

PSP0201

Week 3

Writeup

Group Name: Undecided

Members

ID	Name	Role
1211101390	Aslamia Najwa Binti Ahmad Khadri	Leader
1211100431	Mohammad Omar Torofder	Member
1211103388	Vishnu Karmegam	Member
1211103092	Farryn Aisha binti Muhd Firdaus	Member

Day 10 : Networking – Don't be sElfish!

Tools used: Kali Linux, Firefox

Solution/walkthrough:

Question 1

Enter the 'enum4linux -h' command to display help message where they explain the option in detail.

```
127.0.0.1@kali ~$ enum4linux -h
enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (ml@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com). Some additional
features such as RID cycling have also been added for convenience.

Usage: ./enum4linux.pl [options] ip

Options are (like "enum"):
-U get userlist
-M get machine list
-S get sharelist
-P get password policy information
-G get group and member list
-d be detailed, applies to -U and -S
-u user specify username to use (default "")
-p pass specify password to use (default "")

The following options from enum.exe aren't implemented: -L, -N, -D, -f

Additional options:
-a Do all simple enumeration (-U -S -G -P -r -o -n -i).
  This option is enabled if you don't provide any other options.
-h Display this help message and exit
-r enumerate users via RID cycling
-R RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
-k n keep searching RIDs until n consecutive RIDs don't correspond to
  a username. Implies RID range ends at 999999. Useful
  against DCs.
-l Get some (limited) info via LDAP 389/TCP (for DCs only)
-s file brute force guessing for share names
-k user User(s) that exists on remote system (default: administrator,guest,krbtgt,admins,root,bin,one)
  Used to get sid with "lookupsid known_username"
  Use commas to try several users: "-k admin,user1,user2"
-o Get OS information
-i Get printer information
-w wkg Specify workgroup manually (usually found automatically)
-n Do an smblookup (similar to nbtstat)
-v Verbose. Shows full commands being run (net, rpcclient, etc.)
-A Aggressive. Do write checks on shares etc

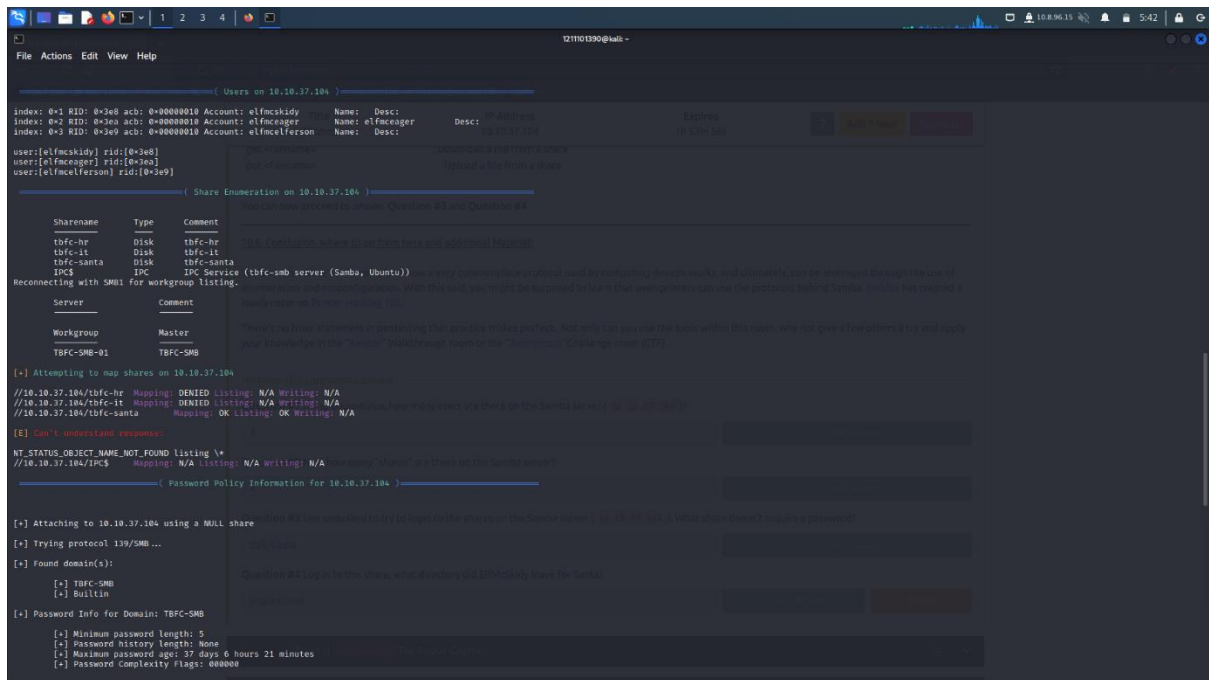
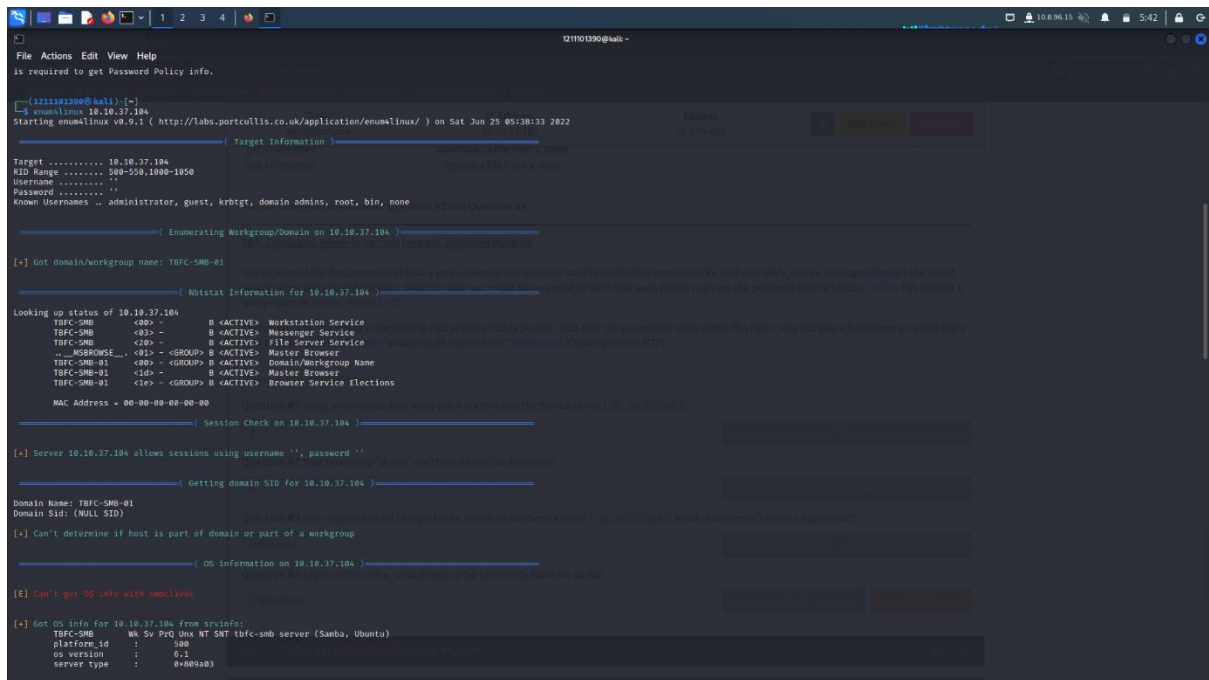
RID cycling should extract a list of users from Windows (or Samba) hosts
which have RestrictAnonymous set to 1 (Windows NT and 2000), or "Network
access: Allow anonymous SID/Name translation" enabled (XP, 2003).

NB: Samba servers often seem to have RIDs in the range 3000-3050.

Dependency info: You will need to have the samba package installed as this
script is basically just a wrapper around rpcclient, net, smblookup and
smbclient. Poileum from http://labs.portcullis.co.uk/application/poileum/
is required to get Password Policy info.
```

