**🧠 1. Radare2 Nedir?**

**Radare2 (r2)**, açık kaynak kodlu, çok yönlü bir **binary analiz, hata ayıklama (debugging)** ve tersine mühendislik aracıdır.

* Çeşitli mimariler ve dosya formatlarını destekler
* Disassembly, debugging, patching, exploit geliştirme işlemlerini yapabilir
* CLI (komut satırı) tabanlıdır, ancak görsel arayüzleri de mevcuttur (Cutter, r2ghidra).

📌 IDA Pro ve Ghidra’ya ücretsiz ve güçlü bir alternatif olarak bilinir.

**🎯 2. Ne İşe Yarar?**

| **Özellik** | **Açıklama** |
| --- | --- |
| 🔍 Disassembly | Makine kodunu assembly’ye çevirir |
| 🐞 Debugging | Canlı olarak program çalışmasını izleme |
| 🧩 Binary patching | Çalışan veya derlenmiş kodu değiştirme |
| 📊 Malware analizi | Zararlı yazılım davranışını inceleme |
| 🛠️ Exploit geliştirme | Hafıza manipülasyonu, ROP chain oluşturma |
| 🔐 Kriptografik analiz | Şifreleme algoritmalarının tespiti |

**⚙️ 3. Kurulum (Kali / Linux)**

**✅ 1. Paket yöneticisi ile:**

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**✅ 2. Kaynak koddan kurulum (en güncel sürüm için):**

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🚀 4. Temel Kullanım Komutları**

**✅ 1. Dosya açma:**

r2 binaryfile

**✅ 2. Analiz başlatma:**

aa # Tüm analizleri yap

afl # Fonksiyon listesini göster

**✅ 3. Disassembly görüntüleme:**

pdf # Mevcut fonksiyonun assembly kodunu göster

**✅ 4. Debug modunda başlatma:**

r2 -d ./program

**✅ 5. Görsel mod:**

V # Görsel disassembly moduna geç

V! # Graf moduna geç

**📋 5. Örnek Terminal Çıktısı**metin, ekran görüntüsü, ekran, görüntüleme, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🧠 6. Kullanım Senaryoları**

| **Senaryo** | **Açıklama** |
| --- | --- |
| 🐞 Yazılım güvenlik testi | Binary reverse engineering ile zafiyet bulma |
| 🧩 Exploit geliştirme | Hafıza manipülasyonu ile güvenlik açığı kullanma |
| 🕵️‍♂️ Malware analizi | Zararlı yazılımın işleyişini inceleme |
| 🛠️ Binary patching | Mevcut kodu düzenleme ve yeniden paketleme |

**🎯 7. Öğrenim Kazanımları**

* Disassembly ve binary analiz becerilerini geliştirme
* Komut satırı tabanlı tersine mühendislik araçlarını kullanma
* Debugging ve patching tekniklerini öğrenme
* Exploit geliştirme mantığını kavrama