**Drozer**, Android uygulamalarını analiz etmek, güvenlik açıklarını tespit etmek ve Android işletim sisteminde kötüye kullanılabilecek yapılandırma sorunlarını bulmak için kullanılan **mobil güvenlik test framework’üdür**.

Python tabanlıdır ve hem cihaz üzerinde **agent** olarak çalışır hem de Kali Linux üzerinde **komut satırı istemcisi** ile yönetilir.

**Bu Aracın Özellikleri**

* Android uygulama paketleri (**APK**) üzerinde statik ve dinamik analiz
* **IPC (Inter-Process Communication)** bileşenleri test etme (Activity, Service, BroadcastReceiver, ContentProvider)
* Hassas izinleri ve verileri kontrol etme
* Cihaz üzerinde doğrudan güvenlik testleri gerçekleştirme
* Modüler yapıda komutlar ile geniş analiz yeteneği

**Kali Linux Üzerinde Drozer Kurulumu ve Kullanımı**

**Adım 1: Drozer’ı Kur**

Drozer, Kali deposunda bulunmaz; doğrudan kaynak kod veya paket üzerinden kurulur.

“sudo apt update”

“sudo apt install openjdk-11-jdk python3-pip adb -y”

“pip3 install drozer”

**Adım 2: Android Cihaz Bağlantısını Hazırla**

Cihazda **USB hata ayıklama (USB Debugging)** açık olmalı.

“adb devices”

**Adım 3: Drozer Agent APK’sini Cihaza Yükle**

Drozer agent APK’si resmi GitHub sayfasından veya Drozer paketinden alınır.

“adb install drozer-agent.apk”

**Adım 4: Cihaz Üzerinde Agent’ı Başlat**

Telefon veya emülatörde Drozer Agent uygulamasını aç, **“Embedded Server”** modunu etkinleştir.

**Adım 5: Kali’den Drozer İstemcisine Bağlan**

Drozer, TCP 31415 portundan haberleşir.

“drozer console connect --server 127.0.0.1”

**Adım 6: Örnek Bir Uygulama Analizi**

“dz> run app.package.list”

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

Açıklama otomatik olarak oluşturuldu

“dz> run app.activity.info -a com.vulnerable.app”

**Adım 7: İçerik Sağlayıcı Testi (Content Provider)**

“dz> run scanner.provider.finduris -a com.vulnerable.app”

