NMAP REPORT

Network mapper or Nmap in short is a widely-used free and open source port scanner and network exploration tool. It is renowned for its capabilities as a port scanner, allowing users to discover open ports on target systems and gather information about network services running on those ports. It serves as a great tool for security professionals and penetration tester but unfortunately can be used by malicious actors for unethical activity.

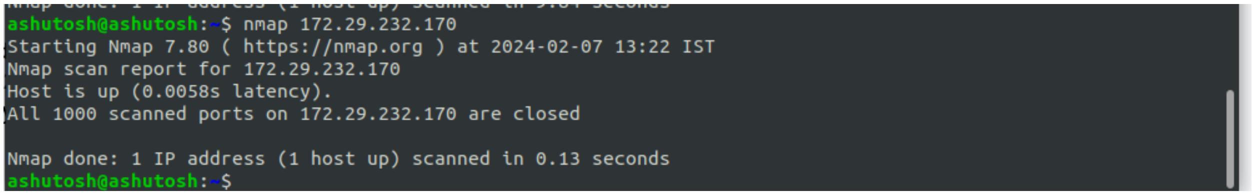
This report briefly uncovers my findings gathered by using Nmap on the assigned port.

1) First of all, I performed a basic scan using nmap by running the command

nmap 172.29.232.170

The above nmap command scans the first 1000 ports as they are well-known ports.

Output:



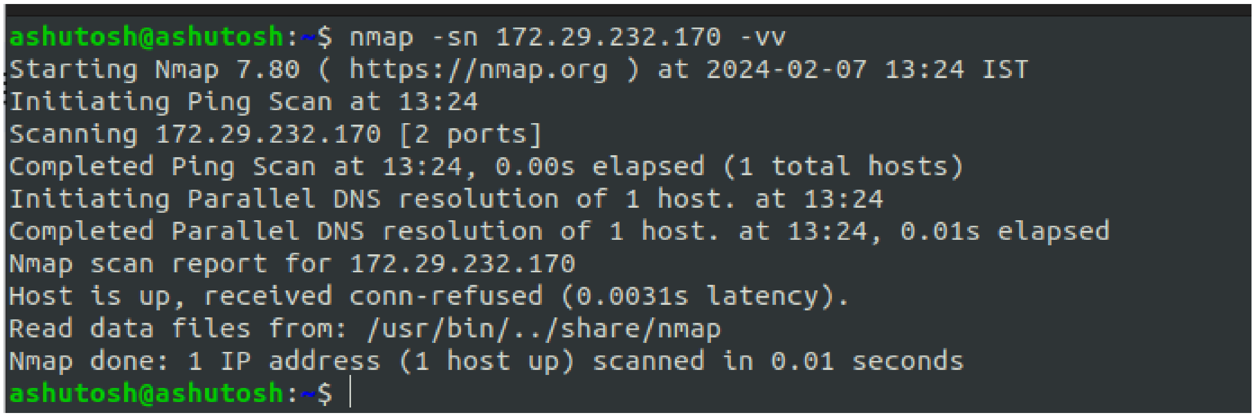
```
Nmap done: 1 IP address (1 host up) scanned in 9.04 seconds
ashutosh@ashutosh:~$ nmap 172.29.232.170
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-07 13:22 IST
Nmap scan report for 172.29.232.170
Host is up (0.0058s latency).
All 1000 scanned ports on 172.29.232.170 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
ashutosh@ashutosh:~$
```

The output shows that all the first 1000 ports are closed.

Then, I performed a ping scan which just pings the target to see if it responds. -sn switch of Nmap helps in doing it. It disables the port scan. It performs light reconnaissance of a target network quickly and without attracting much attention. Knowing how many hosts are up is more valuable to attackers than the list of every single IP and host name. There are three levels of verbosity provided by the tool. -vv specifies two levels of verbosity.

nmap -sn 172.29.232.170 -vv

Output:



