Mongod

Álvaro Delgado Hernández

```
┌──(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
```

Explanation of Each Argument

-sS: SYN Scan

This performs a TCP SYN scan, which is a stealthy scan method. It sends SYN packets and waits for SYN-ACK responses, allowing you to discover open ports without completing the TCP handshake.

-p-: Scan All Ports

This option tells Nmap to scan all 65,535 TCP ports instead of just the default 1,000 ports.

-sV: Version Detection

This option tells Nmap to detect the versions of the services running on open ports.

-O: OS Detection

This flag enables OS detection, allowing Nmap to determine the operating system of the target host.

-A: Aggressive Scan

This enables several advanced and intrusive options, including OS detection (-O), version detection (-sV), script scanning (-sC), and traceroute.

--top-ports 30000: Scan the Top 30,000 Ports

This tells Nmap to scan the top 30,000 most commonly used ports, which covers a large subset of all 65,535 ports.

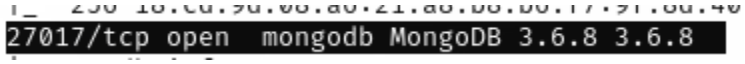
-oN scan.txt: Output to a File

This option specifies that the scan results should be saved in normal format to a file named scan.txt.

How many TCP ports are open on the machine?

2

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



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?

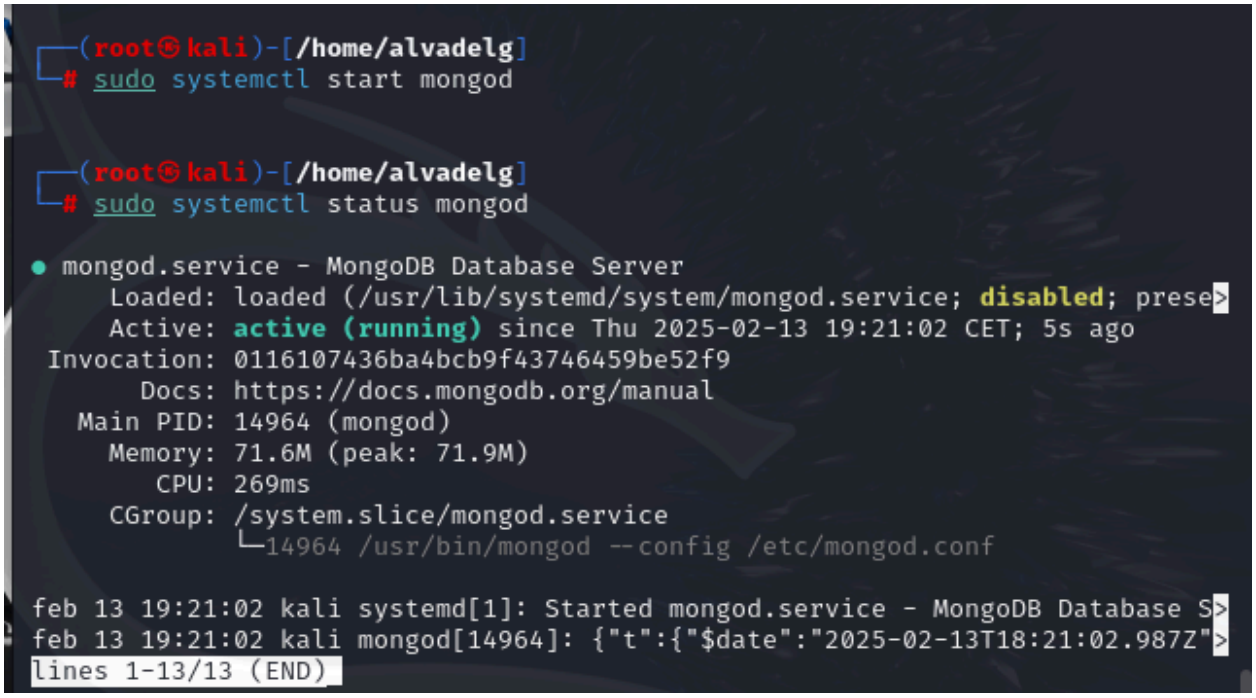
Mongosh

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

In this machine, I encountered issues with the latest version of MongoDB while attempting to perform a specific technique. To resolve these issues, I had to install version 3.6.8 of MongoDB. The older version was necessary because the latest version was causing errors and compatibility problems with the technique I was using.



