**Modlishka**, gelişmiş phishing (oltalama) saldırılarında kullanılan, ters proxy tabanlı ve güçlü bir **man-in-the-middle (MitM)** aracıdır. Kullanıcı ile hedef web sitesi arasına girerek gerçek zamanlı oturum verilerini (cookie, token, kimlik bilgileri) toplamak için kullanılır. Özellikle 2FA (iki faktörlü kimlik doğrulama) mekanizmalarını atlatabilme kabiliyeti ile dikkat çeker.

**Bu aracın özellikleri nelerdir?**

**Ters Proxy Mimarisi:** Gerçek site ile kurban arasındaki trafiği proxy üzerinden geçirir.

**Gerçek Zamanlı Veri Yakalama:** Kullanıcı adı, şifre, session cookie gibi kritik bilgileri anında elde edebilir.

**2FA Bypass:** Kullanıcının OTP’sini (tek kullanımlık şifre) de yakalayarak oturum açılmasını sağlar.

**SSL/TLS Desteği:** HTTPS trafiğini şeffaf bir şekilde yönlendirebilir.

**Gerçekçi Arayüz:** Kurbanlar orijinal site arayüzüyle karşılaştığı için kandırılmaları kolaydır.

**Otomatik Yapılandırma:** config dosyası ile hedefin sahte kopyası kolayca oluşturulabilir.

**Açık Kaynak:** GitHub üzerinden erişilebilir ve özelleştirilebilir.

**Bu aracı Kali Linux'a kurma ve kullanma adımları:**

**Adım 1: Gerekli Yazılımları Kurun (Go Programlama Dili)**

Modlishka, Go diliyle yazılmıştır. Bu nedenle sisteminizde Go dili yüklü değilse öncelikle aşağıdaki komutlarla yüklenmesi gerekir:

“sudo apt update

sudo apt install golang-go”

**Adım 2: GitHub Üzerinden Modlishka’yı İndirin**

Bu komut sayesinde Modlishka’nın kaynak kodlarını GitHub üzerinden sisteminize klonlarsınız. Sonrasında ise indirdiğiniz dizine girin”

“git clone <https://github.com/drk1wi/Modlishka.git>

cd Modlishka”

**Adım 3: Modlishka’yı Derleyin (Build Edin)**

İndirdiğiniz kaynak dosyaların bulunduğu dizine girdikten sonra, aşağıdaki komutu kullanarak modlishka isimli çalıştırılabilir dosyayı oluşturun:

“go build -o modlishka”

Bu adım başarıyla tamamlandığında, çalıştırılabilir modlishka dosyası oluşur.

**Adım 4: Konfigürasyon (config.json) Dosyasını Oluşturun**

Modlishka’nın çalışabilmesi için, hedef sitenin detaylarını ve yönlendirme yapılandırmalarını içeren bir JSON formatında konfigürasyon dosyası gereklidir. Örnek bir config.json dosyasında şu alanlar yer alabilir:

* Hedef domain (target)
* Sahte domain (phishingDomain)
* HTTPS sertifika ayarları
* Oturum günlüğü dosya yolları

Bu dosya manuel olarak hazırlanabilir veya GitHub’daki örneklerden faydalanılabilir.

**Adım 5: Modlishka’yı Başlatın**

Yapılandırma dosyanız hazır olduktan sonra aşağıdaki komutu kullanarak aracı başlatabilirsiniz:

“./modlishka -config config.json”

metin, ekran görüntüsü, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu