

CISCO EXAM –WRITE UP

FLORENCE MUSIMBI MWITA CS-EH03-25129.

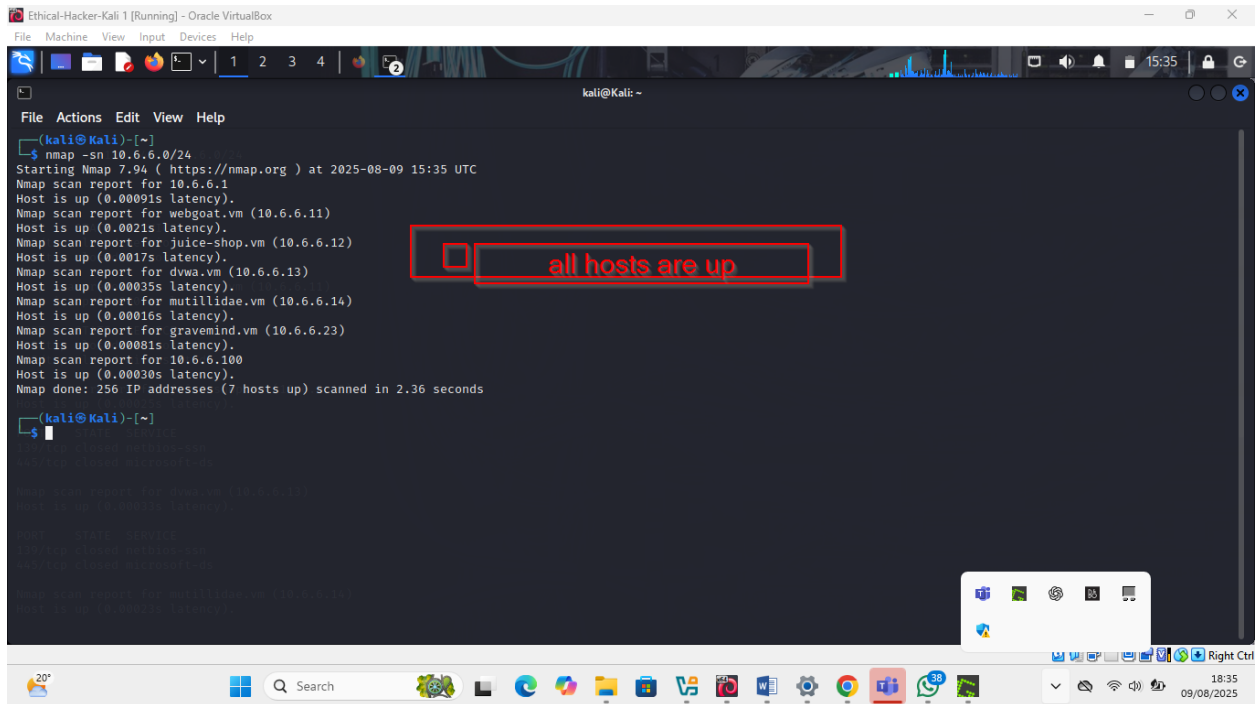
1.RECONNAISSANCE

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



```

Ethical-Hacker-Kali 1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@Kali: ~
File Actions Edit View Help
(kali@Kali)-[~]
$ nmap -sn 10.6.6.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2025-08-09 15:35 UTC
Nmap scan report for 10.6.6.1
Host is up (0.00091s latency).
Nmap scan report for webgoat.vm (10.6.6.11)
Host is up (0.0021s latency).
Nmap scan report for juice-shop.vm (10.6.6.12)
Host is up (0.0017s latency).
Nmap scan report for dwva.vm (10.6.6.13)
Host is up (0.00035s latency).
Nmap scan report for mutillidae.vm (10.6.6.14)
Host is up (0.00016s latency).
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00081s latency).
Nmap scan report for 10.6.6.100
Host is up (0.00030s latency).
Nmap done: 256 IP addresses (7 hosts up) scanned in 2.36 seconds
(kali@Kali)-[~]
$
```

