

National University of Computer and Emerging Sciences



Assignment # 1

**Student:**

Abdul Rehman ………… 19L-1135

**Section:**

Information Security (BCS-7H)

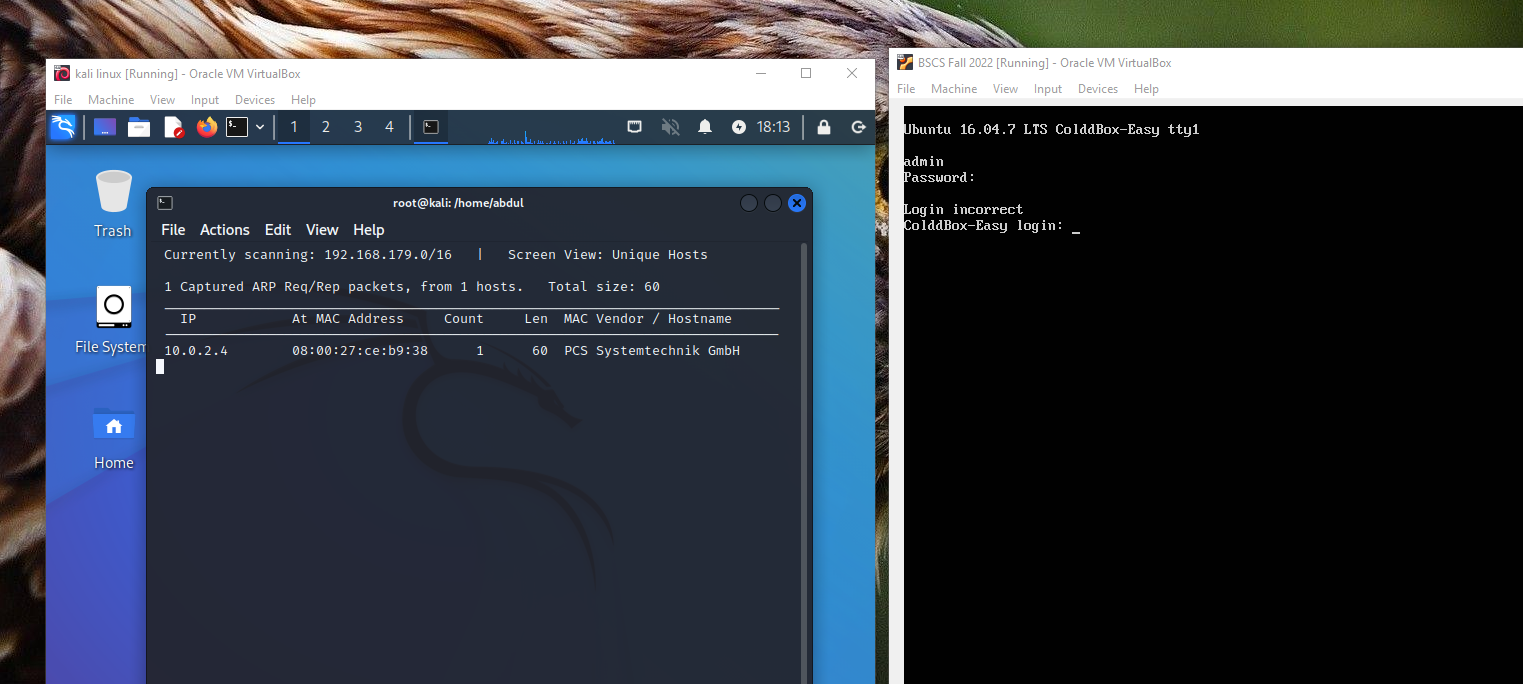
**Instructor:**

**Ahmad Ali Shah**

Report

Getting the target machine IP address

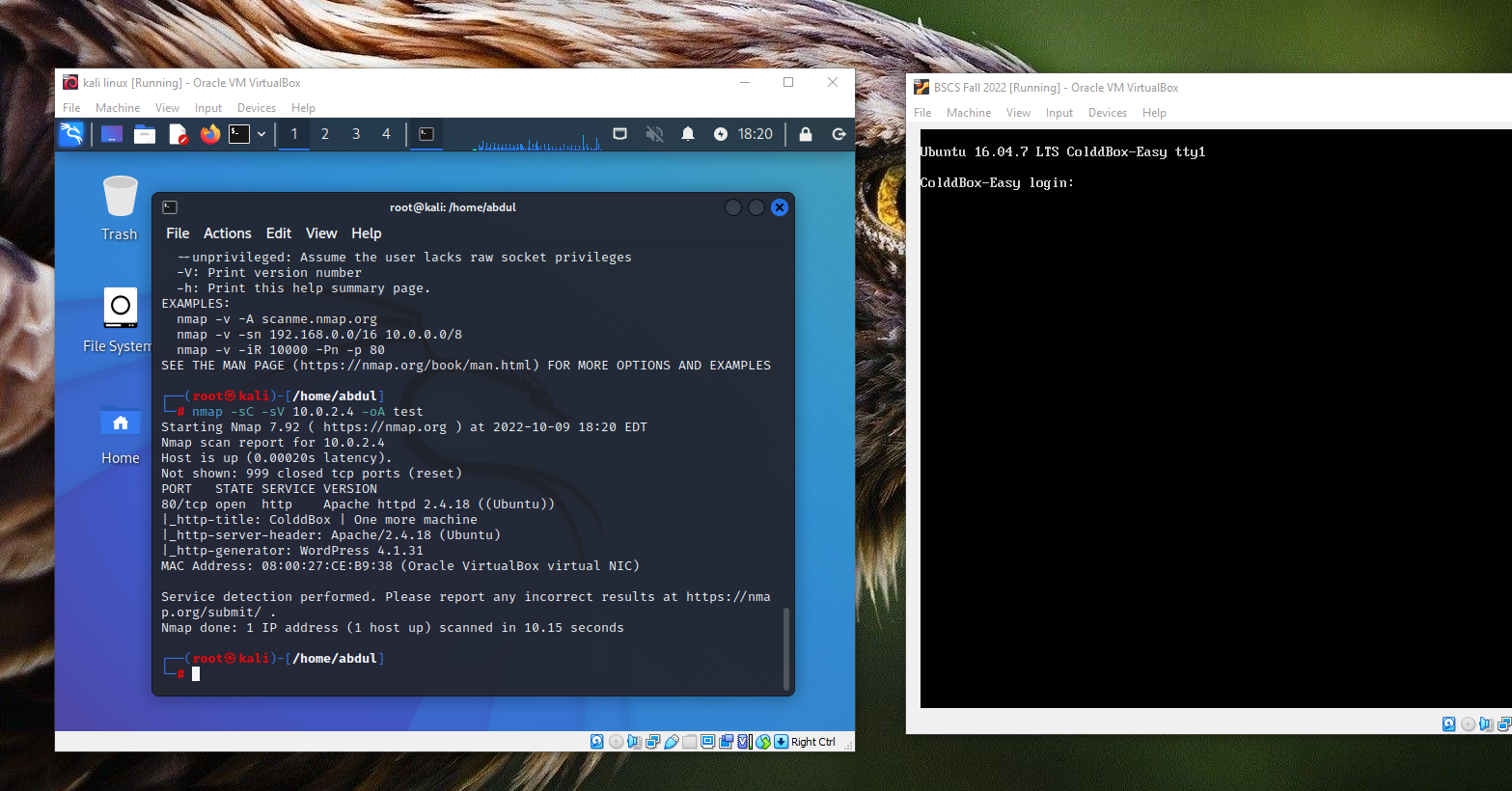
I used a NAT network on VirtualBox and then, I identified the target machine IP address by running the netdiscover command.



