**BloodHound**, Active Directory (AD) ortamlarında **yetki yükseltme yollarını, ilişkileri ve hak zincirlerini görsel olarak analiz eden** açık kaynaklı bir güvenlik analiz aracıdır. Kırmızı takım (red team) ve mavi takım (blue team) tarafından hem saldırı hem savunma amacıyla kullanılır.

Graf tabanlı veri modeli kullanır ve saldırganın bir kullanıcıdan domain admin’e giden tüm yolları çıkarabilir.

**Bu Aracın Özellikleri Nelerdir?**

* **Active Directory haritalaması** (kullanıcı, grup, bilgisayar, ilişki)
* **Neo4j veritabanı altyapısı**
* **PowerShell, C#, Python destekli veri toplayıcılar**
* **Graph-based görselleştirme**
* **Custom sorgular (queries) ile analiz imkânı**
* **Yetki yükseltme yollarının otomatik gösterimi**

**BloodHound Aracını Kali Linux’ta Kurma ve Kullanma Adımları**

BloodHound 4 ana bileşenden oluşur:

1. Neo4j (graph veritabanı)
2. BloodHound GUI (Electron tabanlı uygulama)
3. SharpHound (veri toplayıcı)
4. JSON veri yükleme ve analiz

**Adım 1: Neo4j Veritabanını Kur**

“sudo apt update

sudo apt install neo4j -y”

**Adım 2: Neo4j Servisini Başlat**

“sudo neo4j console”

**Adım 3: BloodHound GUI’yi Kur ve Başlat**

“sudo apt install bloodhound -y”

“bloodhound”

metin, ekran görüntüsü, yazılım, multimedya yazılımı içeren bir resim

Açıklama otomatik olarak oluşturuldu

**Adım 4: Neo4j Arayüzüne Giriş ve Şifre Belirleme**

Tarayıcıdan şu adrese gir:

<http://localhost:7474>

İlk girişte:

* Username: neo4j
* Password: neo4j (değiştirmeniz istenir)

**Adım 5: SharpHound ile Veri Toplama**

**Komut (Windows sistemde PowerShell ile):**

“.\SharpHound.exe -c all”

metin, yazı tipi, ekran görüntüsü içeren bir resim

Açıklama otomatik olarak oluşturuldu

**Adım 6: Toplanan Veriyi BloodHound GUI’ye Yükle**

1. BloodHound arayüzünden “Upload Data”
2. 20250801\_Collection.zip dosyasını seç
3. JSON içeriği yüklenir ve graf oluşur

**Adım 7: Sorgulama ve Yükseltme Yolu Analizi**

Örnek sorgular:

* “Shortest path to Domain Admins”
* “Users with admin rights”
* “Kerberoastable users”