cs-sa07-24019
John_Mbithi_Mutave

CYBER SHUJAA SECURITY ANALYST

COHORT 2 - 2024 MID EXAMINATION

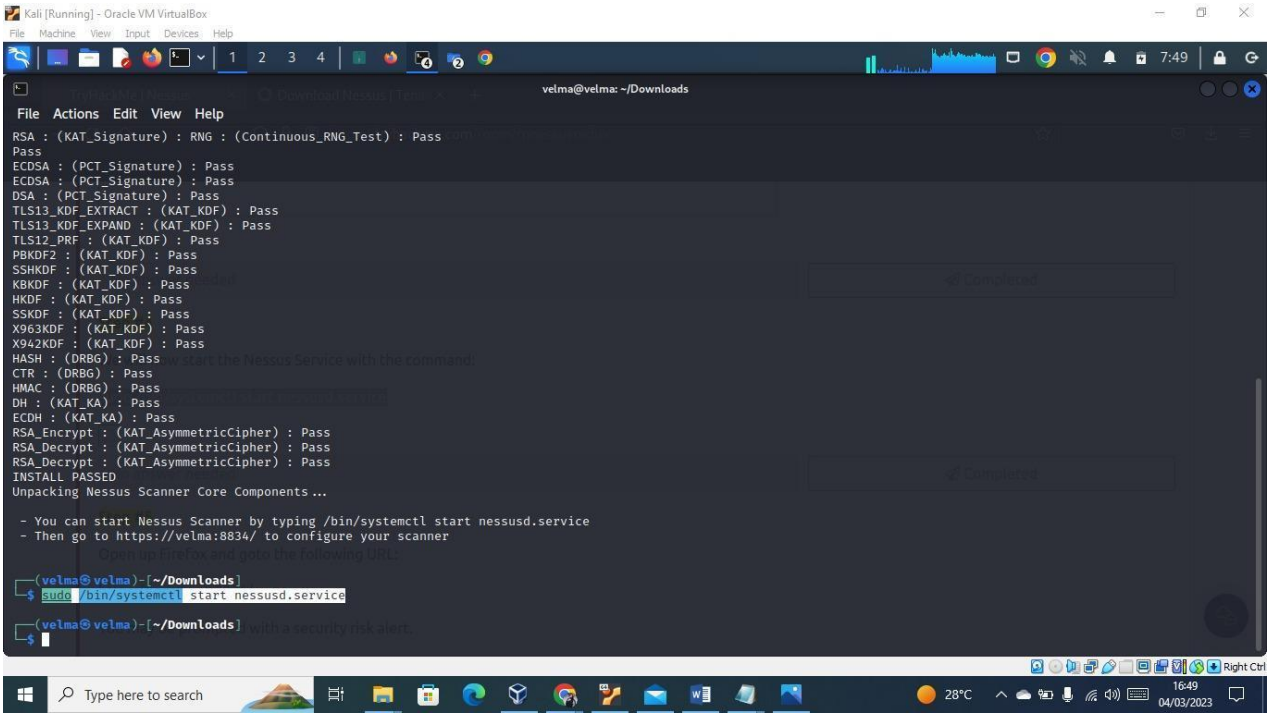
PRACTICAL QUESTIONS

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.**



cs-sa07-24019
John_Mbithi_Mutave

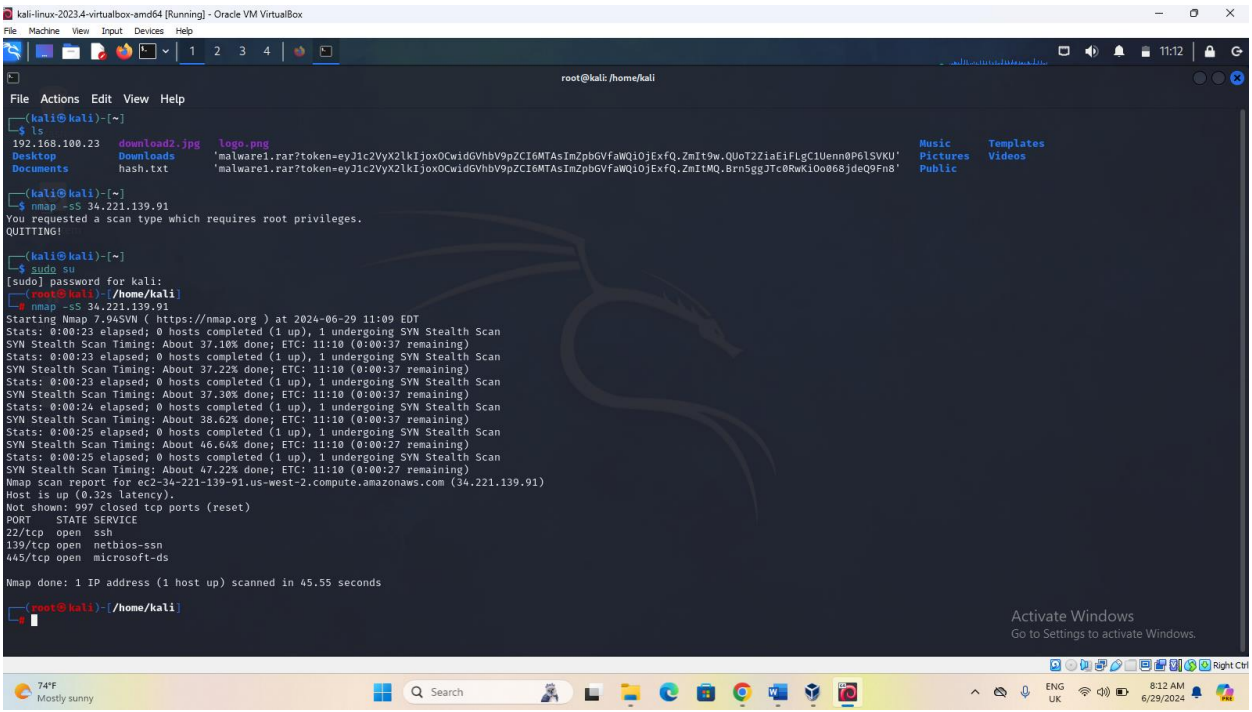
MID EXAM PRACTICAL (30 marks)