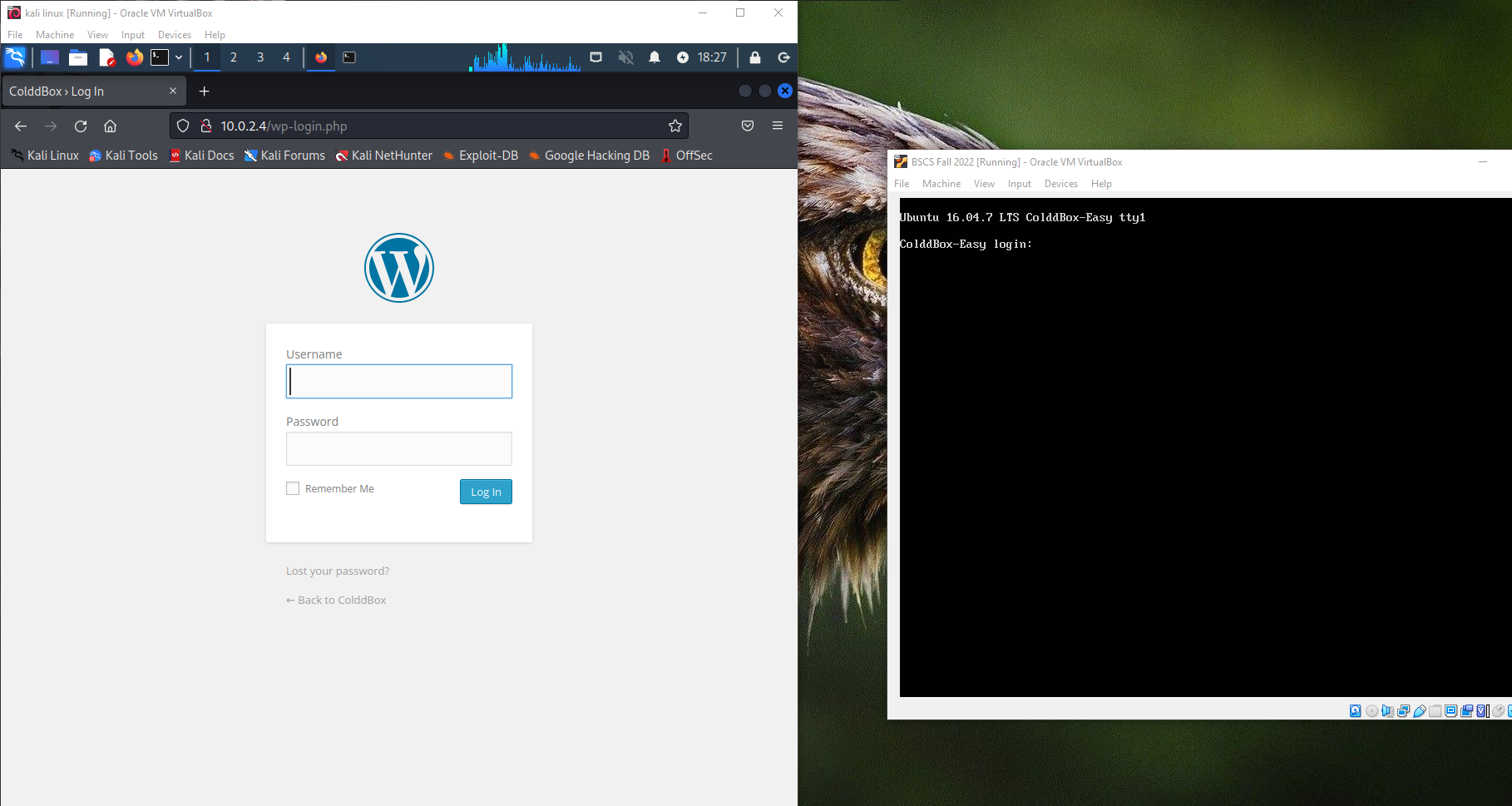
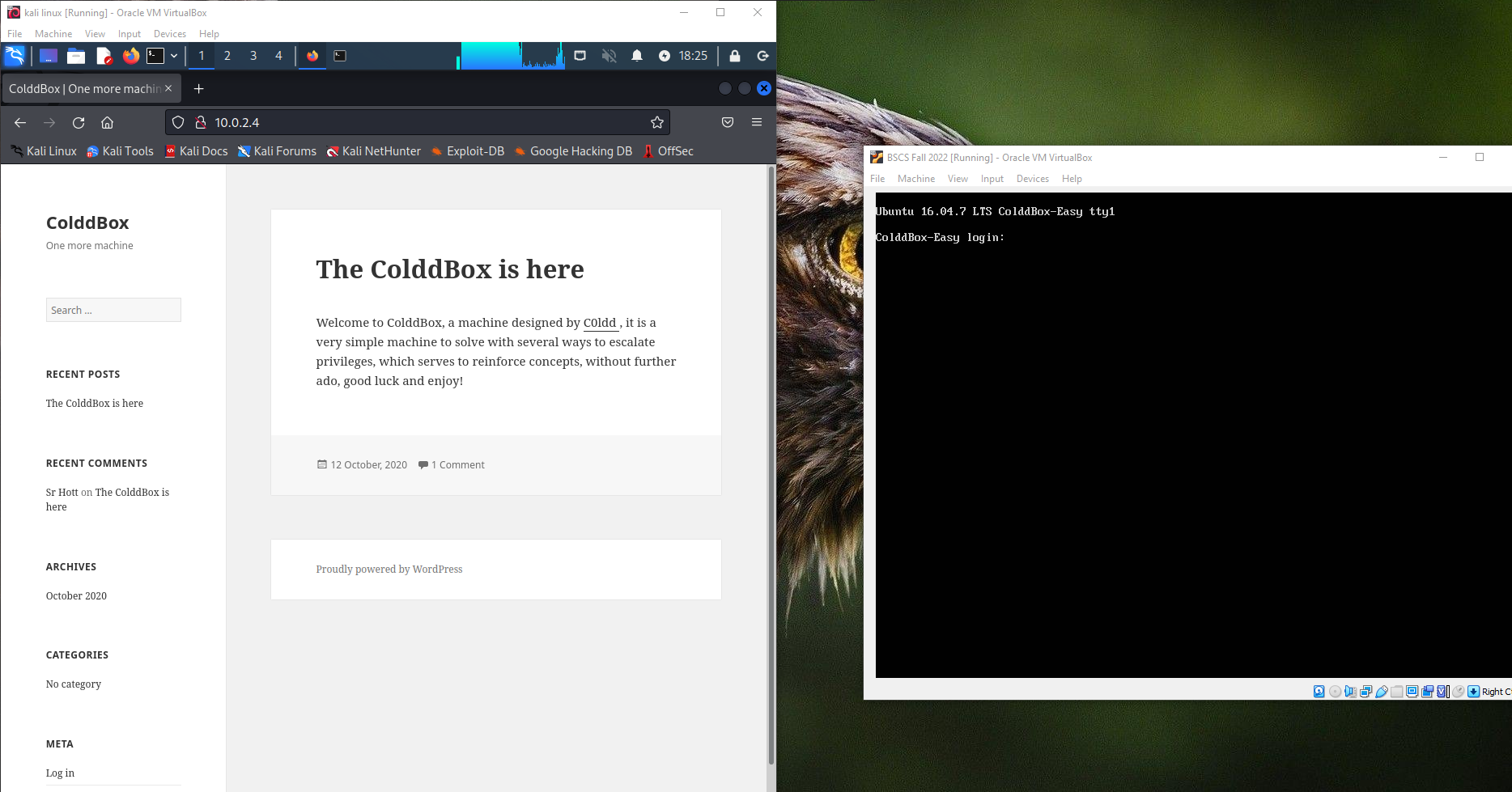
The identified target machine IP was 10.0.2.4.

