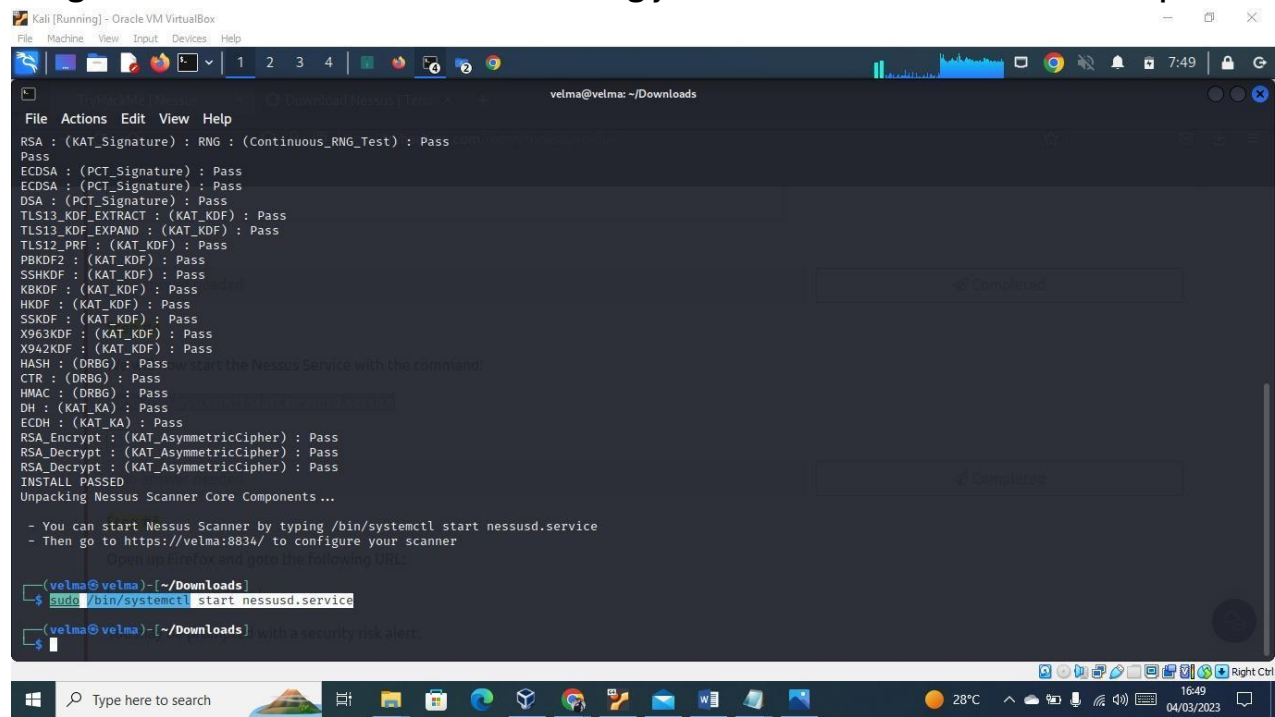


CYBER SHUJAA SECURITY ANALYST  
COHORT 2 - 2024 MID EXAMINATION

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.



```
Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

velma@velma: ~/Downloads
File Actions Edit View Help
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components ...

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://velma:8834/ to configure your scanner

velma@velma:~/Downloads$ sudo /bin/systemctl start nessusd.service
velma@velma:~/Downloads$
```

