Beef

> **BeEF (Browser Exploitation Framework)**, web tarayıcılarını hedef alarak sistemlere sızmak veya güvenlik açıklarını analiz etmek için kullanılan bir **penetrasyon testi aracıdır**. BeEF, özellikle istemci tarafı (client-side) saldırılarına odaklanır ve hedef kullanıcının tarayıcısını "hook" ederek, yani kontrol altına alarak çeşitli komutlar çalıştırmanı sağlar.

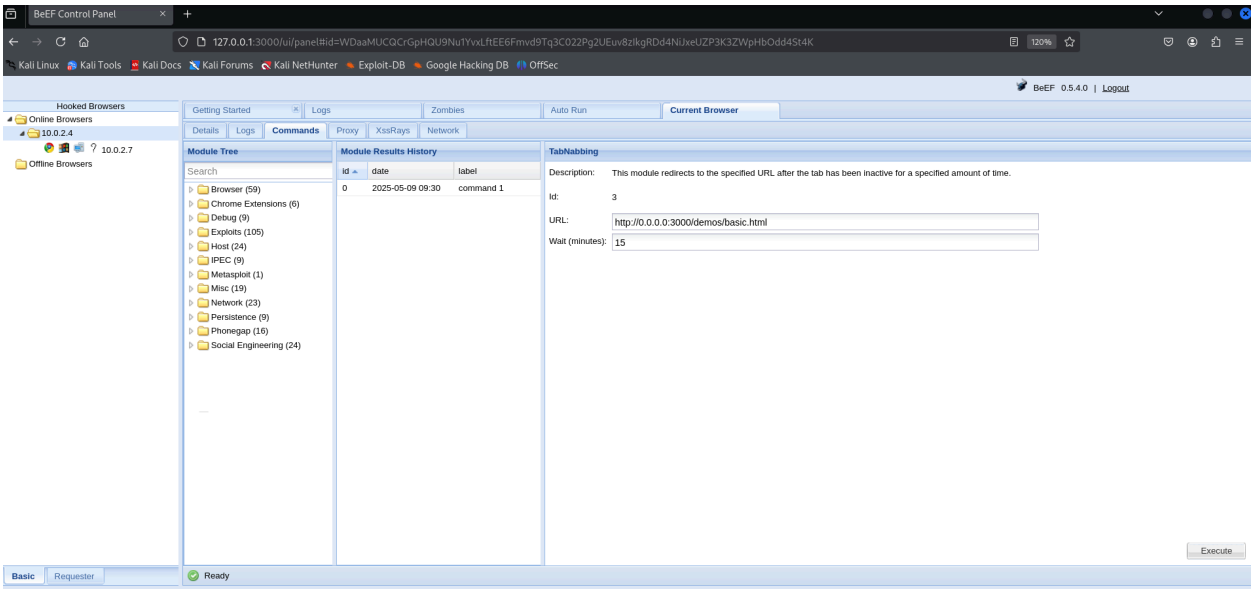
- `beef-xss` komutuyla çalıştırılır.
- Verilen web sitesinden giriş yapılır.(kullanıcı adı beef,şifre terminalden belirlenecek.)
- Terminalde yer alan hookdaki adresin bir web sitesinde olması yeterlidir.Kurban bilgisayara bu web sitesini verirsek oltalamış oluruz.

Ağ içi saldırı yapmak

- `service apache2 start` ile sunucuyu açalım.
- Ardından sunucu dosyamızdaki index.html dosyasını düzenleyelim. (*var→www→html*)
- Hook'un altında yer alan örnek kod kendi ip adresimize göre düzenlenip bu dosyaya eklenir.(Kali ip adresi)

bettercap ile JS enjeksiyonu

- beefcustom.zip dosyası indilir ve içindeki dosyalar caplets klasörüne atılır. (*usr→share→bettercap→caplets*)
- Dosyalardaki ip adresi kendimize göre ayarlanır.
- `bettercap -iface th0 -caplet /usr/share/bettercap/caplets/beefcustom/beefcustom.cap` komutuyla dosya çalıştırılır.
- Beef panelinden yönetilir.



Beef control panel

🖋Ömer Faruk Baysal