Sigurnost računala i podataka

Lab 6: Online and Offline Password Guessing

Prvo smo instalirali nmap, aplikaciju koja služi za skeniranje otvorenih portova na nekom serveru.

Zatim smo se pomoću ssh spojili na osobni host:

```
ssh biuk_ivan@biukivan.local
```

Preuzeli smo alat hydra koji služi za izvršavanje različitih vrsta napada na password-based autentifikacije.

Prvo smo pokrenuli brute force napad koji testira sve moguće lozinke koje odgovaraju zadanim uvjetima:

`hydra -l biuk_ivan -x 4:6:a biukivan.local -V -t 4 ssh` 4:6 označava da je duljina lozinke između 4 i 6 znakova a broj 4 da koristimo 4 niti (threada) za izvršavanje ovog napada.

Dok se napad izvršavao procijenili smo vrijeme koje će biti potrebno da pogodimo lozinku brute force metodom.

Password space sadrži 25^4 + 25^5 + 25^6 lozinki, odnosno možemo uzeti najveći član pa reći da trebamo provjeriti 25^6 lozinki. U pravilu je potrebno provjeriti polovicu svih lozinki unutar password spacea da bi se pogodila ispravna lozinka. U našem slučaju to je 25^6 / 2 lozinki, a ako uzmemo u obzir brzinu od 64 pokušaja u minuti vidimo da će nam biti potrebno malo manje od 4 godine da pogodimo ispravnu lozinku. Zato prekidamo brute force napad te pokrećemo precomputed dictionary napad.

Svoj dictionary preuzimamo sa servera pomoću naredbe:

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

Napad aktiviramo naredbom:

```
hydra -l biuk_ivan -P dictionary/g1/dictionary_online.txt biukivan.local -V -t 4 ssh
```

Nakon nekoliko minuta (dictionary napad je puno brži od brute force napada zato što testira samo 1000 lozinki), dobijamo ispravnu lozinku te se s njom možemo logirati.

host: biukivan.local login: biuk_ivan password: ondtha

Offline Password Guessing

Sada pomoću alata hashcat pokušavamo pronaći lozinku za nekoga od usera na našem hostu.

Prvo pokušavamo s brute force napadom:

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

Password space je ponovno 25^6 a predviđeno vrijeme trajanja napada je 17 dana.

Naravno da nam to nije prihvatljivo vrijeme pa odlučujemo izvršiti napad pomoću dictionarya: dictionary_offline.txt

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

Sada je predviđeno vrijeme trajanja 7 minuta, pa izvršimo napad do kraja.

Pronašli smo lozinku te smo potvrdili njenu ispravnost prijavom kao ciljani user.