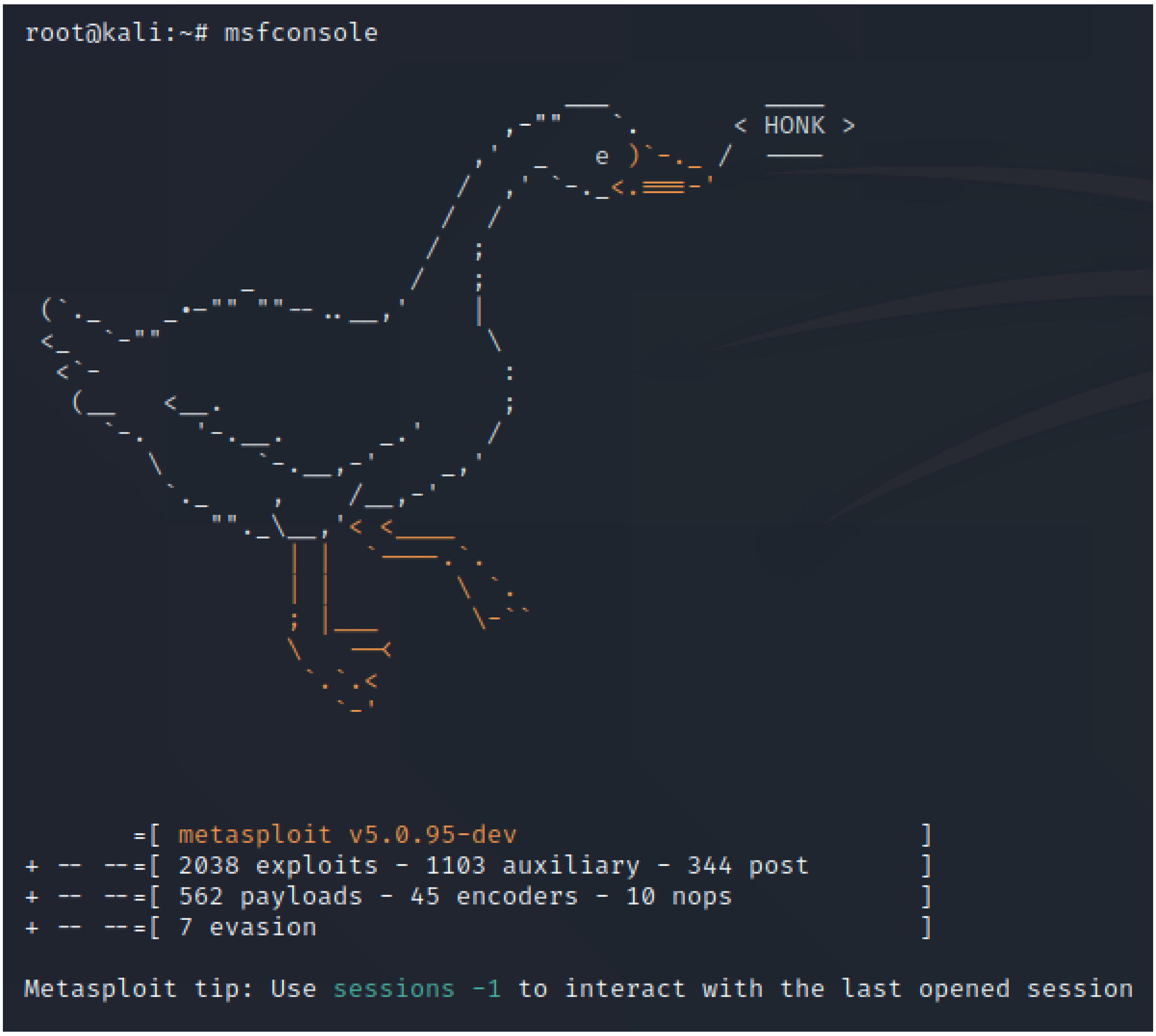
Enumerating SMB

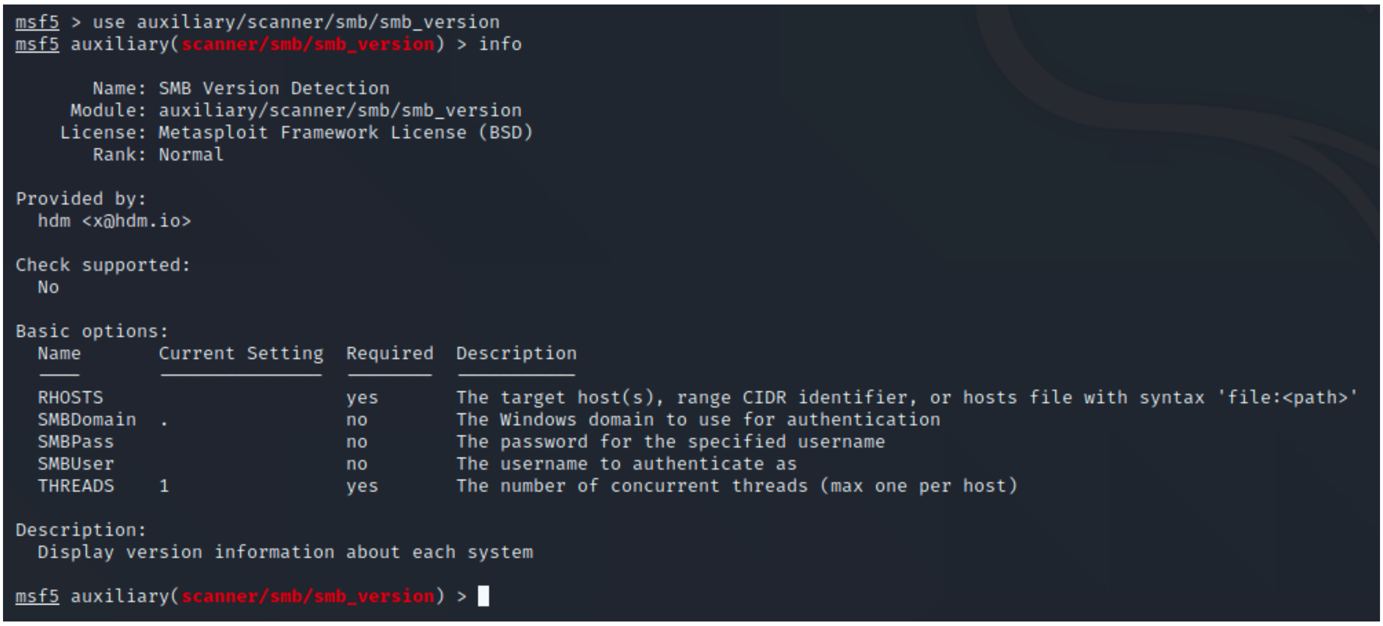
SMB is a file share service. In the Nmap scan we can see that the SMB service isn running on port 139. We will use Metasploit to enumerate the service on port 139. Open Metasploit using `msfconsole` command as shown below:



```
root@kali:~# msfconsole

