

# Lab 6: Online and Offline Password Guessing

## 1. Online password guessing

- preuzeli smo challenge iz datoteke
- naredbom ssh se pokušavamo spojiti na port 22 naredbom ssh
- potrebna nam je lozinka da se spojimo
- lozinka sadrži 4-6 malih slova što znači  $26^4 + 26^5 + 26^6$  mogućih kombinacija
- testiramo brute-force attack pomoću hydre za otkrivanje passworda → predugo traje (otprilike 9,10 godina)
- da ubrzamo, koristimo kreirani dictionary i testiramo manji broj lozinki(490)
- pronašli smo lozinku: **theips**

## 2. Offline password guessing

- pokušavamo naći lozinku za korisnika kojeg odaberemo
- lozinka sadrži 4-6 malih slova
- tražimo lozinku tako da uspoređujemo hash vrijednosti lozinki s hash vrijednostima zapisanim u bazi
- pronašli smo lozinku