PSP0201 Week 3 Writeup

Group Name: ikun no 1

Members
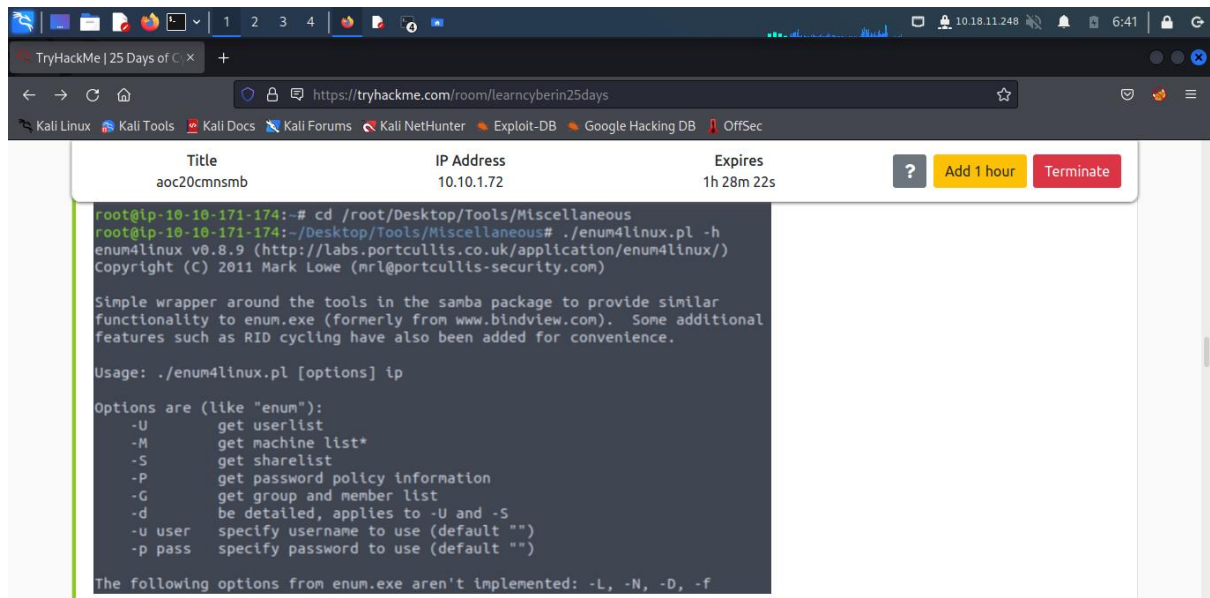
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

