**BlueHound Nedir?**

BlueHound, **Blue Team** (savunma ekibi) için geliştirilmiş, saldırı yüzeyini analiz etmeye ve ağ üzerindeki tehditleri görselleştirmeye yarayan açık kaynaklı bir güvenlik aracıdır. Özellikle Active Directory (AD) ortamlarında potansiyel güvenlik açıklarını ve saldırganların kullanabileceği yolları tespit etmek için kullanılır.

Adını, saldırganlar için kullanılan **BloodHound** aracından alır. Ancak BlueHound, savunmacıların perspektifinden ağ haritalama ve analiz yapmalarına odaklanır.

**BlueHound’un Özellikleri**

* Active Directory yapılarını analiz eder.
* Saldırganların kullanabileceği saldırı yollarını ortaya çıkarır.
* Görselleştirme desteği ile ilişkileri ve zayıf noktaları gösterir.
* CSV ve JSON çıktılarıyla detaylı analiz yapılabilir.
* Blue Team uzmanlarının karar alma sürecini kolaylaştırır.

**Kullanım Alanları**

* Kurumsal ağlarda Active Directory güvenliğini test etmek
* Savunma amaçlı güvenlik zafiyetlerini haritalamak
* Penetrasyon testi sonrası savunma planı oluşturmak
* SOC (Security Operations Center) ekiplerinin analizleri

**Kimler Kullanmalı?**

* Blue Team (savunma ekipleri)
* Ağ güvenliği yöneticileri
* SOC ve SIEM analistleri
* Siber güvenlik eğitimi alan öğrenciler
* Active Directory yöneticileri

**Kurulum Aşaması** (Adım Adım)

**Not**: BlueHound bir betik (script) dizisidir. Genellikle Linux ortamında ya da WSL altında kullanılır. İşte temel kurulum adımları:

1. Sistemde Git ve Python kurulu olmalı: 
2. BlueHound’u klonla: 

-Farklı sürümleri olabileceği için orijinal repo ismini kontrol et. Eğer yukarıdaki link geçerli değilse güncel kaynak kullanılmalı.

1. Klasöre gir: 
2. Gerekli bağımlılıkları yükle: 

#### 5. Konfigürasyon dosyasını oluştur ve düzenle:

Çoğu zaman örnek bir config.json dosyası bulunur. Gerekirse düzenlemen gerekebilir.

### ****BlueHound’un Özellikleri****

1. **Active Directory (AD) Analizi Yapar:**  
   Kurumsal ağlardaki Active Directory yapılarını tarayarak potansiyel güvenlik zafiyetlerini tespit eder.
2. **Saldırı Yollarını Görselleştirir:**  
   Saldırganların kullanabileceği yolları grafiksel olarak ortaya koyar.
3. **Blue Team Odaklıdır:**  
   BloodHound’un aksine saldırmak için değil, savunma stratejisi geliştirmek için kullanılır.
4. **Zayıf İzin ve Yetki İlişkilerini Gösterir:**  
   Kullanıcılar, gruplar ve makineler arasındaki zayıf veya hatalı izin yapılarını belirler.
5. **JSON ve CSV Çıktısı Üretebilir:**  
   Analiz sonrası detaylı raporlar elde etmek için farklı formatlarda çıktı verir.
6. **Karmaşık Yapıları Haritalar:**  
   Büyük ağlardaki bağlantı ve kullanıcı ilişkilerini anlaşılır hale getirir.
7. **Açık Kaynaklıdır:**  
   GitHub üzerinden indirilebilir ve herkes tarafından geliştirilebilir.
8. **Python ile Yazılmıştır:**  
   Platformdan bağımsız çalışabilir, özelleştirme yapılması kolaydır.
9. **BloodHound Verileriyle Uyumlu Çalışabilir:**  
   BloodHound’dan alınan verileri kullanarak savunma perspektifinden analiz yapar.
10. **Kurumsal Güvenlik Planlarına Destek Olur:**  
    Güvenlik açıklarının düzeltilmesi ve sistemlerin sertleştirilmesi için yol haritası sunar.

### ****Sonuç Olarak:****

BlueHound, modern ağ güvenliğinde savunma ekiplerinin ihtiyaç duyduğu analizleri sağlayan, özellikle Active Directory yapılarında güçlü bir analiz ve görselleştirme aracıdır. BloodHound’un saldırı perspektifine karşılık savunma penceresini açar ve kurum içi güvenliğin artırılmasına yardımcı olur.