Empire (Python) C2 - Eğitim Materyali

# 1. Empire Nedir?

Empire, Python ve PowerShell tabanlı açık kaynaklı bir Command and Control (C2) framework’tür. Gelişmiş saldırı sonrası (post-exploitation) yetenekler sunar ve Windows, Linux, macOS sistemleri üzerinde çalışabilir. Python Empire sürümü, daha çok platformlar arası kullanım ve Linux ortamında çalışmak isteyenler içindir.

# 2. Temel Özellikleri

* Python ve PowerShell implant desteği (platformlar arası uyumluluk)
* HTTPS, HTTP, SMB gibi iletişim protokolleri
* Post-exploitation modülleri: keylogger, mimikatz, privilege escalation
* GUI yerine CLI (komut satırı) kullanımı
* Dinamik modül yükleme ve özel modül desteği

# 3. Nerelerde Kullanılır?

* Red Team ve sızma testi senaryoları
* Öğrenci eğitimlerinde saldırı sonrası analiz ve keşif uygulamaları
* C2 iletişim yapılarını öğretmek
* Python temelli implant geliştirme çalışmaları

# 4. Kurulum Adımları (Python Empire)

## Gerekli Bağımlılıkların Kurulumu

## 

## Empire'ı Klonla

## 

## Kurulum Klasörüne Gir

## 

## Kurulum Script'ini Başlat

## 

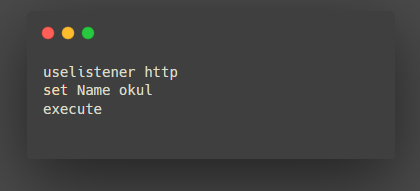
## Empire'ı Başlat

# 

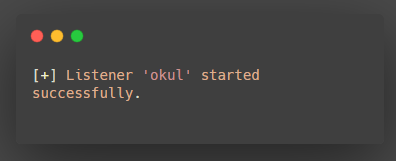
# 5. Örnek Terminal Komutları ve Çıktıları

## Listener Oluşturma

**Kodu:**

****

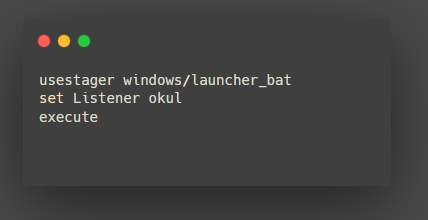
**Çıktı:**

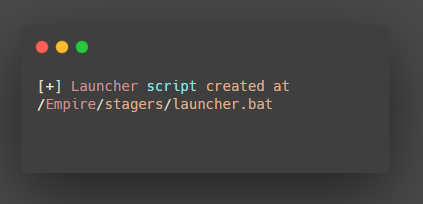


| **Komut** | **Görevi** |
| --- | --- |
| **uselistener http** | **HTTP türünde bir listener hazırlamak** |
| **set Name okul** | **Listener’a isim vermek** |
| **execute** | **Listener’ı başlatmak** |
| **Çıktı** | **Listener’ın başarıyla başlatıldığını gösterir** |

## Stager Oluşturma

**Kodu:**

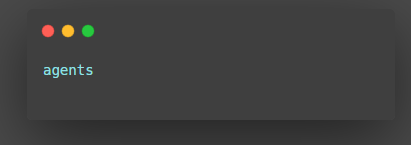
****

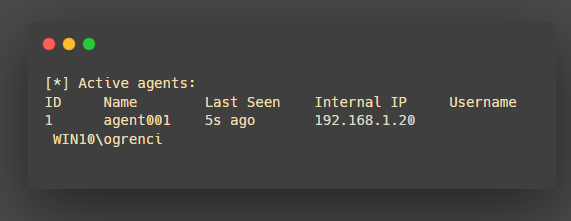
**Çıktı:**  
  


| **Komut** | **Görevi** |
| --- | --- |
| usestager windows/launcher\_bat | .bat dosyası formatında bir stager oluşturulacağını belirler |
| set Listener okul | Stager’ın hangi listener’a bağlanacağını belirtir |
| execute | Stager’ı oluşturur ve Empire dizinine kaydeder |
| Çıktı | Oluşan .bat dosyasının konumunu gösterir |

## Bağlanan Agent’ı Görme

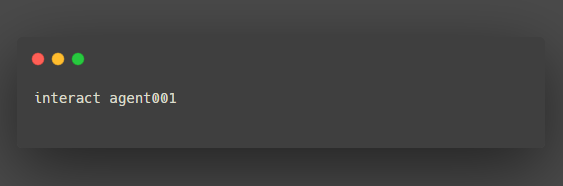
**Kodu:**

****

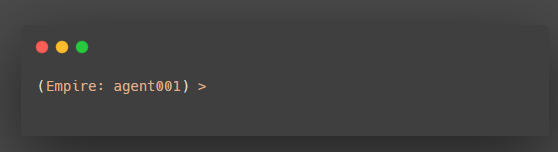
**Çıktı:**  
  


## Komut Gönderme

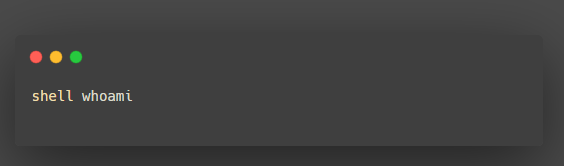
**1. Komut:**



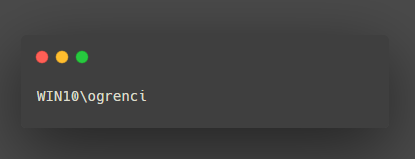
**1. Çıktı:**



**2. Komut:**



**2. Çıktı:**



# 6. Öğrenciler İçin Aktiviteler

* Empire ile listener ve stager oluşturma pratiği
* Agent yakalama ve 'whoami', 'ipconfig' gibi komutlar gönderme
* Arka planda çalışan implantlarla bilgi toplama
* Basit PowerShell modüllerini çalıştırma