                                              < HONK >

       =[ metasploit v5.0.95-dev                          ]
+ -- --=[ 2038 exploits - 1103 auxiliary - 344 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Use sessions -1 to interact with the last opened session
```

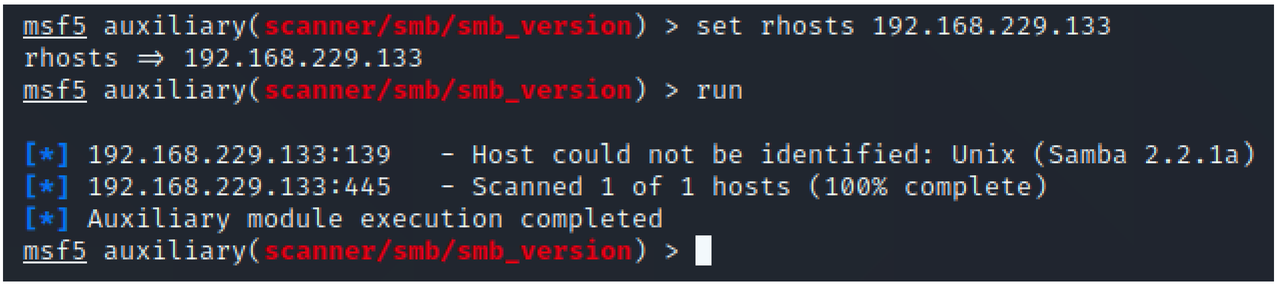
We will use the `Auxiliary` modules to perform the scanning and enumeration.