Getting open port details

After getting the target machine IP address, I used the Nmap command to find the open ports and services on the machine as seen.

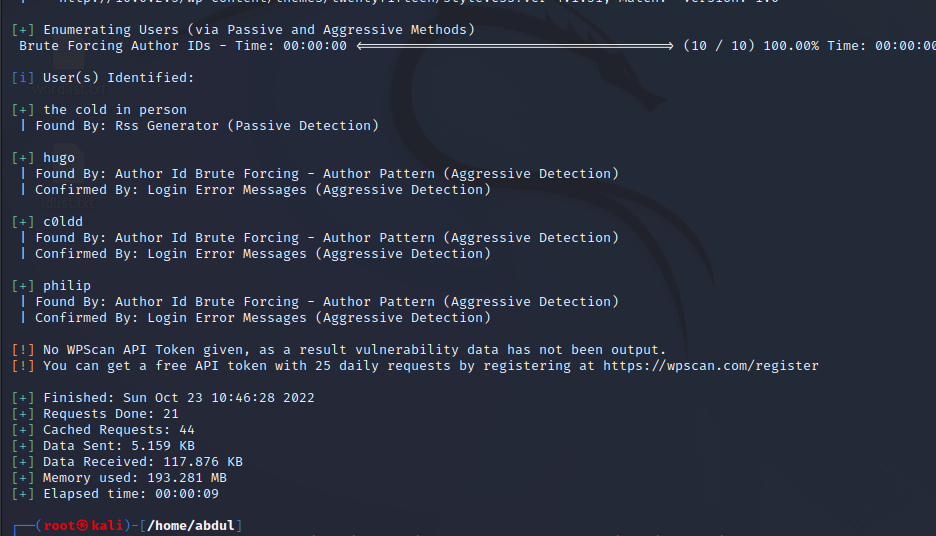


I then opened the target machine IP address on the browser to see the running web application. The admin page was accessible, so I ran a WordPress vulnerability scanner on this website using command wpscan.



