Social-Engineer Toolkit (SET) Kullanım Kılavuzu

Social-Engineer Toolkit (SET), sosyal mühendislik saldırılarını simüle etmek için kullanılan güçlü bir araçtır. Bu kılavuz, SET aracı ile kimlik avı (phishing) senaryosu hazırlamak isteyenler için temel adımları Türkçe olarak açıklar.

# 1. Ana Menü

SET’i başlattığınızda karşınıza şu menü gelir:  
  
 1) Sosyal Mühendislik Saldırıları  
 2) Sızma Testi (Fast-Track)  
 3) Üçüncü Parti Modüller  
 4) SET'i Güncelle  
 5) Konfigürasyonları Güncelle  
 6) Yardım ve Hakkında  
  
 99) Çıkış  
  
Buradan '1' yazarak Sosyal Mühendislik Saldırıları bölümüne giriyoruz.

# 2. Sosyal Mühendislik Saldırı Türleri

1) Java Applet Saldırısı  
2) Metasploit Tarayıcı Açığı Yöntemi  
3) Kimlik Bilgisi Toplayıcı (Credential Harvester)  
4) Sekme Değiştirme (Tabnabbing)  
5) Web Jacking  
6) Çoklu Saldırı (Multi-Attack)  
7) HTA Saldırısı  
  
Bu listeden ‘3’ seçilerek Kimlik Bilgisi Toplayıcı yöntemi kullanılır.

# 3. Web Sayfası Kopyalama Seçenekleri

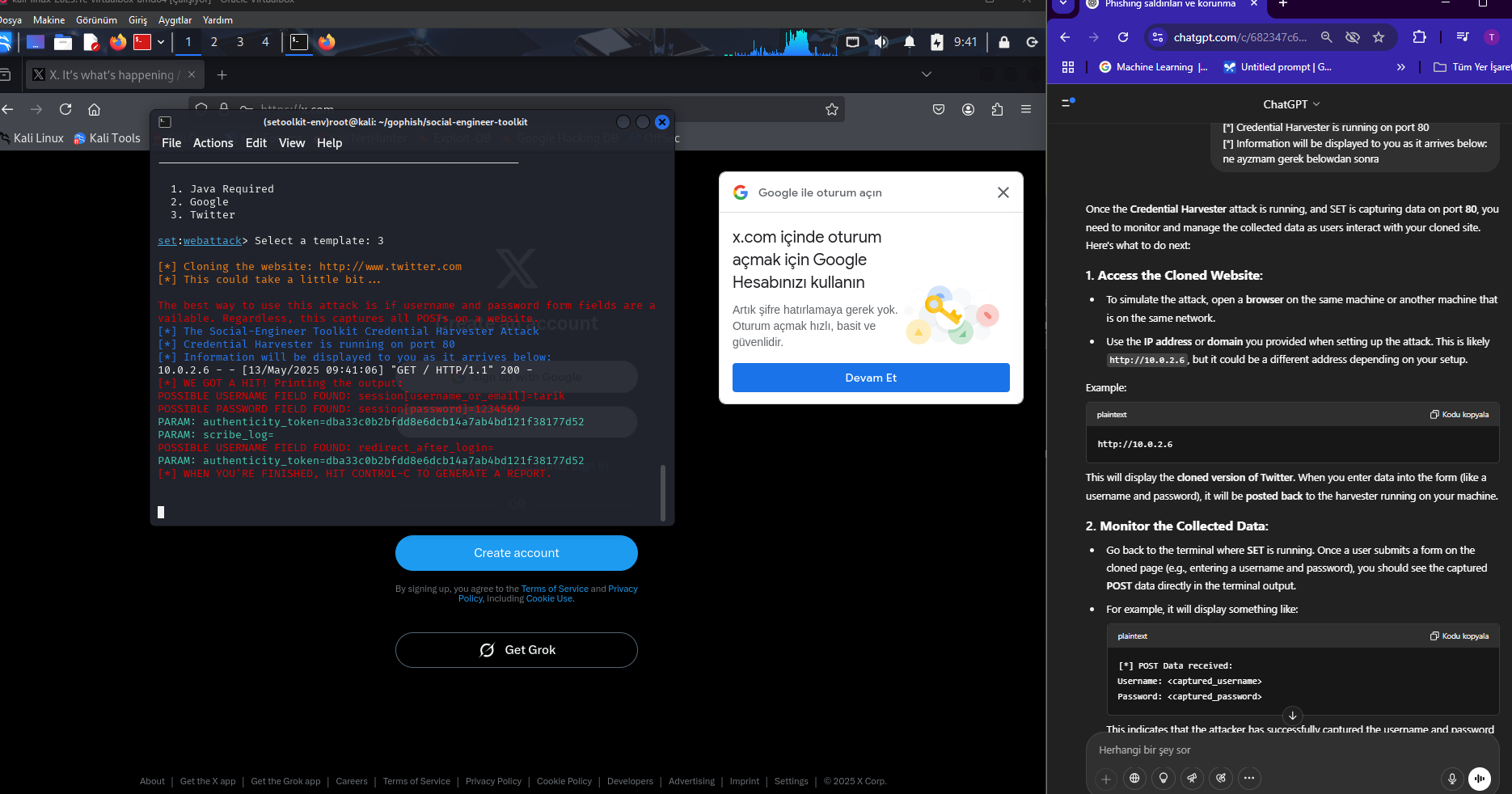
1) Hazır Web Şablonları  
2) Site Klonlayıcı  
3) Özel Site Yükle (Import)  
  
Buradan '2' seçilerek klonlanacak bir web sitesi (örnek: http://www.twitter.com) girilir.

# 4. IP Adresi Girişi

SET, yakalanan verileri nereye göndereceğini bilmek için sizden bir IP adresi ister.  
  
Sanal makine kullanıyorsanız, terminalde `ip a` komutuyla `inet` satırındaki IP adresinizi bulun (örnek: 10.0.2.6) ve girin.

# 5. Saldırıyı Başlatma ve Bilgi Toplama

Gerekli adımlar tamamlandıktan sonra SET, 80 numaralı port üzerinde sahte siteyi çalıştırır. Hedef kişi bu siteye giriş yaptığında kullanıcı adı ve şifre bilgileri SET ekranında görünür.  
  
Bu bilgiler aynı zamanda log dosyasına kaydedilir.



Örnekde görüldüğü gibi şifre ve kullanıcı adı.

Twitter giriş template ise bu oluyor ve porttan iletişim kurarak tbilgileri gönderiyor.  
