# YARA Aracı Nedir? Ne İşe Yarar?

Hedef Kitle: Lise Öğrencileri İçin Basit Anlatım

## 1. Giriş: Siber Dünyada Bir Dedektif

Bilgisayarlar her geçen gün daha çok tehdit altında. Virüsler, trojanlar, casus yazılımlar... Bunları yakalamak için siber güvenlik uzmanları özel araçlar kullanır. İşte bu araçlardan biri YARA’dır.  
  
YARA, kötü amaçlı yazılımları tespit etmek için kullanılan bir kural tabanlı analiz aracıdır.

## 2. YARA Ne İşe Yarar?

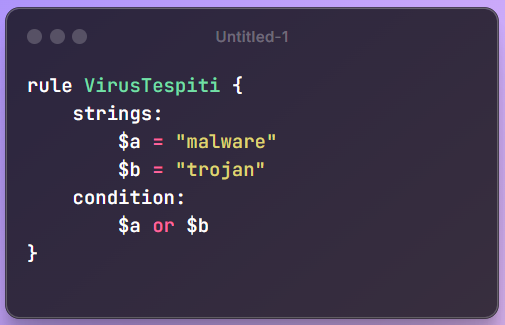
YARA, bilgisayardaki dosyaları belirli kurallara göre tarar. Bu kurallar sayesinde dosyanın içinde şüpheli bir kelime, kod ya da imza varsa onu yakalar.  
  
Kısaca:  
“Bir dosyada ‘virüs izi’ varsa, bana haber ver!” diyebileceğiniz bir araçtır.

## 3. YARA Nasıl Çalışır?

YARA’nın çalışma mantığı oldukça basittir:  
- Kural yazılır: Dosyada aranan şüpheli kelimeler/kodlar belirtilir.  
- Taramaya başlanır: Kurallarla bilgisayardaki dosyalar taranır.  
- Uyarı verilir: Eğer kural eşleşirse, “şüpheli dosya bulundu” mesajı gösterilir.

## 4. YARA Kuralları Nasıl Yazılır?

Bir YARA kuralı genellikle şu bölümlerden oluşur:



Bu örnekte:  
- "malware" veya "trojan" geçen dosyalar şüpheli kabul edilir.

## 5. YARA Nasıl Kullanılır?

- YARA’yı İndir: Resmi GitHub sayfasından ya da terminal komutlarıyla.  
- Kural Dosyası Oluştur: Kurallar `.yar` uzantılı dosyalara yazılır.  
- Dosyayı Tara: Örnek komut:

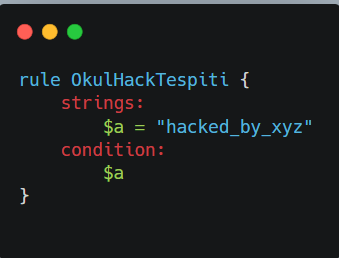
## 

## 6. Nerelerde Kullanılır?

- Siber güvenlik analizlerinde  
- Zararlı yazılım incelemelerinde  
- Bilgisayar adli tıbbı (digital forensics) alanında  
- Antivirüs şirketlerinin tespit sistemlerinde

## 7. Gerçek Hayattan Örnek

Diyelim ki bir hacker, okul sunucusuna zararlı bir dosya yerleştirdi. Bu dosya içinde "hacked\_by\_xyz" yazısı var.  
  
Sen bir YARA kuralı yazarsın:

******

Bu kuralla o zararlı dosya kolayca tespit edilebilir.

## 8. Neden Önemlidir?

- Kendi kurallarını yazabilirsin (kişiselleştirilebilir).  
- Antivirüslerin kaçırabileceği tehditleri yakalayabilir.  
- Gelişmiş analiz ve güvenlik sağlar.

## 9. Sonuç: Siber Güvenliğin Gizli Kahramanı

YARA, virüsleri yakalamakta kullanılan bir “dedektif” gibidir. Özellikle siber güvenlik kariyerine ilgi duyan öğrenciler için öğrenilmesi çok değerli bir araçtır.