**YARA-X**, zararlı yazılım (malware) tespiti için kullanılan, YARA’nın yeni nesil ve yüksek performanslı bir sürümüdür. **YARA** kuralları ile ikili dosyaları, bellek imajlarını veya dosya sistemlerini taramak için geliştirilmiştir. **YARA-X**, Rust programlama diliyle yazılmıştır ve geleneksel YARA’ya göre çok daha hızlı çalışır.

YARA-X, özellikle büyük boyutlu dosyalarda, düşük kaynak kullanımı ve yüksek tarama hızı ile öne çıkar. Gelişmiş hata ayıklama ve daha sağlam bir kurallar motoru sunar.

**Bu Aracın Özellikleri Nelerdir?**

**Yüksek Performans**: Rust ile yazıldığı için çok hızlı ve kaynak dostudur.

**YARA Uyumluluğu**: Eski YARA kurallarını destekler.

**Kapsamlı Dosya Taraması**: Belirli dizinleri veya dosyaları kurallara göre tarar.

**Bellek Dostu**: Daha az RAM kullanır.

**YAML ve JSON Çıktı Desteği**: Çıktılar otomasyon sistemleriyle uyumlu olabilir.

**Kolay Kullanım**: Komut satırı üzerinden basit çağrılarla kullanılabilir.

**Açık Kaynak ve Aktif Geliştirme**: GitHub üzerinden erişilebilir.

**Bu Aracı Kali Linux’a Kurma ve Kullanma Adımları**

**Adım 1: Rust Programlama Dili Kurulumu**

YARA-X, Rust ile yazıldığı için önce Rust kurulmalıdır:

“curl https://sh.rustup.rs -sSf | sh

source $HOME/.cargo/env”

**Adım 2: YARA-X Reposunu Klonlayın**

YARA-X’in kaynak kodları sisteminize GitHub üzerinden klonlamak gerekir ve sonrasında klonlanan dizine girilir.

“git clone https://github.com/VirusTotal/yara-x.git

cd yara-x”

**Adım 3: Derleme ve Kurulum**

“cargo build –release”

İşlem tamamlandığında target/release/yarax dosyası oluşur.

Kullanımı kolaylaştırmak için binary dosyasını /usr/local/bin dizinine kopyalayın:

“sudo cp target/release/yarax /usr/local/bin/” Şimdi yarax komutu sistem genelinde tanınır.

**Adım 4: Basit Bir Kural ve Taramayı Test Etme**

“nano test\_rule.yar” ile örnek bir Yara kural dosyası oluşturun

İçeriği şu şekilde olsun

metin, yazı tipi, ekran görüntüsü, sayı, numara içeren bir resim

Açıklama otomatik olarak oluşturuldu

Bu kural, PE dosyalarının başında bulunan “MZ” karakterini arar.

**Şimdi bir dosyayı bu kurala göre tarayın:**

“yarax scan -r test\_rule.yar /bin/ls”

Örnek çıktı :

metin, ekran görüntüsü, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu