## Websploit Nedir, Neden Kullanılır?

Websploit, açık kaynak kodlu, Python tabanlı gelişmiş bir sızma testi aracıdır. Özellikle **MITM (Man-in-the-Middle)** saldırıları, ağ keşifleri ve Exploit testleri üzerine odaklanır. Kali Linux gibi birçok güvenlik dağıtımı ile önceden yüklü gelir. Metasploit Framework ile entegre çalışabilir.

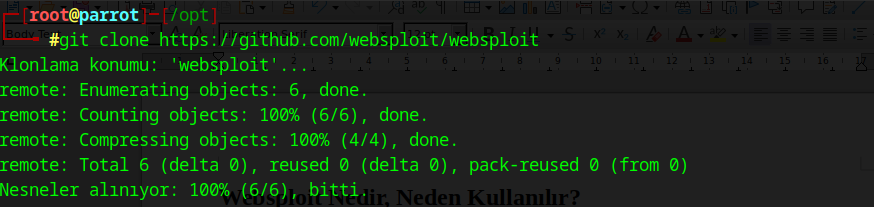
Bu araç; ağ dinleme, ARP spoofing, DNS spoofing, web saldırı simülasyonları ve daha fazlası için güçlü modüller içerir. Saldırganlar ya da sızma testi uzmanları için, bir hedef ağ ortamında kullanıcı trafiğini yönlendirmek, manipüle etmek ya da zafiyetleri analiz etmek amacıyla tercih edilir.

Websploit’in amacı, güvenlik uzmanlarına ve etik hacker’lara bir dizi modül aracılığıyla, hızlı şekilde saldırı senaryoları gerçekleştirme imkânı tanımaktır. Hem eğitim hem de gerçek saldırı senaryolarında ağ bazlı analiz ve manipülasyonlarda etkili bir rol oynar.

## Kurulum

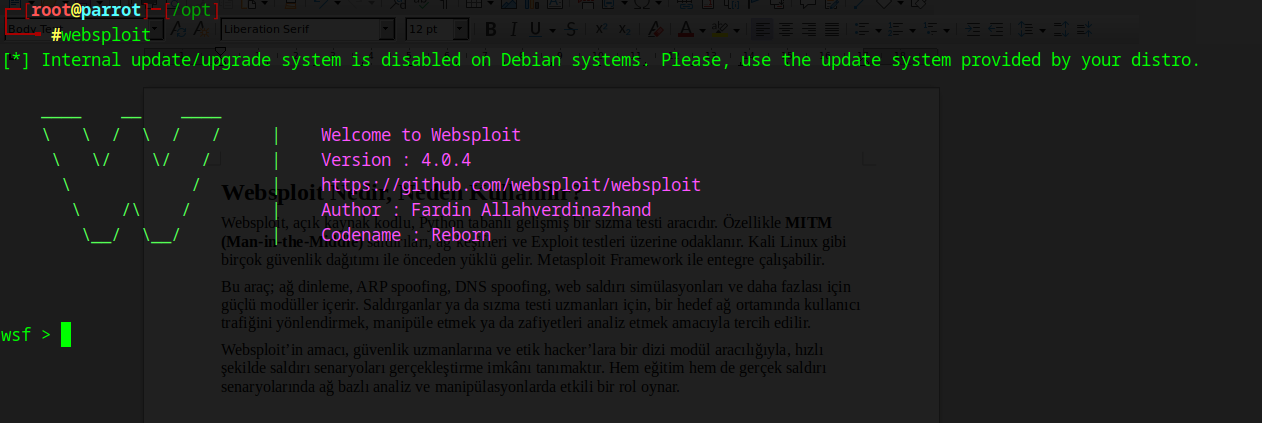
Websploit, çoğu güvenlik test sisteminde yüklü gelir. Yüklü değilse aşağıdaki komutlarla kurulabilir:

* sudo apt update
* sudo apt install websploit



## Kullanım Örneği

Websploit açıldığında interaktif bir terminal arayüzü karşınıza çıkar. Buradan modüller seçilip kullanılabilir. Örneğin, ağdaki cihazlara karşı ARP spoofing yaparak trafik yönlendirmek için şu adımlar izlenebilir:



Arayüz açıldıktan sonra:

* wsf > use network/arp\_spoof
* wsf:arp\_spoof > set TARGET 192.168.1.5
* wsf:arp\_spoof > set GATEWAY 192.168.1.1
* wsf:arp\_spoof > run

Bu işlemle hedef sistem ile ağ geçidi arasına girilerek, hedefin trafiği dinlenebilir hale gelir.

## Elde Edilebilecek Bilgilerden ve Etkilerden Örnekler

Websploit üzerinden yapılabilecek saldırılar neticesinde aşağıdaki bilgilere erişilebilir:

* Hedef sistemin HTTP istekleri ve yanıtları dinlenebilir.
* Kimlik bilgileri (şifre, kullanıcı adı) gibi hassas veriler elde edilebilir.
* DNS istekleri manipüle edilerek hedef farklı sitelere yönlendirilebilir.
* Web formlarına sahte giriş ekranları yerleştirilerek credential harvesting yapılabilir.
* JavaScript enjeksiyonu ile oturum çalma (cookie theft) gerçekleştirilebilir.

Ayrıca Metasploit entegrasyonu sayesinde keşif sonrası exploit süreci doğrudan başlatılabilir.

## Kullanılabilecek Özellikler ve Modüller

Websploit, modüler mimarisiyle birçok saldırı vektörünü destekler. Öne çıkan modüller şunlardır:

* **network/arp\_spoof**: Hedef ile ağ geçidi arasına girerek trafik yönlendirmesi yapar.
* **network/dns\_spoof**: DNS isteklerini sahte yanıtlarla değiştirerek kullanıcıyı sahte sitelere yönlendirir.
* **network/webkiller**: Hedef tarayıcıda belirli bağlantıları düşürerek servis kesintisi yaratır.
* **exploit/java\_applet**: Java eklentisi üzerinden sistem istismarı yapılmasını sağlar.
* **network/wifi\_jammer**: Kablosuz ağ trafiğini karıştırarak ağ kesintisi oluşturur.
* **web/microsploit**: Mikroservis sistemlerine karşı exploit denemeleri içerir.
* **autopwn**: Otomatik exploit zinciri oluşturma ve Metasploit ile bağlantı kurma işlevi görür.

Ayrıca show modules komutu ile tüm mevcut modüller listelenebilir ve her biri için info komutuyla detaylar öğrenilebilir.

Websploit, MITM saldırılarında, trafik manipülasyonlarında ve web uygulama güvenlik testlerinde güçlü bir yardımcıdır. Basit komut seti, modüler yapısı ve Metasploit uyumluluğu sayesinde, hem öğrenme sürecinde hem de pratik güvenlik testlerinde çok yönlü olarak kullanılabilir.