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)**

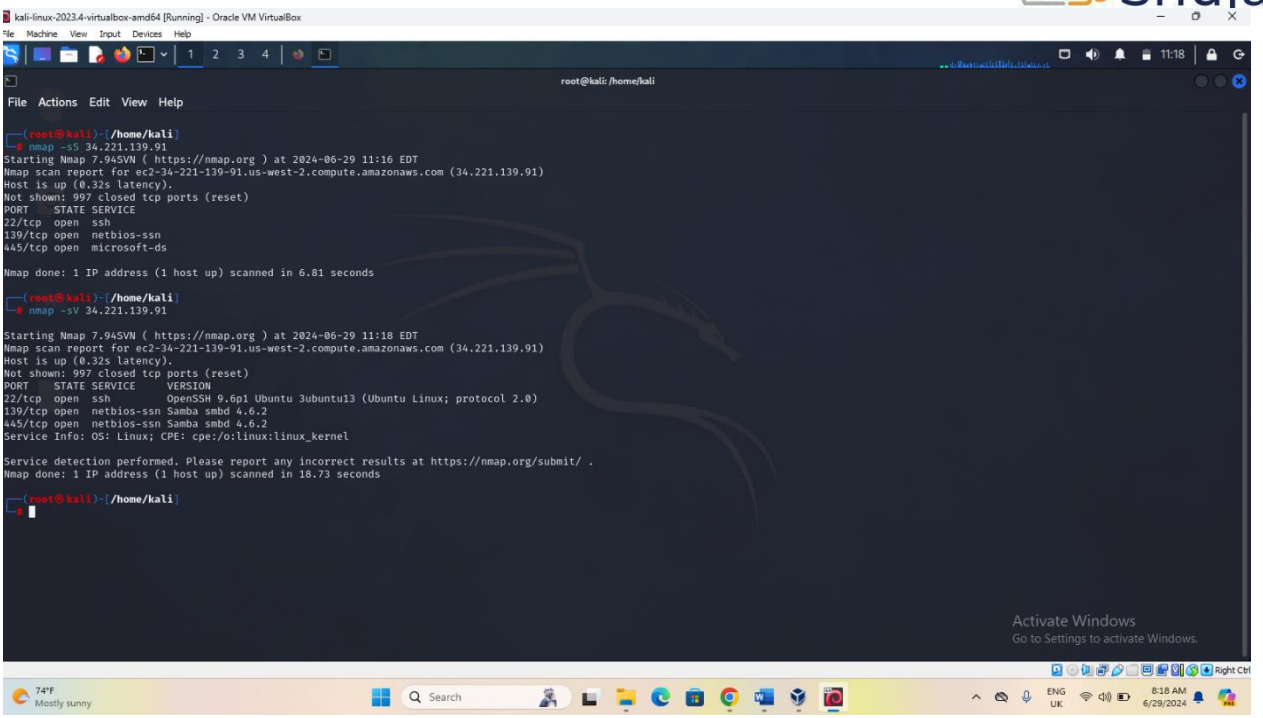
Run an Nmap scan on each server to identify open ports.



