**FOCA**

**FOCA** (Fingerprinting Organizations with Collected Archives), dosyaların içinde gizli kalan metadata (meta veriler) bilgilerini keşfetmek, toplamak ve analiz etmek için kullanılan bir siber güvenlik aracıdır. Özellikle Word, PDF, Excel gibi belgelerde bulunan yazılım bilgileri, yazar adı, tarih, IP adresi, dosya yolu gibi kritik bilgiler FOCA ile çıkarılır. Bu bilgiler sızma testlerinde ve güvenlik analizlerinde hedef organizasyon hakkında değerli bilgiler sağlar.

**Özellikleri**

* **Çeşitli Dosya Türlerini Destekler:** Word, Excel, PowerPoint, PDF, OpenOffice ve daha birçok doküman türündeki metadata’yı analiz edebilir.
* **İnternet ve Yerel Kaynaklardan Tarama:** FOCA, hedef organizasyonun web sitesinden veya yerel dosya sisteminden dosya indirip metadata toplama yapabilir.
* **Gelişmiş Metadata Çıkarımı:** Yazar bilgileri, yazılım versiyonu, oluşturulma ve değiştirilme tarihleri, kullanıcı isimleri, IP adresleri gibi birçok meta veriyi tespit eder.
* **Raporlama:** Toplanan verileri detaylı raporlar halinde sunar.
* **Kullanıcı Dostu Arayüz:** Grafiksel kullanıcı arayüzü (GUI) sayesinde kolay kullanım sağlar.
* **Arama Motorları ile Entegrasyon:** Google, Bing gibi arama motorlarını kullanarak hedef domain üzerindeki dökümanları otomatik tarayabilir.

**Kullanım Alanları**

* **Sızma Testleri ve Güvenlik Analizleri:** Hedef organizasyon hakkında bilgi toplama aşamasında kritik meta veri keşfi için.
* **Siber İstihbarat (OSINT):** Açık kaynaklardan bilgi toplamada organizasyonun yapısı, kullanılan yazılımlar, kullanıcılar hakkında veri elde etmek için.
* **Döküman Güvenliği Değerlendirmesi:** Belgelerde gereksiz metadata bulunup bulunmadığını kontrol etmek ve temizlemek için.
* **Bilgi Sızıntısı Risk Analizi:** Organizasyonun iç bilgilerini ifşa eden metadata risklerini değerlendirmek.

**Kurulum Aşaması**

FOCA genellikle Windows ortamında çalışır. Kali Linux gibi bazı Linux dağıtımlarında Wine ile çalıştırmak mümkün olsa da en yaygın ve stabil kullanımı Windows’ta olur.

1. **Gereksinimler:**
   * Windows işletim sistemi (Windows 7 ve üzeri önerilir)
   * .NET Framework (varsayılan olarak Windows’ta bulunur)
   * İnternet bağlantısı (tarama ve güncelleme için)
2. **Kurulum:**

* FOCA’yı resmi web sitesinden indirmeniz önerilir:

**Resmi FOCA Web Sitesi:**  
https://www.elevenpaths.com/labstools/foca/index.html

* Kurulum sihirbazını takip ederek programı kurarsınız.
* Program açıldıktan sonra hedef domain veya dosya yolu girilerek analiz başlatılır.

1. **Kullanım:**

* FOCA arayüzünden “New Project” ile yeni analiz başlatılır.
* Hedef domain girilir ve arama motorları kullanılarak dökümanlar toplanır.
* İndirilen dosyalardaki metadata otomatik çıkarılır ve raporlanır.

**Dikkat Edilmesi Gerekenler**

* **Yasal İzin:** FOCA ile yapılacak taramalar ve analizler için hedef organizasyondan izin alınmalıdır. Aksi halde yasal sorunlar yaşanabilir.
* **Veri Gizliliği:** Toplanan metadata hassas bilgiler içerebilir. Elde edilen bilgiler gizli tutulmalı ve sadece yetkili kişilerle paylaşılmalıdır.
* **Tarama Limiti:** Çok büyük hedeflerde arama motorlarının kısıtlamaları ve IP engelleme riski olabilir.
* **Güncel Sürüm Kullanımı:** FOCA’nın güncel sürümleri kullanılarak yeni dosya formatları ve meta veri tipleri desteklenmelidir.
* **Fals-positive ve Fals-negative Durumlar:** Bazı meta veriler eksik veya yanıltıcı olabilir, bu nedenle sonuçlar dikkatle yorumlanmalıdır.