Day 10 - Don't be sElfish!

Scenario

Day 10: Don't be so sElfish - Prelude

The Best Festival Company (TBFC) has since upscaled its IT infrastructure after last year's attack for all the other elves to use, including a VPN server and a few other services. You breathe a sigh of relief... *"That's it, Me, Elf McEager saved the Christmas of 2020! I can't wait to---"*

But suddenly, a cold shiver runs down your spine, interrupting your monologue...

You suddenly recall that Elf McSkidy had set up a Samba file server just before the attack occurred - could this have been hacked too?! What about our data...Oh no, **quick!** Find out what usernames may have been leaked and attempt to login to the server yourself, noting down any vulnerabilities found to report back to Elf McSkidy.

Watch DarkStars video on solving this task!

let's use enum4linux to find the users in Samba server & we've found 3 users in the Samba server

```
 ==========================
|    Users on 10.10.87.70  |
 ==========================
Use of uninitialized value $users in print at ./enum4linux.pl line 874.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 877.

user:[elfmcskidy] rid:[0x3e8]
user:[elfmceager] rid:[0x3ea]
user:[elfmcelferson] rid:[0x3e9]

 ============================================
```

Question #1 Using enum4linux, how many users are there on the Samba server (`10.10.87.70`)?
-3

now we check the results again to find how many shares does the samba server have
//we've found 4 shares

```
 ==========================================
|    Share Enumeration on 10.10.87.70      |
 ==========================================

        Sharename       Type      Comment
        ---------       ----      -------
        tbfc-hr         Disk      tbfc-hr
        tbfc-it         Disk      tbfc-it
        tbfc-santa      Disk      tbfc-santa
        IPC$            IPC       IPC Service (tbfc-smb server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available
```

Question #2 Now how many "shares" are there on the Samba server?
-4

now let's find which shares that doesn't need credential, we can use smbmap to automate the process
//here it shows that "tbfc-santa" share we've read,write permission on this share as guest

```
┌──(nobodyatall㉿0×DEADBEEF)-[~]
└─$ smbmap -u '' -p '' -H 10.10.87.70
[+] Guest session       IP: 10.10.87.70:445     Name: 10.10.87.70
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        tbfc-hr                                                 NO ACCESS       tbfc-hr
        tbfc-it                                                 NO ACCESS       tbfc-it
        tbfc-santa                                              READ, WRITE     tbfc-santa
        IPC$                                                    NO ACCESS       IPC Service (tbfc-smb server (Samba, Ubuntu))
```

Question #3 Use smbclient to try to login to the shares on the Samba server (`10.10.87.70`). What share doesn't require a password?
-tbfc-santa

now let's login into the share & find the notes that mcskidy left
//note_from_mcskidy.txt seems to be the notes that left by mcskidy

```
┌──(nobodyatall㉿0×DEADBEEF)-[~]
└─$ smbclient //10.10.87.70/tbfc-santa
Enter WORKGROUP\nobodyatall's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Dec 12 10:51:03 2020
  ..                                  D        0  Wed Nov 11 20:32:21 2020
  jingle-tunes                        D        0  Wed Nov 11 21:10:41 2020
  note_from_mcskidy.txt               N      143  Wed Nov 11 21:12:07 2020

                10252564 blocks of size 1024. 5191832 blocks available
smb: \>
```

get the note & read the content

```
smb: \> get note_from_mcskidy.txt
getting file \note_from_mcskidy.txt of size 143 as note_from_mcskidy.txt (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)
smb: \> !cat note_from_mcskidy.txt
Hi Santa, I decided to put all of your favourite jingles onto this share - allowing you access it from anywhere you like! Regards ~ ElfMcSkidy
smb: \>
```

so it seems that mcskidy left a 'jingle-tunes' directory for santa to let it access santa's favourite jingles in this share

```
  ..                                  D        0  Wed Nov 11 20:32:21 2020
  jingle-tunes                        D        0  Wed Nov 11 21:10:41 2020
  note_from_mcskidy.txt               N      143  Wed Nov 11 21:12:07 2020
```

Question #4 Log in to this share, what directory did ElfMcSkidy leave for Santa?
-jingle-tunes