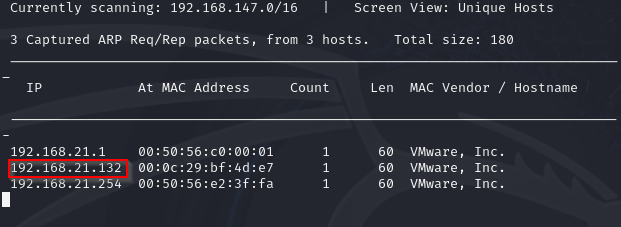
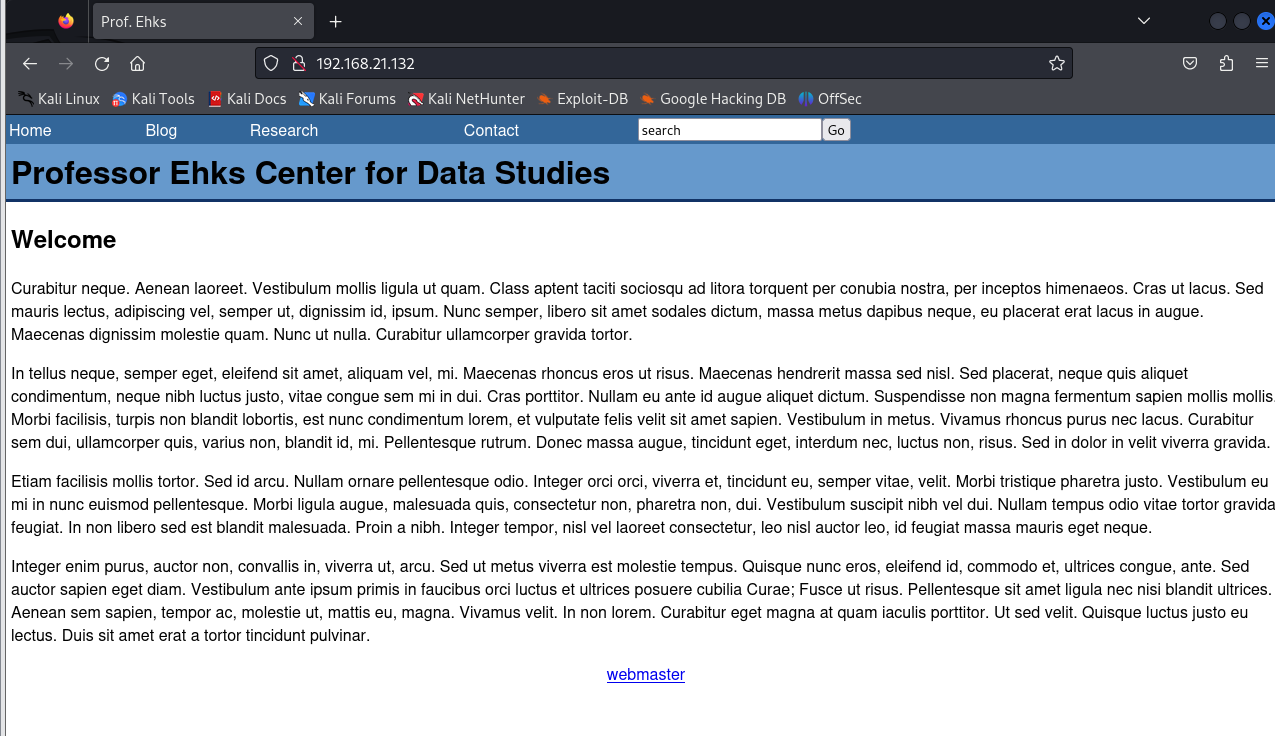
LAMPSecurity CTF4

Objetivo de entrar en la máquina objetivo: entrar siendo root.

Empecemos escaneando la red para encontrar nuestro objetivo.

