**3. Ebowla – Payload Şifreleme ile AV Atlatma Aracı**

**Nedir?**

Ebowla, oluşturulan payload'ları şifreleyerek antivirüs (AV) yazılımlarının tespitinden kaçırmak için kullanılan bir obfuscation ve encryption framework’üdür. Özellikle Meterpreter ve benzeri payload’ları şifreleyip farklı programlama dillerine entegre ederek tahmin edilebilir davranışları gizlemeyi amaçlar.

**Özellikleri**

✓Payload’ı AES, XOR, vb. algoritmalarla şifreleyebilir

✓Sonuçta elde edilen şifreli payload'ı C, Python, Powershell, Go gibi dillere gömebilir

✓Statik analiz araçlarını yanıltmak için davranışların yapısı değiştirilir

✓Özelleştirilebilir encoder ve decoder mekanizması içerir

✓Hem 32-bit hem 64-bit destek sunar

**Kullanım Alanları**

✓AV/EDR sistemlerini bypass ederek zararlı payload’ın hedef sisteme sızmasını sağlamak

✓Eğitim ve test ortamlarında gerçek saldırı senaryolarını simüle etmek

✓Mevcut shellcode/payload’ları özelleştirerek gizlemek

✓Penetrasyon testlerinde özel binary oluşturmak

**Kurulum Aşamaları**

**- Gereksinimler:**

•Python 2.7 (Ebowla Python 3 ile uyumlu değildir)

•Wine (Windows payload oluşturmak için Linux'ta çalışıyorsan)

•Mono (bazı C# işlemleri için)

**Kurulum Adımları:**

**1**. GitHub üzerinden klonlayın: 

**2**. Konfigürasyon dosyasını düzenleyin:

-Payload tipi, şifreleme metodu, dil seçimi (örneğin: config.json)

**3**. Payload şifreleme işlemi: 

**4**. Üretilen şifreli payload çıktısını istenen dile gömerek, compile edin (örneğin: C, Python, PowerShell)

**Dikkat Edilmesi Gerekenler**

✓Python 2.7 kullanmak zorundasın, yeni sürümlerle çalışmaz.

✓Üretilen dosya sadece decoder içeren sisteme uygun compile edilmelidir.

✓AV sistemleri tarafından bazı davranışlar hâlâ tespit edilebilir, şifreleme metodunu çeşitlendirmek önemlidir.

✓Kodun gerçek bir sisteme uygulanması yasal izin gerektirir, aksi durumda hukuki sonuç doğurabilir.