Hackviser Query Gate Write Up

Öncelikle herkese merhaba bugün Hackviser platformundaki Query Gate isimli Isınmayı çözeceğiz

Başlangıçta bize MYSQL hakkında bilgi vermiş

MySQL, verileri yönetmek ve işlemek için Structured Query Language (SQL) kullanan bir ilişkisel veritabanı yönetim sistemidir (RDBMS). MySQL, web uygulamalarının veritabanları için yaygın olarak kullanılan açık kaynaklı bir sistemdir.

Toplamda 8 sorumuz var sırasıyla

- Hangi port(lar) açık?
- Çalışan servisin adı nedir?
- MySQL'e bağlanmak için kullanabileceğimiz en yetkili kullanıcı adı nedir?
- Hedef makinede çalışan MySQL'e bağlanmak için komut satırı aracında hostname i belirtmek için hangi parametre kullanılır?
- Bağlandığınız MySQL sunucusunda kaç veritabanı var?
- Hangi komutla bir veritabanı seçebiliriz?
- detective_inspector veritabanındaki tablonun adı nedir?
- Beyaz şapkalı hacker'ın kullanıcı adı nedir?

Tarama ile başlayalım

rustscan -a <ip adresi>

3306 ve 33060 portlarının açık olduğunu görüyoruz. (1. sorumuzun cevabı)

Şimdi daha detaylı bilgi için nmap çalıştıralım.

nmap -Pn -n -O -sV -p 3306,33060 <ip adresi> -oN nmapV.txt

- Pn : hedefin çevrimdışı olduğunu varsayar ve host keşif aşamasını atlar.
- -n : Bu seçenek, DNS çözümlemesini devre dışı bırakır. Yani, IP adreslerinin isim çözümlemesi yapılmadan tarama gerçekleştirilir.
- -O: Bu seçenek, işletim sistemi tespiti yapılmasını sağlar. Nmap, çeşitli teknikler kullanarak ağ üzerindeki cihazların işletim sistemlerini tespit etmeye çalışır.
- -sV : Hizmet versiyonlarını belirlemek için kullanılan bir seçenektir. Nmap, açık portlar üzerinde çalışan servislerin hangi versiyonlarının kullanıldığını saptamak için bu seçeneği kullanır.
- -p : Portları belirtmek için kullanılır

```
┌──(root㉿berk)-[~/Documents/Hackviser]
└─# nmap -Pn -n -p 3306,33060 172.20.4.64 -oN nmapV.txt -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-23 15:21 EDT
Nmap scan report for 172.20.4.64
Host is up (0.084s latency).

PORT      STATE SERVICE VERSION
3306/tcp  open  mysql   MySQL 8.0.34
33060/tcp open  mysqlx?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port33060-TCP:V=7.94SVN%I=7%D=9/23%Time=66F1BFAB%P=x86_64-pc-linux-gnu%
SF:r(NULL,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(GenericLines,9,"\x05\0\0\0\x
SF:0b\x08\x05\x1a\0")%r(GetRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(HTT
SF:POptions,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(RTSPRequest,9,"\x05\0\0\0\
SF:x0b\x08\x05\x1a\0")%r(RPCCheck,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSV
SF:ersionBindReqTCP,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSStatusRequestTC
SF:P,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x
SF:0fInvalid\x20message\"\x05HY000")%r(Help,9,"\x05\0\0\0\x0b\x08\x05\x1a\
SF:0")%r(SSLSessionReq,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\
SF:x01\x10\x88'\x1a\x0fInvalid\x20message\"\x05HY000")%r(TerminalServerCoo
SF:kie,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(TLSSessionReq,2B,"\x05\0\0\0\x0
SF:b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20messag
SF:e\"\x05HY000")%r(Kerberos,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(SMBProgNe
SF:g,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(X11Probe,2B,"\x05\0\0\0\x0b\x08\x
SF:05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x05
SF:HY000")%r(FourOhFourRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LPDStri
SF:ng,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LDAPSearchReq,2B,"\x05\0\0\0\x0b
SF:\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message
SF:\"\x05HY000")%r(LDAPBindReq,46,"\x05\0\0\0\x0b\x08\x05\x1a\x009\0\0\0\x
SF:01\x08\x01\x10\x88'\x1a\*Parse\x20error\x20unserializing\x20protobuf\x2
SF:0message\"\x05HY000")%r(SIPOptions,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(
SF:LANDesk-RC,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(TerminalServer,9,"\x05\0
SF:\0\0\x0b\x08\x05\x1a\0")%r(NCP,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(Note
SF:sRPC,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1
SF:a\x0fInvalid\x20message\"\x05HY000")%r(JavaRMI,9,"\x05\0\0\0\x0b\x08\x0
SF:5\x1a\0")%r(WMSRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(oracle-tns,3
SF:2,"\x05\0\0\0\x0b\x08\x05\x1a\0%\0\0\0\x01\x08\x01\x10\x88'\x1a\x16Inva
SF:lid\x20message-frame\.\"\x05HY000")%r(ms-sql-s,9,"\x05\0\0\0\x0b\x08\x0
SF:5\x1a\0")%r(afp,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\
SF:x10\x88'\x1a\x0fInvalid\x20message\"\x05HY000");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.64 seconds
```

