**SocialFish Nedir?**

SocialFish, sosyal mühendislik temelli phishing saldırıları için geliştirilmiş bir açık kaynaklı Python tabanlı araçtır. Özellikle sosyal medya ve popüler platformların giriş sayfalarını taklit ederek hedefin kullanıcı adını ve şifresini ele geçirir. Web tabanlı arayüzü sayesinde kullanıcı dostudur, ayrıca Android mobil kontrol uygulaması desteği de vardır.

**SocialFish ile Neler Yapılabilir?**

Sosyal medya platformları (Facebook, Instagram, Twitter, LinkedIn, GitHub vb.) için sahte giriş sayfaları hazırlayabilir.

Otomatik olarak ngrok entegrasyonu ile internetten erişilebilir bağlantılar oluşturur.

Hedefin girdiği kullanıcı adı, şifre, hatta IP ve konum bilgilerini anlık olarak toplar.

Kendi Özelleştirilmiş mobil uygulama aracılığıyla saldırıyı yönetme imkânları sunar.

**SocialFish Kurulumu & Başlatma**

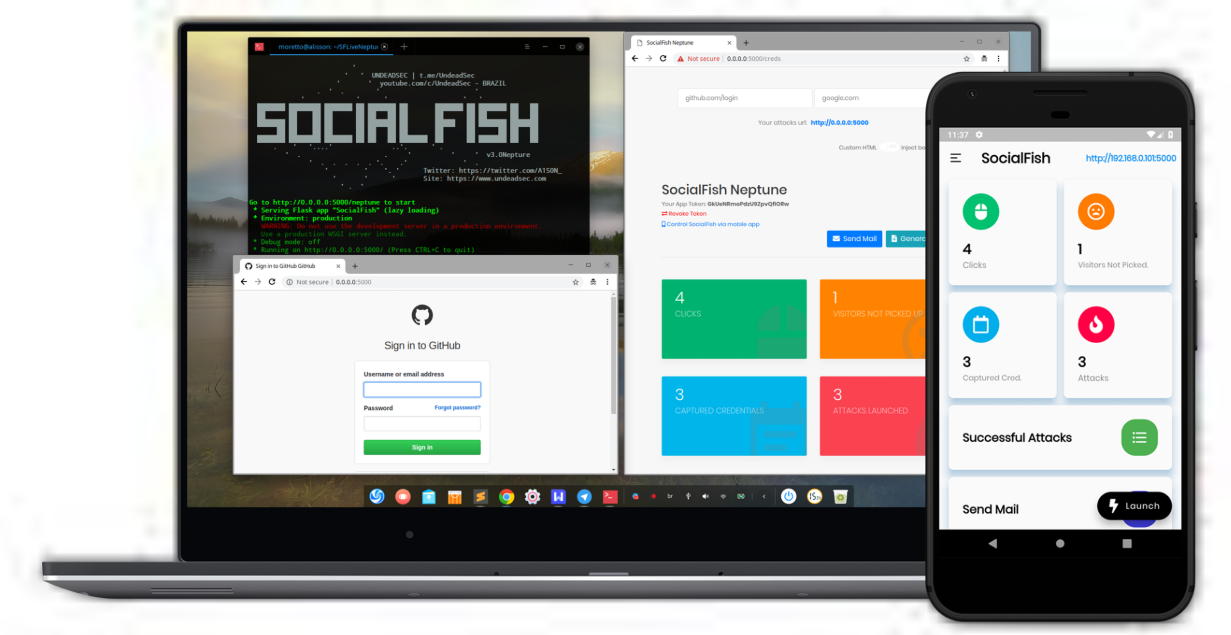
***git clone https://github.com/UndeadSec/SocialFish.git***

***cd SocialFish***

***pip3 install -r requirements.txt***

***chmod +x SocialFish.py***

***python3 SocialFish.py <admin-user> <admin-pass>***

******

Bu ekran SocialFish arayüzündeki şablon seçimi, saldırı linki oluşturma ve kampanya yönetim bölümlerini göstermektedir.

**Konfigürasyon – Web Şablonu Hazırlamak**

Admin panelden platform seçilir.

(İsteğe bağlı) BeEF entegrasyonuyle bağlantı eklenebilir.

"Start attack" veya "Generate link" butonuna basılır.

ngrok ile oluşturulan link hedefe gönderilir.



Bu ekranda SocialFish konsolunda, ngrok linki oluşturma ve hedefin girdiği kullanıcı adı/parola gibi bilgilerin gerçek zamanlı izlendiği bölüm yer alıyor.

**Olayın Detaylı İşleyişi (Post Log)**

Hedef linke tıkladığında:

* Giriş bilgileri kaydedilir.
* Hedef, genelde orijinal siteye yönlendirilir (redirect).
* Log sekmesinden veriler detaylı incelenebilir.

**Öğrencilere Uyarılar**

* Yalnızca **yetkilendirilmiş sistemler** üzerinde test yapılmalı. Aksi hâlde hukuki sorunlar yaşanabilir.
* Phishing saldırıları ciddi gizlilik ve veri güvenliği sorunu oluşturur.
* Loglarda **alakasız sonuçlar** görülebilir; şüpheli linklerin kullanımı yaygındır (örneğin facebook.victim.site gibi).
* Bu aracı eğitimsel veya yasal penetrasyon testi amaçlı kullanmak temel gerekliliktir.

**Neden SocialFish Öğretici?**

Bu araç, phishing saldırısının gerçekte ne kadar kolay ve fark edilir olmadığını gösterir. Güvenlik farkındalığı eğitimlerinde sosyal mühendislik temeline dayalı saldırı örneklerinin en iyi görsel anlatımıdır.