

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.

```
# nmap -A -Pn 172.20.4.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-06 14:29 +03
Nmap scan report for 172.20.4.103
Host is up (0.075s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
3306/tcp  open  mysql   MySQL 8.0.34
|_ssl-date: TLS randomness does not represent time
|_ssl-cert: Subject: commonName=MySQL_Server_8.0.34_Auto_Generated_Server_Certificate
|_Not valid before: 2023-09-12T15:15:05
|_Not valid after: 2033-09-09T15:15:05
|_mysql-info:
|_  Protocol: 10
|_  Version: 8.0.34
|_  Thread ID: 10
```

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.

```
(root@kali)-[/home/kali]
# mysql -h 172.20.4.103 -u root --ssl=DISABLED
Warning: option 'ssl': boolean value 'DISABLED' wasn't recognized. Set to OFF.
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 23
Server version: 8.0.34 MySQL Community Server - GPL

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> █
```

Ben ssl sertifikası 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.

```
MySQL [(none)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| detective_inspector |
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
5 rows in set (0.084 sec)
```

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?

```
MySQL [(none)]> USE detective_inspector;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [detective_inspector]> SHOW TABLES;
+-----+
| Tables_in_detective_inspector |
+-----+
| hacker_list |
+-----+
1 row in set (0.085 sec)
```

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?

```
MySQL [detective_inspector]> SELECT * FROM hacker_list;
```

id	firstName	lastName	nickname	type
1001	Jed	Meadows	sp1d3r	gray-hat
1002	Melissa	Gamble	c0c0net	gray-hat
1003	Frank	Netsi	v3nus	gray-hat
1004	Nancy	Melton	s1torml09	black-hat
1005	Jack	Dunn	psyod3d	black-hat
1006	Arron	Eden	r4nd0myfff	black-hat
1007	Lea	Wells	pumq7eggy7	black-hat
1008	Hackviser	Hackviser	h4ckv1s3r	white-hat
1009	Xavier	Klein	oricy4l33	black-hat

9 rows in set (0.079 sec)

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.