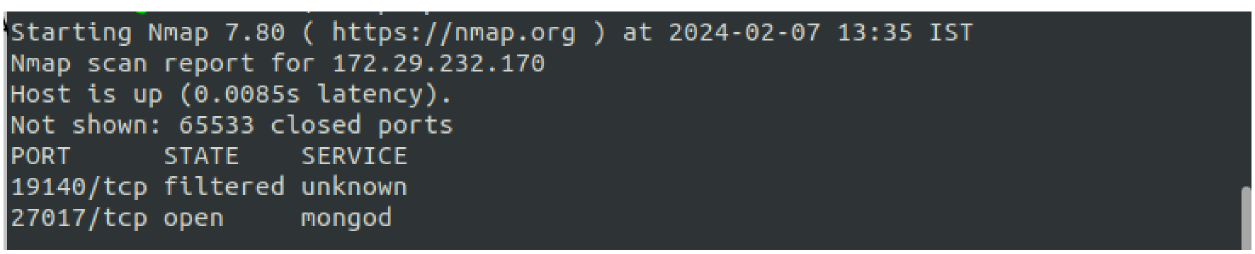
```
ashutosh@ashutosh:~$ nmap -sn 172.29.232.170 -vv
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-07 13:24 IST
Initiating Ping Scan at 13:24
Scanning 172.29.232.170 [2 ports]
Completed Ping Scan at 13:24, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:24
Completed Parallel DNS resolution of 1 host. at 13:24, 0.01s elapsed
Nmap scan report for 172.29.232.170
Host is up, received conn-refused (0.0031s latency).
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds
ashutosh@ashutosh:~$ 
```

The output is not that informative and just tells us whether the host is up or not. So, I decided to try other types of scans by using different switches provided by Nmap tool. I also intended to scan all the ports as all the first 1000 ports seems to be closed.

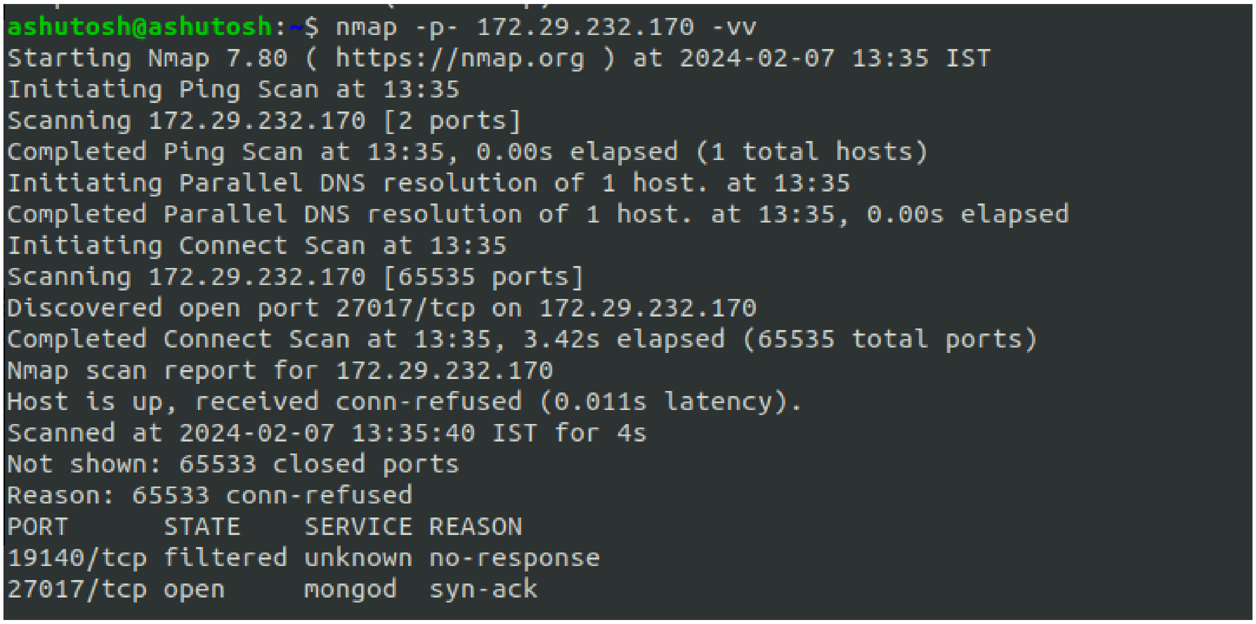
Now, I run the Nmap on all the 65535 ports. In nmap, we can use -p- to specify all ports. In the below command , -oN switches tells nmap to store the output in the normal mode and Allport is just the filename where I wanted to store the output.

nmap -p- -oN Allport 172.29.232.170

Output:



```
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-07 13:35 IST
Nmap scan report for 172.29.232.170
Host is up (0.0085s latency).
Not shown: 65533 closed ports
PORT      STATE    SERVICE
19140/tcp filtered unknown
27017/tcp open     mongod
```



```
ashutosh@ashutosh:~$ nmap -p- 172.29.232.170 -vv
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-07 13:35 IST
Initiating Ping Scan at 13:35
Scanning 172.29.232.170 [2 ports]
Completed Ping Scan at 13:35, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:35
Completed Parallel DNS resolution of 1 host. at 13:35, 0.00s elapsed
Initiating Connect Scan at 13:35
Scanning 172.29.232.170 [65535 ports]
Discovered open port 27017/tcp on 172.29.232.170
Completed Connect Scan at 13:35, 3.42s elapsed (65535 total ports)
Nmap scan report for 172.29.232.170
Host is up, received conn-refused (0.011s latency).
Scanned at 2024-02-07 13:35:40 IST for 4s
Not shown: 65533 closed ports
Reason: 65533 conn-refused
PORT      STATE    SERVICE REASON
19140/tcp filtered unknown no-response
27017/tcp open     mongod  syn-ack
```

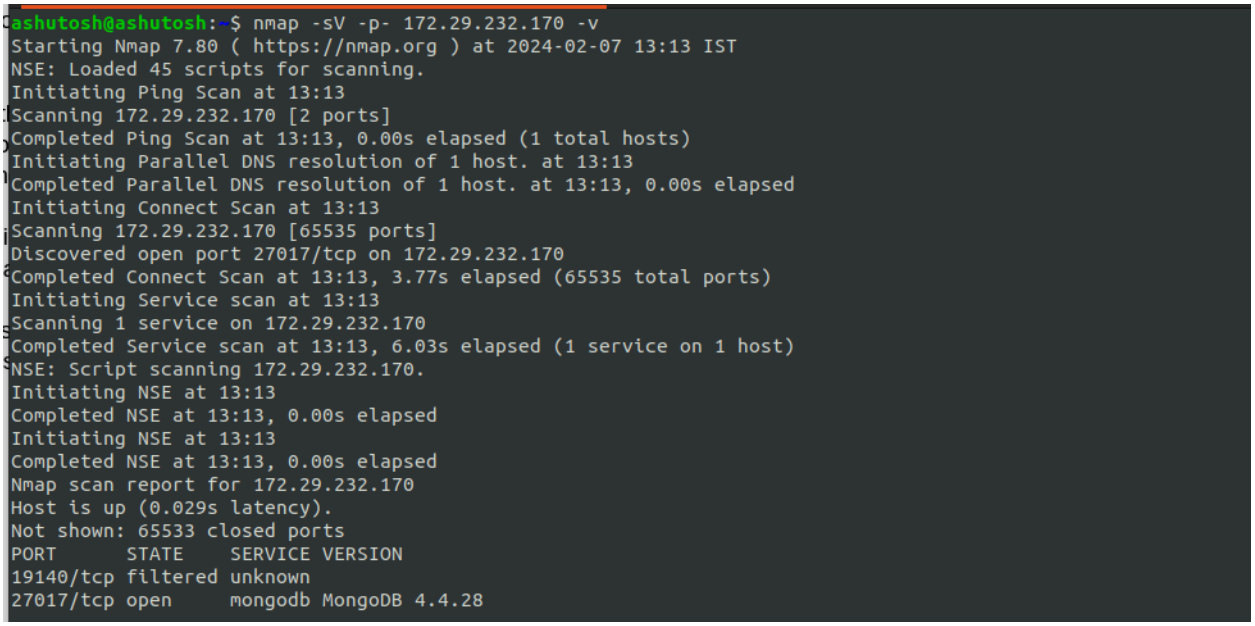
The output shows that only 2 out of 65535 ports are open. Using -vv we also get to know the reason why nmap classifies port 19140 as filtered. The port 27017 is open and mongod service is running on it. Mongod is the daemon used by MongoDB system. Hence, we can infer that target is running a MongoDb instance.

The port 19140 is filtered which means that something is blocking the port ,maybe a firewall. Hence, nmap is unable to determine whether it's open or closed. Nmap also provides swithces for firewall evasion which we can use to possibly uncover information about the services running on the port 19140.

Since, we found a service running, it's good idea to use -sV switch of Nmap which probe open ports to determine service/version info. When performing a version scan (-sV), Nmap sends a series of probes, each of which is assigned a rarity value between one and nine. The lower-numbered probes are effective against a wide variety of common services, while the higher-numbered ones are rarely useful. The intensity level specifies which probes should be applied. The higher the number, the more likely it is the service will be correctly identified. However, high intensity scans take longer. The intensity must be between 0 and 9. The default is 7.

nmap -sV -p- 179.29.232.170

Output:



```
ashutosh@ashutosh:~$ nmap -sV -p- 172.29.232.170 -v
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-07 13:13 IST
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 13:13
Scanning 172.29.232.170 [2 ports]
Completed Ping Scan at 13:13, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:13
Completed Parallel DNS resolution of 1 host. at 13:13, 0.00s elapsed
Initiating Connect Scan at 13:13
Scanning 172.29.232.170 [65535 ports]
Discovered open port 27017/tcp on 172.29.232.170
Completed Connect Scan at 13:13, 3.77s elapsed (65535 total ports)
Initiating Service scan at 13:13
Scanning 1 service on 172.29.232.170
Completed Service scan at 13:13, 6.03s elapsed (1 service on 1 host)
NSE: Script scanning 172.29.232.170.
Initiating NSE at 13:13
Completed NSE at 13:13, 0.00s elapsed
Initiating NSE at 13:13
Completed NSE at 13:13, 0.00s elapsed
Nmap scan report for 172.29.232.170
Host is up (0.029s latency).
Not shown: 65533 closed ports
PORT      STATE    SERVICE VERSION
19140/tcp filtered unknown
27017/tcp open     mongodb MongoDB 4.4.28
```

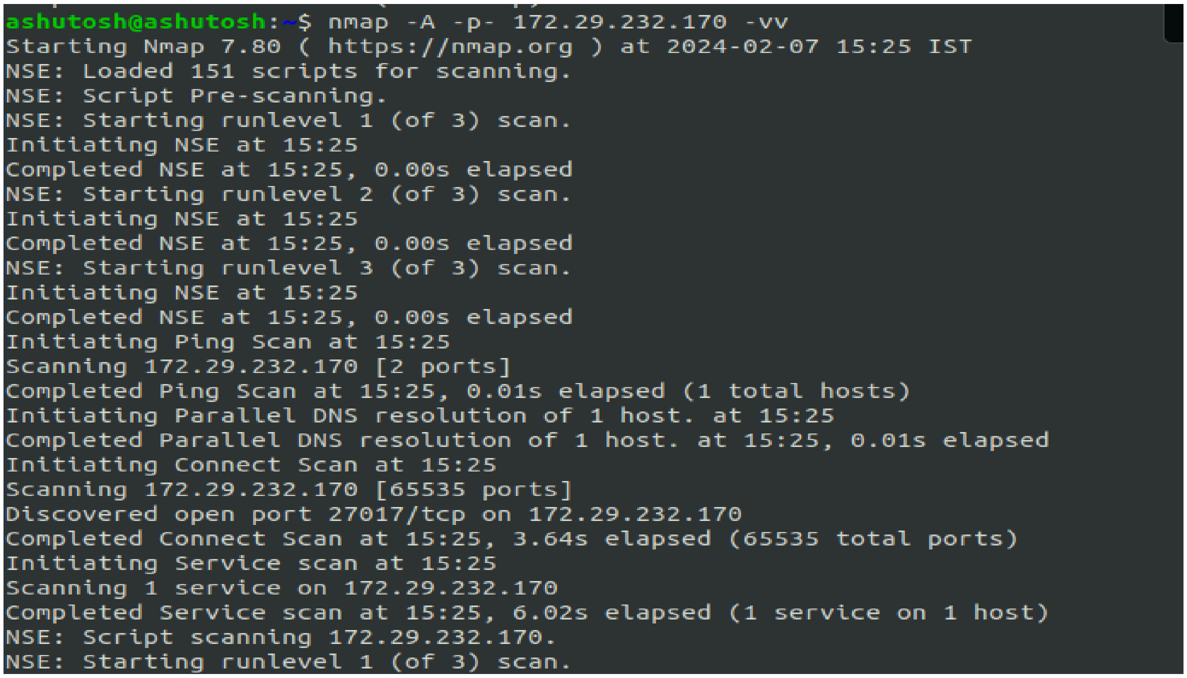
As expected, it gives us the mongodb version running on the system - 4.4.28. The latest version of MongoDB is 7.0. The system is running quite old version of MongoDb and hence can be vulnerable to various security issues.

