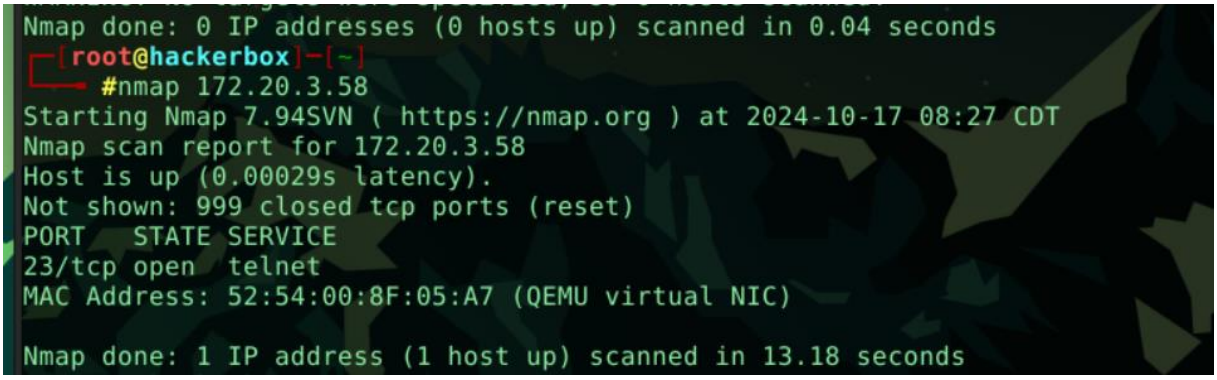
Hackviser Isınmalar

1.Isınmalar:

1-ARROW:

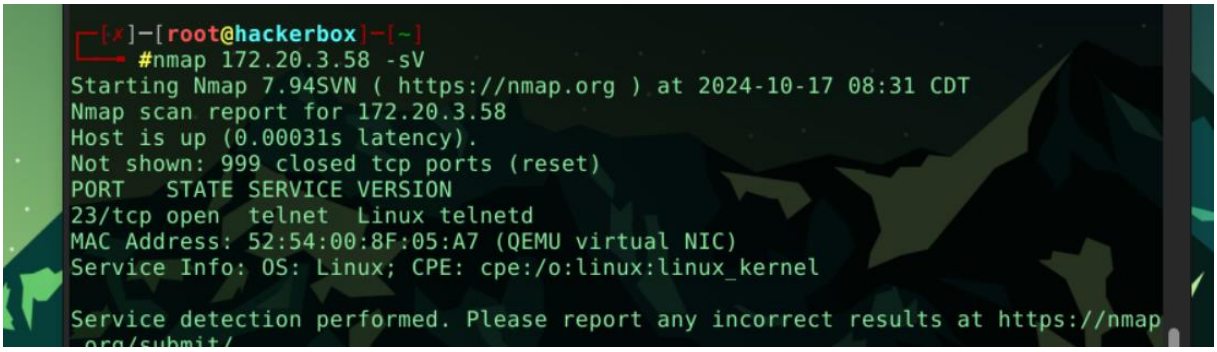
1.SORU: Hangi port açık?

nmap taraması yaptım.



2.SORU: Çalışan servis adı?

nmap taramasında çıkmıştı ama diğer bir yöntemi daha göstermek için nmap ..... -sV yi kullandım.



3.SORU: Hostname nedir?

Hostname makine ismini verir yani arrow

4.SORU: Telnet'e bağlanmak için kullandığınız username:password nedir?

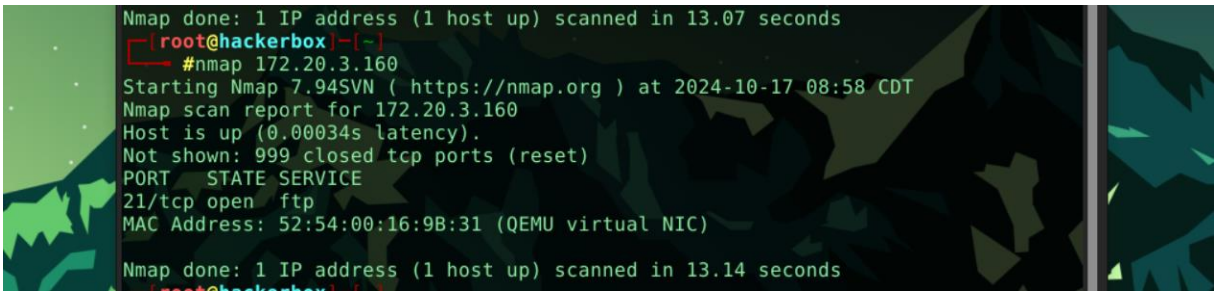
5.SORU: Telnet'e bağlandığınızda çalışma dizini konumunuz nedir?

pwd komutu ile buluruz.

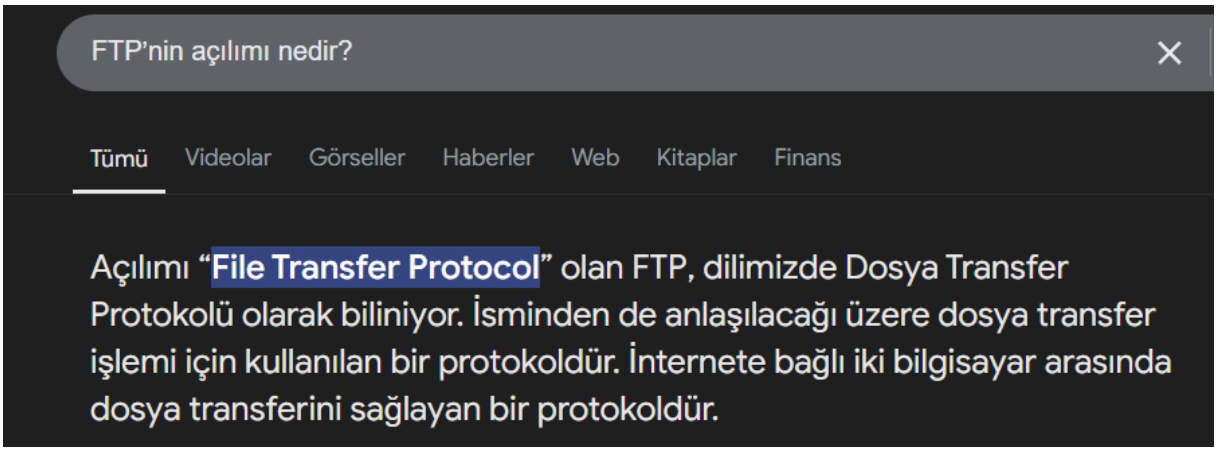
2-File Hunter:

1.SORU: Hangi port(lar) açık?

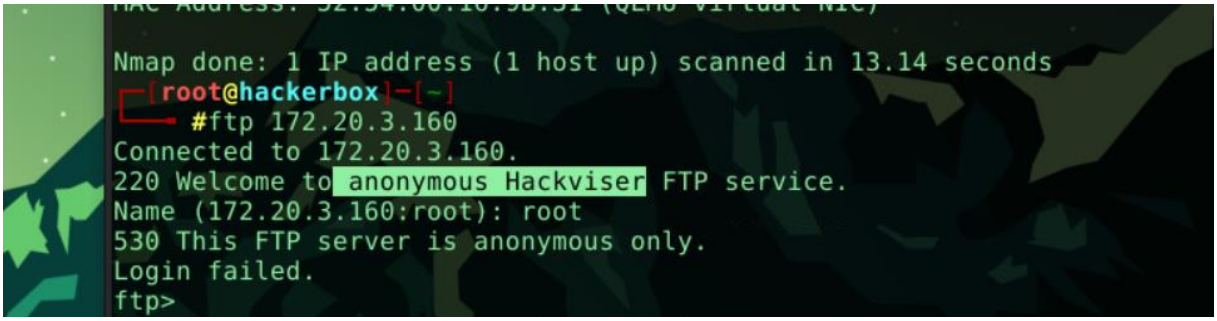
Nmap araması yaptım yine.



2.SORU: FTP'nin açılımı nedir?

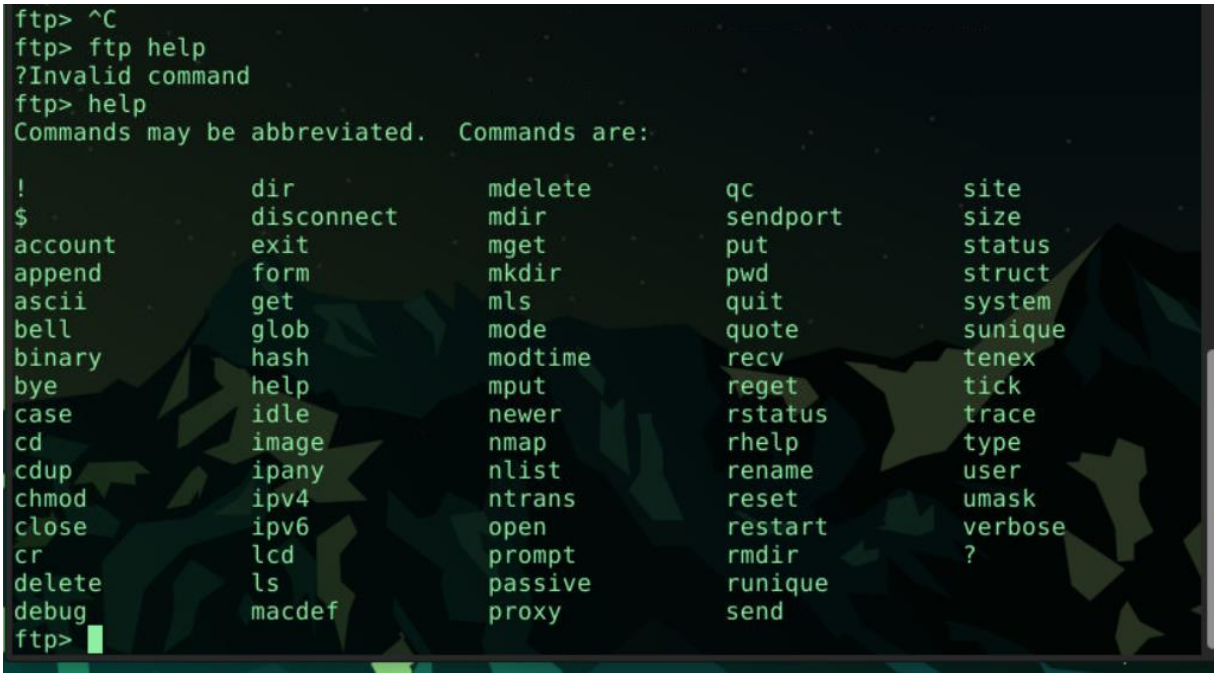


3.SORU: FTP'ye hangi kullanıcı adı ile bağlandınız?



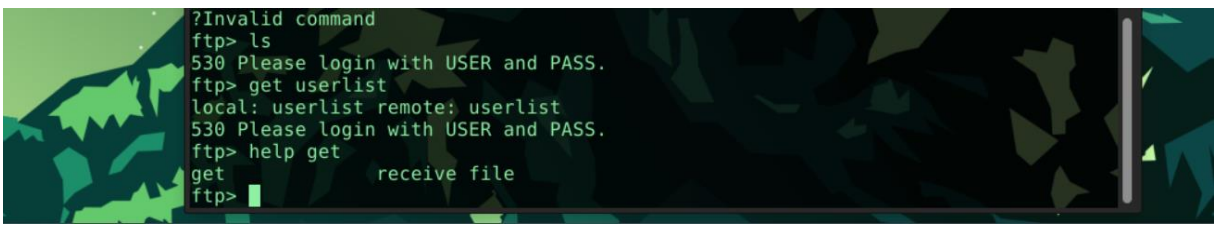
4.SORU: Hangi komut FTP sunucusunda hangi komutları kullanabileceğimizi gösterir?

ftp dizinine girdiğimde help komutuyla.



5.SORU: Bir FTP sunucusundan dosya indirmek için kullanabileceğimiz komut nedir?

get komutunu kullanabiliriz.