Enumerating and Identifying Vulnerability in WordPress

Now, I have to find a way to get access in the website, so in order to do that, I enumerated the username by using the command:   
wpscan --url http://10.0.2.4 --enumerate u

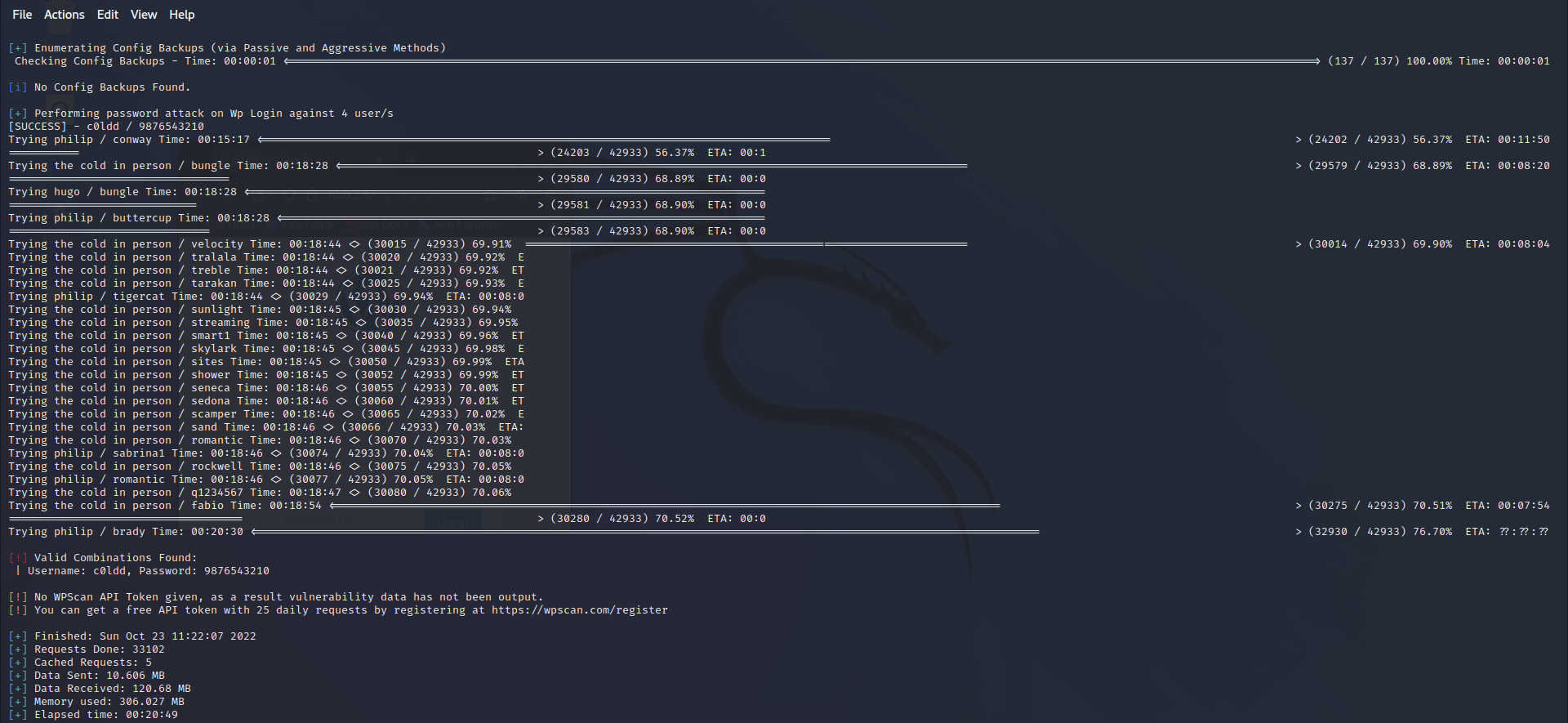
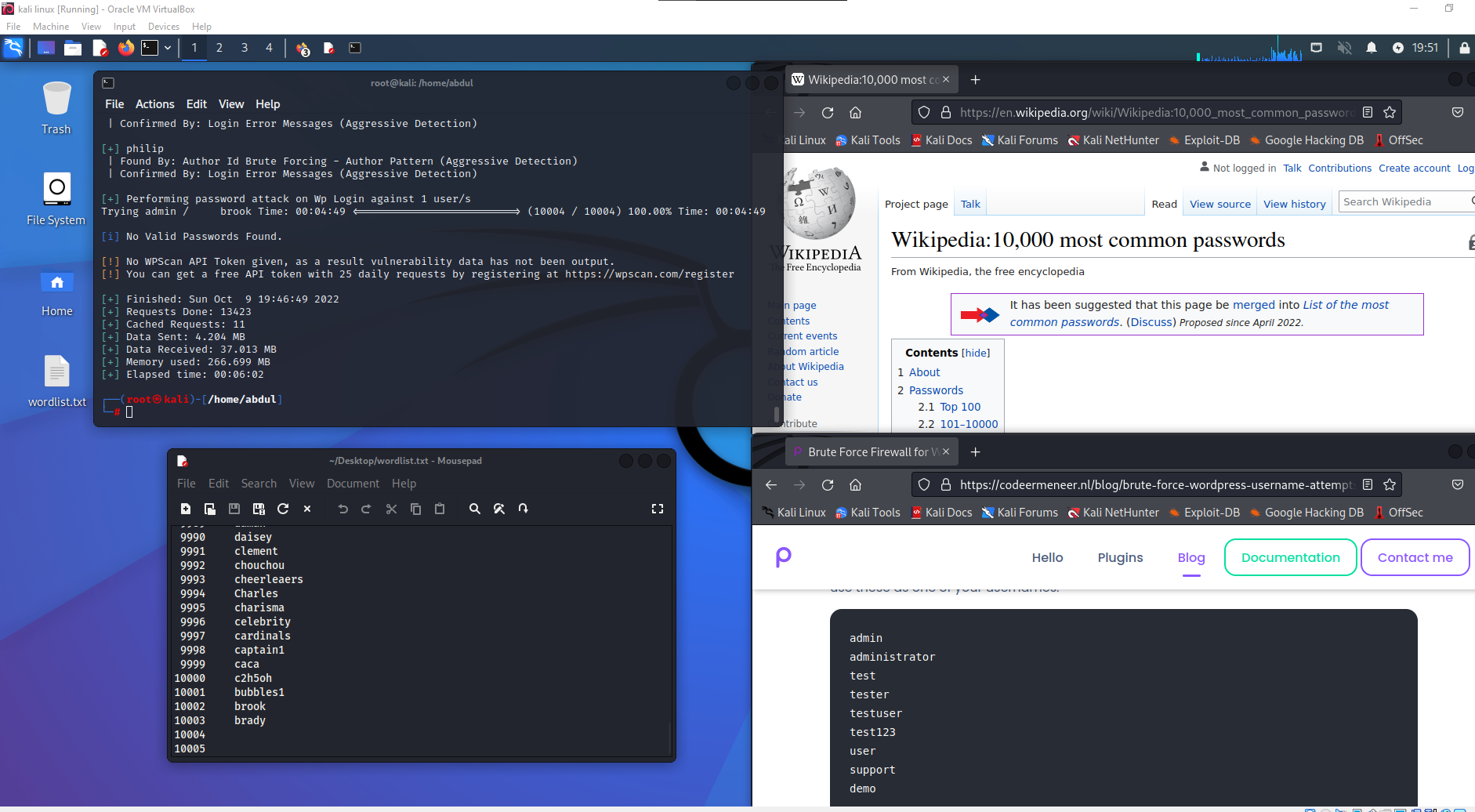


These are the users I was able to identify.