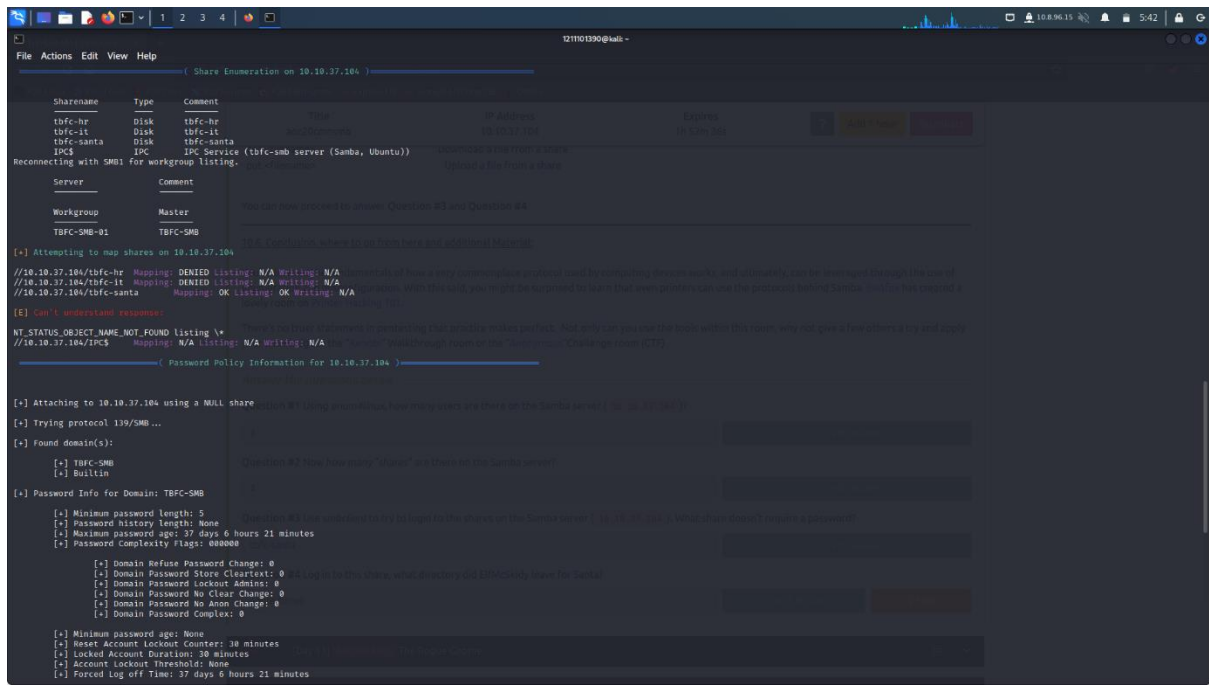
Question 2

Enter the command 'enum4linux 10.10.37.104'. The IP address was provided from the machine of the task in tryhackme.com. This command allows us to see how many users are there on the Samba server.



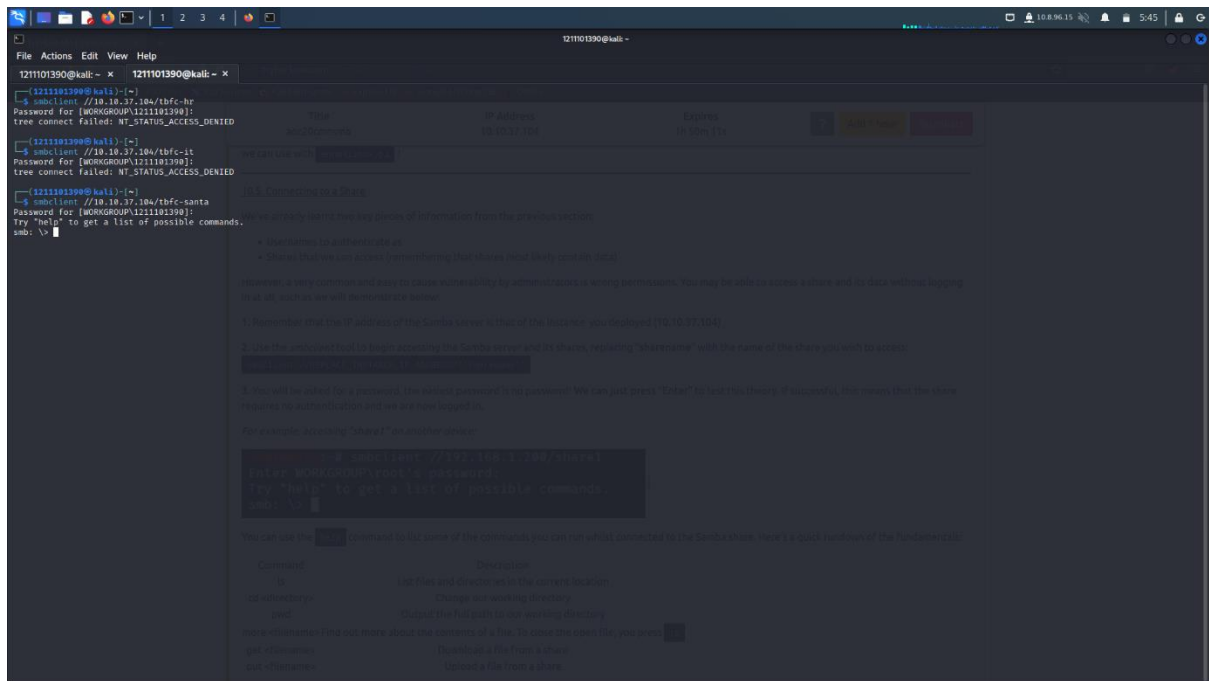
Question 3

From the command we had entered earlier, we scroll down to see more information until we found the ‘Share Enumeration on 10.10.37.104’ where we can see the amount of ‘shares’ on the Samba server.



