2. SharpSploit – C# ile Yazılmış Sızma Sonrası Araç Kütüphanesi

**Nedir?**

SharpSploit, Red Team ve penetration testing faaliyetlerinde kullanılmak üzere geliştirilmiş, C# diliyle yazılmış açık kaynaklı bir post-exploitation (sızma sonrası) kütüphanedir. PowerSploit’in .NET sürümü olarak düşünülebilir ve modern .NET uygulamalarıyla uyumludur.

**Özellikleri:**

✓Modüler yapıdadır – İstenilen işlevler kod içerisine eklenebilir.

✓.NET Framework ile yazılmış güvenlik araçları geliştirmek için temel sağlar.

✓Reflective DLL Injection, shellcode çalıştırma, credential dumping, keystroke logging gibi özellikleri vardır.

✓AV/EDR atlatımı için özel yazılmış teknikleri destekler.

**Kullanım Alanları:**

•Red Team operasyonlarında özel payload ve sızma sonrası modüller geliştirmek

•AV/EDR atlatımı için .NET temelli özel araçlar oluşturmak

•PowerSploit kullanan yapıları modern sistemlerde kullanıma uygun hale getirmek

•Güvenlik araştırmaları ve eğitimlerde pratik çözümler geliştirmek

**Kurulum Aşamaları**

**- Ön Gereksinimler:**

-Windows işletim sistemi

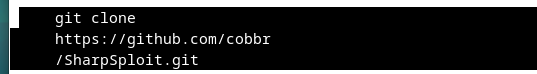
-Visual Studio

-.NET Framework (4.0 ve üzeri)

**Adımlar**:

**1** .SharpSploit GitHub sayfasına gidin:

https://github.com/cobbr/SharpSploit

**2.** Kodu klonlayın: 

**3**.Visual Studio ile projeyi açın.

**4**. Gerekli bağımlılıkları ekleyin ve build (derleme) işlemini yapın

**5**. Kütüphaneyi kendi .NET projenize dahil ederek dilediğiniz gibi kullanabilirsiniz.

**Dikkat Edilmesi Gerekenler**

✓AV/EDR sistemleri tarafından bazı modüller imza bazlı olarak tespit edilebilir, bu yüzden kaynak kod üzerinde özelleştirme yapılmalıdır.

✓Yalnızca izinli ve kontrollü test ortamlarında kullanılmalıdır.

✓Kodun düzgün çalışabilmesi için .NET sürüm uyumluluğu ve çalışma zamanı (runtime) ortamları kontrol edilmelidir.

✓Gerçek sistemlerde çalıştırmadan önce offline test edilmesi önerilir.