**BloodHound-python**, Active Directory ortamlarında bilgi toplamak amacıyla kullanılan bir **sızma testi keşif aracıdır**. PowerShell’e alternatif olarak Python ile yazılmıştır ve PowerShell engelli ortamlarda BloodHound verisi elde etmek için kullanılır. Toplanan veriler .json formatında dışa aktarılır ve **BloodHound GUI** üzerinde analiz edilir.

**Bu Aracın Özellikleri Nelerdir?**

* **PowerShell gerektirmez**: Python tabanlıdır.
* **Active Directory nesneleri hakkında veri toplar**:
  + Kullanıcılar
  + Gruplar
  + Bilgisayarlar
  + Oturumlar
  + ACL’ler
* **Neo4j destekli BloodHound ile uyumludur**
* **Linux ortamında çalıştırılabilir**
* **LDAP protokolü ile veri çeker**
* **LDAP üzerinden doğrudan DC ile iletişim kurar**

**BloodHound-python Aracını Kali Linux Üzerinde Kurma ve Kullanma Adımları**

**Adım 1: Gerekli Paketleri Kurun**

BloodHound-python için Python3 ve pip3 gereklidir:

“sudo apt install python3 python3-pip git –y”

**Adım 2: BloodHound-python Reposunu Klonlayın**

“git clone https://github.com/fox-it/BloodHound.py.git

cd BloodHound.py”

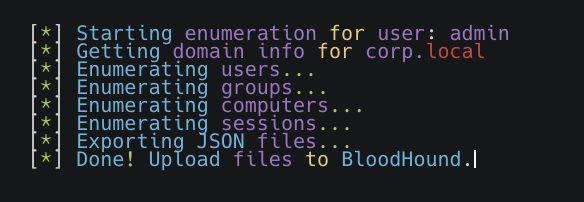
**Adım 3: Gereksinimleri Yükleyin**

“pip3 install -r requirements.txt”

**Adım 4: Bilgi Toplama (Tüm Bilgiler)**

Örnek bir tam keşif komutu:

“python3 bloodhound-python -u admin -p 'P@ssw0rd' -d corp.local --dc-ip 10.10.10.2 -c all”



**Adım 5: JSON Çıktılarını BloodHound Arayüzüne Yükleyin**

Oluşan dosyalar:

computers.json

groups.json

users.json

sessions.json

trusts.json

Tarayıcıdan http://localhost:7474 adresine gidin ve BloodHound arayüzüne bu dosyaları yükleyin.