

# Information and communication Technology Security ความมั่นคงเทคโนโลยีสารสนเทศและการสื่อสาร

	٠U	
1.นายจิรวัฒน์	สกุลวานิชเจริญ	573021386-8
2.นายพงศธร	กาบจันทร์	573020812-2
3.นางสาวสุภัทธา	เภกะสุต	573020829-5
4.นางสาวเอื้อมเดือน	ฮาดดา	573020835-0
5.นางสาวอรทัย	ประเสริฐโส	573020832-6

ผ้จัดทำ

อาจารย์ที่ปรึกษา รศ.ดร.จักรชัย โสอินทร์

ภาคเรียนที่ 1 ปีการศึกษา 2559 ภาควิชาวิทยาการคอมพิวเตอร์ สาขาเทคโนโลยีสารสนเทศและการสื่อสาร คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น

#### หลักการและเหตุผล

ในปัจจุบันมีการเข้าถึงอินเตอร์เน็ตได้ง่ายมากขึ้น โดยทั่วทุกมุมโลกสามารถใช้อินเตอร์เน็ตในหลาย ด้านแตกต่างกันออกไปทั้งถูกทางและไม่ถูกทาง อินเตอร์เน็ตทำให้เกิดความสะดวกและรวดเร็วมากขึ้นสำหรับ ผู้ใช้งาน อีกทั้งยังมีการพัฒนาซอฟต์แวร์และฮาร์ดแวร์ขึ้นอย่างมากมายที่ใช้เป็นเครื่องมือในหลายๆด้านรวมถึง ในด้านการรักษาความปลอดภัยของระบบ การถูกคุกคาม ซอฟต์แวร์ที่ติดตั้งเป็นระบบรักษาความปลอดภัยมี การเริ่มใช้อย่างแพร่หลายในปัจจุบัน หากใช้ในทางที่ผิดก็อาจจะทำให้เกิดความผิดพลาดและเกิดความเสียหาย ได้ ซึ่งปัจจุบันมีอาชญากรแอบแฝงมากมายอาจจะไล่ตามข้อมูลไปทำสิ่งที่ไม่ดี อย่างเช่น พวกเขามักจะใช้ คอมพิวเตอร์จำนวนมากเพื่อทำให้เว็บไซต์ล่มหรือละเมิดระบบรักษาความปลอดภัยของเว็บไซต์ หรือแม้แต่ดึก จับรหัสของเราเพื่อค้นเอาข้อมูลลับอีกด้วย

#### วัตถุประสงค์

- 1. เพื่อศึกษาวิธีการหรือขั้นตอนการทำงานของโปรแกรม Cain & Abel
- 2. เพื่อศึกษาการโจมตี web Security
- 3. เพื่อตรวจสอบความแข็งแกร่งของรหัสผ่าน
- 4. เพื่อทำการทดสอบการดักจับข้อมูลรหัสผ่านจากเครือข่าย
- 5. เพื่อใช้ในรายวิชา 322376 Information and communication Technology Security

#### งานวิจัยที่เกี่ยวข้อง

#### 1. โปรแกรม : Saf etyPass

ผู้จัดทำ นางสาวทันยา เสมอภาค และคณะ

ที่มา : http://csperson.kku.ac.th/chakchai/images/322376\_2015/g17\_safe\_password.jpg



#### 2. โปรแกรม : KKU Internet Authen

ผู้จัดทำ นายศรัณย์ พงโสภณ และคณะ

ที่มา : http://csperson.kku.ac.th/chakchai/images/322376\_2015/g10\_kku\_authen.jpg



### ขั้นตอนการติดตั้งโปรแกรม Cain & Abel

ทำการดาวน์โหลดโปรแกรม Cain & Abelที่ <u>http://www.oxid.it/cain.html</u>

การติดตั้ง Cain and Abel นั้น จะแบ่งออกเป็น 2 ขั้นตอนด้วยกัน คือ ติดตั้งโปรแกรม Cain and Abel และ ติดตั้ง WinPCAP (จะรวมอยู่ในชุดติดตั้ง Cain and Able อยู่แล้ว) ซึ่งจำเป็นสำหรับการใช้งานในแบบ sniffer เพื่อทำการดักข้อมูลจากเครือข่าย โดยวิธีการติดตั้ง มีดังนี้

 ที่โฟลเดอร์ซึ่งเก็บไฟล์ที่ดาวน์โหลดมา ให้ทำการดับเบิลคลิกไฟล์ CA\_Setup.exe ซึ่งจะได้หน้า ไดอะล็อกดังรูปที่ 1



รูปที่ 1 Cain and Abel Installation

2.ที่หน้าไดอะล็อกดังรูปที่ 1 ให้คลิก Next เพื่อเริ่มทำการติดตั้งโปรแกรม ซึ่งจะได้หน้าไดอะล็อกดังรูปที่ 2



รูปที่ 2 License Agreement

3. ทีหน้าไดอะล็อก License Agreement ดังรูปที่ 2 ให้คลิก next



รูปที่ 3 Select Destination

 ที่หน้าไดอะล็อกดังรูปที่ 3 ให้เลือกตำแหน่งที่จะติดตั้งโปรแกรม (ค่าดีฟอลท์เป็น C:\Program Files\Cain) เสร็จแล้วให้คลิก Next



รูปที่ 4 Ready to Install

5. ที่หน้าไดอะล็อกดังรูปที่ 4 ให้คลิก Next เพื่อทำการติดตั้งโปแกรม รอจนการติดตั้งแล้วเสร็จ ซึ่งจะได้ หน้าไดอะล็อกดังรูปที่ 5 ให้คลิก Finish เพื่อจบการติดตั้งโปรแกรม Cain and Abel



รูปที่ 5 Install Completed

6. จากนั้นระบบจะถามว่าต้องการติดตั้ง WinPcap หรือไม่ ดังไดอะล็อกรูปที่ 6 ให้คลิกปุ่ม Install หาก ต้องการใช้งานแบบการดักจับข้อมูลจากเครือข่าย หากไม่ต้องการให้คลิกปุ่ม Don't Install



รูปที่ 6 WinPcap Installation

7. ที่หน้าไดอะล็อก WinPcap 4.0.1 Setup ดังรูปที่ 7 ให้คลิก Next เพื่อทำการติดตั้ง WinPcap



