Redeemer

Task 1

Which TCP port is open on the machine?
`6379`

- I ran `sudo nmap -A -p- -T4` and these were the results

```
Nmap scan report for 10.129.180.159
Host is up (0.083s latency).
Not shown: 65534 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
6379/tcp open  redis   Redis key-value store 5.0.7
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=7.92%E=4%D=5/13%OT=6379%CT=1%CU=41464%PV=Y%DS=2%DC=T%G=Y%TM=627F0
OS:83B%P=x86_64-pc-linux-gnu)SEQ(SP=FF%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)SE
OS:Q(SP=FF%GCD=1%ISR=109%TI=Z%CI=Z%TS=A)OPS(O1=M505ST11NW7%O2=M505ST11NW7%O
OS:3=M505NNT11NW7%O4=M505ST11NW7%O5=M505ST11NW7%O6=M505ST11)WIN(W1=FE88%W2=
OS:FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M505NNSN
OS:W7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%D
OS:F=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O
OS:=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W
OS:=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%R
OS:IPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops

TRACEROUTE (using port 23/tcp)
HOP RTT      ADDRESS
1   94.90 ms 10.10.14.1
2   91.32 ms 10.129.180.159

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 309.15 seconds
```

Task 2

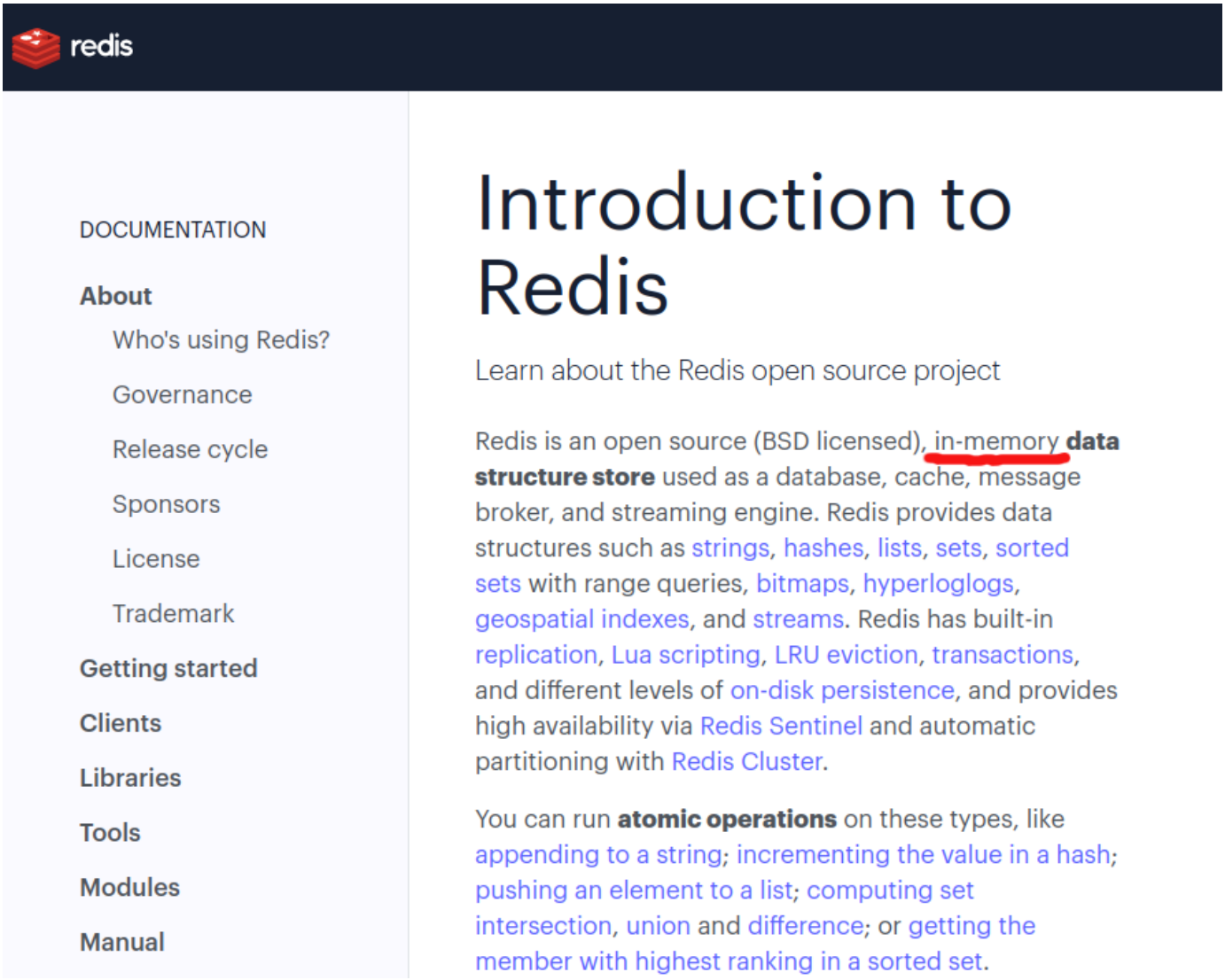
Which service is running on the port that is open on the machine?
`redis`

```
PORT     STATE SERVICE VERSION
6379/tcp open  redis   Redis key-value store 5.0.7
```

Task 3

What type of database is Redis? Choose from the following options: (i) In-memory Database, (ii) Traditional Database
`In-memory Database`

- Consult the [Redis documentation]



Task 4

Which command-line utility is used to interact with the Redis server? Enter the program name you would enter into the terminal without any arguments.

`redis-cli`

- Go to the Manual for Redis and seek the chapter titled CLI.