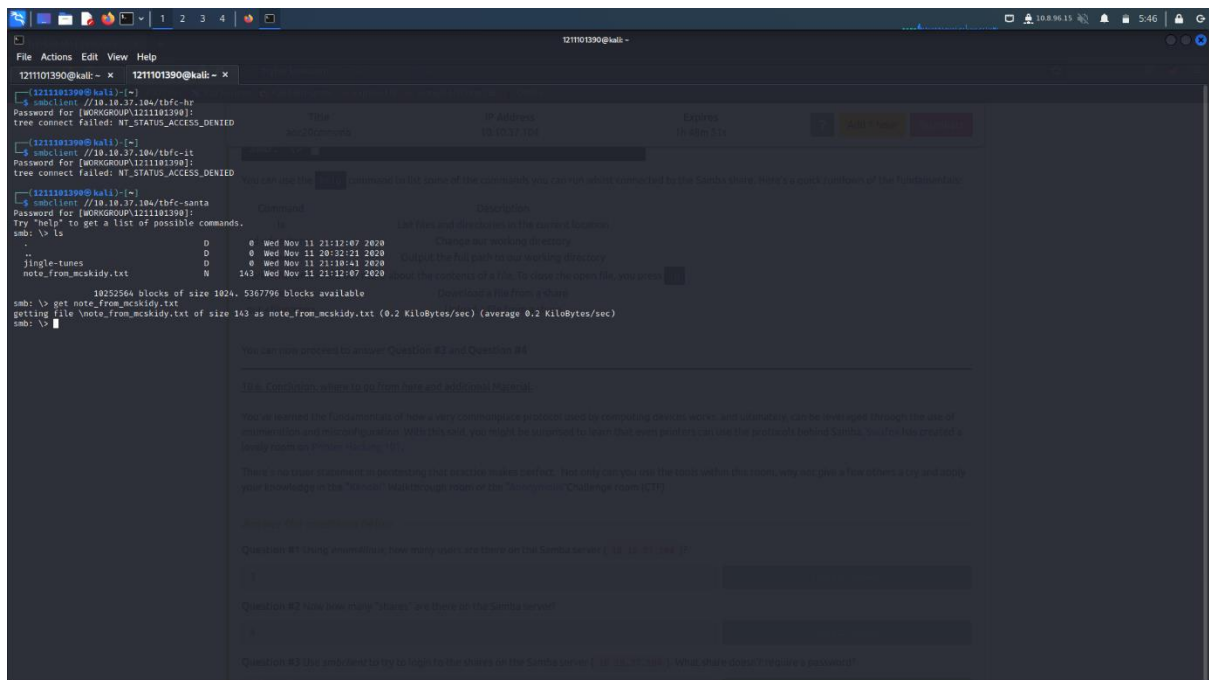
Question 4

We use 'smbclient //10.10.37.104/*shares*' to try logging to the shares on the Samba server. After a few trials and error, we found that the share 'tbfc-santa' doesn't require password so we logged into the share with it.