รูปที่ 7 WinPcap 4.0.1 Setup



8. ที่หน้าไดอะล็อก Setup wizard ดังรูปที่ 8 ให้คลิก Next เพื่อเริ่มทำการติดตั้ง WinPcap

รูปที่ 8 WinPcap Setup wizard

 ที่หน้าไดอะล็อก License Agreement ดังรูปที่ 9 ให้คลิก I Agree เพื่อเริ่มทำการติดตั้ง WinPcap แล้วรอจนการติดตั้งแล้วเสร็จ ซึ่งจะได้หน้าไดอะล็อกดังรูปที่ 10 ให้คลิก Finish เพื่อจบการติดตั้ง โปรแกรม WinPcap



รูปที่ 9 License Agreement



รูปที่ 10 Install Completed

## ขั้นตอนวิธีการใช้โปรแกรม

## ขั้นตอนการใช้เมนู Decode Wireless Password

1. เปิดโปรแกรม Cain & Abel โดยดับเบิลคลิกที่ไอคอนของโปรแกรม ซึ่งจะได้หน้าต่างโปรแกรม

	Table Mile	
💰 Decoders 🔮 Network 📦 Sr	niffer 🥩 Cracker 🔕 Traceroute 💷 CCDU 🐝 Wireless 🔂 Query	
Cached Passwords Protected Storage Cached Passwords Cached Storage Cached Storag	Press the + button on the toolbar to dump the Wireless Passwords	
http://www.oxid.it	Wireless Passwords	li.

2.เลือกไปที่เมนู Wireless Password แทบซ้ายมือ

- <b>-</b>		×
Eile View Configure		
□ ● ● ☆ 職 職 早	+ 3/ 18/ 57 100 100 10 10 10 10 10 10 10 10 10 10 1	_
💰 Decoders 🔮 Network 🗐 S	Sniffer 🥑 Cracker 🞕 Traceroute 🛄 CCDU 🕅 Wireless 🚯 Query	
& Cached Passwords		
Protected Storage LSA Secrets Viridess Passwords ET78/9 Passwords Dialup Passwords Edit Boxes Edit Boxes Enterprise Manager Viridows Vault	Press the + button on the toolbar to dump the Wireless Passwords	
http://www.exid.it		1.

3.คลิกไปที่พื้นที่ว่างด้านขวาแล้วคลิกที่ ปุ่ม add to list

		-	×
Eile View Configure	Tools Help		
😑 🏟 😔 🎪 😹 🐯 📮	🕂 📎 😼 🖳 🕙 🚥 🖼 🖬 🖬 ன 🥵 💋 🔋 🏦		
💰 Decoders 🔮 Network 🗐	Sniffer 🥑 Cracker 🔯 Traceroute 💷 CCDU 😵 Wireless 🚯 Query		
Cached Passwords     Protected Storage     LSA Secrets     Wireless Passwords     El 7/8/9 Passwords     Dialup Passwords     Dialup Passwords     Edit Boxes     Edit Boxes     Credential Manager     Windows Vault	Press the + button on the toolbar to dump the Wireless Passwords		
	St Wireless Passwords		
http://www.oxid.it			- 10

4.หน้าจอจะแสดง SSID และ Password ของWi-Fi ที่เครื่องนี้เคยเข้าใช้

Decoders 🔮 Network 🗐	Sniffer 🥑 Cracker	C Tracero	ute 🛄 CCD	U 🧏 Wireless 🚯	Query	
ached Passwords	Adapter GUID	Descr	Туре	SSID	Password	Hex
Protected Storage LSA Secrets Wireless Passwords IE 7/8/9 Passwords Windows Mail Passwords	(EAA576E3-6748 {EAA576E3-6748 {EAA576E3-6748 {EAA576E3-6748 {EAA576E3-6748 {EAA576E3-6748 {EAA576E3-6748	©oem33.i ©oem33.i ©oem33.i ©oem33.i ©oem33.i ©oem33.i	WPA2-PSK WPA2-PSK WPA2-PSK WPA2-PSK WPA2-PSK WPA2-PSK	Kakhom Mintracafe Picnic Garden Wireless_TP-LINK JIRA2006 JIRA1106	hairyseebear 12341234 picnicgarden2016 043342427 nakkham999 nakkham999	686169727973656562656172 313233431323334 70696346696357617244656632303 303433333432343237 6661668686516D393939 6661668686516D393939
g Dialup Passwords ≣ Edit Boxes ≜ Enterprise Manager ▶ Credential Manager ∦ Windows Vault	(EAA576E3-6748 (EAA576E3-6748 (EAA576E3-6748	Coem33i Coem33i Coem33i	WPA2-PSK WPA2-PSK WPA2-PSK	AumikowA Nutda MoeyłymuaY	12345678 17110113 moey5617	3132333435363738 3137313130013133 6D6F657935363137

## ขั้นตอนการใช้เมนู Crack Dictionary

1.คลิกไปที่ Cracker เมนูบนแทบด้านบน จากนั้นคลิกไปที่ Hash Calculator 📟

- -					
Eile View Con	figure Tools Help				
	8 🛱 🛛 🕇 🔊 👒	1 %4 M 100 E	s 🛯 🖬 🗖 🎖 ն 🚺	¥ IL	
💰 Decoders 🔮 Network	: 🟟 Sniffer 🥑 Crack	er 🔯 Traceroute	e 🛄 CCDU 🦹 Wireless 🚯	Query	
Cracker A	MD5 Hash	Password	Note		
- 🏨 LM & NTLM Hast					
- MTLMv2 Hashes (					
- MS-Cache Hasher					
- A PWL files (0)					
- Cisco IOS-MD5 H					
Cisco PIX-MD5 H.					
- APOP-MD5 Hash					
- CRAM-MD5 Hash					
- OSPF-MD5 Hashe					
- + RIPv2+MD5 Hashe					
- VRRP-HMAC Has					
VINC-SUES (U)					
- MD2 Hashes (0)					
nd MDS Hashes (0)					
Se Child a 1 Marchar (7)					
181 SHA-2 Harber (7)					
R RIDEMD, 140 Hark					
-85 KerbS PreAuth Ha Y					
< >	MD5 Hashes				
http://www.oxid.it					h.

