**OSQuery Nedir?**

**osquery**, sistem bilgilerini SQL sorguları ile analiz etmeye yarayan açık kaynaklı bir güvenlik aracıdır. Facebook tarafından geliştirilmiştir. Sistem yöneticileri ve güvenlik uzmanları için tehdit tespiti, analiz ve izleme amacıyla kullanılır.

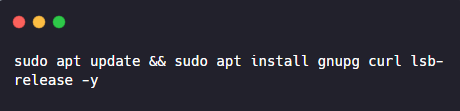
**Özellikleri:**

* SQL sorguları ile sistem bilgilerine ulaşma
* Aktif süreçleri, kullanıcıları, ağ bağlantılarını analiz etme
* Dosya bütünlüğü kontrolü
* Uyumluluk denetimleri (CIS, PCI-DSS)
* Dağıtık yapı desteği (Fleet, Kolide vb.)
* Log toplama ve olay korelasyonu

**Kali Linux Üzerine OSQuery Kurulumu**

**1.Gerekli Bağımlılıkların Yüklenmesi-Komut:**

**sudo apt update && sudo apt install gnupg curl lsb-release -y**

****

**2. GPG Anahtarını Ekleyin-Komut: sudo mkdir -p /etc/apt/keyrings**

**curl -fsSL https://pkg.osquery.io/gpg.key | sudo gpg --dearmor -o /etc/apt/keyrings/osquery-archive-keyring.gpg**

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.**

**3. OSQuery Kaynağını APT’ye Ekleyin-Komut: echo 'deb [signed-by=/etc/apt/keyrings/osquery-archive-keyring.gpg] https://pkg.osquery.io/deb deb main' | sudo tee /etc/apt/sources.list.d/osquery.list**

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.**

**4. Paket Listesini Güncelleyin-Komut**: **sudo apt update**

ekran görüntüsü, grafik, tasarım içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**5. OSQuery’yi Yükleyin-Komut: sudo apt install osquery -y**

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.**

**6. Kurulum Sonrası Test-Komut: osqueryi**

**ekran görüntüsü, metin içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.**

**Örnek Sorgu ve Çıktısı**

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.**