GhostPack Aracı - Eğitim Materyali

# 🔍 GhostPack Nedir?

GhostPack, güvenlik testleri ve Red Team operasyonları sırasında kullanılan gelişmiş Windows post-exploitation (sömürü sonrası) araçlarının bir koleksiyonudur. Bu araçlar C# diliyle yazılmıştır ve saldırganların sistemdeki zafiyetleri keşfetmesine, kimlik bilgilerini ele geçirmesine veya hak yükseltme işlemlerine yardımcı olur.

# 🔧 Özellikleri

- Credential Dumping (Kimlik bilgisi çıkarma)  
- Token Manipulation (Yetki devri / impersonation)  
- Kerberos saldırıları (Pass-the-Ticket, Ticket Extraction)  
- Hak yükseltme (UAC bypass, dll injection vs.)  
- Sistem keşfi (lokal kullanıcılar, gruplar, domain bilgileri)

# 📌 Kullanım Alanları

- Red Team testlerinde  
- Adli bilişim analizlerinde  
- Güvenlik farkındalığı eğitimlerinde  
- Zafiyet analizlerinde

# 📁 GhostPack Araçları

GhostPack şu popüler araçları içerir:  
- Rubeus → Kerberos bileti işlemleri  
- Seatbelt → Sistem keşif aracı  
- SharpUp → Hak yükseltme kontrolleri  
- SafetyKatz → Mimikatz alternatifi (C#)  
- SharpDump → LSASS dump alma aracı  
- SharpRoast → Kerberoasting için

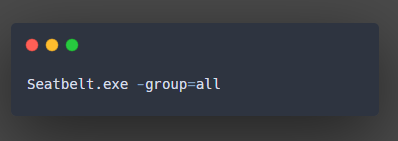
# 💻 Kurulum ve Kullanım (Temel)

GhostPack araçları kaynak kod olarak gelir. Bunları .NET (C#) ortamında derlemek gerekir.

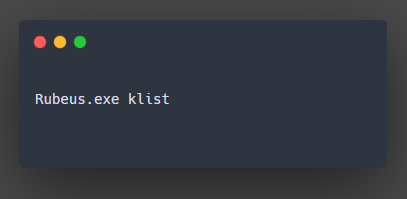
Ancak eğitim amaçlı olarak, derlenmiş (compiled) EXE dosyaları Red Team kaynaklarında bulunabilir.

# 🧪 Örnek Terminal Kullanımı (Windows)

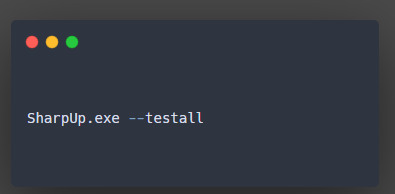
🔹 Seatbelt.exe ile sistem bilgisi toplama:



🔹 Rubeus ile Kerberos bileti listeleme:

******

🔹 SharpUp ile UAC bypass testleri:



# 🧠 Öğrenci Notları

- GhostPack araçları genellikle AV tarafından tespit edilir, bu nedenle test ortamlarında kullanılmalıdır.  
- Bu araçları kullanmak için temel Windows sistem mimarisi ve kimlik doğrulama bilgisi faydalıdır.  
- Yasal olmayan sistemlerde kullanımı suç teşkil eder.

# 🔧 Detaylı Kurulum Adımları

1️⃣ GhostPack kaynak kodlarını GitHub üzerinden klonlayın:

git clone https://github.com/GhostPack/Seatbelt.git

git clone https://github.com/GhostPack/Rubeus.git

2️⃣ Windows ortamında Visual Studio Community Edition kurulmalıdır.

- Visual Studio'yu https://visualstudio.microsoft.com adresinden indirebilirsiniz.

- .NET Framework 4.0 veya üstü yüklü olmalıdır.

3️⃣ İlgili proje klasöründe bulunan .csproj dosyasını Visual Studio ile açın.

Örneğin: Seatbelt/Seatbelt.csproj

4️⃣ Visual Studio'da üst menüden Build > Build Solution seçeneği ile derleyin.

- 'Release' modunu seçmeyi unutmayın.

5️⃣ Derleme tamamlandığında, bin\Release\ klasöründe .exe dosyası oluşur:

Örnek: Seatbelt.exe veya Rubeus.exe

6️⃣ Bu dosyaları hedef Windows sistemine taşıyıp PowerShell veya CMD üzerinden çalıştırabilirsiniz.

⚠️ Not: Çoğu antivirus bu araçları tespit edebilir. Sanal test ortamı dışında çalıştırmak önerilmez!