CISCO EXAM –WRITE UP

FLORENCE MUSIMBI MWITA CS-EH03-25129.

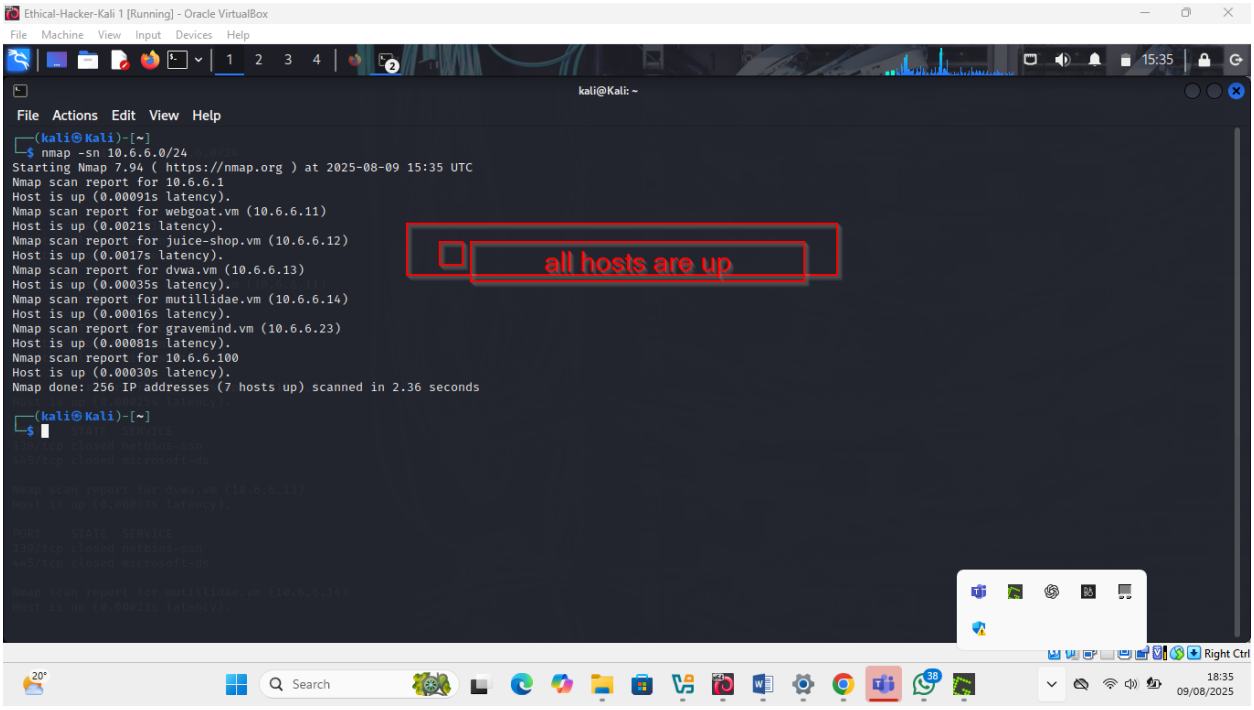
1.RECONNAISANCE

1.Using Nmap, find the different hosts running on the subnet and describe each of them: 10.6.6.0/24. (5 Marks)

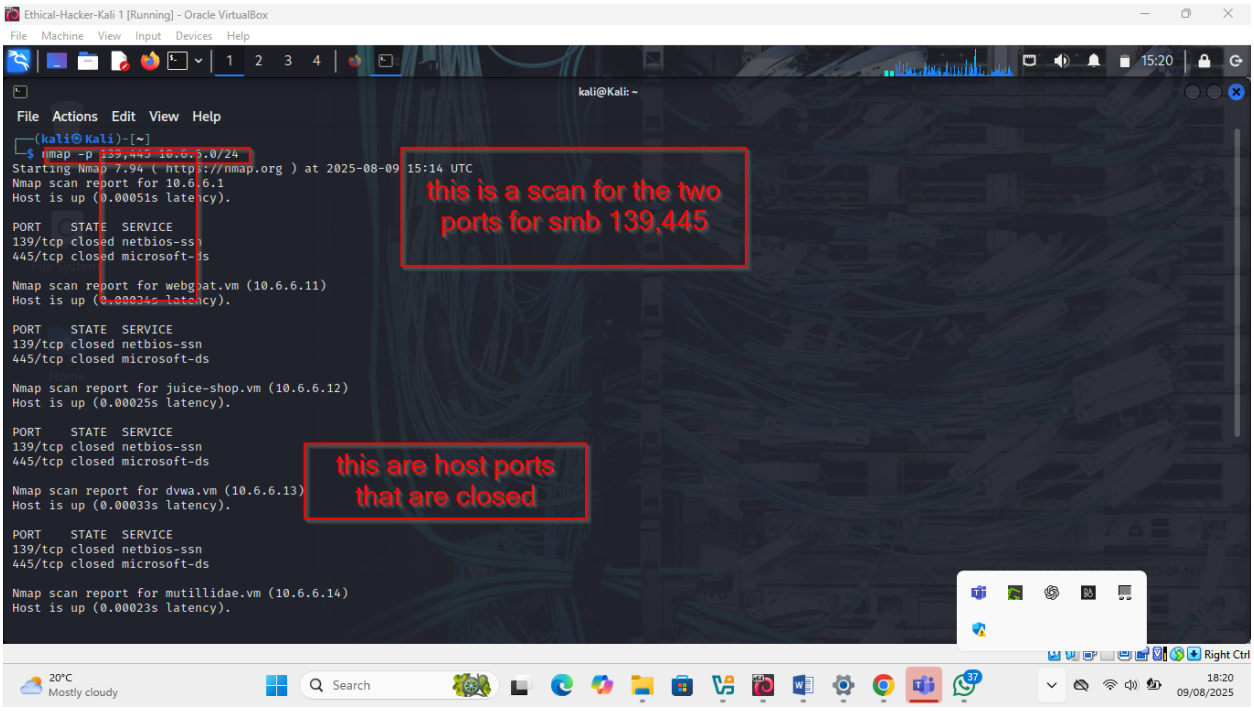
Answer format: 10.6.6.x Server X, 10.6.6.xx Server Y, 10.6.6.xxx Server Z

Paste screenshot(s) demonstrating the answer here

We are scanning hosts running on the subnet being that its smb we are going to do a direct scan by using nmap –p 139,445 10.6.6.0/24



