Redeemer

Which TCP port is open on the machine?

6379

```
om]─[~]
└── [*]$ nmap -p- -min-rate 5000 10.129.106.77
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-22 10:54 CST
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Sca
SYN Stealth Scan Timing: About 50.34% done; ETC: 10:55 (0:00:07 remaining)
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Sca
SYN Stealth Scan Timing: About 52.32% done; ETC: 10:55 (0:00:07 remaining)
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Sca
SYN Stealth Scan Timing: About 87.67% done; ETC: 10:55 (0:00:02 remaining)
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Sca
SYN Stealth Scan Timing: About 95.39% done; ETC: 10:55 (0:00:01 remaining)
Nmap scan report for 10.129.106.77
Host is up (0.26s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
6379/tcp open  redis
```

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

redis

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

In-memory Database

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

```
┌[us-starting-point-2-dhcp]─[10.10.14.45]─[blackdogg@htb-j2kdelqeo1-htb-cloud
om]─[~]
└─ [*]$ redis-cli -h 10.129.106.77
10.129.106.77:6379> info
# Server
redis_version:5.0.7
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:66bd629f924ac924
redis_mode:standalone
os:Linux 5.4.0-77-generic x86_64
arch_bits:64
multiplexing_api:epoll
atomicvar_api:atomic-builtin
gcc_version:9.3.0
process_id:751
```

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

-h

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

info

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

5.0.7

```
┌─[us-starting-point-2-dhcp]─[10.10.14.45]─[blackdogg@htb-j2kdelqeo1-htb-cloud
om]─[~]
└──[★]$ nmap -A -sV -sC 10.129.106.77 -p 6379
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-22 10:57 CST
Nmap scan report for 10.129.106.77
Host is up (0.30s latency).

PORT     STATE SERVICE VERSION
6379/tcp open  redis   Redis key-value store 5.0.7
Warning: OSScan results may be unreliable because we could not find at least 1
pen and 1 closed port
Aggressive OS guesses: Linux 4.15 - 5.8 (96%), Linux 5.3 - 5.4 (95%), Linux 2.
32 (95%), Linux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A o
211 Network Camera (Linux 2.6.17) (95%), ASUS RT-N56U WAP (Linux 3.4) (93%), L
ux 3.16 (93%), Linux 5.0 - 5.4 (93%)
No exact OS matches for host (test conditions non-ideal).
```

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

SELECT

To select a specific database in Redis from the command line, you use the `SELECT` command followed by the database's zero-based index (e.g., `SELECT 1`), or you can specify the database number directly with `redis-cli` using the `-n <dbnum>` flag or a URI with `/dbnum`, like `redis-cli -n 1` or `redis-cli -u redis://host:port/1` to switch to database 1. 🔗

Using `SELECT` command

- **Syntax:** `SELECT <index>`.
- **Example:** To switch to the second database (index 1): 🔗

```
Code                                            ⧉

    SELECT 1
```

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

4

```
repl_backlog_active:0
repl_backlog_size:1048576
repl_backlog_first_byte_offset:0
repl_backlog_histlen:0

# CPU
used_cpu_sys:1.337198
used_cpu_user:1.280444
used_cpu_sys_children:0.001992
used_cpu_user_children:0.000000

# Cluster
cluster_enabled:0

# Keyspace
db0:keys=4,expires=0,avg_ttl=0
10.129.106.77:6379>
```

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

KEYS *

```
10.129.106.77:6379> KEYS *
1) "temp"
2) "stor"
3) "numb"
4) "flag"
10.129.106.77:6379>
```

Redis

For Redis, you can use the `KEYS *` command. 🔗

- `KEYS *` : This command returns all keys in the currently selected database. 🔗

Warning: The `KEYS` command can block the server for a long time if you have a large number of keys and should be used with extreme care in production environments. A more efficient, non-blocking alternative for production is the `SCAN 0` command, which allows for incremental iteration over the keys. 🔗

FLAG.txt

```
10.10.10.127:6379> get numb
"bb2c8a7506ee45cc981eb88bb81dddab"

10.10.10.127:6379> get flag
"03e1d2b376c37ab3f5319922053953eb"
```

"03e1d2b376c37ab3f5319922053953eb"