CYBER SHUJAA SECURITY ANALYST

COHORT 2 - 2024 MID EXAMINATION

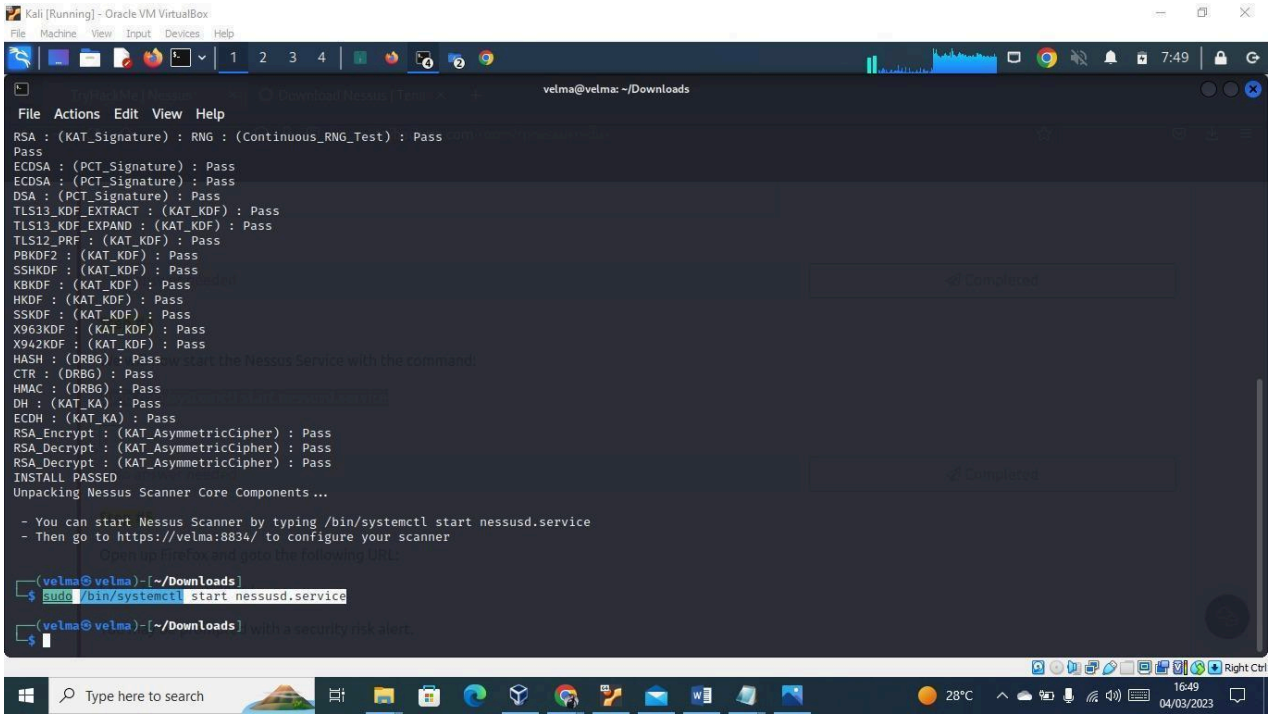
PRACTICAL QUESTIONS

TIME ALLOWED: 2 HOURS

TOTAL: 30 MARKS

Instructions:

1. Answer **ALL** questions
2. The exam should **NOT be** worked on in groups or with assistance from others.
3. Use this file as your write-up reporting template as you complete each task outlined and answer the questions.
4. Rename this file with your full names and Cyber Shujaa ID.
5. Once you have completed your work, save the file and upload it for marking.
6. Before leaving the exam, ensure you have uploaded the correct file capturing all the work you have submitted for marking.
7. Ensure you compile a detailed report write-up that outlines your approach to addressing the various exam challenges. Ensure that your write up is authentic. Show screenshots of the working for all answers showing how you got your answers.
8. The screen shots should capture your full screen and display the command you ran to get the answer. Include a taskbar showing your machine taskbar and time stamp.

