

how-to: capture wifi Over-The-Air packets with kali linux and wifi adapter

Posted on November 24,2017 by inzoolee

This tutorial explains how to capture OTA(Over-The-Air) wifi packets step by step. Prerequisites:

Wifi adaptor that supports monitor mode

Linux with necessary tools installed

Steps: In this example, Kali bootable USB drive(Kali Linux 17.02 64bit) and external Alfa AWUS051NH USB wifi adaptor are used for wifi packet sniffing. But any linux distribution with necessary tools (aircrack-ng, iwconfig, iw) installed and wifi adaptor that supports monitor mode can be used in theory. If you're using Ubuntu instead of Kali, you'll need to install aircrack-ng and wireless-tools.(ex. `sudo apt-get install aircrack-ng; sudo apt-get install wireless-tools.`) 1. Boot PC or laptop from external Kali linux bootable USB drive. Every PC or laptop is different but when PC or laptop boots up, it will usually show message how to get into boot or Bios setup menu and from there you can select USB boot option(press F2, F12 or ESC etc.) 2. If PC or laptop boots from bootable USB drive, it will show "Kali Linux Live Boot Menu". Select "Live system" and hit Enter to continue boot process. This will launch Kali linux in RAM without touching internal hard disk. If you're asked login, Kali linux's default root password is "toor"



reverse to "root"(without double quotation of course)

3.

Once Kali linux is fully up and logged in, open terminal program and enter "iwconfig" to find built-in existing wifi interface. Usually internal wifi interface comes up as "wlan0" and other non wifi interfaces will show "no wireless extensions". Below output shows this laptop has one built-in wifi interface, wlan0.

```
root@kali:~# iwconfig
wlan0 IEEE 802.11 ESSID:"Picasso_AP" Mode:Managed Frequency:2.412 GHz Access Point:
E0:B9:E5:DE:EC:F7
Bit Rate=6 Mb/s Tx-Power=20 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off
Link Quality=70/70 Signal level=-29 dBm
```

```
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0 Tx excessive retries:0 Invalid misc:2 Missed beacon:0
```

```
eth0 no wireless extensions.
```

```
lo no wireless extensions.
```

4. Now insert external USB wifi adapter and enter "iwconfig" again to find which wifi interface it came up with. Below is example showing "iwconfig" output after external USB wifi adapter is plugged in. It came up as wlan1 interface.

```
root@kali:~# iwconfig
```

```
wlan0 IEEE 802.11 ESSID:"Picasso_AP" Mode:Managed Frequency:2.412 GHz Access Point: E0:B9:E5:DE:EC:F7
```

```
Bit Rate=6 Mb/s Tx-Power=20 dBm
```

```
Retry short limit:7 RTS thr:off Fragment thr:off
```

```
Encryption key:off
```

```
Power Management:off
```

```
Link Quality=70/70 Signal level=-29 dBm
```

```
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0 Tx excessive retries:0 Invalid misc:2 Missed beacon:0
```

```
eth0 no wireless extensions.
```

```
lo no wireless extensions.
```

```
root@kali:~# iwconfig
```

```
wlan1 IEEE 802.11 ESSID:off/any Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
```

```
Retry short long limit:2 RTS thr:off Fragment thr:off
```

```
Encryption key:off
```

```
Power Management:off
```

```
wlan0 IEEE 802.11 ESSID:"Picasso_AP" Mode:Managed Frequency:2.412 GHz Access Point: E0:B9:E5:DE:EC:F7
```

```
Bit Rate=6 Mb/s Tx-Power=20 dBm
```

```
Retry short limit:7 RTS thr:off Fragment thr:off
```

```
Encryption key:off
```

```
Power Management:off
```

```
Link Quality=70/70 Signal level=-27 dBm
```

```
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0 Tx excessive retries:0 Invalid misc:4 Missed beacon:0
```

```
eth0 no wireless extensions.
```

```
lo no wireless extensions.
```

```
root@kali:~#
```

5. Now check if external USB wifi adaptor has "monitor mode" capability with "iw list" command. It will show capabilities of 2 wifi interfaces, one for built-in wlan0(Wiphy phy0) and the other for external USB wifi adapter wlan1(Wiphy phy1). Below is example output of "iw list" command (iw list has long output and only relevant part is displayed here). Here external USB wifi adaptor supports monitor mode along with other modes.

```
root@kali:~# iw list
Supported interface modes:
* IBSS
* managed
* AP
* AP/VLAN
* WDS
* monitor * mesh point
```

6. Now we need to find out in which channel AP(Access Point) is in which you want to sniff WiFi packets from. For that, we're going to use airmmon-ng and airodump-ng to find channel number that AP is in. First enter "airmon-ng check kill" to kill all processes that can interrupt our wifi sniffing job. Then enter "airmon-ng start wlan1" to create dedicated monitoring mode WiFi interface. Then enter "iwconfig" to find which WiFi monitoring mode interface is created.(Usually it is mon0, but here wlan1mon is created). Now finally enter "airodump-ng [Monitoring mod interface name]". Below is example output of each command and here monitoring mode interface is wlan1mon. AP that we want to sniff is MY_WIFI_AP and "airodump-ng wlan1mon" output shows it is on channel 1(2.442 Ghz).

```
root@kali:~# airmon-ng check kill
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 kill (some of) them!
-e
PID Name
2887 NetworkManager
3081 wpa_supplicant
Killing all those processes...
root@kali:~#
root@kali:~#
root@kali:~# airmon-ng start wlan1
Interface Chipset Driver
wlan0 Unknown brcmsmac - [phy0]
wlan1 Ralink RT2870/3070 rt2800usb - [phy1]
(monitor mode enabled on mon0)
root@kali:~#
root@kali:~#
root@kali:~# iwconfigwlan1mon IEEE 802.11 Mode:Monitor Frequency:2.442 GHz Tx-Power=20
dBm
Retry short long limit:2 RTS thr:off Fragment thr:off
Power Management:off

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:off
eth0 no wireless extensions.
lo no wireless extensions.
root@kali:~#
root@kali:~#
root@kali:~# airodump-ng wlan1mon
CH 10 ][ Elapsed: 12 s ][ 2017-08-04 15:49 BSSID          PWR Beacons  #Data, #/s CH MB
ENC CIPHER AUTH ESSID
F8:18:97:1F:F5:CE -74      22      5  0  1 54e WPA2 CCMP PSK MY_WIFI_AP

```

7. Now put USB wifi adaptor into "monitor mode", set channel to the number that AP is in. In this example, we'll sniff packets to and from MY_WIFI_AP SSID which is in channel 1. Bring down wlan1mon, put wifi adaptor in monitor mode, set channel to 1 and bring wlan1mon up again.

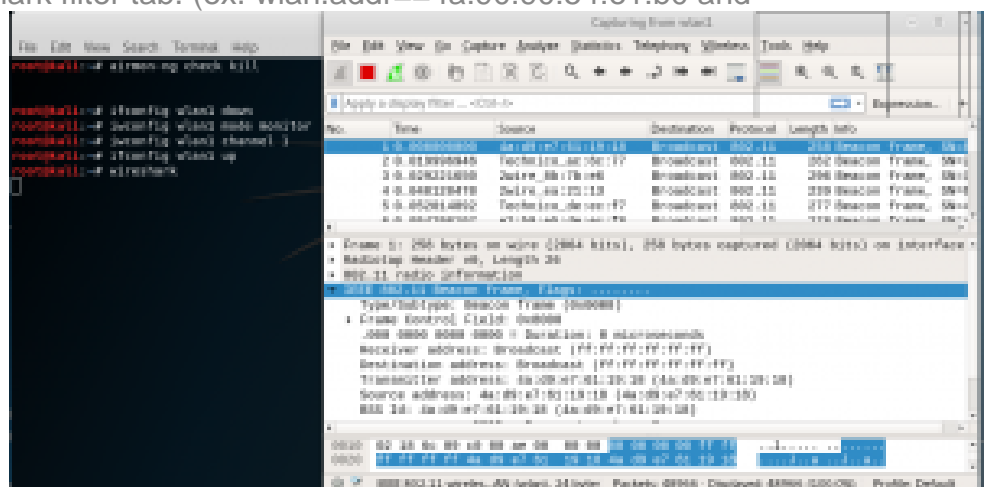
```

root@kali:~# ifconfig wlan1mon down
root@kali:~# iwconfig wlan1mon mode monitorroot@kali:~# iwconfig wlan1mon channel 1
root@kali:~# ifconfig wlan1mon up
root@kali:~# ifconfig wlan1mon
wlan1mon: flags=867<UP,BROADCAST,NOTRAILERS,RUNNING,PROMISC,ALLMULTI> mtu
1500
unspec 44-33-4C-47-E5-42-00-00-00-00-00-00-00-00-00 txqueuelen 1000 (UNSPEC) RX
packets 729 bytes 88595 (86.5 KiB)
RX errors 0 dropped 586 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

8. Now start wireshark from terminal(enter "wireshark"), select wlan1mon interface when wireshark comes up and then click start button to start capturing packets on interface wlan1mon interface. WiFi network is noisy so that there are a lot of traffic. So you want to apply wireshark filter to see only traffic that you are interested in. For example you can filter in wifi packets which contains only AP or WiFi client MAC address or both in wireshark filter tab. (ex. wlan.addr==4a:90:90:54:e1:b0 and

wlan.addr==88:41:fc:8c:3a:c4)



9.

Once you're done, unplug bootable USB drive, and reboot Kali Linux from right top corner menu. PC or laptop will boot from built-in hard disk to original OS.

Posted in:How-to | | With 0 comments