ReconDog Eğitim Materyali

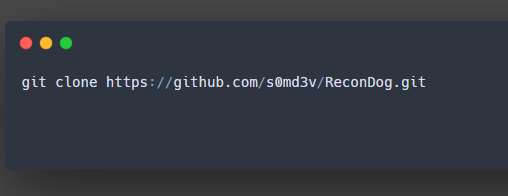
# ReconDog Nedir?

ReconDog, Python tabanlı, açık kaynak bir bilgi toplama (reconnaissance) aracıdır. Özellikle siber güvenlik uzmanlarının, pentester’ların ve meraklıların hedef sistem hakkında bilgi edinmesi için kullanılır. Temel olarak pasif bilgi toplama işlemlerini otomatikleştirir.  
  
Kullanım Alanları:  
- Etik hacking ve pentest çalışmaları  
- Güvenlik açığı araştırmaları öncesinde hedef analizi  
- Siber güvenlik eğitimleri

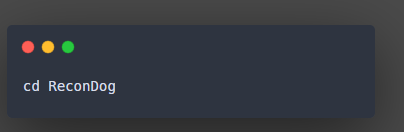
# Kurulum Adımları (GitHub Üzerinden)

1. Python’un sisteminizde kurulu olduğundan emin olun.

2. Terminali açın ve aşağıdaki komutu girerek aracı klonlayın:

******

3. Klasöre geçin:

******

4. Aracı başlatın:

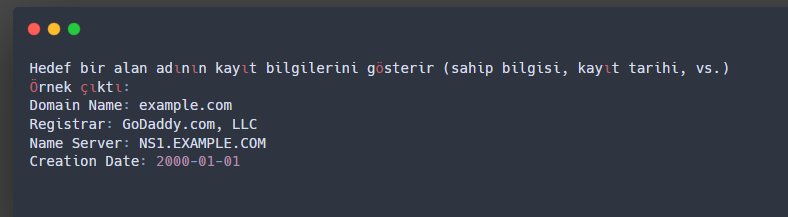
# 

# Ana Menü Seçenekleri

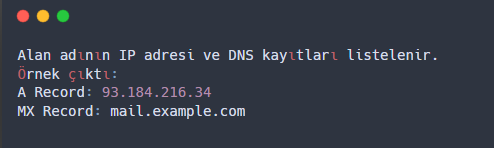
ReconDog çalıştırıldığında aşağıdaki gibi bir ana menü ile karşılaşırsınız:  
  
Select one of the options:  
  
1) Whois Lookup  
2) DNS Lookup  
3) GeoIP Lookup  
4) Subnet Calculator  
5) Port Scanner  
6) HTTP Header Grabber  
7) Extract Page Links  
8) Exit

# Örnek Bilgi Toplama İşlemleri

1. Whois Lookup

******

2. DNS Lookup

******

3. HTTP Header Grabber

# 

# Eğitim İpuçları (Pasif Bilgi Toplama)

- Yasal Sınırlar: ReconDog sadece pasif bilgi toplar, yani doğrudan hedefe zarar vermez. Ancak hedefin izni olmadan kullanılmaması etik değildir.  
- Kendi Web Sitenizde Deneyin: Öğrenciler için en iyi yöntem kendi oluşturdukları basit siteler üzerinde bu araçları denemektir.  
- Terminal Okuryazarlığı: Komut satırını kullanma becerisi kazandırmak, siber güvenliğin temelidir.  
- Kavramları Açıklayın: “DNS nedir?”, “Whois neden önemlidir?” gibi temel kavramları kısa açıklamalarla destekleyin.