3306 portunda MySQL servisi çalışıyor, versiyonu 8.0.34. Burası MySQL'in klasik veri tabanı bağlantı noktası, yani buradan veritabanına bağlanılabiliyor. 33060 portunda ise MySQLX diye daha modern bir protokol aktif. Bu, JSON ve NoSQL ile çalışmak için kullanılıyor. Nmap, buradaki servisi tam tanımlayamamış ama bir 'Invalid message' hatası dönmüş. Yani servisin var olduğunu görüyoruz ama doğru bir yanıt alınamamış. İki port da açık olduğuna göre güvenlik önlemleri almak önemli, özellikle erişimi sınırlamak ve güçlü şifreler kullanmak işimizi garantiye alır. (bu da 2. sorunun cevabı)

Şimdi mysql'e giriş yapmayı deneyelim

mysql -u root -h <ip adresi>

```
┌──(root㉿berk)-[~/Documents/Hackviser]
└─# mysql -u root -h 172.20.4.64
ERROR 2026 (HY000): TLS/SSL error: self-signed certificate in certificate chain

┌──(root㉿berk)-[~/Documents/Hackviser]
└─# mysql -u root -h 172.20.4.64 --skip-ssl
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 45
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)]>
```

ilk denememizde bize sertifika hatası verdiği için bunu atlayarak giriş yapmayı deniyor ve başarılı oluyoruz

mysql -u root -h <ip adresi> --skip-ssl

Root olarak giriş yapmayı deniyoruz çünkü root en yetkili kullanıcı (3. sorunun cevabı)

giriş yaparken hostu -h parametresiyle belirtiyoruz (4. sorunun cevabı)

SHOW DATABASES; komutunu çalıştırarak kaç tane veri tabanı olduğuna bakıyoruz. (5. sorunun cevabı)

```
MySQL [(none)]> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| detective_inspector |
| information_schema  |
| mysql               |
| performance_schema  |
| sys                 |
+--------------------+
5 rows in set (0.097 sec)

MySQL [(none)]>
```

en çok dikkat çeken **detective_inspector** veri tabanına bakalım buna bakmak için önceclikle veri tabanının içerisine **USE** komutu ile girelim.(6. sorunun cevabı)

```
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]>
```

ardından tablonun içerisindeki verileri listelemek için **SHOW TABLES;** komutunu kullanalım

```
Database changed
MySQL [detective_inspector]> SHOW TABLES;
+------------------------------+
| Tables_in_detective_inspector |
+------------------------------+
| hacker_list                  |
+------------------------------+
1 row in set (0.089 sec)

MySQL [detective_inspector]>
```

hacker_list adlı bir tablonun olduğunu görüyoruz. (7. sorunun cevabı)

hacker_list tablosunun içerisindeki verileri okumak için **SELECT * FROM hacker_list;** komutunu kullanıyoruz

```
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 (0.178 sec)

MySQL [detective_inspector]>
```

Ve 8. soruda bizden istenilen beyaz şapkalı hacker'in kullanıcı adı nedir sorusunun cevabını buluyoruz **1008 | Hackviser | Hackviser | h4ckv1s3r | white-hat** (8. sorunun cevabı)

Başka bir yazıda görüşmek üzere !

Linkedin

Github

İnstagram

Medium

Ayberk İlbaş