

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



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 <u>http://www.tplinkwifi.net</u>

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.

			Fengwei
← → C' 🗋 tpli	inkwifi.net		☆ 🛇 ≡
TP-L			reless N Router odel No. TL-WR841N
	1		
	P		
	Log	gin	
	Copyright © 2015 TP-LINK Techno	logies Co., Ltd. All rights reserved.	

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"

TP-LINK	°6		
Status			
Quick Setup	Wireless Settings		
WPS			
Network		[
Wireless	Wireless Network Name:	Hack3r	(Also called the SSID)
- Wireless Settings	Mode:	11bgn mixed	
- Wireless Security	Channel Width:	Auto ᅌ	
- Wireless MAC Filtering	Channel:	6	
- Wireless Advanced			
- Wireless Statistics			
Guest Network		Enable Wireless Router Radio	
DHCP		Enable SSID Broadcast	
Forwarding		Enable WDS Bridging	
Security			
Parental Control			
Access Control		Save	



Step 5: Confugure 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.

TP-LIN	K°		
Status			
Quick Setup	Wireless Security		
WPS			
Network			
Wireless	 Disable Security 		
- Wireless Settings			
- Wireless Security	 WPA/WPA2 - Personal(Recommended) 		
- Wireless MAC Filtering	Version:	Automatic ᅌ	
- Wireless Advanced	Encryption:	AES	
- Wireless Statistics	Wireless Password:	password	
Guest Network		(You can enter ASCII characters	between 8 and 63 or Hexadecimal
DHCP	Group Key Update Period:	0 Seconds	
Forwarding		(Keep it default if you are not sur	e, minimum is 30, 0 means no upda
Security	O WPA/WPA2 - Enterprise		
Parental Control	Version:	Automatic ᅌ	
Access Control	Encryption:	Automatic ᅌ	
Advanced Routing	Radius Server IP:		
Bandwidth Control	Radius Port:	1812 (1-65535, 0 stands for c	lefault port 1812)
IP & MAC Binding	Radius Password:		
Dynamic DNS	Group Key Update Period:	0 (in second, minimu	m is 30, 0 means no update)
IPv6 Support	○ WEP		
System Tools	Туре:	Automatic ᅌ	
Logout	WEP Key Format:	Hexadecimal	
	Key Selected	WEP Key	Кеу Туре
	Key 1: •	WEP Ney	Disabled 🗘
	Key 2:		Disabled ᅌ
	Key 3: 🔿		Disabled ᅌ
	Key 4: 🔿		Disabled ᅌ



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.

• • •	🚄 The Wireshark Network Analyzer	
	k ← → ≝ T 👱 👤 📃 🔍 Q Q 🎹 .	
📕 Apply a display filter <೫/>		Expression +
Welcome to Wireshark		
Open		
/Users/fengwei/Desktop/test1.p	сар (2808 КВ)	
Capture		
using this filter: 📕 Enter a cap	oture filter	•
Ethernet: en0	h_h_h_h_h_h_h_h_h_h_h_h_h_h_h_h_h	
Thunderbolt FireWire: fw0 Thunderbolt Bridge: bridge0		
utun0		
Learn		
User's Guide 🔸 Wiki 🔸 Ques	tions and Answers 🕐 Mailing Lists	
You are running Wireshark 2.0.2	(v2.0.2-0-ga16e22e from master-2.0).	
Ready to load or capture	No Packets	Profile: Default



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.

		Input Output	Options				
Interface	▲ Traffic	Link-layer Header	Promiscuous	Snaplen (B)	Buffer (MB)	Monitor Mode	Capture Filter
Ethernet: en0	l	Ethernet	disabled	default	2	n/a	
Loopback: Io0		BSD loopback	disabled	default	2	n/a	
Thunderbolt 1: en2		Ethernet	disabled	default	2	n/a	
Thunderbolt 2: en3		Ethernet	disabled	default	2	n/a	
Thunderbolt Bridge:	bridge0	Ethernet	disabled	default	2	n/a	
Thunderbolt FireWire	: fw0	Apple IP-over-IEEE 1394	disabled	default	2	n/a	
▶ utun0		BSD loopback	disabled	default	2	n/a	
vmnet1		Ethernet	disabled	default	2	n/a	
vmnet8	۸۸	Ethernet	disabled	default	2	n/a	
Wi-Fi: en1		802.11	disabled	default	2	enabled	
Enable promiscuous m	node on all interfaces						Manage Interfaces

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.



Interface	▲ Traffic	Link-layer Header	Promiscuous	Snaplen (B)	Buffer (MB)	Monitor Mode	Capture Filter		
awdl0		_ Ethernet	enabled	default	2	n/a			
Ethernet: en0		- Ethernet	disabled	default	2	n/a			
gif0		BSD loopback	enabled	default	2	n/a			
Loopback: Io0		BSD loopback	disabled	default	2	n/a			
p2p0		Raw IP	enabled	default	2	n/a			
stf0		_ BSD loopback	enabled	default	2	n/a			
Thunderbolt 1: en2		_ Ethernet	disabled	default	2	n/a			
Thunderbolt 2: en3		_ Ethernet	disabled	default	2	n/a			
Thunderbolt Bridge: bri	dge0	_ Ethernet	disabled	default	2	n/a			
Thunderbolt FireWire: f	w0	_ Apple IP-over-IEEE 1394	disabled	default	2	n/a			
▶ utun0		_ BSD loopback	disabled	default	2	n/a			
▶ utun1		_ BSD loopback	enabled	default	2	n/a			
vmnet1		_ Ethernet	enabled	default	2	n/a			
vmnet8		_ Ethernet	enabled	default	2	n/a			
Wi-Fi: en1		Per-Packet Information	enabled	default	2	disabled			
Enable promiscuous mo	de on all interfaces							Mana	age Interfaces.
Capture filter for selected ir	nterfaces: 📙 Enter a c	apture filter							Compile BPF

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.

	🛃 Capturi	ng from Wi-Fi: en1		
🚺 🗖 🙋 🔳	📑 🍝 🍳 🖏 📓		$ \oplus $	
📘 Apply a display filter < 🕯	€/>			Expression +
No. Time	Source	Destination	Protocol Length	
3073 15.311477	fe80::8634:97ff:feac:b61a	ff02::1:2		Solicit XID: 0x49df32 CID: 00030
3074 15.312063		SenaoNet_16:57:74		Clear-to-send, Flags=
3075 15.312140		SenaoNet_16:57:74		Acknowledgement, Flags=
3076 15.313600	fe80::a2:ed94:1dff:feac:b61a	ff02:0:80:4800::2d		Solicit XID: 0x49df32 CID: 00030
3077 15.346313	5e:8f:e0:ca:07:dc	Broadcast		Beacon frame, SN=2371, FN=0, Fla
3078 15.348764 3079 15.351170	Technico_c2:37:1a ce:03:fa:c2:37:1b	Broadcast Broadcast		Beacon frame, SN=596, FN=0, Flag
3079 15.351170	SenaoNet 16:57:76	Broadcast		Beacon frame, SN=597, FN=0, Flag Beacon frame, SN=1751, FN=0, Flag
3080 15.309074	Senaoner_10:57:76	SenaoNet_16:57:74		Clear-to-send, Flags=
3082 15.407124	Tp-LinkT_b2:fa:da	Broadcast		Beacon frame, SN=1580, FN=0, Fla
3083 15.451011	Technico c2:37:1a	Broadcast	802.11 253	
3084 15.452842	ce:03:fa:c2:37:1b	Broadcast		Beacon frame, SN=599, FN=0, Flag
3085 15.509380	Tp-LinkT_b2:fa:da	Broadcast		Beacon frame, SN=1581, FN=0, Fla
	on wire (2904 bits), 363 bytes captured	(2904 bits) on inter	face Ø	
	esponse, Flags:R			
	s LAN management frame			
	-			
0000 50 08 3a 01 00 1		(Cr.T		
0010 cc 03 fa 72 b4 5 0020 64 00 11 04 00 0		.T.\ C% HO ME-B454.		
0030 08 82 84 8b 96 2				
0040 01 00 30 18 01 0	0 00 0f ac 02 02 00 00 0f ac 040.			
0050 00 0f ac 02 01 0		2		
0060 98 60 2d 1a bd 1 0070 00 00 00 00 00 00 0				
0080 06 08 11 00 00 0				
0090 00 00 00 00 00 0		PJ		
🔘 🎽 Wi-Fi: en1: <live capt<="" td=""><td>ure in progress></td><td></td><td>Packets: 3085 · Di</td><td>splayed: 3085 (100.0%) Profile: Default</td></live>	ure in progress>		Packets: 3085 · Di	splayed: 3085 (100.0%) Profile: Default



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 handsake

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.

• • •						🚄 Wi	-Fi: en1					
	<u>a</u> 💿	01010	🗙 🙆	0	(🔶 🖄	T 🛓		Ð. (
eapol												Expression +
4224 4232	Time 13.051622 13.053079 13.063941 13.072599	Tp-LinkT	_b2:fa:da _b2:fa:da _b2:fa:da :7d:0c				Destination Apple_20 Apple_20 Apple_20 Tp-LinkT	1:7d:0c	Protocol EAPOL EAPOL EAPOL EAPOL	137 217	Info Key (Message Key (Message Key (Message Key (Message	e 1 of 4) e 3 of 4)
► IEEE 8 ► Logics	 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 											
0010 f4 0020 88 0030 00 0040 bc 0050 d7 0060 00 0070 00	02 3a 01 04 d 12 6d b2 fa d 8 02 03 00 5 00 01 3b fd 4 aa 8f 79 42 07 88 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4	a 00 00 f 02 00 3 af f3 a 3f c0 0 00 00 0 00 00	7d 0c f4 1 06 00 aa a 8a 00 10 6 42 ad 00 2 3 c6 10 00 00 00 0 00 00 00 6 63	a 03 0 0 00 0 2 77 0 2 8 1 0 00 0 0 00 0	00 00 00 00 13 e7 f6 01 00 00 00 00	00 00 e4 8c 00 00	V- } ;.C B yB.?. # 0<. c					
0 2	wireshark_pcapng_e	n1_201604011	162628_7xrgbL					Packets: 8459 ·	Displayed: •	4 (0.0%) · [Dropped: 0 (0.0%)	Profile: Default



Step 4: Save the captured traffic

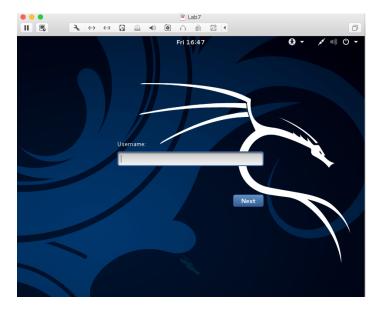
Click File -> Save as option to save the captured traffic to a pcap file. Screenshot below shows the example. The saved pcap file name is: test.pcap

$\bullet \bigcirc \bigcirc \bigcirc$				Wi-Fi: en1		
	1		🖹 🚺 🤇 🔶 🖻	2 🏹 🛃 📃		
eapol		:		Save Capture File As		Expression +
	Time 13.05162	Look in:	/Users/fengwei	0	0 й 🗉 🗉	Message 1 of 4)
4224	13.05307	LOOK IN:	/Osers/lengwei			Message 1 of 4)
4232	13.06394	Comp	Name	Size Kind	Date Modified	Message 3 of 4)
4238	13.07259	-	AndroidStudioProjects	Folder	1/28/16 3:41 PM	Message 4 of 4)
		fengw	ei 📄 Applications	Folder	9/2/15 1:13 PM	
			coreboot.rom	1.0 MB rom File	e 11/24/:44 PM	
			Desktop	Folder	4/1/16 4:28 PM	
			Documents	Folder	3/17/1:02 PM	
			📄 Downloads	Folder	4/1/16 2:24 PM	
	4223: 137		📴 Dropbox	Folder	3/23/16 3:52 PM	
	02.11 Qos		minicom.log	35 bytes log File	12/15/:07 PM	
5	l-Link Co		i Movies	Folder	9/1/15 10:25 AM	
▶ 802.1X	Authent:		📄 Music	Folder	9/3/15 9:32 AM	
			E Pictures	Folder	9/23/15 1:53 PM	
			E Public	Folder	9/1/15 10:25 AM	
			🔤 快盘	Folder	10/9/1:48 AM	
	02 3a 01 f2 6d b2					
	8e 02 03				Save	
	00 01 3b	File name:	test			
	aa 8f 79				Cancel	
	07 88 00 00 00 00	Save as:	Wireshark/tcpdump/ pcap (*.pca	ap *.pcap.gz * cap * cap.gz *.dn	np *.c 🗘 🛛 🗤 🗤	
	00 00 00			the theorem and techings to the	Help	
	00 00 00		Compress with gzip			
			Compress with gzip			
		_				
🔵 🏹 🗤	wireshark pea	nng en1 201604	01162628_7xrgbL	Packets: 9450	Displayed: 4 (0.0%) · Dropp	ed: 0 (0.0%) Profile: Default
	anesnark_pca	plig_ell1_201004		Fackets. 0409	Displayed. 4 (0.0%) * Dioppi	ea. o (0.0%) Frome. Default



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 testinstructor-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
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-instructormonitor.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 E	Edit View Search Termin	nal Help	
op/te Openi	st-instructor-monit		fern-wifi/common.txt ~/Deskt
#	BSSID	ESSID	Encryption
1 2 3 4 5 6	60:FE:20:6C:6D:5A 5E:8F:E0:CA:07:DC 10:86:8C:98:2E:04 5E:8F:E0:90:E6:30 F4:F2:6D:B2:FA:DA 6E:8F:E0:CA:07:DC	ATT896 C^ NDI Hack3r xfinitywifi	No data - WEP or WPA No data - WEP or WPA No data - WEP or WPA No data - WEP or WPA WPA (1 handshake) None (0.0.0.0)
7 8 9 10 11	12:86:8C:95:85:DC 6D:E2:06:E5:7E:9F CE:03:FA:C2:37:1B 1C:87:2C:E4:B8:18 54:BE:E7:F4:BD:D8		No data - WEP or WPA No data - WEP or WPA None (0.0.0.0) WPA (0 handshake) No data - WEP or WPA
12 13 14 15 16	5C:8F:E0:CA:07:DC A0:63:91:83:DE:5F A0:63:91:B7:71:D9 12:86:8C:98:2E:04	DetroitLiving Bill Wi the Science Fi IIMD ?? AbrahamLinksy	No data - WEP or WPA No data - WEP or WPA No data - WEP or WPA None (0.0.0.0) 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.



				гоо	t@k	ali: '	~								•	Θ	\otimes
File Edit View Search	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		B8 88 F9 08															
Transient Key	CC 8B	DB 76 5D 50 32 38 85 F3) DD E BE	93 FC	0A 0D	5D 42	F3 D0	03 8B	1B D6	D7 BA	0D E5	4C 11	A8 2A	14 A8	53 10		
EAPOL HMAC root@kali:~#	: cc	C4 E#	V C6	63	DF	DO	19	C6	B6	77	E1	78	19	BA	2F		

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

		root@kali: ~	- • ×		
File E	dit View Search Termin	al Help			
root@kali:~# aircrack-ng -w /usr/share/wordlists/fern-wifi/common.txt ~/Deskt op/test-instructor-promiscuous.pcap Opening /root/Desktop/test-instructor-promiscuous.pcap Read 1821 packets.					
#	BSSID	ESSID test-instructor-	Encryption		
1 2 3 4 5 6 7 8	74:44:01:43:C5:D0 00:14:51:76:6C:B3 82:C1:DE:71:6D:0A 09:73:41:70:A3:E4	HGL-guest HGL shoen lame The house of unrecognized IJGFR-Network	No data - WEP or WPA WEP (1 IVs) Unknown		
9 10	C0:A0:BB:8D:0C:D9 AA:96:54:94:5F:F6	shoen lame	No data - WEP or WPA None (0.0.0.0)		
11		HGL	No data - WEP or WPA Unknown Unknown WEP (1 IVs) Unknown		



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

root@kali: ~	•	•	8			
File Edit View Search Terminal Help						
Index number of target network ? 1 monitor pcap						
Opening /root/Desktop/test-instructor-promiscuous.pcap Reading packets, please wait						
Aircrack-ng 1.2 rc2 test-instructor-						
[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 Aircrach-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!