LeakLooker Aracı Nedir ve Ne İşe Yarar?

LeakLooker, bulut ortamlarında güvenlik açığı oluşturabilecek şekilde yanlış yapılandırılmış ve herkese açık bırakılmış veri depolarını (bucket) tespit etmek için kullanılan açık kaynaklı bir Python aracıdır. Bu araç; Amazon S3, Google Cloud Storage ve Azure Blob gibi yaygın platformlarda tarama yapabilir.

Ne Yapar?

Bulut servislerinde açık bırakılmış veri havuzlarını bulur.

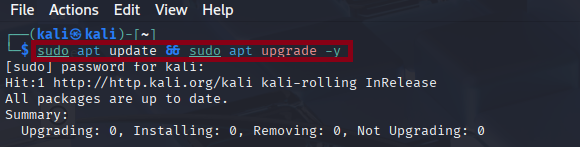
İçerik listesi, izin durumu gibi bilgiler verir.

Siber güvenlik uzmanları bu aracı footprinting veya sızma testi öncesi keşif aşamasında kullanır.

Kali Linux’ta LeakLooker Kurulumu

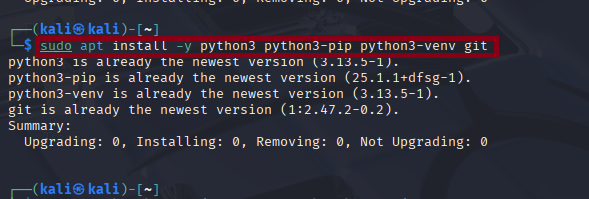
Adım 1: Sistem Güncellemeleri

sudo apt update && sudo apt upgrade -y



Şekil -Kali Linux'ta sistem güncellemeleri

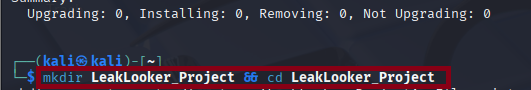
sudo apt install -y python3 python3-pip python3-venv git



Şekil Kali Linux'ta LeakLooker için gerekli araçların kurulumu.

Adım 2: Proje Klasörü Oluşturma

mkdir LeakLooker\_Project && cd LeakLooker\_Project



Şekil -LeakLooker için proje klasörü oluşturulması ve klasöre geçilmesi.

Adım 3: Sanal Ortam Kurulumu

Sanal Ortam Nedir ve Neden Kullanılır?

Python'da çalışırken her projenin ihtiyaç duyduğu kütüphaneler farklı olabilir. Sanal ortam (virtual environment), her proje için izole bir Python çalışma alanı sağlar. Böylece:

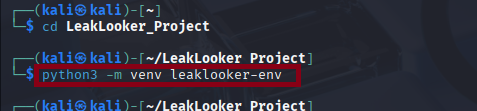
Başka projelerle kütüphane çakışması yaşamazsınız.

Sistemin genel Python kurulumuna müdahale etmeden çalışırsınız.

Projeyi taşırken (başka bir makineye aktarırken) hangi kütüphanelerin kullanıldığını kolayca belirleyebilirsiniz.

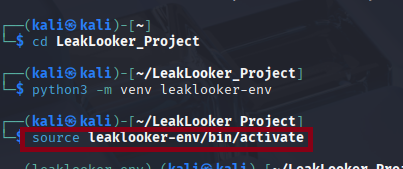
Özellikle sızma testlerinde kullanılan araçların versiyonları hassas olduğundan, sanal ortamda çalışmak en güvenli yoldur.

python3 -m venv leaklooker-env



Şekil -Python sanal ortamın oluşturulması.

source leaklooker-env/bin/activate # Sanal ortamı etkinleştir

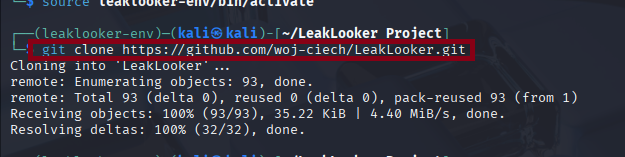


Şekil -Sanal ortam oluşturulduktan sonra aktif hale getirilmiş hali.

Not: Artık terminalinizde (leaklooker-env) ön eki görünecek

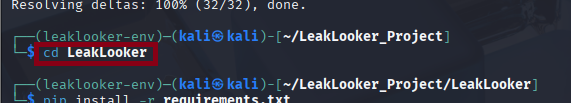
Adım 4: LeakLooker'ı İndirme

git clone <https://github.com/woj-ciech/LeakLooker.git>



Şekil -LeakLooker projesinin GitHub üzerinden klonlanması.

cd LeakLooker

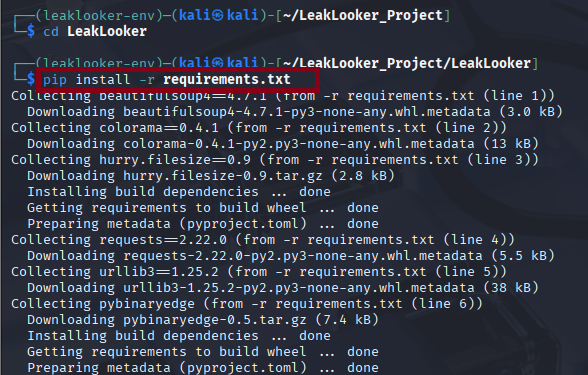


Şekil -Klasöre geçiş.

Adım 5: Gereksinimleri Yükleme

pip install -r requirements.txt

Bu komut, proje için gerekli Python kütüphanelerini kurar



Şekil -LeakLooker'ın ihtiyaç duyduğu Python paketlerinin yüklenmesi.

Kullanım Örnekleri

# Tekli tarama

python3 leaklooker.py -t "hedef\_kelime"

# Toplu tarama

python3 leaklooker.py -t targets.txt

# JSON çıktısı alma

python3 leaklooker.py -t "confidential" --json results.json

#Şirket Veri Sızıntısı Kontrolü

python3 leaklooker.py -t "sirketimiz" --json sirket\_audit.json

Yasal Uyumluluk İçin

* Mutlaka yazılı izin alın.
* Sadece test yetkiniz olan sistemleri tarayın.
* Bulduğunuz açıkları sorumlu şekilde bildirin.