Day 10: Networking Don't be sElfish!
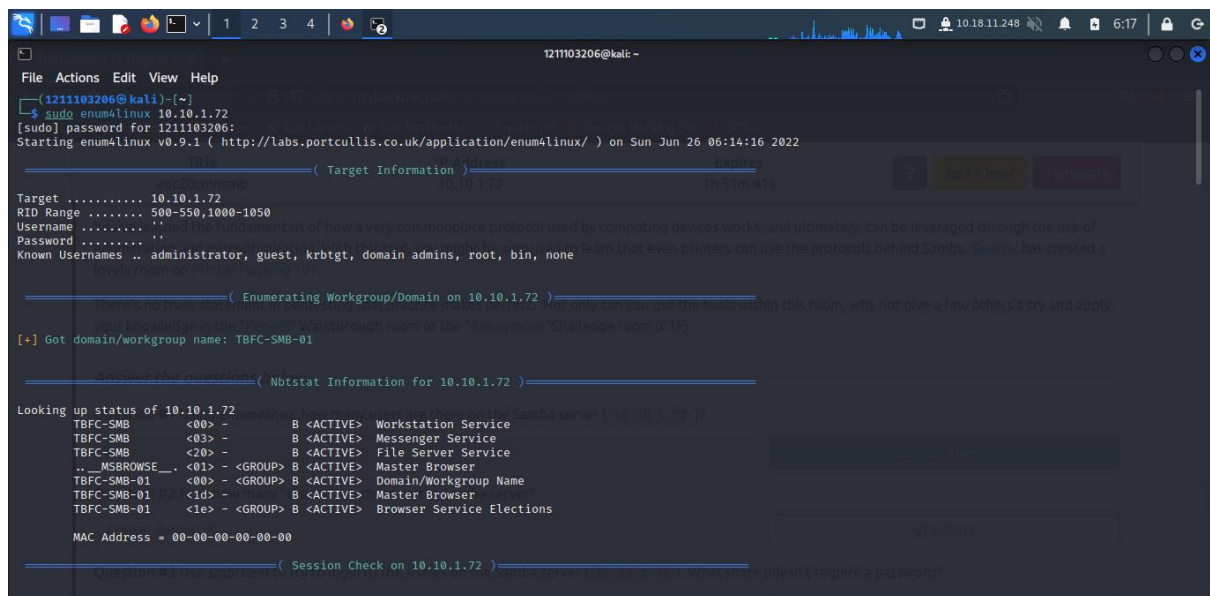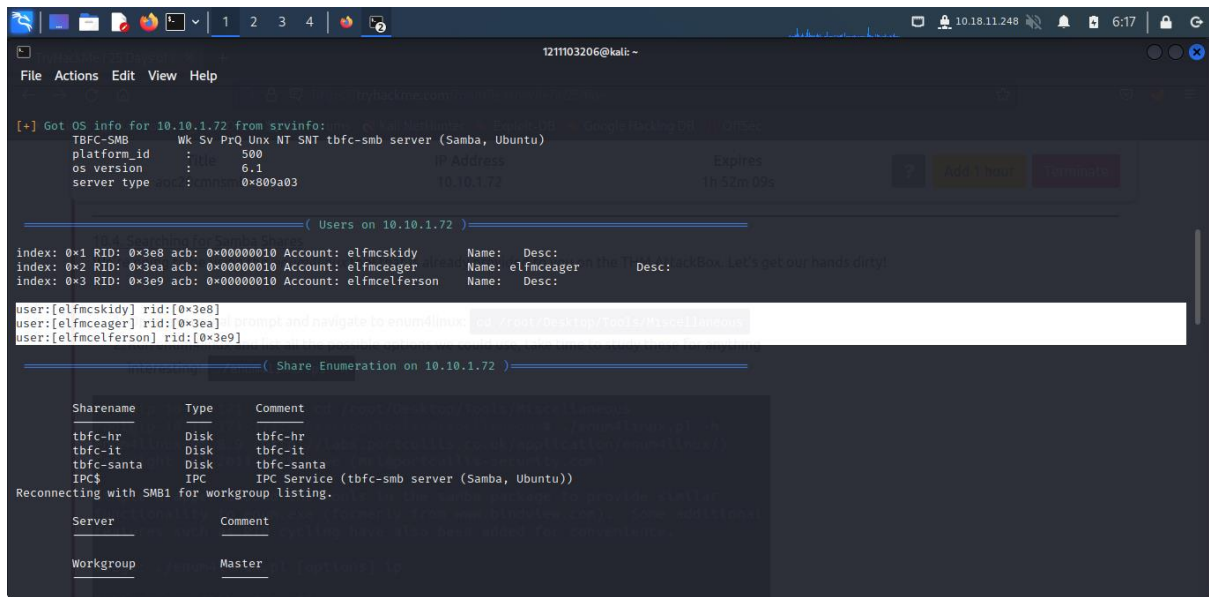
Tool used: Kali-Linux

Solution/walkthrough:

Question 1

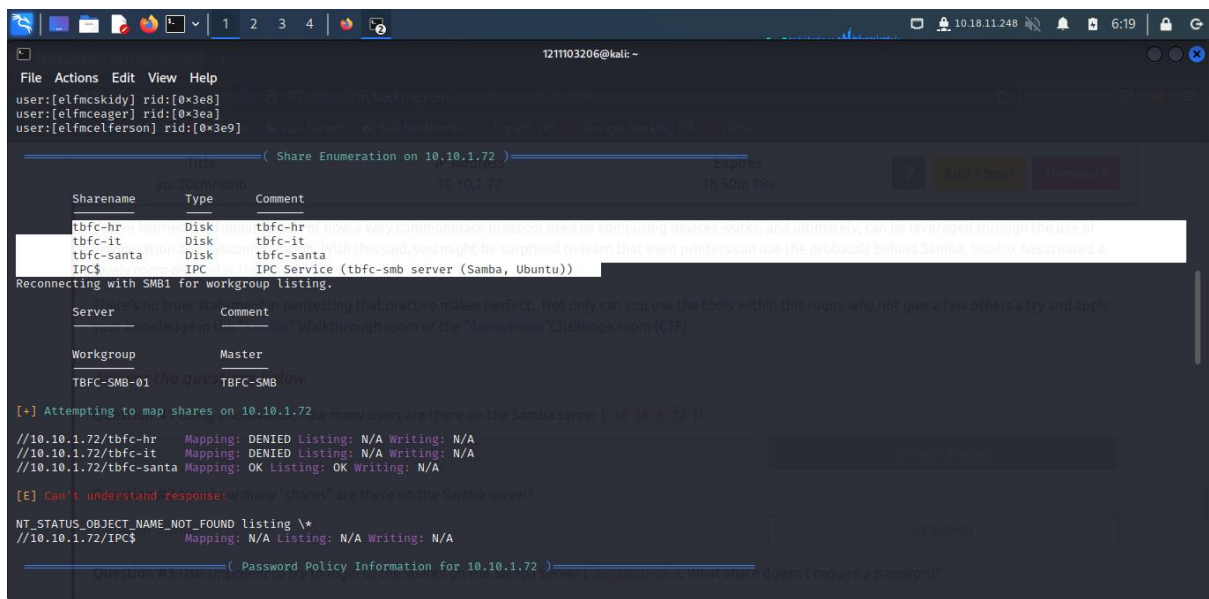Search the answer in THM or the help option.