This shows all hosts are up hence we'll use the other commands of nmap since its an smb scan



Most ports are closed but two ports are open which are

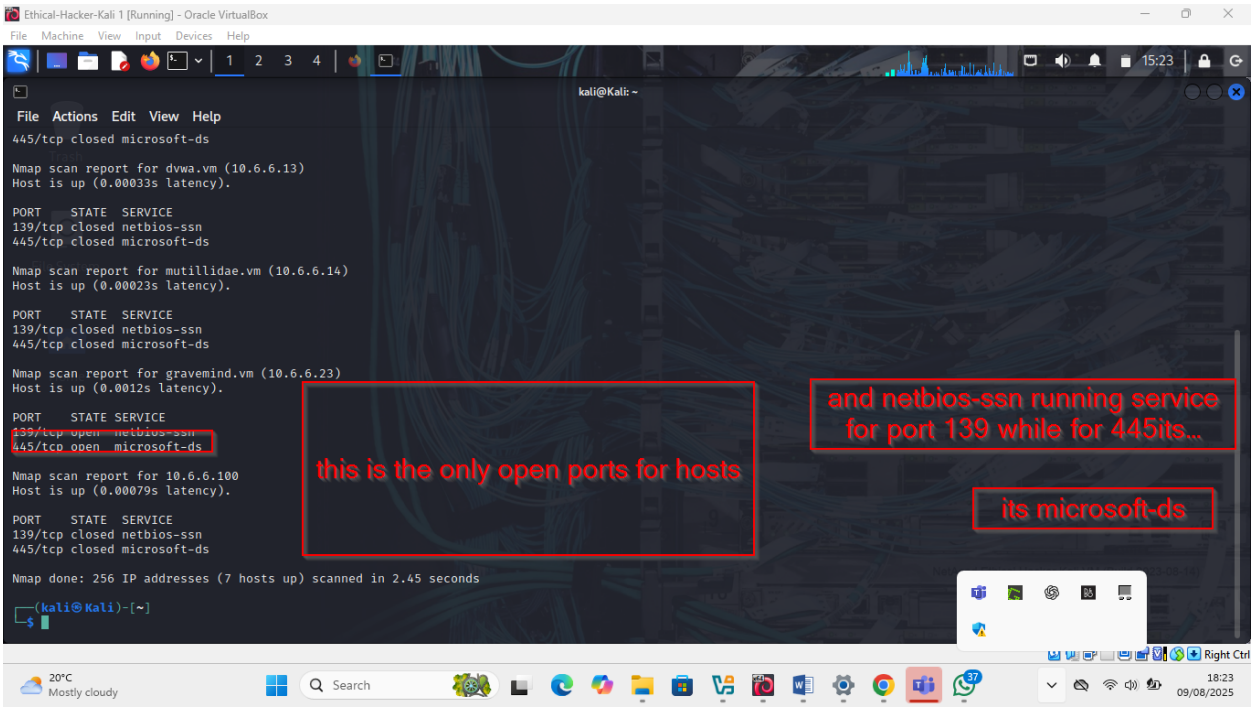
map scan report for gravemind.vm (10.6.6.23)

Host is up (0.0012s latency).

2.Which of these host IPs shows open SMB ports? (3 Marks)

Answer format: 10.6.6.x

Paste screenshot(s) demonstrating the answer here



PORT STATE SERVICE

139/tcp open netbios-ssn

445/tcp open microsoft-ds

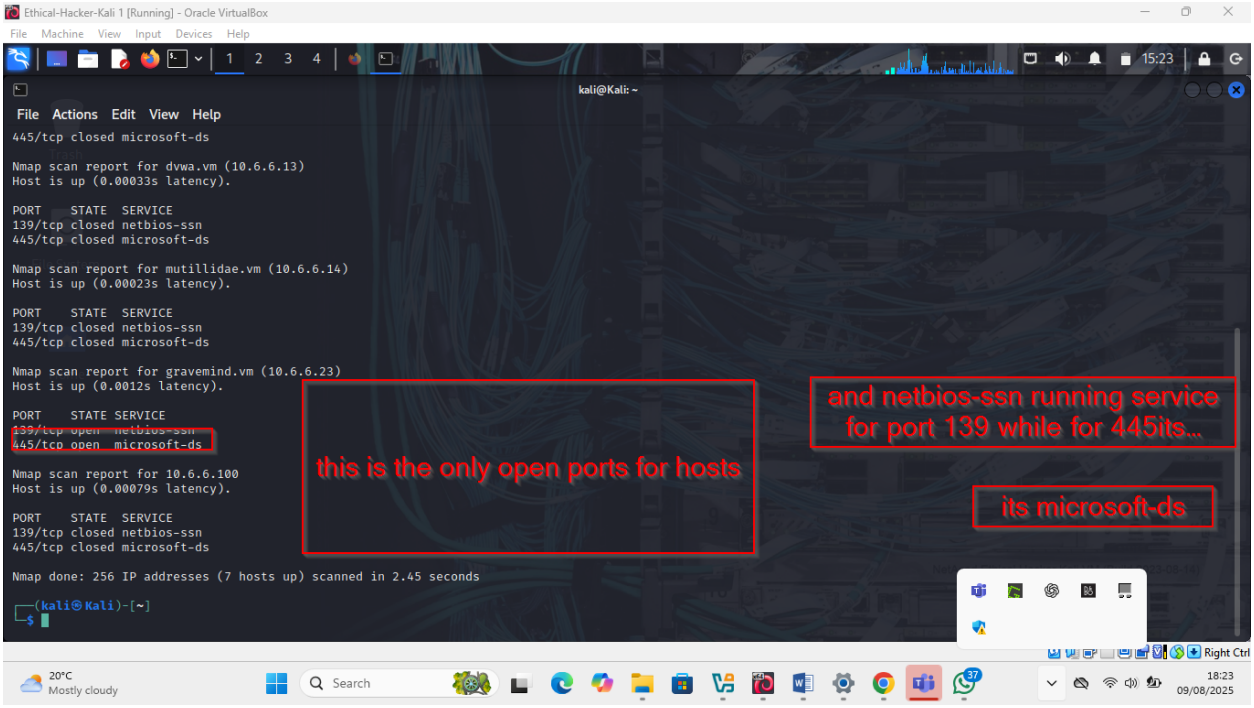
10.6.6.23 is the ip address of the host that is up

3.What specific open ports indicate that a device is running SMB services? (2 Marks)

Answer format: Ports 123, 567

Paste screenshot(s) demonstrating the answer here

3. the ports that indicate that the port is running smb services is the port 139 and 445



ENUMERATION PHASE

4.Use an enumeration tool to discover available SMB shares on the host identified in (2).

