LAB # 2: Breaching WPA2 Personal

CS 6343, Summer 2022

Marty and Wendy Byrde are at it again. This time, they plan to send an email to Navarro but want to make it look like the email came from Darlene Snell. They want to get Darlene into trouble with the cartel as the contents of the email are, to put it simply, not your cup of tea. They know that Navarro will trace the email back to the originating router, so they have made a plan to hack into Darlene's router and use her Wi-Fi to send out the email.

One of the concepts we have repeatedly talked about in this class is the brute-forcing of a crypto system. In this lab you will get some hands-on experience with a limited form of brute-force (i.e., a dictionary-driven attack) on a widely used system. Another notion we have seen later in the course is that a cryptographic system could be attacked by exploiting how its various components are put together and without necessarily attacking the cipher itself. This lab will also give you a feel of this notion as you will breach an AES-oriented system without attacking AES itself.

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 dominant encryption standard for Wi-Fi security as of today is WPA2. WPA2 however also falls to a dictionary attack if configured with a weak passphrase.

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-6343-2022*. To launch the attack you will need to use a Wireless Network Adapter which supports packet injection and can be configured to operate in monitor mode. If you have a fairly high-tech computer, its Wireless Network Adapter should have these features out of the box. If not, you may have to borrow our USB Wireless Network Adapter (the line will be long!) or buy one for yourself (e.g., from Amazon or Best Buy). Before buying one however, be sure to "consult" Google to help you determine whether it supports *aircrack-ng*.

The experiment must ***only*** be done with our class Access Point (SSID: *CS-6343-2022*). 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, you should consider: (1) dual boot OS option, (2) using Virtualbox again (might be tricky for this lab!), or, (3) using a Live USB (recommended[1]). The following link

[1] If you might restart your system before completing the experiment, consider working in persistence mode so you don't lose your changes and data.

should be of help for those doing Option 3 -- https://www.kali.org/docs/usb/. For the other options feel free to dig up your own resources. 🙂

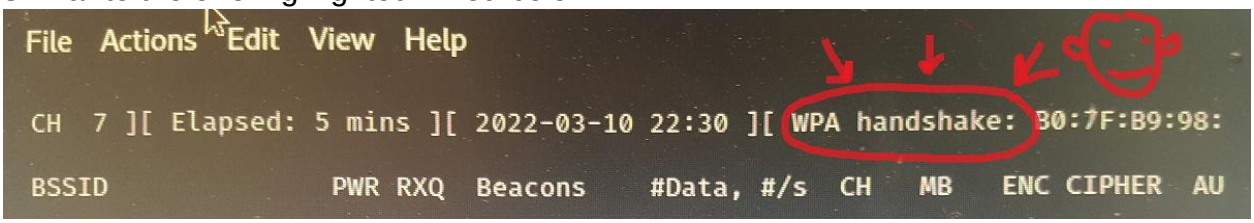
PART 1

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-4331-2019 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 Access_Point_MAC –c Client_MAC wlanxxmon

   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 highlighted in red below.



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.

PART 2

You will attack the same network using a different tool, **Wifite2**. Perform research on the necessary commands for this tool and rerun the attack. Please only attack the network set up for this class. Show/describe screenshots for all your work.

Questions:

You will be expected to do the following:

(1) record screenshots for each stage of the experiment and give brief descriptions of the meanings of the content seen in each screenshot. If your screenshots have very tiny fonts that are difficult to read, you will lose points. I will evaluate all screenshots exactly as submitted; I wont zoom in to parts of your submission.
(2) using your knowledge of the WPA2 handshake/setup, explain what is happening in Steps 6-7.
(3) In your opinion, how could WPA2 be protected from this attack? Discuss as many ideas as possible.

NOTE:

1- While you are not barred from consulting with colleagues, you must note that this is not group work. Every individual student is expected to execute the experiment, capture their own handshake and run the attack on it. Before you begin the experiment, please do the following.

If you have a recent Kali installation, your default shell should likely be *zsh*. Add the following text at the top of the *~/.zshrc* file.

cowsay "Welcome *First Name Last Name*! Today is $(date '+%A %B %d %Y %r')"

Install *cowsay* before restarting the terminal and make sure the name and date displayed show up in all the screenshots you will submit in blackboard. *First Name* should be your first name and *Last Name* should be your last name. If your shell is bash, the edit should be made to *~/.bashrc* instead.

2- Your responses to Questions (2) and (3) above need to be the first things on Page 1 of your submission. All the other stuff should come later.