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

```
File Actions Edit View Help
(kali@kali)-[~]
$ nmap -p 139,445 10.6.6.0/24
Starting Nmap 7.94 ( http://nmap.org ) at 2025-08-09 15:14 UTC
Nmap scan report for 10.6.6.1
Host is up (0.00051s latency).

PORT      STATE SERVICE
139/tcp    closed netbios-ssn
445/tcp    closed microsoft-ds

Nmap scan report for webchat.vm (10.6.6.11)
Host is up (0.00024s latency).

PORT      STATE SERVICE
139/tcp    closed netbios-ssn
445/tcp    closed microsoft-ds

Nmap scan report for juice-shop.vm (10.6.6.12)
Host is up (0.00025s latency).

PORT      STATE SERVICE
139/tcp    closed netbios-ssn
445/tcp    closed microsoft-ds

Nmap scan report for dwa.vm (10.6.6.13)
Host is up (0.00033s latency).

PORT      STATE SERVICE
139/tcp    closed netbios-ssn
445/tcp    closed microsoft-ds

Nmap scan report for mutillidae.vm (10.6.6.14)
Host is up (0.00023s latency).
```

this is a scan for the two ports for smb 139,445

this are host ports that are closed

Most ports are closed but two ports are open which are

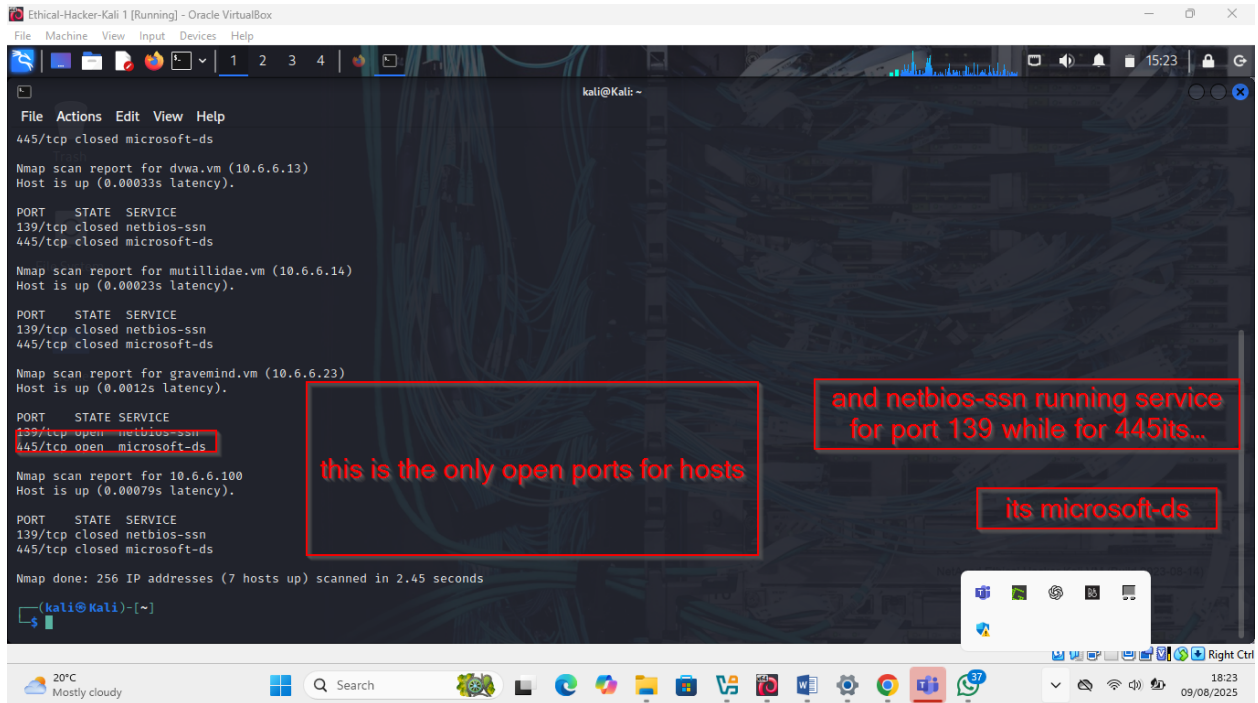
map scan report for gravemind.vm (10.6.6.23)