Q4a: List all the discovered share names. (5 marks)

Answer format: Share 1, Share 2, Share 3...

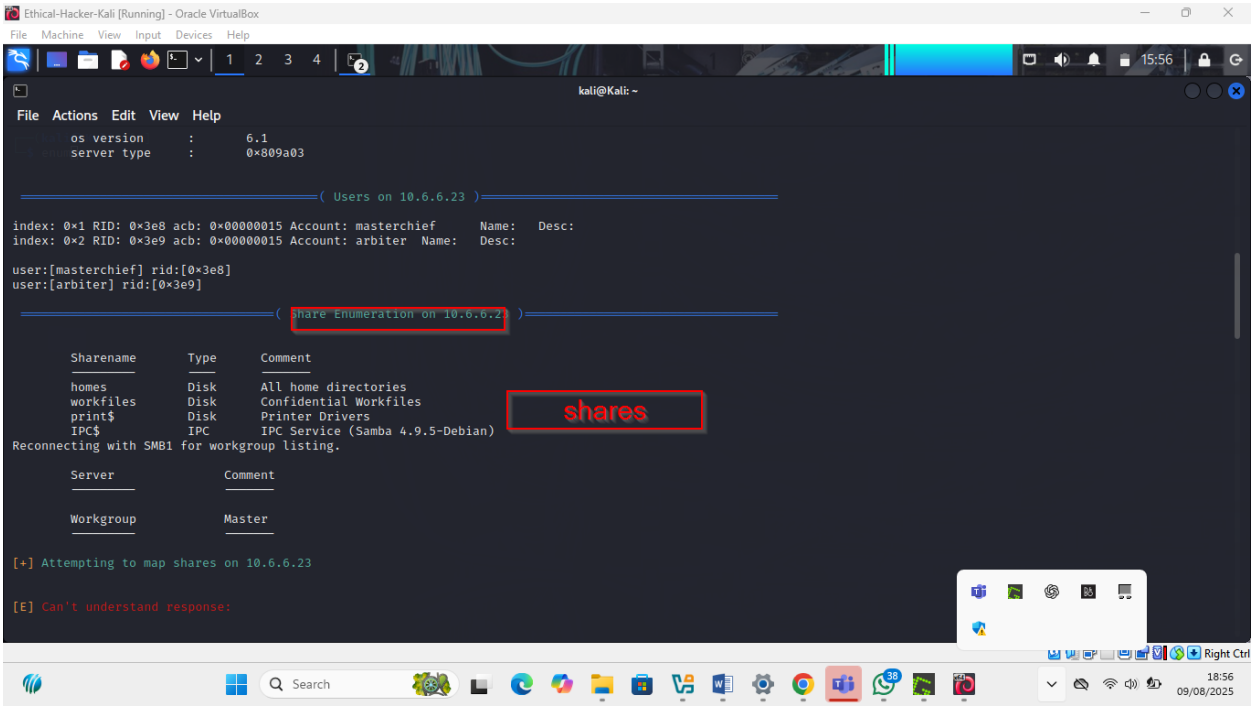
Paste screenshot(s) demonstrating the answer here

Q4b: Which of these shares are accessible without credentials (as an anonymous user)? (5 marks)

Answer format: Share name1, Share name2, share name2 …

Paste screenshot(s) demonstrating the answer here.

This enum4linux is the used to list shares



This is the shares I have found after enumerating

Share1:homes	Disk	All home directories

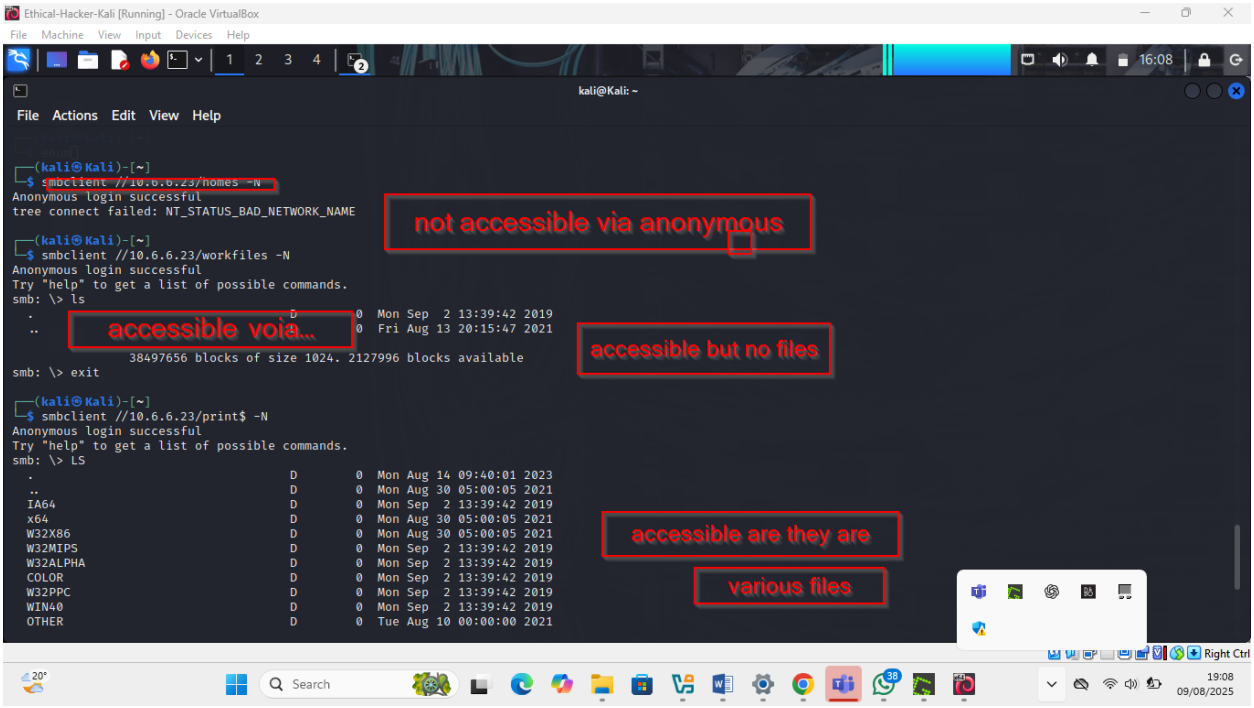
Share2: workfiles Disk Confidential Workfiles

