CS-4331-Special Topics in Security

Fall 2016

LAB # 2: Hacking WPA2 Personal

In this lab, you will launch an attack on a WPA2-protected Wi-Fi network to recover the passphrase (aka Pre-shared Key or PSK). With good old WEP completely broken, the gold standard in Wi-Fi security is now WPA2. Unlike WEP whose key can be recovered by simply capturing a lot of traffic and performing cryptanalysis on it, an attack on WPA2 is not guaranteed to succeed. The weak link under WPA2 is the passphrase, which can be broken if weak. No other attack on WPA2 is currently feasible.

We have set up our WPA2-protected WLAN with a weak passphrase. Your task will be to use aircrack-ng in conjunction with a dictionary to break this passphrase. The SSID of the network is CS-4331-2016. To launch the attack you will need to use a wireless adapter which supports packet injection and can be configured to operate in monitor mode. It is quite likely that the wireless adapter in your laptop will not have this functionality. You may borrow our adapter, which is an Alfa AWUS036H 1000mW 1W 802.11b/g network adapter, or buy one for yourself (e.g., from Amazon at about $20 -$30). For those who may want to explore the different kinds of network adapters which support this experiment, Google is your friend.

The experiment is meant to give you hands-on practice with the concepts covered in class and must *only* be done with our class Access Point (SSID: CS-4331-2016). Note that it is a federal crime to access a computing device without authorization or to exceed authorized access. For details, refer to the Computer Fraud and Abuse Act (18 U.S.C. 1030). Carrying out this kind of attack on any Wi-Fi network other than the one set up for this class (or one owned by you) is a crime under state and federal laws.

It is recommended that you use Kali Linux for this experiment since all the tools you need are already installed in this Linux distribution. For those of you who don't have Kali as your main OS or dual boot OS option, you may opt to: (1) use your VM again; however, this option can sometimes be troublesome, (2) boot Kali from a flash drive.

I recommend that you boot Kali from a flash drive. You may download and install Lili -- Linux Live USB Creator -- to convert your flash drive into a bootable flash drive. You can choose to have Lili download the Kali ISO for you; or you can choose to download it separately and pass it to Lili.

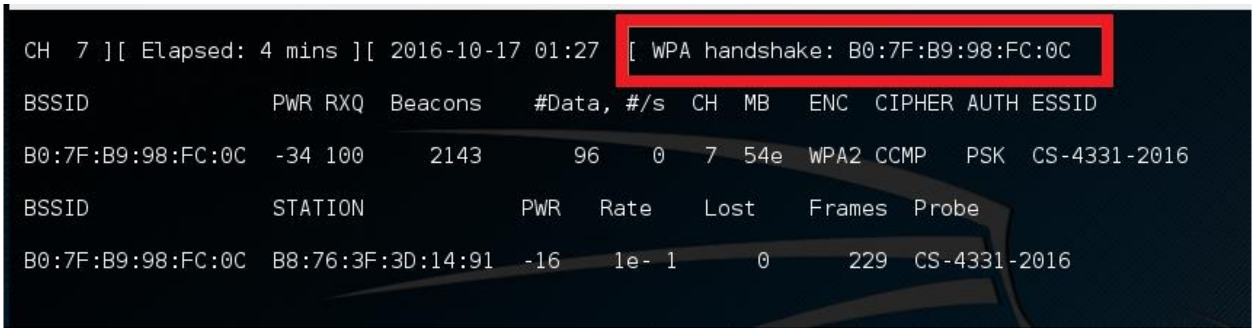
Experiment Steps

1. After booting into Kali, type the command *airmon-ng* to determine if your wireless adapter is "seen" by Kali Linux. It should show the interface, chipset, and driver.

2. Use airmon-ng to put your wireless adapter in monitor mode. This will require a command of the form *airmon-ng start wlanxx.* You will obtain the value of xx from the relevant wireless interface returned in the previous step.
3. Use the command *airodump-ng* wlanxxmon to display critical information about the wireless networks being “seen” by your wireless adapter.
4. From the information displayed in the previous step, identify the record corresponding to our CS-4331-2016 network. From this record identify the BSSID, and channel of our adapter. Observe at least one host connected to this BSSID.
5. You will now capture and save traffic associated with the channel and BSSID identified in the previous step. Use the command *airodump-ng* --bssid x -c *a* --write *y z*, where *x* is the BSSID, *a* is the channel, *y* is the file name to which you will save the captured data and *z* is the name of the interface which you earlier set into monitor mode.
6. To capture the handshake, force one or more clients currently associated with the Access Point (AP) to disassociate. Use the command: *aireplay-ng* -- deauth 1 –a Acess_Point_MAC –c Client_MAC Interface_name

   The value of 1 means a burst of 64 deauth packets. Wait for a couple of seconds to see if the handshake is captured. You may have to try the previous command multiple times until the handshake is captured.

   You will know that you have captured the handshake when you see a message similar to the one in the red bounding box in the figure below.



```
CH  7 ][ Elapsed: 4 mins ][ 2016-10-17 01:27 [ WPA handshake: B0:7F:B9:98:FC:0C

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

B0:7F:B9:98:FC:0C  -34 100     2143       96    0   7  54e  WPA2 CCMP   PSK  CS-4331-2016

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

B0:7F:B9:98:FC:0C  B8:76:3F:3D:14:91  -16    1e- 1     0      229  CS-4331-2016
```

It may be convenient for you to run steps 3 through 6 in separate terminal windows so you can reference information easily between commands. One cool way to do this is to install the *terminator* program. This program allows you to split your screen into multiple segments each of which has a terminal.

7. Once the handshake is captured, you may now crack the password using aircrack-ng x –w y, where x is the name of the file which we earlier used to store the information in step 5 and y is the absolute path to the password file or dictionary.

   The directory of the password file is: /usr/share/wordlists/

The actual password list is in the zipped file: rockyou.txt.gz
Note that you will have to unzip this file first.

Step # 7 is offline; so you can go and execute it at your convenience. The step might take a while.

You will be expected to:

(1) record screenshots for each stage of the experiment
(2) What do you understand by the term monitor mode used in Step #2?
(3) Using your knowledge of the WPA2 handshake, explain what is happening in Step 7.
(4) Would MAC address whitelisting prevent this attack? Why/why not?