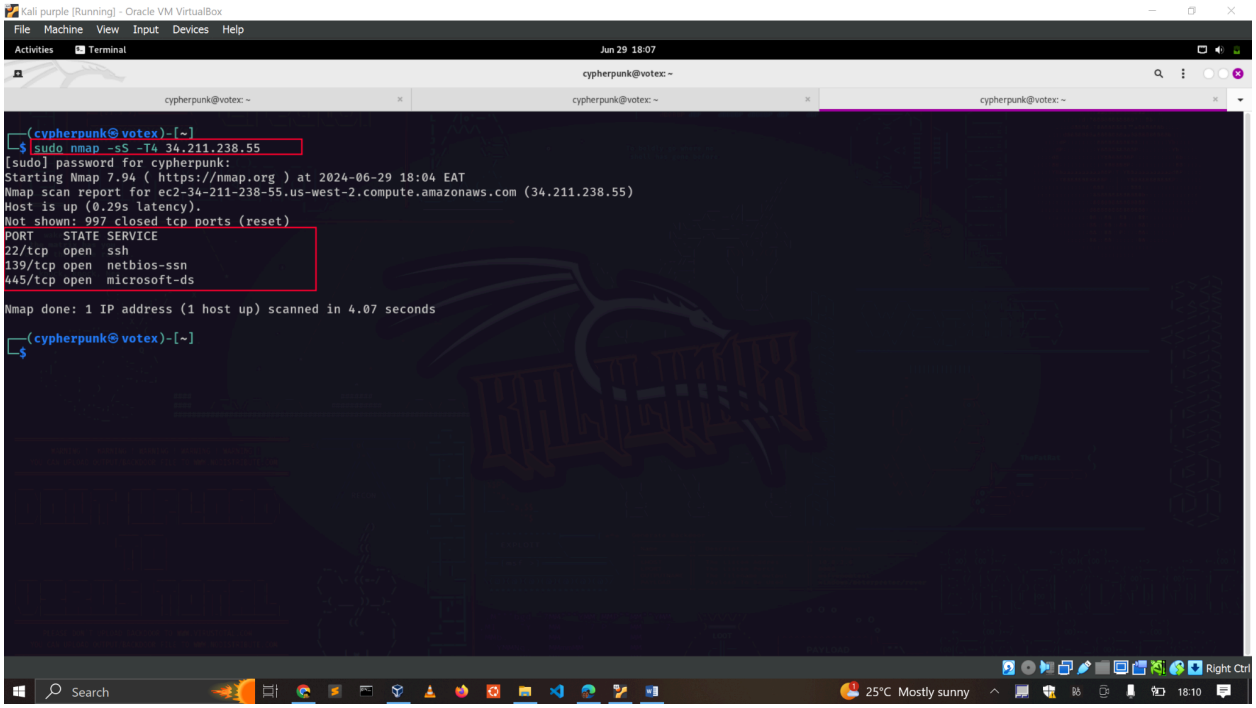


MID EXAM PRACTICAL (30 marks)

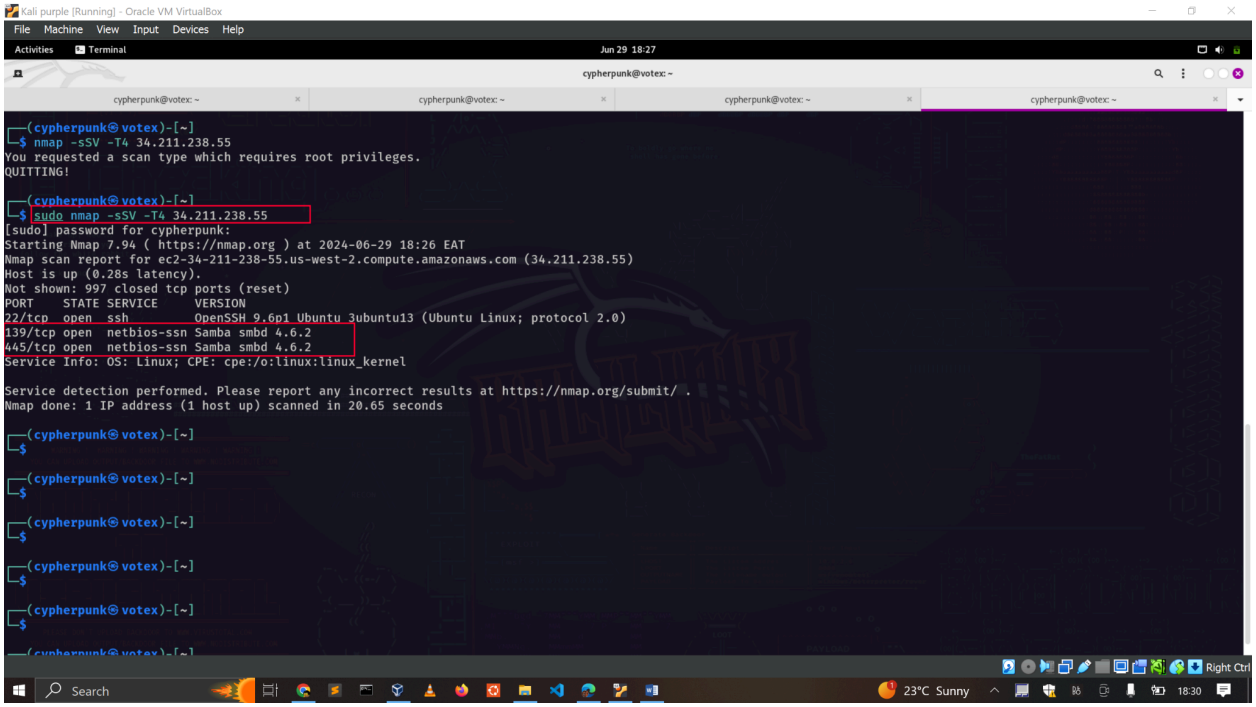
Retrieve the credentials required to log on to the provided server and answer the questions below.

