PSP0201 Week 3 Writeup

Group Name: ikun no 1

Members

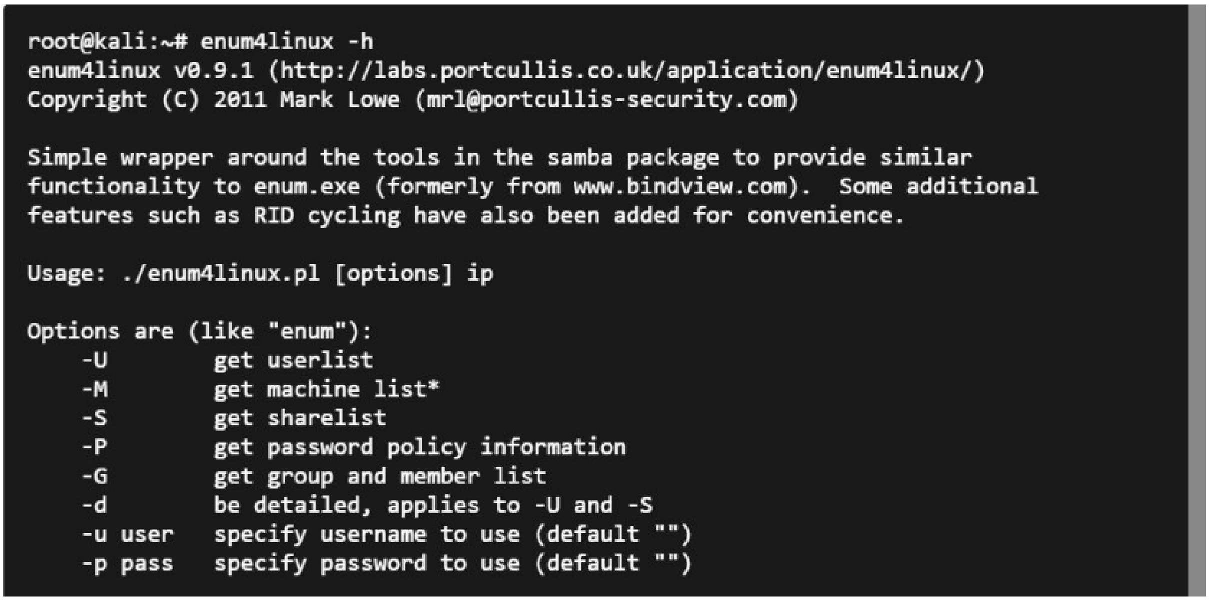
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

Day 10 -[Networking] Don't be sElfish!

Tool used: kali Linux, Firefox, enum4linux, smbcilent

Solution/Walkthrough:

Q1

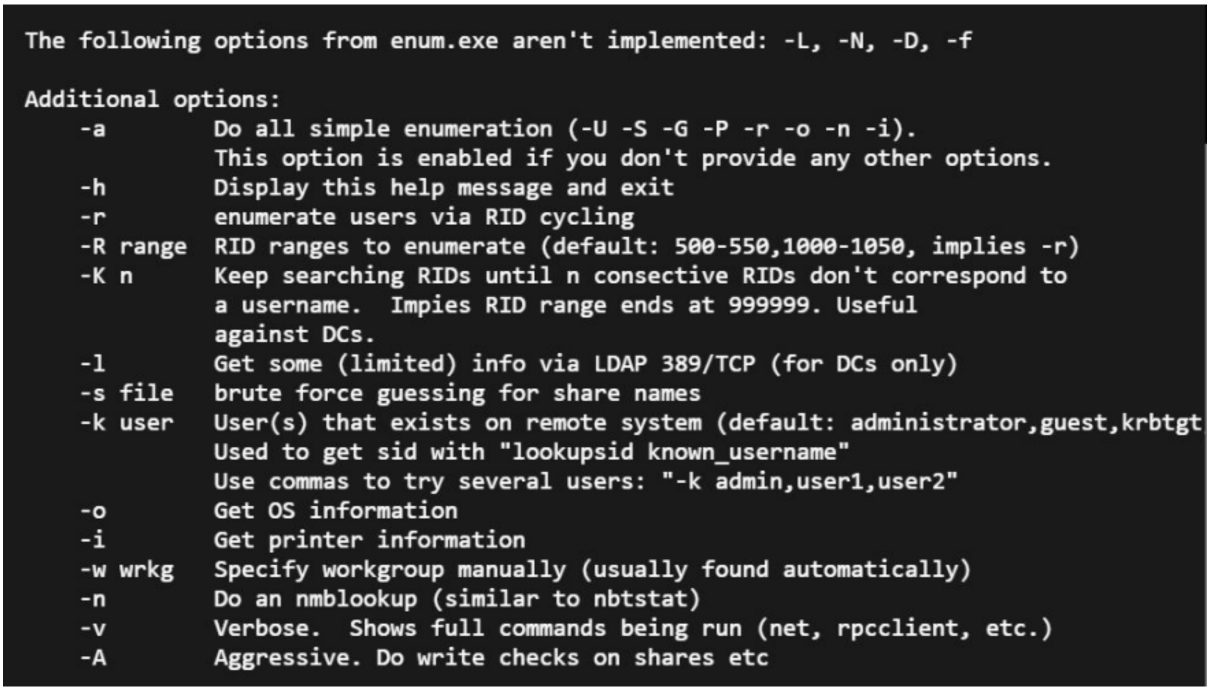


```
root@kali:~# enum4linux -h
enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

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 "")
```

