**FIRMADYNE Nedir?**

Firmadyne, gömülü cihazlara ait firmware dosyalarını analiz etmek ve bu firmware’leri emülatör üzerinde çalıştırarak test etmek için kullanılan bir açık kaynaklı otomatik firmware analiz aracıdır.

Kısaca şöyle düşünebilirsin:   
> Bir modem ya da router gibi cihazların içinde çalışan özel yazılımlar vardır (firmware). Bu yazılımı alıp, sanal bir ortamda çalıştırmak ve güvenlik açıklarını görmek istersen, işte burada Firmadyne devreye girer.

**Ne İşe Yarar?**

-Gömülü sistemlerin firmware dosyasını analiz eder.

-O firmware’in içinde çalışan sistemi sanal olarak çalıştırır (emüle eder).

-İçindeki servisleri, açık portları ve varsa zafiyetleri görmeni sağlar. -Otomatik analiz yapar, bu yüzden çok zaman kazandırır.

**Nasıl Çalışır?**

1. Firmware Dosyası Verilir: .bin ya da .img gibi uzantılarla.

2. Firmware’i Açar: İçinde hangi sistemler, dosyalar, servisler var gösterir. 3. Sanal Ortamda Çalıştırır: QEMU gibi emülatörlerle sanal ortamda başlatır.

4. Ağ Trafiği ve Portlar Dinlenir: Cihaz sanki çalışıyormuş gibi analiz edilir. 5. Zafiyetler Tespit Edilir: Hangi güvenlik açıkları var, neler yapılabilir görülür.

**Avantajları:**   
-Otomatikleştirilmiş analiz sağlar.

-Cihazı fiziksel olarak elinde tutmadan analiz edebilirsin.

-Gerçek sisteme benzer koşullarda test imkânı sunar. -Açık kaynaklı ve ücretsizdir.

**Sınırlamaları:**   
-Kurulumu biraz karmaşık olabilir.

-Her firmware çalışmayabilir (özellikle özel yapılandırılmış olanlar). -Yüksek sistem kaynağı gerektirebilir (çünkü emülasyon kullanır). -Detaylı Linux bilgisi gerekebilir.

**- Öğrenci Gözünden Özetle:**   
Firmadyne, modem, router gibi cihazların içini açıp sanal bir bilgisayarda çalıştırmamızı sağlar. Böylece o cihazı hiç dokunmadan siber güvenlik testleri yapabiliriz. Özellikle CTF yarışmaları, sızma testleri ve IoT güvenliği ile ilgilenen öğrenciler için süper bir araçtır.