22/tcp open ssh
139/tcp open netbios-ssn
445/tcp open microsoft-ds

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

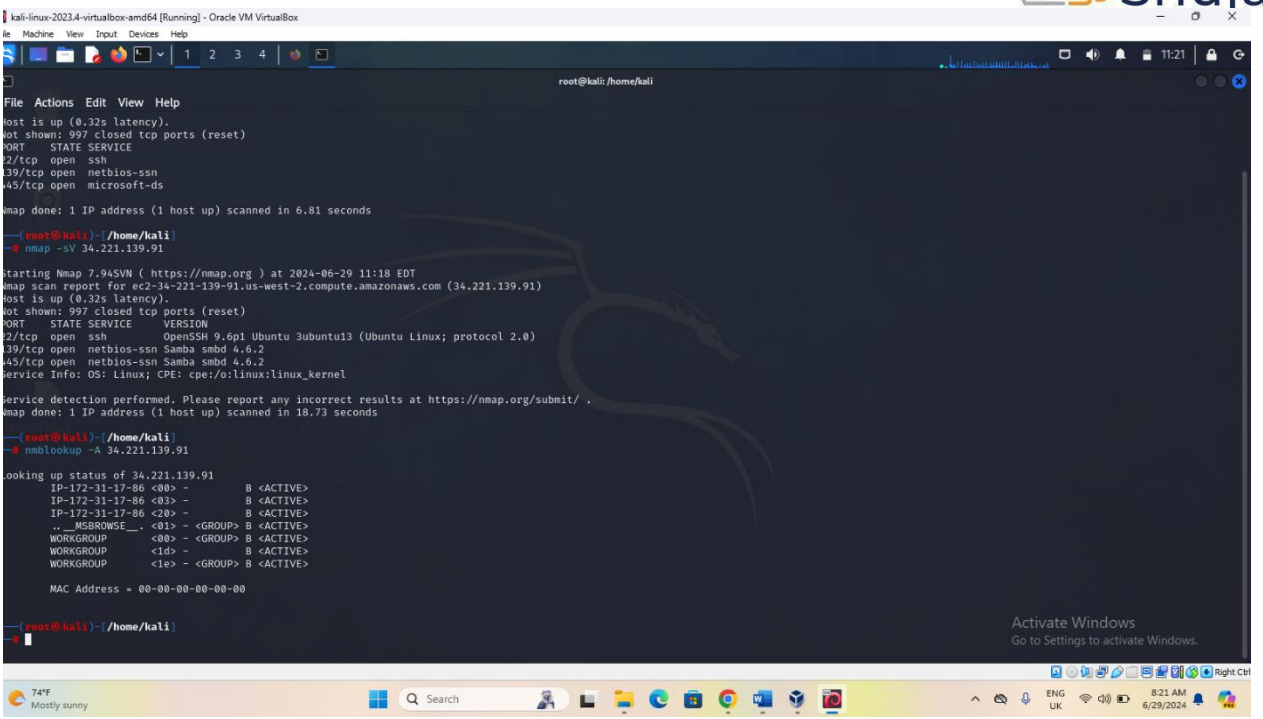
Check the Nmap scan results for services running on multiple ports and their versions using command -sV



22/tcp open ssh OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
139/tcp open netbios-ssn Samba smbd 4.6.2
445/tcp open netbios-ssn Samba smbd 4.6.2

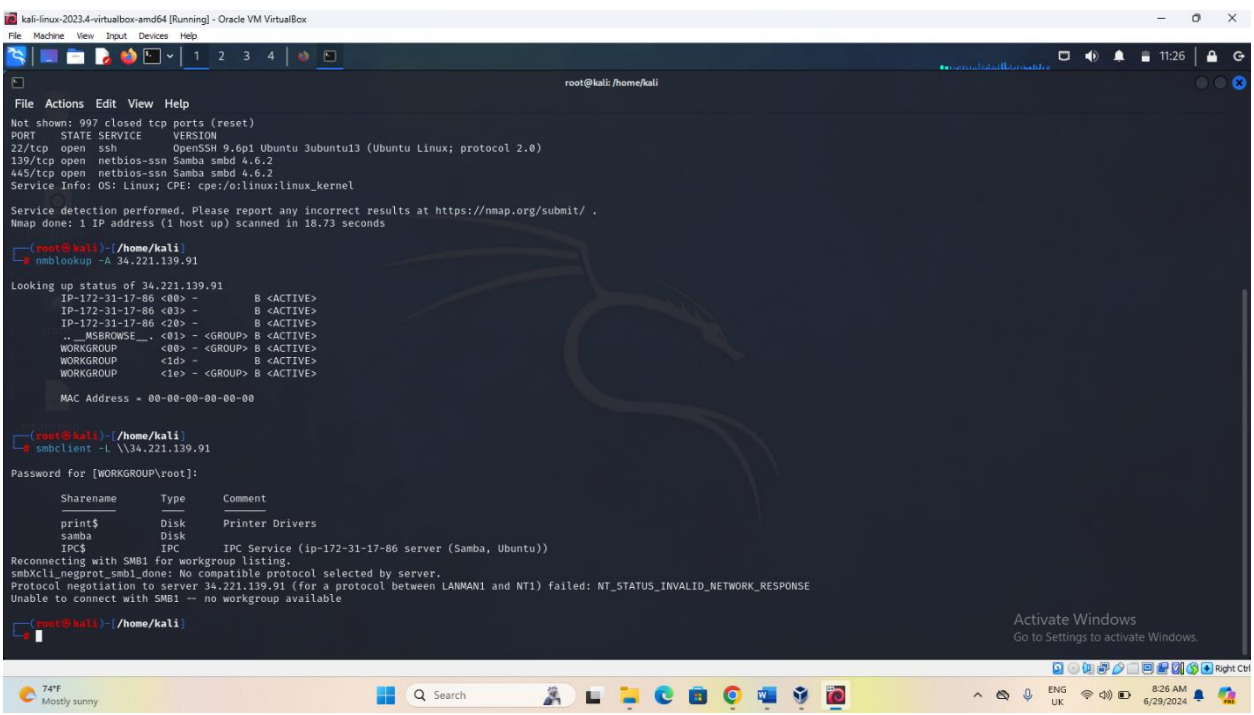
3. What is the netbios name of the server? (1 mk)

I used `nmblookup` to find the NetBIOS name.



