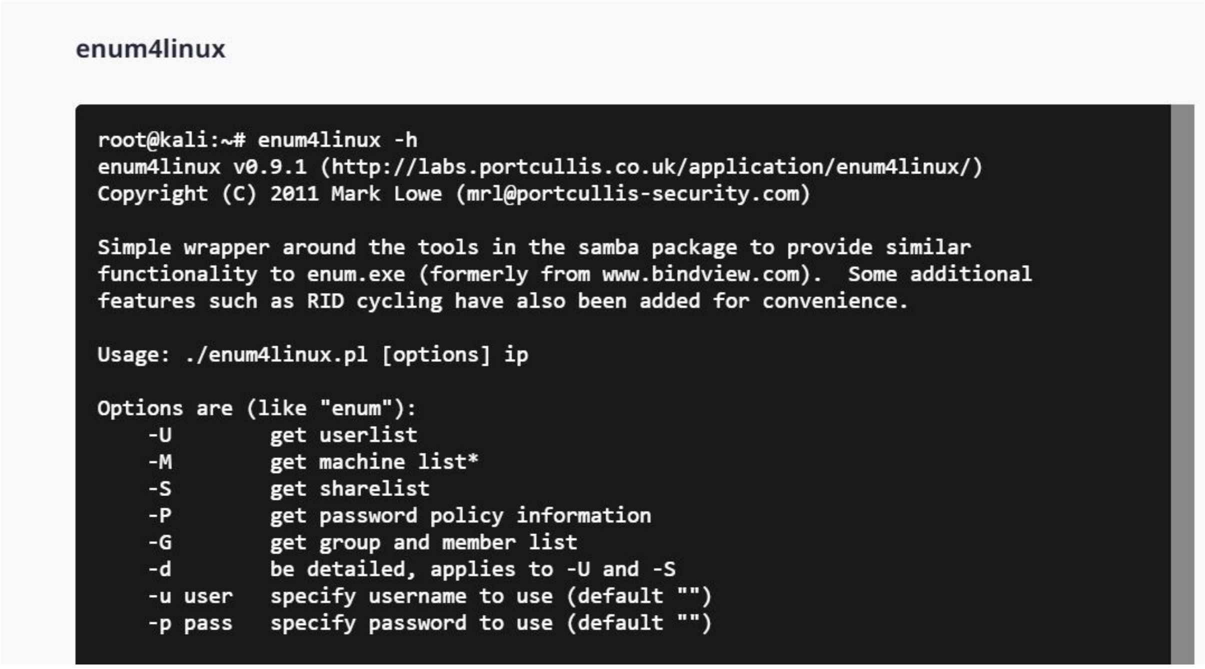
Day 10 -[Networking] Don't be sElfish!

Tool used: kali Linux, Firefox, enum4linux, smbcilent

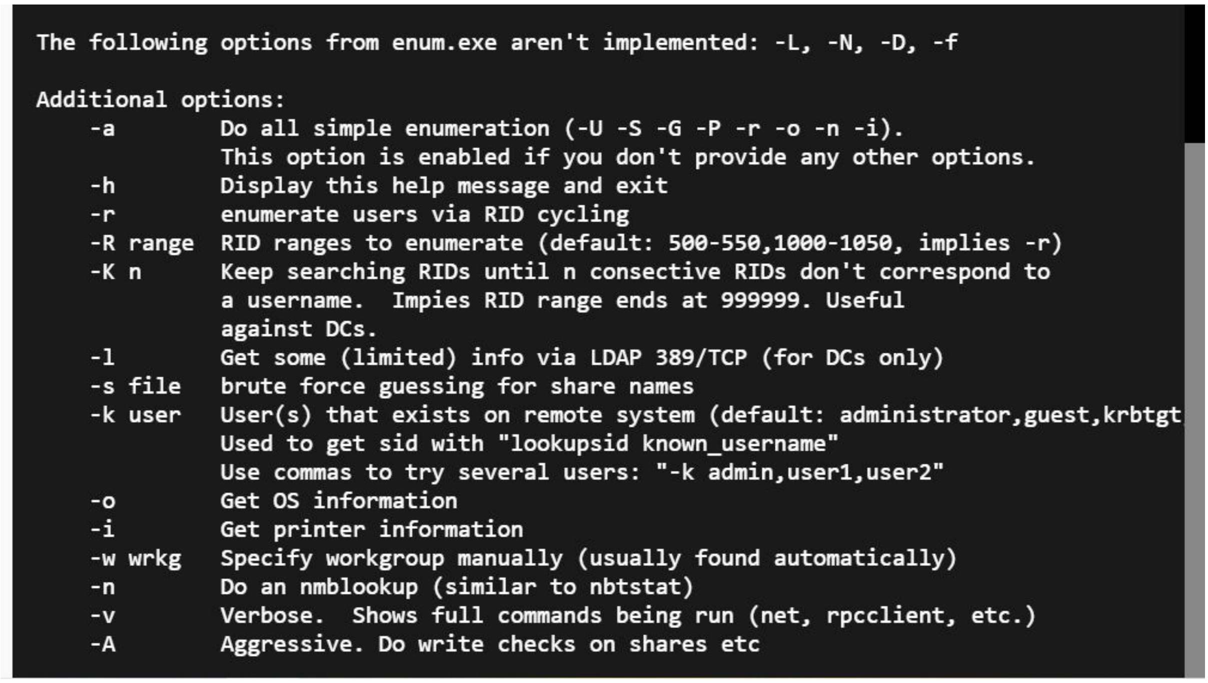
Solution/Walkthrough:

Q1



enum4linux

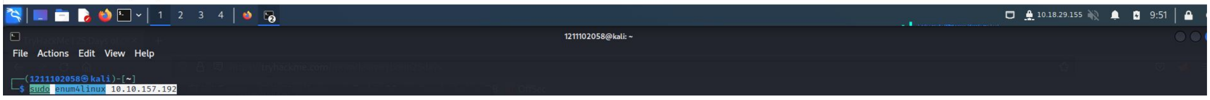
```
root@kali:~# enum4linux -h
enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

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 "")
```



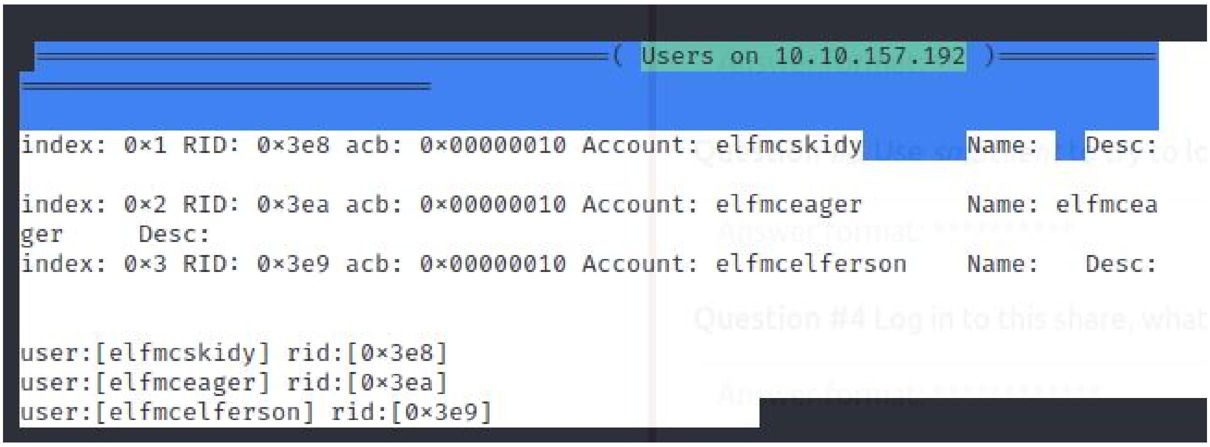
```
The following options from enum.exe aren't implemented: -L, -N, -D, -f

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
```

Research and study from here.

