Evilginx2 Eğitim Materyali

# 📌 Evilginx2 Nedir?

Evilginx2, sosyal mühendislik saldırıları için kullanılan bir MITM (Man-in-the-Middle) frameworküdür. Temel amacı, kullanıcıların oturum çerezlerini çalarak 2FA (İki Faktörlü Kimlik Doğrulama) korumasını atlatmak ve hesaplara erişim sağlamaktır. Özellikle kimlik avı (phishing) saldırıları için kullanılır.

# ⚙️ Evilginx2’nin Özellikleri

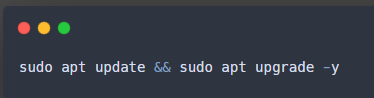
* 🔐 2FA korumasını atlatabilir (çerez yakalama ile).
* 🌐 HTTPS desteğiyle sahte web siteleri barındırabilir.
* 🎯 Hedefe özel oturum çerezi (session token) toplar.
* 🧰 Modüler yapıdadır, farklı hedefler için phishlet kullanılabilir.
* 🧩 Açık kaynaklıdır (Go dilinde yazılmıştır).

# 📍 Nerelerde Kullanılır?

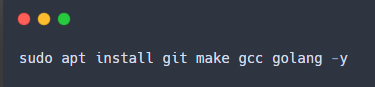
* 🛡️ Siber güvenlik eğitimlerinde (pentest çalışmaları).
* 🧪 Güvenlik farkındalık testlerinde.
* 🔬 Sosyal mühendislik zafiyetlerini analiz etmede.
* 👨‍💻 Bilgi güvenliği laboratuvarlarında.

# 🧪 Evilginx2 Kurulumu – Kali Linux (Adım Adım)

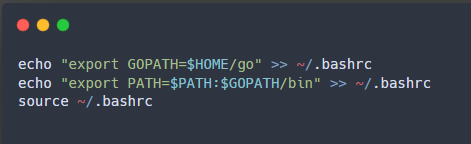
1. 1. Sistem Güncellemesi

******

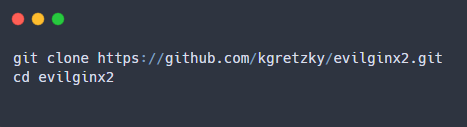
2. Gerekli Bağımlılıkları Kur

******

3. Go Ortam Değişkenlerini Ayarla

******

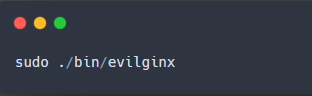
4. Evilginx2 Kaynak Kodunu Klonla

******

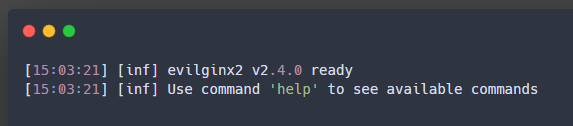
5. Derleme

******

6. Çalıştırma

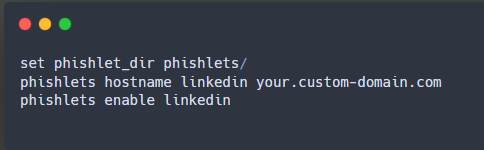
******

✔️ Beklenen Çıktı

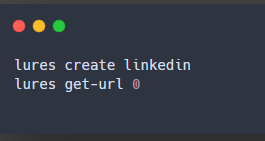
**

# 🔧 Basit Evilginx2 Kullanımı (Örnek)

1. DNS Ayarlarını Yap

******

2. Link Oluştur

******

3. Hedef linke tıkladığında, yakalanan bilgiler

# 

# 🎓 Kısa Notlar – Öğrenciler İçin

* Evilginx2 etik olmayan amaçlarla kullanılmamalıdır.
* Sadece izinli sistemlerde test yapılmalıdır.
* 2FA her zaman güvenli değildir, özellikle oturum çerezleri ele geçirilebilir.
* DNS ve HTTPS konularını öğrenmek, Evilginx2’nin nasıl çalıştığını anlamak için önemlidir.
* Siber güvenlik eğitimleri, bilinçli kullanıcılar yetiştirmek içindir – saldırganlar değil.