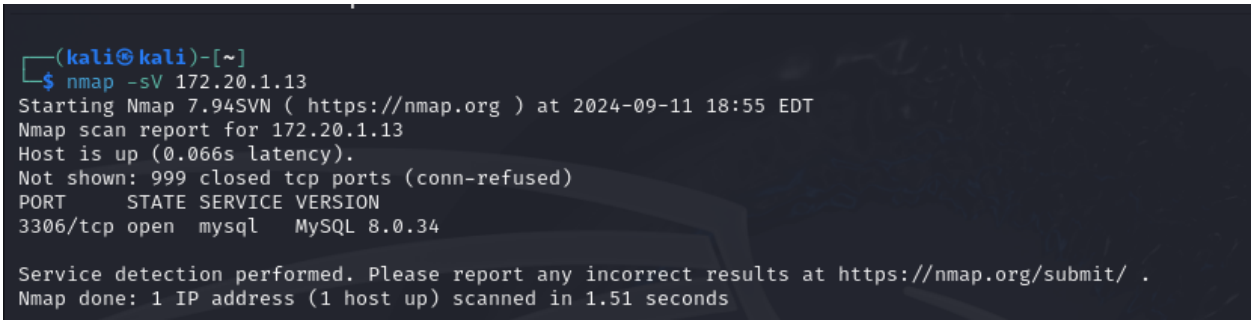
warmups 1-Query Gate

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

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

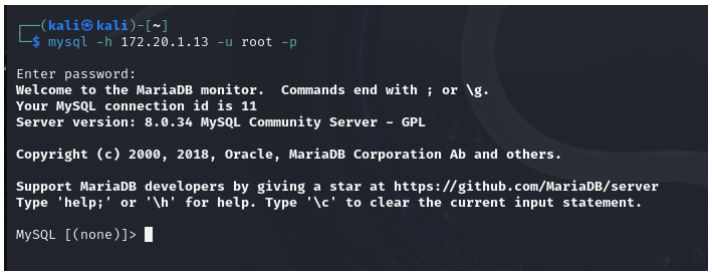


Burada açık port olarak “3306” portu ve çalışan servisin “mysql” gözüküyor.

Ardından mysql ye “root:root” bilgileri ile giriş yapmaya çalışıyorum

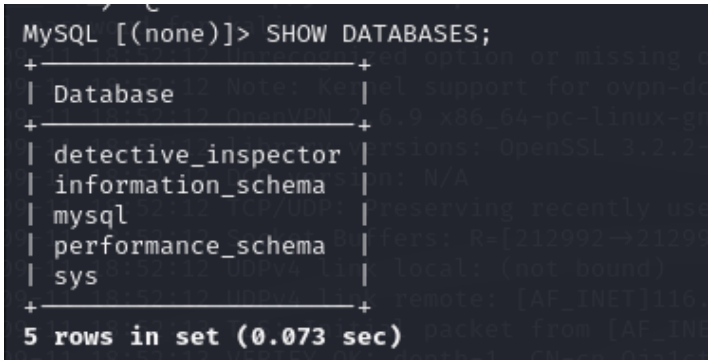
Bu kısımda access denied hatası alıyoruz. satır sonunda “using password: YES” kısmını gördükten sonra şifre girmeden de giriş yapabilme ihtimali aklıma geldi.

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



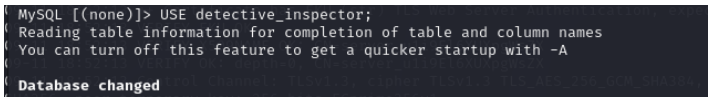
başarılı bir şekilde giriş yaptık

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



Burada detective_inspector db’sini merak ediyorum.

“USE detective_inspector;” komutu ile detective_inspectordb’sine geçiş yapıyorum



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    | 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 (0.069 sec)

MySQL [detective_inspector]>
```

Beyaz şapkalı hackerın username bilgisini bu şekilde elde ediyoruz

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