Lab 6: Notes

- tema: prikaz online i offline password guessing napada

- **online password guessing napadi**
- preuzimamo osobne izazove iz datoteke
- pomoću secure shella se spajam na pupacickarla.local naredbom:

```
ssh pupacic_karla@pupacickarla.local
```

- testiramo brute force napad
- koristimo hydra alat za taj pokušaj

```
hydra -l pupacic_karla -x 4:6a pupacickarla.local -V -t 4 ssh
```

- 4:6 - veličina lozinke
- 4 - broj threadova
- u prosjeku bi se ovom metodom trebalo provjeriti pola od ~25^6 lozinki, za što bi nam brzinom od 64 lozinke po minuti trebalo nešto manje od 4 godine (otprl. 7 i pol godina za provjeru svih lozinki)
- testiramo napad dictionaryjem

```
hydra -l pupacic_karla -P dictionary/g2/dictionary_online.txt pupacickarla.local -V -t 4 ssh
```

- lozinka pronađena!

- **offline password guessing napadi**

- koristimo hashcat

```
cat /etc/passwd
```

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

- /etc/passwd —> zastarjela verzija
- /etc/shadow —> novije, samo root može pristupiti
- ?l?l?l?l —> zapis 4 lowercase (l) znaka (?)
- tražimo lozinku pomoću hash vrijednosti (imamo hash lozinke, pa pomoću dictionaryja hashiramo kombinacije slova dok ne naiđemo na jednaku hash vrijednost)
- brute force napad: ~17 dana u našem slučaju
- dictionary napad: ~7 minuta u našem slučaju