Hack The Box - Lame	
Sistema Operativo:	**Linux**
Dificultad:	**Easy**
Release:	**14/03/2017**

Skills Required

- Basic knowledge of Linux
- Enumerating ports and services

Skills Learned

- Identifying vulnerable services
- Exploiting Samba

En este reto planteado por la plataforma Hack The Box, se realizó una exploración exhaustiva de un servicio Samba expuesto, utilizando herramientas como smbclient para navegar los recursos compartidos. Aunque inicialmente no se identificó información de alto valor en los directorios remotos, se detectó una instalación vulnerable de Samba en su versión 3.0.2. Esta versión presenta la debilidad crítica CVE-2007-2447, la cual permite la ejecución remota de comandos a través de la mala sanitización de entradas en funciones MS-RPC, abriendo la puerta a una escalada de privilegios.

Este proceso demuestra habilidades de reconocimiento de servicios, explotación de vulnerabilidades conocidas, escalado de privilegios y post-explotación orientada a recolección de credenciales.

Enumeración

La dirección IP de la máquina víctima es 10.129.29.209. Por tanto, envié 5 trazas ICMP para verificar que existe conectividad entre las dos máquinas.

```
┌──(administrador㉿kali)-[~/HTB/permx]
└─$ ping -c 5 10.129.29.209 -R
PING 10.129.29.209 (10.129.29.209) 56(124) bytes of data.
64 bytes from 10.129.29.209: icmp_seq=1 ttl=63 time=51.3 ms
RR:     10.10.16.2
        10.129.0.1
        10.129.29.209
        10.129.29.209
        10.10.16.1
        10.10.16.2

64 bytes from 10.129.29.209: icmp_seq=2 ttl=63 time=52.7 ms     (same route)
64 bytes from 10.129.29.209: icmp_seq=3 ttl=63 time=51.3 ms     (same route)
64 bytes from 10.129.29.209: icmp_seq=4 ttl=63 time=54.9 ms     (same route)
64 bytes from 10.129.29.209: icmp_seq=5 ttl=63 time=75.4 ms     (same route)

--- 10.129.29.209 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4278ms
rtt min/avg/max/mdev = 51.262/57.108/75.444/9.260 ms
```

Una vez que identificada la dirección IP de la máquina objetivo, utilicé el comando **nmap -p- -sS -sC -sV --min-rate 5000 -vvv -n -Pn 10.129.29.209 -oN scanner_lame** para descubrir los puertos abiertos y sus versiones:

- **(-p-)**: realiza un escaneo de todos los puertos abiertos.
- **(-sS)**: utilizado para realizar un escaneo TCP SYN, siendo este tipo de escaneo el más común y rápido, además de ser relativamente sigiloso ya que no llega a completar las conexiones TCP. Habitualmente se conoce esta técnica como sondeo de medio abierto (half open). Este sondeo consiste en enviar un paquete SYN, si recibe un paquete SYN/ACK indica que el puerto está abierto, en caso contrario, si recibe un paquete RST (reset), indica que el puerto está cerrado y si no recibe respuesta, se marca como filtrado.
- **(-sC)**: utiliza los scripts por defecto para descubrir información adicional y posibles vulnerabilidades. Esta opción es equivalente a --script=default. Es necesario tener en cuenta que algunos de estos scripts se consideran intrusivos ya que podría ser detectado por sistemas de detección de intrusiones, por lo que no se deben ejecutar en una red sin permiso.
- **(-sV)**: Activa la detección de versiones. Esto es muy útil para identificar posibles vectores de ataque si la versión de algún servicio disponible es vulnerable.
- **(--min-rate 5000)**: ajusta la velocidad de envío a 5000 paquetes por segundo.
- (**-Pn**): asume que la máquina a analizar está activa y omite la fase de descubrimiento de hosts.

```
┌──(administrador㉿kali)-[~/HTB/lame]
└─$ cat nmap/scanner_lame
# Nmap 7.95 scan initiated Thu Apr  3 02:00:28 2025 as: /usr/lib/nmap/nmap -p- -sS -sC -sV --min-rate 5000 -vvv -n -Pn -oN nmap/scanner_lame 10.129.29.209
Nmap scan report for 10.129.29.209
Host is up, received user-set (0.056s latency).
Scanned at 2025-04-03 02:00:29 CEST for 78s
Not shown: 65530 filtered tcp ports (no-response)
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 10.10.16.2
|      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 AAAAB3NzaC1kc3MAAACBALz4hscBa2Srq4nlW960qV8xmBG0JC+jI7fWxmSMETIJH4tKr/xUTwsTYEYnaZLzcOiy21D3ZvOwYb6AA3765JdgCd2Tgand7F0YD5UtXG7b7fbz99chReivL0SIWEG/E96Ai+pqYMP2
AIBKCpnNXzi1TyP+QJIFa3MOaLqCVWIOWe/AR1XrzpBO3/dtXhTJXCeYisKqcdwdtyInBOUCOyrIjgNuA2QW217nQ6wKpbFh+5AQmBHl3bAC6oAlX3Pte+Y4dp0lzfWHwZ/jzHwtuaDQaok7u1f971lEazeJLqfiWrAzoklqSWy
/CQamGgQLtYy5S0ueoks81MoKdOMNhKVwqdr80nvCBdNKjIEd3gH6oBk/YRnjzxlEAYBsvCmM4a0jmhz0oNiRWlc/F+bkUeFKrBx/D2fdfZmhrOg==
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFWBOZvO3WTEjP4TUdjeWkIVNdTq6kboEDiteOfc65Tll7sRvQBwqAhQieevyIk8TS5eMDkODakSlSXvLDcmcdYfxeIF0ZSuT+nkRhij7XSSA/Oc5QSk3s3/SInfb78
jYucg87JjLeC66I7+dlEYX6zT8l1XYwa/L1vZJqSJ1SGVu8kRPikHv/cNSvKi4j+QDYyZ2E5497WO7+Ed46/8P42LNGoOV8OcX/ro6pAcbEPU0UEfkJqq1ZYXbhvwIJ9gFMb6wfe5cnQew==
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 3.0.20-Debian (workgroup: WORKGROUP)
3632/tcp open  distccd     syn-ack ttl 63 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-security-mode: Couldn't establish a SMBv2 connection.
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 49899/tcp): CLEAN (Timeout)
|   Check 2 (port 12606/tcp): CLEAN (Timeout)
|   Check 3 (port 60688/udp): CLEAN (Timeout)
|   Check 4 (port 2861/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| 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: 2025-04-02T20:01:49-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 2h00m40s, deviation: 2h49m45s, median: 37s
|_smb2-time: Protocol negotiation failed (SMB2)

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Apr  3 02:01:47 2025 -- 1 IP address (1 host up) scanned in 78.65 seconds
```

