**🧠 1. Sn1per Nedir?**

**Sn1per**, hedef sistemler üzerinde bilgi toplamak, port taraması yapmak, servis bilgilerini analiz etmek ve bilinen güvenlik açıklarını taramak için kullanılan **hepsi bir arada (all-in-one) bir sızma testi (pentest) aracıdır**.

📌 Geliştirici: 1N3  
📌 Kullanım Amacı: Recon + Port tarama + Zafiyet Tespiti + Raporlama

**🛠️ 2. Sn1per Ne İşe Yarar?**

| **Özellik** | **Açıklama** |
| --- | --- |
| 🌐 Hedef hakkında bilgi toplar | WHOIS, DNS, subdomain, IP, servis bilgileri |
| 🔍 Otomatik port taraması | Nmap ile TCP/UDP servislerini tespit eder |
| 🛡️ Zafiyet taraması | Nikto, Nmap Scripting Engine, SSLScan vb. entegredir |
| 🧠 CMS tanıma + directory brute | Web uygulamalarını analiz eder |
| 📊 Raporlama ve çıktı alma | HTML ve text formatında raporlar oluşturur |

**⚙️ 3. Kurulum (Kali Linux)**

**✅ 1. Gerekli paketleri yükle:**

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**✅ 2. Sn1per’ı indir ve kur:**

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🚀 4. Kullanım Modları**

Sn1per birden fazla mod içerir:

| **Mod** | **Açıklama** |
| --- | --- |
| normal | Temel bilgi toplama (pasif tarama) |
| recon | WHOIS, subdomain, DNS, servis bilgileri |
| full | Tüm modlar + zafiyet taramaları |
| web | Web uygulaması testleri (dirb, CMS tespiti, nikto) |
| stealth | Sessiz/pasif tarama (detection riskine karşı) |
| airstrike | Çoklu hedefleri otomatik olarak tarar |

**💻 5. Kullanım Örnekleri**

**✅ Temel kullanım:**

sniper -t https://targetsite.com -m normal

**✅ Tüm detaylı taramaları çalıştır:**

sniper -t https://targetsite.com -m full

**✅ Belirli IP aralığında otomatik tarama:**

sniper -f targets.txt -m airstrike

**✅ Web uygulaması odaklı test:**

sniper -t http://example.com -m web

**📋 6. Örnek Terminal Çıktısı**metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

| **Araç** | **Görevi** |
| --- | --- |
| **🔍 Nmap** | **Port ve servis tarama** |
| **🛡️ Nikto** | **Web zafiyet tarayıcısı** |
| **🌐 WhatWeb** | **Web teknolojisi tanıma** |
| **🧱 WAFW00F** | **Web Application Firewall tespiti** |
| **📁 Dirb / Gobuster** | **Dizin/brute-force taraması** |
| **🔐 SSLScan** | **SSL/TLS yapılandırma analizi** |

**📊 8. Çıktılar ve Raporlar**

* **loot/ klasörü altında hedefe özel klasör açılır**
* **HTML ve TXT raporlar otomatik olarak oraya kaydedilir**
* **Her tarama çıktısı ayrı ayrı klasörlerde tutulur**

**🎯 9. Öğrenim Kazanımları**

* **Otomatik bilgi toplama süreçlerini öğrenme**
* **Web uygulaması ve servis keşfi yapma becerisi kazanma**
* **Zafiyet tarayıcılarının nasıl entegre çalıştığını anlama**
* **Red Team operasyonları için hedef analizi gerçekleştirme**
* **Terminal tabanlı rapor üretimi ve çıktı incelemesi yapma**