Invoke-Obfuscation - PowerShell Obfuscation Aracı Eğitim Materyali

# 🔍 Invoke-Obfuscation Nedir?

Invoke-Obfuscation, PowerShell komutlarını ve betiklerini analizden kaçırmak amacıyla karıştırmak (obfuscate) için kullanılan açık kaynaklı bir araçtır.  
Kötü amaçlı yazılımlar veya Red Team operasyonları sırasında tespit edilmekten kaçmak için sıklıkla kullanılır.

# 🔧 Özellikleri

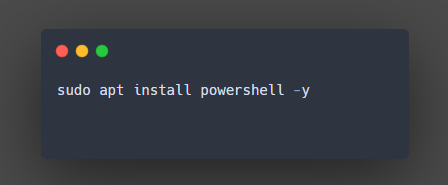
- PowerShell komutlarını farklı yollarla obfuscate eder.  
- Dinamik olarak kod üretir, her seferinde farklı sonuçlar alınabilir.  
- Farklı obfuscation tekniklerini zincirleme olarak uygulayabilir.  
- Tespit ve analizden kaçınmayı amaçlar.

# 📌 Kullanım Alanları

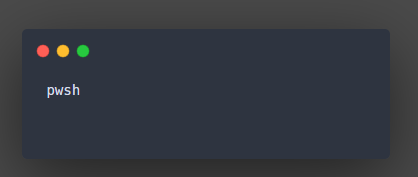
- Red Team / Pentest operasyonları  
- Malware analiz eğitimi  
- Güvenlik ürünlerini test etme  
- Güvenlik farkındalığı eğitimi

# 💻 Kurulum (Kali Linux - PowerShell 7 üzerinden)

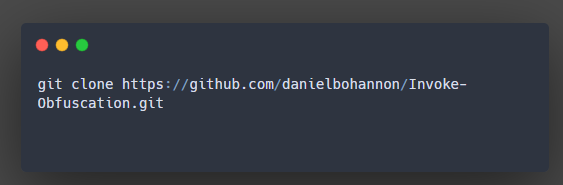
1. PowerShell'i yükleyin (eğer yüklü değilse):



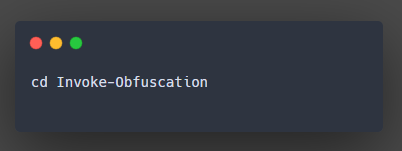
* 2. PowerShell'i başlatın:



3. Aracı klonlayın:



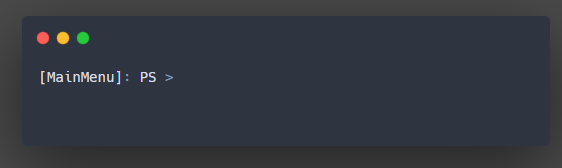
4. Dizin içerisine girin:



5. Script'i PowerShell'de çalıştırın:

# 

Çıktı:

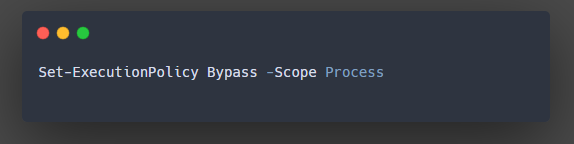


# 🧪 Kullanım Menüsü

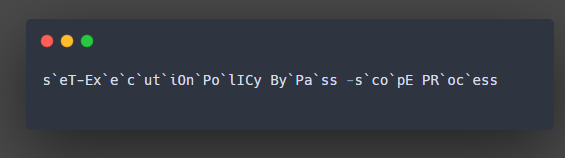
Invoke-Obfuscation çalıştırıldığında aşağıdaki gibi etkileşimli bir menü açılır:  
  
 [MainMenu]: PS >   
  
Buradan aşağıdaki seçenekler sırasıyla seçilir:  
  
- COMP (Command Obfuscation)  
- STR (String Obfuscation)  
- ENC (Encoding - Base64 vb.)

# 🖥️ Örnek Komut ve Obfuscation Çıktısı

🟨 Komut:



🟥 Obfuscate Edilmiş Çıktı:



Yukarıdaki örnek, karakter aralarına ` (escape character) eklenerek okunabilirlik azaltılmıştır.

# 🧠 Öğrenci Notları

- Obfuscation teknikleri, savunma tarafında analiz ve tespit becerilerini geliştirmek için önemlidir.  
- Gerçek sistemlerde kullanılmadan önce etik ve hukuki izin alınmalıdır.  
- Gelişmiş EDR sistemleri bu teknikleri artık tespit edebilmektedir.