Imagen que contiene nombre de la empresa

El contenido generado por IA puede ser incorrecto.

Maquina: LAME, SO: Linux

**IP: 10.10.10.3**

Lame es una maquina Linux publicada en Hack The Box, solía ser la primera maquina para los nuevos usuarios, solo requiere un exploit para obtener acceso como root.

Lo que veremos será una guía de paso a paso la solución para acceder como root y capturar las flags de la máquina, detallaremos algunos parámetros para explicarlos y que me ayudo a entender.

**Habilidades Requeridas**

* Conocimientos básicos de Linux
* Enumeración de puertos y servicios

**Habilidades Adquiridas**

* Identificación de servicios vulnerables
* Explotación de **Samba**

El primer paso que haremos será conectarnos a una VPN de HackTheBox, podremos descargar el archivo desde la propia plataforma, nos descargará un archivo. ovpnque tendremos que ejecutar utilizando Openvpn que se usa para iniciar y gestionar conexiones VPN, nos permite conectarnos de forma segura a una red privada a través de internet.

para poder conectarnos lo que haremos será escribir el siguiente comando.



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



Una vez ejecutado el comando, podremos ver que nuestra ip ha cambiado, si no estas seguro puedes ejecutar el comando ifconfig y veras como aparece una nueva interfaz de red:

tun0 → si es una conexión TUN (más común)

tap0 → si es una conexión TAP (menos común, capa 2)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Vamos a comprobar que tenemos conectividad entre nuestro equipo y la maquina atacada.

El parámetro -c 1 le dice a ping que solo envié 1 paquete ya que por defecto manda infinitos hasta cancelarlo.

Texto

El contenido generado por IA puede ser incorrecto.

Una cosa que podemos fijarnos si en algún caso no sabemos con que maquina nos encontramos es en el parámetro **TTL**

|  |  |
| --- | --- |
| Sistema operativo | TTL inicial común |
| Windows | 128 |
| Linux/Unix/macOS | 64 |
| Routers/Cisco | 255 |

Así que, si ves un TTL de 64, 128 o 255 en la respuesta, puedes adivinar desde qué sistema te están respondiendo

Texto

El contenido generado por IA puede ser incorrecto.Texto

El contenido generado por IA puede ser incorrecto.Texto

El contenido generado por IA puede ser incorrecto.

Texto

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto

El contenido generado por IA puede ser incorrecto.



Texto

El contenido generado por IA puede ser incorrecto.

No es la versión que tiene la puerta trasera

Texto

El contenido generado por IA puede ser incorrecto.

Texto

El contenido generado por IA puede ser incorrecto.Texto

El contenido generado por IA puede ser incorrecto.Texto

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto

El contenido generado por IA puede ser incorrecto.



Texto

El contenido generado por IA puede ser incorrecto.

Texto

El contenido generado por IA puede ser incorrecto.

Texto

El contenido generado por IA puede ser incorrecto.Texto

El contenido generado por IA puede ser incorrecto.Texto

El contenido generado por IA puede ser incorrecto.Interfaz de usuario gráfica, Texto

El contenido generado por IA puede ser incorrecto.