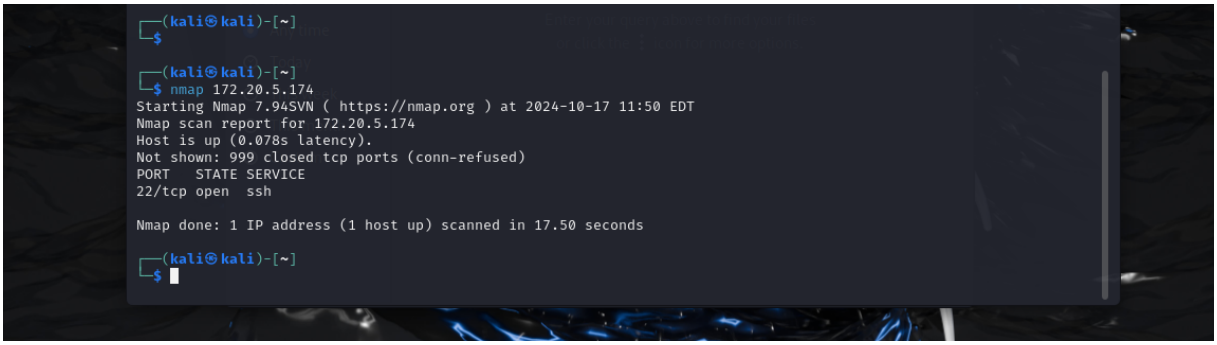
6.SORU: Dosyada hangi kullanıcıların bilgileri vardır?

```
root💀hackerbox:~# cat userlist
jack:hackviser
root:root
```

3-Secure Command:

1.SORU: Hangi port(lar) açık?,

Nmap taraması yaptım.

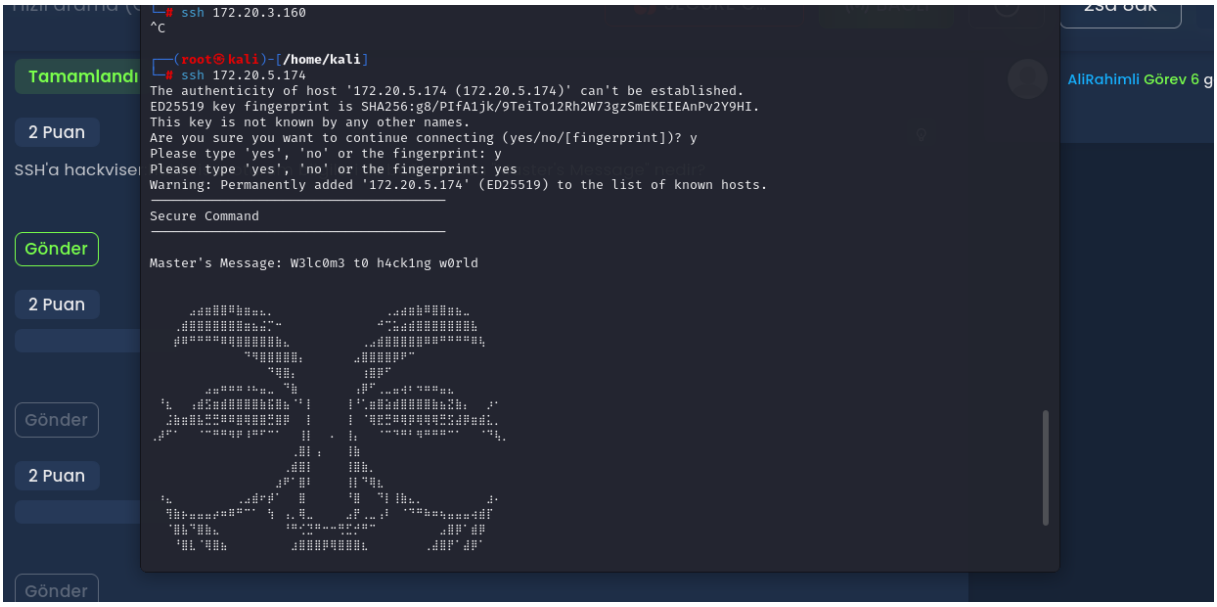


2.SORU: Çalışan hizmet adı nedir?

Nmap -sV ile arama yapıyorum.

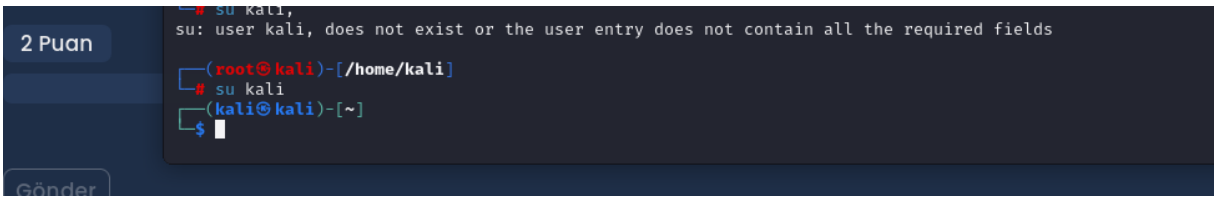
3.SORU: SSH'a hackviser:hackviser oturum bilgileri ile bağlanırken "Master's Message" nedir?