QUESTIONS

1. Conduct an Nmap scan on the provided Linux machine. Identify the open ports. (2 mks)
    - Port 22,139,445.

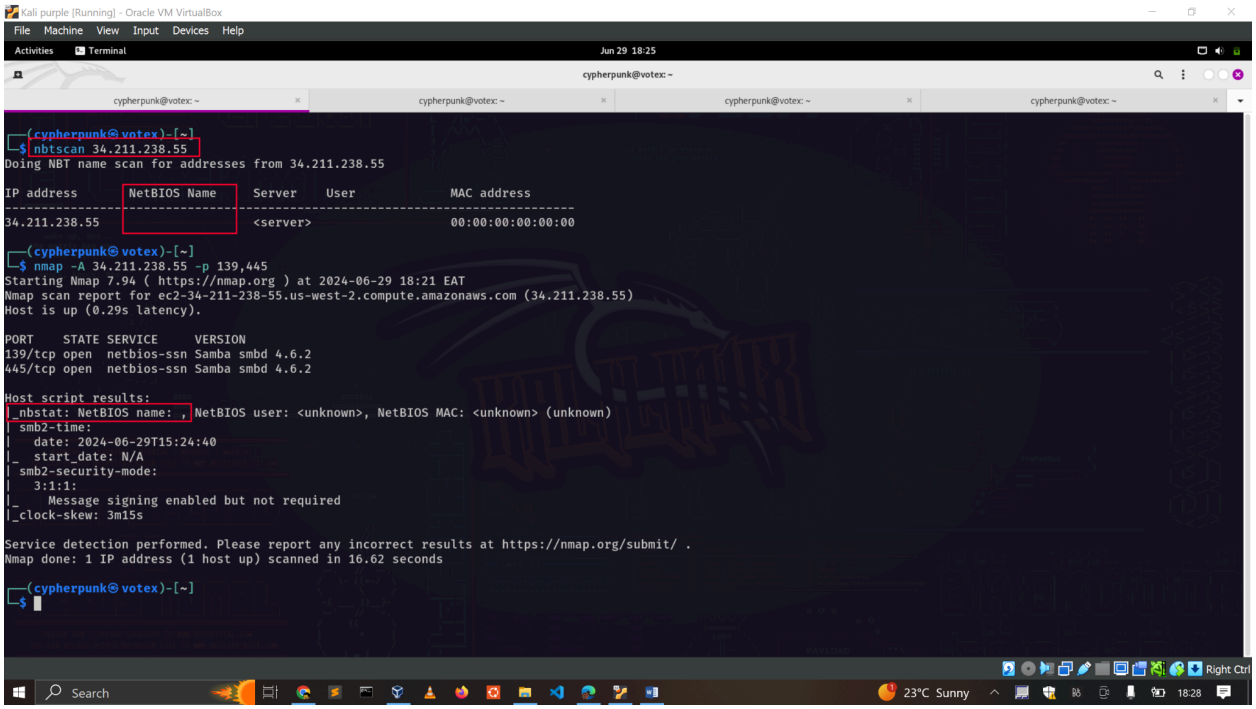


2. A service is running on more than one port of the system. What is the version of the service? (1 mk)
    - Samba smbd 4.6.2

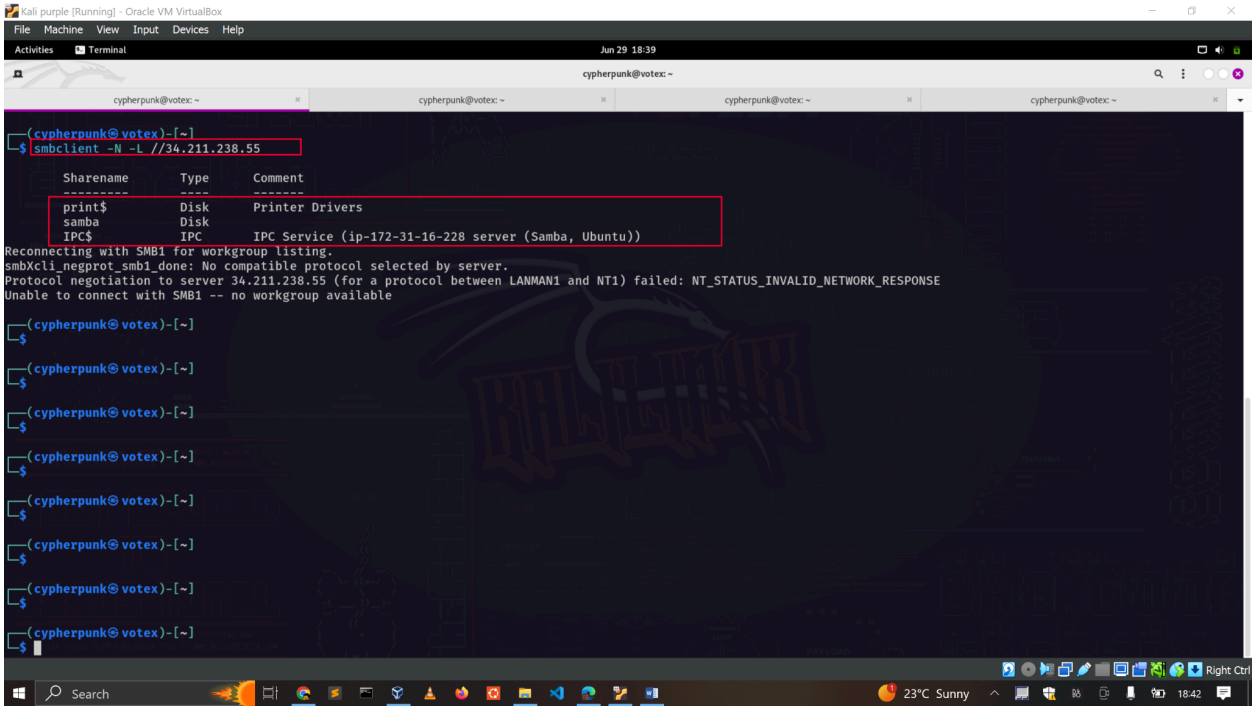


3. What is the netbios name of the server? (1 mk)

The server has no NetBios name since it is a Linux Machine. NetBios Names are assigned to Windows Computers only.