2.ใส่รหัสแบบง่ายๆ จากนั้นจะถอดรหัสออกมา Copy Hash ของ Type MD5 แล้วกด Calculate

- <u>-</u>		
Eile View Configure Tools	fash Calculator	×
😑 💩 😞 🎪 識 體 📮 🕇	Text to hash	1
💰 Decoders 🔮 Network 📦 Sniffer	password	
Cracker ^ MD5 Hash	C Bytes to hash (HEX)	1
- 🉀 LM & NTLM Hast		
- MTLMv2 Hashes (		
- MS-Cache Hashe	Type Hash	
-& PWL files (0)	MD 2 E02001A00FEE 2012EERE FFEREERED	
- Cisco IOS-MD5 H	MD4 8A9D093F14F8701DF177328288182C74	
Cisco PIX-MD5 H.	MD5 SF4DICC085AA765DG1D8327DE8882CF98	
- APOP-MD5 Hash	SHA-2 (256) 56848980A28047151D0E56F8DC6292773603D0D6AA88DD62A11EF721D1542C	
- CRAM-MD5 Hash	SHA-2 (394) A98648A8D0ACA91A598D8877618421D4F28838290D3A758A0F21F28E8C4558	
- OSPF-MD5 Hashe	[SHA-2 (S12) B105P3888C244E882441317E0060618850080009838EP0185E07394C706A88E [RIPEMD.150 2006E855884750A78966E263426C6380.824EE31	
- IPv2-MD5 Hashe	LM E52CAC6741949422	
- VRRP-HMAC Has	NT 8846F7EAEE9F8117AD068DD83087586C	
- VNC-3DES (0)	MySQLSHA1 2470C0C06DEE42FD16188B99005ADCA2EC9D1E19	
- 2 MD2 Hashes (0)	Cisco PK NuLKvvWGg.x9HEKD	
MD4 Hashes (0)	Bate64 cGF2c3dvomQ+	
		-
B DIDEND 160 Hoch	< > >	
25 KarbS Bradath Mase	Calculate Cancel	1
MD5 H	Calculate Cancel	
http://www.prid.b		-
nap://www.coetic		le la

3.จากนั้นคลิกขวาตรงพื้นที่ว่าง และเลือก Add to list

acoder: D Network	la 🛨 🔤 🛛 🐨	Traceroude		• all	
acker A	MD5 Hash	Password	Note		
LM & NTLM Hast	meana	Passiona	Inoce		
NTLMv2 Hashes (					
MS-Cache Hasher					
PWL files (0)		Dictio	onary Attack		
Cisco IOS-MD5 H		Brute	-Force Attack		
Cisco PIX-MD5 H.		Crypt	tanalysis Attack via RainbowTables		
APOP-MD5 Hash-					
CRAM-MD5 Hash		Raint	bowcrack-Unline	2	
OSPF-MD5 Hashe		Activ	eSync	>	
RIPv2-MD5 Hashe					
VRRP-HMAC Has		Selec	t All		
VNC-3DES (0)		Note			
MD2 Hashes (0)		T			
MD4 Hashes (0)		Test p	password		
MD5 Hashes (0)		Add	to list	Insert	
SHA-1 Hashes (0)		Remo	ové.	Delete	
SHA-2 Hashes (0)		Picture 2			
RIPEMD-160 Hark		Kema	ove All		

4.วางรหัสที่เรา Copy มา แล้วกด OK

Decoders 🔮 Network	🔹 🟟 Sniffer 🥑 Cr	acker 🙋 Traceroute	🛄 CCDU 🦹 Wireless 🛙	Query	
Cracker ^	MD5 Hash	Password	Note		
LM & NTLM Hast					
NTLMv2 Hashes (					
MS-Cache Hashe					
Circo IOS MDS H					
CISCO IUS-MUS H	-	MD5 H	lash (in HEX)	×	
ADOD, MDS Harb		les un			
CRAM-MDS Hash		5F4L	CC385AA765D61D8327DE8882CF5	134	
OSPE-MD5 Hashe			ОК	Cancel	
RIPv2-MD5 Hashe		1.0			
VRRP-HMAC Has					
VNC-3DES (0)					
MD2 Hashes (0)					
d MD4 Hashes (0)					
d MD5 Hashes (0)					
SHA-1 Hashes (0)					
SHA-2 Hashes (0)					

5.หน้าจอจะแสดง รหัสที่ช่องMD5 Hash

- 					
Eile Yiew Cor	nfigure Tools <u>H</u> elp				
🔄 🏟 😣 🛤 🖩	* 📮 🕇 🗑 😼	P. 🕙 🚥 🔛	s 🖬 🖬 🚍 🥞 💋	1 90	
& Decoders 🔮 Network	k 🕼 Sniffer 🥑 Cracker	C Traceroute	CCDU 😵 Wireless	D Query	
Cracker A	MD5 Hash	Password	Note		
📲 LM & NTLM Hast	¥ 5F4DCC385AA765D61				
- MTLMv2 Hashes (					
MS-Cache Hashe					
PWL files (0)					
Cisco IOS-MD5 H					
Cisco PIX-MD5 H.					
APOP-MD5 Hash					
- CRAM-MD5 Hash					
- 🕂 OSPF-MD5 Hashe					
- 🕂 RIPv2-MD5 Hashe					
- VRRP-HMAC Has					
- K VNC-3DES (0)					
- MD2 Hashes (0)					
- MD4 Hashes (0)					
-nd MD5 Hashes (1)					
-See SHA-1 Hashes (0)					
-Sta SHA-2 Hashes (0)					
- B RIPEMD-160 Hash					
KerbS PreAuth Ha ~	MD5 Hashes				
http://www.coid.it					

6.คลิกขวา แล้วเลือก Dictionary Attack

oders 🔮 Networ	k 🖄 Sniffer 🥑 🤇	Cracker 🙋 Tracerou	te 🛄 CCDU 🚀 Wireless 🛙	D Query	
ker A	MD5 Hash	Password	Note		
M & NTLM Hast TLMv2 Hashes (	X 5F4DCC385A476	Dictionary Attack			
IS-Cache Hashe: WL files (0) isco IOS-MD5 H		Brute-Force Attack Cryptanalysis Attack	via RainbowTables		
ISCO PIX-MD5 H		Rainbowcrack-Onlin	e >		
RAM-MD5 Hash		ActiveSync	>		
Pv2-MD5 Hashe RP-HMAC Has		Select All Note			
VC-3DES (0) D2 Hashes (0)		Test password			
D4 Hashes (0)		Add to list	Insert		
D5 Hashes (1) IA-1 Hashes (0)		Remove All	Delete		

## 7.หน้าจอจะแสดงแบบนี้

- <b>-</b>	Dictionary Attack	×	
Eile View Configure	Dictionary		
- + + 084 084 FR	File	Position	
	E:\Program Files (x96)\Cain\Wor	dists\Wordlist.bt 2026488	
💰 Decoders 🔮 Network 🗐 Sr			
Cracker ^ MDS H			
HIM & NTLM Hast X 5E4D			
- MTLMv2 Hashes (	Key Bate	Options	
MS-Cache Hashe		At Is (Pattword)	
- Reversion PWL files (0)		Reverse (PASSWORD - DROWSSAP)	
Cisco IOS-MD5 H	Dictionary Position	Double (Pass - PassPass)	
Cisco PIX-MD5 H.		Lowercase (PASSWORD - password)	
- D APOP-MDS Hash		Uppercase (Password - PASSWORD)	
CRAM-MD5 Hash	Current password	Num. sub. perms (Pass Mass Pabs P455 P455)	
- OSPF-MD5 Hashe		Two numbers Hubrid Baste (Pass0)	
- RIPv2-MD5 Hashe	L		
VRRP-HMAC Has	I have at the MER 1		
ad MD2 Hockey (0)	Press the Start button	to begin dictionary attack	
ad MOA Hashes (0)			
ed MDS Hashes (1)			
SHA-1 Hashes (0)			
SHA-2 Hashes (0)			
B. RIPEMD-160 Hash			
- C KerbS PreAuth Ha ~			
< ME			
http://www.exid.it		Start Exit	4

8.คลิกขวา แล้วเลือก Reset initial file position

- <b>1</b>	C	Dictionary Attack		>	×	
Elle View Cont	figure T	Dictionary File	Position		]	
Decoders SNR BBS SR	inter se	C:\Program Files (x86)\Cain\Wordlists\Wordlist.bt	2026488	Add to list	Insert	
Carden .	A HOLE IL			Change initial file position	=	
HIM & NTIM Hast	MUS Ha	1		Reset initial file position	-	
- M NTLMv2 Hashes (	A 36404	Key Rate	Options	Reset all initial file positions		
- MS-Cache Hashe: - 👶 PWL files (0) - 🏧 Cisco IOS-MD5 H		Dictionary Position	As Is (Passw Reverse (PA Double (Pas	Remove from list Remove All		
Cisco PIX-MD5 H. APOP-MD5 Hash CRAM-MD5 Hash CRAM-MD5 Hash CRAM-MD5 Hashe RIPv2-MD5 Hashe		Current password	Lowercase (PA     Uppercase (PA     Uppercase (Pai     Num. sub. perm     Case perms (Pa     Two numbers H	SSWORD - password) ssword - PASSWORD) is (Pass.P4ss.Pa5sP45sP455) iss.pAss.pa5sPa5sPASS) lybrid Brute (Pass0Pass99)		
VRRP-HMAC Has     VRRP-HMAC Has     VNC-3DES (0)     VNC-3DES (0)     VMC-4DES (0)	ngi MD	1 hashes of type MD5 loaded Press the Start button to begin did	tionary att	ack		
http://www.cxid.it				Start Exit		h.

## 9.จากนั้นกดปุ่ม Start

-	Dictionary Attack	×	
File View Configure	Dictionary		
	File	Position	
Bo S Main 2007 2007 2007 2007 2007 2007 2007 200	C:\Program Files (x86)\Cain\Wordlists\Wordlist bit		
- BL LM & NTLM Hast X 5F4 - B NTLMv2 Hashes ( - B MS-Cache Hashe	D( Key Rate 2257950 Patt/Sec	Options	
- Reversion PWL files (0)	Dictionary Position	Reverse (PASSWORD - DROWSSAP)	
Cisco PIX-MD5 H.	502222 ( 15%)	Lowercase (PASSWORD - password)	
CRAM-MD5 Hash	Current password	Uppercase (Password - PASSWORD)  Volume sub. perms (Pass, PAss, Pa5s,, PA5s,, PA5s) Case perms (Pass, pAss, paSs,, PASs,, PASs)	
- RIPv2-MD5 Hashe	cheesemongerly	V Two numbers Hybrid Brute (Pass0Pass99)	
VNC-3DES (0)			
-nd MD4 Hashes (0) -nd MD5 Hashes (1)			
- State SHA-1 Hashes (0) - State SHA-2 Hashes (0) B PIDENAD, 160 March			
C KerbS PreAuth Ha V	0		
http://www.coid.it		Stop Exit	h.

10.เมื่อโหลดเสร็จโปรแกรมจะถอดรหัสออกมาเป็นรหัสที่เราหรอก

- <b>1</b>	(	Dictionary Attack		×	
Elle View Con	figure T	Dictionary			
		File	Position		
🗍 🛥 🔊 😌 🖄 🔠 🖫	8 🛱 🛛	C:\Program Files (x86)\Cain\Wordlists\Wordlist.txt	2026498		
💰 Decoders 🔮 Network	: 📦 Sn				
Cracker A	MD5 Ha				
- 😹 LM & NTLM Hast	¥ 5F4D0	J			
- 🙀 NTLMv2 Hashes (		Key Rate	ptions		
MS-Cache Hashe		5	As Is (Password)		
- 😤 PWL files (0)			Reverse (PASSW0	ORD - DROWSSAP1	
Cisco IOS-MD5 H		Unchonary Position	Double (Pass - Pas	::Pass)	
Cisco PIX-MD5 H.		5	Lowercase (PASS)	w/ORD - password)	
- APOP-MD5 Hash			Uppercase (Passw	ord - PASSWORD)	
- CRAM-MD5 Hash		- Constanting	Num. sub. perms (F	Pass,P4ss,Pa5s,P45sP455)	
- OSPF-MD5 Hashe		Cutters password	Case perms (Pass.)	pAss,paSs,PaSsPASS)	
- RIPv2-MD5 Hashe		P I I I I I I I I I I I I I I I I I I I	<ul> <li>Two numbers Hybr</li> </ul>	nd Brute (Pass0Pass99)	-
- VRRP-HMAC Has		[			
- K VNC-3DES (0)		Plaintext of 5F4DCC3B5AA765D61D8327E	EB882CF99 is	password	
		Attack stopped!			
- MD4 Hashes (0)		I OL I Mashes Cracked			
-nd MD5 Hashes (1)					
-SHA-1 Hashes (0)					
-Sta SHA-2 Hashes (0)					
- RIPEMD-160 Hast					
< KerbS PreAuth Ha v < >	ng MD				
http://www.oxid.it				Start Exit	h.

### ขั้นตอนการใช้เมนู Crack Brute Foce

1.คลิกไปที่ Cracker เมนูบนแทบด้านบน จากนั้นคลิกไปที่ Hash Calculator 📟

· 🗾	From Tech Mile				
	₩ 📮 🛛 🕇 🕲   😹	P. 🕙 📼 B	9 🖻 🖻 🚭 💖 💋	0 ? İ	
💰 Decoders 🔮 Network	k 🗐 Sniffer 🥑 Cracker	C Tracerout	e 🛄 CCDU 🦹 Wireles	s 🚯 Query	
🕑 Cracker 🛛 🔺	MD5 Hash	Password	Note		
CRAM-MDS Hashe  CRAM-MDS HASHABANA-CRAM-MDS	\$45F4DCC385AA765D61	password			
P DIDEA ID ACOLIA					
KiPEMD-160 Hash	nd MD5 Hashes				
http://www.oxid.it					

2.ใส่รหัสแบบง่ายๆ จากนั้นจะถอดรหัสออกมา Copy Hash ของ Type MD5 แล้วกด Calculate

🔄 🏟 😔 📩 🎆 🖁	8 📮 🛛 🕇	Test to hash		^	
& Decoders 🔮 Network	k 😰 Sniffer	onaja			
Cracker  Cracker  LM & NTLM Hast  MS-Cache Hashes  MS-Cache Hashes	MD5 Hash	C Bytes to has	Hash	- ^	
VWL hites (0)     Cisco IOS-MD5 H     Cisco IOS-MD5 H     Cisco PIX-MD5 Hash     OSPF-MD5 Hash     OSPF-MD5 Hash     VRP-MD5 Hash     VRP-MD5 Hash     VRRP-HMAC Has     VMC-30E5 (0)     MD2 Hashes (0)     MD4 Hashes (0)     MD5 Hashes (1)     SHA-1 Hashes (0)		MD2 MD4 MD5 SH4-1 SH4-2 (384) SH4-2 (384) SH4-2 (384) SH4-2 (384) SH4-2 (384) SH4-2 (384) SH4-2 (384) My50L323 My50L323 My50L323 My50L324 My50L323 My50L5H41 Girco PtX VNC Hath Bate64	06395FC470D67E300A8564830C88F2CA FA7237871CD30E731847AC0E38F300A 6500587E40571A557A0076X556E00C408 8051AC87785716FD7AE5FAE84068F314237F558848 D27C3002693915471C939312CDD3F238829703DC371C9A0840A901068CA0A05291E8E1 46803530018D31537481C883A0D5A2AA71489459755ED0D275ED38EC3345A78 8E7581A265300287756553C2856F8CC28895859C 884464E3364FD350 D3AD80894F2951C3087A320FFDE5838 44030531F841C2528C024062E7028975868ACA3C RHbwLUWA2LPISK 6493316534E8E830 b25hamE =	×	
Kerb5 PreAuth Ha v	MD5 H	<	Calculate Cancel		

3.จากนั้นคลิกขวาตรงพื้นที่ว่าง และเลือก Add to list

	방 및 🕈 🕑 🕺	Traceroute	E M E E CCDU	🕑 😵 🔟	
acker ^	MD5 Hash	Password	Note		
LM & NTLM Hast	SF4DCC385AA765D61	password			
NTLMv2 Hashes (	Dict	ionany Attack			
PWL files (0)	Red	e Energe Attack			
Cisco IOS-MD5 H	brut	e-Porce Attack			
Cisco PIX-MD5 H.	Cyr	stanalysis Attack v	a Kainbow lables		
APOP-MD5 Hash	Rain	bowcrack-Online		>	
CRAM-MD5 Hash					
OSPF-MD5 Hashe	Acti	vesync		2	
RIPv2-MD5 Hashe	Sele	ct All			
VRRP-HMAC Has	Not	e			
VNC-3DES (0)					
MD2 Hashes (0)	Test	password			
MD4 Hashes (0)	Add	to list	Insert		
MUS Hashes (1)	Rem	10108	Delete		
SHA-1 Hashes (0)	Page 1	A11	D'DEN		
DIDENTE HOSINES (V)	Nerr	IOVE AII			

### 4.วางรหัสที่เรา Copy มา แล้วกด OK

a na 😔 💀 🕅 🕅 🕅	19 🖳 🕂 🕹 😼 🔤	P. 9 📼 🖻	
Cracker	MDS Hack	Parcounted	Mate
LM & NTLM Hast NTLMv2 Hashes ( MS-Cache Hashe	SF4DCC3B5AA765D61	password	THE
Cisco IOS-MD5 H Cisco PIX-MD5 H		MD5 H	Hash (in HEX) X
APOP-MD5 Hash     CRAM-MD5 Hash     OSPF-MD5 Hash		[364D	IDF9CE4C601A96FA030C2C98ECD408
RIPv2-MD5 Hashe VRRP-HMAC Has			
MD2 Hashes (0) MD2 Hashes (0)			
MD5 Hashes (1) SHA-1 Hashes (0)			
SHA-2 Hashes (0)			

5.คลิกขวา แล้วเลือก Brute-Force Attack

File Yiew Con	figure Tools	s Help ③	ute 🚾 CCDU 🔭 Wire	S 👔 🥲	L.	
Cracker A	MD5 Hash	Password	Note			
🙀 LM & NTLM Hast	SF4DCC3	85AA765D61 password				
MTLMv2 Hashes (     MS-Cache Hashes     PWI Filer (0)	X 364DF	Dictionary Attack Brute-Force Attack				
Cisco IOS-MD5 H		Cryptanalysis Attack via I	RainbowTables			
APOP-MD5 Hash		Rainbowcrack-Online	3			
CRAM-MD5 Hash     OSPF-MD5 Hashe		ActiveSync	3			
RIPv2-MD5 Hashe     VRRP-HMAC Has		Select All Note				
MD2 Hashes (0)	-	Test password		-		
MD4 Hashes (0) MD5 Hashes (2) Sta SHA-1 Hashes (0) Sta SHA-2 Hashes (0)		Add to list Remove Remove All	Insert Delete			
- B RIPEMD-160 Hash - C KerbS PreAuth Ha ~	MD5 H	lashes		-		

### 6.หน้าจอจะแสดงผลแบบนี้

🔹 😔 號 🎆 🖩	8 📮 🛛 <sup>6</sup>	irute-Force Attack		×	
Decoders 🔮 Network racker ^ LM & NTLM Hast NTLMv2 Hashes (	MD5 Ha SF4D0 X 364DF	Charset  C Predefined abcdefghijk/mnopgrtuwwge0123456789  C Duttom	_	Password length Min 1 Max 16 Start from	
MS-Cache Hashe: PWL files (0) Cisco IOS-MDS H Cisco PIX-MD5 H & APOP-MD5 Hash CRAM-MD5 Hash OSPF-MD5 Hashe		Keyspace 8.1860514273734411E+024 Key Rate	Current password		
RIPv2-MD5 Hashe VRRP-HMAC Has VNC-3DES (0) MD2 Hashes (0) MD4 Hashes (0) MD5 Hashes (2) SHA 1 Hashes (0)		1 hashes of type MDS loaded Press the Start button to begin	in brute-force attack		
SHA-1 Hashes (U) SHA-2 Hashes (U) RIPEMD-160 Hash Kerb5 PreAuth Ha		1		Start Exit	

## 7.จากนั้นกดปุ่ม Start

🔄 🏟 😔 📩 🎆 🖩	¥ 📮 🛛	Brute-Force Attack		×	
Decoders Vetwork	MD5 Ha ND5 Ha SF4D0 X 364DF	Charset C Predefined abcdelghijklmnopgstuwngz0123456789 C Custom	<u>×</u>	Password length Min 1	
Cisco IOS-MD5 H Cisco IOS-MD5 H Cisco PIX-MD5 H APOP-MD5 Hash CSPF-MD5 Hash CSPF-MD5 Hash CSPF-MD5 Hash VRRP-HMAC Has VRC-3DE5 (0) MD2 Hashes (0) MD4 Hashe		Keyspace 8.1860514273734411E+024 Key Rate	Current password		
S RIPEMD-160 Hash S KerbS PreAuth Ha ∨ >	ngd MD5	nasnes	L	Stop Exit	

8.เมื่อโหลดเสร็จโปรแกรมจะถอดรหัสออกมาเป็นรหัสที่เราหรอก

	8 🖭   <sup>8</sup>	rute-Force Attack		×	
Cracker	MD5 Ha P SF4D0 X 364DF	Charset Predefined abcdefghijktmnopgrstuwweje0123496789 C Dustom		Password length Min 5 ÷ Max 16 ÷	
PWL files (0)				onaja	
Cisco IOS-MD5 H Cisco PIX-MD5 H APOP-MD5 Hash CRAM-MD5 Hash		Keyspace 8.1960514273734411E+024 Key Rate	Current password		
RIPv2-MD5 Hashe     VRRP-HMAC Has     VNC-3DES (0)     MD2 Hashes (0)     MD4 Hashes (0)		Plaintext of 364DF9CE4C601A96FA0 Attack stopped! 1 of 1 hashes cracked	3DC2C98ECD4DB is beam	8	
MD5 Hashes (2) Sea SHA-1 Hashes (0)					
SHA-2 Hashes (0)		1		9 w   6 w	
151 KerbS Breduth Haw				Star Ext	

## ขั้นตอนการใช้เมนู Wireless

1.คลิกไปที่ Wireless เมนูบนแทบด้านบน

-									
Decoders ♀ Network ⊯ Sniffer	Cracker	. 🕙 🚾 🖼 🖗		8 🔯 🛛 🚯	Query				
Microsoft									
\Device\NPF_{4E6519D4-7205-4F43-BC1A-0	F1C76804E92}							• A	ctive Scan
AirPcap Driver version: not installed Current channet	BSSID	Last seen	Vendor	Signal	SSID	Enc	Mode	Channel	Rates (Mbps)
Lock on channel	1								
Capture WEP IVs to dump ivs file Analyze Delete Save As									
VEP Injection TxRate (Mbps)									
VPA-PSK Authe 7 Send to Cracker									
://www.cxid.it	<								>

2.จากนั้นเลือก Microsoft ไหนก็ได้ แล้วจากปุ่ม Active Scan

Image: Sever Cigningulare Tools	Ela Vian Configura Toole	No.		
Decoders          Network	· · · · · · · · · · · · · · · ·			
UbeviceVNFF_(4E65190.4-7205-4F43.8C1A.0F1C76804E92)	, Decoders 🔮 Network 🟟 Sniffer	🧭 Cracker 🧟 Traceroute 🛄 CCDU 💱 Wireless 🚯 Query		
Werker VIFF (4E65130.4-7205-4F43.8C1A.0F1C76804E32)     hannel     Rates (Mbp       Werker VIFF (22894248.CE8C-48EE 8291-C20506FDF51F)     hannel     Rates (Mbp       Capture WEP (Vs to dump ivs file	Device/NPF {4E6519D4-7205-4F43-8C1A	0F1C76804E92)	Ac	tive Scan
OverviceVIPF     (EAACOTIE F92842440_45830EC61500)     Phannel     Rates (Mbp)       OverviceVIPF     (22894248_CE8C_48EE 63291-C20506FDF51F)     Phannel     Rates (Mbp)       Capture WEP IVs to dump ivs file	Device/NPF_(4E6519D4-7205-4F43-8C1A	OF1C76804E92)		· ·
Lock on channel  Capture WEP IVs to dump ivs IRe  Analyze Delete Save As WEP Injection ARP Requests 6 WPA-PSK Auths F Send to Cracker  <	Device/NPF_IEAA5/2E38748-4A38-8E06 'Device/NPF_I87A80718-F938-4888-8675 'Device'NPF_(2289A248-CE9C-48EE-8291 Content Content Conten	15004254024E5) ES96D156C16D) -C2D506FDF51F)	Channel	Rates (Mbps)
Z Capture WEP IVs to dump, ivs file       Analyze       Delete       Save As       WEP Injection       TxR ale (Mbps)       6       WPA/PSK Auths       WPA/PSK Auths	Lock on channel	1		
VEP Injection TxRate (Mbps) ARP Requests 6 v VPA-PSK Auths 7 Send to Cracker	Capture WEP IVs to dump.ivs file			
VPA-PSK Autha	VEP Injection TxRate (Mbps)			
<	WPA-PSK Auths			
		<	_	>
://www.cxid.it	c//www.coid.it		-	

a 的 谷 統 謝 院 中 二十 1 Decoders 文 Network 的 Sniffer i ficrosoft Device/NPF(EAA576E 3-6748-4A38-8E-06-13	Cracker 🔐 Tr	) 🖾 🖼 🚾 (	ED 🛛 😵	Vireless 🚯	Image: Contract of the second seco			-	Stop
Li/Pcao			,						
invertiers not installed	BSSID	Last seen	Vendor	Signal	SSID	Enc	Mode	Channel	Rates (Mbp
ment channel	& DCSFDBFFCF	27/11/2016 - 23		-44 dBm	kku-wifi	No	Infrastructure	1 (2412000	1, 2, 5, 11,
	& DCSFDBFFCF	27/11/2016 - 23		-54 dBm	kku-wifi-s	Yes	Infrastructure	1 (2412000	1, 2, 5, 11,
ock on channel	0 DC9FD87088	27/11/2016 - 23		-18 dBm	kku-wifi	No	Infrastructure	1 (2412000	1, 2, 5, 11,
Υ	& DC9FDBFFCF	27/11/2016 - 23		-48 dBm	eduroam	Yes	Infrastructure	1 (2412000	1, 2, 5, 11,
-	0 DC9FD87088	27/11/2016 - 23		-18 dBm	eduroam	Yes	Infrastructure	1 (2412000	1, 2, 5, 11,
Capture WEP IVs to dump ivs file	& DC9FD87088	27/11/2016 - 23		-20 dBm	kku-wifi-s	Yes	Infrastructure	1 (2412000	1.2.5.11.
	00F288088500	27/11/2016 - 23		-56 dBm	.@ TRUEWIFI	No	Infrastructure	1 (2412000	12, 18, 24,
	& DCSFDBFFCE	27/11/2016 - 23		0 dBm	kku-wifi	No	Infrastructure	6 (2437000	1, 2, 5, 11,
Analyze Delete Save As	& DCSFDBFFCE	27/11/2016 - 23		0 dBm	eduroam	Yes	Infrastructure	6 (2437000	1.2.5.11.
	\$ 58AC78EEB294	27/11/2016 - 23		-66 dBm	kku-wifi-s	Yes	Infrastructure	6 (2437000	12, 18, 24,
/EP Injection TxRate (Mbps)	A DCSFDBFFCE	27/11/2016 - 23		-44 dBm	kku-wifi	No	Infrastructure	11 (246200	1.2.5.11.
ARP Requests 6	& DCSFDBFFCE	27/11/2016 - 23		-44 dBm	eduroam	Yes	Infrastructure	11 (245200	1, 2, 5, 11,
	& DCSFDBFFCE	27/11/2016 - 23		-44 dBm	kku-wifi-s	Yes	Infrastructure	11 (246200	1, 2, 5, 11,
/PA/PSK.Auths	A OOFEC8EFE682	27/11/2016 - 23		-84 dBm	ICT free WIFI by	No	Infrastructure	11 (246200	12, 18, 24,
Send to Cracker	▲ 58AC78C78485	27/11/2016 - 23		-92 dBm	eduroam	Yes	Infrastructure	11 (246200	12, 18, 24,

3.เมื่อกดปุ่ม Active Scan หน้าจอจะแสดงชื่อWi-Fi ที่ใช้งานอยู่ปัจจุบัน

## ขั้นตอนการใช้เมนู Sniffer

1.เลือกที่เมนู Sniffer

aíŋ									
File	View Configure	Tools Help		1.5					
🖻 🏟 😔	****************	+ 🗑 😼 🗞	5) 🔤 🔤 🚾 🧰	8 💈 🚺	<b>?</b>   <b>I</b>	1			 
& Decoders	🔮 Network 🔹	Sniffer 🥑 Cracker 🧔	Traceroute 🛄 CCDU 🖏	Wireless 🚯	Query				 
IP address	MAC address	OUI fingerprint	Host name	B B	. B8	Gr N	10 M1	M3	
- 	400 At 0	(A)	10				_		
B Hosts	APK T Routing	🦄 Passwords 🦚 V	410						
http://www.oxid	3.10								

2.คลิกไปที่ Configure แทบด้านบน เลือก IP เครื่องเรา จากนั้นกด OK

File	View Configure	Tools Help	Configuration Dialog X Challenge Spooling   Filters and ports   HTTP Fields	
Decoders	Network      Nork     Network      Nork     Network      Nork     Nork	Sniffer 💕 Cracker	Mill         Mill <th< th=""><th></th></th<>	
Hosts 🚱	APR 🕂 Routing	🖒 Passwords 🛿	VDevice VNPF_(EAA57563-6748-4A38-8E06-19DAF2FACAE5)       WARNING III Only ethemet adapters supported       Options       Start Suffer on startup       Don't use Promiscuous mode       Start APR on startup       OK     Cancel       Apply       Help	

Decoders 🔮 Networ	k 🗐 Sniffer 🥑 Cracker 😋	Tracero Taront	
IP address MAC ad	dress OUI fingerprint	F       All hosts in my subnet         C       Range         Form       132.168.1.1         To       132.168.1.254         Promiscuour-Mode Scanner         ARP Test (Broadcast 31-bk)         ARP Test (Broadcast 16-bk)         ARP Test (Broadcast 16-bk)         ARP Test (Broadcast 20-bk)         ARP Test (Broadcast 20-bk)         ARP Test (Broadcast 20-coup 0)         ARP Test (Multicast group 0)         ARP Test (Multicast group 3)         AIR Tests         OK	

3.จากนั้นคลิกปุ่ม Start/Stop Sniffer และ ปุ่ม Add to list แล้วกด OK

4.หน้าจอจะแสดง IP ที่ใช้งานอยู่

Decoders	Network	iniffer 🥑 Cracker 😨 T	raceroute 🛄 CCDU 🏹	Wireless	Query				
address	MAC address	OUI fingerprint	Host name	B B	88	Gr	M0 I	M1 M3	
.168.1.1	9CE3743AD77D								
.168.1.33	80EA9638FD20	Apple							
.168.1.35	0071CC2E8DC1								
.168.1.37	606DC7CDC7CD								

5.เลือก APR ที่แทบด้านล่าง

	Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address	1
R-Cert (12)								
R-SSH-1 (0)								
R-HTTPS (0)								
R-RDP (0)								
R-FTPS (0)								
R-POP3S (0) R-IMAPS (0)	Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address	
R-LDAPS (0)								
R-SIPS (0)								

6.กดปุ่ม Add to list แล้วเลือก IP เครื่องที่จะดักจับด้านซ้าย แล้วเลือก IP เครื่องเราด้านขวา แล้วกด OK

APR         APR-Cert (12)           APR         APR-Cert (12)           APR-SSH-1 (0)         APR-SSH-2 (0)	Stat	APR enables yo directions. If a s machine has no all other hosts o	Routing ou to hijack IP traffic be elected host has routing it the same performance in your LAN.	WAF ween the selected h g capabilities WAN to of a router you could	INING III out on the left list and affic will be intercepte d cause DoS if you se	all selected hosts on th d as well. Please note it t APR between your Dr	e right list in both hat since your efault Gateway and	
을 APR-ProxyHTTPS (0) 응용 APR-RDP (0) 음 APR-FTPS (0) 음 APR-POP35 (0) 음 APR-IMAPS (0) 음 APR-LDAPS (0) 음 APR-LDAPS (0)	Stat	IP address 192 168.1.1 192 168.1.33 192 168.1.35 192 168.1.37	MAC 9CE3743AD77D 80EA9638FD20 0071CC2E80C1 606DC7CDC7CD	Hostname	IP address 192,168,1.35 192,168,1.33 192,168,1.1	MAC 0071CC2E80C1 80EA9638F020 9CE3743A0770	Hostname	
	0	<		>	<	OK	> Cancel	

7.หน้าจอจะแสดงจากทำงานของ IP เครื่องที่เราเลือก

ders 🔮 Networ	Status	Cracker     Q     T     IP address	MAC address	Packets ->	<- Packets	MAC address	IP address	
R-Cert (12) R-DNS	Aldle	192.168.1.37	606DC7CDC7CD			0071CC2E8DC1	192.168.1.35	
R-SSH-1 (0)	a idle	192.168.1.37	606DC7CDC7CD			9CE3743AD77D	192.168.1.33	
R-ProxyHTTPS (0)								
R-RDP (0) R-FTPS (0)								
R-POP3S (0) R-IMAPS (0)	Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address	
R-LDAPS (0)								
n-aira (u)								

8.กดปุ่ม Start/Stop APR จะแสดงการทำงานของเครื่องที่ดักจับ

-Cert (13)	oning 192	2.168.1.37	606DC7CDC7CD	-				
SSH-1 (0)	anian 103		www.crebereb	0	0	0071CC2E8DC1	192.168.1.35	
SSH-1 (0) A Pair	oming 192	2.168.1.37	606DC7CDC7CD	0	0	80EA9638FD20	192.168.1.33	
77.00	oning 192	2.168.1.37	606DC7CDC7CD	3	2	9CE3743AD77D	192.168.1.1	
HTTPS (0)								
ProxyHTTPS (0)								
RDP (0)								
FTPS (0)								
POP35 (0)								
IMAPS (0) Status	IP a	address	MAC address	Packets ->	<- Packets	MAC address	IP address	
LDAPS (0) DAPS (0)	routing 192	2.168.1.37	606DC7CDC7CD	1	1	9CE3743AD77D	74.125.130.189	
SIPS (0) D Full	routing 192	2.168.1.37	606DC7CDC7CD	373	531	9CE3743AD77D	202.28.94.53	
Full	routing 192	2.168.1.37	606DC7CDC7CD	1	1	9CE3743AD77D	54.88.3.157	
Full	routing 192	2.168.1.37	606DC7CDC7CD	183	361	9CE3743AD77D	115.87.71.144	
		7 4 6 9 3 4 6 9 3 4 6	606067606760	6	e	000074340770	F # #03 #F0 333	
Full-	routing 192	2.108.1.37	00000/000/00	0	2	9CE3/43AD//D	54.192.159.252	

9.จากนั้นเลือก Passwords แทบด้านล่าง จะแสดง Usernameและ Password ของเครื่องที่ดักจับ

🔄 🏟 😔 前日 開始 開 Decoders 🔮 Network	왕 후 🛛 🕂 🥹 🛛 R ( 🏟 Sniffer 🕑 Crao	ker 🔮 Tracerou	🖭 💽 🖬 🕻	🕽 🧐 🔯 🚺	Query	
Passwords ^	Timestamp	HTTP server	Client	Username	Password	URL
FTP (0)     HTTP (1)     HTTP (1)     HTTP (1)     IMAP (0)     DAP (0)     SMB (0)     Teinet (0)     Toinet (0)     Tois (0)     Tois (0)     Tois (0)     Tois (0)     SMTP (0)     OEERPC (0)     Mixterbs-Preduth     Radius-Kess (0)	30/11/2016 - 21:21:27	202.28.94.53	192,168,1,37	573020829-5	829-5	http://202.28.94.53/lims/
Radius-Users (0)     King (0)     King (0)	< Энтр					