LOGS (REGISTROS DE AUDITORIA)

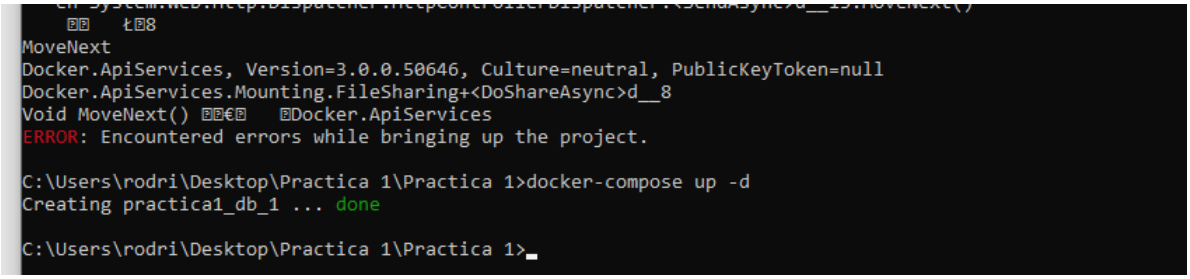
Rodrigo Yerena Herrera

UNIVERSIDAD MODELO | ESCUELA DE INGENIERÍA | DTS | 5TO SEMESTRE | ADMINISTRACIÓN DE BASE DE DATOS | ING. ALFREDO BOLIO DOMÍNGUEZ

Objetivo de la práctica:

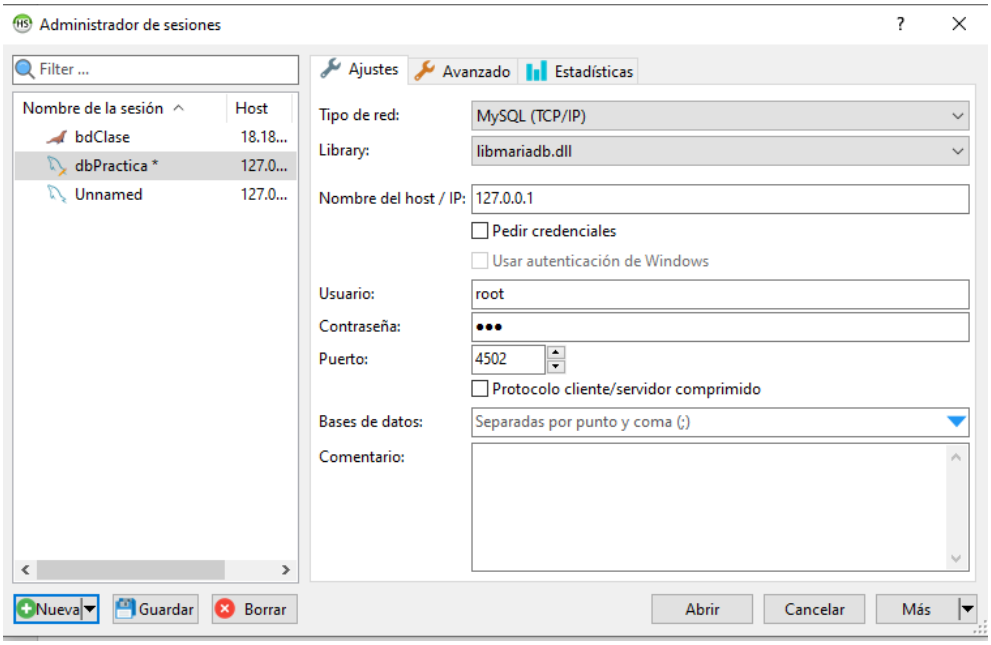
Conocer a través de registros de auditoría quienes intentan realizar ataques masivos a nuestros servidores de bases de datos por medio de contraseñas que normalmente son conocidas y son las mas básicas que puede llegar a utilizarse al momento de guardar nuestras bases de datos en nuestros servidores.

Desarrollo de la práctica:

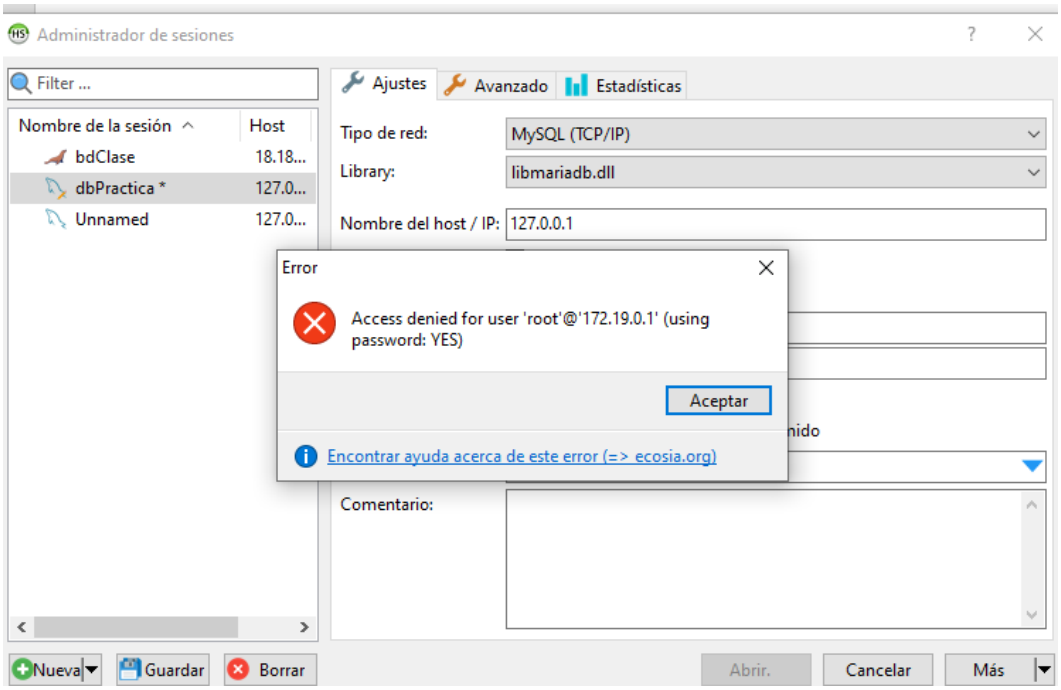


Primero procedemos a posicionarnos en el directorio o carpeta en donde se encuentra nuestro archivo “docker-compose.yml” y procedemos a ejecutar el archivo en la consola de comando con “docker-compose up -d”.

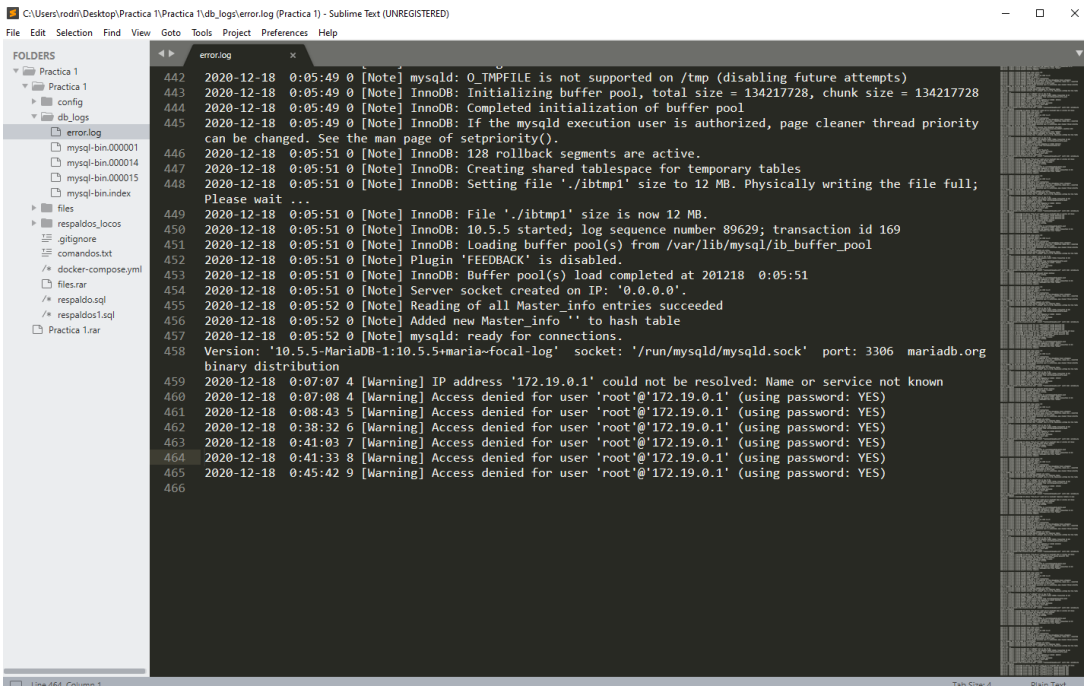
Una vez ya levantado nuestro archivo, lo que procederemos a hacer es recolectar la evidencia de logs. Para ello procederemos a abrir nuestro gestor de base de datos, en mi caso es HeidiSQL y procederemos a crear una base de datos.



Se ha configurado una IP con una respectiva contraseña y un puerto, lo que procederemos a verificar es que los registros de logs se estén guardando en el archivo error.log, esto con el fin de verificar quienes están tratando de ingresar a nuestro servidor de base de datos.



Como podemos ver nos ha denegado el acceso ya que no tenemos las credenciales correctas.



En nuestro archivo error.log, es donde se irán recopilando todos intentos de accesos denegados a nuestro servidor, Con ayuda de un editor de texto, podemos darnos cuenta que por cada intento de ingreso denegado a nuestro servidor, se irá agregando este registro a nuestro archivo.log, Como se puede apreciar en la imagen el usuario con dirección IP 172.19.0.1 intentó ingresar a nuestro servidor seis veces. Al tercer intento de que un usuario intente ingresar sin éxito, y notamos que esta registrado en nuestro archivo.log podemos llegar a la conclusión de que estamos siendo víctimas de un ataque masivo, lo cual puede

llevar a que corramos el riesgo de que nuestro servidor sea hackeado muy fácilmente si no sabemos registrar este tipo de mensajes.

Conclusión y planteamiento de solución

Como podemos apreciar en esta práctica, pudimos aprender a conocer el registro de logs cuando se intenta ingresar a nuestro servidor de base de datos y conocer exactamente con que dirección IP un usuario pudo realizar un ataque masivo a nuestro servidor.

Una planteamiento de solución posible a este problema, lo que se puede hacer y puede resultar una muy buena alternativa, es crear un algoritmo especial que recolecte una dirección IP y un puerto de ingreso, y cuando este intente ingresar por tercera vez sin éxito, este realice un bloqueo total a esta dirección IP con dicho puerto y continuar así con todas las IP's y puertos que no correspondan a los que se tienen definidos los autorizados