Question 2

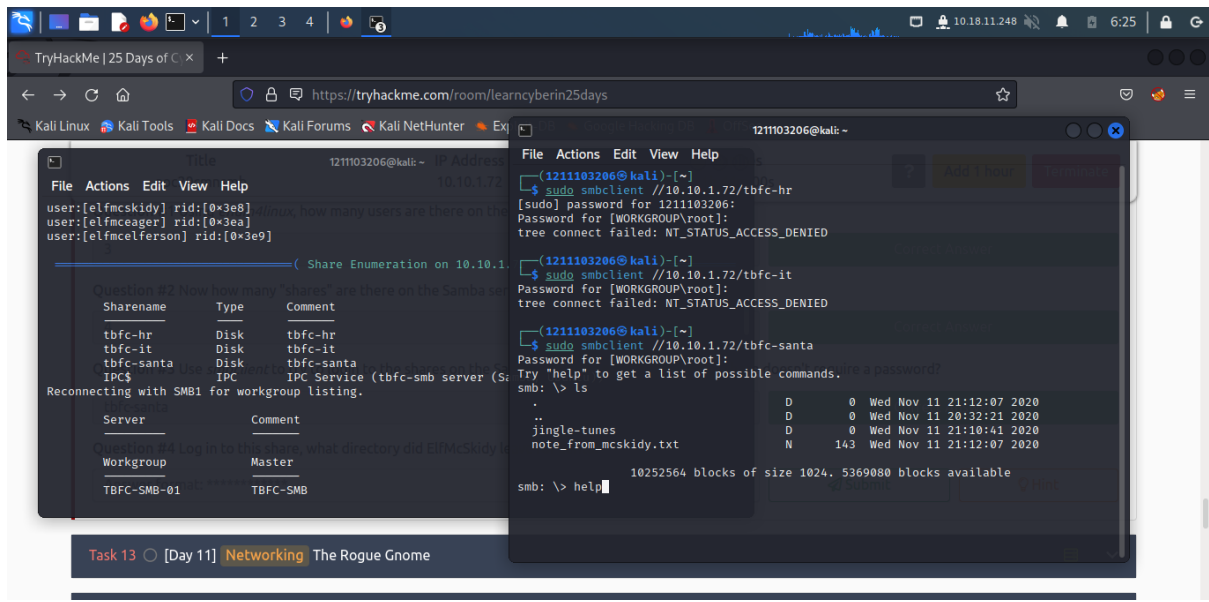

Open the terminal and use enum4linux to enter the server.

```
[+] Got OS info for 10.10.1.72 from srvinfo:
        TBFC-SMB       Wk Sv PrQ Unx NT SNT tbfc-smb server (Samba, Ubuntu)
        platform_id    :      500
        os version     :      6.1
        server type    :      0x809a03

===============================( Users on 10.10.1.72 )===============================
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy      Name:   Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager      Name: elfmceager    Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson   Name:   Desc:

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

===========================( Share Enumeration on 10.10.1.72 )===========================

        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))
Reconnecting with SMB1 for workgroup listing.

        Server          Comment
        ---------       -------

        Workgroup       Master
        ---------       ------
```

Find the answer in the users on ip address.

Question 3


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

===========================( Share Enumeration on 10.10.1.72 )===========================

        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))
Reconnecting with SMB1 for workgroup listing.

        Server          Comment
        ---------       -------

        Workgroup       Master
        ---------       ------
        TBFC-SMB-01     TBFC-SMB

[+] Attempting to map shares on 10.10.1.72

//10.10.1.72/tbfc-hr     Mapping: DENIED Listing: N/A Writing: N/A
//10.10.1.72/tbfc-it     Mapping: DENIED Listing: N/A Writing: N/A
//10.10.1.72/tbfc-santa  Mapping: OK Listing: OK Writing: N/A

[E] Can't understand response:

NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
//10.10.1.72/IPC$        Mapping: N/A Listing: N/A Writing: N/A

