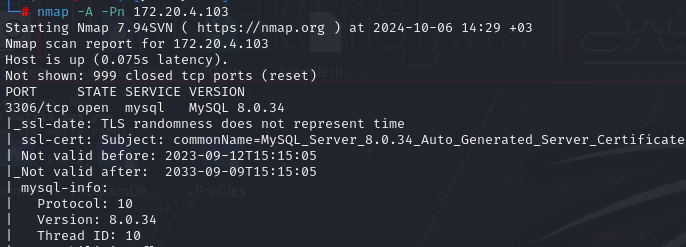
**QUERY GATE WİRTE-UP**

Bu yazımda sizlere Hackviser platformundaki Query Gate adlı warmups çözümü anlatacağım.

**SORU 1:** Hangi port(lar) açık?

Nmap taraması ile bu sonucu bulmaya çalışacağım.



**3306** (MySql) portunun açık olduğunu buluyoruz.

**SORU 2:** Çalışan servisin adı?

**MySql** servisin ismidir.

**SORU 3:** MySQL'e bağlanmak için kullanabileceğimiz en yetkili kullanıcı adı nedir?

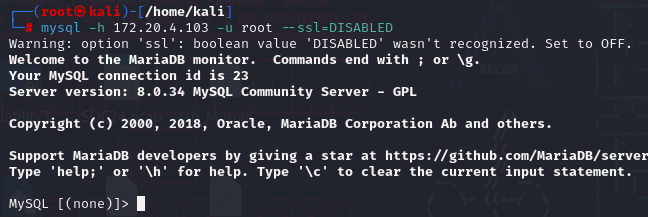
Mysql’e bağlanmak için kullanılan en yetkili kullanıcı **root**’tur.

**SORU 4:** Hedef makinede çalışan MySQL'e bağlanmak için komut satırı aracında hostname i belirtmek için hangi parametre kullanılır?

**-h** parametresi kullanılır.

**SORU 5:** Bağlandığınız MySQL sunucusunda kaç veritabanı var?

Bu soruyu çözmemiz için önce mysql bağlantısı kurmamız gerekmektedir.

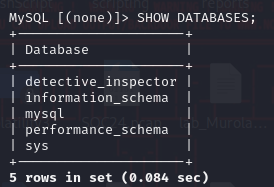


Ben ssl sertfikası hatası aldığımdan dolayı –ssl=DISABLED komutunu girdim.

Burada –h: target IP

-u: kullanıcı görevleri görüyor.

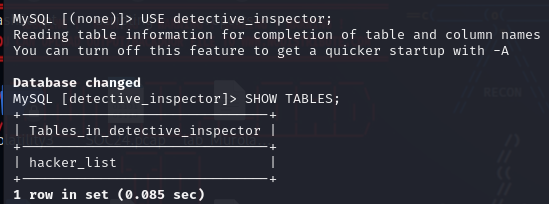
Bağlantı kurduğumuza göre kaç tane tablo olduğunu görmemiz için Show databases; komutunu çalıştırmamız gerekmektedir.

 Burda toplam **5** tane veritabanı olduğunu bulduk.

**SORU 6:** Hangi komutla bir veritabanı seçebiliriz?

**USE** komutu seçme işlemine yarar.

**SORU 7:** detective\_inspector veritabanındaki tablonun adı nedir?

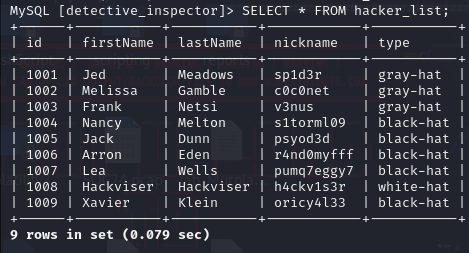


USE detective\_inspector: Bu komut ile detective\_inspector tablosunu seçtik.

SHOW TABLES: Bu komut ile de tabloları listeleyip isimlerine bakmış olduk.

Burada tablomuzun isminin **hacker\_list** olduğunu bulduk.

**SORU 8:**  Beyaz şapkalı hacker'ın kullanıcı adı nedir?



SELECT \* FROM hacker\_list: Bu komut ile hacker\_list tablosundaki tüm verileri göstermemizi sağlıyor.

Bize soruda beyaz şapkalı hacker(White-hat) kullanıcı ismini soruyor.

Type kısmında White-hat kullanıcısının hackviser isimli kullanıcıya ait olduğunu görüyoruz.

Kullanıcı adı da **h4ckv1s3r** olduğunu bulduk.