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

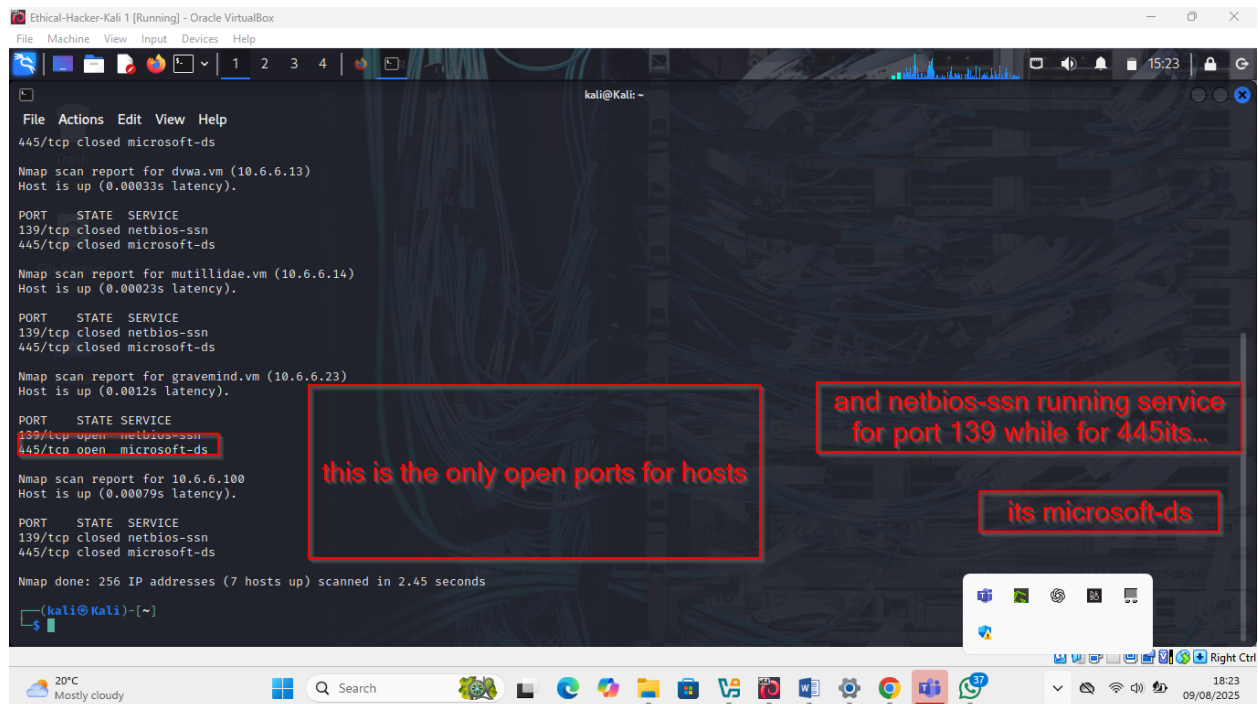
10.6.6.23 is the ip address of the host that is up

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.

Share2: workfiles Disk Confidential Workfiles

Share3: print\$ Disk Printer Drivers

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

EXPLOITATION PHASE

4b.

```

(kali@kali)-[~]
$ smbclient //10.10.10.10/homes -N
Anonymous login successful
tree connect failed: NT_STATUS_BAD_NETWORK_NAME

(kali@kali)-[~]
$ smbclient //10.6.6.23/workfiles -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.
..
38497656 blocks of size 1024, 2127996 blocks available
smb: \> exit

(kali@kali)-[~]
$ smbclient //10.6.6.23/print$ -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> LS
.
..
IA64
X64
W32X86
W32MIPS
W32ALPHA
COLOR
W32PPC
WIN40
OTHER

```

not accessible via anonymous

accessible via...

