Chapter 8: WPA2 Cracking Lab

1. Start and login to your Kali Linux virtual machine as user kali with a password of **kali**.

2. View the current dictionary file that will used to crack WPA2 passphrases by typing **sudo cat /usr/share/wordlists/rockyou.txt**. Press **CTRL+C** until the display of the file contents is interrupted and stops.

3. Change to the current user home directory by typing **cd** and pressing **ENTER**.

4. Type **ls** and notice the wpa-06.cap capture file. This file capture was captured on a WiFi network and contains the authentication traffic used by a valid client initially connecting to the WPA2 preshared key (PSK) network. Attackers will normally force existing clients to disconnect from the WiFi network thus forcing them to reconnect. This technique is called *deauthentication*.

5. Begin the attack by typing **sudo aircrack-ng wpa-06.cap -w /usr/share/wordlists/rockyou.txt**. After a few moments press **CTRL+C** to stop the attack (no passphrase is found).

6. You will now add a passphrase to the dictionary file used in the attack. Type **sudo nano /usr/share/wordlists/rockyou.txt**. At the top of the file type in (or copy from here) **2W4335102288**; this is the actual WiFi passphrase; attackers normally use multiple dictionaries containing tens of millions of potential passphrases. Press **CTRL+X**, **Y** and press **ENTER** to save the change to the file.

7. Run the attack again by typing **sudo aircrack-ng wpa-06.cap -w /usr/share/wordlists/rockyou.txt**. This time notice the WPA2 passphrase is shown next to the text “KEY FOUND”. Bear in mind that this is an *offline* attack; intruder detection settings on the WiFi access point/router will not pick up on this attack.