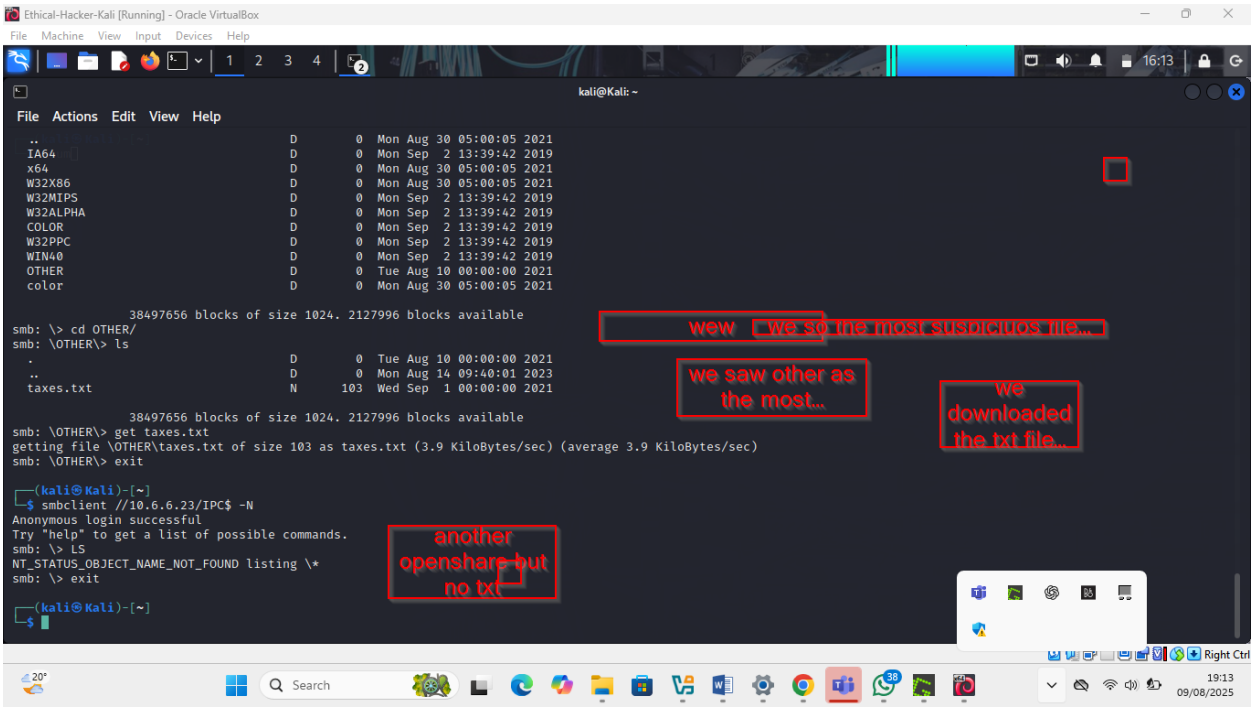
Share3: print$ Disk Printer Drivers

Share4: IPC$ IPC IPC Service (Samba 4.9.5-Debian)

EXPLOITATION PHASE

4b.





These screenshots show how we tried to acess different shares and some were accessible but no file while this were accessible are as follows

SHARE1;Workfiles

SHARE2;Print$

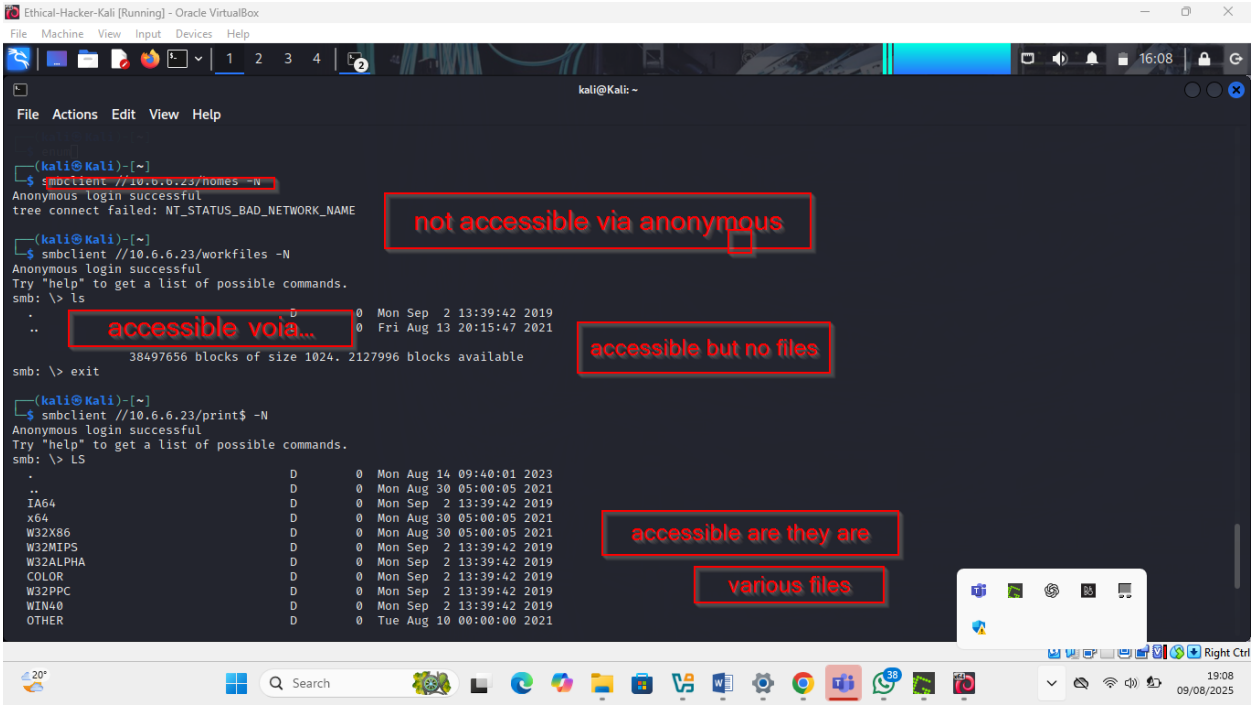
SHARE3;IPCC$

But only print$ had the text file to open

Part B: Access and Exploration (20 Marks)

Describe how you would use SMBCLIENT or an equivalent tool to connect anonymously to one of the discovered shares. Demonstrate this and provide the command used. (5 Marks)

Paste screenshot(s) demonstrating the answer here.



