SMB enumeration is a very important skill for any pentester. Before learning how to enumerate SMB , we must first learn what SMB is . So let's get started.

SMB stands for server message block. It's a protocol for sharing resources like files, printers, in general any resource which should be retreivable or made available by the server. It primarily runs on port 445 or port 139 depending on the server . It is actually natively available in windows, so windows users don't need to configure anything extra as such besides basic setting up. In linux however ,it is a little different. To make it work for linux, you need to install a samba server because linux natively does not use SMB protocol.

Obviously some sort of authentication will be in place like a username and password and only certain resources made shareable. So it's not like everyone can access everything, a strong authentication.

So lets talk about the security flaws in this. The first obvious flaw is using default credentials or easily guessable and sometimes even no authentication for access of important resources of the server. Admins should make sure to use strong passwords for users who want to access resources using SMB.

The second flaw is the samba server. Samba servers are notorious for being tremendously insecure . Don't believe me? Just type in google "samba server exploit" and you'll get a list of publicly available exploits quite easily. Hell, even metasploit houses so many auxillary scanners and exploits for samba server. So make sure the Samba server is patched.

Ok ,so how do we enumerate when we find that in our nmap scan port 445 is open with samba server on. I only said samba server because linux is predominantly used by enterprises , around 75% to be precise. That being said, the process of enumeration for SMB is the same for both linux and windows with the exception that in linux , you have to check the samba version as well and check if it is vulnerable or not.

So what I like to do the first thing is use Nmap scripting engine or commonly known as NSE. It is a very powerful feature of Nmap and would probably require a separate article to demonstrate it's usefulness . So to enumerate version, type

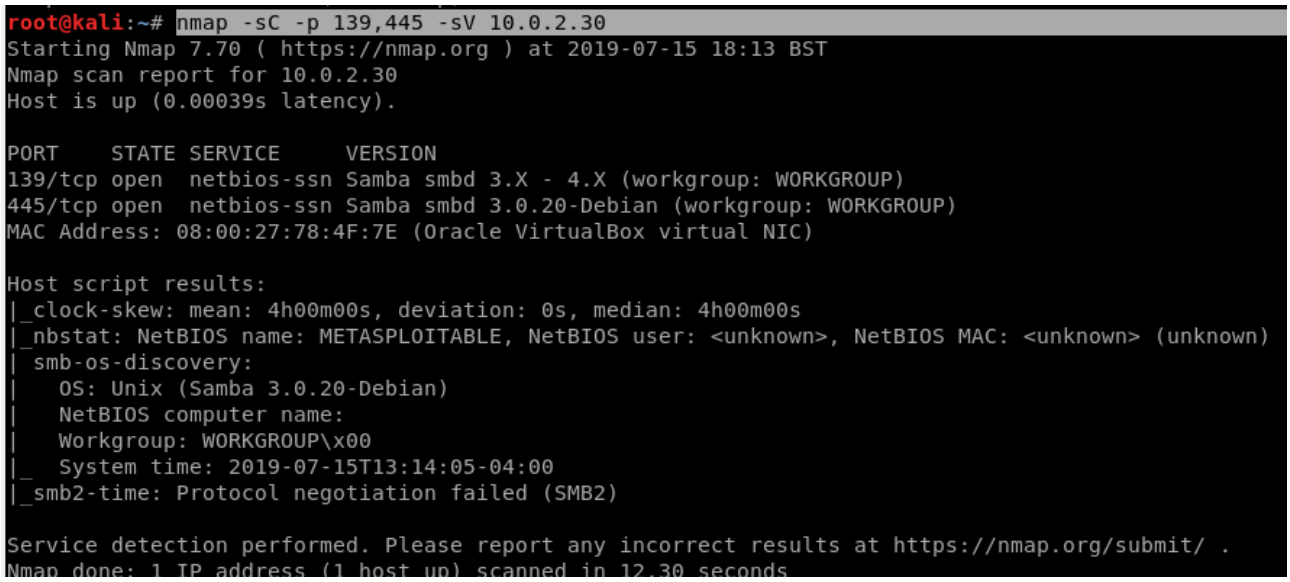
nmap -p445 — script smb-protocols <target ip>

nmap -p139 — script smb-protocols <target ip>

Note we are trying to enumerate both port numbers . We could also try to enumerate smb using default scripts of the NSE by typing:

nmap -sC -p 139,445 -sV 10.0.2.30

These are the results when I ran it against a metasploitable



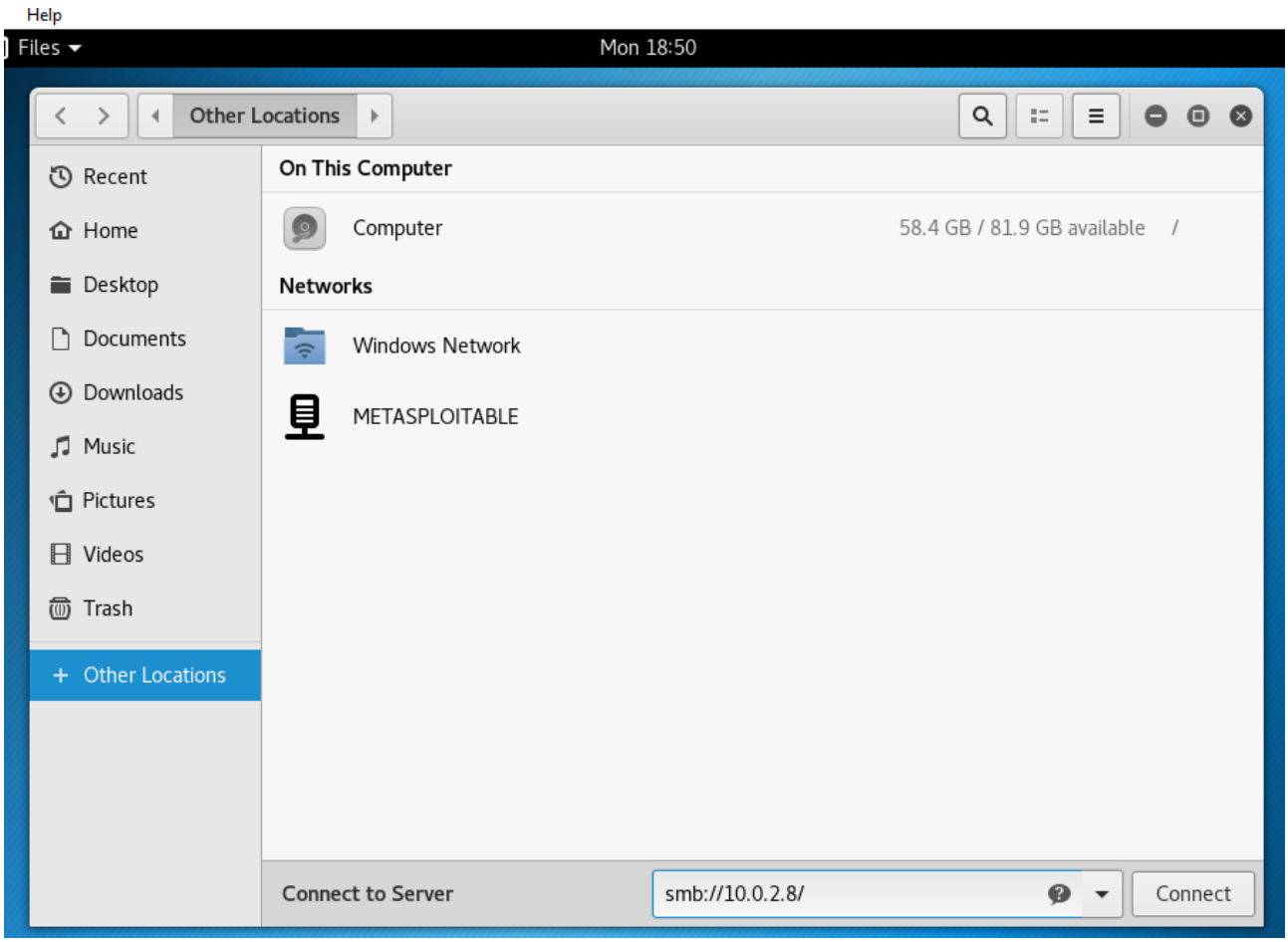
Default scriptscan for nmap

Nice ! we found out the version of Samba running in the server. Now just go to google and search whether the given version is vulnerable or not.

That's great , but what if the samba server was patched, or didn't have a samba server to begin with?

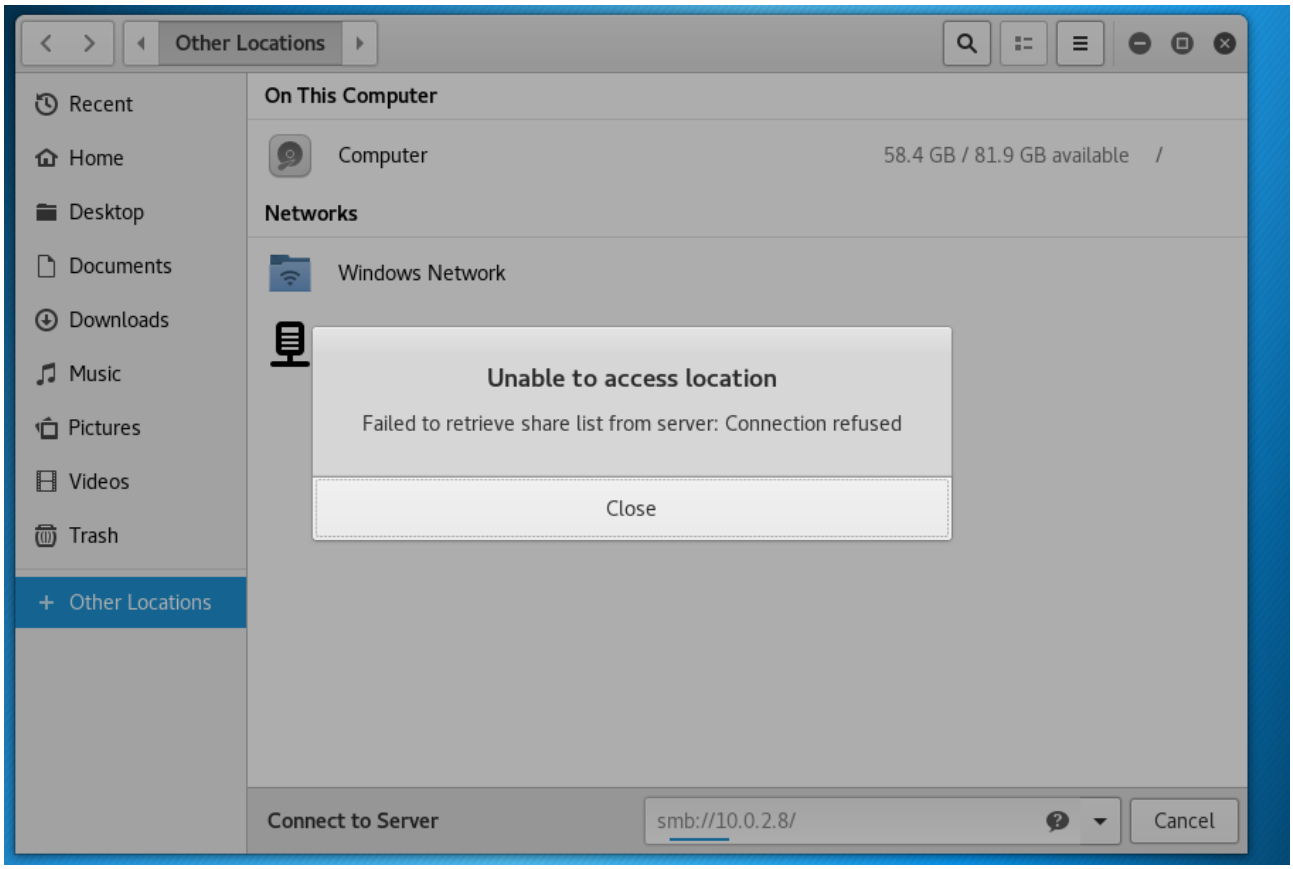
There are many ways to enumerate the service itself. The quickest way is to use a tool called enum4linux. However I have noticed that sometimes the output is not very pleasing. Other tools which I feel better are smbclient and smbmap. I will also show how to manually access smb folder , but sometimes that fails. So primarily , you should be well versed with smbclient and smbmap , they are much more reliable.

As promised , let us first access it manually. To manually access the smb shares, go to folders and type this:



You can connect like this also

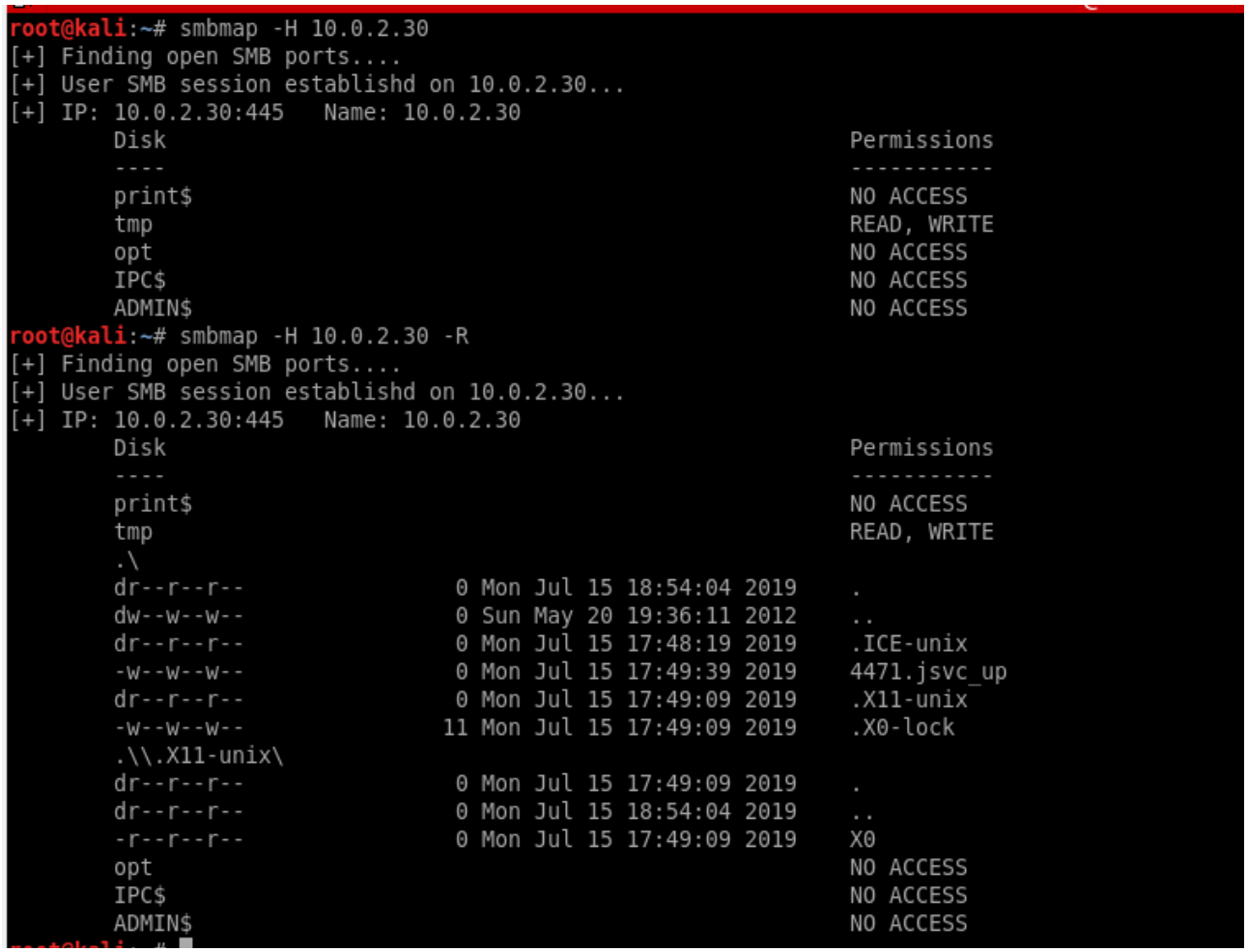
Unfortunately, it fails



In few machines this fails

I am actually not sure why.It does work on a lot of machines, not sure why it's not working here. Anyway , this kind of makes my point why smbclient and smbmap are better.

Let's first use smbmap . To use it's basic version , type



The -H argument is for hostname and the -R is recursive switch, meaning it will go through each directory and list out the files. Although I must tell you that it's working now only because anonymous login is allowed, i.e. in a real life , you'd probably need a username and password.

Now you can actually retrieve the files using smbmap as well, I'll leave that as an exercise. But what if we wanted a full fledged command prompt like a ftp prompt? That's very much possible with smbclient. Lets try to do that.

```
root@kali:~# smbclient -N -L \\\\10.0.2.30
WARNING: The "syslog" option is deprecated
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
        ADMIN$          IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

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

        Workgroup            Master
        ---------            -------
        WORKGROUP            METASPLOITABLE
root@kali:~#
```

A smbclient connection is made to enumerate information

This command tries to establish an anonymous login with metasploitable so that we can see what all files we can access. You can see that it was successful and we have access to shares namely opt and tmp.

Now how do I get a smbshell in either of the disks? Simple, just type like this

```
root@kali:~# smbclient \\\\10.0.2.30\\tmp
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Jul 15 19:33:03 2019
  ..                                 DR        0  Sun May 20 19:36:12 2012
  .ICE-unix                          DH        0  Mon Jul 15 17:48:20 2019
  4471.jsvc_up                        R        0  Mon Jul 15 17:49:40 2019
  .X11-unix                          DH        0  Mon Jul 15 17:49:10 2019
  .X0-lock                           HR       11  Mon Jul 15 17:49:10 2019

                7282168 blocks of size 1024. 5418716 blocks available
smb: \>
```

As promised a smb interactive shell

Yay , we got a shell in tmp disk. Now we can download or upload files into the share. As you can see , this is actually useful for both system administrators and pentesters. That's why, the best way to start your ethical hacking career is to first be a system or network admin. It becomes easier down the lane if you start from there.

Hope it helped out some of the folks! Also , smb knowledge is must for enumerating oscp level machines. Thanks y'all