4. Using smbclient tool identify the available shares (2 mks)

I have Listed the shares using smbclient

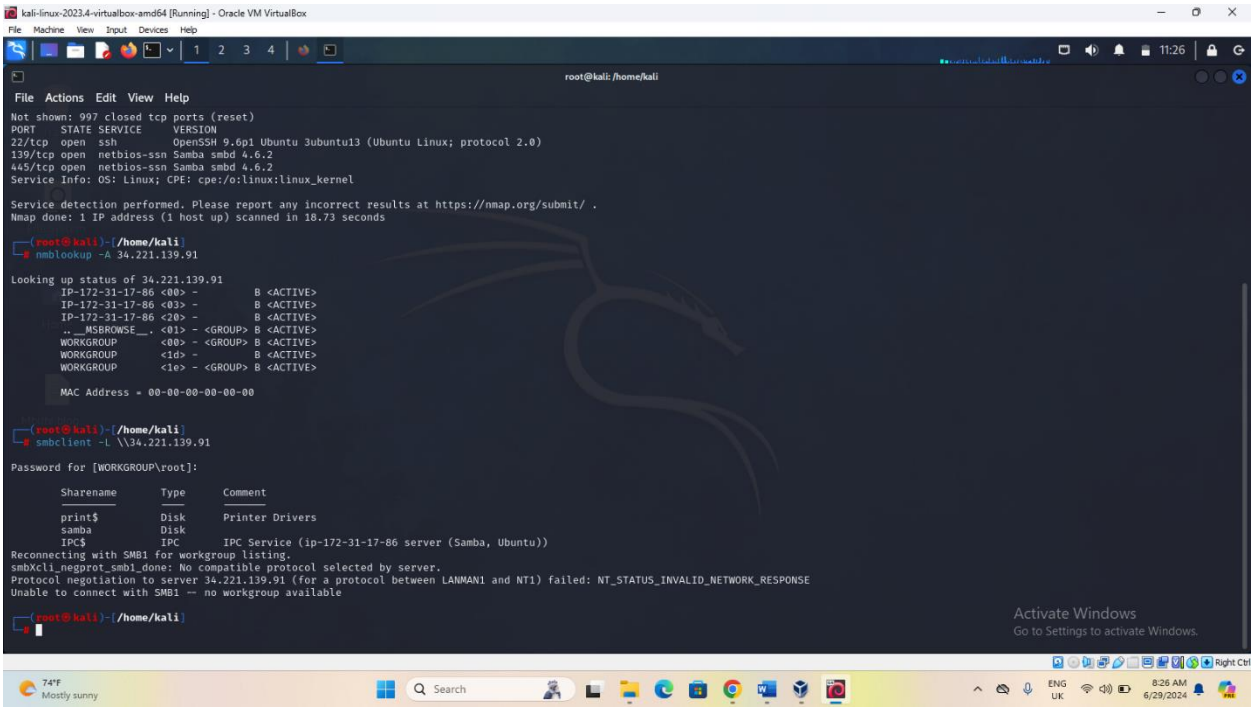


Sharename Type Comment

print$ Disk Printer Drivers
samba Disk
IPC$ IPC IPC Service (ip-172-31-28-33 server (Samba, Ubuntu))

5. **How many hidden shares are among the identified shares above. Name them. (2 mks)**