Now, I use -A switch of nmap which enables Os Detection, version detection, script scanning, and traceroute. -A switch is equivalent to specifying -O -sV -sC --traceroute. I already performed version detection and since I found only two ports open, it’s a good idea to use the -A switch instead of performing each types of scans separately.

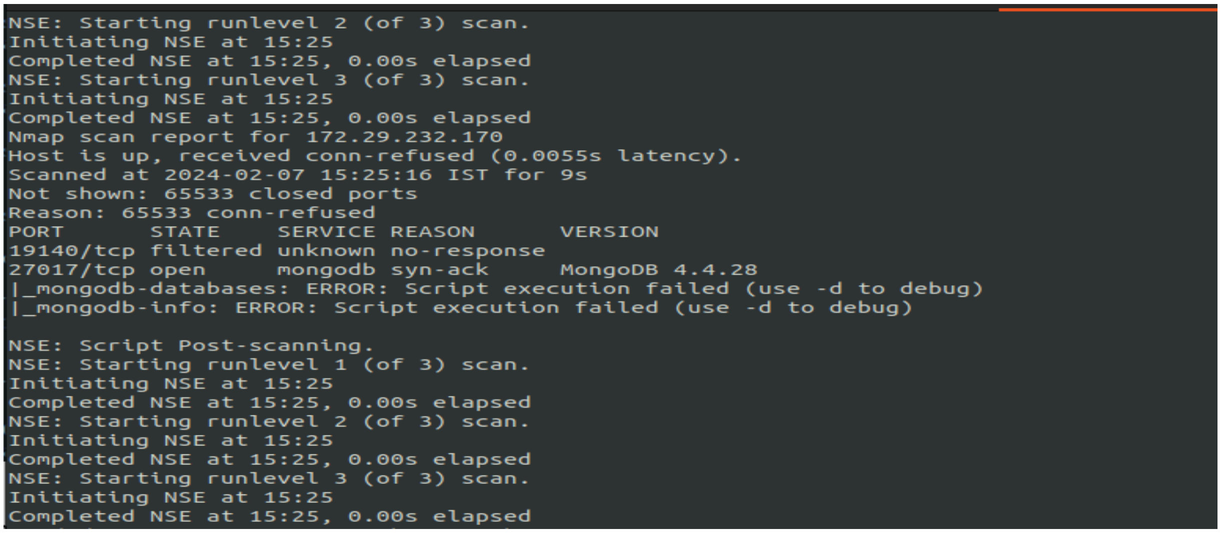
nmap -A -p- 172.29.232.170 -vv

Output:

```
PORT      STATE    SERVICE VERSION
19140/tcp filtered unknown
27017/tcp open     mongodb MongoDB 4.4.28
|_mongodb-databases: ERROR: Script execution failed (use -d to debug)
|_mongodb-info: ERROR: Script execution failed (use -d to debug)
```



```
ashutosh@ashutosh:~$ nmap -A -p- 172.29.232.170 -vv
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-07 15:25 IST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 15:25
Completed NSE at 15:25, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 15:25
Completed NSE at 15:25, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 15:25
Completed NSE at 15:25, 0.00s elapsed
Initiating Ping Scan at 15:25
Scanning 172.29.232.170 [2 ports]
Completed Ping Scan at 15:25, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:25
Completed Parallel DNS resolution of 1 host. at 15:25, 0.01s elapsed
Initiating Connect Scan at 15:25
Scanning 172.29.232.170 [65535 ports]
Discovered open port 27017/tcp on 172.29.232.170
Completed Connect Scan at 15:25, 3.64s elapsed (65535 total ports)
Initiating Service scan at 15:25
Scanning 1 service on 172.29.232.170
Completed Service scan at 15:25, 6.02s elapsed (1 service on 1 host)
NSE: Script scanning 172.29.232.170.
NSE: Starting runlevel 1 (of 3) scan.
```

