**PowerSploit**

**PowerSploit**, Microsoft PowerShell ortamında çalışan modüler bir güvenlik araç setidir. Sızma testi (penetration testing) ve güvenlik değerlendirmeleri sırasında bilgi toplama, sistem istismarı (exploitation), bellek içi kod yürütme (in-memory execution) gibi amaçlarla kullanılır. PowerSploit, Windows ortamlarında PowerShell komutlarını kullanarak saldırganların sistem üzerinde kalıcı olmayan, iz bırakmayan işlemler yapmasına imkan sağlar.

**Özellikleri**

* **Bilgi Toplama:** Ağ bilgileri, kullanıcı hesapları, sistem konfigürasyonları, yüklü programlar gibi pek çok bilgiyi toplayabilir.
* **Exploit Modülleri:** Windows sistemlerde güvenlik açıklarını kullanarak exploitler gerçekleştirebilir.
* **Dosyasız Saldırı (Fileless Attack):** Kod doğrudan bellekte çalıştırılarak disk üzerinde iz bırakmaz.
* **Kolay Entegrasyon:** PowerShell komutları olarak çalıştığı için diğer araçlarla kolayca entegre olabilir.
* **Modüler Tasarım:** İhtiyaca göre farklı modüller (bilgi toplama, yükseltme, payload oluşturma vb.) kullanılabilir.
* **Scripting İmkanı:** Komutlar script haline getirilip otomatikleştirilebilir.
* **Açık Kaynak:** GitHub üzerinden ücretsiz erişilebilir ve geliştirilebilir.

**Kullanım Alanları**

* **Pentesting (Sızma Testi):** Hedef Windows sistemlerde güvenlik açıklarını tespit etmek ve exploit etmek için.
* **Bilgi Toplama:** Hedef sistem ve ağ hakkında detaylı veri toplamak için.
* **Red Team Operasyonları:** Saldırgan taktiklerini simüle etmek için dosyasız saldırılar gerçekleştirmek.
* **Güvenlik Analizi ve Eğitim:** PowerShell tabanlı saldırı tekniklerini incelemek ve öğrenmek için.
* **Post-Exploitation:** Sisteme erişim sağlandıktan sonra kalıcılık, keşif ve lateral hareket için kullanılabilir.

**Kurulum Aşaması**

PowerSploit, genellikle Kali Linux, Parrot OS gibi pentest odaklı dağıtımlarda veya doğrudan Windows ortamında PowerShell ile kullanılır.

1. **Gereksinimler:**
   * PowerShell 3.0 veya üzeri
   * İnternet bağlantısı (modülleri GitHub’dan çekmek için)
   * Windows hedef sistemde PowerShell izinleri (saldırı simülasyonu için)
2. **Kurulum:**

PowerSploit’un ana deposu GitHub’dadır: 

-Windows ortamında PowerShell’i açıp modülleri içeri aktarabilirsiniz:



-(Veya ihtiyacınız olan spesifik modülü)

1. **Doğrudan PowerShell’de Komutları Çalıştırma:**

PowerSploit script dosyalarını doğrudan PowerShell’de çağırarak modülleri kullanabilirsiniz.

**Dikkat Edilmesi Gerekenler**

* **Yasal İzin:** PowerSploit yalnızca izinli sızma testlerinde veya eğitim amaçlı kullanılmalıdır. İzinsiz kullanım yasal sonuçlara yol açar.
* **Antivirüs ve Endpoint Güvenlik Yazılımları:** PowerSploit komutları genellikle antivirüsler tarafından zararlı olarak algılanabilir. Test ortamında bu durum göz önünde bulundurulmalıdır.
* **Windows PowerShell Versiyonu:** Hedef sistemin PowerShell sürümü bazı modüllerin çalışmasını etkileyebilir.
* **Güncelleme:** PowerSploit sürekli gelişen bir araçtır, düzenli güncellemeleri takip etmek önemlidir.
* **Sistem Etkisi:** Bazı modüller sistem üzerinde yüksek kaynak kullanımı veya beklenmedik etkiler yaratabilir, canlı sistemlerde dikkatli olunmalıdır.
* **İz Bırakmama:** Dosyasız saldırılar iz bırakmadan yapılabilir ancak log kayıtları ve diğer güvenlik çözümleri tarafından tespit edilebilir.