**🧠 1. CrackQ Nedir?**

**CrackQ**, popüler parola kırma aracı **Hashcat** için geliştirilmiş **web tabanlı bir yönetim ve izleme arayüzüdür**.

📌 Temel özellikleri:

* Hashcat işlerini web üzerinden yönetme
* GPU hızlandırma desteği
* Otomatik wordlist ve mask attack seçenekleri
* İş durumu, hız, kalan süre gibi bilgileri anlık izleme

**🎯 2. Ne İşe Yarar?**

| **Özellik** | **Açıklama** |
| --- | --- |
| 🌐 Web arayüz | Tarayıcı üzerinden Hashcat çalıştırma |
| 🖥️ GPU optimizasyonu | NVIDIA / AMD GPU’lar ile yüksek hız |
| 📄 Çoklu hash desteği | MD5, SHA1, NTLM, bcrypt vb. |
| 🛠️ Saldırı türleri | Dictionary, mask, kombinasyon, hybrid |
| 📊 Raporlama | Kırılan hash sayısı, kalan süre tahmini |

**⚙️ 3. Kurulum (Kali / Linux)**

**✅ 1. Gerekli bağımlılıkları yükle:**

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**✅ 2. CrackQ’yu indir:**

**metin, ekran görüntüsü, yazı tipi, grafik içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.**

**✅ 3. Web arayüzünü başlat:**

python3 crackq.py

Varsayılan olarak [**http://localhost:5000**](http://localhost:5000) adresinden erişilir.

**🚀 4. Kullanım**

**✅ 1. Hash yükleme:**

* Web arayüzünden **Add Job** seçeneği ile hash dosyası yüklenir.

**✅ 2. Saldırı yöntemi seçme:**

* **Dictionary Attack**: Wordlist ile deneme
* **Mask Attack**: Belirli karakter deseni ile brute force
* **Hybrid Attack**: Wordlist + mask kombinasyonu

**✅ 3. Saldırıyı başlatma:**

* GPU seçilir, Hashcat parametreleri ayarlanır ve “Start” butonu ile çalıştırılır.

**✅ 4. Sonuçları görüntüleme:**

* Kırılan hash’ler tabloda listelenir.
* Rapor JSON veya TXT olarak indirilebilir.

**📋 5. Örnek Terminal/Web Arayüz Çıktısı**

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

💻 Web Arayüzünde:

* **Progress Bar** ile işlem ilerleme durumu
* Kırılan şifrelerin listesi
* GPU kullanım grafikleri

**🧠 6. Desteklenen Hash Türleri**

* MD5
* SHA1 / SHA256 / SHA512
* NTLM
* bcrypt
* LM Hash
* MySQL Hash
* Wordpress Hash

**🧪 7. Kullanım Senaryoları**

| **Senaryo** | **Açıklama** |
| --- | --- |
| 🧠 Adli bilişim | Unutulan şifreleri kurtarma |
| 🔍 Penetrasyon testi | Hash dump sonrası parola kırma |
| 🛡️ Red Team hazırlığı | Kırılan şifrelerin yeniden kullanımını test etme |
| 📊 Kurumsal güvenlik denetimi | Parola politikalarının sağlamlığını ölçme |

**🎯 8. Öğrenim Kazanımları**

* Hashcat’in web arayüzünden yönetimini öğrenme
* GPU hızlandırmalı parola kırma mantığını kavrama
* Dictionary, mask, hybrid saldırı tekniklerini uygulamalı öğrenme
* Hash türleri ve zorluk seviyeleri hakkında pratik bilgi edinme