Egress-Assess Aracı –Eğitimi Materyali

# 1. Egress-Assess Nedir?

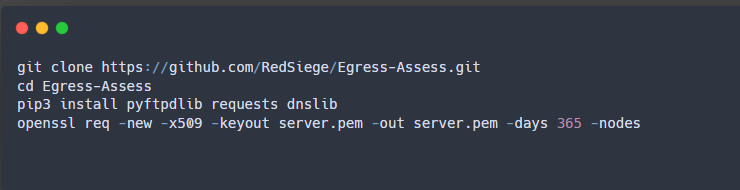
Egress-Assess, ağ içinden dışarıya veri sızdırılmasını (data exfiltration) simüle ederek, egress trafiği tespit yeteneklerini test eden açık kaynaklı bir araçtır. FTP, HTTP, HTTPS, SMTP, ICMP, DNS gibi çoklu protokol destekler.  
  
Red Team ve Blue Team çalışmalarında, bir kurumun ağ çıkışında veri güvenliğinin nasıl kontrol edildiğini analiz etmek için kullanılır.

# 2. Ne İşe Yarar?

- Network sınırlarında veri çıkışı fark edilebiliyor mu, bunu test eder.  
- Zararsız sahte veri ya da gerçek dosyalar göndererek tespit edilip edilmediğini ölçer.  
- FTP, HTTP, HTTPS, SMTP, ICMP, DNS, DNS\_Resolved, SMB gibi protokolleri destekler.

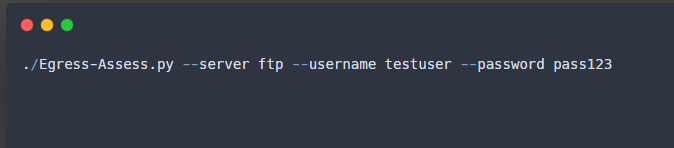
# 3. Kali Linux Kurulumu

Kurulum Adımları:

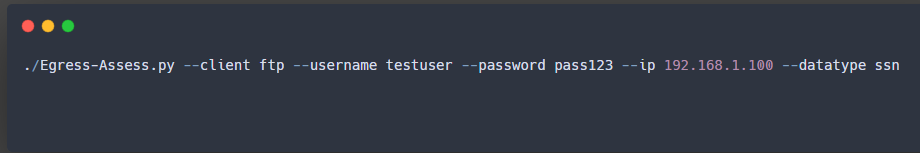


# 4. Temel Kullanım Örnekleri

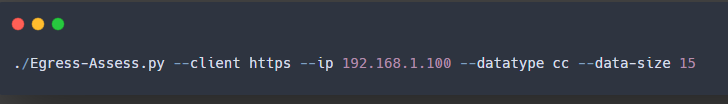
A) FTP ile Sahte Veri Gönderimi:

Sunucu: 

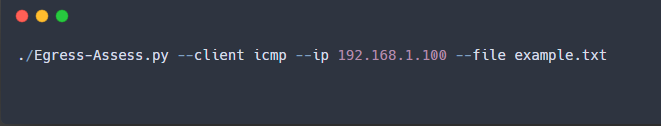
İstemci:



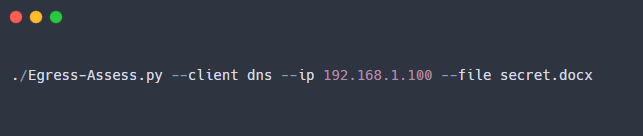
B) HTTPS (şifreli) veri gönderimi:



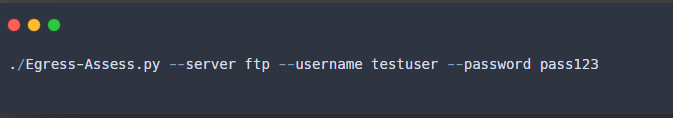
C) ICMP ile veri gönderimi:



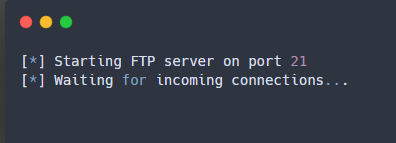
D) DNS ile veri tünelleme:



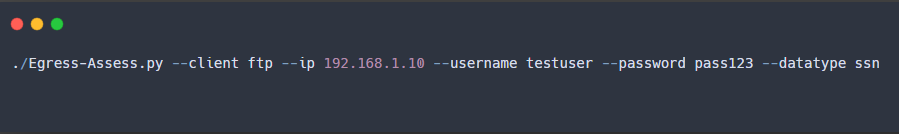
Komut: FTP Server Başlat



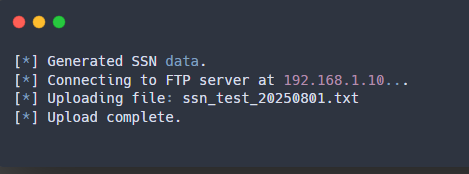
Çıktı:



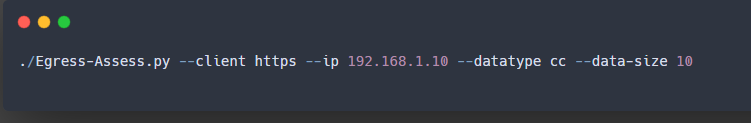
Komut: Sahte Veri Gönderimi (SSN)



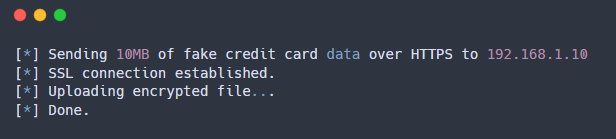
# Çıktı:



**Komut: HTTPS Üzerinden Kredi Kartı Sahte Verisi Gönderme**



Çıktı:



# 5. Örnek Saldırı Senaryosu

Senaryo:  
- Kali Linux'ta Egress-Assess kurulu.  
- Basit bir FTP sunucu başlatılır.  
- İstemciden sahte veri gönderilir.  
- Veri, sunucu tarafında kaydedilir.  
- IDS ya da log kayıtları analiz edilir.

# 6. Öğrenciler İçin Uygulama Görevleri

1. Egress‑Assess’i Kali Linux'a kurun.

2. FTP sunucusu başlatın ve veri gönderin.

3. HTTPS ile veri gönderimi sağlayın.

4. ICMP veya DNS protokolü kullanarak veri gönderin.

5. Exfil işlemi esnasında IDS/log kayıtlarını inceleyin.

# 7. Özet Tablo

Araç: Egress-Assess

Amacı: Egress trafik tespiti ve veri exfil simülasyonu

Destek Protokoller: FTP, HTTP, HTTPS, SMTP, ICMP, DNS, DNS\_Resolved, SMB

Platform: Python script, CLI arayüz

Kullanım Alanı: Red Team, Blue Team, Güvenlik Testi