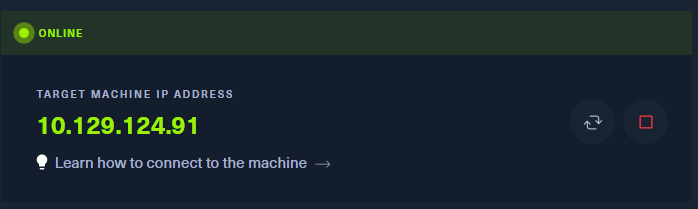
ANALISIS MAQUINA VIRTUAL APPOINTMENT

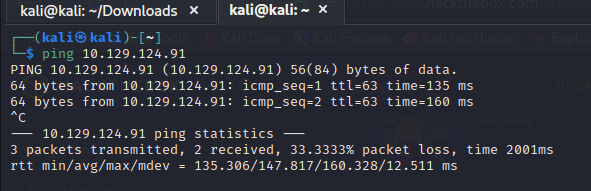
Dificultad: Facil

Etiqueta: SQL, SQLI

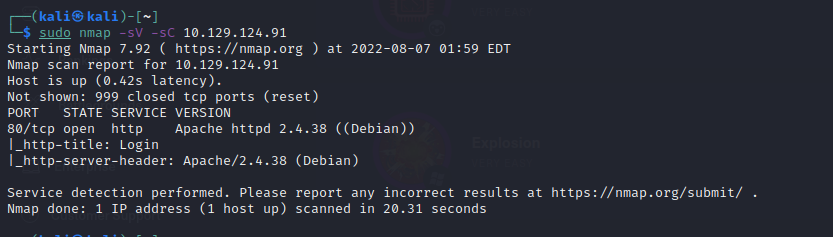
IP Maquina



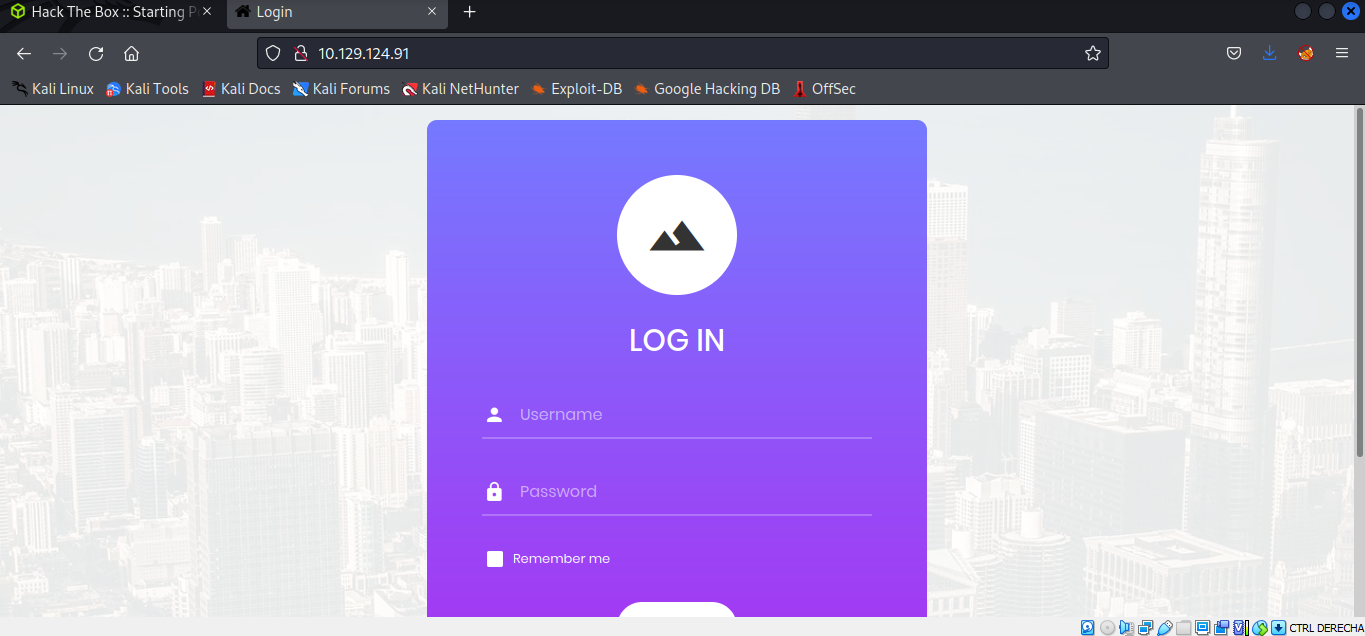
Realizamos ping para ver si tenemos conexión



Escaneamos para ver los puertos y servicios



Tenemos el puerto 80 abierto por lo cual significa que hay una pagina web detrás, por lo cual ingresaremos a ella colocando en el navegador la dirección de la maquina virtual



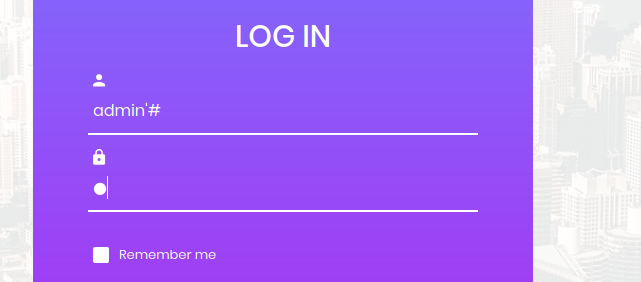
Podemos usar dirbuster o burpsuite pare recorrer los directorios y buscar información que nos pudieran dar las credenciales pero primeramente podemos probar si las entradas están sanitizadas para evitar inyección sql.

Normalmente siempre tenemos los usuarios admin por lo cual usaremos ese nombre de usuario y lo mezclaremos con otros caracteres para realizar una inyección sql la cual seria:

Username: admin’#

Password: #

Con el símbolo # estamos comentando todo el código por lo cual la consulta sql a la base de datos solo estaría comparando el usuario admin





Bandera: e3d0796d002a446c0e622226f42e9672