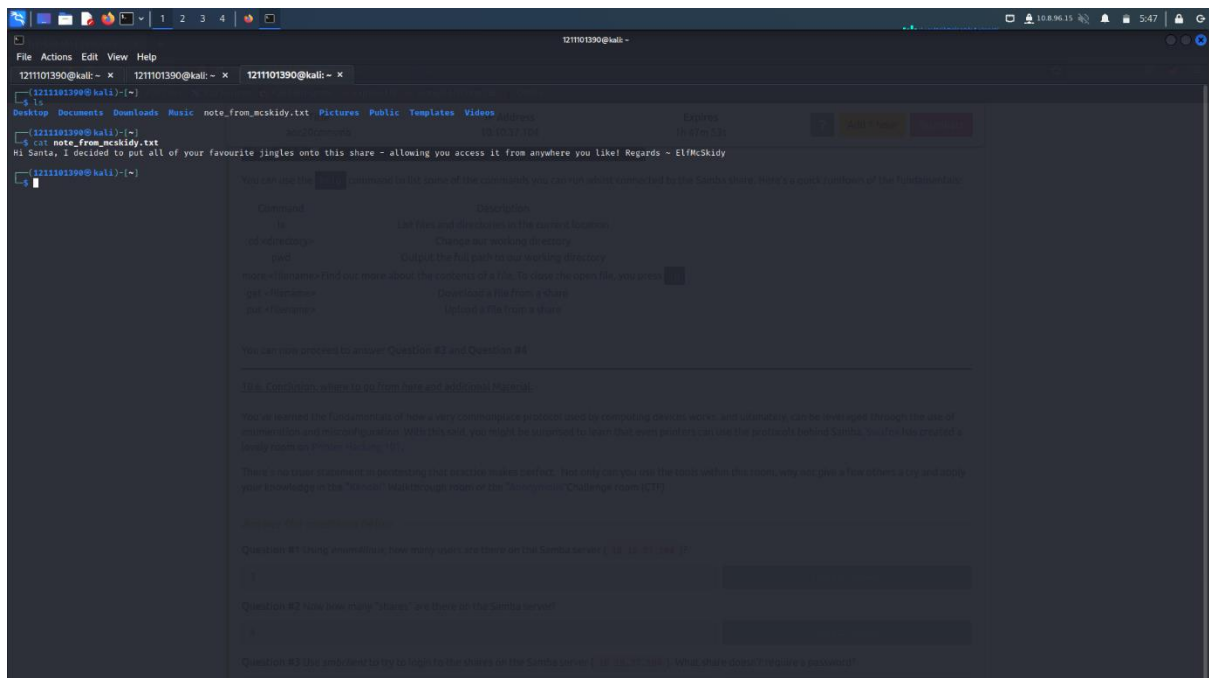
Question 5

We use 'ls' command to see the directory list and found a few files. We decided to download the text file named 'note_from_mcskidty.txt' using the get command.



```
121101390@kali: ~  
[121101390@kali:~]$ smbclient //19.18.37.104/tbfc-hr  
Password for [WORKGROUP\121101390]:  
tree connect failed: NT_STATUS_ACCESS_DENIED  
[121101390@kali:~]$  
[121101390@kali:~]$ smbclient //19.18.37.104/tbfc-it  
Password for [WORKGROUP\121101390]:  
tree connect failed: NT_STATUS_ACCESS_DENIED  
[121101390@kali:~]$  
[121101390@kali:~]$ smbclient //19.18.37.104/tbfc-santa  
Password for [WORKGROUP\121101390]:  
Try 'help' to get a list of possible commands.  
smb: \> ls  
.  
..  
jingle-tunes  
note_from_mcskidty.txt  
10252564 blocks of size 1024. 5367796 blocks available  
smb: \> get note_from_mcskidty.txt  
getting file \note_from_mcskidty.txt of size 143 as note_from_mcskidty.txt (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)  
smb: \>
```

In another tab, we use the 'cat' function to display the text file that has been downloaded earlier and found mcskidty's note to santa. We understood then that the directory 'jingle-tunes' was left for santa from mcskidty.



```
121101390@kali: ~  
[121101390@kali:~]$ ls  
Desktop Documents Downloads Music note_from_mcskidty.txt Pictures Public Templates Videos  
[121101390@kali:~]$  
[121101390@kali:~]$ cat note_from_mcskidty.txt  
Hi Santa, I decided to put all of your favourite jingles onto this share - allowing you access it from anywhere you like! Regards - El(McSkidy  
[121101390@kali:~]$
```

Thought Process/Methodology:

After thorough read, we open the terminal to start our work. We enter the 'enum4linux -h' command to display help message where they explain the option in detail. In there, we

learn more option and are able to answer the first question. Next, we enter the command 'enum4linux 10.10.37.104'. The IP address was provided from the machine of the task in tryhackme.com so it may vary with users. This command allows us to see how many users are there on the Samba server. Under 'Users on 10.10.37.104', we found 3 user which are elfmcskidy, elfmcager, eldmcelferon. Then, we continue scrolling down for more information until we stumbled across the 'Share Enumeration on 10.10.37.104'. Under it are the sharename for the Samba server. With 'smbclient //10.10.37.104/*shares*' command, we tried logging to the shares on the Samba server in a new tab. After a few trials and error, we found that the share 'tbfc-santa' doesn't require password, so we logged into the share with it. Afterward, we use 'ls' command to see the directory list. We decided to download the text file named 'note_from_mcskidy.txt' using the get command. Once again, we open a new tab and display the text file that has been downloaded earlier with the 'cat' function. We read the note left for santa by mcskidy and concluded that the directory 'jingle-tunes' is the directory left for santa.