## **Koadic (JScript RAT) Nedir, Neden Kullanılır?**

**Koadic**, tam adıyla **Koadic Command & Control (C2) Framework**, Windows sistemleri hedef alan, **JScript tabanlı bir uzaktan erişim aracı (RAT)** ve **post-exploitation** framework’tür. Metasploit ve Empire gibi gelişmiş sızma sonrası platformlara benzer şekilde çalışır, ancak farkı şuradadır: Koadic, komutlarını Windows’un yerleşik olarak desteklediği **Windows Script Host (WSH)** üzerinden, yani **JScript ve VBScript** aracılığıyla yürütür. Bu özelliği sayesinde çoğu sistemde dış bağımlılık olmadan kod yürütülebilir ve antivirüs yazılımlarının tespiti zorlaşır.

Koadic, “living off the land” (sistemde zaten var olan bileşenlerle saldırı gerçekleştirme) yaklaşımını benimser. Yani kurban sistemde herhangi bir ek yazılım çalıştırmadan, sadece Windows’un kendi iç yapısı (örneğin wscript.exe) kullanılarak saldırı gerçekleştirilir. Bu durum, araçların güvenlik duvarları veya antivirüsler tarafından daha az fark edilmesine neden olur.

Koadic’in en önemli kullanım alanı **sızma testi sonrası işlemler**dir. Yani hedef sisteme erişim sağlandıktan sonra kalıcılık kurmak, bilgi toplamak, komut çalıştırmak veya ağ içi yayılma (lateral movement) gibi işlemler için kullanılır. Red Team senaryolarında sıkça tercih edilen bir araçtır.

## Kurulum

Koadic, Python 2.7 ile çalışır ve genellikle Kali Linux üzerinde kullanılır. Kurulum için:

* git clone https://github.com/zerosum0x0/koadic
* cd koadic
* ./koadic

## Kullanım Örneği

Koadic arayüzü Metasploit'e benzer modüler bir yapıya sahiptir. Dinleyici (listener) oluşturulur, ardından payload hazırlanır ve hedefe iletilir.

**1. Listener Başlatmak:**



Bu komutla mshta.exe üzerinden çalışan bir stager başlatılır.

**2. Hedefe Payload iletmek:**

**Hedef sistemde aşağıdaki komut çalıştırılır:**



## **Elde Edilebilecek Bilgiler ve Etkiler**

Koadic ile aktif bağlantı kurulduğunda aşağıdaki işlemler yapılabilir:

* Komut satırı erişimi (cmd shell)
* Dosya yükleme / indirme
* Keylogger çalıştırma
* SAM veritabanından hash alma
* Token bilgisi çekme
* PowerShell betiği çalıştırma
* Ağ içi keşif (net view, arp -a)
* Kullanıcı bilgisi toplama
* UAC atlatma ve kalıcılık sağlama

## Parametreler ve Özellikler

Koadic, etkileşimli CLI (komut satırı arayüzü) ile çalışır. En çok kullanılan komutlar:

* use <module> → Modül seçimi
* set <parametre> <değer> → Parametre atama
* info → Modül hakkında bilgi
* run → Modülü çalıştırma
* jobs → Aktif görevleri görüntüleme
* zombies → Aktif bağlantıları (oturumları) listeleme

Kullanılan modüller genellikle stager/js/... veya implant/elevate/... gibi isimlendirilmiştir.

Koadic, sızma testi sonrası aşamalarda kullanılan, hafif, sessiz ve oldukça etkili bir **post-exploitation framework**tür. Windows Script Host (WSH) üzerinden çalıştığı için sistemdeki doğal bileşenleri kullanır ve tespiti zordur. Özellikle antivirüslerden kaçınma, network keşfi yapma ve iç ağda hareket etme gibi işlemleri hızlıca yapabilmesi nedeniyle, Red Team çalışmalarında ve saldırı simülasyonlarında sıkça tercih edilmektedir.