I Checked the shares list for hidden shares - those ending with a $

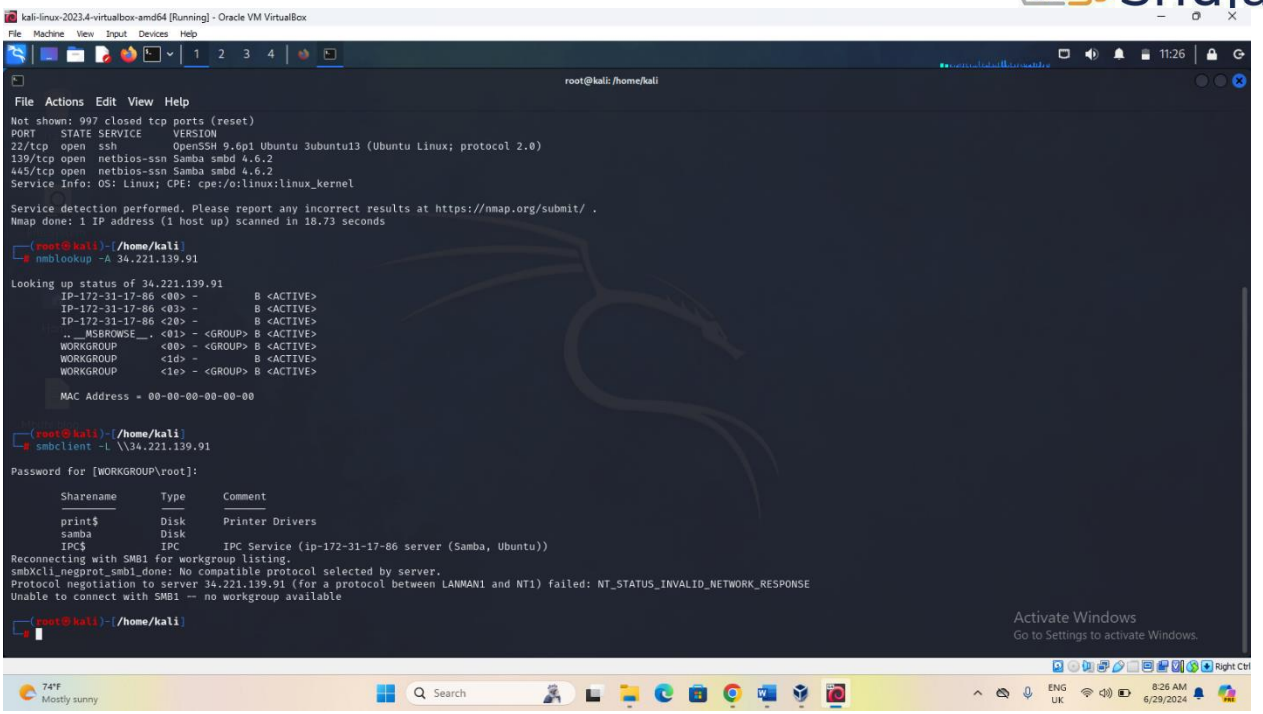


IPC$ IPC IPC Service (ip-172-31-28-33 server (Samba, Ubuntu))
print$ Disk Printer Drivers

6. **What is the name of the share that is accessible? (1 mk)**

I Checked the shares list for accessible shares (those not ending with a $).

