**Rengine Nedir?**

Rengine (Reconnaissance Engine), açık kaynaklı, web tabanlı bir bilgi toplama (OSINT) platformudur. Hedef domain (alan adı) üzerinden kapsamlı bilgi toplamak için kullanılır ve kullanıcı dostu bir web arayüzü sunar. Özellikle siber güvenlik öğrencileri, bilgi güvenliği uzmanları ve CTF katılımcıları için oldukça kullanışlıdır.

Python ile yazılmış olan bu araç, çeşitli alt modüllerle alt alan adı keşfi, port tarama, whois analizi, e-posta toplama, DNS kayıtları ve daha fazlasını tek bir arayüzden yapmaya imkân tanır.

**Rengine Ne İşe Yarar?**

* Alan adı üzerinden alt alan adlarını toplar.
* Whois bilgilerini listeler.
* DNS kayıtlarını analiz eder (A, MX, TXT, NS vs.).
* Açık portları ve çalışan servisleri tespit eder.
* Teknoloji yığını (web server, JS framework) tanımlar.
* Google Dork’ları ile gelişmiş aramalar yapar.
* OSINT verilerini merkezi bir arayüzde toplar.

**Kurulum:**

Kali Linux / Ubuntu

***git clone https://github.com/yogeshojha/rengine***

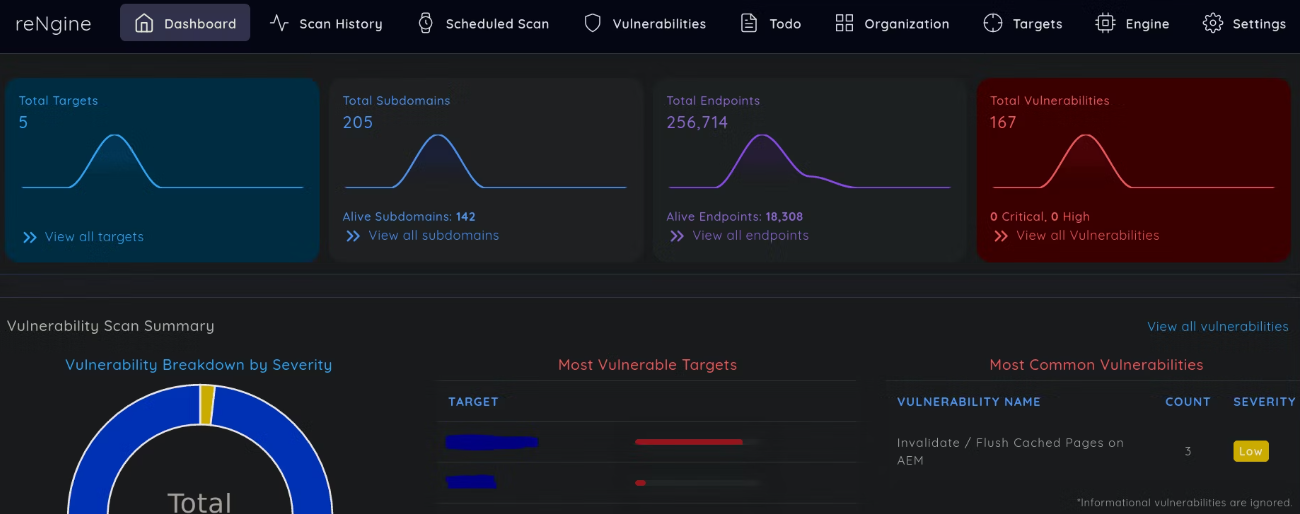
***cd rengine***

***./install.sh***

Kurulumdan sonra web arayüzü varsayılan olarak http://127.0.0.1 üzerinden çalışır.

**Kullanım Arayüzü**

1. Web arayüzü üzerinden hedef domain girilir.
2. "New Scan" sekmesi ile bilgi toplama başlatılır.
3. Sonuçlar tablolar ve grafikler şeklinde kullanıcıya sunulur.



Bu görsel; temel ölçümler, grafikler, ayrı paneller ve kullanıcı arayüzü gibi dashboard bileşenlerini içeriyor.

**Eğitim Notları**

Rengine, farklı bilgi toplama araçlarını tek bir çatı altında birleştirerek, manuel işlem yükünü azaltır. Özellikle web tabanlı arayüzü, öğrencilerin siber güvenlik testlerine görsel ve sezgisel bir şekilde yaklaşmalarını sağlar. Rengine’in raporlama özelliği ile elde edilen bilgiler dışa aktarılabilir ve ileri analizler için kullanılabilir.

Kapsamlı bilgi toplama işlemlerinde, Nmap, Amass, theHarvester gibi araçlarla birlikte kullanıldığında çok güçlü sonuçlar üretir.

Rengine, sadece bilgi toplamakla kalmaz, aynı zamanda toplanan verileri analiz etmek ve yorumlamak için de görsel bir ortam sunar. Alt alan adı haritalama, DNS çözümleme ve port tarama gibi modüller sayesinde hedef sistem hakkında detaylı bir saldırı yüzeyi haritası çıkartmak mümkündür. Özellikle güvenlik testlerinin hazırlık aşamasında kullanıldığında, saldırı yüzeyini doğru tanımlamak ve zaman kazanmak açısından büyük avantaj sağlar.

Ayrıca Rengine’in modüler yapısı sayesinde yeni araçlar ve API servisleri entegre edilebilir. Bu da aracı sadece pasif bilgi toplama için değil, aynı zamanda gelişmiş keşif (recon) operasyonları için de uygun hale getirir. Otomasyon yetenekleri ve geniş raporlama desteğiyle, öğrencilerin hem pratik yapmasını hem de gerçek sızma testi senaryolarını anlamasını kolaylaştırır.