====================( Password Policy Information for 10.10.1.72 )====================
```
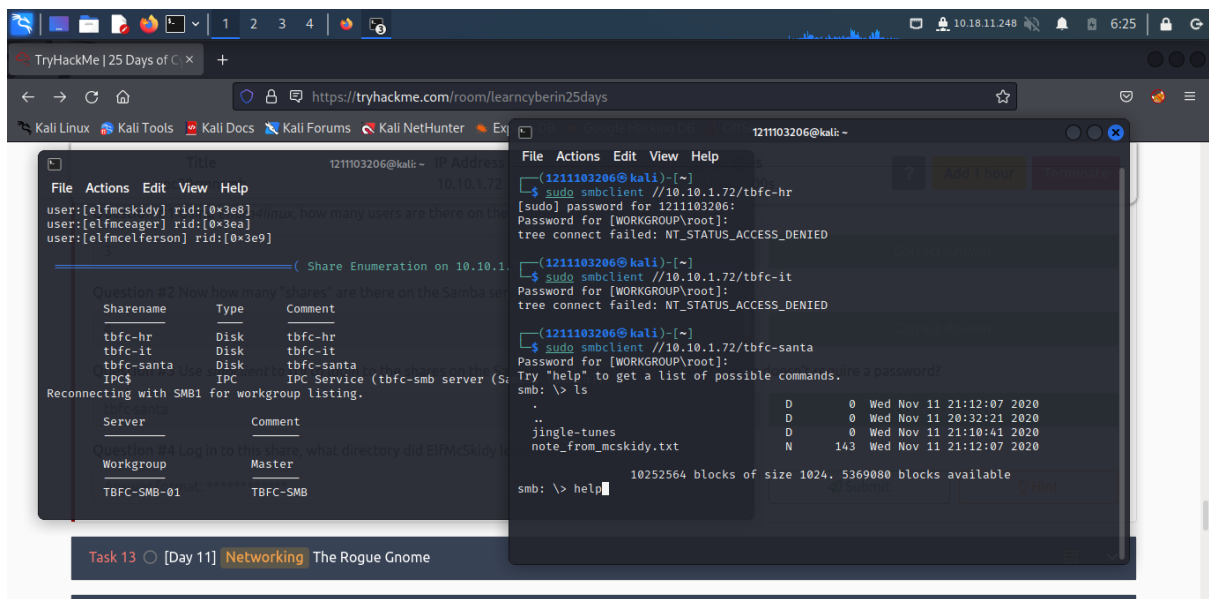
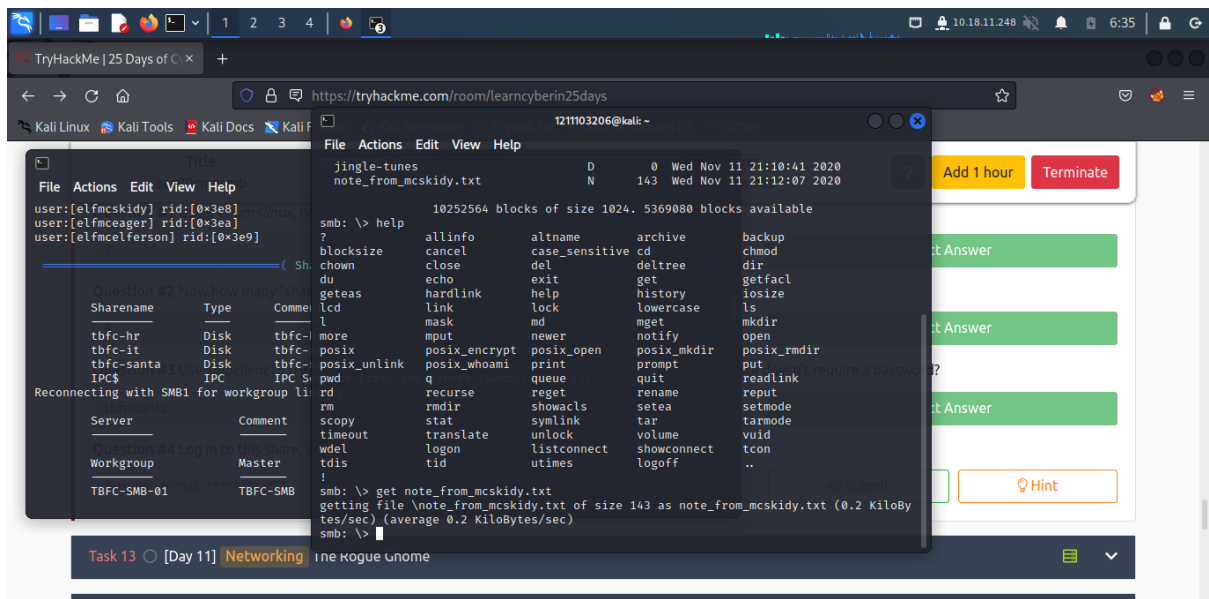Find the answer in the share enumeration.

Question 4

First, use sudo smbclient //<ip address>/ (share name) to find which