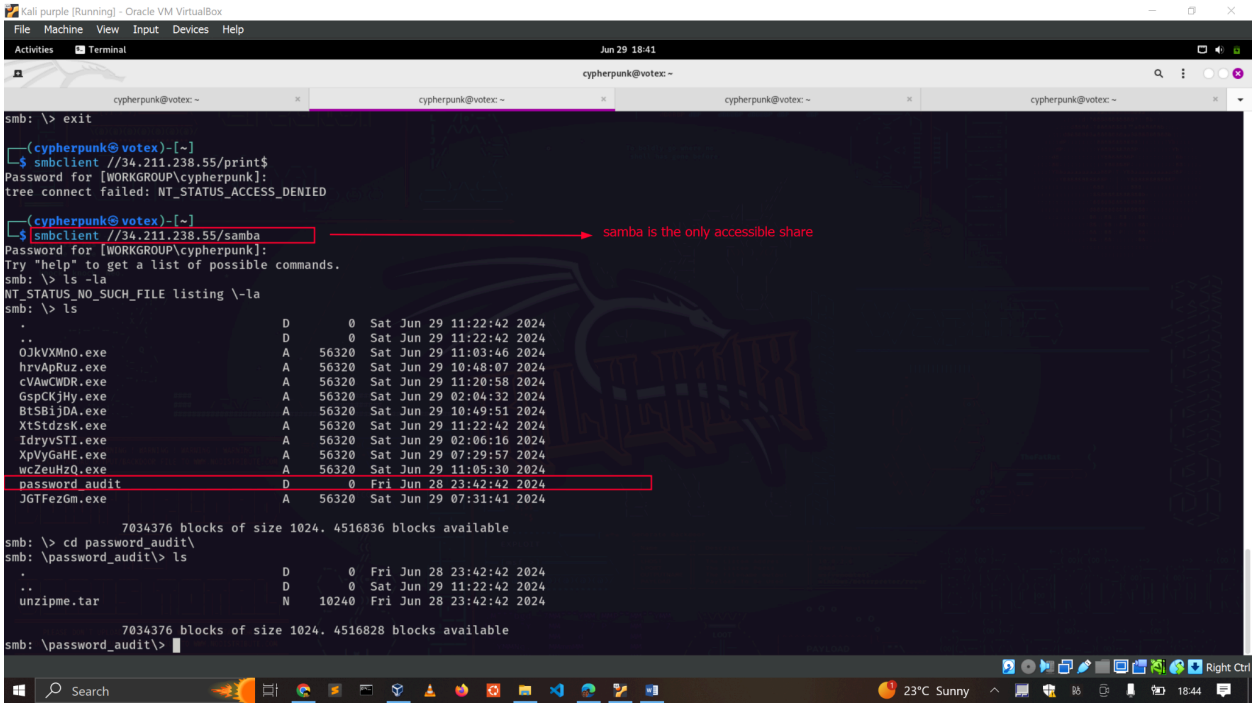
4. Using smbclient tool identify the available shares (2 mks)
    - The available shares are 3, the print$, samba and IPC$ share.



5. How many hidden shares are among the identified shares above. Name them. (2 mks)
    - From the screenshot above, there are two hidden shares. The ones appended with the $ at the end, that is, print$ and IPC$

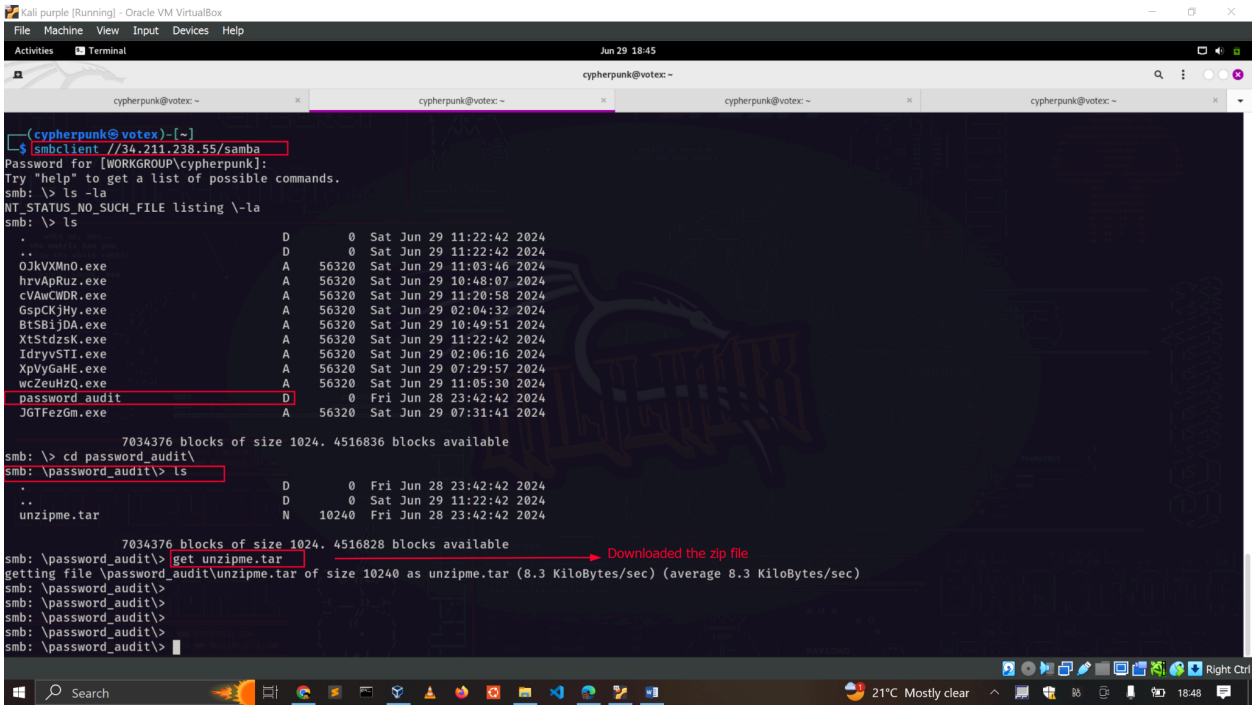
Note: The screenshots are large since I took them using flameshot. I will use the above screenshot for this question to keep my report within the filesize limit.

