# Kali Linux

and

# Wireless

## Deep Dive

Kali Linux & Wireless Deep Dive

Presented at WLPC Phoenix 2024

Lab Guide

# Day 1

# Hands-on Lab 1-1: Kali

Follow the onscreen instructions.

1. Username is ______, password is ______.
2. Open a terminal window.
3. Once the terminal window opens type in **halt** to shut down Kali Linux. In the latest version of Kali you may have to elevate your privilege to do certain commands. You do this by preceding the command with the word **sudo**. So, in this case, for example, **sudo poweroff**.
4. Wait until you see **System Halted**, or the screen goes black.
5. You have now successfully started up and shut down your Kali Linux Kit.

- - - END OF LAB - - -

# Hands-on Lab 1-2: System Maintenance and some Preparation

It is good to keep Kali up-to-date. Before we start doing installs you will need to update the repositories. Also, we will get you to download a zip file to give you some files that will make things easier.

1. Login to your Kali Laptop and open a Terminal Window.

2. Connect to the internet SSID.

3. Type **sudo apt update**. Kali will update the repositories.

4. Download the class files, your instructor will provide a resource (e.g.a Github site), and instructions.

5. This will give the following files:
   **PasswordList** - a password list for you to use. This is the list of the 500 most common passwords in use, with Candy123 added. Be aware some of the passwords are quite vulgar, but we are all adults here, and people actually use these passwords.
   **hostapd** – a config file for hostapd.
   **psk.conf** – a config file for wpa_supplicant.
   **ColorFilters** – colored filters for Wireshark.

6. **Throughout this document anything appearing in <> is a replaceable parameter. For example, <BSSID> means you have to type in an actual BSSID value.**

7. **Under no circumstances should you ever type “sudo apt upgrade” or “sudo apt full-upgrade -y” during class!!! Also, if you decide to upgrade “rolling Kali”, make a backup (or two) before you do this.**

- - - END OF LAB - - -

# Hands-on Lab 2-1: Find a Hidden SSID

The **airmon-ng suite** is the foundation for all Wi-Fi hacking and pentesting. One of the most important stages of hacking/pentesting is reconnaissance. The **airodump-ng tool** is very important to learn. Most people think it just shows SSIDs, but it can do a lot more…

1. Login to your Kali Laptop and open a Terminal Window.

2. Type **sudo airmon-ng start wlan1**. Notice you may get an error about interfering processes. You can remove these processes by typing **sudo airmon-ng check kill.** (You will no longer be able to connect to the internet as you just stopped the networking service and wpa_supplicant processes). The easiest solution here is to simply reboot Kali if you want to connect to the internet again. Probably a good idea to complete all internet activities before you run the check kill command!

3. Type **sudo airodump-ng wlan1mon** and view the output. You see a lot of information. You should see a list of multiple BSSIDs, and their ESSID names. You may also see clients too, and who they are probing for. If a client is associated to an AP, the BSSID of the client will be filled in with its APs BSSID address. Notice you see information about the SSIDs and what security they are using. Pay attention to the ENC column and the AUTH column. Stop the command with Ctrl-C. (If you are having trouble finding clients move on to step 4).

4. Type **sudo airodump-ng –c 11 wlan1mon** and view the output. You should now see a list of multiple BSSIDs, and their ESSID names but restricted to channel 11 (note: you may see other channels, ask the instructor why…) You should also see clients probing on channel 11 too. If you wanted to restrict your search to 2.4GHz or 5GHz, you could use the **--band g or --band a** option. As our USB devices are 2.4GHz only, this parameter won't work. Stop the command with Ctrl-C.

5. Type **sudo airodump-ng –c 11 --bssid <BSSID> wlan1mon** and view the output. Here you will need to select one of the BSSIDs you have already found, and use that in place of <BSSID> (note --bssid has two '-' before the letters – typically when you use a letter or number as a parameter, you use only one '-', but when you use a word, you need two '-'). You should see any clients associated to a given AP. Stop the command with Ctrl-C. Keep trying this until you see clients (you may need to change to a different channel).

6. Type **sudo airodump-ng –c 11 wlan1mon --manufacturer** to view manufacturer information on APs.

7. Type **sudo airodump-ng –c 11 --bssid <BSSID> wlan1mon** and view the output. Make a note of one of the SSID names. Press Ctrl-C. Now type **sudo airodump-ng –c 11 --essid "<SSID_name>" wlan1mon** to view a given SSID (you must use quotes here).

8. Another feature of **airodump-ng** is its ability to show different screens. Once again type **sudo airodump-ng –c 11 wlan1mon** and view the output. Press the **tab** key. Using the arrow keys you can move up and down the list highlighting different SSIDs. Notice that when you highlight an SSID, any clients of that SSID are also highlighted.

9. Select an SSID and press the **m** key. Notice you can select colors by continuing to press the **m** key. Again, any clients show up in the same colors.

10. You can also change what is displayed. Press **s**, to scroll through different sorting options. Press **d**, to reset to default.

11. Press **a**, to scroll through different views and combination views of APs, clients, and ACKs.

12. One trick here, is to press **tab** and select an SSID that is showing as **<length: #>**, (where **#** is a number). This is a hidden SSID. Once you have it highlighted, select a color using **m**. Leave it running, and if a client connects to the hidden network, the SSID will be displayed in the color you selected. This is an easy way to discover hidden networks!

13. Try this by highlighting the hidden network with a BSSID of xx:xx:xx:xx:06:42, and asking your instructor to connect to reveal the SSID name. It actually doesn't matter if you use the correct key or not!

    - - - END OF LAB - - -

# Hands-on Lab 3-1: Deauthentication, *en masse*

One other tool in your airmon-ng toolset is aireplay-ng. This tool can be used to deauthenticate clients. This is an important tool to make clients connect to what you want them to connect to.

1. Restart your Kali Linux box, to reset everything. (Use **sudo reboot**, it's easier).

2. Login to your Kali Laptop and open a Terminal Window.

3. Type **cd** to make sure you are in your home directory. If not, simply type **cd ~** to move to your home directory.

4. Type **sudo airmon-ng start wlan1**.

5. You may get an error regarding channel number. There are two ways to fix this. Try to rerun the command with the **--ignore-negative-one parameter**. Alternatively, you can run **sudo airodump-ng –c 11 wlan1mon** to make wlan1mon be on the same channel as the BSSID you are attacking. (In this case channel 11).

6. Run a deauthenticate attack on the SSID WLPChax1using the following command: **sudo aireplay-ng -0 0 –a <bssid> wlan1mon** (use the BSSID of the SSID – you know how to find that now remember!). This will de-auth all stations on the wireless network, and cause them to re-connect.

   - - - END OF LAB - - -

# Hands-on Lab 3-2: Deauthentication, Targeted

Sometimes you need to be a little more subtle. Instead of doing a broadcast de-auth, try something a little quieter…

1. From your Terminal Window…

2. Type **cd** to make sure you are in your home directory. If not, simply type **cd ~** to move to your home directory.

3. Type **sudo airodump-ng –c 11 –a --bssid <BSSID> wlan1mon** and view the output. Note a client address connected to the SSID WLPChax1. If there aren't any, ask the instructor for help.

4. Is there a de-auth attack that can target a client? How would you find out? Try it…

5. Hint, use help…

   - - - END OF LAB - - -

# Hands-on Lab 3-3: Deauthentication, Defeated

Is it always this easy? Well, try this…

1. From a Terminal Window…

2. Type **cd** to make sure you are in your home directory. If not, simply type **cd ~** to move to your home directory.

3. Connect to WLPChax2 with your phone. The password is **Candy123**.

4. Repeat the broadcast de-auth attack, using the WLPChax2 SSID. Use **airodump-ng** to find the BSSID, and try to deauthenticate the clients.

5. Not so easy, eh? This SSID has 802.11w/PMF enabled.

   - - - END OF LAB - - -

# Hands-on Lab 4-1: Wifite

SO, let's attack some Wi-Fi. In this Lab we are going to use Wifite. Wifite simplifies a WPA/WPA2 attack. Wifite is a scripted tool that will easily attack WPA/WPA2 Personal SSIDs. Wifite is easy to use, and will actually start to de-auth clients on the network to get them to reconnect, so you can capture the 4-way handshake. You are going to be using a dictionary attack, so first you will need to copy over the dictionary.

1. Restart your Kali Linux box, to reset everything.

2. Login to your Kali Laptop and open a Terminal Window.

3. Type **cd** to make sure you are in your home directory. If not, simply type **cd ~** to move to your home directory.

4. Type **cp /usr/share/wordlists/rockyou.txt.gz .** to copy the rockyou wordlist to your current directory. (Note: that is not a typing error, type it in as seen, you are copying to the current directory '.').

5. Type **ls** to view the directory. You should see the file **rockyou.txt.gz** file.

6. Type **gunzip rockyou.txt.gz** to extract the dictionary file. While this unzips, the screen may appear to freeze, be patient, and wait for it to complete.

7. Type **ls** to view the directory. You should see the file **rockyou.txt**. It auto deleted the **rockyou.txt.gz** file when it extracted the **rockyou.txt** file.

8. Type **sudo wifite --wpa --dict ./rockyou.txt --kill** to attack WPA/WPA2 only and use rockyou.txt as the dictionary file, and to stop interfering process (basically Wifite's version of **airmon-ng check kill**).

9. Wifite will start and check for dependencies. All should be good, if any show up in red, it is okay for now, you can ignore these.

10. Wifite will ask you to select an interface, choose **wlan1**. (Note you may need to press **2** to select **wlan1**).

11. Wifite will immediately start finding networks. When you see **WLPChax1** pop up, press **Ctrl-C**. Select its number as a target from the list, and press Enter.

12. Depending on your version of Wifite, it may or it may not do steps 13-16> If you get any of these options deal with them as shown. If you jump straight to the handshake attack, continue from step 17.

13. If Wifite tries a WPS attack (Pixie-Dust) terminate this with **Ctrl-C**. Press **c <enter/return>** to continue attacks.

14. If Wifite tries a WPS NULL PIN attack, press **Ctrl-C**. Press **c <enter/return>** to continue attacks.

15. If Wifite tries a WPS PIN attack, press **Ctrl-C**. Press **c <enter/return>** to continue attacks.

16. Wifite may fail to run a PMKID attack, as relevant components are not installed. It also may skip this entirely, newer versions of Wifite are getting smarter.

17. Once Wifite starts the Handshake attack, it will try and discover clients. If it is having trouble capturing the 4-way handshake, it will then start de-auth attacks against the network, forcing clients to re-authenticate so it can capture the 4-way handshake. The process is easy now, you sit back and watch. Once it captures a 4-way handshake, it immediately starts the dictionary attack. Pretty soon the cracked PSK will appear. (Should take a few minutes).

18. If you are finding it is taking too long, simply use the password.txt list in the folder you downloaded in lab 1-2, or create your own .txt dictionary file, and use a small number of words, putting Candy123 in the wordlist. Then re-run Wifite using your dictionary instead of **rockyou.txt**. You may find Wifite is smart enough to notice you are attacking an SSID it has already captured a handshake for, to make it go through the process of capturing handshakes again, use the **--new-hs** flag to make it recapture the handshakes.

19. In testing, some testers found intermittent errors, that they kept getting “key not found” even though the key is there. If this happens to you, try the attack again, but this time attack the **peeskay1** SSID. We found that rebooting the AP fixed this issue…

- - - END OF LAB - - -

# Hands-on Lab 4-2: Some Things You Can Do, Now You've Cracked the Key…

Use Wireshark to view frames unencrypted.

1. Run **sudo airodump-ng -c <channel AP is on> --bssid <BSSID of SSID> -w test1 wlan1mon**.

2. Connect to WLPChax1 yourself using the password of Candy123.

3. Wait until you see **WPA Handshake:…** appear in the top right. Then press **Ctrl-C** to stop airodump-ng.

4. Connect again if needed.

5. Type **ls**. Find the **test1-xx.cap** file with the biggest number in xx. (There may be multiple files if you run the command several times).

6. Type **wireshark test1-xx.cap**, this will load Wireshark.

7. Select **View > Coloring Rules… > Import**. Select the file **colorfilters** in the folder **ColorFilters** you downloaded int lab 1-2. Select **OK**. You have loaded our Friend Eddie's coloring filters. They are F.A.B.!

8. Enter a filter of **eapol**, select the final frame, then remove the filter. Do you see data frames with data in after exchange number 4? Nope, they should be encrypted. Try and search for the following protocols: ARP, DHCP, DNS, and maybe HTTPS or HTTPS, you should not see any.

9. Select **Edit > Preferences > Protocols > IEEE 802.11**.

10. Select **Decryption keys > Edit**.

11. Select the **+** key. Change **Key Type** to **wpa-pwd**, and then enter **Candy123:WLPChax**1 in the Key field. Press **Enter**.