Brute forcing on WordPress login

So, I applied brute force method, creating a file of top 10,000 common passwords and the username list (of the accounts I was able to identify above) for wordpress by using the command:

wpscan --url 10.0.2.4 -passwords /home/abdul/Desktop/wordlist.txt –usernames /home/abdul/Desktop/idlist.txt



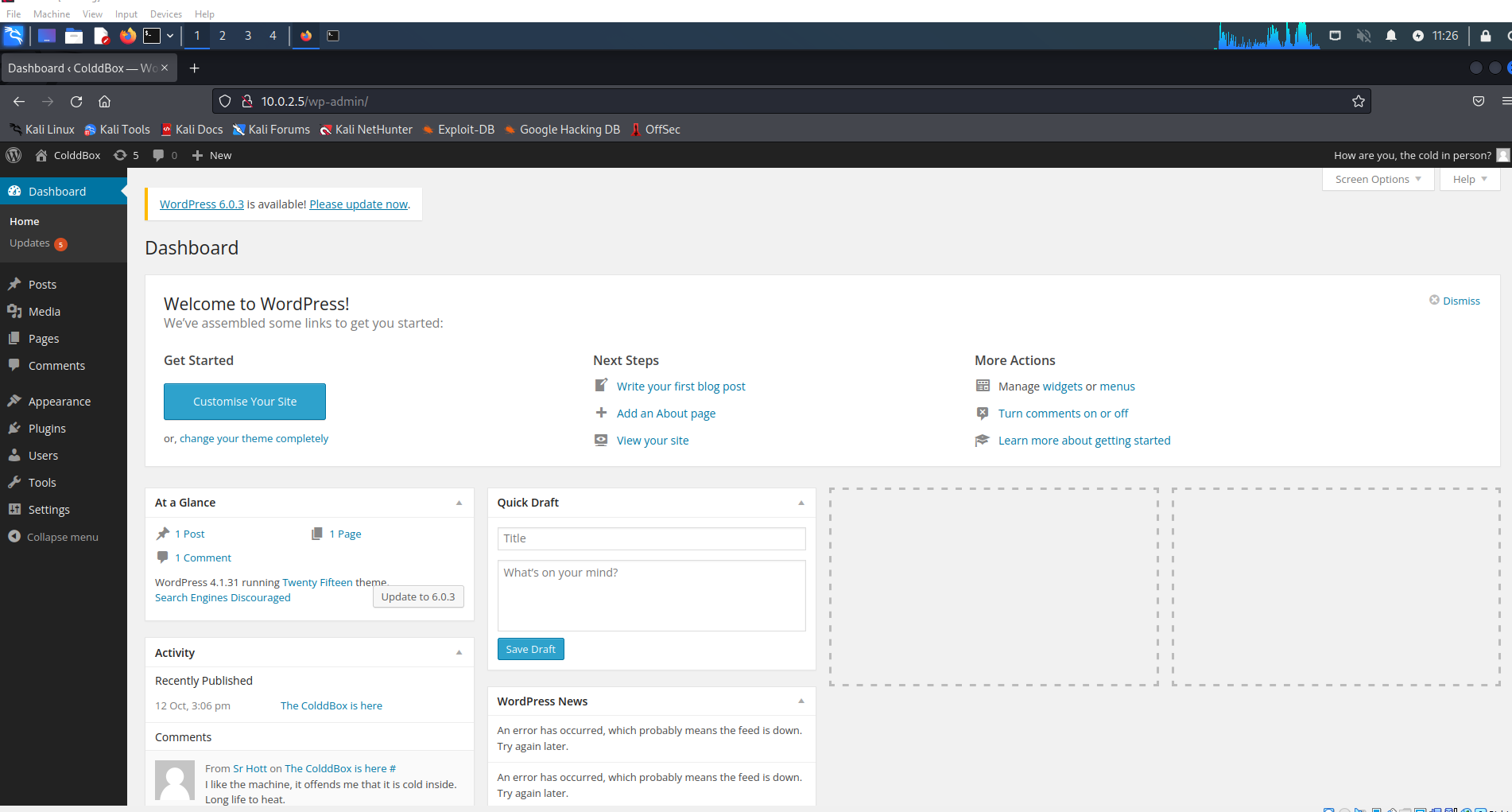
After applying all the possible combination of the provided list of usernames and passwords on the site, the valid credentials that were found were:

Username: c0lld

Password: 9876543210

Login with the detected username and password to open admin dashboard

So, I used the found credentials and was able to access account on dashboard:



In conclusion, I have profoundly understood the working and methods of attack and the mechanism for conducting such attacks. And this was a very informative assignment.