We need to have the same version of mongo:

```
└─# mongo --version

MongoDB shell version v3.6.8
git version: 6bc9ed599c3fa164703346a22bad17e33fa913e4
OpenSSL version: OpenSSL 1.1.1f  31 Mar 2020
allocator: tcmalloc
modules: none
build environment:
    distmod: debian92
    distarch: x86_64
    target_arch: x86_64
```

```
┌──(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]
>
```

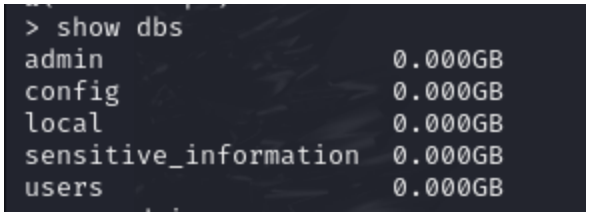
Explanation of Each Argument

mongo:

This is the command-line client for MongoDB databases. It is used to interact with the MongoDB server.

--host 10.129.229.30:

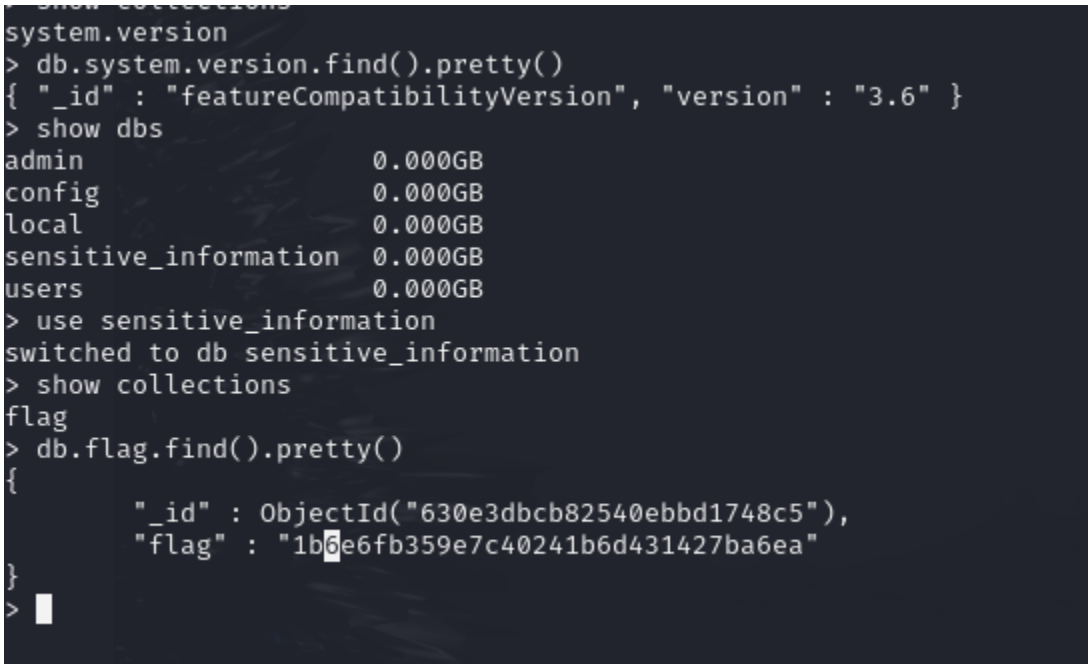
This specifies the IP address of the MongoDB server you want to connect to. In this case, the MongoDB server is located at the IP address 10.129.229.30.