12. Select **OK**, and **OK** again.

13. Again enter a filter of **eapol**, select the final frame, then remove the filter. Do you now see data frames with data in after exchange number 4? Yes! You should see data frames. Try and search for the following protocols: ARP, DHCP, DNS, and maybe HTTPS or HTTPS.

14. Advanced: take a peek at the broadcast beacons. Look for **RSN IE 48**. This tells you all about the security being used.

- - - END OF LAB - - -

# - - - END OF DAY1 - - -

# Day 2

# Hands-on Lab 5-1: To Break EAP, You Need a Hammer. Demo.

In this lab you will be introduced to EAPHAMMER. This is a very convoluted attack so it will be done as a demo to show you what to do. Then you will have a chance to do it yourself.

1. Restart your Kali Linux box, to reset everything.

2. Login to your Kali Laptop and open a Terminal Window.

3. Type **cd** to make sure you are in your home directory. If not, simply type **cd ~** to move to your home directory.

4. Sign into **WLPChax4** on your phone using **user1/Candy123!**. You may be asked to accept and trust the certificate.

5. Type **git clone https://github.com/s0lst1c3/eaphammer.git**.

6. Type **cd eaphammer**.

7. Type **sudo ./kali-setup**. Confirm with **y** if prompted. This may take a while. You may get some errors, but it should work.

8. Type **./eaphammer --cert-wizard** to generate a certificate.

9. Create a certificate.

10. To launch attack type **sudo ./eaphammer -i wlan1 --channel <X> --auth wpa-eap --essid WLPChax4 –creds**. (<X> represents the channel. Use the correct channel that the SSID is on).

11. Erase the SSID from your phone, now try and reconnect, this time enter a false username and password.

12. What happened?

13. Are you scared yet?

14. Have you learned the importance of certificate validation?

    - - - END OF LAB - - -

# Hands-on Lab 5-2: To Break EAP, You Need a Hammer. Your Turn!

In this lab you will be introduced to EAPHAMMER. This time, it is YOUR turn.

1. Restart your Kali Linux box, to reset everything.

2. Login to your Kali Laptop and open a Terminal Window.

3. Type **cd** to make sure you are in your home directory. If not, simply type **cd ~** to move to your home directory.

4. Connect to the class Wi-Fi.

5. Type **sudo apt update**.

6. Type **git clone https://github.com/s0lst1c3/eaphammer.git**.

7. Type **cd eaphammer**.

8. Type **sudo ./kali-setup**. Confirm with **y** if prompted. This may take a while. You may get some errors, but it should work.

9. Type **./eaphammer --cert-wizard** to generate a certificate.

10. Create a certificate.

11. To launch attack type **sudo ./eaphammer -i wlan1 --channel 6 --auth wpa-eap --essid <yourname> –creds**.

12. Sign into **<yourname>** SSID on your phone. Accept and trust the certificate. Use a username and password of your choosing.

13. Are you impressed?

14. Experiment using Apple IoS devices, Android devices, Windows 10 & 11, Mac (try different versions of OS).

15. Congratulations you just hacked WPA2-Enterprise.

- - - END OF LAB - - -

# Hands-on Lab 6-1: Kismet

In this section, we will introduce the basic features of Kismet. Kismet is not really an attack tool, but it does reveal a ton of information about wireless networks.

1. Restart your Kali Linux box, to reset everything.

2. Login to your Kali Laptop and open a Terminal Window.

3. Type **cd** to make sure you are in your home directory. If not, simply type **cd ~** to move to your home directory.

4. Type **sudo kismet -c wlan1** to start Kismet.

5. Open a browser to **localhost:2501**

6. For first time running, it will ask you to configure a username and password.

7. Use **admin/P@ssw0rd**.

8. Select the 3 horizontal lines (burger bar) in the top left-hand corner, and select **Data Sources**.

9. Kismet should find your devices. Select **wlan1**, and choose **Enable Source**.

10. Close the last window that popped up, and you should see data on the Wi-Fi network.

11. Open a new Terminal window.

12. Type **sudo airmon-ng start wlan2**.

13. Type **sudo airodump-ng wlan2mon**.

14. Find the channel **peesakay1** is on.

15. Type **sudo airodump-ng -c <channel> wlan2mon**.

16. Press **Ctrl-C** and note the BSSID given to you by your instructor.

17. Type **sudo aireplay-ng -0 0 –a <bssid> wlan2mon**. This will de-auth all stations on the wireless network, and cause them to re-connect. Did Kismet pick up the attack?

    - - - END OF LAB - - -