6. What is the name of the share that is accessible? (1 mk)
    - The samba share is the one accessible.

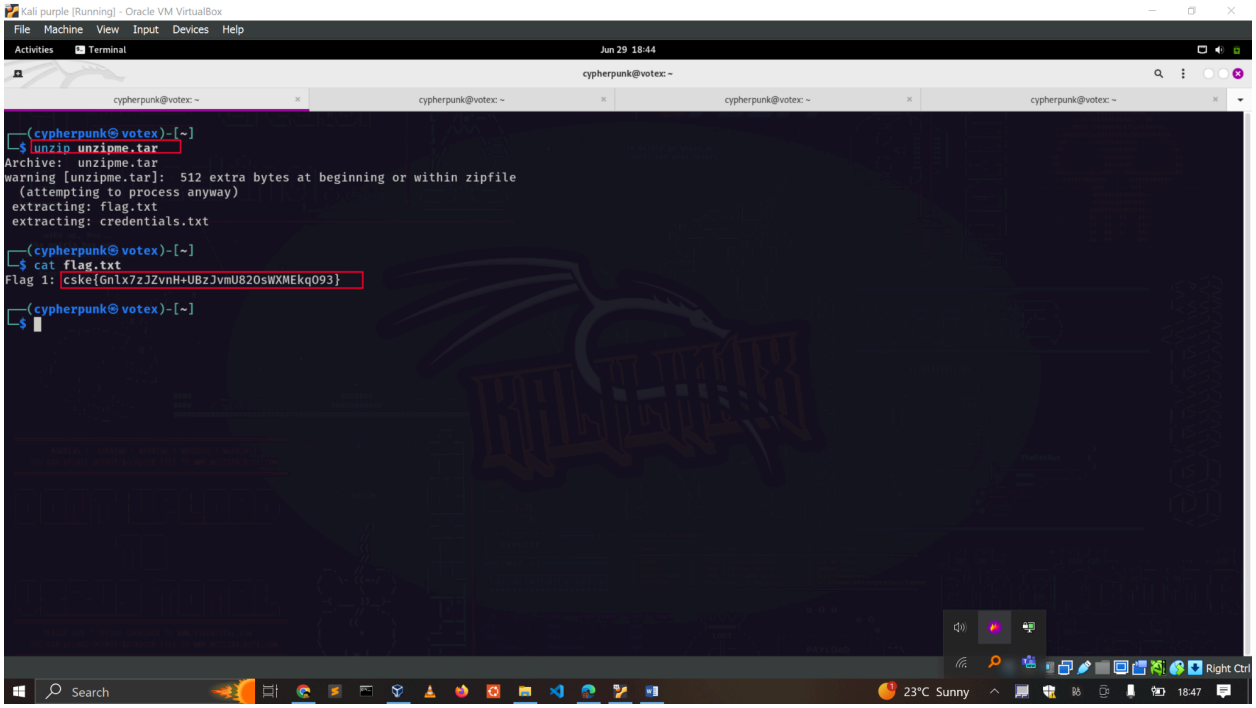


7. Access the share using null authentication, what is the folder's name discovered within the share? (2 marks)
    - Foldername is **password_audit** as highlighted above

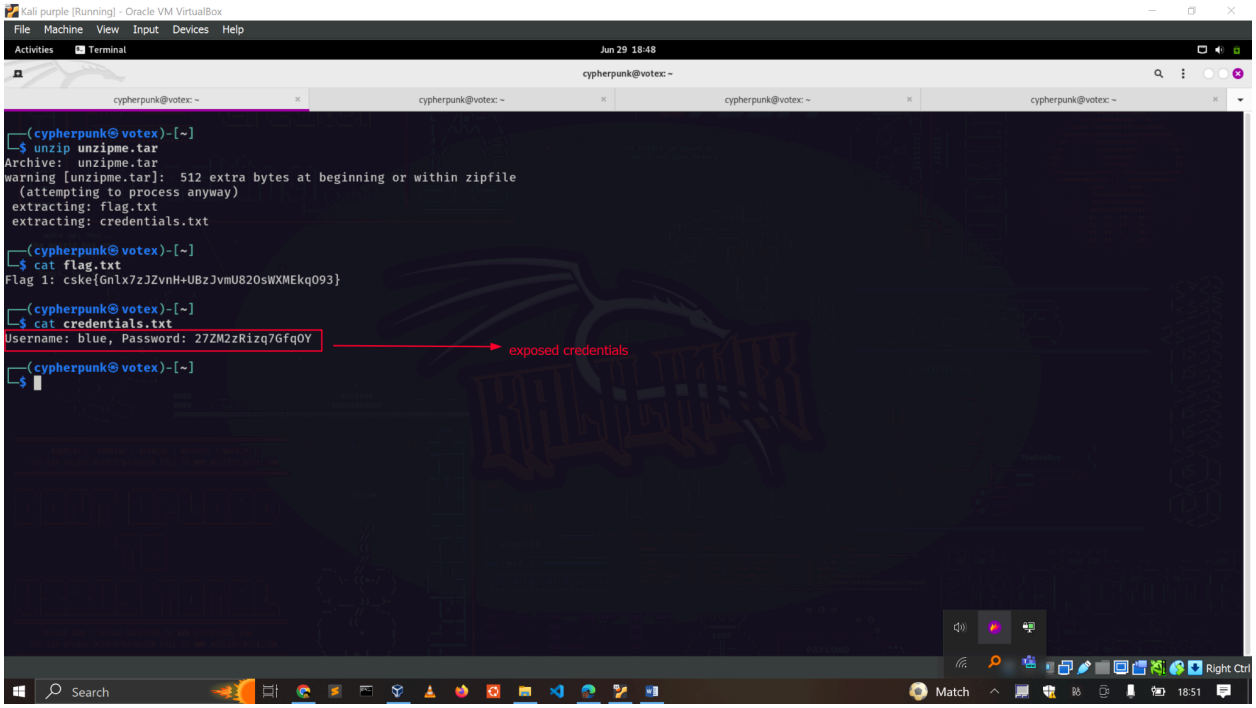
8. Download the files inside the folder and read the contents. What is the flag? (2 mks)



- After downloading the file using the get command and unzipped it, we can see the flag highlighted below.