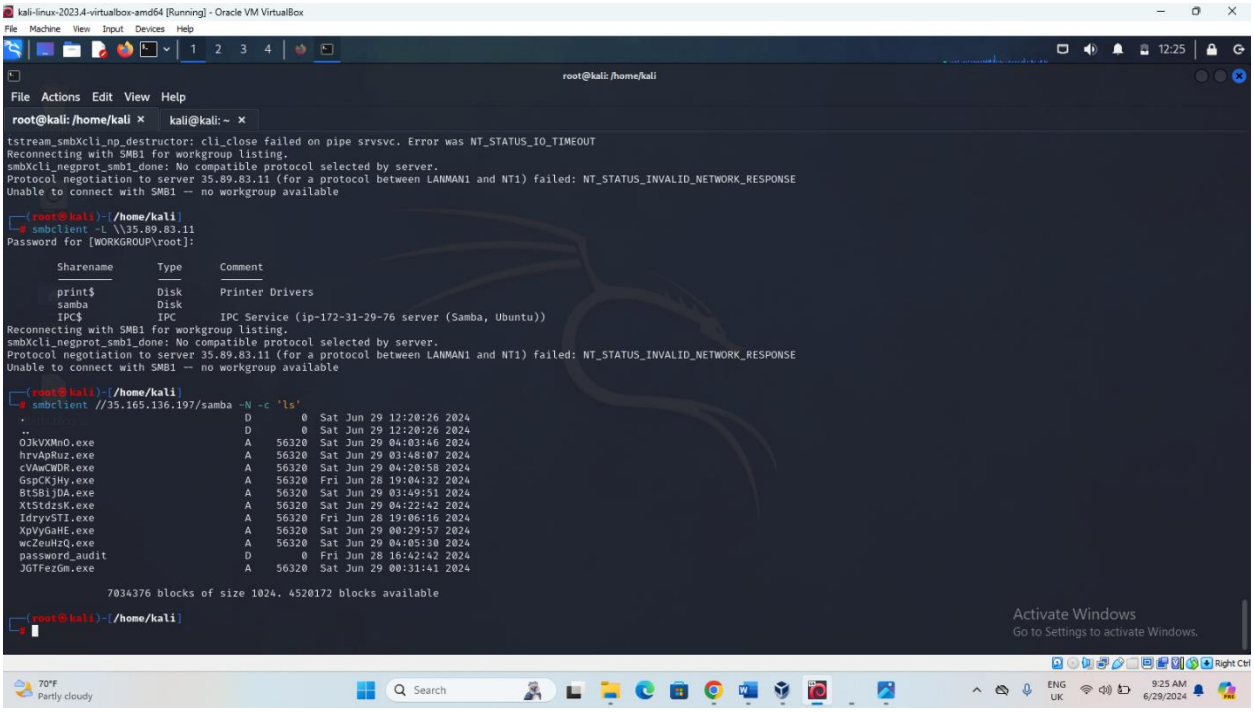
cs-sa07-24019
John_Mbithi_Mutave



samba Disk

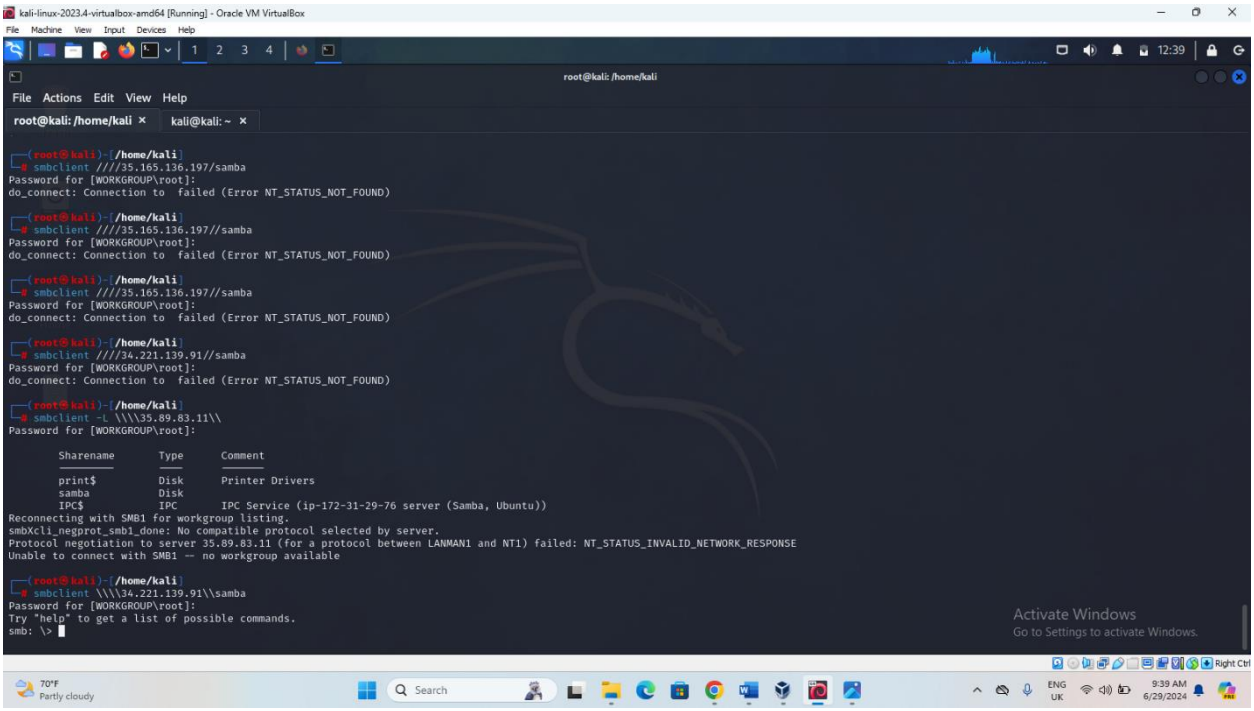
7. Access the share using null authentication, what is the folder's name discovered within the share? (2 marks)

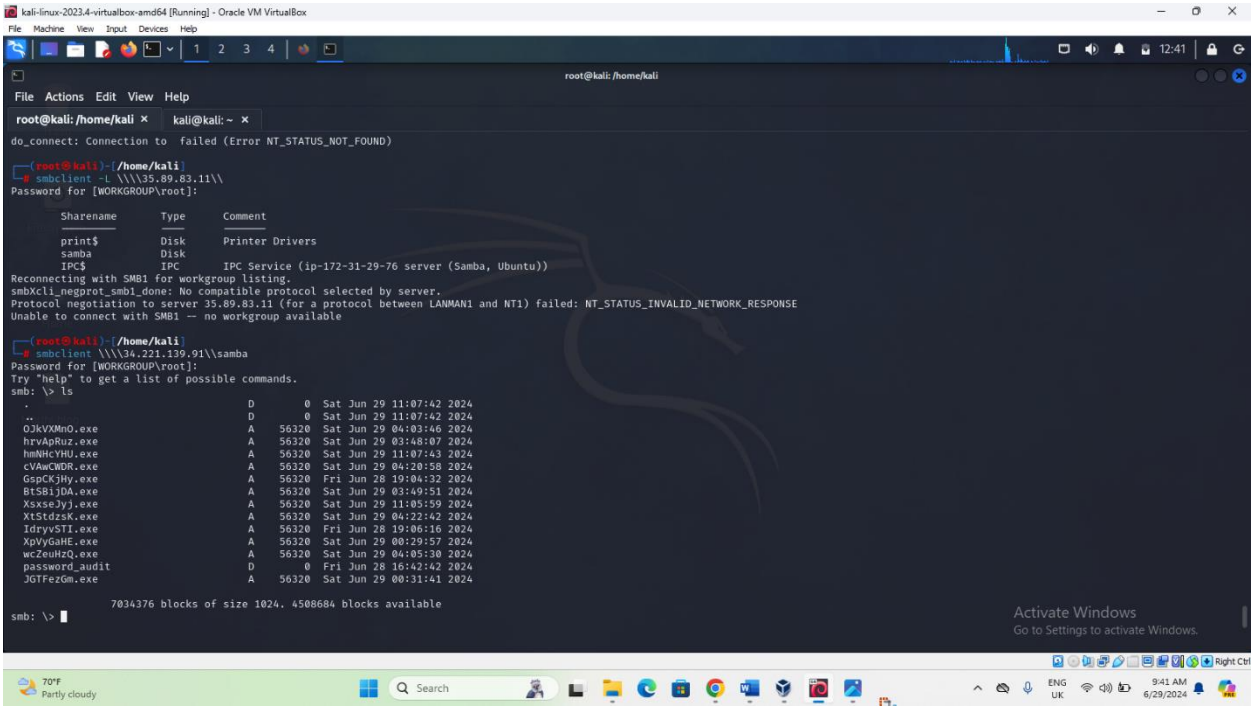
I have used command below smbclient //35.165.136.197/samba -N -c 'ls'