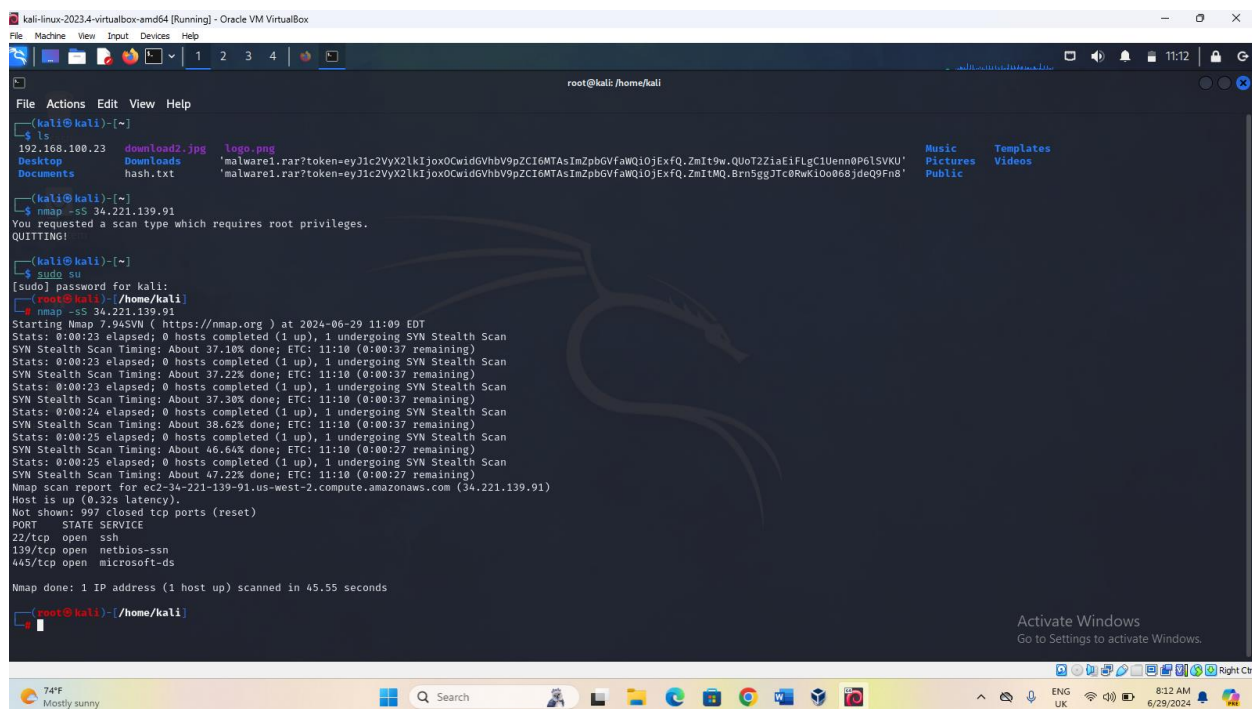
# MID EXAM PRACTICAL (30 marks)

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.



```
kali@kali:~$ nmap -sS 34.221.139.91
Nmap scan report for ec2-34-221-139-91.us-west-2.compute.amazonaws.com (34.221.139.91)
Host is up (0.32s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 45.55 seconds
```

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

cs-sa07-24019

John\_Mbithi\_Mutave



```
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali

(root@kali)~/home/kali
# nmap -sS 34.221.139.91
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-29 11:16 EOT
Nmap scan report for ec2-34-221-139-91.us-west-2.compute.amazonaws.com (34.221.139.91)
Host is up (0.32s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 6.81 seconds

(root@kali)~/home/kali
# nmap -sV 34.221.139.91
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-29 11:18 EOT
Nmap scan report for ec2-34-221-139-91.us-west-2.compute.amazonaws.com (34.221.139.91)
Host is up (0.32s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.73 seconds

(root@kali)~/home/kali
```

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.

cs-sa07-24019

John\_Mbithi\_Mutave



```
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali

File Actions Edit View Help
Host is up (0.32s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 6.81 seconds

root@kali: /home/kali
# nmap -sV 34.221.139.91

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-29 11:18 EDT
Nmap scan report for ec2-34-221-139-91.us-west-2.compute.amazonaws.com (34.221.139.91)
Host is up (0.32s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 18.73 seconds

root@kali: /home/kali
# nmblookup -A 34.221.139.91

Looking up status of 34.221.139.91
IP-172-31-17-86 <00> - B <ACTIVE>
IP-172-31-17-86 <03> - B <ACTIVE>
IP-172-31-17-86 <20> - B <ACTIVE>
.._MSBROWSE_.. <01> - <GROUP> B <ACTIVE>
WORKGROUP <00> - <GROUP> B <ACTIVE>
WORKGROUP <1d> - B <ACTIVE>
WORKGROUP <1e> - <GROUP> B <ACTIVE>

MAC Address = 00-00-00-00-00-00

root@kali: /home/kali
```