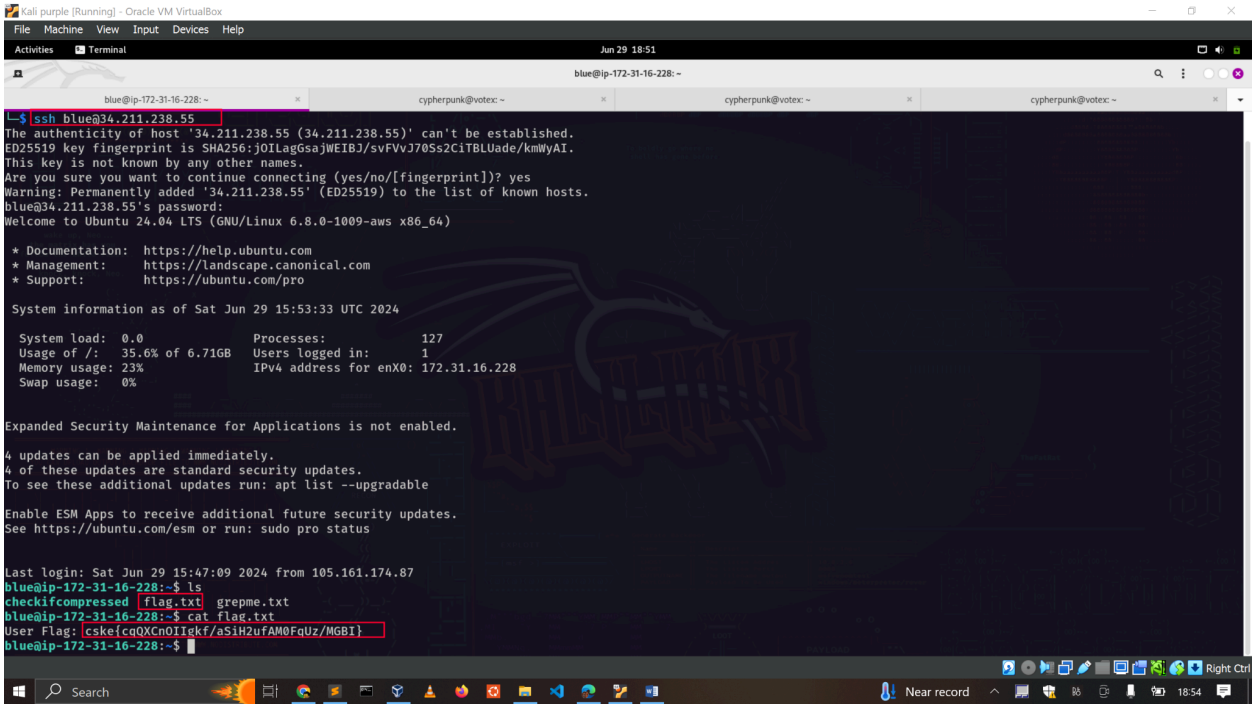


9. What is the exposed username and password? (1 mk)
    - The exposed username and password are highlighted below.



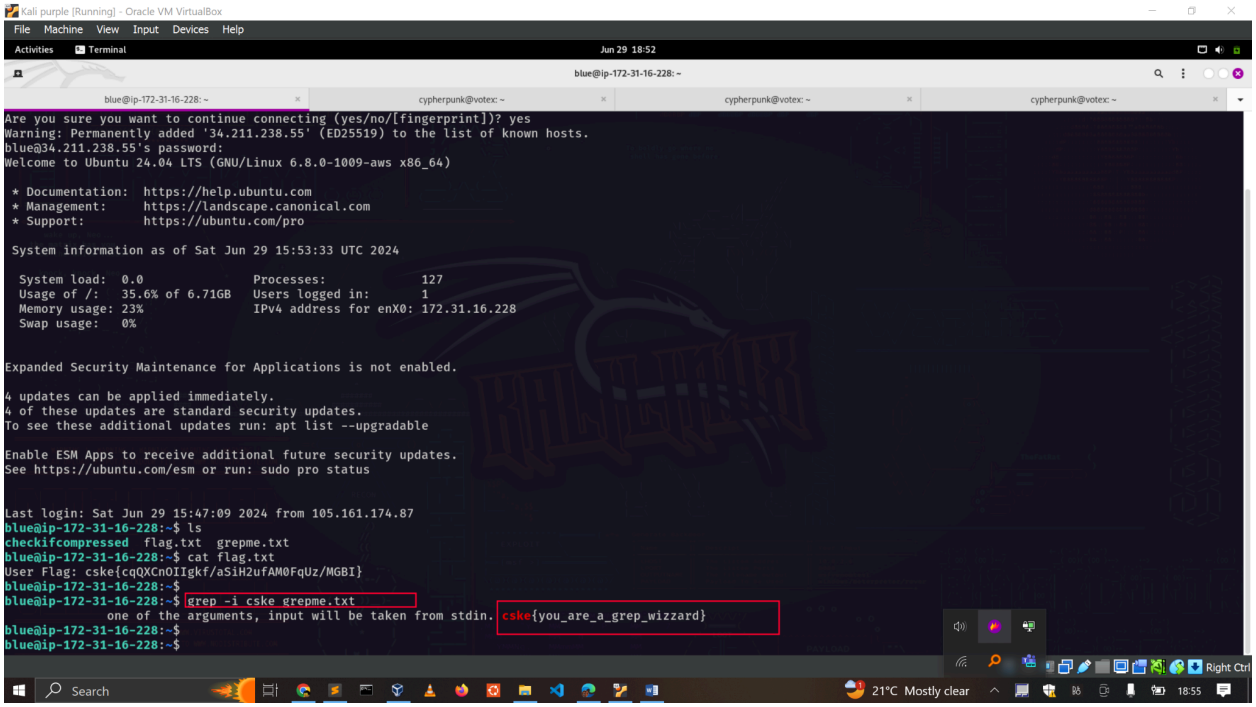
10. Ssh into the machine and retrieve the flag in the user's home directory. (1 mk)

