USB Wifi Cihazım Packet Injection'ı Destekliyor mu?

NOT: Bu belge sonucunda aldığım USB dongle'ın packet injection desteğine sahip olduğunu öğrenmiş bulunmaktayım.

USB Wifi cihazının packet injection'ı destekleyip desteklemediği şu şekilde öğrenilebilir. Öncelikle usb wifi cihazını monitör moda geçirmemiz gerekmektedir. Bunun için usb wifi cihazını bilgisayara takalım ve Ubuntu masaüstünün sağ üst köşesinde yer alan internet simgesine tıklayıp usb wifi bir ağa bağlanmışsa disconnect edelim. Ardından USB wifi'ın interface adını öğrenmek için aşağıdaki kodu girelim:

> ifconfig

Output:

```
eth0      Link encap:Ethernet  HWaddr 20:cf:30:64:a9:d5
          inet addr:192.168.2.201  Bcast:192.168.2.255  Mask:255.255.255.0
          ….....….

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          ….....….
wlan0     Link encap:Ethernet  HWaddr 48:5d:60:38:0a:ff
          inet addr:192.168.2.70  Bcast:192.168.2.255  Mask:255.255.255.0
          ….....….
wlan2     Link encap:Ethernet  HWaddr ec:08:6b:17:c4:24
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          ….....….
```

USB Wifi cihazı takılı değilken wlan2 interface'i olmadığından ve USB wifi cihazı takılı olduğunda wlan2 interface'i olduğundan Usb Wifi cihazının interface'inin wlan2 olduğunu anlarız. Şimdi bu interface adını kullanarak aşağıdaki kodları terminale girelim.

```
> airmon-ng stop wlan2       // USB Dongle'ımızın monitor modu eğer açıksa disable edilir.
> ifconfig wlan2 down        // USB Dongle'ımızın çalışması sonlandırılır.
> airmon-ng start wlan2 4    // USB Dongle'ımız monitor modda ve channel 1'de başlatılır.
```

NOT: Airmon-ng'nin aldığı 4 numarası usb wifi'ın dinleyeceği channel'ı ifade eder. Channel 4'ün seçilmesinin nedeni sonraki aşamalarda, seçilen modem'in channel 4'ten çalıştığı hatasını vermesinden dolayıdır. Bir başka router seçildiğinde eğer başka bir channel hata olarak veriliyorsa o zaman bu aşamaya dönülüp channel'ın istenilen değerde girilmesi gerekmektedir.

Son kod girildikten sonra eğer işlem başarılı olduysa aşağıdaki output ekrana gelir:

Output:

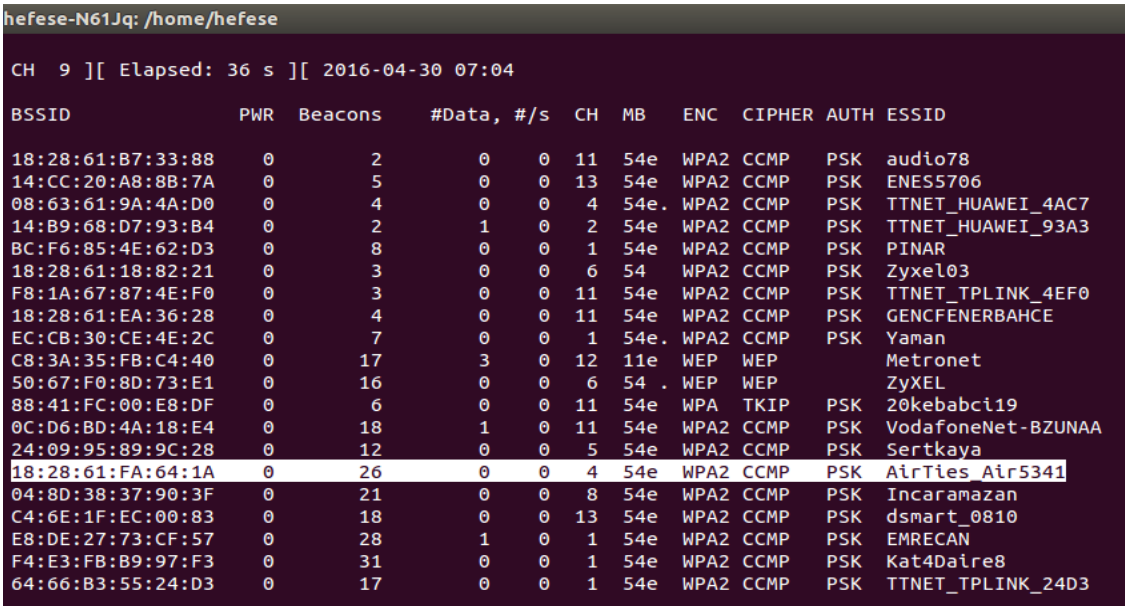
Found 1 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them.

PID	Name
7301	dhclient

Interface	Chipset	Driver
wlan2	Atheros AR9271	ath9k – [phy0] (monitor mode enabled on **mon0**)

Dikkat edilirse wlan2 interface'i ayrı bir interface ile monitor moda alınmıştır. Yani monitor modda olan interface şu an wlan2'nin kardeşi olan mon0 'dur. Dolayısıyla sonraki kodun birinde monitor modda olan mon0 interface'i kullanılacaktır. Şimdi etraftaki router'ları tespit etmek için airodump-ng'yi kullanalım:

> airodump-ng wlan2 // USB Dongle'ımız etrafı sniff'lemeye başlar.



```
hefese-N61Jq: /home/hefese

CH  9 ][ Elapsed: 36 s ][ 2016-04-30 07:04

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

18:28:61:B7:33:88    0        2        0    0  11  54e  WPA2 CCMP   PSK  audio78
14:CC:20:A8:8B:7A    0        5        0    0  13  54e  WPA2 CCMP   PSK  ENES5706
08:63:61:9A:4A:D0    0        4        0    0   4  54e. WPA2 CCMP   PSK  TTNET_HUAWEI_4AC7
14:B9:68:D7:93:B4    0        2        1    0   2  54e  WPA2 CCMP   PSK  TTNET_HUAWEI_93A3
BC:F6:85:4E:62:D3    0        8        0    0   1  54e  WPA2 CCMP   PSK  PINAR
18:28:61:18:82:21    0        3        0    0   6  54   WPA2 CCMP   PSK  Zyxel03
F8:1A:67:87:4E:F0    0        3        0    0  11  54e  WPA2 CCMP   PSK  TTNET_TPLINK_4EF0
18:28:61:EA:36:28    0        4        0    0  11  54e  WPA2 CCMP   PSK  GENCFENERBAHCE
EC:CB:30:CE:4E:2C    0        7        0    0   1  54e. WPA2 CCMP   PSK  Yaman
C8:3A:35:FB:C4:40    0       17        3    0  12  11e  WEP  WEP         Metronet
50:67:F0:8D:73:E1    0       16        0    0   6  54 . WEP  WEP         ZyXEL
88:41:FC:00:E8:DF    0        6        0    0  11  54e  WPA  TKIP   PSK  20kebabci19
0C:D6:BD:4A:18:E4    0       18        1    0  11  54e  WPA2 CCMP   PSK  VodafoneNet-BZUNAA
24:09:95:89:9C:28    0       12        0    0   5  54e  WPA2 CCMP   PSK  Sertkaya
18:28:61:FA:64:1A    0       26        0    0   4  54e  WPA2 CCMP   PSK  AirTies_Air5341
04:8D:38:37:90:3F    0       21        0    0   8  54e  WPA2 CCMP   PSK  Incaramazan
C4:6E:1F:EC:00:83    0       18        0    0  13  54e  WPA2 CCMP   PSK  dsmart_0810
E8:DE:27:73:CF:57    0       28        1    0   1  54e  WPA2 CCMP   PSK  EMRECAN
F4:E3:FB:B9:97:F3    0       31        0    0   1  54e  WPA2 CCMP   PSK  Kat4Daire8
64:66:B3:55:24:D3    0       17        0    0   1  54e  WPA2 CCMP   PSK  TTNET_TPLINK_24D3
```

USB Wifi'ımızın paket injection'ı destekleyip desteklemediğini öğrenmek için yukarıdaki çıktıdan bir router seçip onun MAC adresini (BSSID'sini) aşağıdaki kodda kullanmamız yeterlidir.

