**🧠 1. S3scanner Nedir?**

**S3scanner**, Amazon Web Services (AWS) altyapısında kullanılan **S3 bucket** servislerini tarayan, erişim durumlarını analiz eden bir siber güvenlik aracıdır.

📌 Hedef:

* Açık bırakılmış S3 bucket’larını bulmak
* Hangi bucket’ların public/read/list erişime sahip olduğunu tespit etmek
* Potansiyel veri sızıntılarını önceden belirlemek

**🎯 2. Ne İşe Yarar?**

| **Özellik** | **Açıklama** |
| --- | --- |
| 🔍 S3 bucket keşfi | Belirli adlara göre bucket’ları arar |
| 🔓 Erişim durumunu kontrol eder | Public olarak listelenebilir mi? Okunabilir mi? |
| 🧪 Bilgi sızıntılarını tespit eder | Açık dosya listeleri, yedekler, .env, config dosyaları |
| 📁 Dosya listelemesi yapar | “list” izni açık olan bucket’larda tüm dosyaları gösterir |
| 📦 AWS yapılandırma denetimi | Geliştirici hataları ve ihmal edilen izinler tespit edilir |

**⚙️ 3. Kurulum (Kali / Linux)**

**✅ 1. Python 3 ve pip kurulu olmalı:**

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**✅ 2. S3scanner’ı yükle:**

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

Alternatif olarak:

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🚀 4. Kullanım Komutları**

**✅ 1. Tek bir bucket adı kontrol et:**

s3scanner example-bucket

**✅ 2. Dosyadan çoklu bucket kontrolü yap:**

s3scanner buckets.txt

buckets.txt içeriği:

example-bucket

dev-files

media-assets

company-backup

**✅ 3. Erişim durumunu detaylı göster:**

s3scanner --include-contents buckets.txt

**✅ 4. JSON çıktısı al:**

s3scanner --json buckets.txt > results.json

**📋 5. Örnek Terminal Çıktısı**

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.**

**🧠 6. S3 Bucket Erişim Türleri**

| **Durum** | **Açıklama** |
| --- | --- |
| ✅ Public Read | Herkes dosyaları görebilir |
| ⚠️ Listable | Herkes dosya listesini görebilir |
| ❌ Private | Sadece sahip yetkisi olan erişebilir |
| ❌ AccessDenied | Varlığı bilinse bile içerik görülemez |

**🧪 7. Kullanım Senaryoları**

| **Senaryo** | **Açıklama** |
| --- | --- |
| 🔎 OSINT / Recon | Şirket, kurum veya kullanıcıya ait açık bucket tespiti |
| 📦 Red Team / saldırı simülasyonu | Hatalı yapılandırılmış cloud verilerini kullanmak |
| 🛡️ Blue Team / güvenlik denetimi | Kurum içi AWS yapılandırma kontrolleri |
| 🧾 Güvenlik raporlaması | Riskli S3 örneklerinin listelenmesi ve düzeltme önerisi |

**🎯 8. Öğrenim Kazanımları**

* Cloud güvenliğinde S3 yapılandırmalarının önemini kavrama
* Açık bucket tespiti, veri sızıntısı ve yetkilendirme hatalarını tanıma
* Python tabanlı tarama araçlarıyla terminal üzerinden analiz yapma
* Kurumsal cloud mimarisinde denetim süreçlerine hakimiyet
* JSON çıktılarla rapor üretme ve otomasyon becerisi