- The flag is highlighted in the screenshot below.



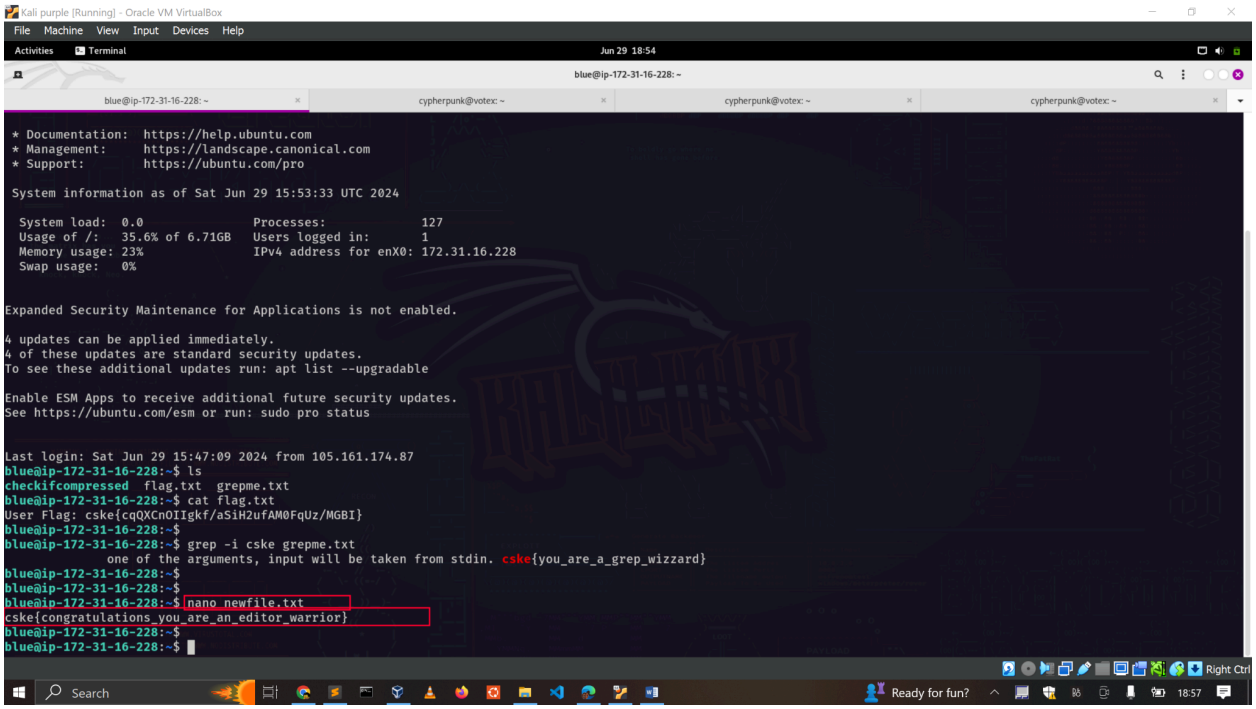
11. Using grep retrieve a flag hidden in the grepme.txt within the user's home directory (2 mks)

- From the the command **grep -i cake grepme.txt** we can retrieve the highlighted flag as shown below.



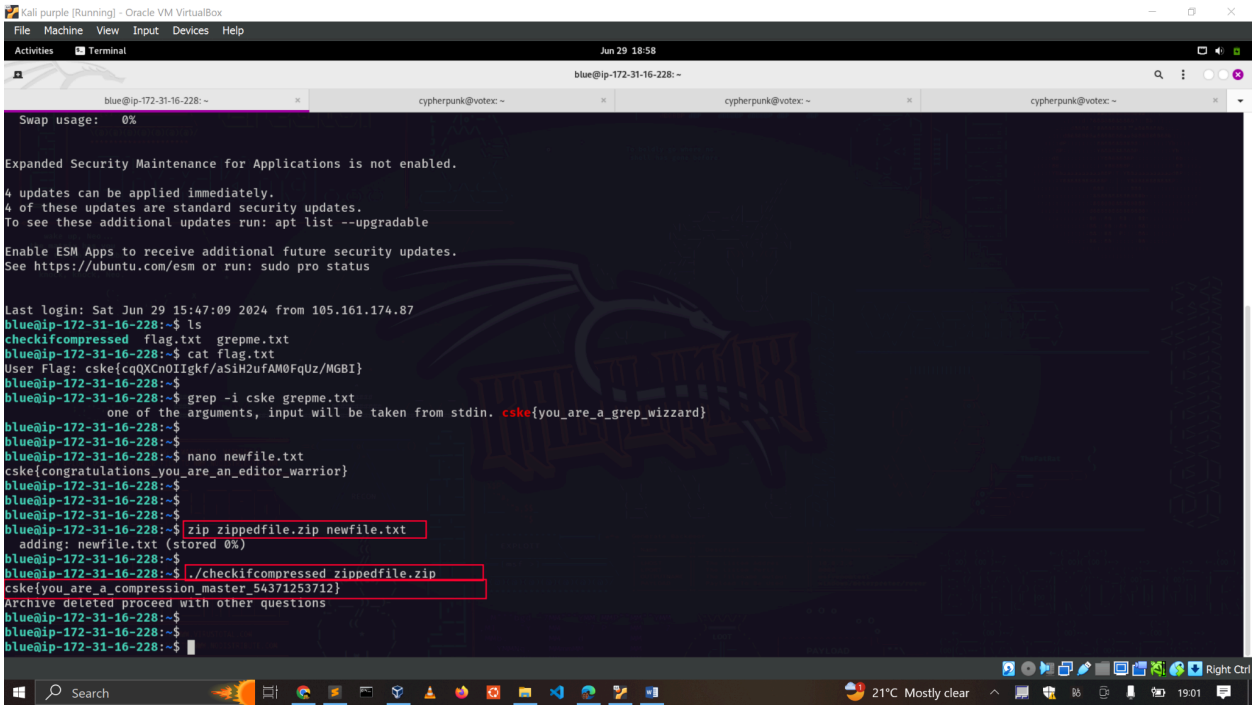
12. Using any editor installed on the server, create a file with the content cybershujaa_exam, save the file, and retrieve the flag. (2 mks)

- After creating a file name **newfile.txt** the flag pops up ash shown below.

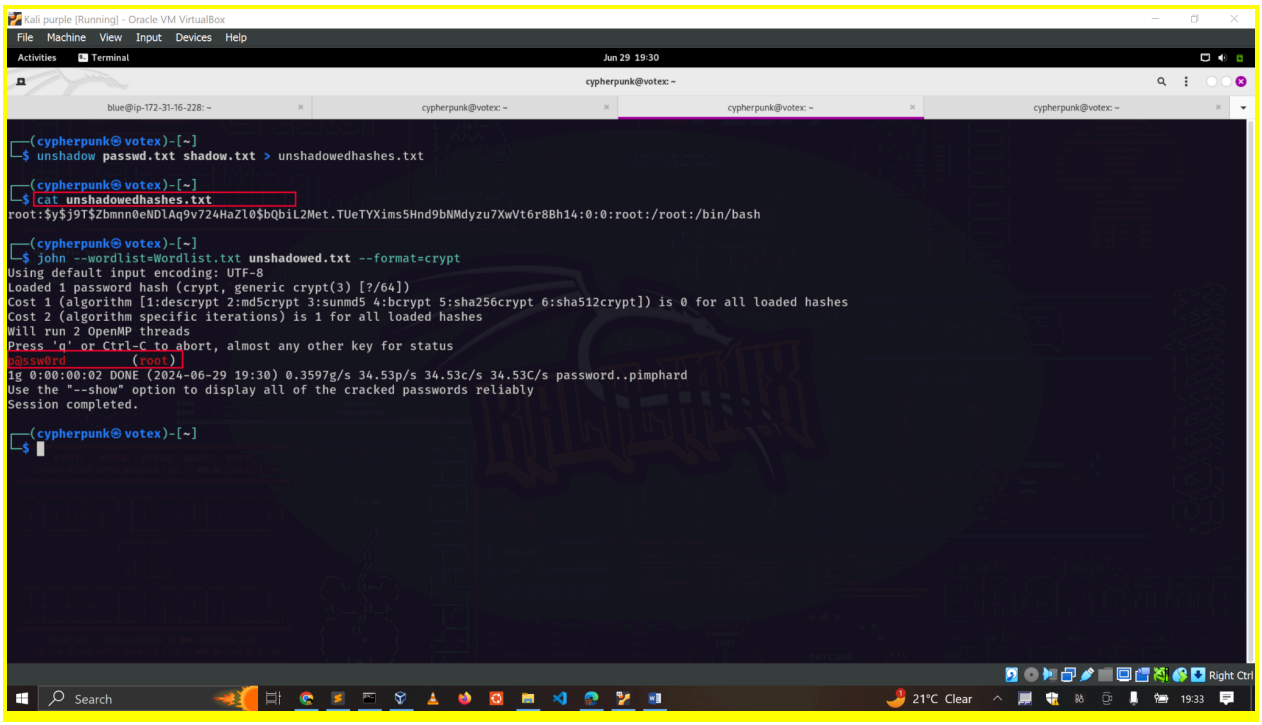


13. Using zip compress the file you have just created above, then run the binary in the user's home directory called "checkifcompressed" giving the name of your zip file as an argument. What is the flag? (4 mks)

- The command **zip zippedfile.zip newfile.txt** compresses our file.
- Running the binary to confirm compression reveals the flag.



14. A misconfiguration is on the shadow file allowing users to read its contents. Retrieve both the password file passwd and the shadow file. Unshadow and crack using John. What is the root password?Use the provided wordlist. (5 mks) HINT: use the format –format=crypt



15. Retrieve the root flag.txt from the root user's home directory. (2 mks)