# FalconHound Kurulum ve Kullanım Rehberi

## 1. Giriş

FalconHound, Active Directory ortamlarında saldırı yüzeylerini analiz etmek ve saldırı yollarını keşfetmek için kullanılan açık kaynaklı bir görselleştirme ve analiz aracıdır. BloodHound ile entegre çalışır ve daha hızlı, daha kullanıcı dostu bir deneyim sunar.

## 2. Gereksinimler

- Windows/Linux sistem  
- Neo4j Graph Database  
- BloodHound verisi (JSON formatında)  
- Python 3.8+  
- Node.js ve npm  
- Git

## 3. Kurulum Adımları

### 3.1 Neo4j Kurulumu

1. Neo4j Community Edition'ı https://neo4j.com/download/ adresinden indirin.  
2. Yönergelere uygun şekilde kurulum yapın.  
3. Neo4j web arayüzünden yeni bir veritabanı oluşturun.

### 3.2 FalconHound Kurulumu

git clone https://github.com/SpecterOps/FalconHound.git  
cd FalconHound  
npm install

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

### 3.3 Python Ortamının Ayarlanması

python -m venv venv  
source venv/bin/activate # Windows: venv\Scripts\activate  
pip install -r requirements.txt

ekran görüntüsü, metin, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

## 4. BloodHound Verilerinin Yüklenmesi

1. SharpHound ile toplanan JSON verilerini hazırlayın.  
2. Aşağıdaki komutla bu verileri Neo4j veritabanına yükleyin:  
  
python3 ingestor.py --folder ./data --neo4j-uri bolt://localhost:7687 --neo4j-user neo4j --neo4j-password yourpassword

ekran görüntüsü, metin, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

## 5. FalconHound Arayüzünü Başlatma

npm run dev  
  
Tarayıcınızda http://localhost:3000 adresine giderek FalconHound arayüzüne erişebilirsiniz.

## 6. Temel Kullanım

- Graph Arama: Belirli bir kullanıcı, grup veya bilgisayar ilişkilerini görselleştirin.  
- Query Builder: Özel sorgular oluşturarak saldırı yollarını analiz edin.  
- Path Finding: Admin erişimi gibi özel yolları otomatik olarak bulun.

## 7. Güvenlik ve Öneriler

- Parola korumalı Neo4j kullanın.  
- Veritabanınızı dış erişime kapatın.  
- Güncellemeleri düzenli kontrol edin.

## 8. Kaynaklar

- https://github.com/SpecterOps/FalconHound  
- https://github.com/BloodHoundAD/BloodHound  
- <https://neo4j.com>

Örnek Çıktı:

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.