We want to find out the SMB version so we will use an auxiliary module to find that. To search for modules that work with SMB, use the `search smb` command to load all modules that work with SMB. We will use `auxiliary/scanner/smb/smb_version`. To load the module, use this command: `use auxiliary/scanner/smb/smb_version`. To view the details of the module, use the `info` command as shown below:



```
msf5 > use auxiliary/scanner/smb/smb_version
msf5 auxiliary(scanner/smb/smb_version) > info

       Name: SMB Version Detection
     Module: auxiliary/scanner/smb/smb_version
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  hdm <x@hdm.io>

Check supported:
  No

Basic options:
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  SMBDomain  .                no        The Windows domain to use for authentication
  SMBPass                     no        The password for the specified username
  SMBUser                     no        The username to authenticate as
  THREADS    1                yes       The number of concurrent threads (max one per host)

Description:
  Display version information about each system

msf5 auxiliary(scanner/smb/smb_version) > 
```

`RHOSTS` refers to the remote host or our target. So we will enter the IP address of our target by following this syntax: `set rhosts <IP_address>`. Enter `run` to run the scan as shown below:

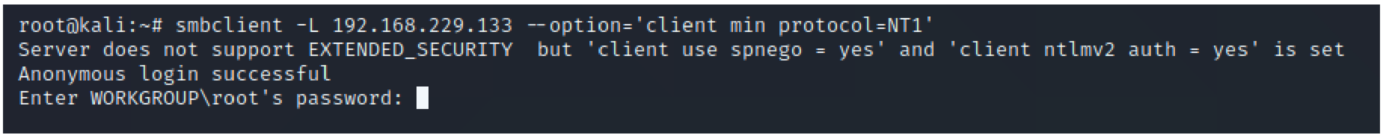


```
msf5 auxiliary(scanner/smb/smb_version) > set rhosts 192.168.229.133
rhosts => 192.168.229.133
msf5 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.229.133:139   - Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.229.133:445   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_version) > 
```

We can see that the target is running `Samba 2.2.1a`.

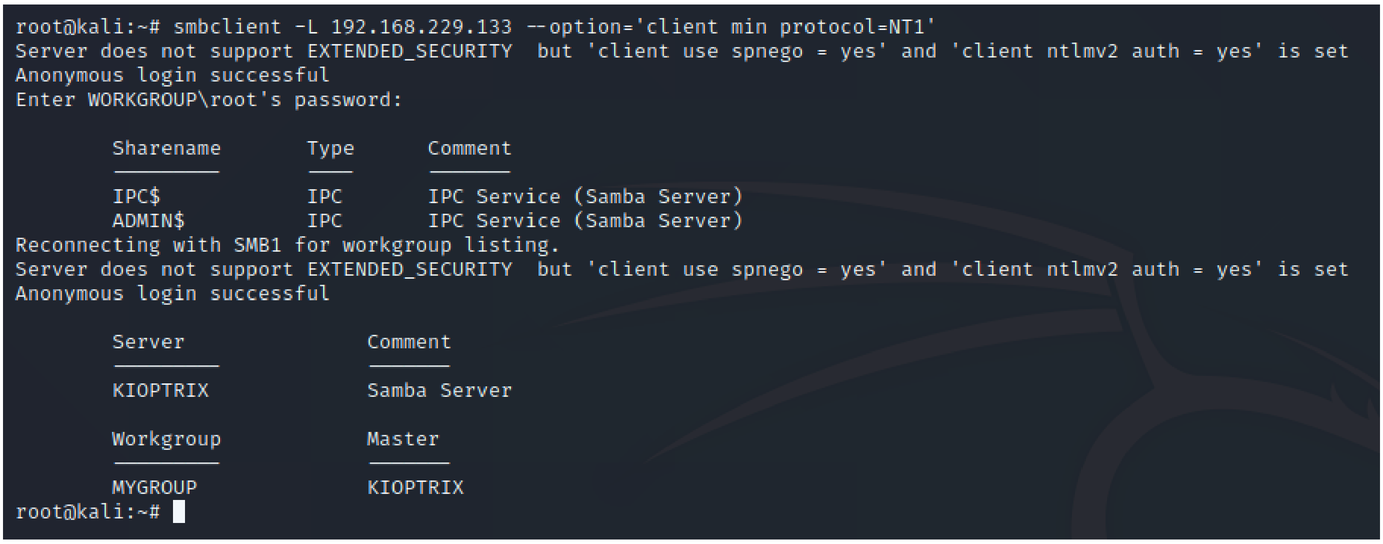
We will use another tool called `smbclient` to attempt connecting to the SMB (Smaba) file share. To run smbclient, use the `smbclient -L \\\\<IP_address>\\` or `smbclient -L \\<IP_address>` command (This command does not work on the Kali 2020.x.x versions because the SMBv1 protocol has been disabled by default). The `-L` lists all the files.