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

I have Listed the shares using smbclient

```
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali

File Actions Edit View Help
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 18.73 seconds

root@kali: /home/kali
# nmblookup -A 34.221.139.91

Looking up status of 34.221.139.91
IP-172-31-17-86 <00> - B <ACTIVE>
IP-172-31-17-86 <03> - B <ACTIVE>
IP-172-31-17-86 <20> - B <ACTIVE>
.._MSBROWSE_.. <01> - <GROUP> B <ACTIVE>
WORKGROUP <00> - <GROUP> B <ACTIVE>
WORKGROUP <1d> - B <ACTIVE>
WORKGROUP <1e> - <GROUP> B <ACTIVE>

MAC Address = 00-00-00-00-00-00

root@kali: /home/kali
# smbclient -L \\34.221.139.91

Password for [WORKGROUP\root]:

Sharename      Type            Comment
-----
print$         Disk            Printer Drivers
samba          Disk
IPC$           IPC             IPC Service (ip-172-31-17-86 server (Samba, Ubuntu))

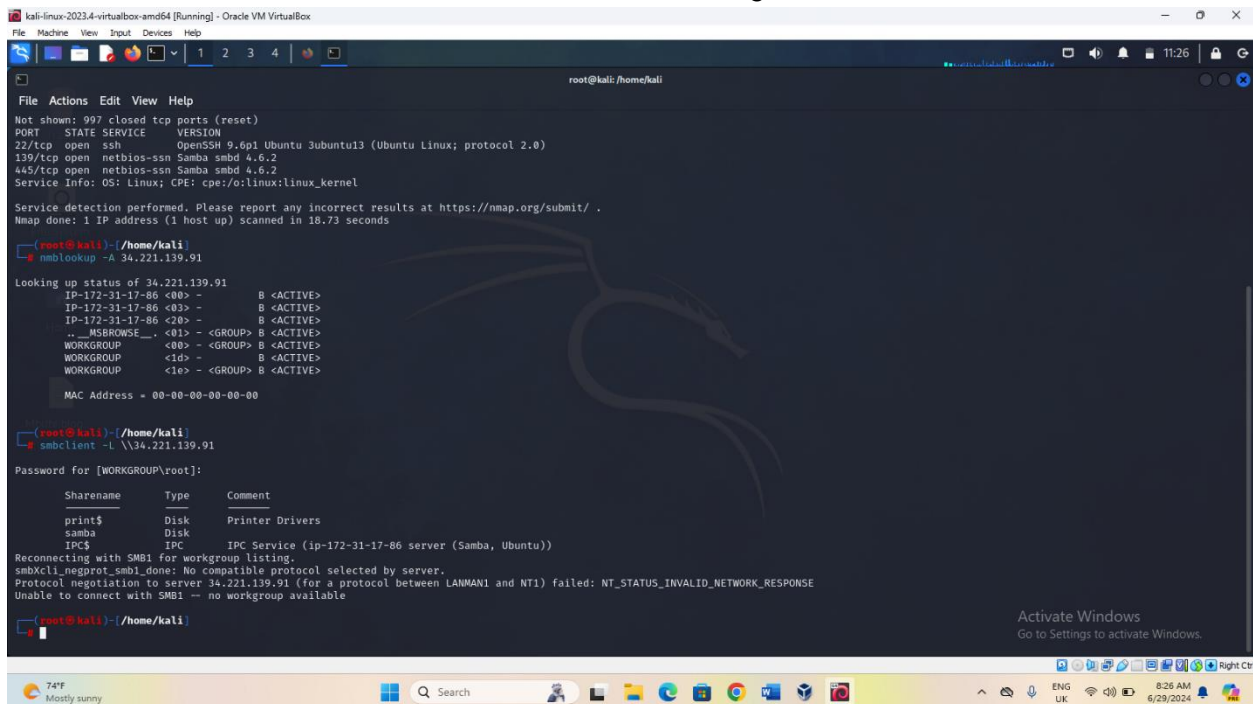
Reconnecting with SMB1 for workgroup listing.
smbcli_negprot_smb1_done: No compatible protocol selected by server.
Protocol negotiation to server 34.221.139.91 (for a protocol between LANMAN1 and NT1) failed: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available

root@kali: /home/kali
```

