Peti izvještaj

Online and offline password guessing

Poanta obe vježbe je doznati lozinku pripadnoga kontejnera online i offline napadom.

Online Password Guessing

Prvo provjeravamo je li računalo spojeno sa serverom, tako što pingamo isti:

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

Nakon što smo potvrdili konekciju, potrebno je ograničiti komunikaciju na uređaje u laboratoriju. Za to smo u bash shellu instalirali alat nmap.

nmap (Network Mapper) - alat koji se koristi za skeniranje portova i adresa na mreži

```
sudo apt-get update
sudo apt-get install nmap

nmap
```

Ograničavamo komunikaciju na 16 IP adresa:

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

Na lokalnom serveru http://a507-server.local/ su se nalazila naša korisnička imena i IP adrese. Pokušali smo se spojiti na kontejner koristeći naš username i adresu pomoću ssh klijenta.

```
ssh kevric_laura@10.0.15.0
```

Pristup serveru nam je onemogućen jer ne znamo lozinku. Za izvršavanje online napada nam je potreban alat **hydra**. Znali smo da se lozinka sastoji od lowercase slova (kojih je 26) i da je dužine od 4 do 6 znakova.

```
hydra -l kevric_laura -x 4:6:a 10.0.15.0 -V -t 1 ssh
```

Po ispisu vidimo da imamo 321254128 mogućih lozinki, a naš napad radi 16 kombinacija po minuti. Zaključujemo da bi naš napad trajao 32 godine, što nema smisla.

Koristit ćemo **dictionary**, kojeg smo preuzeli sa servera:

```
wget -r -nH -np --reject "index.html*" http://a507-server.local:8080/dictionary/g4/
```

Unutra se nalazilo 860 mogućih lozinki, među kojima je jedna bila naša. Ponovnim korištenjem hydra alata izveli smo online napad.

Iz 845. pokušaja sam dobila svoju lozinku koja je bila wingnc.

Offline Password Guessing

Offline password guessing napad ćemo izvršiti korištenjem hasheva u mapi shadow. Uz pomoć sudo naredbe pristupamo mapi:

```
sudo cat /etc/shadow
```

Ispisala nam se lista korisnika i njihovih hasheva. Moj je odabir bio korisnik freddy_mercury:

6ME8D5iBS8SnDejpZ$PHVFN4nnvbxB5oyCIIkT0MNYlKd5kKJfBTfT97LdirX/49rYzrxJWjyNVGSLsIqAkDU1tjyYeLHX8NX28J867/

Hash vrijednost spremamo u datoteku hash.txt na našem lokalnom računalu. Napad izvršavamo alatom **hashcat.**

Provjeravamo je li alat ispravno instaliran:

```
sudo apt-get install hashcat

hashcat
```

Ovdje također imamo dva hinta: lozinka se sastoji od točno 6 lowercase slova.

Započinjemo napad naredbom:

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

Ponovno koristimo dictionary kako bi smanjili broj kombinacija.

```
hashcat --force -m 1800 -a 0 hash.txt dictionary/g4/dictionary_offline.txt --status --status-timer 10
```

Kod zadnjeg ispisa čiji je status cracked je ispisana lozinka. Prijavljujemo se u server preko ssh klijenta kako bi smo potvrdili točnost informacije:

```
ssh freddie_mercury@10.0.15.0
```