Análisis del puerto 21 (FTP)

El sistema objetivo expone el puerto 21/tcp, asociado al protocolo de transferencia de archivos (FTP), sobre el cual se ejecuta el servicio vsftpd en su versión 2.3.4. Esta revisión específica del software presenta una vulnerabilidad crítica catalogada como **CVE-2011-2523**, cuya explotación pone en grave compromiso la seguridad integral de la máquina afectada. La citada debilidad deriva de una alteración maliciosa en el código fuente —introducida durante su distribución entre el 30 de junio y el 3 de julio de 2011— mediante la inserción de una puerta trasera encubierta (backdoor), diseñada para activar una shell arbitraria en el puerto 6200/tcp. Al ser invocada, dicha funcionalidad permite la ejecución remota e irrestricta de comandos, lo que habilita a un atacante para adquirir pleno control sobre el sistema comprometido.

Desde una perspectiva técnica, el fallo subyacente se origina en una deficiente sanitización de caracteres especiales en las cadenas de entrada, derivando en una vulnerabilidad de inyección de comandos. Esta condición ha sido tipificada bajo el estándar CWE-78: *Improper Neutralization of Special Elements used in an OS Command*. Cabe subrayar que se trata de una vulnerabilidad explotable de forma remota, sin requerimiento de autenticación previa, lo que se traduce en una elevada criticidad reflejada en los vectores de puntuación CVSS: 9.8 en la versión 3.1 y 10.0 en CVSS 2.0, ambos indicadores de riesgo máximo.

```
┌──(administrador㉿kali)-[~/HTB/lame]
└─$ ftp 10.129.29.209 21
Connected to 10.129.29.209.
220 (vsFTPd 2.3.4)
Name (10.129.29.209:administrador): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||24553|).
150 Here comes the directory listing.
226 Directory send OK.
ftp>
```

Aunque el framework Metasploit dispone de un módulo específicamente desarrollado para la explotación de esta vulnerabilidad, la ejecución preliminar del exploit resultó en el establecimiento de una sesión sin que se produjeran los efectos previstos. Esta circunstancia obligó a reevaluar el enfoque ofensivo adoptado, replanteando la estrategia de intrusión y explorando vectores alternativos de acceso.

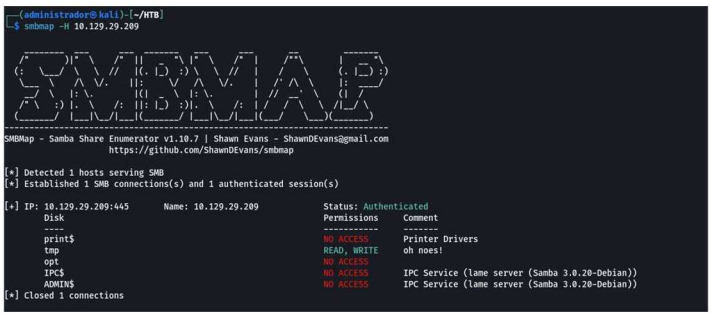
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 10.129.29.209:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.129.29.209:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Análisis del puerto 445 (SMB)