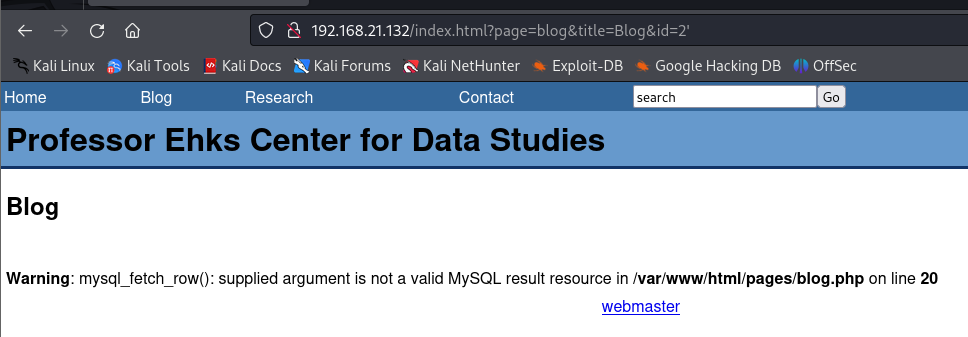


Miramos si podemos entrar por http (puerto 80) la IP 192.168.21.132

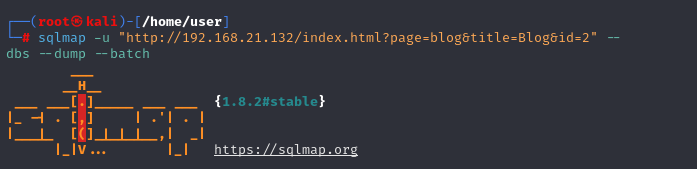


En la pestaña Blog y tras una enumeración más detallada, descubrimos que el parámetro URL "id" es propenso a un error de inyección SQL como se refleja en la siguiente imagen de captura de pantalla.

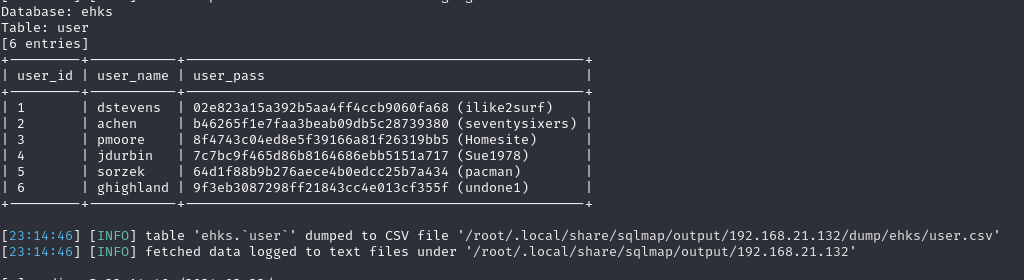
id=2’



Enumeremos las bases de datos con el comando SQLMAP para obtener más detalles.

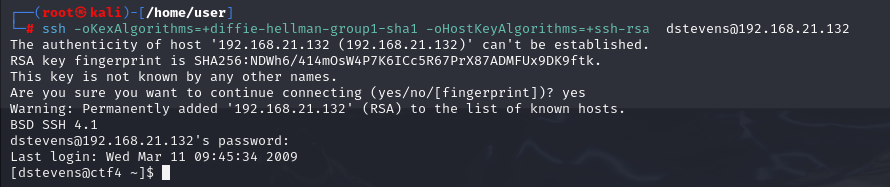


Nos sale una base de datos llamada ehks que contiene la tabla usuarios:



Como se ve en la captura de pantalla anterior, tenemos una lista de todos los usuarios y sus correspondientes credenciales para la tabla de usuarios de la base de datos ehks.

Vamos a intentar entrar con el usuario dstevens y su contraseña a través de SSH. E introducimos la contraseña.



Vemos que este usuario tiene privilegios de root introduciendo el comando sudo su:

