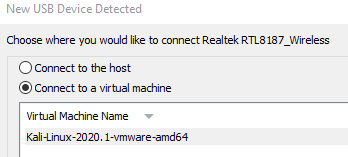
**Practical 11 Wireless Security**

**Exercise Start up Kali virtual machine and connect the Alfa wireless USB adapter**

1. Power on your Kali virtual machine.
2. Connect the Alfa wireless adapter to the desktop or laptop.
3. When you connect a USB device, a popup “New USB Device Detected” will appear. Select “Connect to a virtual machine” and select your Kali virtual machine (see following diagram). Click OK.



It may take a while (1 minute to 3 minutes for the virtual machine to detect the wireless adapter.

**Exercise Using the wireless card in Kali Linux**

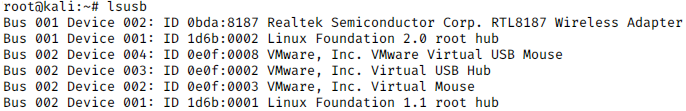
In Kali VM

1. Switch to root account if you are not already the root user.

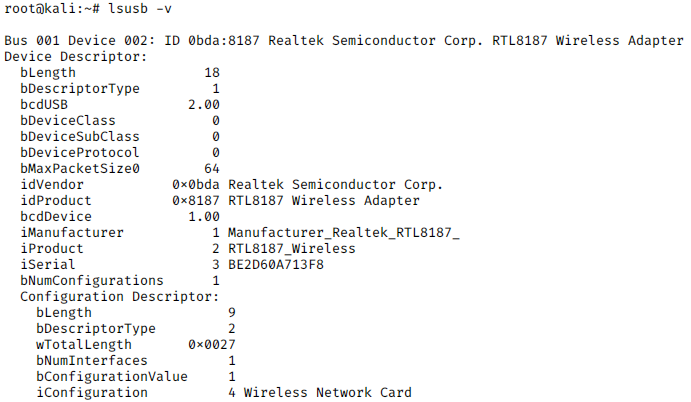
sudo -i

1. Run “lsusb”. All USB devices are listed, including the Alfa wireless adapter (see following diagram).

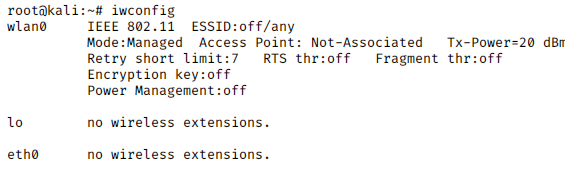
Details of the Alfa wireless adapter. The chipset is displayed : RTL8187



1. If we are using PCI wireless network cards (the internal wireless cards), we can use the lspci command. Try running “lspci” to see the list of current PCI devices.
2. To view more details, you can run “lspci” or “lsusb” with the -v option (verbose mode) or -vv option (more verbose)



1. Type “iwconfig”. The wireless card should have a device interface name of “wlan0” or “ath0”. Currently it is in “managed” mode, and not associated with any Access Point.



Wireless card’s device interface name

1. Type “ifconfig”. The wlan0 network interface may be listed, along with eth0, the wired network card.
2. Type “ifconfig eth0 down” to disable the wired network card.
3. The command “airmon-ng” can also be used to see the status of the wireless devices and the drivers used.

Run “airmon-ng”. Information about the wireless device interface is listed.



1. Type “man iwlist” to see the help page for iwlist command. Run the following command to view a listing of the available wireless APs around you. (Note : the listing may take about 30 seconds to appear)

iwlist wlan0 scan

Sometimes you may get an error like “Network down” or “Device busy”. You can try running the command again.

Some Access Points with SSID starting with “ehd” have been set up in the lab.