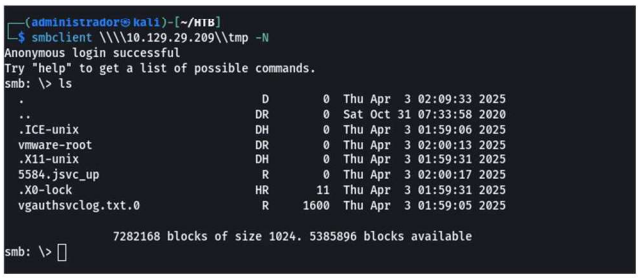
El protocolo Server Message Block (SMB) constituye un mecanismo de comunicación en red diseñado para facilitar el intercambio de archivos, impresoras y diversos recursos entre nodos interconectados, especialmente en entornos regidos por sistemas operativos de la familia Microsoft Windows. Esta tecnología opera en la capa de aplicación del modelo TCP/IP, habilitando a los clientes para establecer conexiones y acceder a elementos compartidos alojados en sistemas remotos. En el presente escenario, se detectó la exposición del puerto 445/tcp en el equipo objetivo, lo que permitió iniciar el proceso de enumeración de recursos compartidos accesibles mediante el usuario "guest", tradicionalmente asociado a sesiones no autenticadas.

Para llevar a cabo dicha enumeración de manera meticulosa, se empleó la herramienta smbmap, un utilitario desarrollado en Python que se ha consolidado como referente en el ámbito del reconocimiento pasivo sobre entornos SMB. Integrando funcionalidades de alto nivel para el análisis de permisos, jerarquías de directorios y configuraciones de acceso, smbmap permite visualizar con precisión los recursos publicados en la red, identificar desajustes en los privilegios y detectar posibles fallos de seguridad susceptibles de ser aprovechados para movimientos laterales.

A través de su capacidad de automatización y exhaustividad, esta herramienta enriquece significativamente la fase de reconocimiento, aportando una panorámica estructurada y detallada de las unidades compartidas, complementando así las capacidades más tradicionales ofrecidas por smbclient.

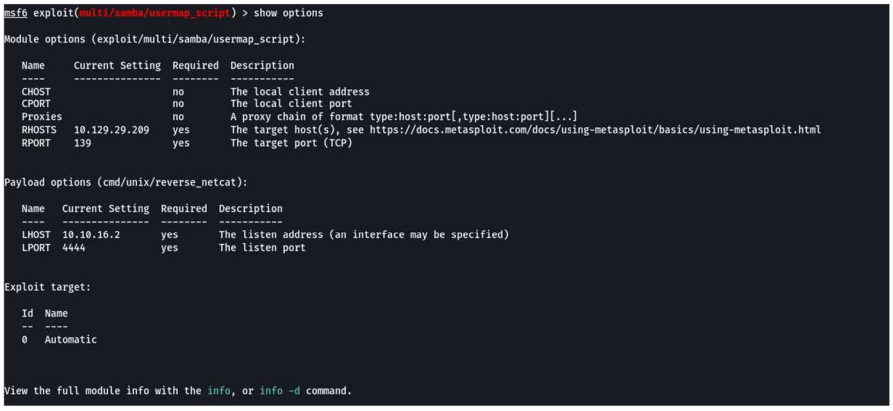


Para explorar dichos recursos, utilicé **smbclient**, una herramienta de la suite Samba que actúa de forma similar a un cliente FTP. Con smbclient se pueden listar directorios, navegar a través de las carpetas compartidas y transferir archivos, ofreciendo una interfaz de línea de comandos flexible y robusta para interactuar con los recursos SMB remotos. Sin embargo, tras listar el contenido de las carpetas, no se encontró información destacable que permitiera avanzar en la explotación o descubrir configuraciones vulnerables.



La versión de Samba que utiliza el sistema objetivo es la 3.0.2, la cual presenta una vulnerabilidad pública identificada como CVE-2007-2447. Esta vulnerabilidad afecta la funcionalidad MS-RPC de smbd en Samba, abarcando las versiones desde la 3.0.0 hasta la 3.0.25rc3. Específicamente, el defecto se origina en la inadecuada sanitización de las entradas que manejan metacaracteres del shell en la función SamrChangePassword cuando la opción username map script se encuentra habilitada en el archivo de configuración smb.conf. Esto permite que un atacante remoto inyecte comandos arbitrarios a través de dichos metacaracteres, comprometiendo la integridad y la seguridad del sistema.

Además, la vulnerabilidad se extiende a otros servicios MS-RPC relacionados con la administración de impresoras remotas y la gestión de ficheros compartidos, lo que posibilita que usuarios remotos autenticados puedan ejecutar comandos con privilegios elevados.



En consecuencia, si el exploit se configura correctamente, se logra obtener acceso privilegiado (root) al sistema, marcando exitosamente el final del reto en la plataforma Hack The Box.