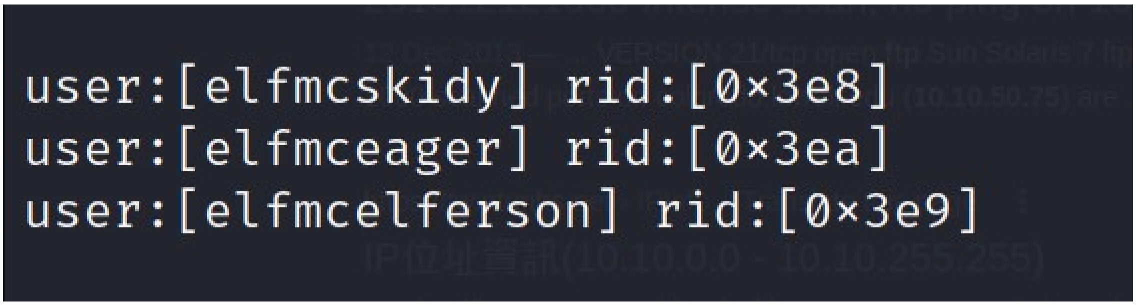


```
The following options from enum.exe aren't implemented: -L, -N, -D, -f

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 range  RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
    -K n      Keep searching RIDs until n consective RIDs don't correspond to
              a username.  Impies 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
              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 wrkg   Specify workgroup manually (usually found automatically)
    -n        Do an nmblookup (similar to nbtstat)
    -v        Verbose.  Shows full commands being run (net, rpcclient, etc.)
    -A        Aggressive. Do write checks on shares etc
```

Match the answer after examining the help options for enum4linux.

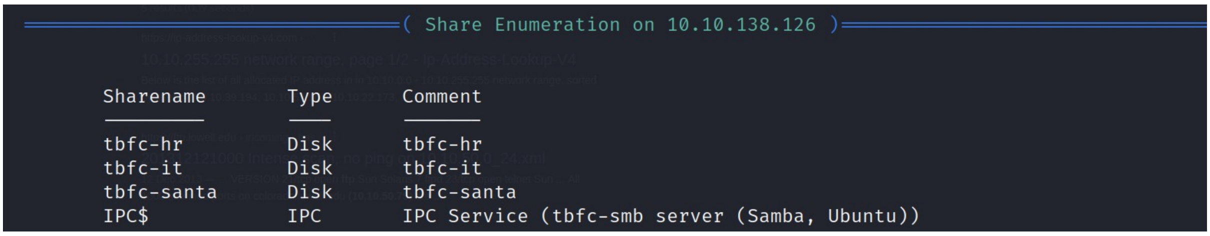
Q2.



```
user:[elfmcskidy] rid:[0×3e8]
user:[elfmceager] rid:[0×3ea]
user:[elfmcelferson] rid:[0×3e9]
```

Users can be found after enum4linux is used on target.

Q3.

