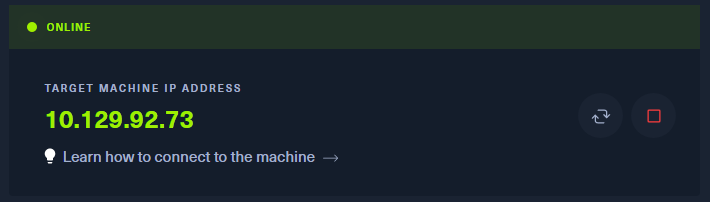
**ANALISIS MAQUINA VIRTUAL SEQUEL**

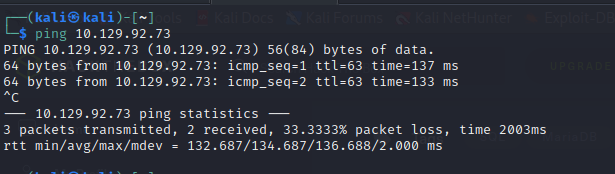
**Dificultad:** Fácil

**Etiqueta:** SQL, Contraseña Débil

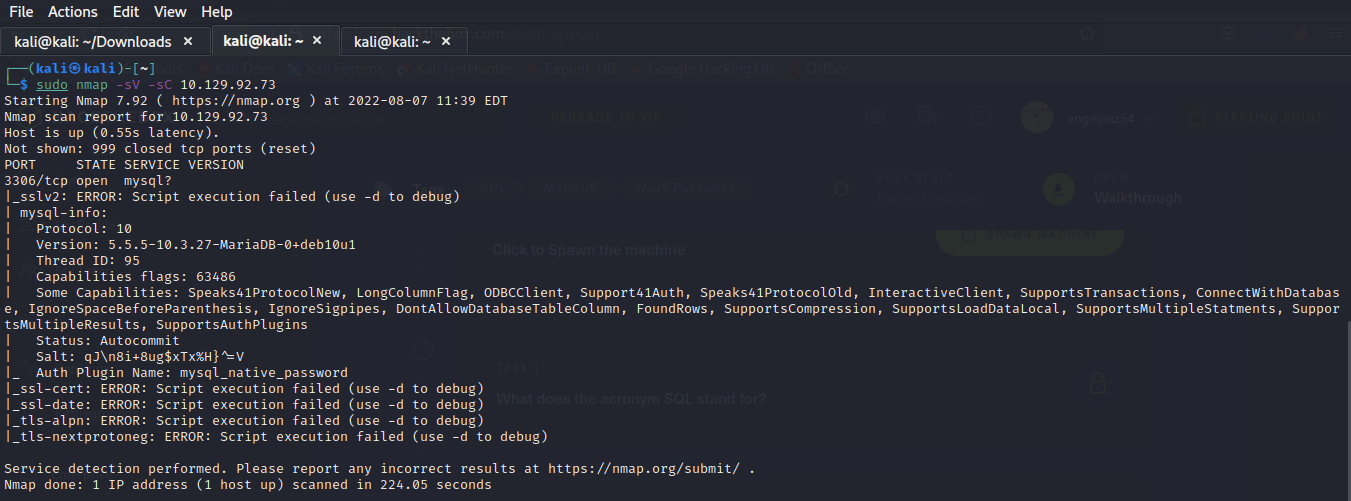
**IP Maquina**



Realizamos ping para ver si tenemos conexión



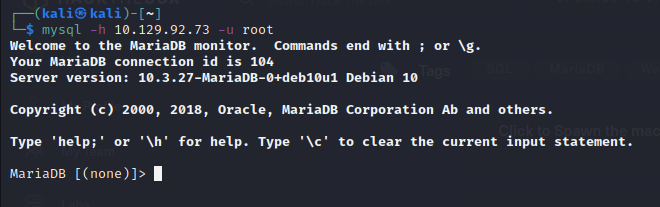
Escaneamos para ver los puertos y servicios



Solo encontramos un puerto abierto: 3306, que ejecuta un servicio llamado MySQL 5.5.5-10.3.27-MariaDB0+deb10u1 . MySQL es un servicio diseñado para la administración de bases de datos: crear, modificar y actualizar bases de datos, cambiar y agregar datos, y más.

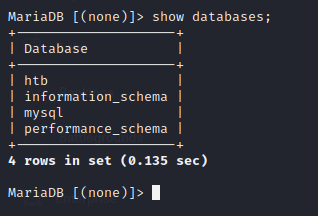
Tengamos en cuenta que los clientes de MySQL generalmente se autentican con el servicio con una combinación de nombre de usuario y contraseña.

Sin embargo, es esencial probar la autenticación sin contraseña, ya que podría haber una configuración incorrecta intencional en el servicio, lo que permitiría que el personal inicie sesión fácilmente en el servicio durante la etapa de implementación del proyecto para interactuar fácilmente con él antes de ponerlo a disposición de otros. colegas. En la situación actual, un intento inicial puede ser intentar iniciar sesión como usuario root , que naturalmente tiene el nivel más alto de privilegios en el sistema.

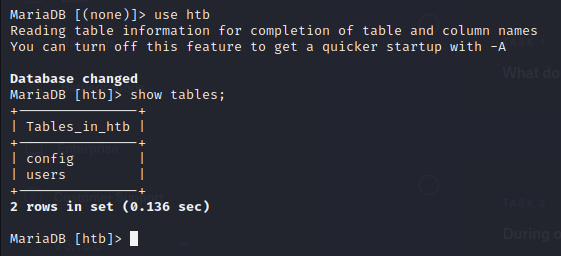


Y obtuvimos acceso en solo probar las malas configuraciones que dejan por default los administradores de las bases de datos, . Estamos colocados en un Shell del servicio MySQL desde donde podemos explorar las tablas y los datos que están disponibles para nosotros.

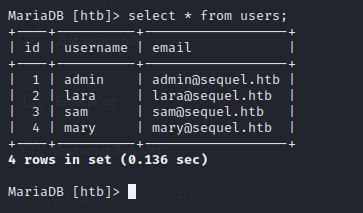
Podemos listas las bases de datos

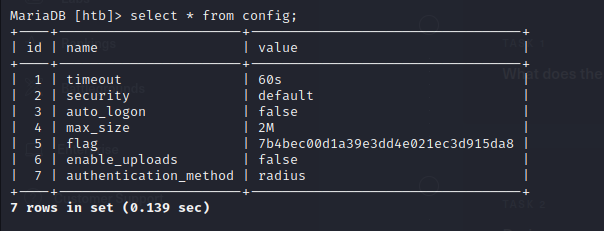


Ver las tablas de cada base de datos



Podemos seguir con comandos para ver el contenido de las tablas config y user





Y en config podemos notar la bandera: 7b4bec00d1a39e3dd4e021ec3d915da8