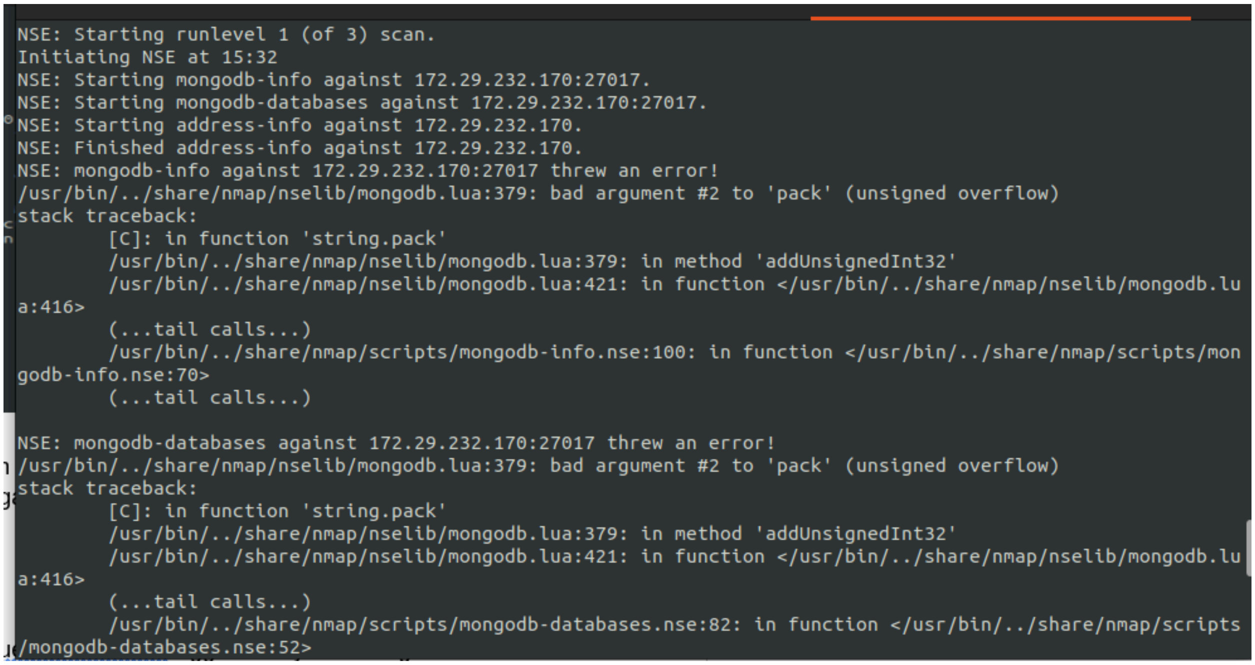


```
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 15:25
Completed NSE at 15:25, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 15:25
Completed NSE at 15:25, 0.00s elapsed
Nmap scan report for 172.29.232.170
Host is up, received conn-refused (0.0055s latency).
Scanned at 2024-02-07 15:25:16 IST for 9s
Not shown: 65533 closed ports
Reason: 65533 conn-refused
PORT      STATE    SERVICE REASON      VERSION
19140/tcp filtered unknown no-response
27017/tcp open     mongodb syn-ack     MongoDB 4.4.28
|_mongodb-databases: ERROR: Script execution failed (use -d to debug)
|_mongodb-info: ERROR: Script execution failed (use -d to debug)

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 15:25
Completed NSE at 15:25, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 15:25
Completed NSE at 15:25, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 15:25
Completed NSE at 15:25, 0.00s elapsed
```

The output shows MongoDB version which is the same result I got by executing -sV switch and it tells us the script it is trying to execute against Mongodb failed for some reason. As suggested by the tool, I used -d to debug the script.

nmap -A -d -p- 172.29.232.170

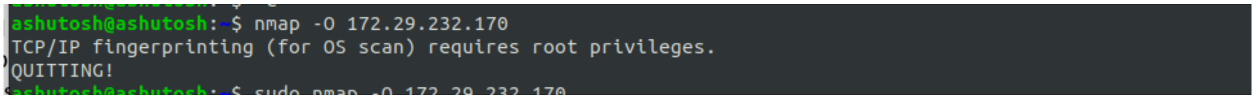
Output:



```
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 15:32
NSE: Starting mongodb-info against 172.29.232.170:27017.
NSE: Starting mongodb-databases against 172.29.232.170:27017.
NSE: Starting address-info against 172.29.232.170.
NSE: Finished address-info against 172.29.232.170.
NSE: mongodb-info against 172.29.232.170:27017 threw an error!
/usr/bin/../share/nmap/nselib/mongodb.lua:379: bad argument #2 to 'pack' (unsigned overflow)
stack traceback:
        [C]: in function 'string.pack'
        /usr/bin/../share/nmap/nselib/mongodb.lua:379: in method 'addUnsignedInt32'
        /usr/bin/../share/nmap/nselib/mongodb.lua:421: in function </usr/bin/../share/nmap/nselib/mongodb.lu
a:416>
        (...tail calls...)
        /usr/bin/../share/nmap/scripts/mongodb-info.nse:100: in function </usr/bin/../share/nmap/scripts/mon
godb-info.nse:70>
        (...tail calls...)

NSE: mongodb-databases against 172.29.232.170:27017 threw an error!
/usr/bin/../share/nmap/nselib/mongodb.lua:379: bad argument #2 to 'pack' (unsigned overflow)
stack traceback:
        [C]: in function 'string.pack'
        /usr/bin/../share/nmap/nselib/mongodb.lua:379: in method 'addUnsignedInt32'
        /usr/bin/../share/nmap/nselib/mongodb.lua:421: in function </usr/bin/../share/nmap/nselib/mongodb.lu
a:416>
        (...tail calls...)
        /usr/bin/../share/nmap/scripts/mongodb-databases.nse:82: in function </usr/bin/../share/nmap/scripts
/mongodb-databases.nse:52>
```