Q2 & Q3

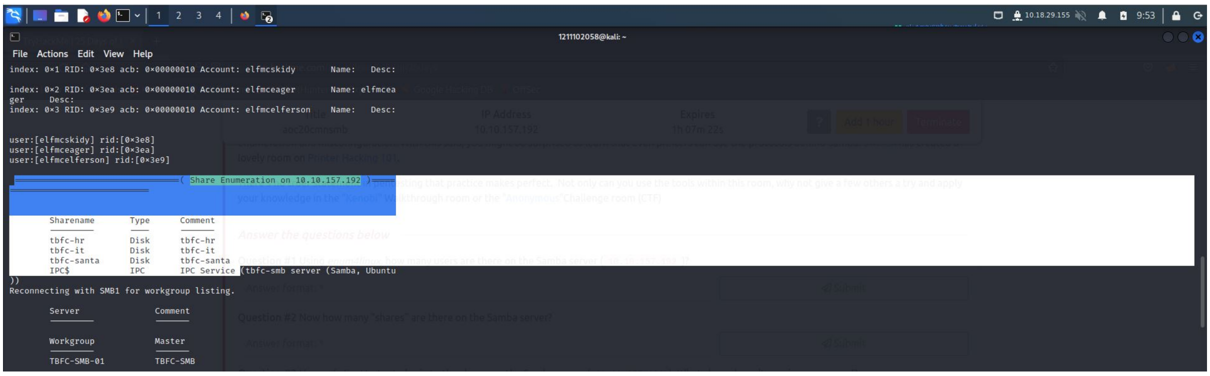


```
┌──(1211102058㉿kali)-[~]
└─$ sudo enum4linux 10.10.157.192
```



```
==========================( Users on 10.10.157.192 )==========================

index: 0×1 RID: 0×3e8 acb: 0×00000010 Account: elfmcskidy    Name:    Desc:

index: 0×2 RID: 0×3ea acb: 0×00000010 Account: elfmceager    Name: elfmcea
ger      Desc:
index: 0×3 RID: 0×3e9 acb: 0×00000010 Account: elfmcelferson    Name:    Desc:


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

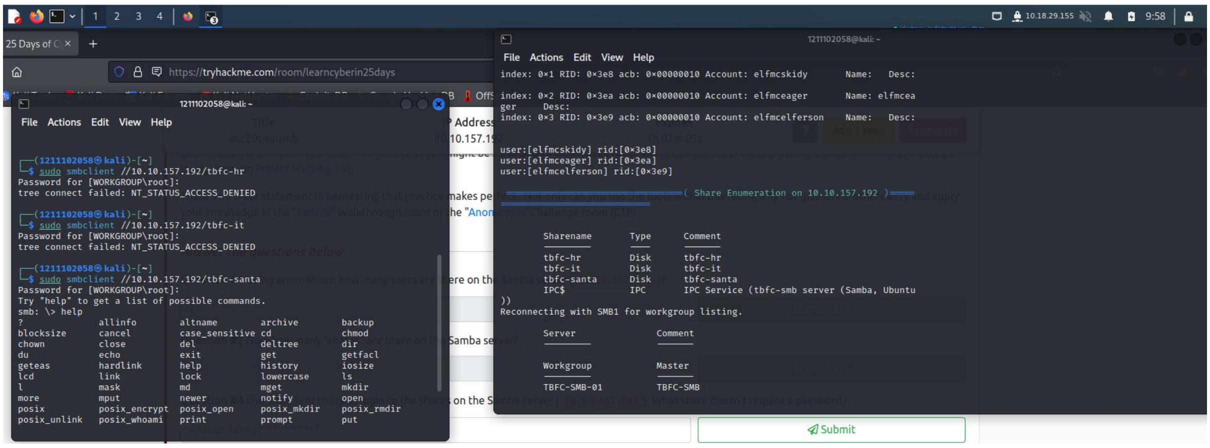
use enum4linux on target. When finished, the number of users is shown.