TIP: To run this command in Kali 2020.x.x versions, use the following command `smbclient -L 192.168.229.133 --option='client min protocol=NT1'`. The results are shown below:



```
root@kali:~# smbclient -L 192.168.229.133 --option='client min protocol=NT1'
Server does not support EXTENDED_SECURITY  but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Enter WORKGROUP\root's password: 
```

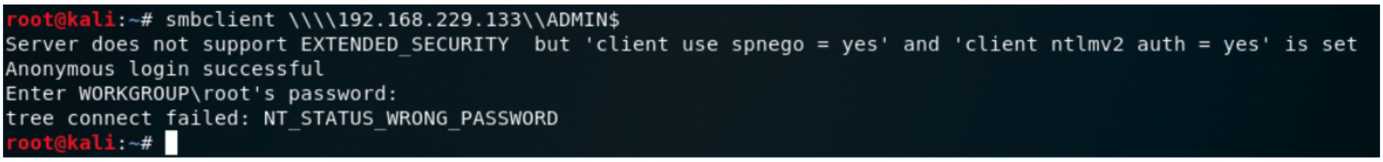
Here we can see that the server allows anonymous logins. Since we don't know the root password, simply hit the `Enter` key and we'll get a list of the shared directories as shown below:



```
root@kali:~# smbclient -L 192.168.229.133 --option='client min protocol=NT1'
Server does not support EXTENDED_SECURITY  but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Enter WORKGROUP\root's password:

        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       IPC Service (Samba Server)
        ADMIN$          IPC       IPC Service (Samba Server)
Reconnecting with SMB1 for workgroup listing.
Server does not support EXTENDED_SECURITY  but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful

        Server               Comment
        ---------            -------
        KIOPTRIX             Samba Server

        Workgroup            Master
        ---------            -------
        MYGROUP              KIOPTRIX
root@kali:~# 
```

Due to some technical issues with Kali 2020, I'll be switching to Kali 2018

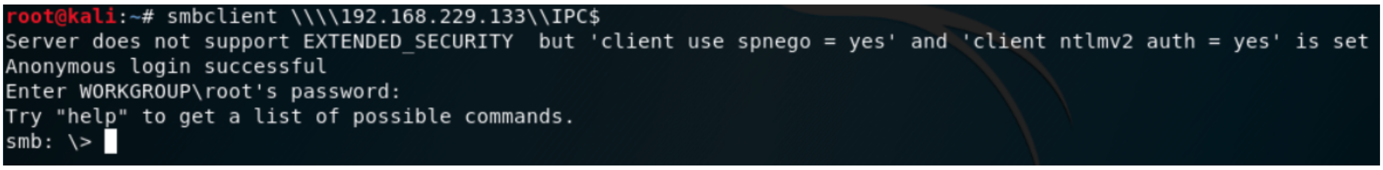
Let's try connecting to the `ADMIN$` share file using the `smbclient \\\\<IP_address>\\ADMIN$` command as shown below:



```
root@kali:~# smbclient \\\\192.168.229.133\\ADMIN$
Server does not support EXTENDED_SECURITY  but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_WRONG_PASSWORD
root@kali:~# 
```

