Websploit Kullanımı

(+) *Bu yazı birerbir denenmiştir ve başarıyla uygulanmıştır.*

Websploit uzak sistemde zafiyet bulmak için kullanılan açık kaynak kodlu bir projedir. Kali'de

root@kali:~$ websploit

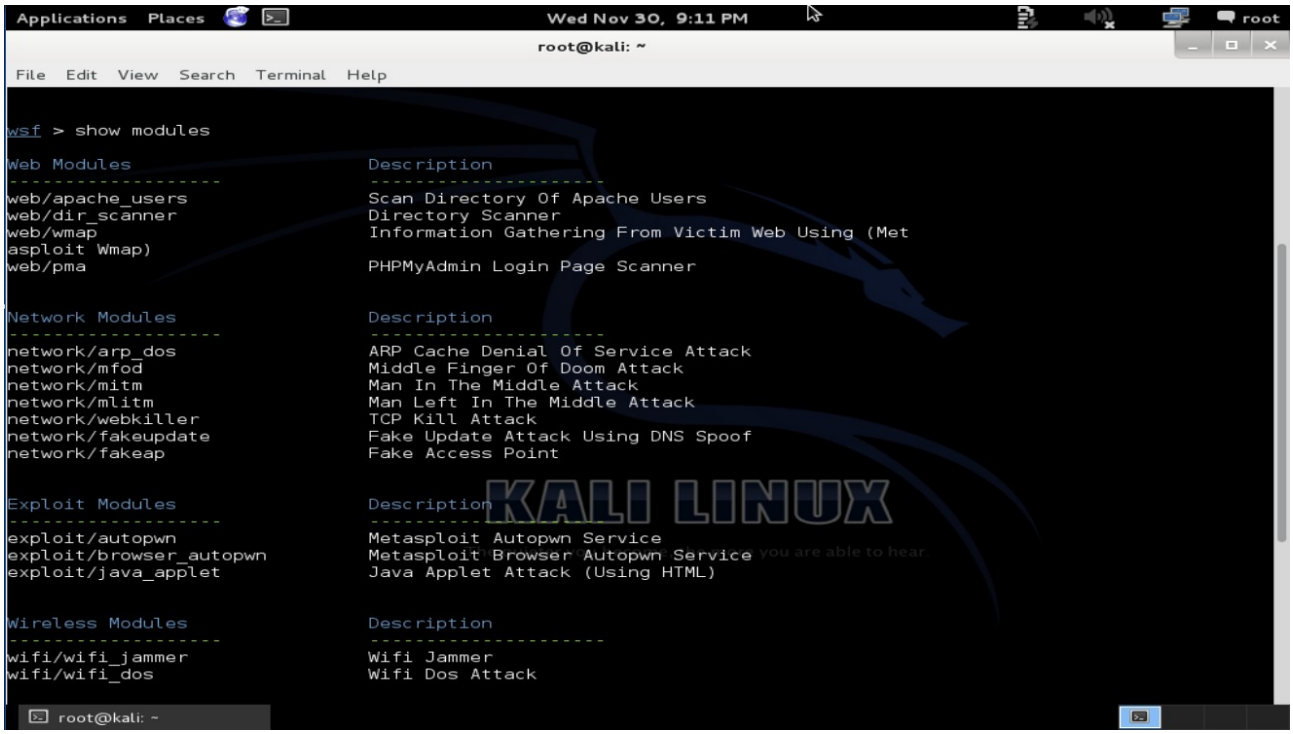
diyerek araç başlatılabilir:

wsf >

Websploit'te yer alan modülleri sıralamak için *show modules* kodu kullanılır:

wsf > show modules

Output:



Modülleri tıpkı Metasploit'te seçtiğimiz gibi seçerek çalıştırabilmekteyiz. Şimdi birkaç modülünün uygulamasını gösterelim:

a) network/arp_dos Modülü

Bu modül yerel network'te (kendi Mac Adresimiz + Router IP'si) şeklinde arp yayını yapar. Böylece router IP'sini yanlış MAC'te gösterir. Bu sebeple yerel network'teki tüm cihazlar internet paketlerini router diye bize gönderecektir ve internet bağlantıları kopacaktır. Kopan bağlantılarını onarmak için Router'ın nerede olduğunu soran arp yayını yapacaklardır. Yani Router'ın MAC'ini soracaklardır. network/arp_dos modülü devamlı (kendi Mac Adresimiz + Router IP'si) şeklinde arp yayını yapacağı için yerel network'teki cihazlar cevap olarak yine yanlış MAC adresi alacaklardır. Böylece internet paketlerini bize göndermeye devam edeceklerinden bağlantıları kesik kalacaktır. Ne zaman

modülü durdurursak o zaman bağlantılarını onarıp internete çıkış sağlayabileceklerdir. Yerel network'te yapılan bu saldırıya (yani yerel network'teki tüm cihazların internet erişimini koparmaya) ARP Flood adı verilmektedir. ARP flood bir DOS çeşididir.

Şimdi bu modülü kullanalım ve yerel network'ümüzdeki cihazların internet erişimini koparalım:

```
wsf > use network/arp_dos
wsf : ARP_DOS > show options

Options     Value          RQ      Description
----------  -------------- ------  –---------------------------
interface   eth0           yes     Network Interface Name
TARGET      192.168.1.3    yes     Target IP Address
ROUTER      192.168.1.1    yes     Router IP Address
```

Varsayılan olarak konulmuş değerleri kendimize göre ayarlayalım:

```
wsf : ARP_DOS > set ROUTER 192.168.0.1
wsf : ARP_DOS > set TARGET 192.168.0.255
```

Hedef olarak broadcast adresi koyduk. Böylece yerel ağdaki her cihaz (bilgisayar + telefon + televizyon) arp flood saldırısına maruz kalacaktır. Ayarlamalar sonrası son olarak modülü çalıştırma işlemi kaldı:

```
wsf : ARP_DOS > run

[*] Attack has been started …

For stop the ARP Dos attack press [ENTER] :
```

Saldırı böylece başlar. Bu modül saldırı için Ettercap aracından faydalanmaktadır. Çünkü saldırı başladığında ettercap ismli bir konsol ekrana gelmiştir. Gözlemlemelerimin sonucunda kardeşimin laptop interneti, annemin laptop interneti, kendi laptop'ımın interneti, annemin telefonunun interneti ve kendi telefonumun interneti gitmiştir. Dolayısıyla diyebiliriz ki evdeki genel internet erişimi komple engellenmiştir. Saldırı durdurulduğunda cihazlardaki internetin geldiği görülmüştür.

Benim Not 1: exploit/autopwn modülü denenmiştir, ancak db_autopwn.rb dosyası bulunamadı diye hata vermiştir. exploit/wmap modülü de denenmiştir, ancak bu da hata vermiştir. Bu iki modül de metasploit'te mevcut olan ve daha önce denediğim modüllerdir. Hatasız kullanılışına bakmak için Yaz Tatili 2014/Kali/Masaüstü/db_autopwn ve wmap plugini.txt dosyasına bakabilirsin.

Benim Not 2: wifi_jammer modülü ve wifi_dos modülü aircrack-ng ailesini kullanmaktadır. wifi_jammer hariçten bir WLAN'da iletişimi sekteye uğratma yaparken wifi_dos içeriden WLAN'da iletişimi sekteye uğratma yapar fikri hasıl oldu. Bunun üzerine wifi_jammer modülü denendi, fakat ekrana belirlediğimiz router'ın istemcilerini airodump aracılığıyla sıralamaktan başka bir işe yaramadı. Yani iletişimi sekteye uğratmadı. wifi_dos'u ise deneme lüzmu görülmemiştir. Çünkü yapacağı şey deuathenticate paketleri ile WLAN ağındaki tüm cihazları hattan düşürmek olacaktır. Bunu zaten Internetten Edinilmiş Kaynaklar/Elden Geçirdiğim Notlar/Aircrack ile Hedefi Hattan Düşürme.docx belgesinde anlatmıştım.

Yararlanılan Kaynak

Web Penetration Testing in Kali Linux, pg. 95