```
index: 0×1 RID: 0×3e8 acb: 0×00000010 Account: elfmcskidy    Name:   Desc:

index: 0×2 RID: 0×3ea acb: 0×00000010 Account: elfmceager    Name: elfmcea
ger      Desc:
index: 0×3 RID: 0×3e9 acb: 0×00000010 Account: elfmcelferson    Name:   Desc:


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

=========================( Share Enumeration on 10.10.157.192 )=====
=========================

        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
```

The amount of “shares” are shown also.

Q4

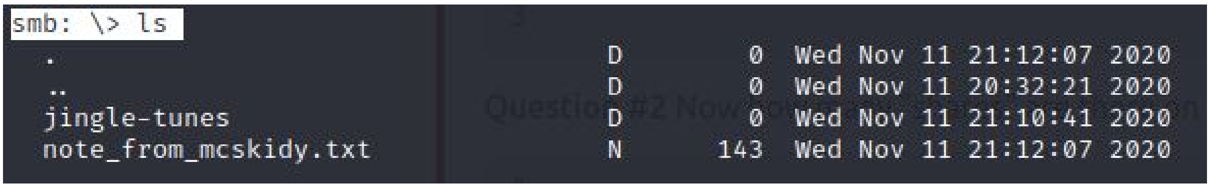


```
┌──(1211102058㉿kali)-[~]
└─$ sudo smbclient //10.10.157.192/tbfc-hr
Password for [WORKGROUP\root]:
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(1211102058㉿kali)-[~]
└─$ sudo smbclient //10.10.157.192/tbfc-it
Password for [WORKGROUP\root]:
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(1211102058㉿kali)-[~]
└─$ sudo smbclient //10.10.157.192/tbfc-santa
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
more           mput           newer          notify         open
posix          posix_encrypt  posix_open     posix_mkdir    posix_rmdir
posix_unlink   posix_whoami   print          prompt         put
```

```
index: 0×1 RID: 0×3e8 acb: 0×00000010 Account: elfmcskidy      Name:   Desc:

index: 0×2 RID: 0×3ea acb: 0×00000010 Account: elfmceager      Name: elfmcea
ger      Desc:
index: 0×3 RID: 0×3e9 acb: 0×00000010 Account: elfmcelferson   Name:   Desc:

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

=========================( Share Enumeration on 10.10.157.192 )=====
=========================

        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
```

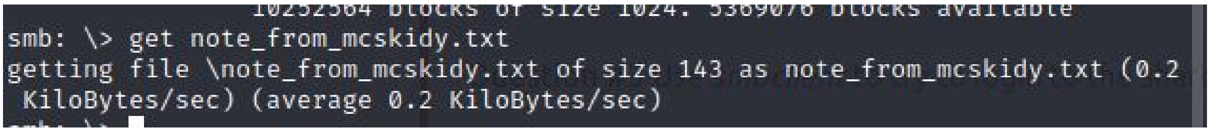
Use smbclient and try to log into the shares. The share that does not require a password is accessible

Q5



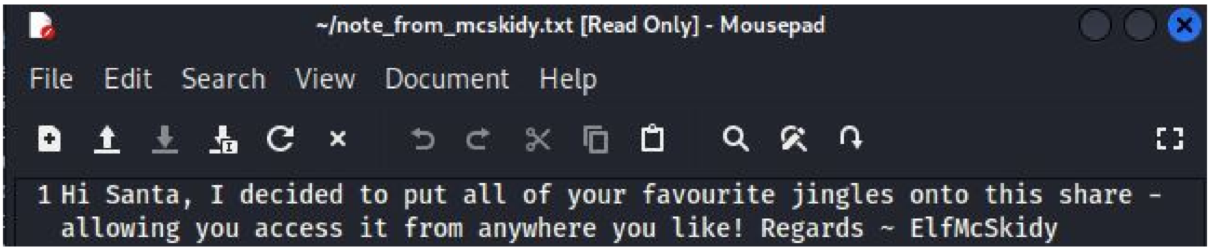
```
smb: \> ls
  .                                   D        0  Wed Nov 11 21:12:07 2020
  ..                                  D        0  Wed Nov 11 20:32:21 2020
  jingle-tunes                        D        0  Wed Nov 11 21:10:41 2020
  note_from_mcskidy.txt               N      143  Wed Nov 11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

in the share, a note from mcskidy is found.



```
                10252364 blocks of size 1024. 5369076 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)
```

Download the .txt file. Read the content.



```
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 the directory Elfmcskidy leaves for santa.