It tells us that the script encountered an error.The error message indicates a problem with argument handling in the mongodb.lua script. It might be a better idea to spend some time resolving the error as the script might uncover a substantial amount of information. Another alternative is to use some other Mongo-DB related script.

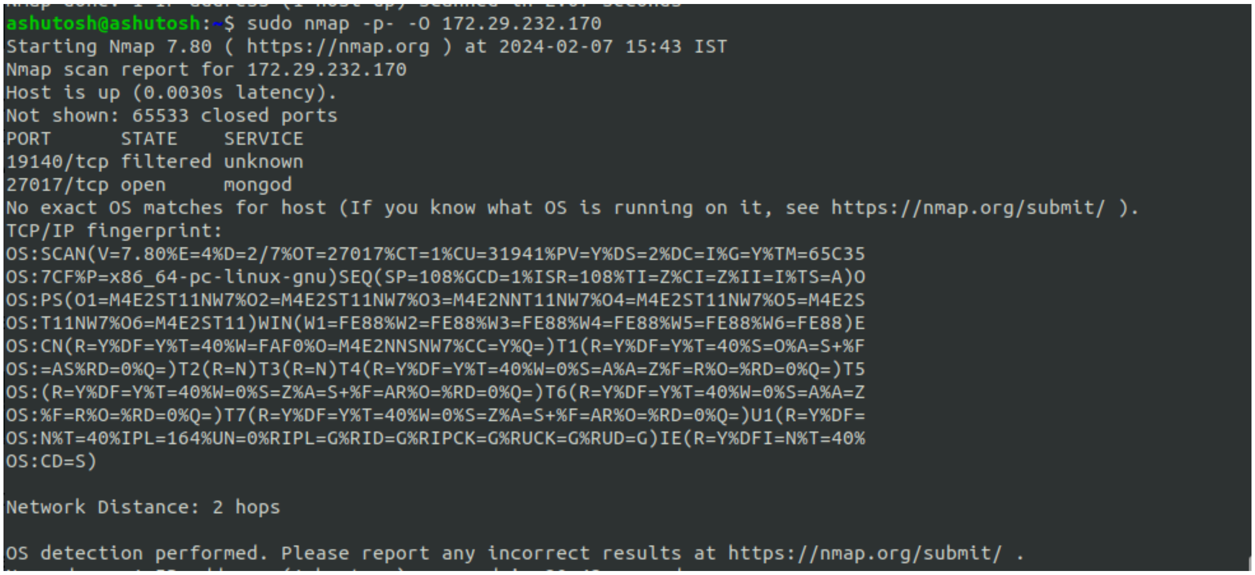
Finally, I make an attempt to discover OS. I earlier used -A command which enables OS detection but Nmap might not be able to do that as it performs OS detection using TCP/IP fingerprinting which requires sudo privileges as shown in the output below:



```
ashutosh@ashutosh:~$ nmap -O 172.29.232.170
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!
ashutosh@ashutosh:~$ sudo nmap -O 172.29.232.170
```