These screenshots shows how I accessed the files the command

smbclient //ip address/shares –N

1.so In the first share I used smbclient //10.6.6.0/homes –N

This could not access anonymously

2.smbclient // 10.6.6.0/workfiles –N

This could be accessed anonymously but no files in its directory

3.smbclient //10.6.6.0/print$

Which got various files..

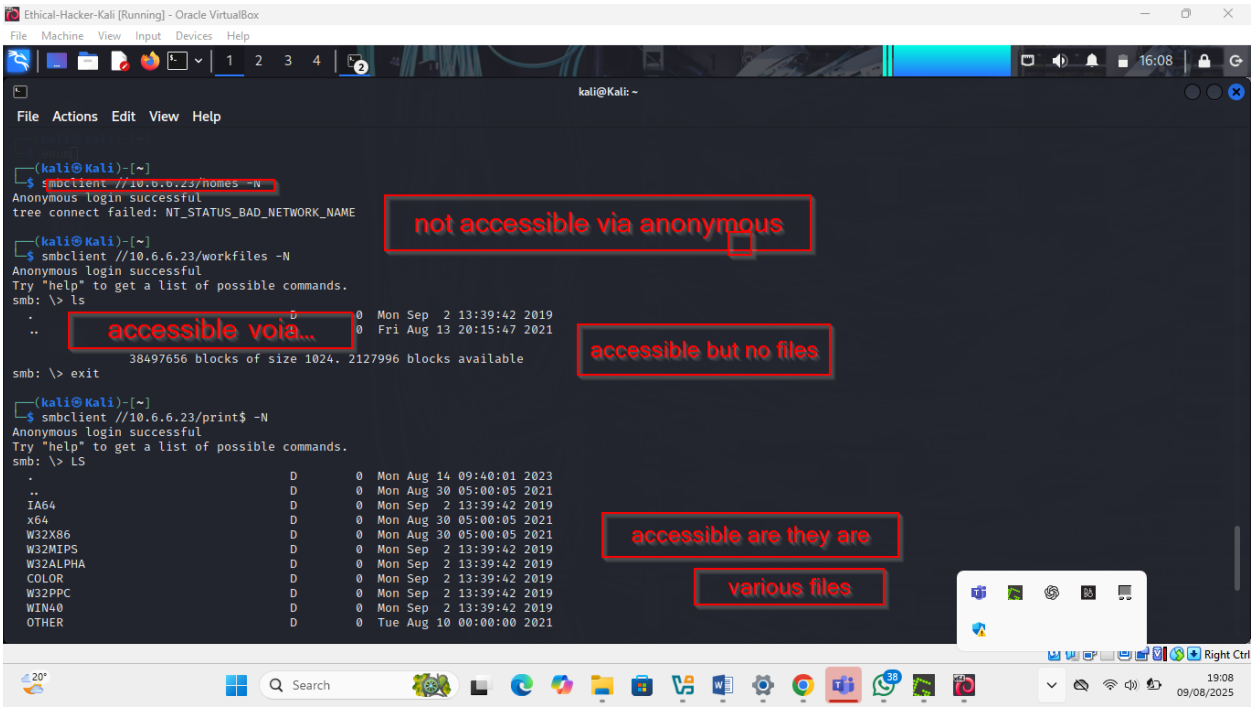
IA64	D	0	Mon Sep 2 13:39:42 2019
x64	D	0	Mon Aug 30 05:00:05 2021
W32X86	D	0	Mon Aug 30 05:00:05 2021
W32MIPS	D	0	Mon Sep 2 13:39:42 2019
W32ALPHA	D	0	Mon Sep 2 13:39:42 2019
COLOR	D	0	Mon Sep 2 13:39:42 2019
W32PPC	D	0	Mon Sep 2 13:39:42 2019
WIN40	D	0	Mon Sep 2 13:39:42 2019
OTHER	D	0	Tue Aug 10 00:00:00 2021

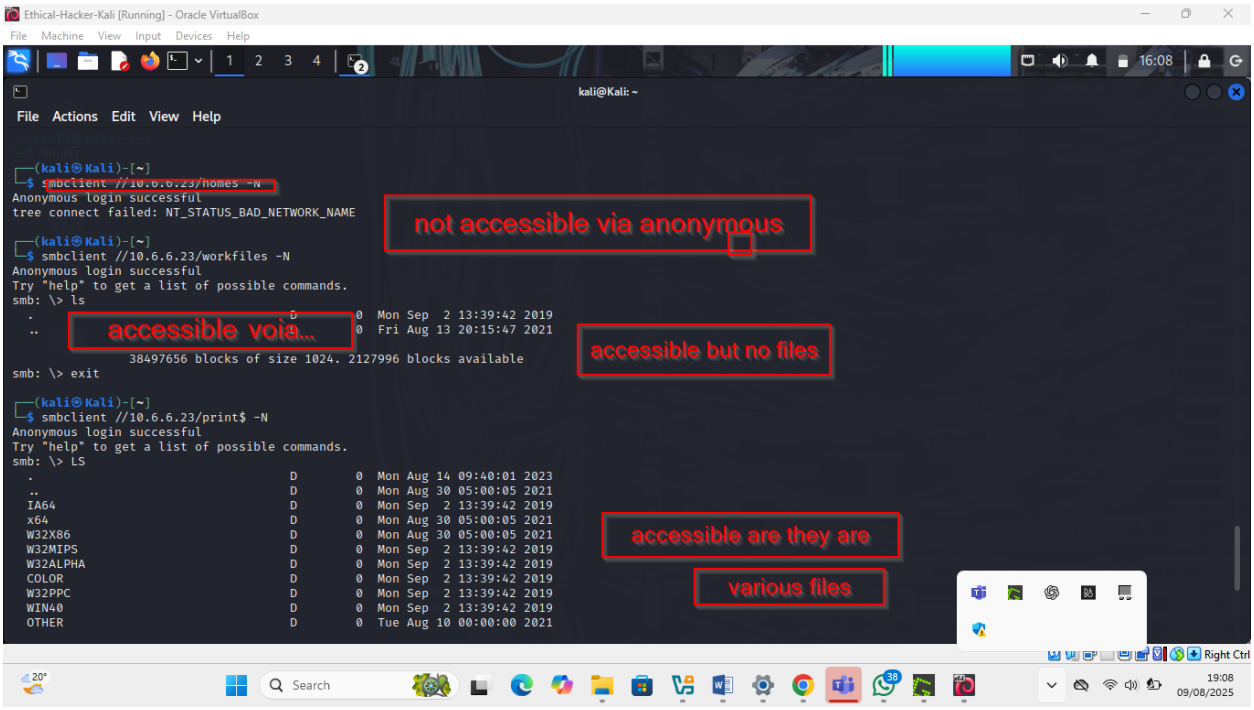
And I accessed directory OTHER since I saw it looks suspicious