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

I have accessed samba



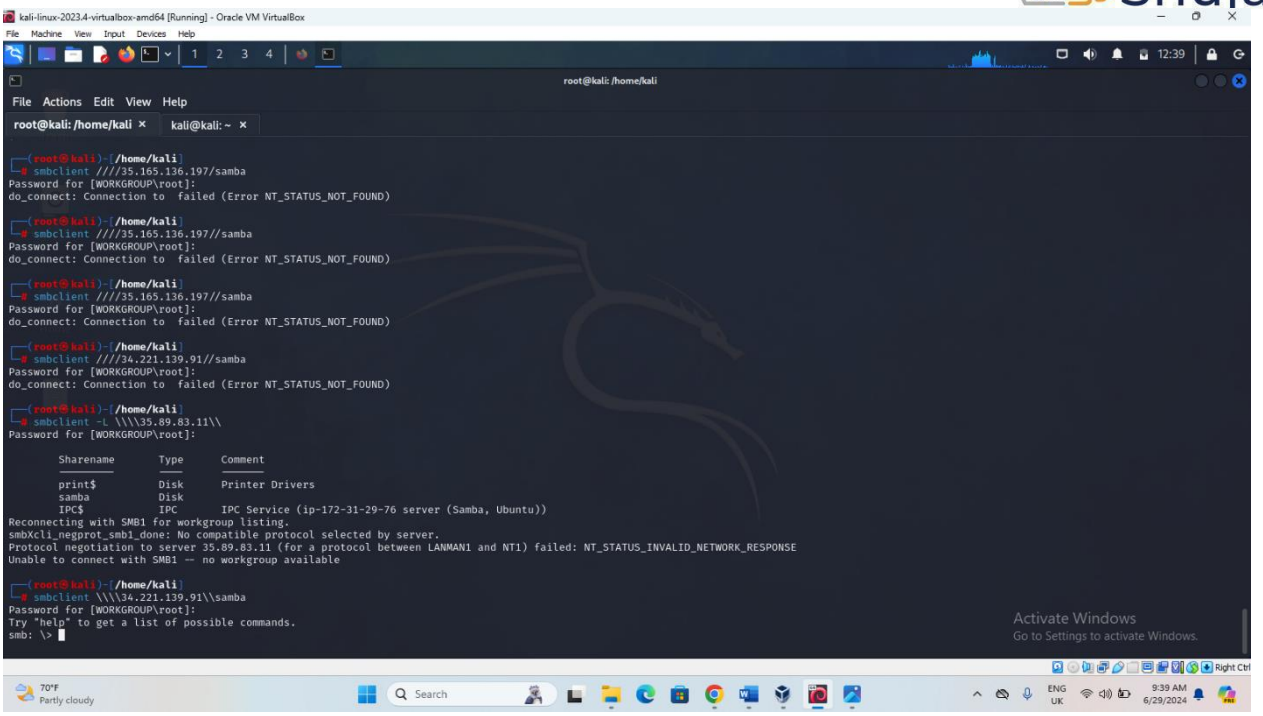


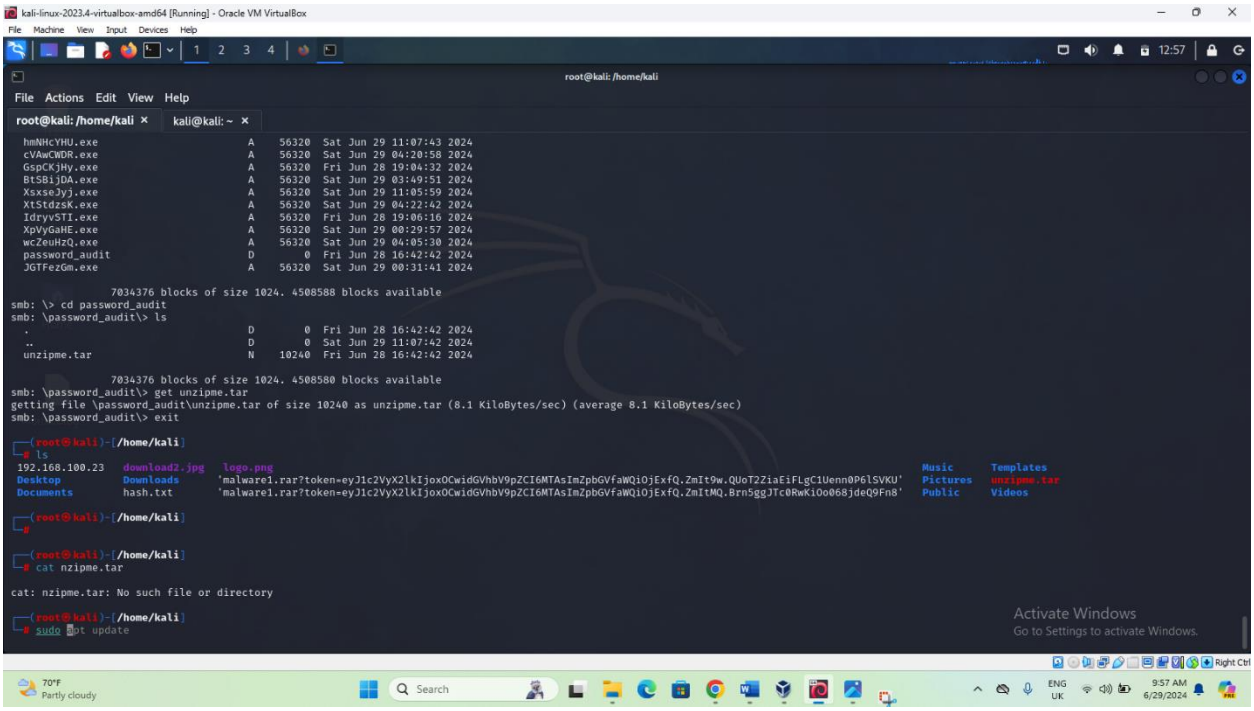
cs-sa07-24019
John_Mbithi_Mutave

```
┌──(root㉿kali)-[/home/kali]
└─# smbclient \\\\34.221.139.91\\IPC$
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_CONNECTION_REFUSED listing \*
smb: \> quit

┌──(root㉿kali)-[/home/kali]
└─# smbclient \\\\34.221.139.91\\samba
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jun 29 11:07:42 2024
  ..                                  D        0  Sat Jun 29 11:07:42 2024
  OJkVXMnO.exe                        A    56320  Sat Jun 29 04:03:46 2024
  hrvApRuz.exe                        A    56320  Sat Jun 29 03:48:07 2024
  hmNHcYHU.exe                        A    56320  Sat Jun 29 11:07:43 2024
  cVAwCWDR.exe                        A    56320  Sat Jun 29 04:20:58 2024
  GspCKjHy.exe                        A    56320  Fri Jun 28 19:04:32 2024
  BtSBijDA.exe                        A    56320  Sat Jun 29 03:49:51 2024
  XsxseJyj.exe                        A    56320  Sat Jun 29 11:05:59 2024
  XtStdzsK.exe                        A    56320  Sat Jun 29 04:22:42 2024
  IdryvSTI.exe                        A    56320  Fri Jun 28 19:06:16 2024
  XpVyGaHE.exe                        A    56320  Sat Jun 29 00:29:57 2024
  wcZeuHzQ.exe                        A    56320  Sat Jun 29 04:05:30 2024
  password_audit                      D        0  Fri Jun 28 16:42:42 2024
  JGTFezGm.exe                        A    56320  Sat Jun 29 00:31:41 2024

                7034376 blocks of size 1024. 4508588 blocks available
smb: \> cd password_audit
smb: \password_audit\> ls
  .                                   D        0  Fri Jun 28 16:42:42 2024
  ..                                  D        0  Sat Jun 29 11:07:42 2024
  unzipme.tar                         N    10240  Fri Jun 28 16:42:42 2024

                7034376 blocks of size 1024. 4508580 blocks available
smb: \password_audit\> get unzipme.tar
getting file \password_audit\unzipme.tar of size 10240 as unzipme.tar (8.1 KiloBytes/sec) (average 8.1 KiloBytes/sec)
smb: \password_audit\>
```

```
do_connect: Connection to  failed (Error NT_STATUS_NOT_FOUND)

┌──(root㉿kali)-[/home/kali]
└─# smbclient -L \\\\35.89.83.11\\
Password for [WORKGROUP\root]:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        samba           Disk
