**🧠 1. MUNKA Nedir?**

**Munka**, Windows sistemlerinde kullanılan modern, esnek ve modüler bir **EDR/AV bypass ve yükleyici (loader)** framework’üdür.

Özellikle **Red Team** ve **Advanced Threat Simulation** görevlerinde kullanılır.

**🔐 2. Munka'nın Amaçları**

| **Amaç** | **Açıklama** |
| --- | --- |
| 🔒 EDR/AV atlatmak | API unhooking, syscalls, DLL injection teknikleri |
| 📦 Fileless Payload çalıştırmak | Bellekte çalışan zararlı kodu diske yazmadan yüklemek |
| ⚙️ Shellcode çalıştırmak | Şifreli shellcode’ları injection ile başlatmak |
| 🔁 Entegre edilebilirlik | Diğer C2 framework’leriyle kullanılabilir (Cobalt Strike, Havoc, vs.) |

**⚙️ 3. Kurulum (Kali Linux üzerinden kaynak derleme)**

**✅ Adım 1: Depoyu klonla**

git clone https://github.com/S4ntiagoP/munka.git

cd munka

**✅ Adım 2: Bağımlılıkları yükle**

Munka, Windows için derleneceği için Kali'de mingw-w64 kullanılır:

sudo apt install mingw-w64

**✅ Adım 3: Örnek payload’ı derle**

x86\_64-w64-mingw32-g++ -o loader.exe munka.cpp -lws2\_32

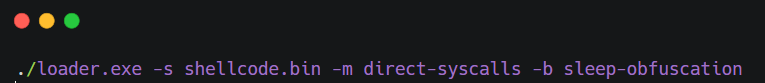
Bu komut, loader.exe adında shellcode yükleyicisi oluşturur.

**🧪 4. Kullanım Senaryosu**

* Belirli bir shellcode (.bin) ya da base64 kodlanmış payload yüklenir
* EDR algılamasını engellemek için:
  + VirtualAlloc yerine NtAllocateVirtualMemory
  + CreateThread yerine NtCreateThreadEx
  + AMSI/ETW patch modülleri uygulanır
* Payload hedef sistemde bellekte çalışır, disk izi bırakmaz

**🧬 5. Komut Örneği**

./loader.exe -s shellcode.bin -m direct-syscalls -b sleep-obfuscation



| **Parametre** | **Anlamı** |
| --- | --- |
| -s | Shellcode dosyası |
| -m | Yöntem: direct syscalls, tread hijack, dll hollowing |
| -b | Bypass tekniği: AMSI bypass, ETW patch, sleep patch |

**📷 6. Örnek Kali Terminal Çıktısı (Kurulum ve Derleme)**

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🎯 7. Öğrenim Kazanımları**

* Shellcode çalışma mantığını ve injection tekniklerini kavrama
* API Hooking ve Unhooking süreçlerini öğrenme
* EDR davranış modellerini bypass etme yöntemlerini anlama
* Windows post-exploitation araçlarının yapı taşlarını öğrenme