nekoliko do desetke godina, što nije vremenski isplativo. Zato kao alternativu koristimo unaprijed definirani Dictionary koji u sebi sadrži moguće kombinacije.

```
hydra -l prezime_ime-P dictionary/g5/dictionary_online.txt 10.0.15.1 -V -t 4 ssh
```

Nakon nekog vremena imamo podudaranje i uspješno smo se prijavili u sustav!

Sada pažnju usmjeravamo na drugi dio vježbe. Radi se o Offline Password Guessing-u.

Koristimo alat Hashcat koji služi za oporavak zaporki.

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

Kao argumente prima Hash vrijednost iz koje želimo doznati originalnu zaporku, duljinu zaporke i specifičnosti kao što je da su sve mala slova. Kao primjer hash-a uzeli smo hash iz /etc/shadow.

Nakon što smo došli do zaključka da bi trebalo previše vremena da se nađe tražena zaporka prebacujemo se na Dictionary način.

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

Sada Hashcat koristi unaprijed definiranu listu zaporki koje isprobava jednu po jednu. Nakon nekog vremena < 30 minuta, dobili smo traženu zaporku.

```
ssh jean_doe@10.0.15.1
```

Nakon unosa dobivene zaporke uspješno se prijavljujemo u sustav.

Razlika između Online i Offline napada je ta što kod Online napada napadač izravno komunicira sa serverom i postoje određena ograničenja kao što su broj pokušaja u jedinici vremena. Dok kod offline napada možemo testirati jako velik broj kombinacija jako brzo.