**Weeman Nedir?**

Weeman, Python (2.7) ile yazılmış, yerel ağ veya Termux üzerinde HTTP tabanlı phishing saldırıları oluşturmak için kullanılan bir araçtır. DNS spoofing veya ngrok gibi yöntemlerle birlikte çalışarak hedef kullanıcıları sahte giriş sayfasına yönlendirip kullanıcı adı, şifre gibi bilgileri toplar.

**Weeman ile Neler Yapabilirsiniz?**

* **Fake HTML sayfa oluşturma**: Target sitenin login sayfası klonlanır.
* **POST yakalama**: Kullanıcının girdiği veriler toplanır.
* **Otomatik orijinal site yönlendirme**: Hedef, bilgilerini girdikten sonra gerçek siteye yönlendirilir.
* **Profil, modül desteği**: Mobil/masaüstü profiller ve eklenti mekanizmaları bulunur.
* **Termux / Linux uyumlu**: Python 2.7 destekli Termux üzerinden çalışabilir.

**Weeman Kurulum & Başlatma**

***git clone https://github.com/evait-security/weeman.git***

***cd weeman***

***pip2 install beautifulsoup4***

***chmod +x weeman.py***

***python2 weeman.py***

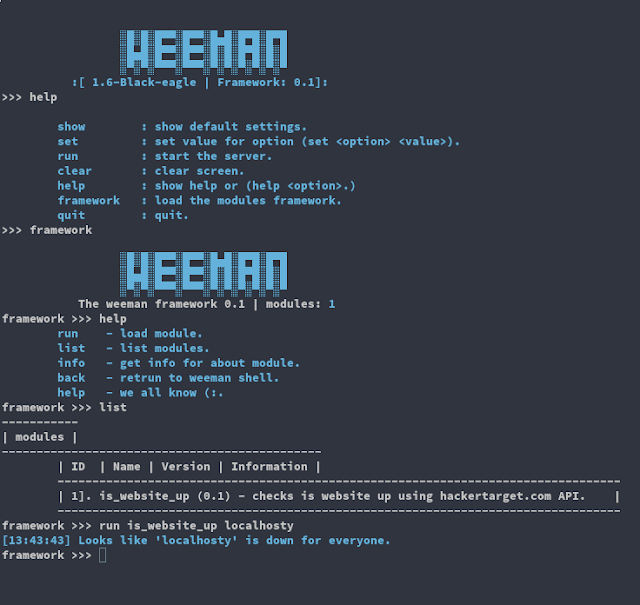
Ardından komut satırında şu adımları takip edersiniz:

***set url http://target.site/login***

***set action\_url http://target.site/post\_login***

***set port 8080***

***run***



Bu görüntüde Weeman aracı açıldığında terminalde:

* set url, set action\_url, set port gibi komutlarla phishing kampanyası yapılandırılıyor.
* run komutu sonrası aktif saldırı ve gelen POST verileri görüntüleniyor.

**Weeman Kullanım Akışı**

* **set url** → hedef login sayfasını klonluyor.
* **set action\_url** → form verilerinin yakalanacağı URL’yi belirliyor.
* **set port** → HTTP sunucusunun dinleyeceği port.
* **run** → phishing sunucusu başlıyor. Bağlı kullanıcılar için oturum kaydını intihal ederek log alınıyor.

**Weeman ile Sınıf İçi Uygulama Senaryosu**

Öğrenciler için uygulamalı bir test önerisi:

1. Lokal veya Termux ortamında Weeman kurun.
2. Hedef olarak sahte bir test sayfası hazırlayın (örneğin, localhost/login).
3. set url → set action\_url → set port komutlarını uygulayın.
4. run komutuyla saldırıyı başlatın ve başka bir tarayıcıdan erişin.
5. Konsolda hedef kullanıcı adı ve şifre girildiğinde log kaydını görün.
6. Otomatik yönlendirme mekanizmasını inceleyin.

**Etik ve Güvenlik Notları**

* **İzinli testler** dışında kullanım yasa dışıdır ve etik değildir.
* **SSL/HTTPS sahtekarlığı**: Hedef site HTTPS ise Weeman bunu bypass edemez, sertifika hatası oluşur.
* **Detaylı loglar**: IP, zaman damgası gibi kritik veriler konsolda ve dosyada yer alabilir.
* **Sosyal mühendislik farkındalığı**: Sahte linkler, domen kontrolü ve URL incelemesi öğretilmeli.

Weeman, sosyal mühendislik temelli phishing saldırılarını pratik ve görünür şekilde uygulamaya imkan tanıdığı için güvenlik eğitimlerinde çok değerlidir. Özellikle:

* Python tabanlı terminal çalışması,
* Phishing saldırısının adım adım loglanması,
* Etik ve hukuki sınırlar dahilinde kullanılması gerekliliği öğretilmesi açısından faydalıdır.