Posh C2 Eğitim Materyali

# 1. Posh C2 Nedir?

Posh C2, açık kaynaklı ve modüler bir Command-and-Control (C2) framework’üdür. Python3 tabanlı sunucu bileşeni ve PowerShell implant’ları içerir. Windows'e odaklansa da Linux/macOS için Python dropper da sunar.

# 2. Temel Özellikleri

* Modüler implantlar: PowerShell, C#, Python3 implantlarla bellek içi çalışma.
* Beacon yapılandırması: süre, jitter, kill-date gibi ayarlar.
* Şifreli iletişim: HTTPS, SMB, domain-fronting desteği.
* GUI ve CLI desteği: autocomplete ve menüler.
* Servis/Docker modu: kolay kurulum ve dağıtım.
* SharpSocks ve SOCKS proxy: pivot imkânı.
* Loglama: tüm işlemler zamanlı kaydedilir.

# 3. Nerelerde Kullanılır?

* Red Team eğitimleri
* Post-exploitation işlemleri
* Proxy/daisy-chaining
* SOC testleri ve tehdit avcılığı

# 4. Kurulum Adımları

## Standart Kurulum

## 

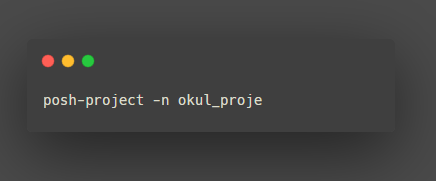
## Geliştirici Branch

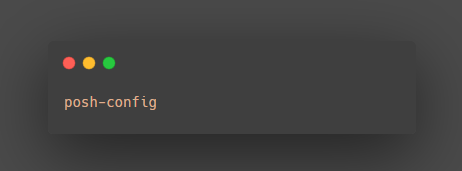
## 

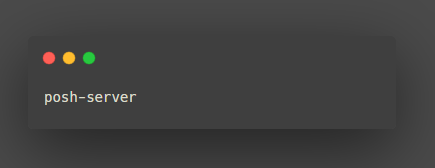
## Docker Kurulumu

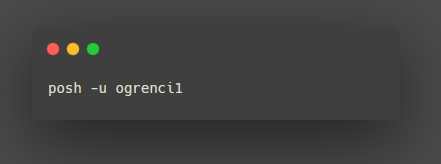
# 

# 5. İlk Çalıştırma ve Kullanım

Projeyi oluştur:  


Konfigürasyonu düzenle:  


C2 sunucusunu başlat:  


Implant handler aç:  


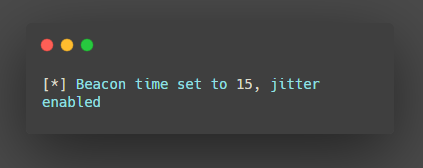
# 6. Kullanım Örnekleri

## 1. Beacon Süresi Ayarlama

## Kodu:

## 

**Çıktı:**

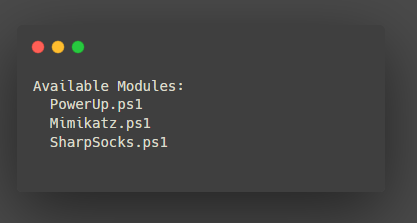


## 2. Modülleri Listeleme

## Kodu:

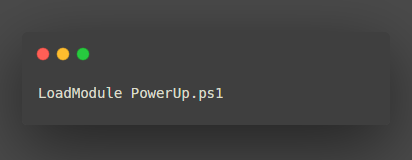
## 

## Çıktı:

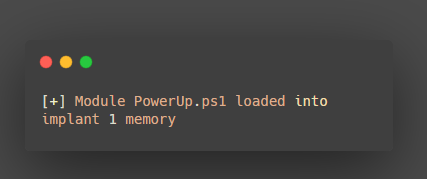


## 3. Modül Yükleme:

## Kodu:



## Çıktı:

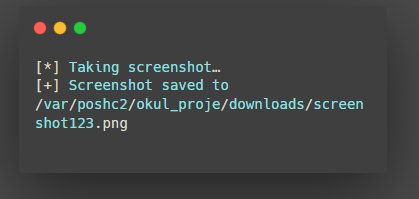


## 4. Ekran Görüntüsü Alma

## Kodu:

## 

## Çıktı:

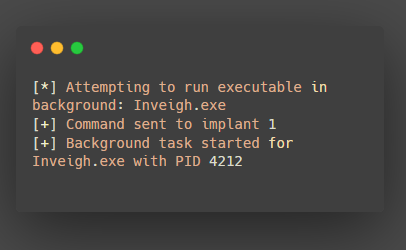


## 5.Arka planda çalıştırma

## Kodu:

# 

## Çıktı:



| Komut | | | Görevi | |
| --- | --- | --- | --- | --- |
| ListModules | | | Kullanılabilir modül (PowerShell script) listesini gösterir | |
| LoadModule PowerUp.ps1 | | | PowerUp.ps1 modülünü belleğe yükler | |
| Invoke-AllChecks | | | Yüklenen modül içindeki zafiyet analiz komutunu çalıştırır | |
| Hide-Implant | | | Sadece görünürlüğü kapatır(arka planda çalışmaya devam eder) | |
| Unhide-Implant | | | Gizlenmiş implantı geri getirir(Görünür olur,aktifse komut alabilir) | |
| Kill-Implant | | | Tamamen sonlandırır, bağlantı kesilir(Tekrar erişim için yeni implant gerekir) | |
|  |  | |  | |

# 8. Lise Öğrencilerine Yönelik Uygulamalar

* Beacon süresini değiştirip gözlemleme
* Hide/Unhide ile implant görünürlüğü
* get-screenshot komutuyla ekran alma
* Modül yükleyerek sistem keşfi