accessible but no files

accessible are they are

various files



These screenshots show how we tried to access 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.

```
(kali@kali)-[~]
$ smbclient //10.6.6.23/homes -N
Anonymous login successful
tree connect failed: NT_STATUS_BAD_NETWORK_NAME

(kali@kali)-[~]
$ smbclient //10.6.6.23/workfiles -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.                D                0    Mon Sep  2 13:39:42 2019
..               D                0    Fri Aug 13 20:15:47 2021
38497656 blocks of size 1024. 2127996 blocks available

smb: \> exit

(kali@kali)-[~]
$ smbclient //10.6.6.23/print$ -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> LS
.                D                0    Mon Aug 14 09:40:01 2023
..               D                0    Mon Aug 30 05:00:05 2021
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
```

not accessible via anonymous

accessible via...

accessible but no files

accessible are they are

various files

```
(kali@kali)-[~]
$ smbclient //10.6.6.23/IPC$ -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.                D                0    Mon Aug 30 05:00:05 2021
..               D                0    Mon Sep  2 13:39:42 2019
IA64              D                0    Mon Aug 30 05:00:05 2021
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
color             D                0    Mon Aug 30 05:00:05 2021

smb: \> cd OTHER/
smb: \OTHER> ls
.                D                0    Tue Aug 10 00:00:00 2021
..               D                0    Mon Aug 14 09:40:01 2023
taxes.txt         N                103  Wed Sep  1 00:00:00 2021

smb: \OTHER> get taxes.txt
getting file \OTHER\taxes.txt of size 103 as taxes.txt (3.9 KiloBytes/sec) (average 3.9 KiloBytes/sec)
smb: \OTHER> exit

(kali@kali)-[~]
$ smbclient //10.6.6.23/IPC$ -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
smb: \> exit

(kali@kali)-[~]
$
```

wew [we saw the most suspicious file...]

we saw other as the most...

we downloaded the txt file...

another openshare but no txt

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.

```
(kali@kali)-[~]
$ smbclient //10.6.6.23/nomes -N
Anonymous login successful
tree connect failed: NT_STATUS_BAD_NETWORK_NAME

(kali@kali)-[~]
$ smbclient //10.6.6.23/workfiles -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.
..
38497656 blocks of size 1024, 2127996 blocks available

(kali@kali)-[~]
$ smbclient //10.6.6.23/print$ -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> LS
.
..
IA64
x64
W32X86
W32MIPS
W32ALPHA
COLOR
W32PPC
WIN40
OTHER
```

```
(kali@kali)-[~]
$ smbclient //10.6.6.23/nomes -N
Anonymous login successful
tree connect failed: NT_STATUS_BAD_NETWORK_NAME

(kali@kali)-[~]
$ smbclient //10.6.6.23/workfiles -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.
..
38497656 blocks of size 1024, 2127996 blocks available

(kali@kali)-[~]
$ smbclient //10.6.6.23/print$ -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> LS
.
..
IA64
x64
W32X86
W32MIPS
W32ALPHA
COLOR
W32PPC
WIN40
OTHER
```

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.

```
(kali@Kali)-[~]
$ smbclient //10.6.6.23/nomes -N
Anonymous login successful
tree connect failed: NT_STATUS_BAD_NETWORK_NAME

(kali@Kali)-[~]
$ smbclient //10.6.6.23/workfiles -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.
..
38497656 blocks of size 1024. 2127996 blocks available

(kali@Kali)-[~]
$ smbclient //10.6.6.23/print$ -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.
..
IA64
x64
W32X86
W32MIPS
W32ALPHA
COLOR
W32PPC
WIN40
OTHER
```

not accessible via anonymous

accessible via...

accessible are they are various files

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.

