**BloodHound Nedir?**

BloodHound, özellikle Windows tabanlı Active Directory (AD) ortamlarında kullanılan güçlü bir güvenlik analiz aracıdır. Temel amacı, AD ortamındaki ilişkileri grafiksel olarak görselleştirerek, kullanıcılar, gruplar, bilgisayarlar ve izinler arasındaki bağlantıları ortaya çıkarır. Bu sayede, sistemdeki güvenlik zafiyetleri, yetki yükseltme yolları (privilege escalation), lateral movement (yatay hareket) ve potansiyel saldırı yolları hızlıca tespit edilir.

BloodHound, saldırganlar tarafından sıkça kullanılan bir araç olmakla birlikte, savunma amaçlı güvenlik testlerinde de organizasyonların zayıf noktalarını bulması için yaygın şekilde tercih edilir.

**BloodHound Ne İşe Yarar?**

* **Active Directory İlişkilerini Haritalama:** AD ortamında bulunan kullanıcılar, gruplar, bilgisayarlar, servis hesapları ve bunların birbirleriyle olan erişim ilişkilerini detaylı şekilde ortaya koyar.
* **Yetki Yükseltme Yollarını Bulma:** BloodHound, sistemdeki düşük yetkili bir kullanıcı hesabından, domain admin (yönetici) haklarına ulaşmak için kullanılabilecek yolları analiz eder.
* **Saldırı Yüzeyini Görselleştirme:** Karmaşık AD ortamlarındaki çok sayıda bağlantıyı grafik şeklinde sunarak, zayıf nokta ve potansiyel saldırı noktalarını kolayca görmeyi sağlar.
* **Saldırı Senaryolarının Simülasyonu:** Güvenlik testi yapanlar için sistemdeki mevcut yapıdaki zafiyetleri keşfetmek ve saldırı öncesi risk analizleri yapmak için kullanılır.
* **Kurumların Güvenlik Seviyesini Ölçme:** İzinlerin ve erişimlerin nasıl yapılandırıldığı konusunda detaylı raporlar sunarak, savunma stratejilerinin geliştirilmesine katkı sağlar.

**BloodHound'un Çalışma Prensibi**

BloodHound, veri toplama (data collection) ve analiz olmak üzere iki ana aşamadan oluşur:

1. **Veri Toplama:** BloodHound, ortamda bulunan AD nesneleri ve ilişkileri toplamak için bir veri toplama aracı olan SharpHound kullanılır. SharpHound, LDAP sorguları, SMB, RPC gibi protokoller üzerinden AD verilerini çeker ve JSON formatında veriler oluşturur.
2. **Veri Analizi ve Görselleştirme:** Toplanan JSON dosyaları BloodHound arayüzüne yüklenir. BloodHound, bu verilerden grafiksel model oluşturur ve kullanıcılara AD ortamının detaylı haritasını sunar.

**BloodHound’un Özellikleri**

* **Kullanıcı ve Grup İlişkileri:** Kim hangi gruba ait, hangi grup hangi kaynaklara erişiyor gibi detaylar.
* **Delegasyon ve Yetkilendirme:** Servis hesapları, delegasyon izinleri ve potansiyel kötüye kullanım yolları.
* **SPN (Service Principal Name) Taraması:** Kerberos servis hesapları üzerinden saldırı senaryoları tespiti.
* **Kritik Haklar ve Nesneler:** Domain admin, schema admin gibi kritik rollere erişim yolları.
* **Sorgu Yeteneği:** Hazır ve özel sorgular ile sistemdeki zafiyetlerin keşfi.

**BloodHound Kurulumu ve Çalıştırılması**

BloodHound, genellikle Windows üzerinde çalışan Electron tabanlı bir uygulamadır. Ancak Linux ve macOS için de sürümleri mevcuttur.

git clone https://github.com/BloodHoundAD/BloodHound.git

cd BloodHound

npm install

npm run start. Komutlarını sırası ile uyguluyoruz;

metin, ekran görüntüsü, ekran, görüntüleme, dikdörtgen içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

Ekrana böyle bir çıktı geliyor ve burada kırmızı butonu yıldız yapıp ok tuşuna basıyoruz.

**BloodHound Arayüzü ile Analiz**

* BloodHound uygulamasını açın.
* Toplanan JSON/ZIP dosyalarını içe aktarın.
* Grafikte kullanıcılar, gruplar ve ilişkileri inceleyin.
* Hazır sorgular veya kendi sorgularınızı kullanarak zafiyetleri analiz edin.
* **Sonuç**
* BloodHound, büyük ve karmaşık Active Directory ortamlarındaki güvenlik açıklarını tespit etmek ve güvenlik açıklarından faydalanabilecek yolları görmek için vazgeçilmez bir araçtır. Hem saldırganların hem de güvenlik uzmanlarının çok kullandığı bu araç, kurumların güvenlik yapısını daha iyi anlamasına ve güçlendirmesine yardımcı olur.