share name login without password. Then the tbfc-santa is answer.
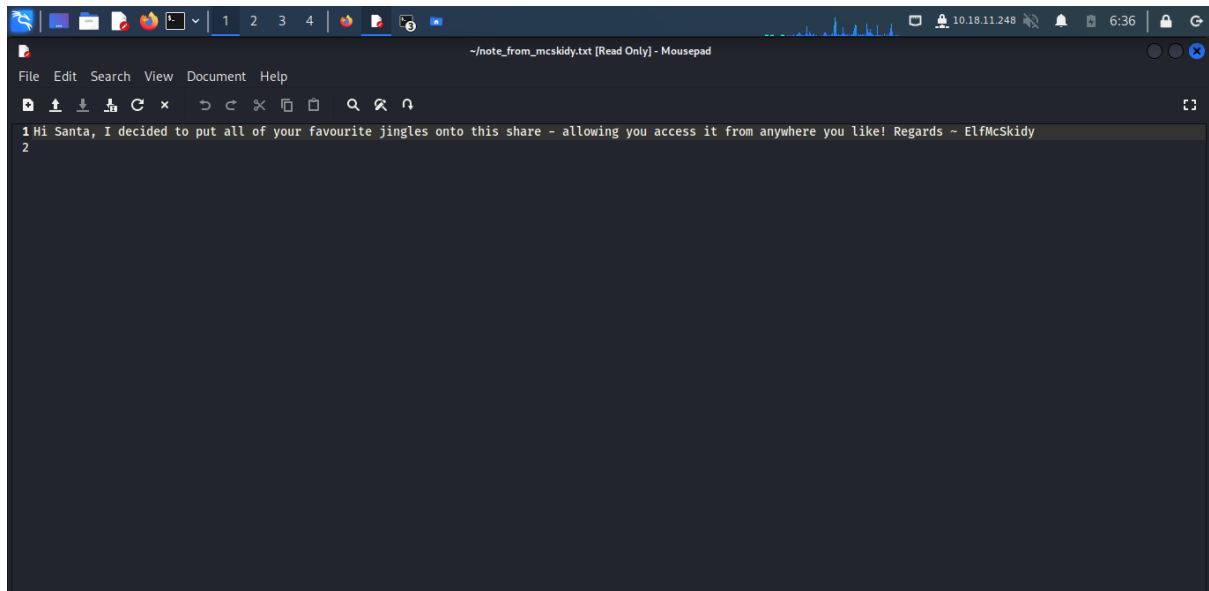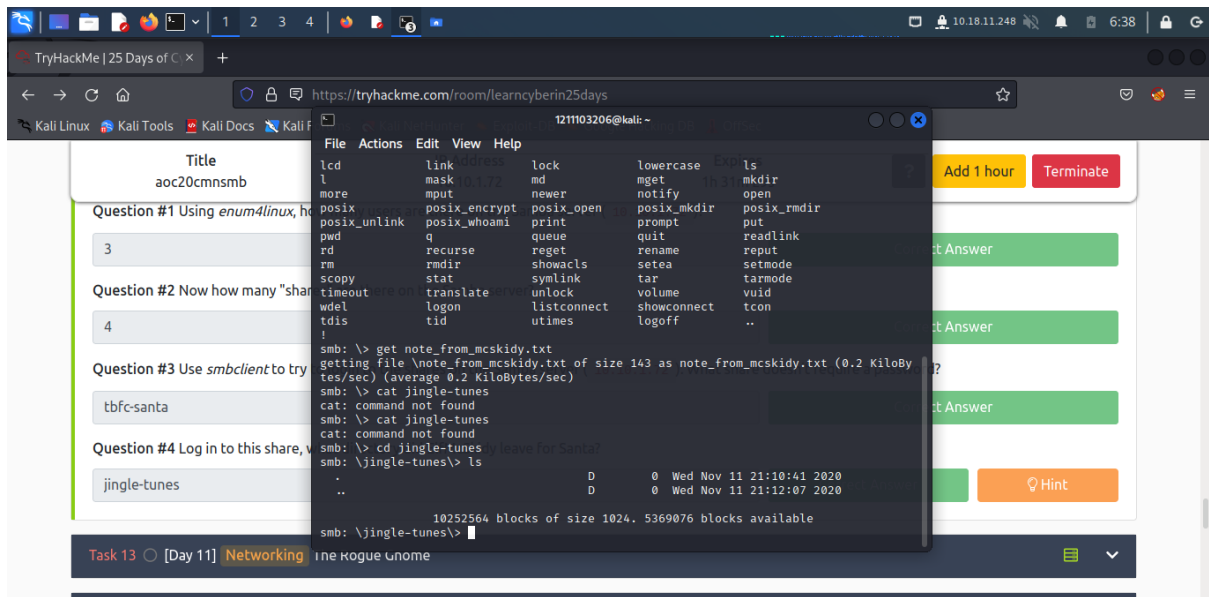
Question 5

Ls the tbfc-santa.

Then, download the note_from_mcskidy.txt

After that, open the txt.

The ElfMcSkidy leave for Santa is the jingle-tunes.