Redis CLI

Overview of redis-cli, the Redis command line interface

The `redis-cli` (Redis command line interface) is a terminal program used to send commands to and read replies from the Redis server. It has two main modes: an interactive REPL (Read Eval Print Loop) mode where the user types Redis commands and receives replies, and a command mode where `redis-cli` is executed with additional arguments and the reply is printed to the standard output.

Task 5

Which flag is used with the Redis command-line utility to specify the hostname?

`-h`

- Go back to CLI chapter until you find a section titled "**Host, port, password and database**".

Host, port, password and database

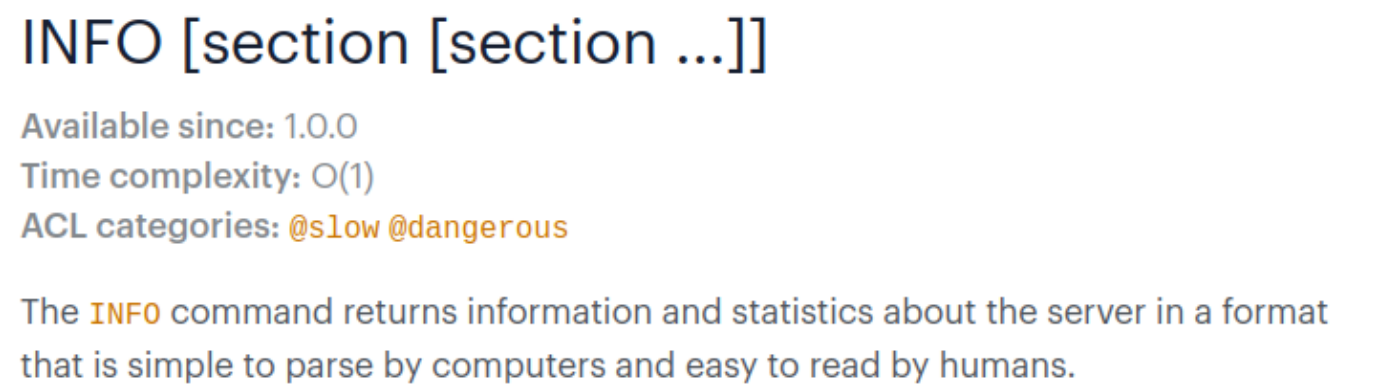
By default `redis-cli` connects to the server at the address 127.0.0.1 with port 6379. You can change this using several command line options. To specify a different host name or an IP address, use the `-h` option. In order to set a different port, use `-p`.

```
$ redis-cli -h redis15.localnet.org -p 6390 PING
PONG
```

Task 6

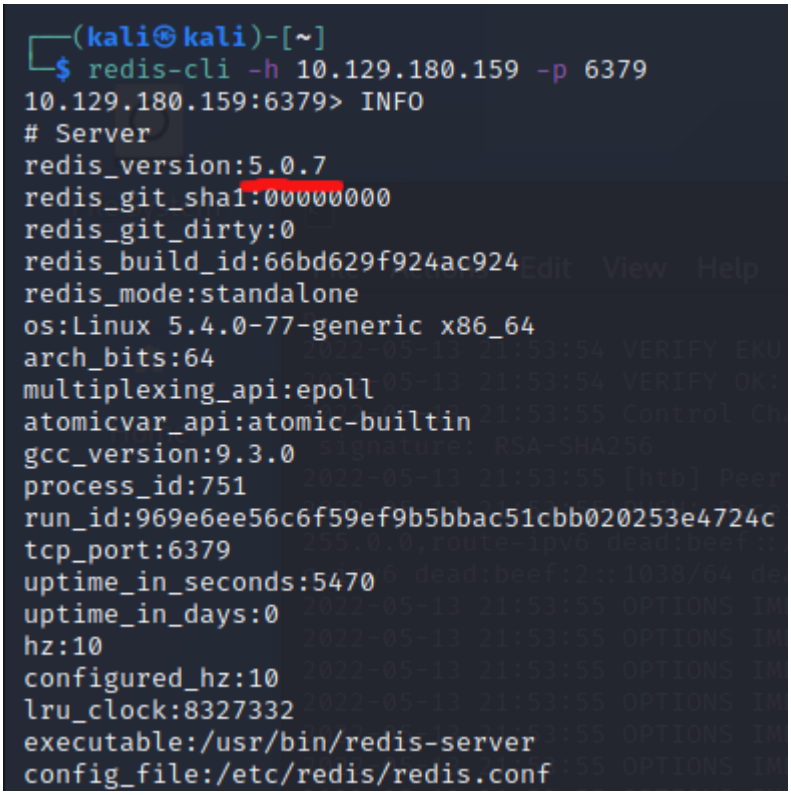
Once connected to a Redis server, which command is used to obtain the information and statistics about the Redis server?
`info`

- Info on the `info` command.



Task 7

What is the version of the Redis server being used on the target machine?
`5.0.7`



Task 8

Which command is used to select the desired database in Redis?
`select`

SELECT index

Available since: 1.0.0
Time complexity: O(1)
ACL categories: @fast @connection

Select the Redis logical database having the specified zero-based numeric index.
New connections always use the database 0.

Task 9

How many keys are present inside the database with index 0?
`4`

```
# Keyspace
db0:keys=4,expires=0,avg_ttl=0
10.129.180.159:6379>
```

Task 10

Which command is used to obtain all the keys in a database?
`keys *`

```
10.129.180.159:6379> KEYS *
```

- This article was helpful for me.

Submit root flag

Submit root flag
`03e1d2b376c37ab3f5319922053953eb`

- Run `GET flag` to find the root flag.

```
10.129.180.159:6379> GET flag
"03e1d2b376c37ab3f5319922053953eb"
```