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 \$



```
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@kali: /home/kali

File Actions Edit View Help
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.73 seconds

root@kali) ~/home/kali
# nmblookup -A 34.221.139.91

Looking up status of 34.221.139.91
IP-172-31-17-86 <00> - B <ACTIVE>
IP-172-31-17-86 <03> - B <ACTIVE>
IP-172-31-17-86 <08> - B <ACTIVE>
IP-172-31-17-86 <09> - B <ACTIVE>
IPC$ <01> - <GROUP> B <ACTIVE>
WORKGROUP <00> - <GROUP> B <ACTIVE>
WORKGROUP <1d> - B <ACTIVE>
WORKGROUP <1e> - <GROUP> B <ACTIVE>

MAC Address = 00-00-00-00-00-00

root@kali) ~/home/kali
# smbclient -L \\34.221.139.91

Password for [WORKGROUP\root]:

Sharename      Type      Comment
-----
print$         Disk     Printer Drivers
samba          Disk
IPC$           IPC      IPC Service (ip-172-31-17-86 server (Samba, Ubuntu))

Reconnecting with SMB1 for workgroup listing.
smbcli_negprot_smb1_done: No compatible protocol selected by server.
Protocol negotiation to server 34.221.139.91 (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
```

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



```
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali

File Actions Edit View Help
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 18.73 seconds

root@kali) ~ # nmblookup -A 34.221.139.91

Looking up status of 34.221.139.91
IP-172-31-17-86 <00> - B <ACTIVE>
IP-172-31-17-86 <03> - B <ACTIVE>
IP-172-31-17-86 <20> - B <ACTIVE>
- _MSBROWSE_ - <01> - <GROUP> B <ACTIVE>
WORKGROUP <00> - <GROUP> B <ACTIVE>
WORKGROUP <1d> - B <ACTIVE>
WORKGROUP <1e> - <GROUP> B <ACTIVE>
MAC Address = 00-00-00-00-00-00

root@kali) ~ # smbclient -L \\34.221.139.91

Password for [WORKGROUP\root]:

Sharename      Type      Comment
-----
print$         Disk      Printer Drivers
samba          Disk
IPC$           IPC       IPC Service (ip-172-31-17-86 server (Samba, Ubuntu))

Reconnecting with SMB1 for workgroup listing.
smbcli_negot_smb1_done: No compatible protocol selected by server.
Protocol negotiation to server 34.221.139.91 (for a protocol between LANMAN1 and NT1) failed: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available

root@kali) ~ #

Activate Windows
Go to Settings to activate Windows.
```

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'`

```
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali

File Actions Edit View Help
root@kali: /home/kali x kali@kali: ~ x
tstream.smbcli_np_destructor: cli_close failed on pipe srvsvc. Error was NT_STATUS_IO_TIMEOUT
Reconnecting with SMB1 for workgroup listing.
smbcli_negot_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) ~ # 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.
smbcli_negot_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) ~ # smbclient //35.165.136.197/samba -N -c 'ls'

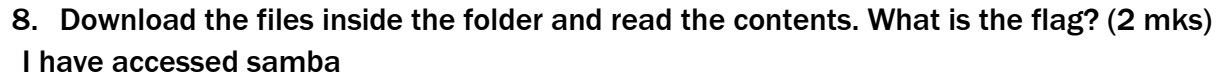
.
D 0 Sat Jun 29 12:20:26 2024
..
D 0 Sat Jun 29 12:20:26 2024
OJkVXm0.exe
A 56320 Sat Jun 29 04:03:46 2024
hryApRuz.exe
A 56320 Sat Jun 29 03:48:07 2024
cVAmCW0r.exe
A 56320 Sat Jun 29 04:20:58 2024
GspCKjHy.exe
A 56320 Fri Jun 28 19:04:32 2024
BtS81jDA.exe
A 56320 Sat Jun 29 03:49:51 2024
XtStdzsk.exe
A 56320 Sat Jun 29 04:22:42 2024
IdryySTL.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. 4520172 blocks available

root@kali) ~ #

Activate Windows
Go to Settings to activate Windows.
```

John\_Mbithi\_Mutave



```
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali x kali@kali: ~ x

(root@kali)~/ /home/kali
# smbclient ///35.165.136.197/samba
Password for [WORKGROUP\root]:
do_connect: Connection to failed (Error NT_STATUS_NOT_FOUND)

(root@kali)~/ /home/kali
# smbclient ///35.165.136.197/samba
Password for [WORKGROUP\root]:
do_connect: Connection to failed (Error NT_STATUS_NOT_FOUND)

(root@kali)~/ /home/kali
# smbclient ///35.165.136.197/samba
Password for [WORKGROUP\root]:
do_connect: Connection to failed (Error NT_STATUS_NOT_FOUND)

(root@kali)~/ /home/kali
# smbclient ///34.221.139.91/samba
Password for [WORKGROUP\root]:
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_negot_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: \>

Activate Windows
Go to Settings to activate Windows.

70°F
Partly cloudy
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali x kali@kali: ~ x

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_negot_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
OJkYmno.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
cVAwCWDOR.exe   A      56320  Sat Jun 29 04:20:58 2024
GspCKJhy.exe    A      56320  Fri Jun 28 19:04:32 2024
RtSIbIda.exe    A      56320  Sat Jun 29 03:49:51 2024
XsxSeZjy.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
XpvyGdHE.exe    A      56320  Sat Jun 29 00:29:57 2024
wc2euitQ.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: \>
```

```
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@kali: /home/kali

File Actions Edit View Help
root@kali: /home/kali x kali@kali: ~ x

root@kali: /home/kali
# smbclient //14.221.139.91\\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 //14.221.139.91\\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
03kVXm0.exe      A 56320 Sat Jun 29 04:03:46 2024
hfvApRuz.exe     A 56320 Sat Jun 29 03:48:07 2024
hmNHeYHU.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
BTSB1jDA.exe     A 56320 Sat Jun 29 03:49:51 2024
Xsxe3jy.exe      A 56320 Sat Jun 29 11:05:59 2024
XtStzsk.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\>

Activate Windows
Go to Settings to activate Windows.

70°F
Partly cloudy
Search
ENG
UK
9:56 AM
6/29/2024

kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@kali: /home/kali

File Actions Edit View Help
root@kali: /home/kali x kali@kali: ~ x

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.
smbcli_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

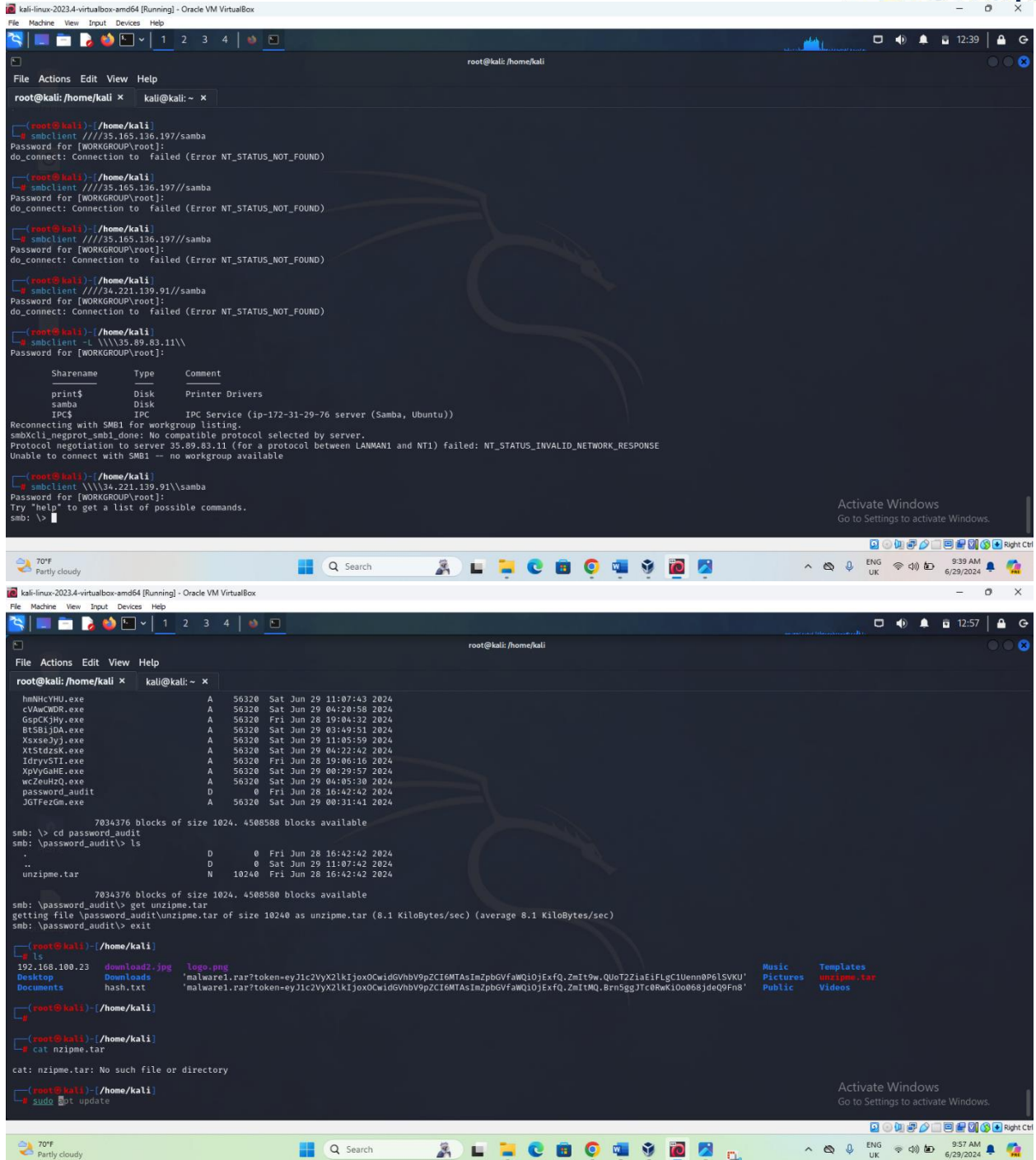
root@kali: /home/kali
