



计算机科学与工程系

Department of Computer Science and Engineering

CS 315 Computer Security Course

Lab 6 Part 2: Wireless Exploitation & Defenses

Introduction

In this lab students will explore ways to perform wireless attacks and understand potential defenses. The attacks that will be covered are inspecting & modifying wireless card parameters, changing the wireless transmission channel, flooding attacks, and cracking keys of WPA2 protected networks.

Software Requirements

All required files are packed and configured in the provided virtual machine image.

- The VMWare Software
<http://apps.eng.wayne.edu/MPStudents/Dreamspark.aspx>
- The Kali Linux, Penetration Testing Distribution
<https://www.kali.org/downloads/>
- Wireshark: Network protocol analyzer
<https://www.wireshark.org/#download>
- Aircrack-ng: a suite of tools to assess WiFi network security
<http://aircrack-ng.en.softonic.com/>



Setup an Access Point

In this lab, we use a TP-LINK Wireless N300 Home Router as an example, but the same concepts or ideas are applicable on other routers. Next, it explains the basic steps to setup the access point's Service Set Identifier (SSID) and security mechanism. If you have done this before, skip this section. Figure below shows a TP-LINK Wireless N300 Home Router that we are using in the classroom.



Step 1: Connect your laptop or desktop to a router.

This step depends on routers. Some routers require using Ethernet cable to physical connect the router. Some other routers may be able to connect via wireless using its Service Set Identifier (SSID). For the router that we are using in the classroom need to physically connect to one of the router's LAN ports. (Note: Think about the security implications for these two types of routers.)

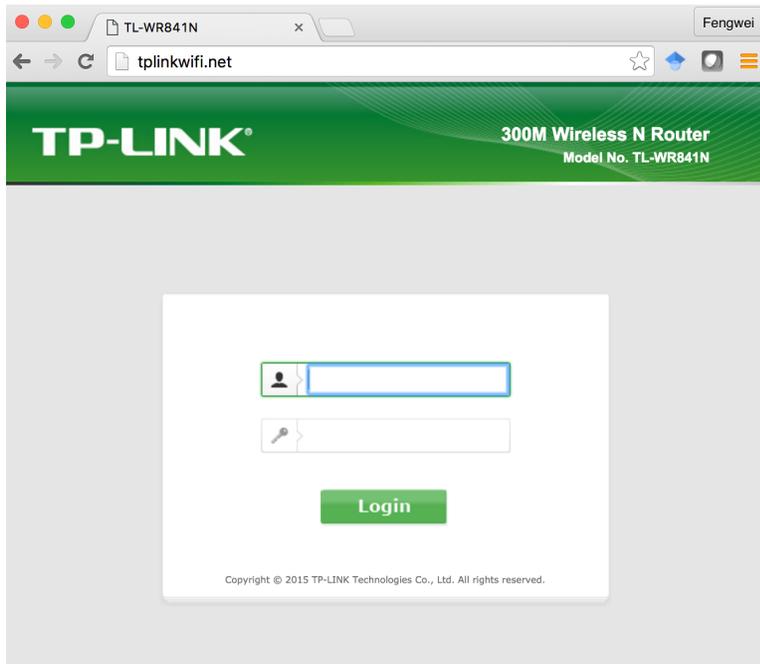
Step 2: Open the web-based setup page

Open a web browser, and type the login IP or hostname in the address field to log in the web-based management page. Normally, you can find the IP address or the hostname from the back of the router. The IP address for our router is 192.168.1.1, and hostname is <http://www.tplinkwifi.net>

Step 3: Enter the username and password to login

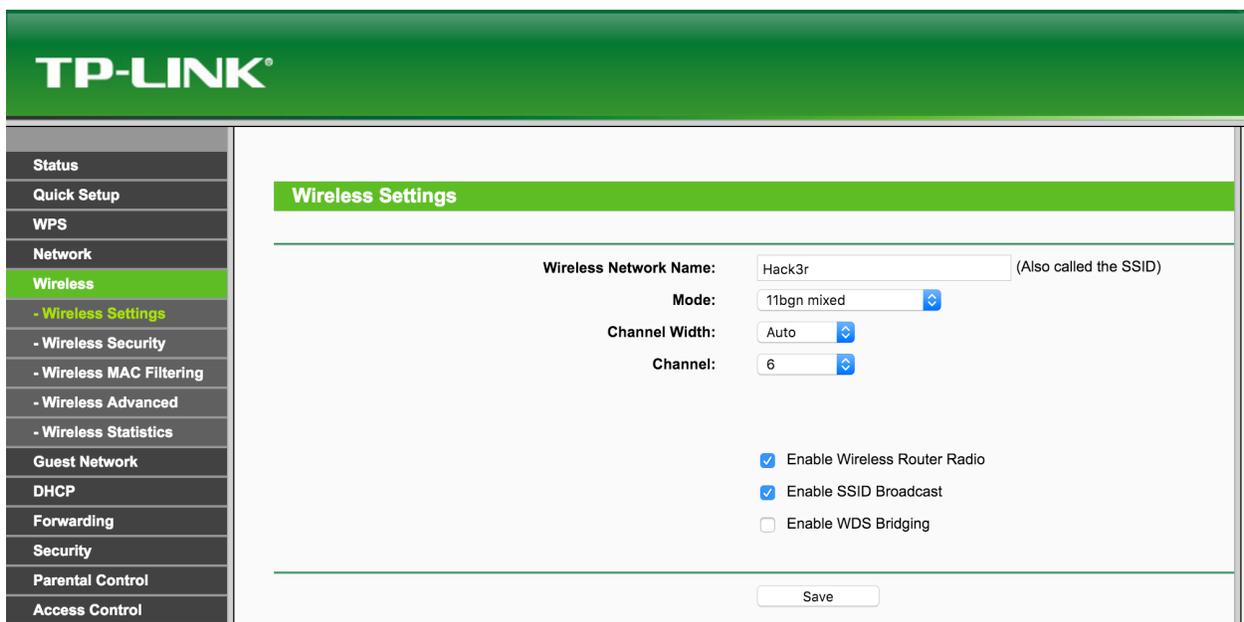
Enter the default username and password to login. For our router, its default username and password are admin and [Same-Password-As-Kali-Linux].

Figure below shows the login page of the router that we are using.



Step 4: Configure the SSID

In our router, go to Wireless -> Wireless settings. Here you can rename your wireless network (i.e., SSID). The SSID for our router is “Hack3r”





Step 5: Configure the passphrase and wireless security.

In our router, go to Wireless -> Wireless Security. Then you can configure the security for the router. In the screenshot below, we configure the security protocol to WPA/WPA2, use AES as the encryption, and the passphrase is "password". Other Security protocols are available such as WEP.

The screenshot shows the TP-Link Wireless Security configuration interface. The left sidebar contains a navigation menu with the following items: Status, Quick Setup, WPS, Network, Wireless (highlighted), - Wireless Settings, - Wireless Security (highlighted), - Wireless MAC Filtering, - Wireless Advanced, - Wireless Statistics, Guest Network, DHCP, Forwarding, Security, Parental Control, Access Control, Advanced Routing, Bandwidth Control, IP & MAC Binding, Dynamic DNS, IPv6 Support, System Tools, and Logout.

The main content area is titled "Wireless Security" and features three radio button options: "Disable Security", "WPA/WPA2 - Personal(Recommended)", and "WPA/WPA2 - Enterprise". The "WPA/WPA2 - Personal(Recommended)" option is selected. Its configuration fields include: "Version" (Automatic), "Encryption" (AES), "Wireless Password" (password), and "Group Key Update Period" (0 Seconds). A note below states: "(You can enter ASCII characters between 8 and 63 or Hexadecimal. Keep it default if you are not sure, minimum is 30, 0 means no update)".

The "WPA/WPA2 - Enterprise" option is also visible with fields for "Version" (Automatic), "Encryption" (Automatic), "Radius Server IP", "Radius Port" (1812), "Radius Password", and "Group Key Update Period" (0). A note below states: "(in second, minimum is 30, 0 means no update)".

The "WEP" option is also visible with fields for "Type" (Automatic), "WEP Key Format" (Hexadecimal), and a table for "Key Selected" with four keys (Key 1 to Key 4), each with a "WEP Key" field and a "Key Type" dropdown menu (all set to Disabled).



Capturing Wireless Packets via Wireshark

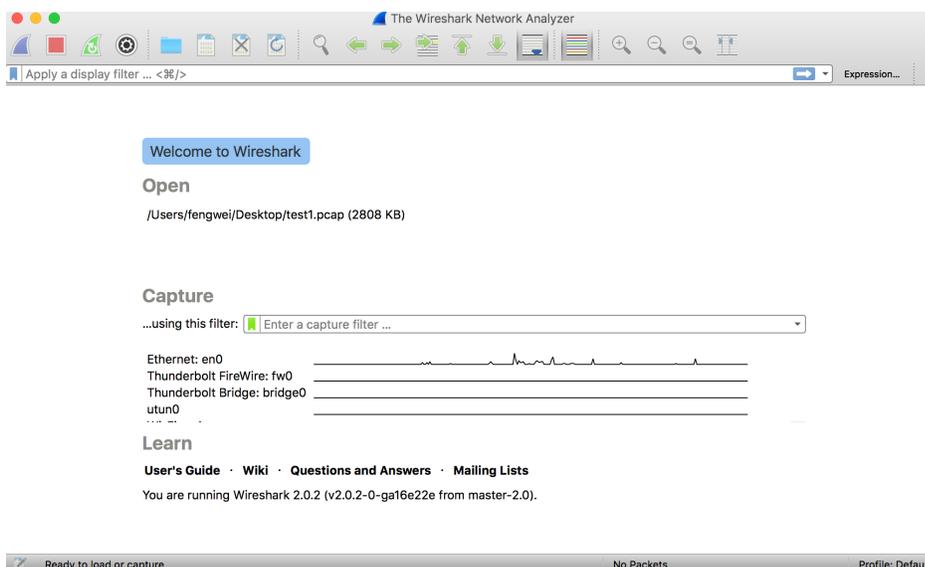
To capture wireless packets, you need to have a wireless network card installed on your machine. There are two kinds of wireless network interface: One is the internal NIC. Most of the laptops will have an internal NIC; the other one is the external NIC. The picture below shows an external network. This is a Wi-Fi USB Adapter from Alfa Network (1000mW High Power Wireless G 802.11g with 5dBi Antenna).



Once you have a wireless network card, you can run packet-sniffing tool to capture the packets as we did in Lab 1.

Step 1: Start the Wireshark program.

In order to sniff the packets, you may need to grant Wireshark root privilege by typing `$ sudo wireshark` in a terminal. Below is the screenshot of the Wireshark interface on my iMac desktop.





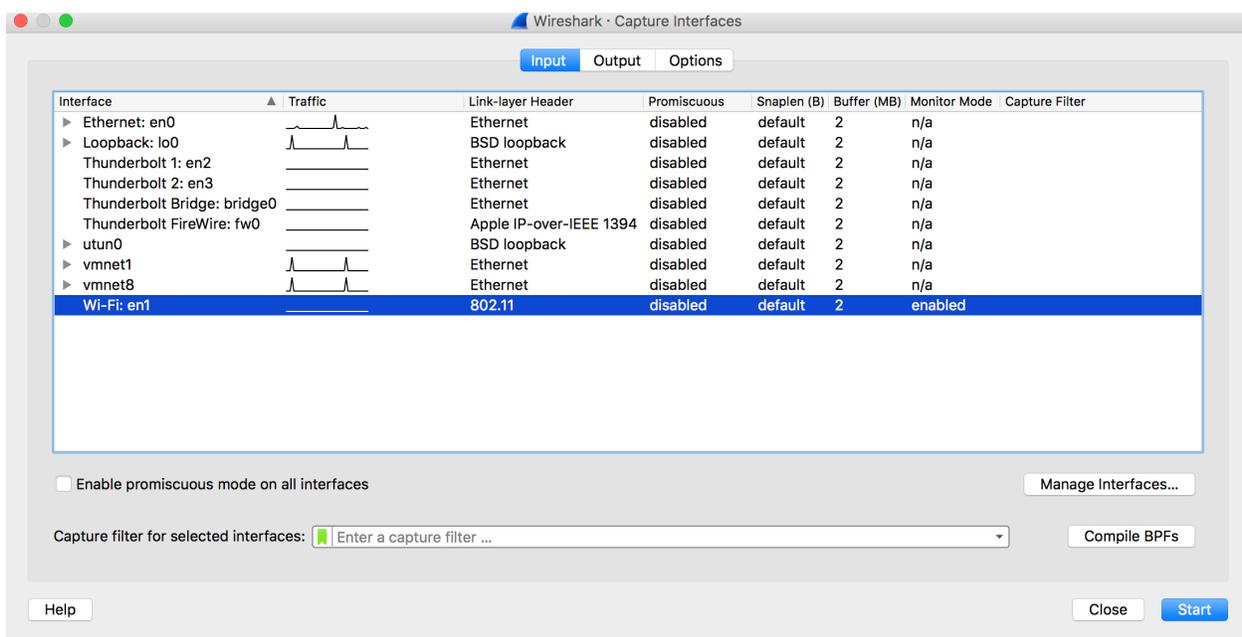
Step 2: Select the WiFi Interface

Click the Capture -> Options in the Wireshark program. Look for the interface for WiFi. Normally, the interface name is wlan0, but it may be a different name that depends on your configuration. For instance, the name of the WiFi interface on my iMac is “Wi-Fi:en1”.

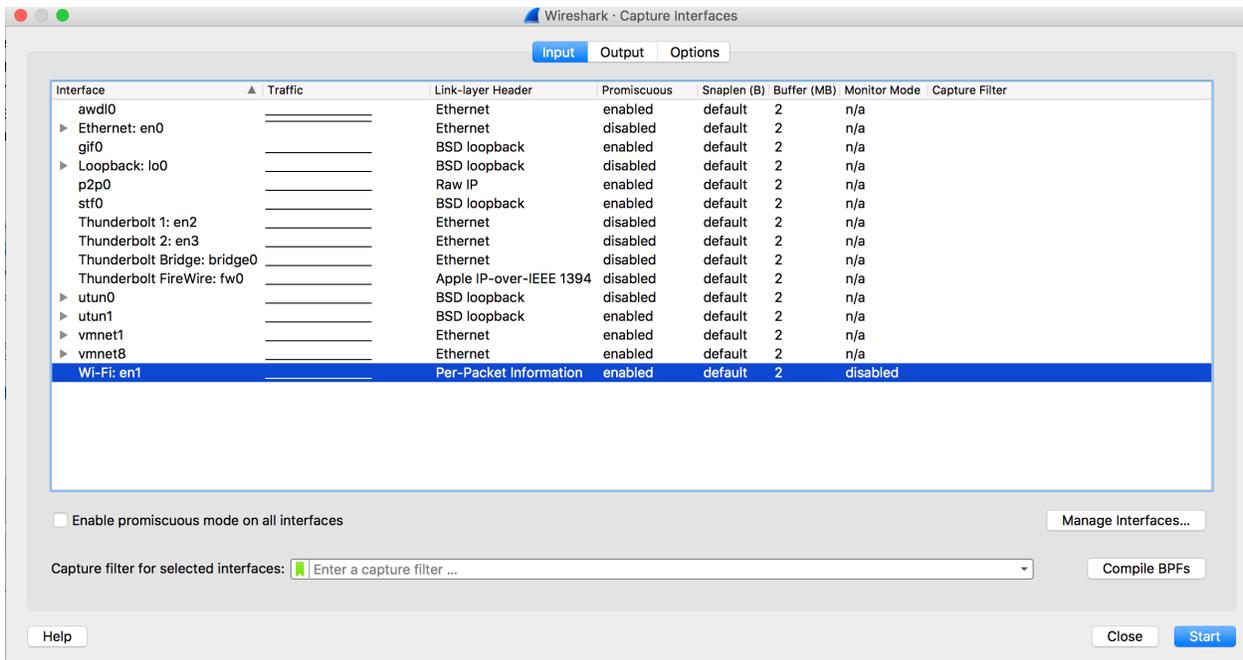
Step 3: Enable the Monitor Mode or Promiscuous Mode

In Monitor Mode, it captures all packets from all SSID in its distance range. Please note that Monitor Mode is different from Promiscuous Mode. For the purpose of this lab, we need to capture all the traffic so that we need to enable the monitor mode or promiscuous mode.

The screenshot below shows the configuration of the capture interface in Wireshark program on my iMac with monitor mode. You need to enable monitor mode and configure the Link-layer Head as 802.11.

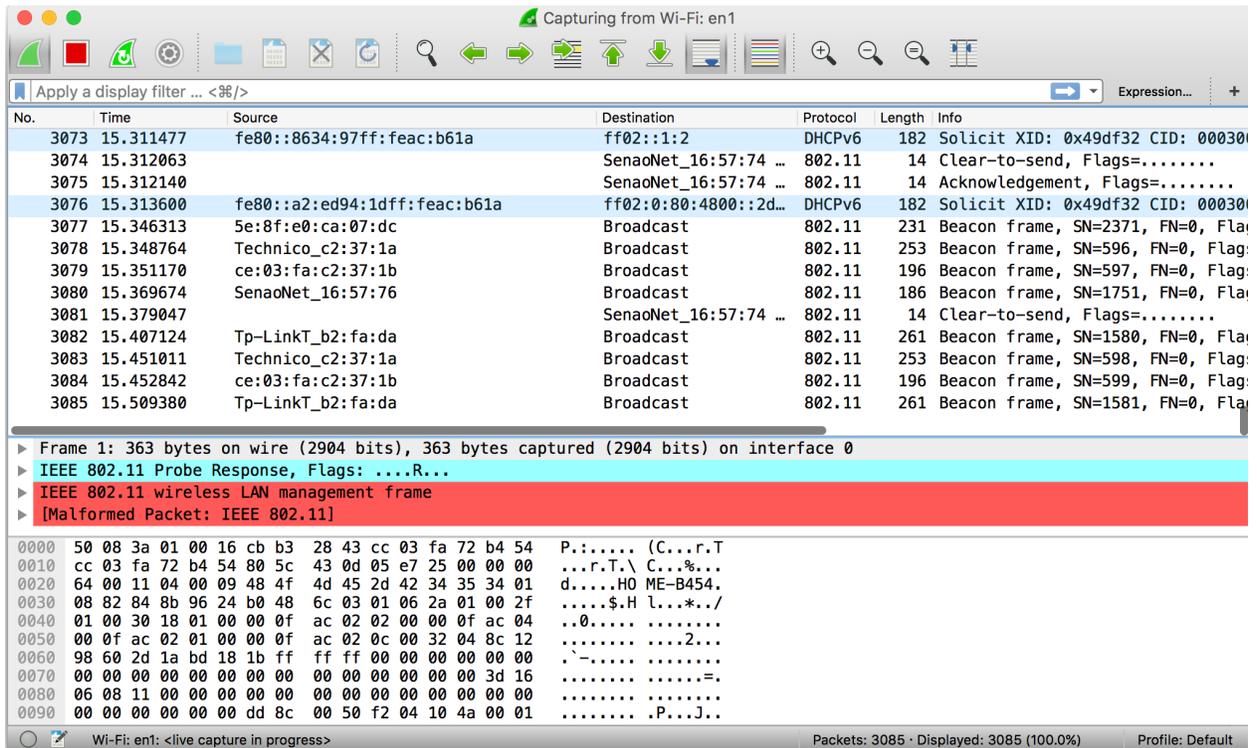


The screenshot below shows the configuration of the capture interface in Wireshark program on my iMac with promiscuous. You need to enable promiscuous mode and configure the Link-layer Head as Per-Packet Information.



Step 4: Start Capturing

Click on start in the capture interfaces window and start capture. The screenshot below shows the interface of Wireshark program while capturing in Monitor Mode.





Capturing the Four-way Handshake

To crack the WPA/WPA2 passphrase, we first need to capture the four-way handshake that contains

Step 1: Start to capture all the traffic

This is what we just did in our previous step. Just the Wireshark program into Monitor Mode and run

Step 2: Connect to the access point using its passphrase

Use your cell phone or laptop connects to the access point. For the purpose of this lab, the SSID of the router in our classroom is “Hack3r”.

Step 3: Stop Wireshark program and identify the four-way handshake

Press the stop button to stop capturing in Wireshark; type keyword “EAPOL” in the filter to identify the four-way handshake. Screenshot below shows the example.

No.	Time	Source	Destination	Protocol	Length	Info
4223	13.051622	Tp-LinkT_b2:fa:da	Apple_2d:7d:0c	EAPOL	137	Key (Message 1 of 4)
4224	13.053079	Tp-LinkT_b2:fa:da	Apple_2d:7d:0c	EAPOL	137	Key (Message 1 of 4)
4232	13.063941	Tp-LinkT_b2:fa:da	Apple_2d:7d:0c	EAPOL	217	Key (Message 3 of 4)
4238	13.072599	Apple_2d:7d:0c	Tp-LinkT_b2:fa:da	EAPOL	137	Key (Message 4 of 4)

▶ Frame 4223: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface 0

- ▶ IEEE 802.11 QoS Data, Flags:F.
- ▶ Logical-Link Control
- ▶ 802.1X Authentication

```

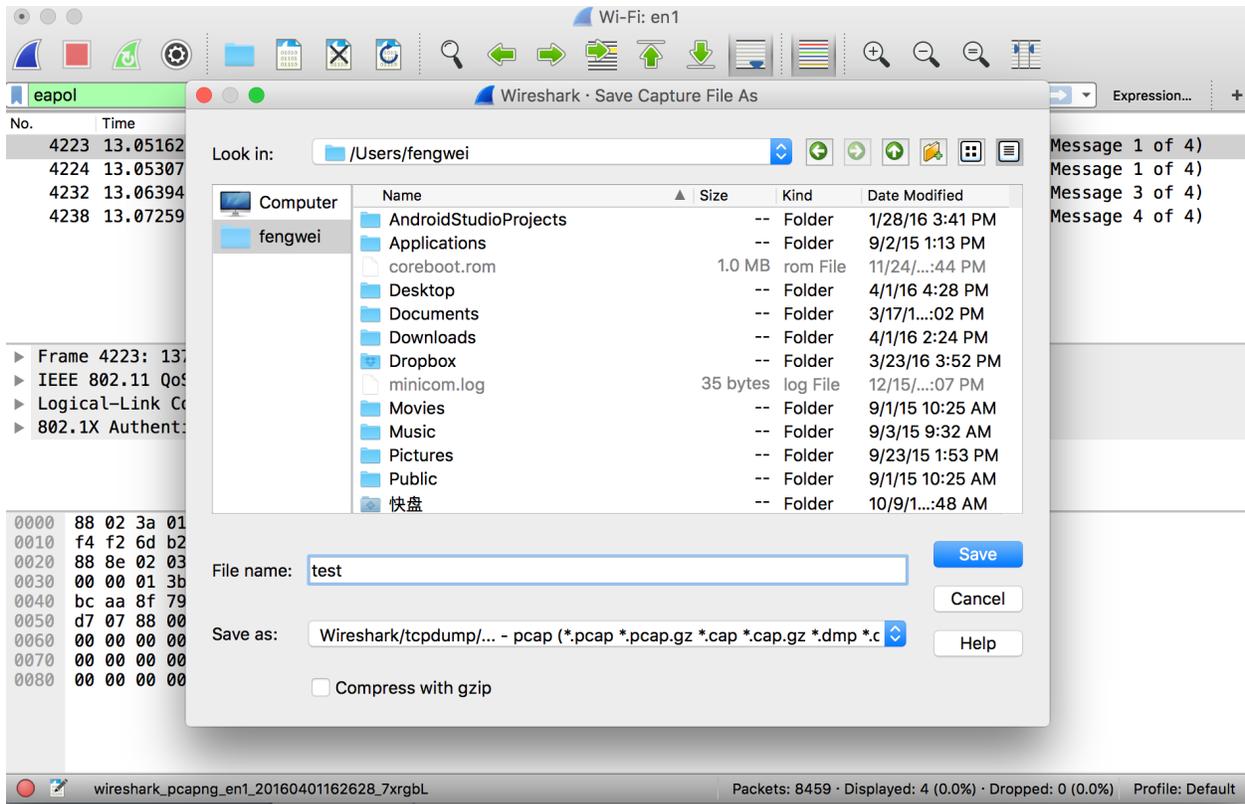
0000  88 02 3a 01 04 db 56 2d 7d 0c f4 f2 6d b2 fa da  .....V- }...m...
0010  f4 f2 6d b2 fa da 00 00 06 00 aa aa 03 00 00 00  ..m.....
0020  88 8e 02 03 00 5f 02 00 8a 00 10 00 00 00 00 00  ....._.....
0030  00 00 01 3b fd 43 af f3 42 ad 00 2e 77 d3 e7 e4  ...;.C.. B...w...
0040  bc aa 8f 79 42 8a 3f c0 23 c6 1b c4 e8 f6 01 8c  ...yB.?. #.....
0050  d7 07 88 00 00 00 00 00 00 00 00 00 00 00 00  .....
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0080  00 00 00 00 00 4f 3c 95 63  .....0<. c
  
```

wireshark_pcapng_en1_20160401162628_7xrgbL Packets: 8459 · Displayed: 4 (0.0%) · Dropped: 0 (0.0%) Profile: Default



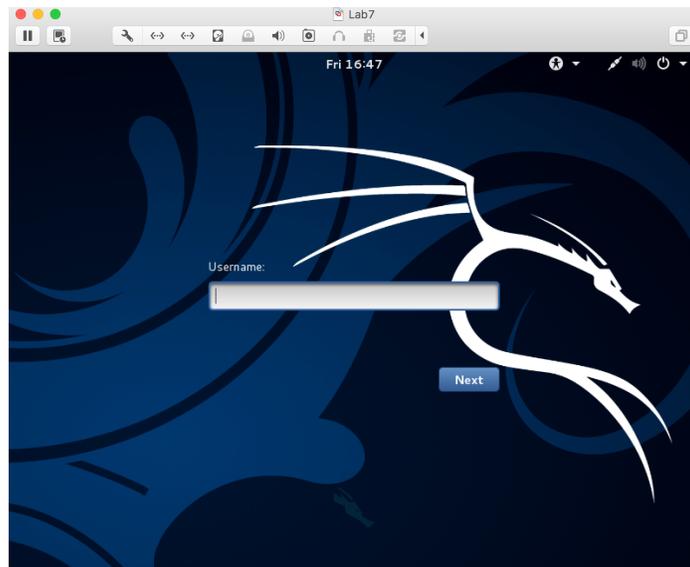
Step 4: Save the captured traffic

Click File -> Save as option to save the captured traffic to a pcap file. Screenshot below shows the example. The saved pcap file name is: test.pcap

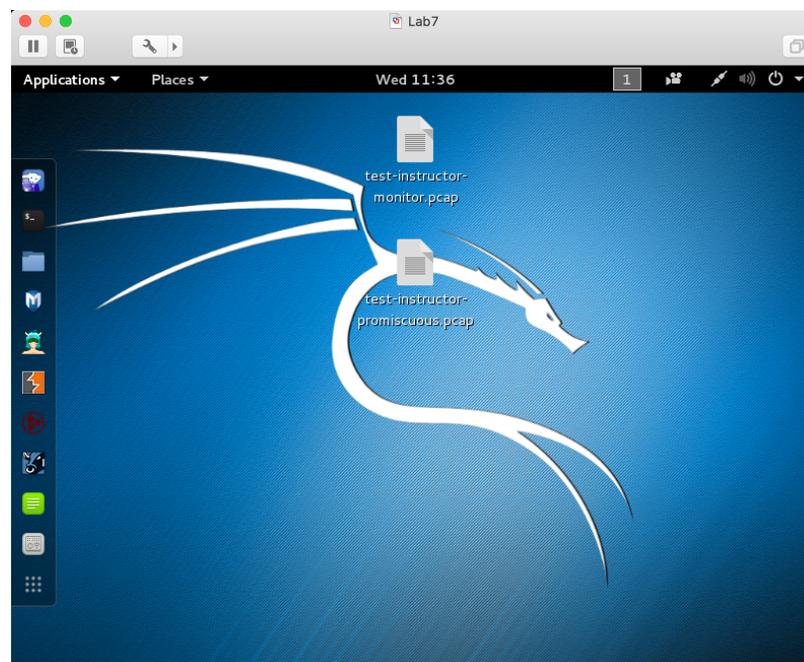


Cracking WPA2 WiFi Passphrase Using Kali Linux

In this lab, we use a Kali Linux to crack the WPA2 WiFi passphrase. Select the VM image named “Lab7”.



Login the Kali image with username root, and password [TBA in the class]. Below is the screen snapshot after login.





Step 1: Copy the test.pcap file into the Kali Linux

In our Kali Linux image, there is a copy of the test-instructor-monitor.pcap and test-instructor-promiscuous files. If you do not have your copy of test.pcap, you can also use these files.

Step 2: Use aircrack-ng to crack the passphrase

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs. Kali Linux has installed it as default.

You can type **\$ man aircrack-ng** to see the manual page of the tool

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# man aircrack-ng
```

```
root@kali: ~  
File Edit View Search Terminal Help  
AIRCRAK-NG(1)          General Commands Manual          AIRCRAK-NG(1)  
  
NAME  
    aircrack-ng - a 802.11 WEP / WPA-PSK key cracker  
  
SYNOPSIS  
    aircrack-ng [options] <.cap / .ivs file(s)>  
  
DESCRIPTION  
    aircrack-ng is an 802.11 WEP and WPA/WPA2-PSK key cracking program.  
    It can recover the WEP key once enough encrypted packets have been  
    captured with airodump-ng. This part of the aircrack-ng suite deter-  
    mines the WEP key using two fundamental methods. The first method is  
    via the PTW approach (Pyshkin, Tews, Weinmann). The main advantage  
    of the PTW approach is that very few data packets are required to  
    crack the WEP key. The second method is the FMS/KoreK method. The  
    FMS/KoreK method incorporates various statistical attacks to dis-  
    cover the WEP key and uses these in combination with brute forcing.  
    Additionally, the program offers a dictionary method for determining  
    the WEP key. For cracking WPA/WPA2 pre-shared keys, a wordlist (file  
    or stdin) or an airolib-ng has to be used.  
  
Manual page aircrack-ng(1) line 1 (press h for help or q to quit)
```



Run the following command to crack the passphrase

```
$ aircrack-ng -w /usr/share/wordlists/fern-wifi/common.txt ~/Desktop/test-instructor-monitor.pcap
```

-w: specify the path to the wordlist

Followed by the pcap file. The screenshot below shows the execution of the command.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# aircrack-ng -w /usr/share/wordlists/fern-wifi/common.txt ~/Desktop/test-instructor-monitor.pcap  
Opening /root/Desktop/test-instructor-monitor.pcap  
Read 25786 packets.  


| #  | BSSID             | ESSID                  | Encryption           |
|----|-------------------|------------------------|----------------------|
| 1  | 60:FE:20:6C:6D:5A | ATT896                 | No data - WEP or WPA |
| 2  | 5E:8F:E0:CA:07:DC | C^                     | No data - WEP or WPA |
| 3  | 10:86:8C:98:2E:04 | NDI                    | No data - WEP or WPA |
| 4  | 5E:8F:E0:90:E6:30 |                        | No data - WEP or WPA |
| 5  | F4:F2:6D:B2:FA:DA | Hack3r                 | WPA (1 handshake)    |
| 6  | 6E:8F:E0:CA:07:DC | xfinitywifi            | None (0.0.0.0)       |
| 7  | 12:86:8C:95:85:DC | ?                      | No data - WEP or WPA |
| 8  | 6D:E2:06:E5:7E:9F | HOME-371A              | No data - WEP or WPA |
| 9  | CE:03:FA:C2:37:1B | p                      | None (0.0.0.0)       |
| 10 | 1C:87:2C:E4:B8:18 | lighthouse             | WPA (0 handshake)    |
| 11 | 54:BE:F7:F4:BD:D8 | HOME-F224-2.4          | No data - WEP or WPA |
| 12 | 5C:8F:E0:CA:07:DC | DetroitLiving          | No data - WEP or WPA |
| 13 | A0:63:91:83:DE:5F | Bill Wi the Science Fi | No data - WEP or WPA |
| 14 | A0:63:91:B7:71:D9 | IIMD                   | No data - WEP or WPA |
| 15 | 12:86:8C:98:2E:04 | ??                     | None (0.0.0.0)       |
| 16 | 5C:8F:E0:90:E6:30 | AbrahamLinksy          | No data - WEP or WPA |


```

Then, we choose index for the WPA2 handshake. We can identify the index by using the SSID. From the screenshot we can see that the index for “Hack3r” is 5.

After enter 5, we can see that aircrack has successfully crack the passphrase as shown in the screenshot below.

```

root@kali: ~
File Edit View Search Terminal Help

Aircrack-ng 1.2 rc2

[00:00:00] 72 keys tested (1013.53 k/s)

KEY FOUND! [ password ]

Master Key      : 41 B8 8E 6A 8A DD E7 D1 C0 AE BB 3E E9 A6 EC 06
                  EE F9 08 7A 69 DE EA 23 63 55 9D B6 09 69 7C 5A

Transient Key   : FA DB 76 3D 12 6E E6 A9 00 4D F5 FE CE 04 89 CD
                  CC 5D 5D DD 93 0A 5D F3 03 1B D7 0D 4C A8 14 53
                  8B 32 3E BE FC 0D 42 D0 8B D6 BA E5 11 2A A8 10
                  5D B5 F3 D0 3F 2E 63 61 4F 67 09 55 9D 93 2F 9C

EAPOL HMAC     : CC C4 EA C6 63 DF D0 19 C6 B6 77 E1 78 19 BA 2F
root@kali:~# █

```

Below are the screenshots for cracking the pcap file captured by monitor mode.

```

root@kali: ~
File Edit View Search Terminal Help

root@kali:~# aircrack-ng -w /usr/share/wordlists/fern-wifi/common.txt ~/Desktop/test-instructor-promiscuous.pcap
Opening /root/Desktop/test-instructor-promiscuous.pcap
Read 1821 packets.

# BSSID          ESSID          test-instructor- Encryption
#               ESSID          promiscuous.pcap
1  F4:F2:6D:B2:FA:DA Hack3r          WPA (1 handshake)
2  4A:F8:B3:FD:B5:4B HGL-guest      None (0.0.0.0)
3  48:F8:B3:FD:B5:4A HGL             No data - WEP or WPA
4  C0:A0:BB:EB:0F:D9 shoen lame     WPA (0 handshake)
5  74:44:01:43:C5:D0 The house of unrecognized talent WPA (0 handshake)
6  00:14:51:76:6C:B3 IJGFR-Network No data - WEP or WPA
7  82:C1:DE:71:6D:0A           WEP (1 IVs)
8  09:73:41:70:A3:E4           Unknown
9  C0:A0:BB:8D:0C:D9 shoen lame     No data - WEP or WPA
10 AA:96:54:94:5F:F6           None (0.0.0.0)
11 45:A3:BB:D0:55:37 HGL            No data - WEP or WPA
12 A5:BD:1C:D1:5D:0A           Unknown
13 6F:04:D2:B2:50:7F           Unknown
14 C2:EF:E5:D0:C7:FF           WEP (1 IVs)
15 4D:9D:A4:B4:A6:78           Unknown

```



After selecting 1 as the target network interface, the screenshot below shows that the password has been cracked.

```
root@kali: ~  
File Edit View Search Terminal Help  
Index number of target network ? 1  
Opening /root/Desktop/test-instructor-promiscuous.pcap  
Reading packets, please wait...  
Aircrack-ng 1.2 rc2  
[00:00:00] 72 keys tested (1218.79 k/s)  
KEY FOUND! [ password ]  
  
Master Key      : 41 B8 8E 6A 8A DD E7 D1 C0 AE BB 3E E9 A6 EC 06  
                  EE F9 08 7A 69 DE EA 23 63 55 9D B6 09 69 7C 5A  
  
Transient Key   : 28 D7 4C E4 95 20 C5 99 7D A7 28 1C 66 C0 D2 49  
                  00 B6 EA 86 E7 0A 4D 84 33 C7 3F 67 1D F2 E4 B1  
                  75 9C AF A7 43 77 9C DF BA BC 0B C6 9A 1D 84 02  
                  1E CB 1F 2F EB 5F 5F DB 11 83 65 3B CF 32 99 47  
  
EAPOL HMAC     : A2 DA 1C 51 DF 50 AC 90 57 62 55 67 F3 3A 7B 81  
root@kali:~#
```

Assignments for Lab 6 Part 2

1. Read the lab instructions above and finish all the tasks.
2. Answer the questions in the Introduction section, and justify your answers. Simple yes or no answer will not get any credits.
 - a. What is the difference between Monitor Mode and Promiscuous Mode
 - b. What lessons we learned from this lab about setting the WiFi password?
3. Change your router to a different passphrase, and use the Wireshark and Aircrarch-ng to crack the passphrase. Show screenshots of the result.

Extra Credit (3pt): Send a broadcast de-authentication packet to force clients to reconnect. Then you can capture the four-way handshake.

Happy Hacking!