**Evilginx2**

**1. Nedir?**

**Evilginx2**, siber güvenlik uzmanları ve Red Team çalışanları tarafından kullanılan, **oturum çalma (session hijacking)** amacıyla kullanılan bir “**phishing framework**” yani gelişmiş oltalama platformudur.  
Kısaca: Kullanıcıların giriş yaptığı **oturum bilgilerini çalmak** için kullanılır. (Amaç eğitim ve testtir.)



**2. Ne işe yarar?**

* Evilginx2 sayesinde sahte bir giriş sayfası oluşturulabilir (örneğin sahte bir Google sayfası).
* Hedef kişi bu sahte sayfaya kullanıcı adı ve şifresini girdiğinde, sadece şifre değil, aynı zamanda **oturum bilgisi** (cookie) de çalınır.
* Bu sayede saldırgan, kullanıcı adı/şifreye bile ihtiyaç duymadan kurbanın hesabına girebilir.

**‼️ Bu araç gerçek hayatta çok tehlikelidir, yalnızca eğitim, test ve etik amaçlarla kullanılır.**

**3. Neden önemlidir?**

* Günümüzde iki faktörlü doğrulama (2FA) bile kullanılsa, Evilginx2 bu korumayı **atlayabilir**.
* Bu, saldırganların gerçekten kimlik doğrulama sistemini aşmasını sağlar.
* O yüzden güvenlik uzmanlarının bu tür tehditleri anlaması ve savunma geliştirmesi **hayati önemdedir.**

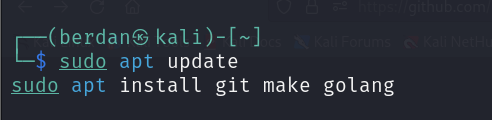
**4. Nasıl Kurulur? (Ubuntu / Kali için)**

Evilginx2 doğrudan Go programlama dili ile kurulabilir.

1. Gerekli paketleri kur:

**sudo apt update**

**sudo apt install git make golang**

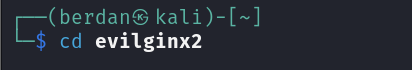
****

1. Evilginx2’yi indir:

**git clone** [**https://github.com/kgretzky/evilginx2.git**](https://github.com/kgretzky/evilginx2.git)



**cd evilginx2**

****

1. Çalıştır:

**./bin/evilginx**

****

Artık terminalden komutlarla sahte siteler ve kampanyalar oluşturabilirsin.

Not: Genelde bir alan adı ve HTTPS sertifikası (Let's Encrypt) da gerekir.

**5. Örnek Bir Anlatım:**

Diyelim ki sahte bir Facebook giriş sayfası kurmak istiyorsun:

1. Evilginx2 ile facebook için bir “phishlet” (hazır ayar) yüklenir.
2. Alan adı (örneğin facebook-login-support.com) alınır.
3. Kurban bu siteye yönlendirilir.
4. Giriş yaptıktan sonra Evilginx2 kullanıcı adı, şifre ve **oturum çerezlerini (session cookie)** alır.
5. Bu çerez başka bir tarayıcıya yapıştırıldığında, Facebook hesabına şifresiz girilebilir.

**Amaç:** Bu saldırıların nasıl yapıldığını görerek, savunma yöntemlerini geliştirmek.