# smbclient //14.221.139.91\\samba
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls
.                D           0 Sat Jun 29 11:07:42 2024
..               D           0 Sat Jun 29 11:07:42 2024
03kVXm0.exe      A 56320 Sat Jun 29 04:03:46 2024
hfvApRuz.exe     A 56320 Sat Jun 29 03:48:07 2024
hmNHeYHU.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
BTSB1jDA.exe     A 56320 Sat Jun 29 03:49:51 2024
Xsxe3jy.exe      A 56320 Sat Jun 29 11:05:59 2024
XtStzsk.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: \>

Activate Windows
Go to Settings to activate Windows.

70°F
Partly cloudy
Search
ENG
UK
9:41 AM
6/29/2024
```





```
root@kali: /home/kali
root@kali: ~
root@kali:~# smbclient //35.165.136.197/samba
Password for [WORKGROUP\root]:
do_connect: Connection to failed (Error NT_STATUS_NOT_FOUND)

root@kali:~# smbclient //35.165.136.197/samba
Password for [WORKGROUP\root]:
do_connect: Connection to failed (Error NT_STATUS_NOT_FOUND)

root@kali:~# smbclient //35.165.136.197/samba
Password for [WORKGROUP\root]:
do_connect: Connection to failed (Error NT_STATUS_NOT_FOUND)

root@kali:~# smbclient //34.221.139.91/samba
Password for [WORKGROUP\root]:
do_connect: Connection to failed (Error NT_STATUS_NOT_FOUND)

root@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.
smbcli_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:~# smbclient //34.221.139.91/samba
Password for [WORKGROUP\root]:
Try 'help' to get a list of possible commands.
smb: \>

70°F
Partly cloudy
9:39 AM
6/29/2024
Activate Windows
Go to Settings to activate Windows.

root@kali: /home/kali
root@kali: ~
root@kali:~# ls
hmlNHcYHU.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
BTSBJjDA.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
XpVydALe.exe       A      56320  Sat Jun 29 00:29:57 2024
wcZeuh2Q.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

7834376 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

7834376 blocks of size 1024. 4508588 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> exit

root@kali:~# ls
192.168.100.23  download2.jpg  logo.png
Desktop         Downloads      'malware1.rar?token=eyJ1c2VyX2lkIjoxO0CwidGVhbnV9p2Ci6MTAsImZpbGVfaWQ10jExfQ.ZmIt9w.QuoT2ZiaEiFlgC1Uenn0P6lSVKU'
Documents       hash.txt      'malware1.rar?token=eyJ1c2VyX2lkIjoxO0CwidGVhbnV9p2Ci6MTAsImZpbGVfaWQ10jExfQ.ZmIt9w.QuoT2ZiaEiFlgC1Uenn0P6lSVKU'

root@kali:~# cat nzipme.tar
cat: nzipme.tar: No such file or directory

root@kali:~# sudo apt update
```

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*