**🧠 1. Bu Araç Nedir?**

**bypass-firewalls-by-DNS-history**, bir web sitesinin geçmiş DNS kayıtlarını inceleyerek, **güvenlik duvarı arkasına alınmadan önce kullanılan IP adreslerini** tespit eden bir OSINT aracıdır.

* CDN (Cloudflare, Akamai vb.) veya WAF (Web Application Firewall) arkasındaki gerçek IP adreslerini bulmaya yarar
* Passive DNS (pDNS) verilerini kullanır
* Web arayüzü ya da terminal üzerinden çalışabilir

📌 Temel amaç: **Doğrudan erişilebilen eski IP adreslerini bulup, güvenlik önlemlerini atlamak**

**🎯 2. Ne İşe Yarar?**

| **Özellik** | **Açıklama** |
| --- | --- |
| 🔍 Passive DNS sorgusu | Alan adının eski IP kayıtlarını bulur |
| 🛠️ WAF/CDN bypass | Gerçek IP adresine doğrudan erişim sağlama |
| 📊 Zaman damgalı DNS kayıtları | IP değişim geçmişini gösterir |
| 🧪 Güvenlik testi | Web uygulama güvenlik duvarı atlatma senaryoları |

**⚙️ 3. Kurulum (Kali / Linux)**

**✅ 1. GitHub’dan indirme:**

ekran görüntüsü, yazı tipi, metin içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.**✅ 2. Python bağımlılıklarını yükleme:**

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🚀 4. Kullanım Komutları**

**✅ 1. Tek domain sorgulama:**

python3 bypass-firewalls-by-DNS-history.py example.com

**✅ 2. Domain listesi ile sorgulama:**

python3 bypass-firewalls-by-DNS-history.py -l domains.txt

**✅ 3. Sonuçları dosyaya kaydetme:**

python3 bypass-firewalls-by-DNS-history.py example.com -o result.txt

**📋 5. Örnek Terminal Çıktısı**

metin, ekran görüntüsü, yazı tipi, ekran, görüntüleme içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🧠 6. Kullanım Senaryoları**

| **Senaryo** | **Açıklama** |
| --- | --- |
| 🧠 Red Team keşfi | Gerçek IP’yi bulup WAF atlatma |
| 🛡️ Blue Team güvenlik testi | Eski IP’lerin hala erişilebilir olup olmadığını kontrol etme |
| 🔍 OSINT araştırması | DNS kayıt geçmişinden bilgi toplama |
| 🧪 Penetrasyon testi | Engellenmiş servisleri eski IP üzerinden test etme |

**🎯 7. Öğrenim Kazanımları**

* Passive DNS kavramını ve kullanımını öğrenme
* WAF/CDN atlatma mantığını kavrama
* Eski IP adreslerinin güvenlik risklerini anlama
* OSINT araçlarının pasif bilgi toplamada nasıl kullanıldığını öğrenme