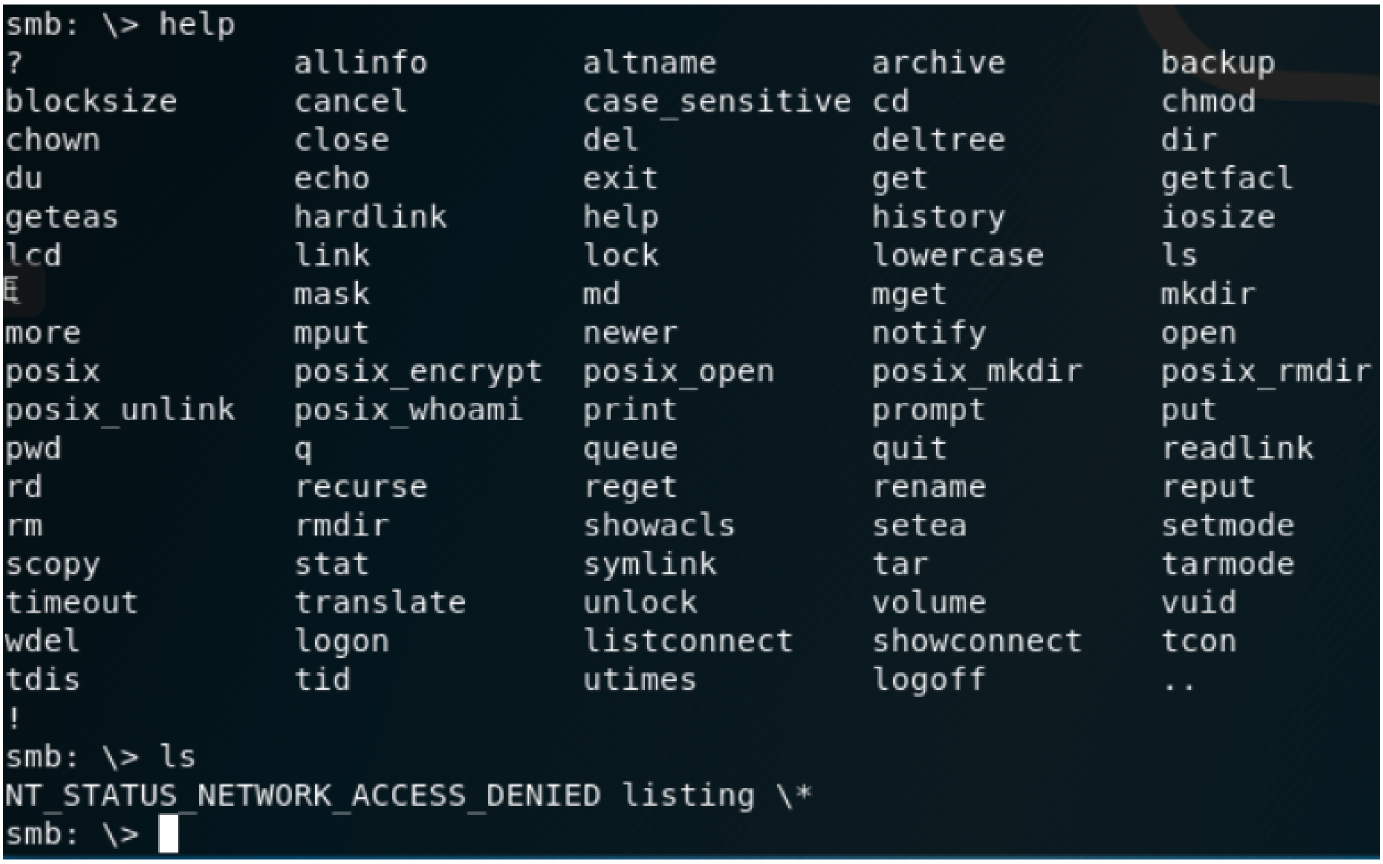
Since we don't know the root password, simply hit the `Enter` key and we'll get an error message saying, `NT_STATUS_WRONG_PSSWORD`.

Let's try connecting to the `IPC$` share file using the `smbclient \\\\<IP_address>\\IPC$` command as shown below:



```
root@kali:~# smbclient \\\\192.168.229.133\\IPC$
Server does not support EXTENDED_SECURITY  but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> 
```

As you can see we were able to login anonymously and we can access the files in the `IPC$` shared folder. It is quite similar to a linux shell. We can use commands such as `help` to list all the commands that can be used. We can also use the `ls` command to list files in the folder as shown below:



```
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
pwd            q              queue          quit           readlink
rd             recurse        reget          rename         reput
rm             rmdir          showacls       setea          setmode
scopy          stat           symlink        tar            tarmode
timeout        translate      unlock         volume         vuid
wdel           logon          listconnect    showconnect    tcon
tdis           tid            utimes         logoff         ..
!
smb: \> ls
NT_STATUS_NETWORK_ACCESS_DENIED listing \*
smb: \> 
```

We can see the listed commands. However, when we used the `ls` command, we got an error: `NT_STATUS_NETWORK_ACCESS_DENIED listing \*`. This is a "dead end". In some cases, where the SMB service is not secured, we can access the files. To exit, use the `exit` command.