Lab 6: Online and Offline Password Guessing

Online Password Guessing

- Za svakog studenta na remote serveru podignut je jedan docker unutar kojeg se vrti servis sshd koji omogućuje povezivanje sa lokalnog racunala preko mreze
- Svaki student će biti u interakciji sa svojin containerom unutar kojeg ima korisnički račun sa korsničkim imenom i hostname-om
- Sa lokalnog računala se pokušavamo spojiti → treba nam šifra
- Spajali smo se na naš local host te pokušali koristiti sa random šifru → neće
- Dodjeljena nam je šifra koja nam treba za pristup
- Ne znamo sifru al znamo da je 4 do 6 malih karaktera **** - ******
- Koliko je space pasworda koji moramo tesirati → 26^4+26^5+26^6 (od aaaa do zzzzzz) → okvirno 26^6
- Koristimo hydra → password cracking tool that uses various network protocols to perform rapid dictionary attacks
- Trebalo bi nam okvirno 10 godina za proći sve
- Kako ubrzati? → Pripremiti neki "pametni dictionary" → prodemo umjesto cijelog dictionary (2^26) oko 70000 mogucih šifri
- Nakon što dobijemo šifru prijavljuemo se na server

Offline password guessing

- Odaberemo korisnika čiju šifru pokušavamo pronaći
- Šifra je 4 do 6 malih karaktera **** - ******
- Uz pomoć hashcat-a i hash vrijednosti odabranog korisnika pronalazimo njegovu šifru sa kojom se možemo prijaviti