The screenshot shows a Kali Linux terminal window titled 'Ethical-Hacker-Kali [Running] - Oracle VirtualBox'. The terminal is in the directory ~/Downloads. A red box highlights the output of the 'ls' command, listing various files including 'eaters-collective-12eHC6FxFPyg-unsplash.jpg', 'eaters-collective-12eHC6FxFPyg-unsplash_with_secret.jpg', 'enc_flag', 'elephants.jpg', 'elephants_with_secret.jpg', and several 'floremcemwita94' files. Another red box highlights the output of the 'cat taxes.txt' command, which displays a congratulatory message: 'Congratulations! You found the flag for Challenge 3! The code for this challenge is A9!15wa2.' The terminal window is overlaid on a Windows desktop environment.

```
(kali@kali)~$ cd Downloads/

(kali@kali)~/Downloads$ ls
SA.pcap          eaters-collective-12eHC6FxFPyg-unsplash.jpg  elephants.jpg          'floremcemwita94(1).ovpn'  'floremcemwita94(4).ovpn'  hash.txt
eaters-collective-12eHC6FxFPyg-unsplash_with_secret.jpg  elephants_with_secret.jpg  'floremcemwita94(2).ovpn'  'floremcemwita94(5).ovpn'  red.png
enc_flag          'floremcemwita94(3).ovpn'  floremcemwita94.ovpn      secret.t

(kali@kali)~/Downloads$ cat taxes.txt
Congratulations!
You found the flag for Challenge 3!
The code for this challenge is A9!15wa2.

(kali@kali)~/Downloads$
```

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.

```
kali@Kali: ~  
File Actions Edit View Help  
.. D 0 Mon Aug 30 05:00:05 2021  
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  
WIN64 D 0 Mon Sep 2 13:39:42 2019  
OTHER D 0 Tue Aug 10 00:00:00 2021  
color D 0 Mon Aug 30 05:00:05 2021  
~/.Downloads  
38497656 blocks of size 1024. 2127996 blocks available  
smb: \> cd OTHER/  
smb: \OTHER> ls  
.. D 0 Tue Aug 10 00:00:00 2021  
taxes.txt N 103 Wed Sep 1 00:00:00 2021  
38497656 blocks of size 1024. 2127996 blocks available  
smb: \OTHER> get taxes.txt  
getting file \OTHER\taxes.txt of size 103 as taxes.txt (3.9 KiloBytes/sec) (average 3.9 KiloBytes/sec)  
smb: \OTHER> exit  
(kali@Kali)-[~]  
$ smbclient //10.6.6.23/IPC$ -N  
Anonymous login successful  
Try "help" to get a list of possible commands.  
smb: \> LS  
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*  
smb: \> exit  
(kali@Kali)-[~]  
$
```

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.

```
kali@Kali: ~/Downloads  
File Actions Edit View Help  
(kali@Kali)-[~]  
$ cd Downloads/  
(kali@Kali)-[~/Downloads]  
$ ls  
SA.pcap elephants.jpg 'floremcmwita94(1).ovpn' 'floremcmwita94(4).ovpn' hash.txt  
eaters-collective-12eHC6FXPyg-unsplash.jpg elephants_with_secret.jpg 'floremcmwita94(2).ovpn' 'floremcmwita94(5).ovpn' red.png  
eaters-collective-12eHC6FXPyg-unsplash_with_secret.jpg enc_flag 'floremcmwita94(3).ovpn' floremcmwita94.ovpn secret.t  
(kali@Kali)-[~/Downloads]  
$ cat taxes.txt  
Congratulations!  
You found the flag for Challenge 3!  
The code for this challenge is A9!15wa2.  
(kali@Kali)-[~/Downloads]  
$
```

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)



```
File Actions Edit View Help
(kali@kali)-[~]
$ cd Downloads/

(kali@kali)-[~/Downloads]
$ ls
SA.pcap          elephants.jpg      'floremcmwita94(1).ovpn' 'floremcmwita94(4).ovpn' hash.txt
eaters-collective-12eHC6FxPyg-unsplash.jpg  elephants_with_secret.jpg 'floremcmwita94(2).ovpn' 'floremcmwita94(5).ovpn' red.png
eaters-collective-12eHC6FxPyg-unsplash_with_secret.jpg  enc_flag              'floremcmwita94(3).ovpn' 'floremcmwita94.ovpn' secret.t

(kali@kali)-[~/Downloads]
$ cat taxes.txt
Congratulations!
You found the flag for Challenge 3!
The code for this challenge is A9!15wa2.

(kali@kali)-[~/Downloads]
$
```

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 their 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 in order to access the shares

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

CONCLUSION

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