> aireplay-ng -9 -a 18:28:61:FA:64:1A mon0

-9 injection testi yap anlamına gelir.
-a router'ın MAC'ini alır.
mon0 usb wifi'ımızın monitor moddaki interface'inin adıdır.

Şayet yukarıdaki kodun çıktısı aşağıdaki gibi olursa demek ki USB Wifi'ımız packet injection desteğine sahiptir deriz.

Output:

```
03:11:10  Waiting for beacon frame (BSSID: 18:28:61:FA:64:1A) on channel 4
03:11:11  Trying broadcast probe requests...
03:11:11  Injection is working!
03:11:12  Found 1 AP

03:11:12  Trying directed probe requests...
03:11:12  18:28:61:FA:64:1A - channel: 4 - 'AirTies_Air5341'
03:11:13  Ping (min/avg/max): 1.204ms/25.796ms/69.065ms Power: 0.00
03:11:13  30/30: 100%
```

Packet Injection neden önemli?

Normalde wireless ağlarında cihazlar default mode'da olurlar. Bu moda göre wireless ortamında bir cihaz kendine ait olmayan paketler gelse de kural gereği kabul etmez ve almaz. Ancak cihaz monitor moda geçerse wireless ortamındaki tüm paketleri kabul eder ve alır. Böylece sniff'ing için elverişli ortam kurulmuş olur. Ancak monitor moddayken kural gereği sadece dinleme modunda olduğumuz için cihazımız herhangi başka bir cihazla paket alışverişinde (gönderiminde ve alımında) bulunamaz. Halbuki USB Wifi adaptörümüz ile etraftaki bir router'ın WPA2-PSK şifresini kırabilmek için bizim hem sniff'leme yapabiliyor olmamız lazım hem de Deuathenticate paketleri gönderebiliyor olmamız lazım.

Not : Hatırlarsan hedef network'teki router'ın WPA2-PSK şifresini kırabilmek için istemciyi Deauthenticate paketleri göndererek hattan düşürüyorduk ve istemci tekrar bağlanmaya çalıştığında 4 way handshake paketlerini havada yakalayarak şifre kırma işlemine başlayabiliyorduk (bkz. Aircrack-ng İle WPA2 Şifre Kırma.docx)

Monitor modundayken madem paket gönderemiyoruz o zaman packet injection özelliğini ortaya atalım demişler. Bu özelliğe göre eğer USB Wifi adaptörü Packet Injection desteğine sahip olursa monitor moddayken aynı zamanda paket gönderiminde de bulunabilmektedir. Böylece monitor modda bir yandan sniff'ing yaparken diğer yandan göndereceğimiz Deauthenticate paketleri ile istemciyi hattan düşürülebilir ve istemcinin tekrar bağlanmak için göndereceği 4-Way Handshake'leri havada yakalayarak WPA2-PSK şifresini kırabiliriz.

Not : Benim USB Wifi Dongle'ım yukarıdaki test işleminde görüldüğü üzere Packet Injection desteğine sahip olduğu için WPA2-PSK şifre kırma işlemini “*Aircrack-ng İle WPA2 Şifre Kırma.docx*” dökümanında bahsedildiği gibi başarıyla gerçekleştire bilmekteyim.

Kaynak

Tez Raporu/Literatür Taraması/İncelenmiş Makaleler/BGA/Pentest Çalışmalarında Kablosuz
Ağ Güvenliği Testleri.docx

http://security.stackexchange.com/questions/76983/what-is-the-need-and-purpose-of-packet-injection-within-wifi-attacks