# 🐾 Redeemer Write-up

**Prepared by:** dotguy

---

# 📌 Introduction

Databases store organized information that can be easily accessed, updated, and managed. They are critical in most systems because they handle:

- Sales transactions
- Product inventory
- Customer profiles
- Marketing data

**Redis** is a special type of database called an **in-memory database**, which means it primarily stores data in **RAM** for faster access.

- Frequently requested data can be cached in Redis for **quick retrieval**.
- Data can also be written to disk for **backup and persistence**.
- This setup allows websites and applications to handle high traffic efficiently while keeping long-term storage stable.

**Objective of this lab:**

- Learn how to **enumerate a Redis server** remotely
- Retrieve data from the database using **redis-cli**
- Understand basic Redis commands and penetration testing methodology

---

# Enumeration

## 1□.Verify Connectivity

Before interacting with the server, check if the target machine is reachable:

```
ping {TARGET_IP}
```

- Two successful replies are sufficient to confirm the connection.
- Short checks are often enough; long-running commands aren’t always necessary.

## 2□.Scan for Open Ports

Use **Nmap** to discover open ports and running services:

```
nmap -sV {TARGET_IP}
```

- Found **port 6379 (Redis)** open → primary entry point for the lab.

---

# 🛠 Understanding Redis

**Redis (REmote DIctionary Server)** is a key-value store used as a database, cache, or message broker.

**Key Features:**

- Stores data in **RAM** for fast access ⚡
- Short-term storage with optional disk backup 💾
- Data organized in **key-value pairs**

**Server and CLI:**

- Redis server listens for connections
- **redis-cli** allows full interaction with the database
- Essential for enumeration, testing, and automation

---

# 💻 Installing and Using redis-cli

Install **redis-cli**:

```
sudo apt install redis-tools
redis-cli -h {TARGET_IP}
```

- Alternatively, you can use **netcat**, but redis-cli is easier.
- Check available options:

```
redis-cli --help
```

**Common Commands:**

- `info` → Show server statistics
- `select <db>` → Switch to a specific database
- `keys *` → List all keys in the database
- `get <key>` → Retrieve the value of a key

**Pro Tip:** Always explore the CLI first to understand available tools and options.

---

# 🔍 Enumerating Redis Server

1. **View server info:**

```
info
```

2. **Select a database (default is 0):**

```
select 0
```

3. **List all keys:**

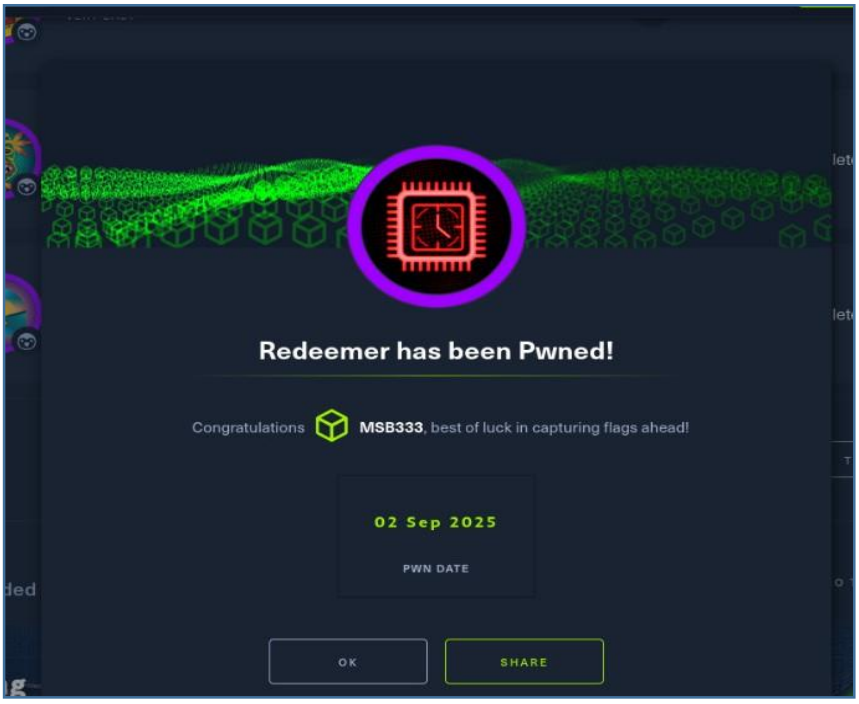
```
keys *
```

4. **Get value of a key:**

```
get <key>
```

- Successfully retrieving the key gives the **flag** ✓

Careful exploration ensures you don’t miss any critical data or attack vectors.




---

# 📝 Key Takeaways

- Understand the technology **before exploiting** it.
- Enumeration, scanning, and CLI tools **work together** in penetration testing.
- Methodical exploration reveals sensitive data efficiently.
- Research, observation, and structured methodology are **more important than speed**.