

## REDDICT WRITE-UP

Merhaba arkadaşlar. Bugün sizlerle Hackviser platformunda bulunan Reddict adlı Warmup' ını yazacağım.

**SORU 1:** Hangi portlar açık?

Burada yeni bulduğum threader3000 aracını kullanacağım. Threader 3000 aracı sadece açık portları bulmak için geliştirilmiş bir tool'dur. [Buradan](#) detaylı inceleyip kullanabilirsiniz.

```
(root@kali)-[/home/kali/Desktop/threader3000]
# python3 threader3000.py

Threader 3000 - Multi-threaded Port Scanner
Version 1.0.7
A project by The Mayor

Enter your target IP address or URL here: 172.20.8.189

Scanning target 172.20.8.189
Time started: 2024-11-26 15:44:12.287525

Port 6379 is open
Port scan completed in 0:00:56.848617
```

Cevap: **6379**

**SORU 2:** Çalışan Redis servisinin versiyonu nedir?

Bu durumda nmap aracı ile sadece port belirterek versiyon taraması yapacağım.

```
(root@kali)-[/tmp]
# nmap -sV -p 6379 172.20.8.189
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-26 15:47 +03
Nmap scan report for 172.20.8.189
Host is up (0.072s latency).

PORT      STATE SERVICE VERSION
6379/tcp  open  redis   Redis key-value store 6.0.16
```

Cevap: **6.0.16**

**SORU 3:** Redis ile bağlantı kurmanızı sağlayan komut satırı programı nedir?

Bu sorunun cevabı redis'in kendisine ait olan **redis-cli** komutudur.

**SORU 4:** Başarılı bir bağlantı kurulduktan sonra PING komutu çalıştırıldığında ne yanıt verir?

Öncelikle redis-cli ile bağlantı sağlamamız gerekiyor. -h ile host -p ile port belirtip bağlanıyoruz.

```
(root@kali)-[/tmp]
# redis-cli -h 172.20.8.189 -p 6379
172.20.8.189:6379> PING
PONG
172.20.8.189:6379> █
```

Cevap: **PONG**

**SORU 5:** Hangi komut sunucu hakkında bilgi ve istatistikleri döndürür?

<https://redis.io/docs/latest/develop/tools/cli/> Sitesinin içinde bu sorunun cevabının **INFO** olduğunu bulduk.

**SORU 6:** Hangi komut tüm anahtarları(keys) döndürür?

<https://redis.io/docs/latest/commands/keys/> redis'in keyler için olan dokümanında bulunuyor.

Cevap: **keys \***

**SORU 7:** Kaç tane anahtar-değer çifti var?

```
172.20.8.189:6379> keys *
1) "session:user-992"
2) "session:user-310"
3) "session:user-569"
4) "session:admin-001"
5) "session:user-230"
6) "session:user-552"
7) "session:user-800"
8) "session:user-822"
9) "session:user-111"
10) "session:user-893"
11) "session:user-878"
172.20.8.189:6379> █
```

CEVAP: **11**

**SORU 8:** Hangi komut anahtarın(key) değerini döndürür?

Bu sorunun cevabını bulmak için Google arama motoruna yazınca cevabın direkt

**GET** olduğunu buluyoruz.

**SORU 9:** Admin'in sessionToken değeri nedir?

```
172.20.8.189:6379> get session:admin-001
"{\"userID\": \"001\", \"lastLogin\": \"2023-12-10T10:10:01\", \"sessionToken\": \"iqtogggtry\", \"isLoggedIn\": true}"
```

Burada cevabın **"iqtogggtry"** olduğunu bulduk.