Thus , I run the following command with sudo privileges:

sudo nmap -p- -O 172.29.232.170

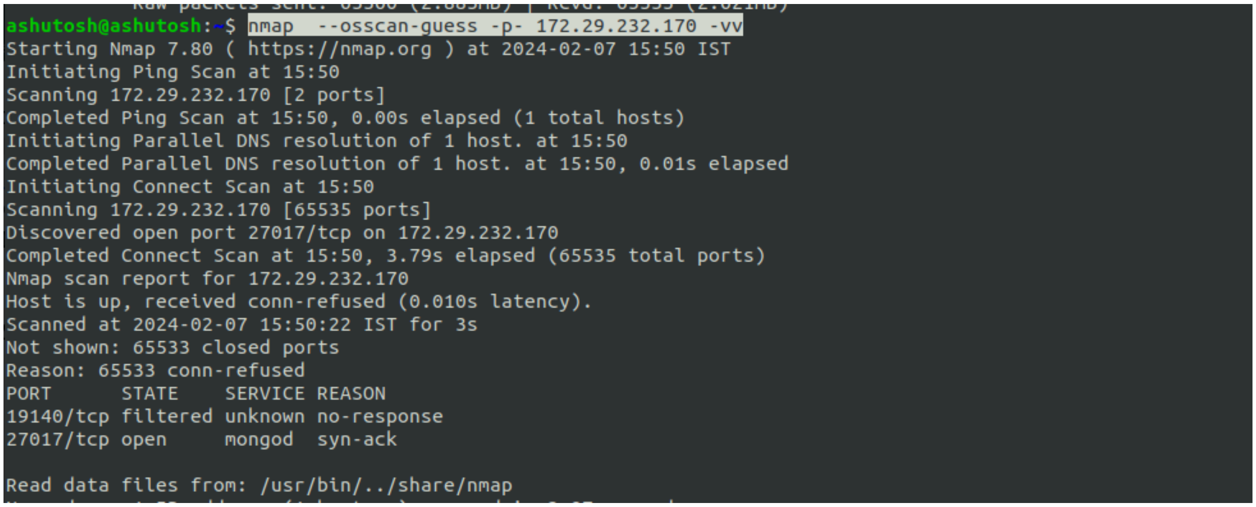


```
ashutosh@ashutosh:~$ sudo nmap -p- -O 172.29.232.170
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-07 15:43 IST
Nmap scan report for 172.29.232.170
Host is up (0.0030s latency).
Not shown: 65533 closed ports
PORT      STATE    SERVICE
19140/tcp filtered unknown
27017/tcp open     mongod
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=2/7%OT=27017%CT=1%CU=31941%PV=Y%DS=2%DC=I%G=Y%TM=65C35
OS:7CF%P=x86_64-pc-linux-gnu)SEQ(SP=108%GCD=1%ISR=108%TI=Z%CI=Z%II=I%TS=A)O
OS:PS(O1=M4E2ST11NW7%O2=M4E2ST11NW7%O3=M4E2NNT11NW7%O4=M4E2ST11NW7%O5=M4E2S
OS:T11NW7%O6=M4E2ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)E
OS:CN(R=Y%DF=Y%T=40%W=FAF0%O=M4E2NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F
OS:=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5
OS:(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z
OS:%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=
OS:N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%
OS:CD=S)

Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

Nmap was not able to identify the OS based on TCP/IP fingerprint. Hence, I used osscan-guess switch which guesses OS more aggressively. Referring to the documentation, Nmap tells you when an imperfect match is found and display its confidence level (percentage) for each guess. Below is the command used and output produced.

nmap --osscan-guess -p- 172.29.232.170

Output:



```
ashutosh@ashutosh:~$ nmap  --osscan-guess -p- 172.29.232.170 -vv
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-07 15:50 IST
Initiating Ping Scan at 15:50
Scanning 172.29.232.170 [2 ports]
Completed Ping Scan at 15:50, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:50
Completed Parallel DNS resolution of 1 host. at 15:50, 0.01s elapsed
Initiating Connect Scan at 15:50
Scanning 172.29.232.170 [65535 ports]
Discovered open port 27017/tcp on 172.29.232.170
Completed Connect Scan at 15:50, 3.79s elapsed (65535 total ports)
Nmap scan report for 172.29.232.170
Host is up, received conn-refused (0.010s latency).
Scanned at 2024-02-07 15:50:22 IST for 3s
Not shown: 65533 closed ports
Reason: 65533 conn-refused
PORT      STATE    SERVICE REASON
19140/tcp filtered unknown no-response
27017/tcp open     mongod  syn-ack

Read data files from: /usr/bin/../share/nmap
```

The output didn't give any new additional information. Nmap was not able to identify the OS running on the system.

Hence, By performing the nmap scan using different switches and functionalities, I found one open port and one filtered port. The open port is running MongoDB version 4.4.28.