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()



db.flag:

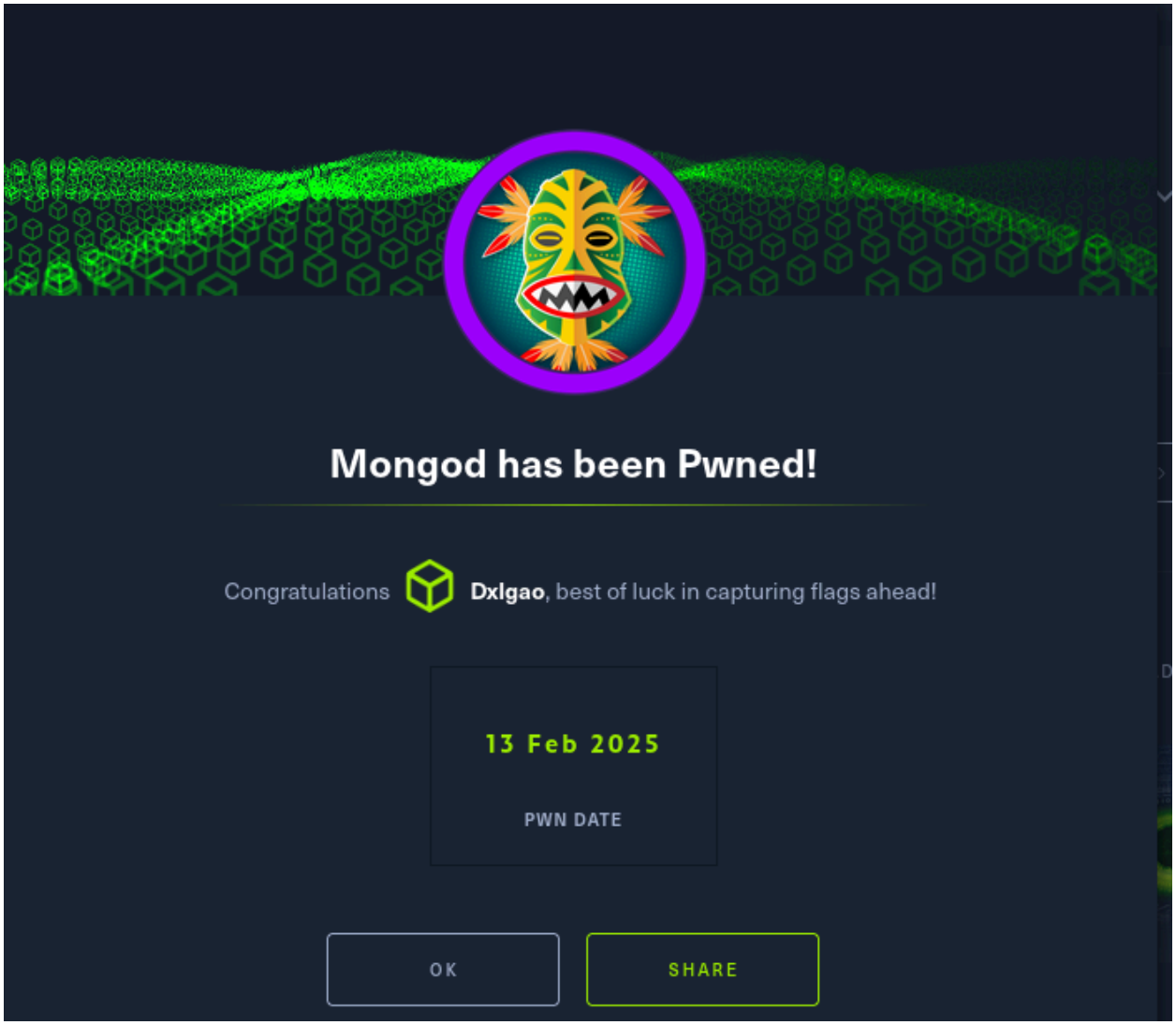
This specifies the collection flag within the currently selected database. The db object represents the current database, and flag is the name of the collection you want to query.

find():

This method retrieves all documents from the specified collection. Without any parameters, find() returns all documents in the collection.

pretty():

This method formats the output of the find() query in a readable, pretty-printed JSON format. This makes it easier to read and understand the structure of the documents


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