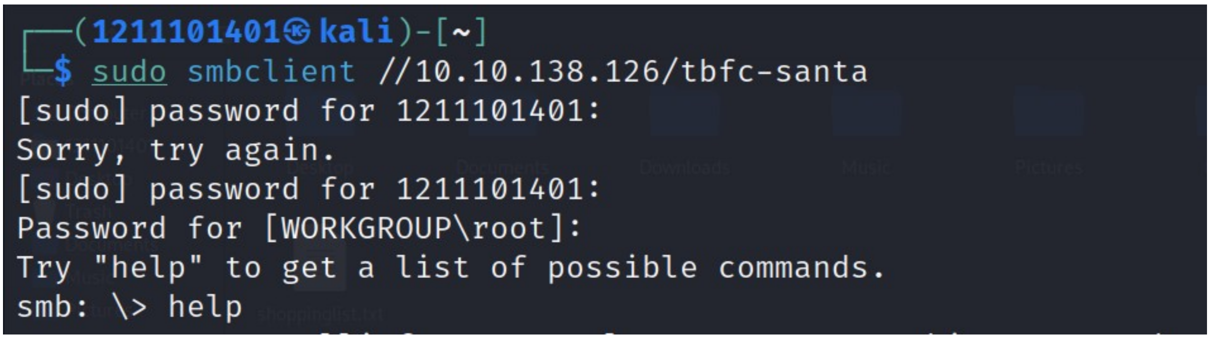


```
========================( Share Enumeration on 10.10.138.126 )========================

        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))
```

Shares can be found below the list of sharename after the enum4linux is used.

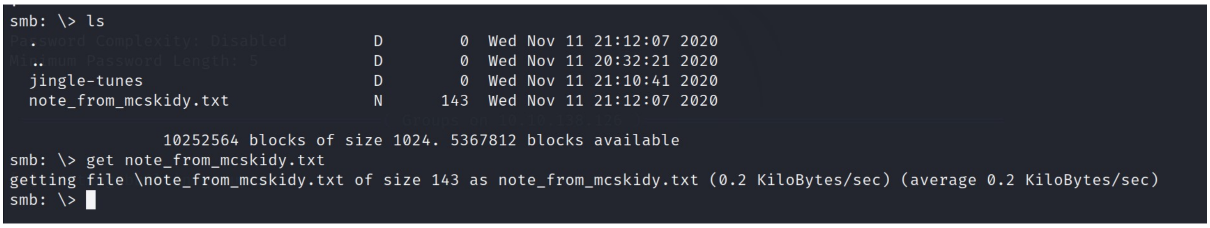
Q4.



```
┌──(1211101401㉿kali)-[~]
└─$ sudo smbclient //10.10.138.126/tbfc-santa
[sudo] password for 1211101401:
Sorry, try again.
[sudo] password for 1211101401:
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> help
```

Try to login to every share in the smbclient. The share that does not require a password is the one that we can access.

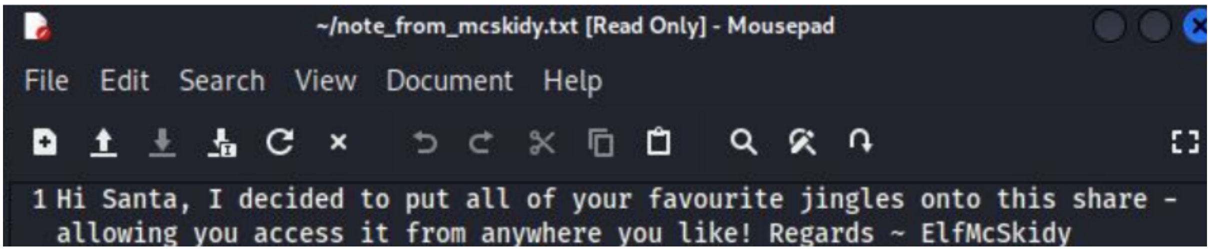
Q5.



```
smb: \> ls
  .                                   D        0  Wed Nov 11 21:12:07 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. 5367812 blocks available
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: \> 
```

From the share we can access. We can see a .txt file which is left by mcskidy. Download the file using get and read it.


~/note_from_mcskidy.txt [Read Only] - Mousepad
File Edit Search View Document Help

```
Hi Santa, I decided to put all of your favourite jingles onto this share -
allowing you access it from anywhere you like! Regards ~ ElfMcSkidy
```

The content shows where mcskidy save all the jungle tones.