        IPC$            IPC       IPC Service (ip-172-31-29-76 server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.
smbXcli_negprot_smb1_done: No compatible protocol selected by server.
Protocol negotiation to server 35.89.83.11 (for a protocol between LANMAN1 and NT1) failed: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available

┌──(root㉿kali)-[/home/kali]
└─# smbclient \\\\34.221.139.91\\samba
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jun 29 11:07:42 2024
  ..                                  D        0  Sat Jun 29 11:07:42 2024
  OJkVXMnO.exe                        A    56320  Sat Jun 29 04:03:46 2024
  hrvApRuz.exe                        A    56320  Sat Jun 29 03:48:07 2024
  hmNHcYHU.exe                        A    56320  Sat Jun 29 11:07:43 2024
  cVAwCWDR.exe                        A    56320  Sat Jun 29 04:20:58 2024
  GspCKjHy.exe                        A    56320  Fri Jun 28 19:04:32 2024
  BtSBijDA.exe                        A    56320  Sat Jun 29 03:49:51 2024
  XsxseJyj.exe                        A    56320  Sat Jun 29 11:05:59 2024
  XtStdzsK.exe                        A    56320  Sat Jun 29 04:22:42 2024
  IdryvSTI.exe                        A    56320  Fri Jun 28 19:06:16 2024
  XpVyGaHE.exe                        A    56320  Sat Jun 29 00:29:57 2024
  wcZeuHzQ.exe                        A    56320  Sat Jun 29 04:05:30 2024
  password_audit                      D        0  Fri Jun 28 16:42:42 2024
  JGTFezGm.exe                        A    56320  Sat Jun 29 00:31:41 2024

                7034376 blocks of size 1024. 4508684 blocks available
smb: \>
```

cs-sa07-24019
John_Mbithi_Mutave





9. What is the exposed username and password? (1 mk)

root

Paste screenshot(s) demonstrating the answer here

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

Paste screenshot(s) demonstrating the answer here

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

Paste screenshot(s) demonstrating the answer here

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)

Paste screenshot(s) demonstrating the answer here

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)

Paste screenshot(s) demonstrating the answer here

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

Paste screenshot(s) demonstrating the answer here

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

Paste screenshot(s) demonstrating the answer here