## **Pupy Nedir, Neden Kullanılır?**

**Pupy**, Python tabanlı, çapraz platform (Windows, Linux, macOS, Android) uyumlu, güçlü bir **post-exploitation** ve **uzaktan erişim aracı (RAT)** olarak tasarlanmıştır. Genellikle hedef sisteme başarılı bir sızmadan sonra kullanılır ve saldırganın hedef üzerinde kalıcılığını sürdürmesini, veri toplamayı ve sistem üzerinde komut çalıştırmayı mümkün kılar.

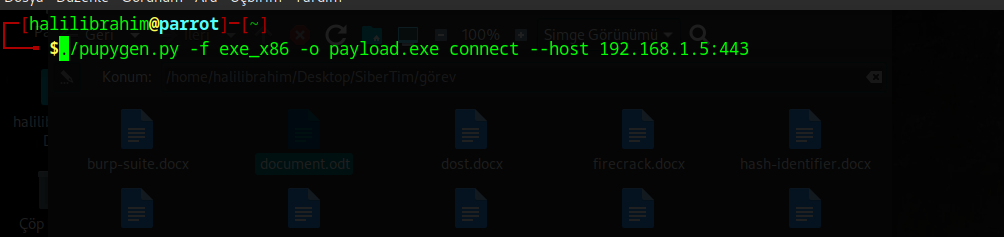
Pupy, aynı zamanda **in-memory** çalışabilme yeteneği sayesinde antivirüsler tarafından tespiti zorlaştırır. Saldırgan, hedef sisteme yüklenen bir payload aracılığıyla tam erişim sağlayabilir. Bu erişim üzerinden komut satırı, dosya aktarımı, ekran görüntüsü alma, keylogger çalıştırma, ağ taraması yapma gibi birçok işlem gerçekleştirilebilir.

## Kurulum

Pupy karmaşık bir araçtır ve genellikle Kali Linux veya benzeri sistemlerde kurulur. Tavsiye edilen kurulum adımları şunlardır:

* git clone https://github.com/n1nj4sec/pupy
* cd pupy
* ./install.sh

**Kullanım Örneği**



Bu komutla payload.exe isimli bir dosya oluşturulur. Hedef sisteme çalıştırıldığında Pupy sunucusuna bağlantı kurar.

* -f exe\_x86 → 32-bit Windows için EXE formatında payload
* --host → Dinleyicinin IP ve port bilgisi

## **Elde Edilebilecek Bilgiler ve Etkiler**

Pupy ile başarılı bağlantı kurulduğunda aşağıdaki işlemler yapılabilir:

* Uzak komut çalıştırma (remote shell)
* Dosya sistemine erişim ve dosya yükleme/indirme
* Keylogger çalıştırma ve tuş kayıtlarını toplama
* Ekran görüntüsü alma
* Kamera/mikrofon gibi çevresel donanımları kullanma
* Network taramaları (örneğin hedefin bağlı olduğu diğer IP’leri görmek)
* Kalıcılık sağlama (persistence)
* Veritabanı, kimlik bilgileri, token ve şifre dosyalarını toplama

Bu yetenekler Pupy’yi yalnızca sızma aracı değil, aynı zamanda **post-exploitation framework** seviyesine çıkarır.

## **Parametreler ve Özellikler**

Pupy çok sayıda parametreyle birlikte gelir, en yaygınları şunlardır:

* pupygen.py → Payload oluşturucu
* -f → Hedef platforma uygun format (örneğin exe\_x86, py, pyinst, apk)
* --host → Bağlantı yapılacak IP:Port bilgisi
* --transport → Bağlantı protokolü seçimi (http, https, ssl, reverse\_tcp)
* pupysh.py → Shell başlatıcı (kontrol arayüzü)

Pupy, gelişmiş özelliklere sahip, modüler yapıda bir uzaktan erişim ve post-exploitation framework’üdür. Python temelli olması sayesinde genişletilebilir, platform bağımsız çalışabilir. Yasal izinlerle yapılan sızma testlerinde hedef sistem üzerinde derinlemesine analiz yapmak, veri toplamak ve kalıcılık senaryoları test etmek için güçlü bir seçenektir.