## DSViper Aracı - Eğitim Materyali

# 🧠 DSViper Nedir?

DSViper, özellikle Active Directory ortamlarında yer alan Windows sistemlerinde kimlik bilgisi, güvenlik açıkları ve yanlış yapılandırmaların hızlı tespiti için geliştirilmiş hafif bir Red Team aracıdır. PowerShell tabanlıdır ve özellikle DLL hijacking, token stealing ve credential dumping gibi işlemleri otomatikleştirmek için kullanılır.

# 🚀 Özellikleri

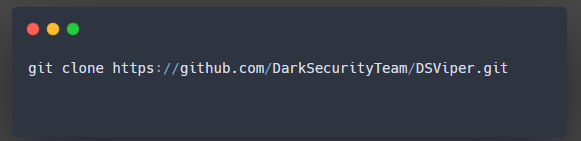
- Credential dumping (LSASS üzerinden)  
- Token stealing ve impersonation  
- DLL hijacking testi  
- Active Directory ortamında hızlı keşif  
- Güvenlik açığı kontrolü ve post-exploitation işlevleri

# 🎯 Kullanım Alanları

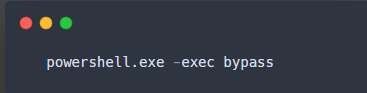
- Red Team ve sızma testleri  
- AD ortamlarında bilgi toplama ve zafiyet keşfi  
- Post-exploitation adımlarında kimlik taklit işlemleri  
- Hafif, taşınabilir PowerShell çözüm arayanlar için ideal

# 🛠️ Kurulum ve Hazırlık

1. GitHub üzerinden indirme:

******

2. PowerShell oturumu başlat:

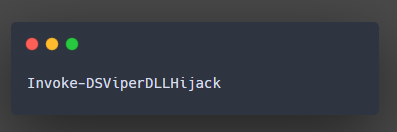
******

3. Script’i içe aktar:

# 

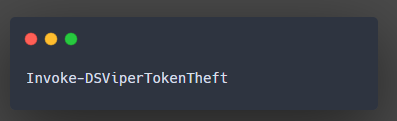
# 🧪 Örnek Komutlar ve Çıktılar

✅ DLL Hijacking Taraması:

******

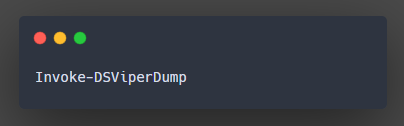
→ Hedef sistemde DLL yüklenme sırasındaki açıklıkları listeler.

✅ Token Stealing ve Impersonation:

******

→ Elde edilen access token’ları görüntüler ve impersonation yapar.

✅ Credential Dumping (LSASS):

******

→ Bellekten kimlik bilgilerini çeker (örn. şifre özetleri).

# 📎 Notlar

- PowerShell Execution Policy `bypass` modda çalışmalıdır.  
- Çoğu antivirus ve EDR, bu tür araçlara karşı duyarlıdır.  
- Gelişmiş AD ortamlarında güvenlik kayıtları oluşturabilir.  
- Yalnızca eğitim ve sızma testi laboratuvarlarında kullanılmalıdır.