W3lc0m3 t0 h4ck1ng w0rld



4.SORU: Linux'ta kullanıcı değiştirmek için kullanılan komut nedir?

Su

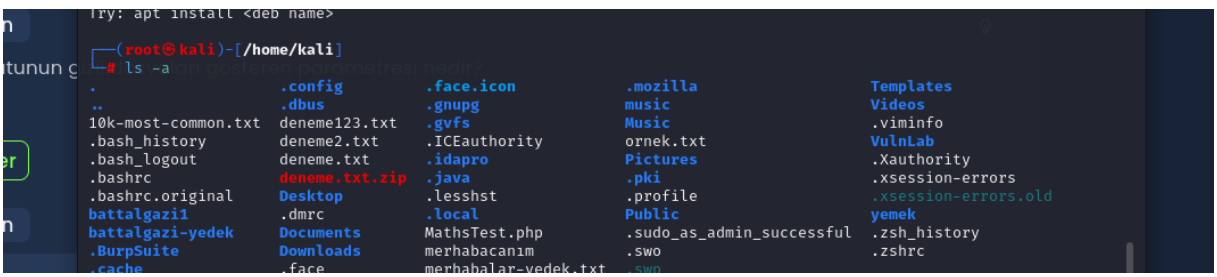


5.SORU: root kullanıcısının parolası nedir?

root

6.SORU: ls komutunun gizli dosyaları gösteren parametresi nedir?

Ls -a komutu tüm dosyaları verir.

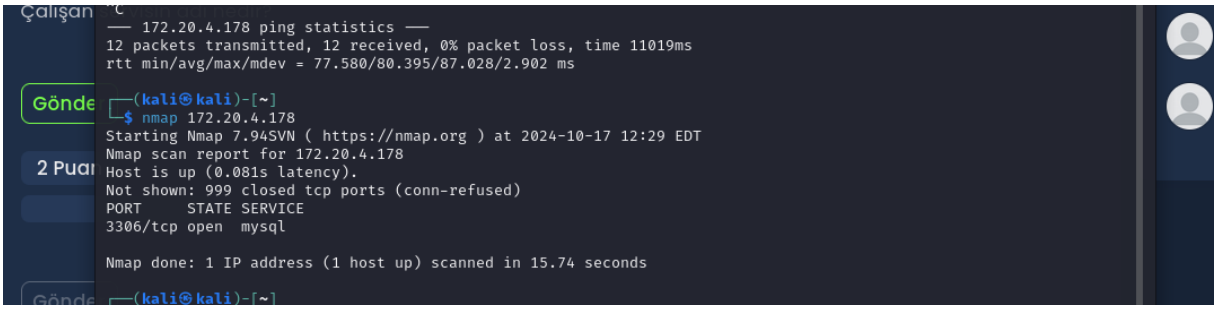


7.SORU: Master’in tavsiyesi nedir?
Dosyalar arasında biraz dolaştıktan sonra root kullanıcısının home dizininde “.advice_of_the_master” adlı ilginç bir gizli dosya bulduk.

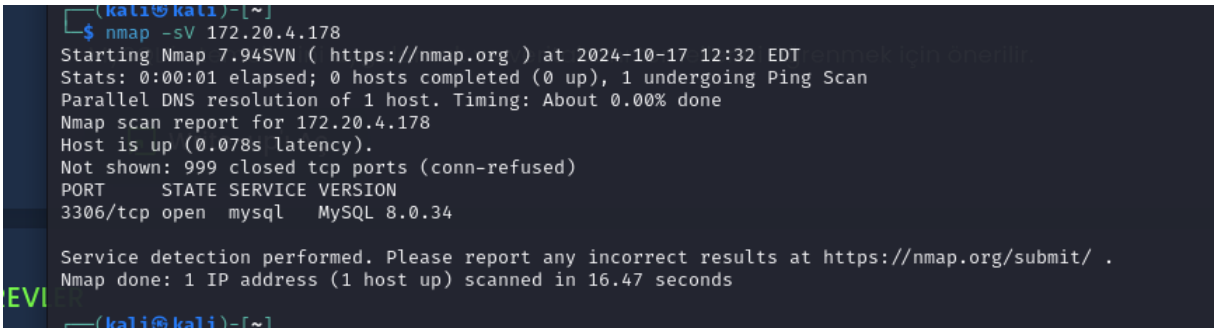
```
root@secure-command:~# cat .advice_of_the_master
st4y cur10us
```

4-Query Gate:

1.SORU: Hangi port(lar) açık?

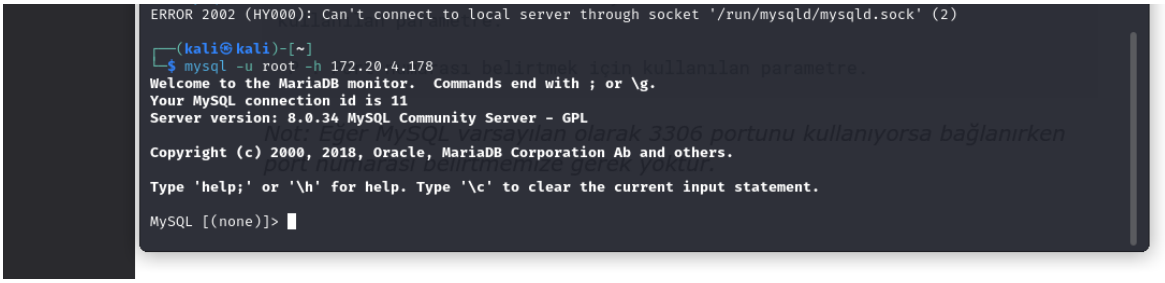


2.SORU: Çalışan servisin adı nedir?

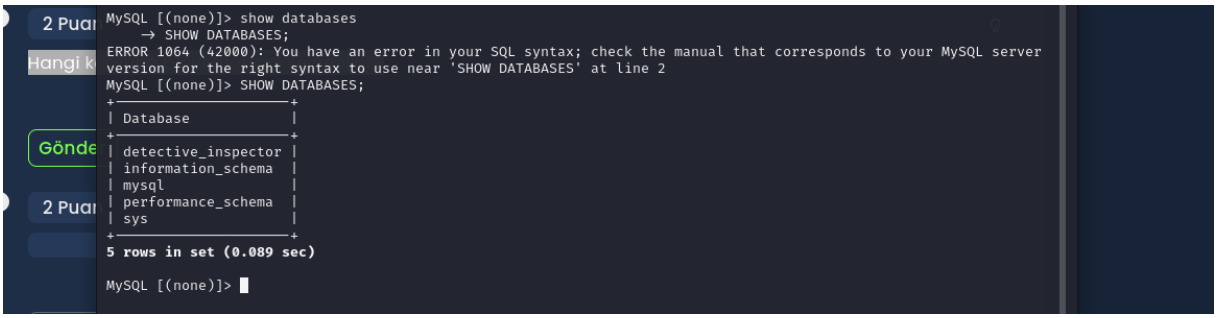


3.SORU: MySQL'e bağlanmak için kullanabileceğimiz en yetkili kullanıcı adı nedir?
Root