And got a document therewhich I downloaded

5.After connecting to a share, how do you navigate the directory structure to find files and subfolders? Include at least three CLI commands and give screenshots of each used. (6 Marks)

Paste screenshot(s) demonstrating the answer here.





I navigated by use of the : ls for viewing the directories or files available

And cd OTHER/: to list files available

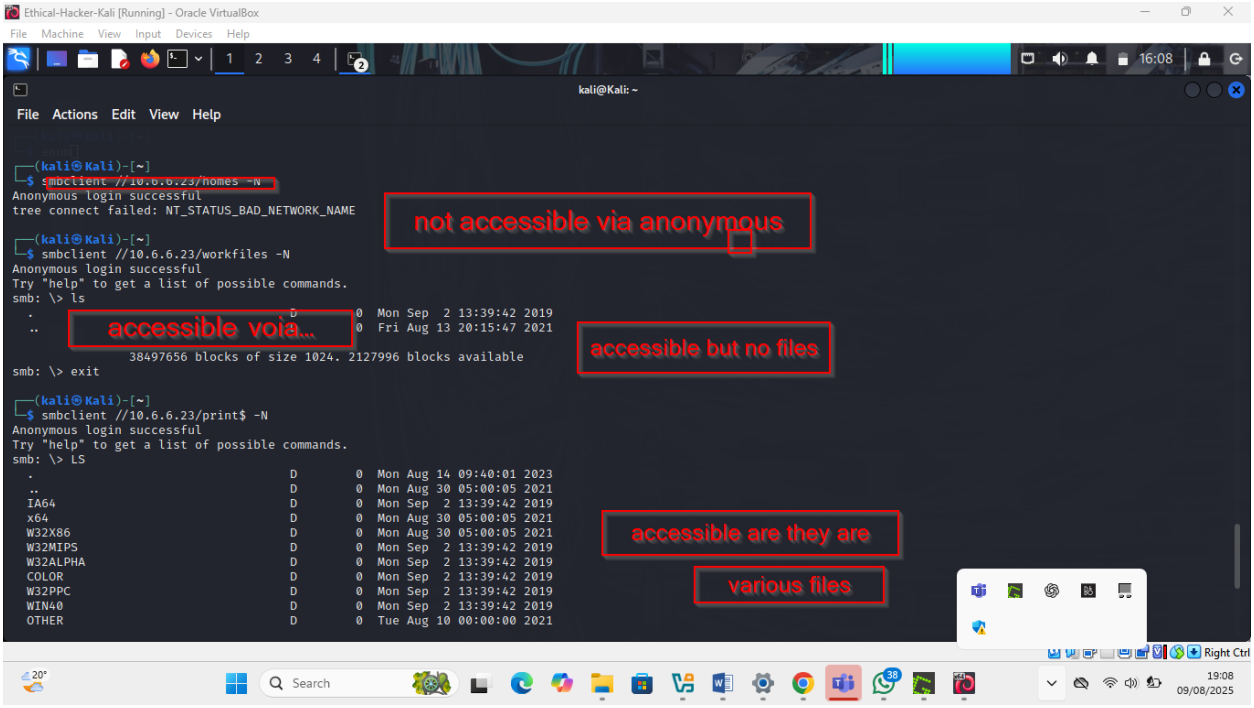
And also used the : get to download the file.txt

And exit to get out of the the smbclient

6. **On which share is an interesting File with a Flag located? Explain (2 Marks)**

Answer format: Share 5

Paste screenshot(s) demonstrating the answer here.