SSID WPA-PSK passphrase SSID WPA-PSK passphrase

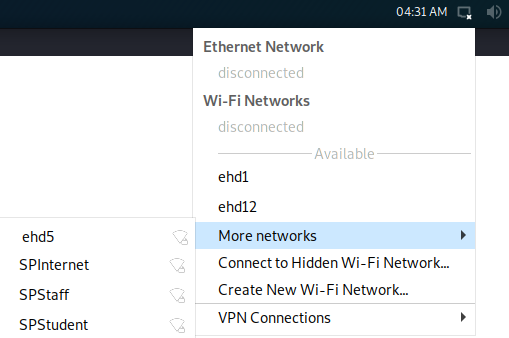
ehd2 sunshine ehd8 business

ehd3 elephants ehd9 dictionary

ehd5 whatever ehd12 keyboard

ehd6 careless ehd13 waterfall

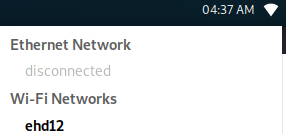
1. In Kali, in the top right corner, click on the Network icon, and click on one of the above ehd networks using WPA-PSK. (see following diagram).



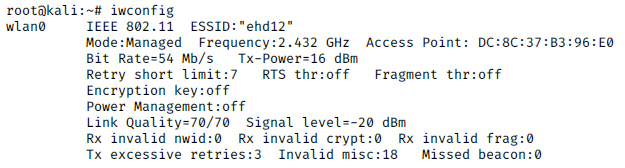
Select one of the ehd networks using WPA-PSK.

You may need to click “More networks” to see more networks around you.

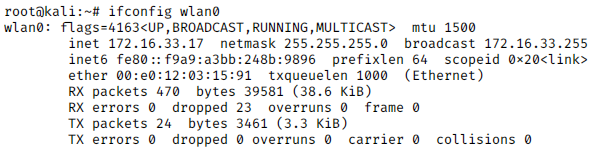
1. Enter the WPA-PSK passphrase and click Connect.
2. If the connection is successful, the Network icon will look like the following. If you click on the Network icon, you will see the name of the wireless network that you are currently connected to.



1. Once you are connected, type “iwconfig”. The ESSID now contains the SSID of the wireless AP you are connected to. The Access Point contains the BSSID or the MAC address of the wireless AP you are connected to. (see following diagram)



1. Type “ifconfig wlan0” to see the IP address assigned to your wireless card. (see following diagram)



1. Start a web browser and check that you can access the Internet.
2. Disconnect from the wireless network.

**Using the WPA Supplicant client program to connect**

If you do not have access to a nice Linux GUI, and have to connect to a wireless AP using WPA through the command line, you can run the wpa\_supplicant client program manually.

*(These steps are for your info only, you do not need to do them as you have access to the Linux GUI, and the wpa\_supplicant process is already running)*

Type “man wpa\_supplicant” to view the man page for wpa\_supplicant.

Create the file /etc/wpa\_supplicant.conf (if it does not already exist) and type the following lines in it.

ctrl\_interface=/var/run/wpa\_supplicant

network={

Change to the SSID of the wireless AP you want to connect to

ssid="ehd12"

proto=WPA

key\_mgmt=WPA-PSK

Change to the pre-shared key of the wireless AP

psk="keyboard"

}

Run the following command to associate with the wireless AP.

wpa\_supplicant –i wlan0 –c /etc/wpa\_supplicant.conf

When you see the message “Connection to xx:xx:xx:xx:xx:xx completed”, open another terminal. Run “iwconfig” to see that you are associated with the wireless AP.

In the other terminal, run the following command to get a DHCP-assigned IP from the wireless AP.

dhclient wlan0

Run “ifconfig wlan0” to see the IP address assigned to your wireless card.

Check that you can access the Internet.

To disconnect, press Control-C to stop the wpa\_supplicant.