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

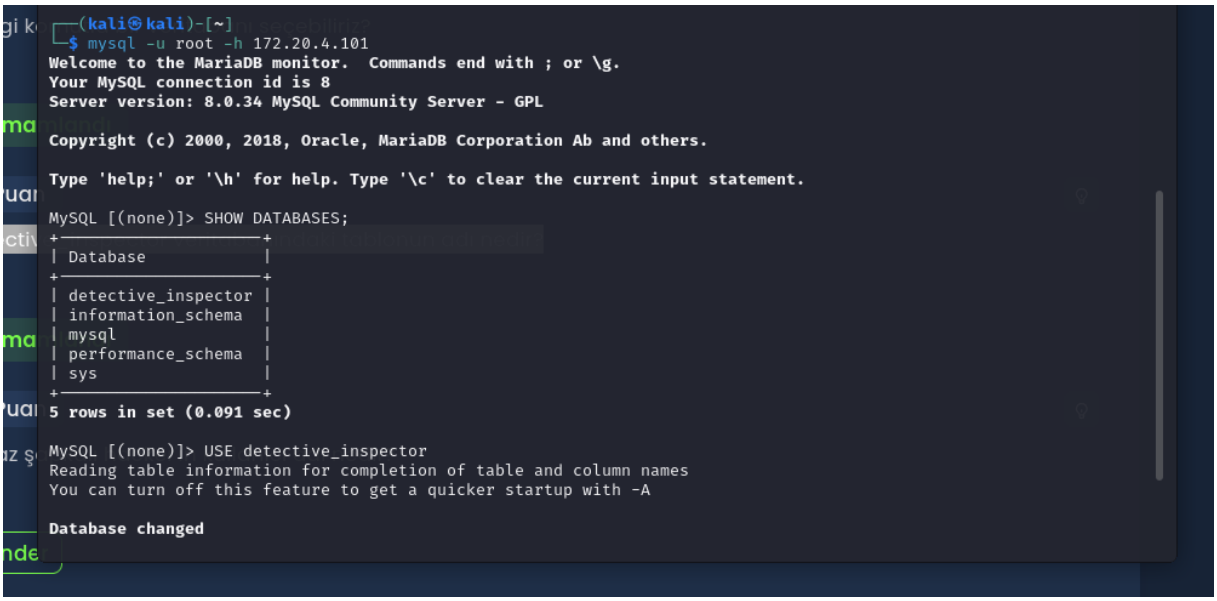


5.SORU: Bağlandığınız MySQL sunucusunda kaç veritabanı var?



```
MySQL [(none)]> show databases
    -> SHOW DATABASES;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server
version for the right syntax to use near 'SHOW DATABASES' at line 2
MySQL [(none)]> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| detective_inspector |
| information_schema  |
| mysql               |
| performance_schema  |
| sys                 |
+--------------------+
5 rows in set (0.089 sec)

MySQL [(none)]>
```

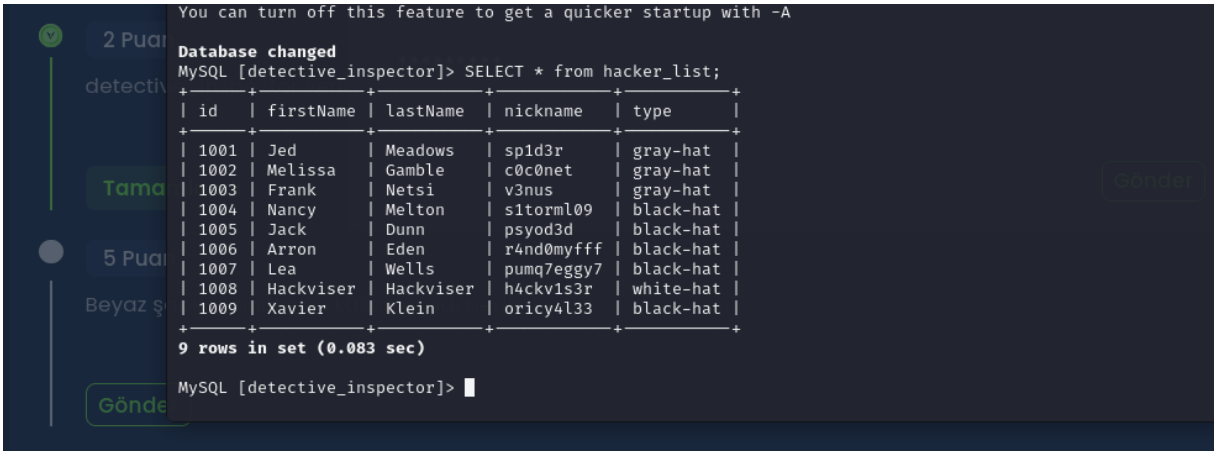
6 ve 7.SORU: Hangi komutla bir veritabanı seçebiliriz? Detective_inspector veritabanındaki tablonun adı nedir?



```
┌──(kali㉿kali)-[~]
└─$ mysql -u root -h 172.20.4.101
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 8.0.34 MySQL Community Server - GPL

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

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 (0.091 sec)

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
```

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

Beyaz şapkalı hacker'ı tespit edebilmek için tablo içeriklerine bakalım.



```
You can turn off this feature to get a quicker startup with -A

Database changed
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 (0.083 sec)

MySQL [detective_inspector]>
```

Isınmalar 1 bitti.