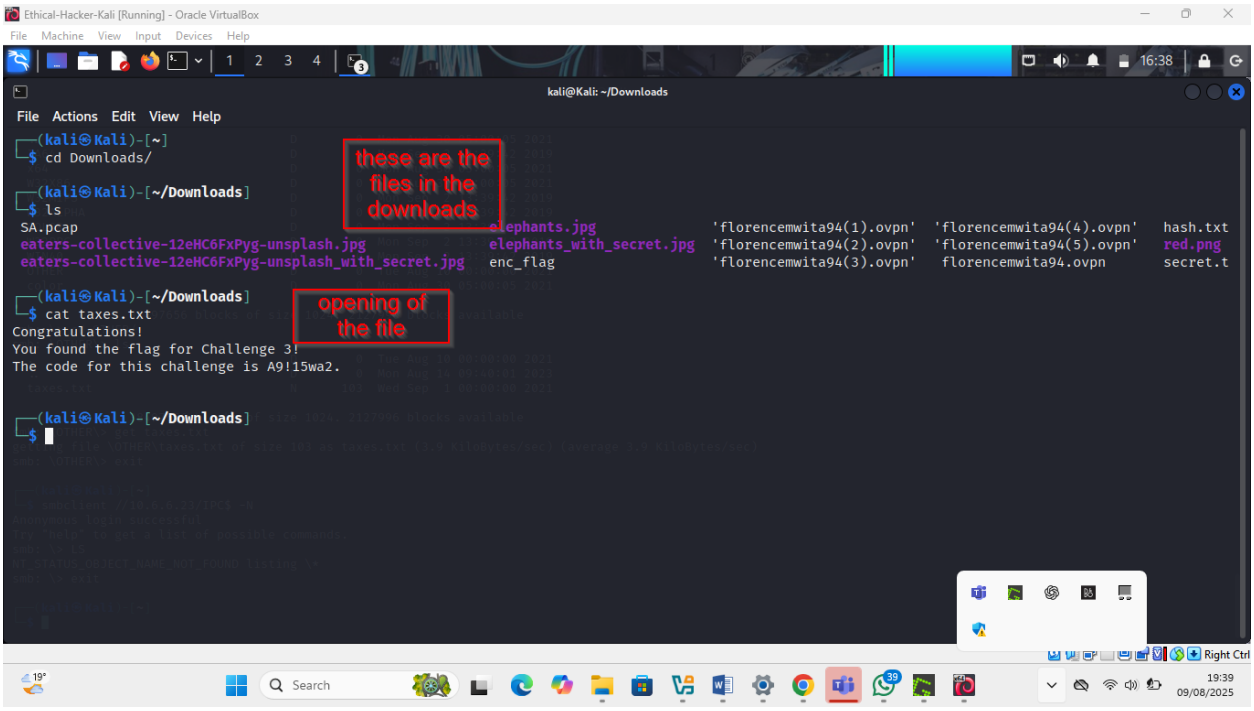


the print$ is the share with the file with flag

7.What is the exact file name containing the Flag? (2 Marks)

Answer format: somefile.txt

Paste screenshot(s) demonstrating the answer here.



On the taxes.txt is where the flag is located

congratulations! This is the words displayed after opening

You found the flag for Challenge 3!

The code for this challenge is A9!15wa2.

8Retrieve and inspect the file with the Flag. (5 marks)

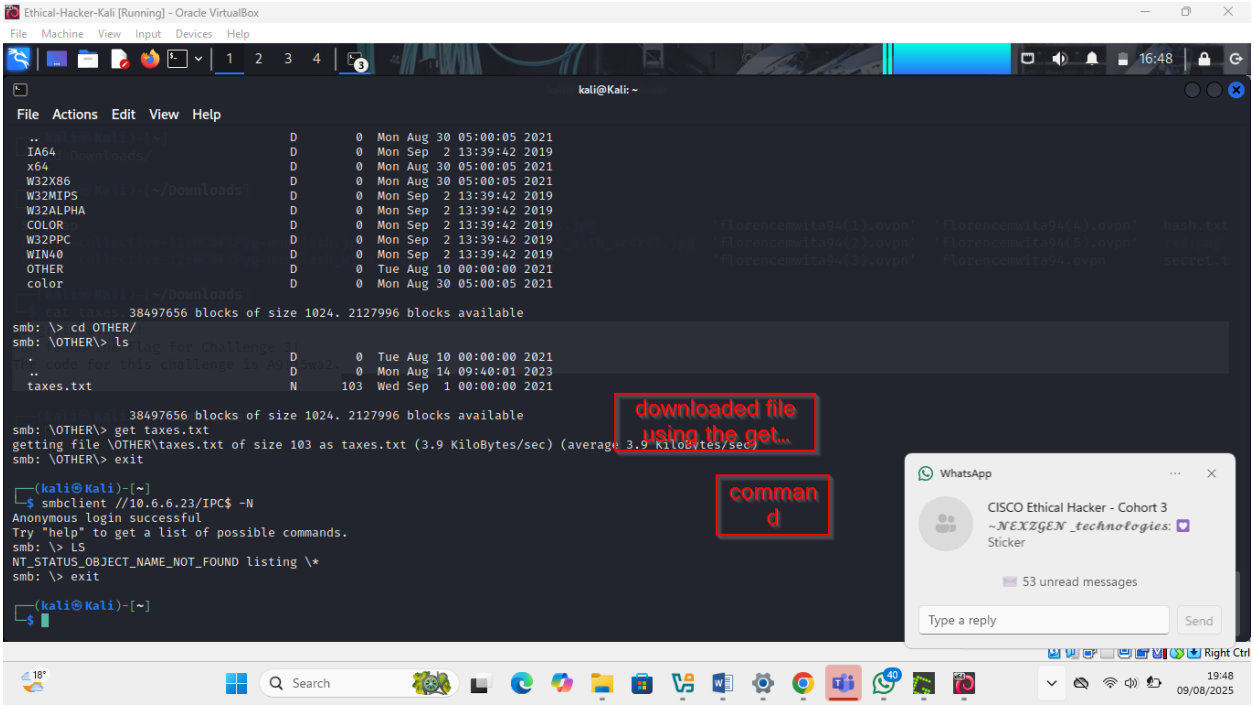
Q8a: How did you download the file locally from the share? Explain your process and provide screenshots. Provide the commands. (2 marks)

Paste screenshot(s) demonstrating the answer here.

Q8b: What method did you use to read or open the file contents? Show the screen contents (2 marks)

