

Shodan.io ile Global Cihaz Keşfi ve Güvenlik Risk Analizi

1. Giriş

Bu rapor, Shodan.io API'si kullanılarak yapılan küresel ağ taramaları ve güvenlik analizlerini ele almaktadır. Proje kapsamı

2. Shodan.io Nedir?

Shodan, internet üzerindeki bazı cihazları indeksleyen bir arama motorudur. Google'dan farklı olarak içerik değil, cihazları

3. Kullanılan Yöntemler

API kimlik doğrulaması ile filtreli sorgular çalıştırılmıştır. Örneğin, "org:'Turk Telekom' port:22 country:'TR'" gibi sorgular

4. Kod Modülleri

- shodanapp.py: Temel API istemcisi
- shodan_ip_details.py: Belirli IP hakkında detaylı analiz
- veri_isleme.py: Ham verilerin temizlenmesi
- çıktı_formatlama.py: JSON ve CSV'de aktarım
- CLI Arayüz: Komut satırından otomatik sorgu ve çıktı alma

5. Çıktı Formatları

Ham veriler JSON ve CSV formatında çıktıya aktarılmıştır. Bu sayede veriler hem okunabilir hem de analiz edilebilir.

6. Karşılaşılan Zorluklar

API sorgu limitleri nedeniyle işlem süresi yavaşlamıştır. Bu problem, sorgular arasında gecikme (sleep) eklenerek ve filtre

7. Güvenlik Analizi

Shodan çıktılarındaki açık bırakılmış kamera sistemleri, FTP sunucuları ve kontrol panelleri tespit edilmiştir. Özellikle

8. Sonuç ve Öneriler

Shodan, sızma testi öncesi hedef keşfi aşamasında güçlü bir kaynaktır. Cihazların filtrelenmesi ve çıktıların yapılandırılması

9. Ek: Kod ve Sorgular

- API Kullanımı: shodan.Shodan(api_key)
- Örnek Sorgu: api.search("port:21 Anonymous")
- Komut Satırı: python3 shodanapp.py --query 'port:80 country:TR' --output results.json