**Exercise Monitoring the wireless signals**

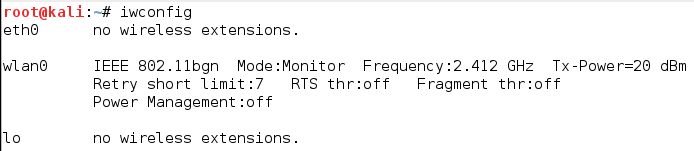
1. In order to monitor the surrounding wireless networks, the wireless card has to be in “monitor” mode. Type the following commands to bring the wireless card down, switch to monitor mode and bring the card up again.

ifconfig wlan0 down

iwconfig wlan0 mode monitor

ifconfig wlan0 up

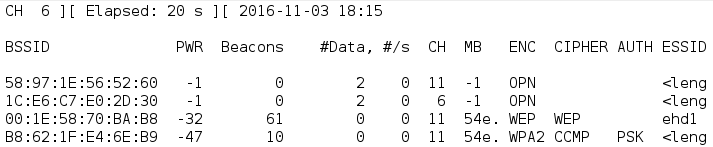
1. Type “iwconfig”. The wireless card is now in “monitor” mode.



1. Use Airodump to see the list of wireless networks around you. Note that the channel number in the top left corner is changing, so the wireless card is hopping across channels, scanning for the different wireless networks.

airodump-ng wlan0

The channel number will change as the wireless card hops across the different channels



\

1. To stop Airodump, press Control-C.
2. Run Wireshark and start capturing wireless frames on the wlan0 interface. Note that due to the speed and number of wireless frames, and depending on the power of the wireless equipment, not all frames may be captured by Wireshark. You can stop the Wireshark capture after a while.
3. You can specify different channels for your wireless card. The following command will set your wireless card to Channel 11.

iwconfig wlan0 channel 11

Run Wireshark again to see the wireless frames captured on this channel.

**Exercise Capturing Wireless frames using Airodump**

[](javascript:void(0))To be able to capture wireless frames and possibly crack encryption keys, the attacker usually requires someone (the victim) to connect to the wireless network. You can use your laptop or a smartphone to act as a victim to connect to the wireless network, while your Kali system captures the wireless frames,

[](javascript:void(0))

[](javascript:void(0))

Attacker capturing wireless frames between Victim and Access Point

“Victim” connecting to Access Point

Some Access Points with SSID starting with “ehd” have been set up in the lab.

SSID WPA-PSK passphrase SSID WPA-PSK passphrase

ehd2 sunshine ehd8 business

ehd3 elephants ehd9 dictionary

ehd5 whatever ehd12 keyboard

ehd6 careless ehd13 waterfall

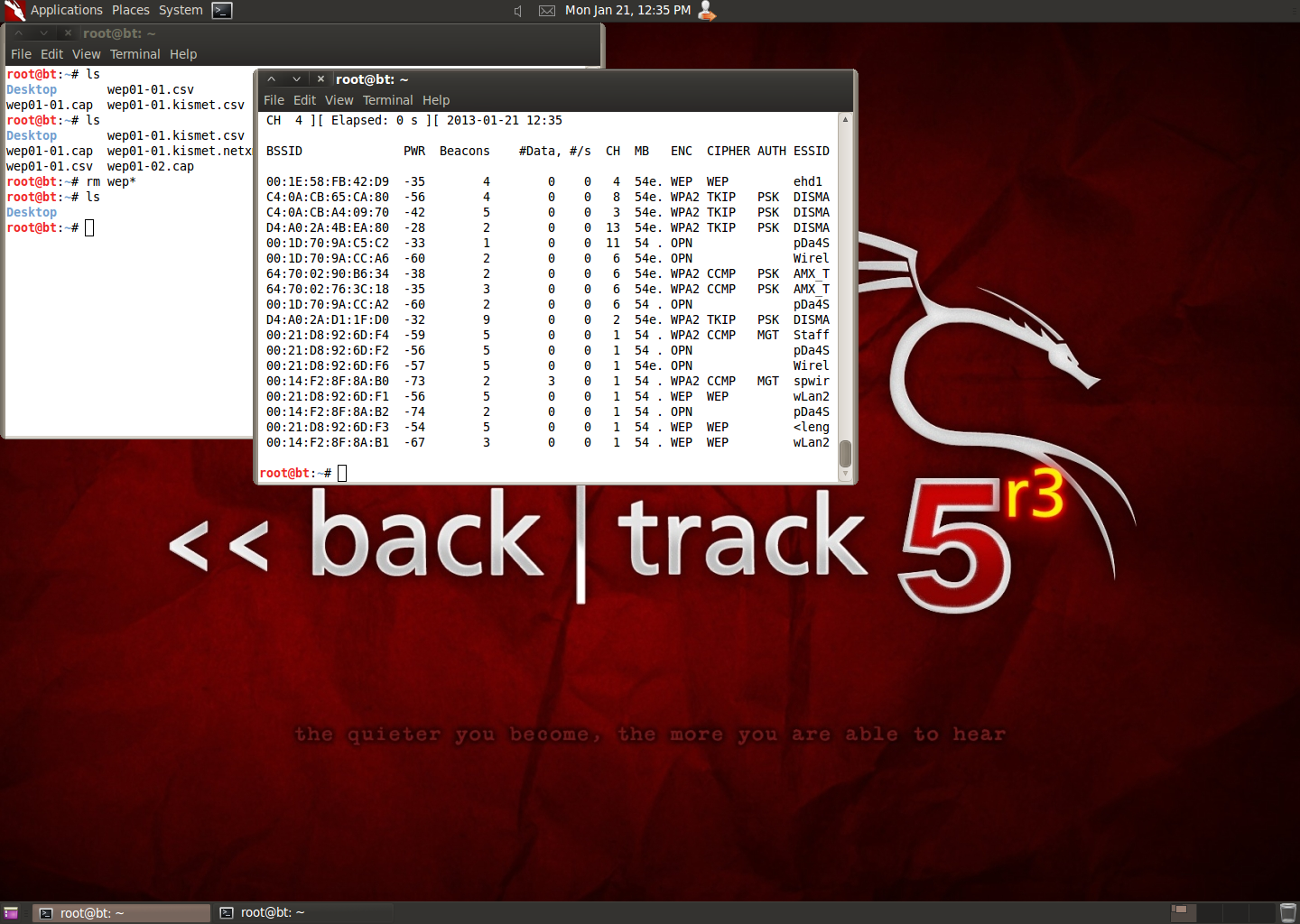
As the victim

1. Use a laptop or smartphone to connect to one of the ehd networks using WPA-PSK.
2. Use Airodump to see the list of wireless networks around you.

airodump-ng wlan0

1. Press Control-C to stop Airodump. Pick the ehd network using WPA-PSK, and take note of its BSSID (MAC address of the access point) and channel number. (see following diagram)

Note the BSSID and Channel number of one of the wireless networks



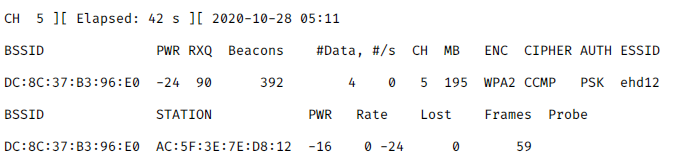
1. Use airodump to capture the wireless frames for your selected BSSID access point and save the frames into a file called “capture01”.

airodump-ng wlan0 –w capture01 –c *(channel)* --bssid *(bssid)*

For example, if the BSSID of the access point is 00:1D:70:9A:C5:04 and the channel being used is 6, you would run

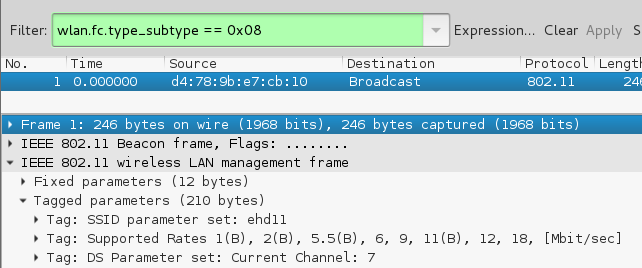
airodump-ng wlan0 –w capture01 –c 6 --bssid 00:1D:70:9A:C5:04

1. While Airodump is running, you can see the MAC addresses of wireless clients currently connected to the Access Point.



MAC address of wireless client currently connected to the Access Point

1. When you have captured a few beacon and data frames, press Control-C to stop.
2. Airodump saved the wireless frames into several files with different formats. The files are in the current directory (your current directory could be /root) Use Wireshark to open the capture01-01.cap file (you may need to run Wireshark as root user in order to open files in /root).
3. Look for the Beacon frame (you can filter by wlan.fc.type\_subtype==0x08)
4. Expand the frame and look for the SSID value.



1. Management frames have the frame type of 0. Look for Management frames by setting the filter to wlan.fc.type == 0x0. (Beacon frames are a subtype of Management frames)
2. Control frames have the frame type of 1. Check if there are any Control frames in your packet capture. You can filter by wlan.fc.type == 0x1.
3. Data frames have the frame type of 2. Check if there are any Data frames in your packet capture. You can filter by wlan.fc.type ==0x02

**Exercise Exploring frames of a non-broadcasting Access Point**

Even if the Access Point is not broadcasting its SSID in the Beacon frame, the SSID name can be found in other frames, eg Probe frames.

There are some non-SSID broadcasting Access Points set up for the class. There should be at least one present in your class.

SSID : ehd1 WPA-PSK passphrase : computer BSSID : C4-0A-CB-A4-0B-50

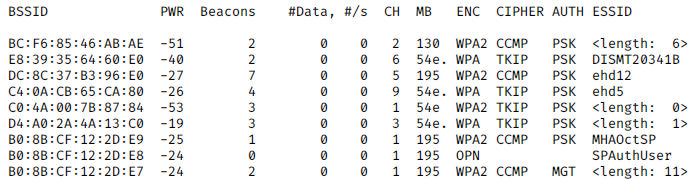
SSID : ehd4 WPA-PSK passphrase : thursday BSSID : C4-0A-CB-A4-09-70

SSID : ehd7 WPA-PSK passphrase : mountain BSSID : D4-A0-2A-D1-1F-D0

1. Use Airodump to see the list of wireless networks around you.

airodump-ng wlan0

1. When you see one of the BSSIDs of the non-broadcasting “ehd” Access Points, press Control-C to stop Airodump. Take note of the BSSID and its channel number.



BSSID

No SSID name displayed

Note : Sometime Airodump is able to find the SSID of non-broadcasting access points from the Probe frames, and display it. That is why sometimes you can see SSIDs which are supposed to be “hidden” listed in the Airodump output.

1. Use Airodump to capture the frames for your selected BSSID access point and save the frames into a file called “nobrdcst01”.

airodump-ng wlan0 –w nobrdcst01 –c *(channel)* --bssid *(bssid)*

1. After a while, press Control-C to stop the capture.
2. Use Wireshark to open the nobrdcst01-01.cap file.
3. Look for the Beacon frame (you can filter by wlan.fc.type\_subtype==0x08)
4. Expand the frame and look for the SSID. The SSID field should be blank this time.
5. Look for the Probe frames (you can filter by wlan.fc.type\_subtype==0x05 to find Probe responses or wlan.fc.type\_subtype==0x04 to find Probe requests)
6. Expand the frame and look for the SSID. Even though the SSID does not appear in the Beacon frame, it will appear in other frames like the Probe frames.

If you are not able to see any Probe frames, you can try the wireless capture again, and use a laptop or smartphone to connect to this non-broadcasting “ehd” Access Point. This will generate frames.

**Exercise Exploring frames of a WPA connection**

As the attacker :

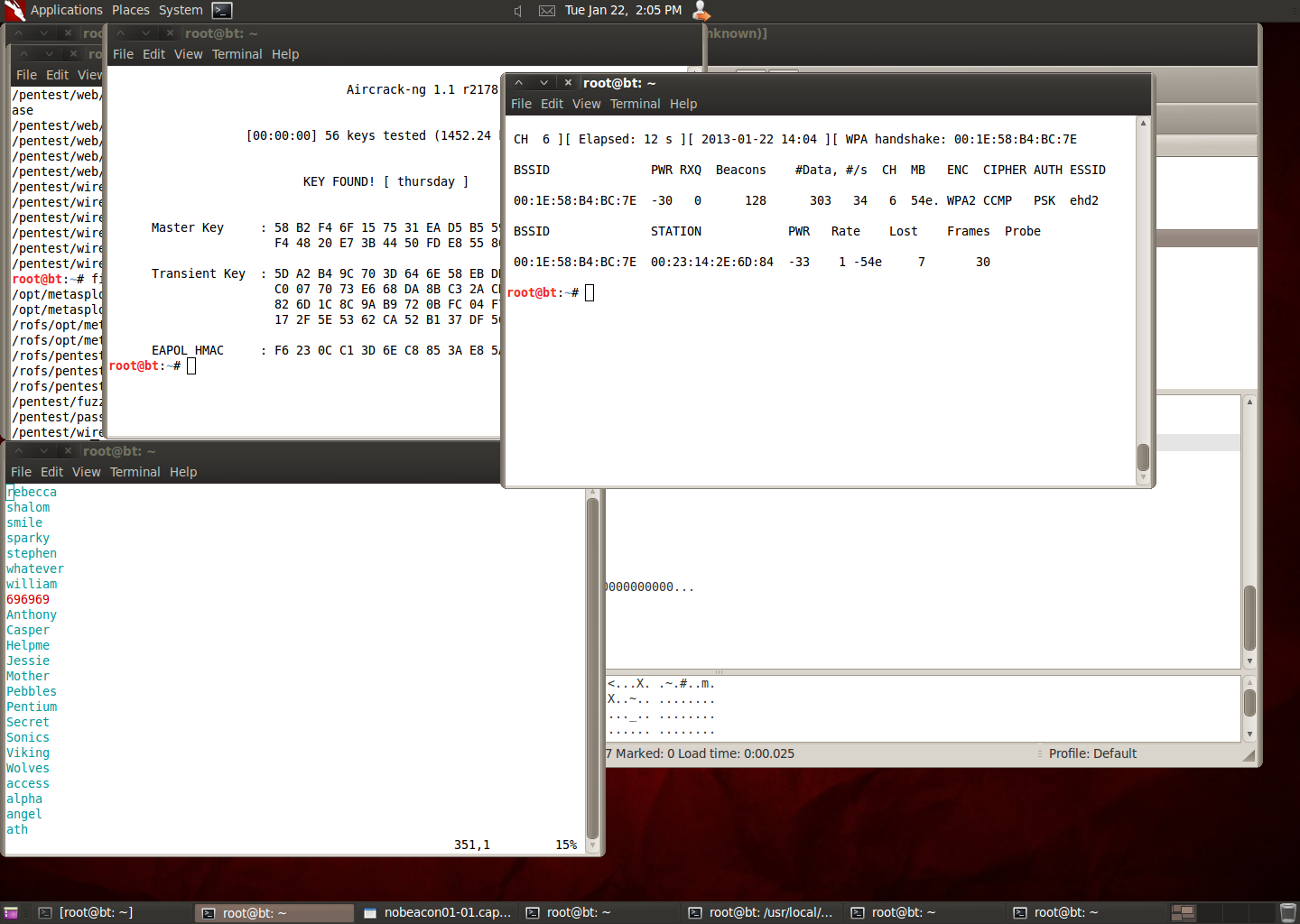
1. Use airodump to capture the frames of one of the “ehd” networks using WPA-PSK (broadcasting or non-broadcasting) and store the frames into a file.

As the victim :

1. Use a computer or smartphone to connect to this “ehd” network. Access the Internet.
2. Note the MAC address of the client.

As the attacker :

1. When the victim connects to the Access Point, you should see the phrase “WPA handshake” appear in airodump-ng. (see following diagram). You have captured the 4-way WPA handshake frames of the victim.



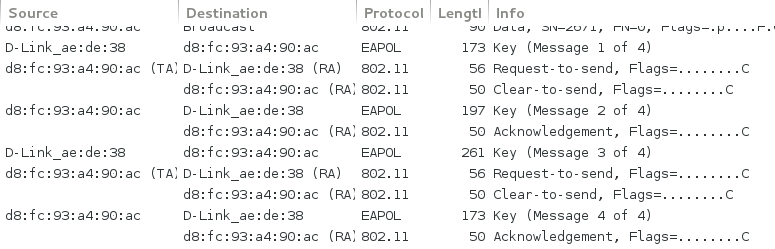
MAC address of client connected to the Access Point

1. Stop the capture. Use Wireshark to open the cap file.
2. Look for the Beacon frame (you can filter by wlan.fc.type\_subtype==0x08). This is the Beacon frame sent out by the Access Point to everyone (the destination address is the Broadcast address FF:FF:FF:FF:FF:FF)
3. Look for the Probe Response (you can filter by wlan.fc.type\_subtype==0x05). This is the Probe Response sent by the Access Point to your laptop/smartphone. Expand the Probe Frames. The SSID value can be found in the Probe Frames even if the Access Point is not broadcasting the SSID.
4. Look for the Authentication Frames (filter by wlan.fc.type\_subtype==0x0B). Expand the Authentication frames and look for the Authentication Algorithm (should be using Open System Authentication)
5. Look for the Association Request (filter by wlan.fc.type\_subtype==0x00).
6. Look for the Association Response (filter by wlan.fc.type\_subtype==0x01).

Note : Sometimes Airodump may not be able to capture all the wireless frames.

After associating, the client is connected to the wireless network. Next is the 4-way WPA handshake.

1. Look for the frames that make up the 4-way WPA handshake (filter by eapol). Note that sometimes not all the frames are able to be captured.



Client and Access Point doing the WPA 4-way handshake to set up temporal encryption keys

**Exercise Cracking WPA encryption**

If a dictionary word is used for the WPA key, it can be cracked.

1. Using the previous cap file which contains the WPA 4-way handshake, we can use Aircrack and a dictionary file to attempt to crack the WPA key. In the following example, we are using the dictionary file that comes with John the Ripper. Other dictionary lists can also be used.

aircrack-ng nobrdcst01-01.cap –w /usr/share/john/password.lst

If the WPA passphrase can’t be cracked using the John the Ripper dictionary file, try another word list. The rockyou.txt dictionary list in /usr/share/wordlists contain about 14 million possible words. Unzip it first and use it in your aircrack command.

Note : Sometimes even though Airodump did not manage to capture a full WPA 4-way handshake, Aircrack can still crack the WPA key. So even though Airodump did not report capturing the WPA 4-way handshake, you can still try using Aircrack on the packet capture file.

**Exercise Deauthenticating wireless clients**

If the client is already connected to the wireless network, the attacker may try to send frames to de-authenticate the client, and wait for the client to try to connect again in order to capture the WPA 4-way handshake.

Note : Only those wireless adapters with chipsets that support frame injection would be able to deauthenticate wireless clients. The deauthentication attempt also depends on the hardware of the wireless client.

1. Use airodump-ng to capture wireless frames of an access point using WPA-PSK and has at least one client connected to it.
2. While airodump-ng is running, in another terminal, use aireplay-ng to send 5 deauthentication attacks (one deauthentication attack consists of 64 frames) to a client connected to the access point

aireplay-ng wlan0 –-deauth 5 –a (*bssid*) –c (*client mac*)

If the deauthentication attack is successful, then hopefully the wireless client will try to connect to the access point again, and the airodump-ng software can capture the WPA 4-way handshake.

**Exercise Return Alfa wireless USB adapters**

1. Return the Alfa wireless adapter to your instructor.

Important : Do not attempt to crack other people’s networks without their permission!!

*End of Practical*