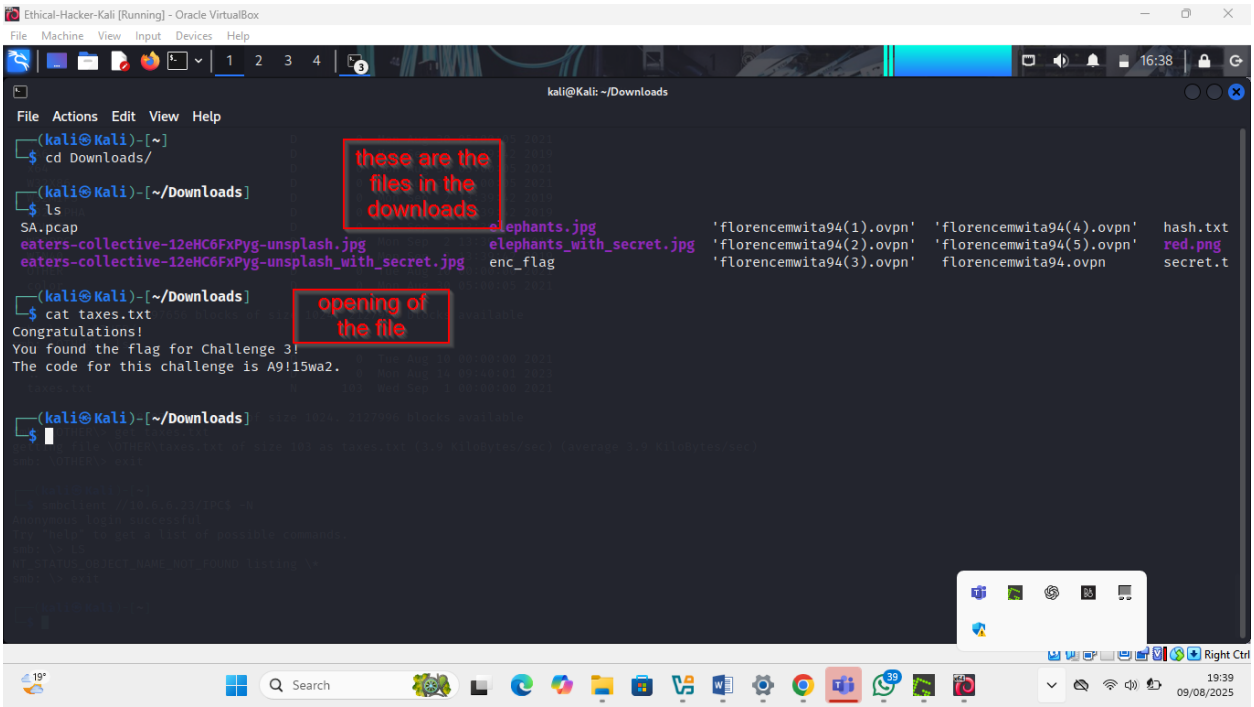
Paste screenshot(s) demonstrating the answer here.

8a.



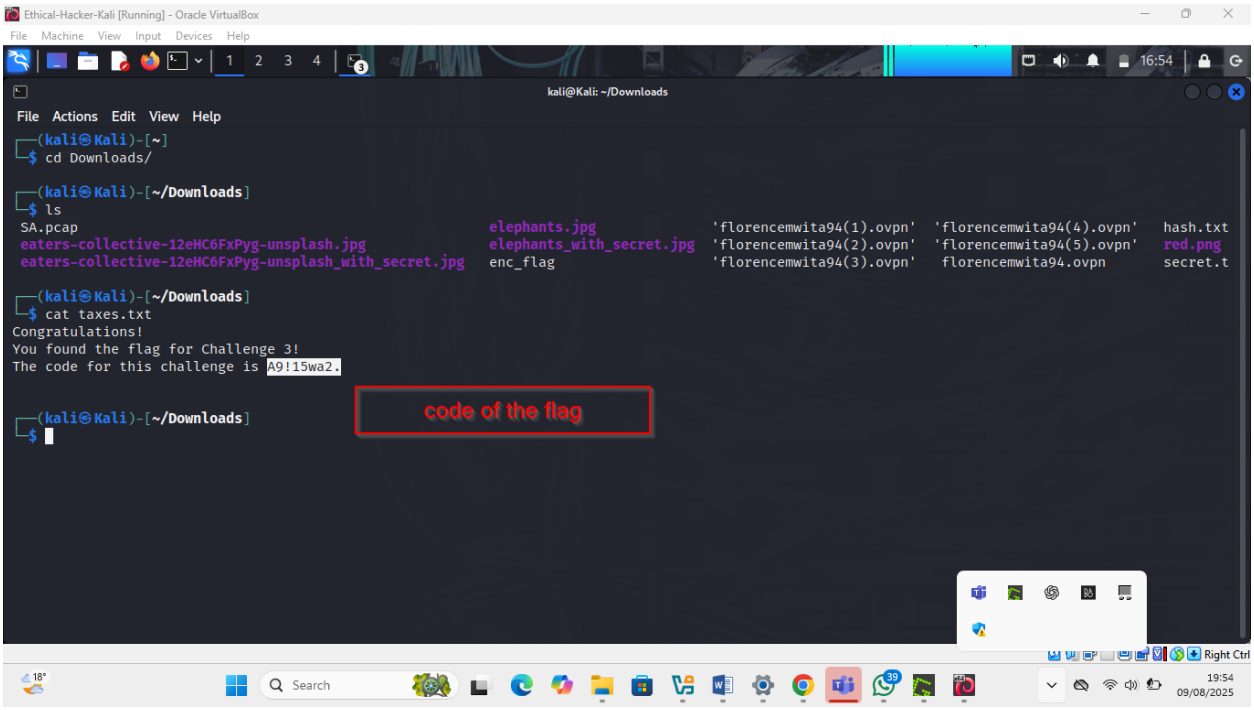
Used the ls command to list files available then used the cd OTHER/ to list the files in that directory then used get command to download the taxes.txt into the downloads

8b.



I used the cat command to open the file content after navigating into the downloads then listed the downloads to see if it was there then used cat to cat it out

9.What is the code for the Flag found in the file? (1 mark)



A9!15wa2. is the code

Part C: Analysis and Reporting (10 Marks)

Scenario-based question:

Suppose the SMB server was intentionally misconfigured to allow anonymous access for internal collaboration. Explain three security risks this setup introduces and suggest three mitigations.

Answer:

Risks (3 marks):

unauthorized data access: this can allow even attackers to get access and manipulate the database for there own good

malware propagation:this will happen when the hackers go in and insert a payload which will disrupt systems and leak information

potential disruption of service:this will happen when an attacker performs man in the middle attack and cause disruptions of services

REMEDIATION PHASE

Mitigations (3 marks):

1.Implement Strong Authentication:

Enforce a stronger use of passwords and usernames which are very hard to guess

2. Enable SMB Encryption and Signing

Enable SMB encryption and signing to protect data in transit and prevent man-in-the-middle attacks. This ensures that data is encrypted before being transmitted

3.Regularly Review and Update Configurations:

Periodically review the SMB server configuration to ensure it is still appropriate for the current environment. Regularly patch the server and its associated operating system to address any known vulnerabilities. Also, ensure that only necessary services are permitted to take place

Name two tools other than NMAP and SMBCLIENT that are commonly used for SMB enumeration, and distinguish each by its strengths. (4 Marks)

1.enum4linux:it is super fast you don't take a lot of time as compared to metasploit inoder to access the shares

2.metasploit:is more powerful but to involving due to its many options but it is still good

CONCLUSION

We conducted a scan but we majored on smb(sender message block) explaoitation this shows us how to scan ,enumerate,exploitand mitigate attacks in smb