LogonTracer - Eğitim Materyali

# 🔍 LogonTracer Nedir?

LogonTracer, Windows sistemlerinden elde edilen güvenlik olay günlüklerini (Security Event Log) görsel olarak analiz eden bir adli bilişim aracıdır.  
Özellikle Windows logon (oturum açma) olaylarının grafiksel olarak ilişkilendirilmesine olanak tanır.  
ElasticSearch ve Neo4j veritabanlarını kullanarak logların analizini gerçekleştirir.

# 🚀 Özellikleri

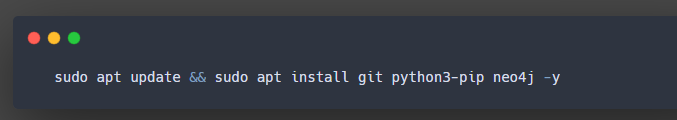
- Event ID 4624, 4625, 4768, 4769, 4776 gibi oturum olaylarını analiz eder.  
- Kullanıcı, bilgisayar ve logon ilişkilerini grafik olarak gösterir.  
- Neo4j veritabanı ile kullanıcı ilişkilerini sorgular.  
- ElasticSearch ile log indeksleme desteği.  
- Web tabanlı görsel arayüz.

# 📌 Kullanım Alanları

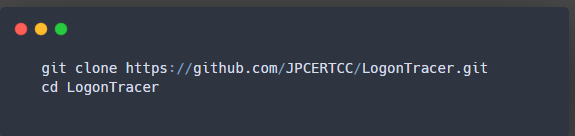
- Windows logon analizi  
- RDP brute force tespiti  
- Yanlış oturum açma denemeleri  
- Lateral movement (yatay hareket) analizi  
- SOC ve Blue Team eğitimleri

# 🛠️ Kurulum Adımları (Ubuntu/Kali)

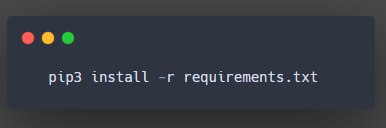
1. Gerekli paketleri yükleyin:

******

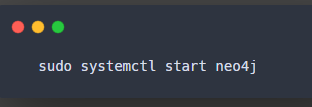
2. LogonTracer'ı klonlayın:

******

3. Python bağımlılıklarını yükleyin:

******

4. Neo4j servislerini başlatın:

******

5. Web arayüzünü çalıştırın:

# 

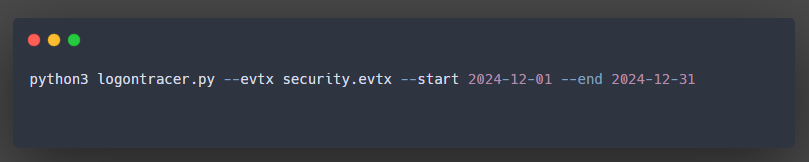
# 🌐 Web Arayüz

Web arayüzüne http://localhost:7474 adresinden erişilir.  
Varsayılan Neo4j kullanıcı adı: neo4j   
İlk girişte sizden yeni parola belirlemeniz istenebilir.

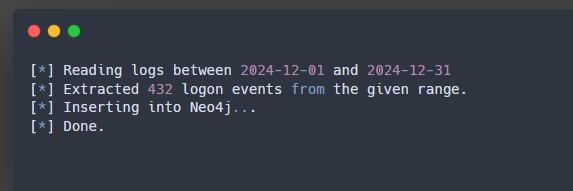
# 🧪 Örnek Kullanım Komutları ve Çıktılar

**✅ 1. Belirli Zaman Aralığında Olayları Analiz Etme**

**Komut:**

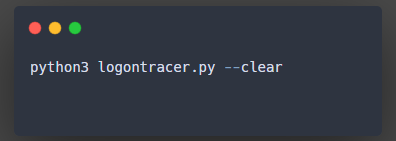


**Açıklama:**  
Sadece 1-31 Aralık 2024 tarihleri arasındaki log kayıtları işlenir. Bu, belirli bir olayla ilişkili dönemleri izlemek için kullanılır.

Çıktı: 

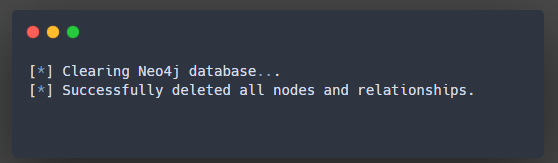
**✅ 2. Mevcut Neo4j Veritabanını Temizleme (yeni yükleme öncesi)**

**Komut:**



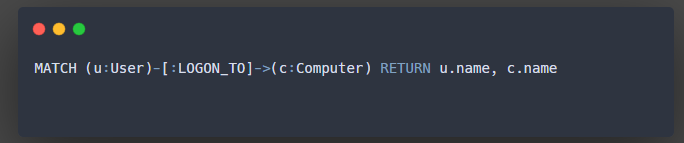
**Açıklama:**  
Tüm geçmiş analizleri ve veritabanındaki verileri siler. Yeni bir analiz başlatılacaksa tavsiye edilir.

Çıktı:



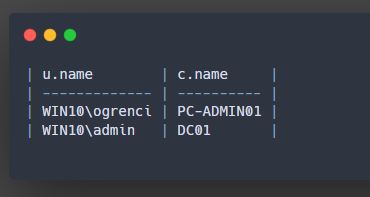
**✅ 3. Loglar yüklendikten sonra Neo4j UI üzerinden Cypher sorgusu örneği**

**Komut (Neo4j Arayüzünde):**



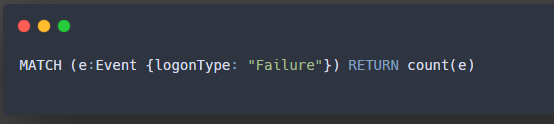
**Açıklama:**  
Hangi kullanıcı hangi bilgisayara giriş yapmış, tablo olarak gösterir.

Çıktı:

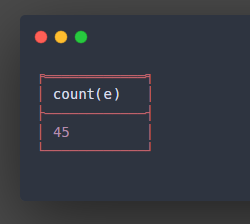


**✅ 4. Failed Login Sayısını Gösterme (Neo4j)**

**Cypher Sorgusu:**

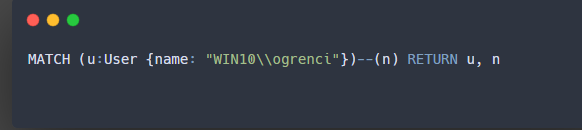


Çıktı:



**✅ 5. Belirli Kullanıcının Tüm Bağlantılarını Görme (Neo4j)**

**Komut:**



**Açıklama:**  
Bu kullanıcı ile ilişkili tüm düğümler (bilgisayar, olay vb.) grafikte listelenir.

# 📎 Notlar

- LogonTracer yoğun bellek kullanabilir, 4 GB+ RAM önerilir.  
- Neo4j ilk açıldığında şifre sıfırlama ekranı gösterebilir.  
- EVTX dosyaları Windows’tan alınmalıdır (Event Viewer > Save All Events As).