QUERY GATE WIRTE-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)
        STATE SERVICE VERSION
PORT
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.

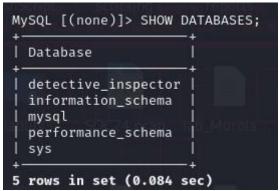
```
(root@ kali)-[/home/kali]
# mysql -h 172.20.4.103 -u root --ssl=DISABLED
Warning: option 'ssl': boolean value 'DISABLED' wasn't recognized. Set to OFF.
Welcome to the MariaDB monitor. Commands end with; or \g.
Your MySQL connection id is 23
Server version: 8.0.34 MySQL Community Server - GPL
Copyright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

MySQL [detective_inspector]> SELECT * FROM hacker_list;				
id	firstName	lastName	nickname	l type
1001 1002 1003 1004 1005 1006 1007 1008 1009	Jed Melissa Frank Nancy Jack Arron Lea Hackviser Xavier	Meadows Gamble Netsi Melton Dunn Eden Wells Hackviser Klein	sp1d3r c0c0net v3nus s1torml09 psyod3d r4nd0myfff pumq7eggy7 h4ckv1s3r	+ Horay-hat gray-hat gray-hat gray-hat black-hat black-hat black-hat white-hat black-hat
9 rows i	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.