

รายงาน

โปรแกรม Ophcrack

โดย ฉว่มชื่ 4

	กลุมท 4	
563020473-7	นางสาวจุฑาชนม์	บุษบงก์
563020956-7	นายเกียรติประวัติ	น้อยทุ่ง
563020960-6	นายณัฐกิตติ์	บุญเรื่อง
563020962-2	นายณัฐิวุฒิ	อินทา
563020968-0	นางสาวพุทธชาติ	คำวงษา
563020972-8	นายสรวิชญ์	โคตรนรินทร์

อาจารย์ที่ปรึกษา : ดร.จักรชัย โสอินทร์

รายงานนี้เป็นส่วนหนึ่งของการศึกษารายวิชา 322 376 Information and Communication Technology Security ภาคเรียน 1 ปีการศึกษา 2558 ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น

โปรแกรม OPHCRACK LiveCD

โปรแกรม OPHCRACK LiveCD เป็นเครื่องมือฟรีแวร์สำหรับใช้ในการตรวจสอบรหัสผ่านผู้ดูแลระบบและผู้ใช้ บนระบบปฏิบัติการ Windows ซึ่งก็สามารถรันจากแผ่นซีดีได้เลยโดยไม่จำเป็นต้องทำการติดตั้งลงเครื่อง สำหรับวิธีการใช้งานก็ไม่ยุ่งยาก การทำงานค่อยข้างเร็วโดยใช้เวลาไม่นานก็สามารถถอดรหัสได้

วิธีป้องกัน

- 1.ตั้ง Password ไม่น้อยกว่า 8 ตัวอักษร
- 2.ใช้อักขระ ตัวพิมพ์ใหญ่ พิมพ์เล็ก สลับกันไป
- 3.ล็อค Bios ด้วยเลย

วิธีการใช้งาน OPHCRACK LiveCD

- 1. ทำการดาวน์โหลดอิมเมจ OPHCRACK LiveCD แล้วเบิร์นลง CD
- 2. ทำการบูตระบบด้วย CD ที่ทำในขั้นตอนที่ 1 ลักษณะหน้าจอของการบูต OPHCRACK LiveCD



รูปที่ 1 OPHCRACK Live CD

 หากเครื่องคอมพิวเตอร์ที่ทำการบูตนั้นมีหลายพาร์ติชั้น OPHCRACK LiveCD จะให้เลือกว่าจะต้องการ พาร์ติชันไหน ก็ให้ทำการเลือกพาร์ตอชันที่ต้องการ จากนั้น OPHCRACK LiveCD ก็จะทำการโหลดหน้า Dumping hashes ดังรูปที่ 2 แล้วทำการถอดรหัสผ่านของ account ที่พบในไฟล์ SAM ลักษณะการทำงาน จะเป็นดังรูปที่ 3

	launch sh; bash 👝 🗔 🗙
Found one partition that contains hashes:	
/mnt/hda1/WINDOWS/system32/config	
Found Windows SYSTEM file :) Found Windows SAM file :) Dumping hashes Starting Ophorack. Press a key to exit	

รูปที่ 2 Dumping hashes



รูปที่ 3 Starting Ophcrack

4. เมื่อถอดรหัสผ่านของ account ได้แล้วก็จะแสดงให้เห็นดังรูปที่ 4 โดยเวลาที่ใช้นั้นก็ขึ้นอยู่กับว่ารหัสผ่าน ที่ตั้งนั้น มีความซับซ้อนมากน้อยแค่ไหน สำหรับการทดสอบนี้ใช้เวลาประมาณไม่ถึง 5 นาที นับตั้งแต่บูตเครื่อง ด้วย OPHCRACK LiveCD จนถึงการถอดรหัสผ่านของ Administrator ได้ (ในการทดสอบนี้ ได้ทำการตั้ง รหัสผ่านเป็นแบบอย่างง่าย เพื่อใช้ในการแสดงให้เห็นการทำงานของโปรแกรมเท่านั้น ไม่แนะนำให้ท่านตั้ง รหัสผ่านตามตัวอย่างนี้)



รูปที่ 4 Password cracked

 จากนั้นก็ให้ทำการบูตระบบตามปกติ แล้วใช้รหัสผ่านที่ได้ในขั้นตอนที่ 4 ในการล็อกออนเข้าระบบวินโดวส์ (ในการใช้งานจริงนั้น ขอแนะนำให้ทำการเปลี่ยนรหัสผ่านทันทีเมื่อทำการล็อกออนเข้าระบบได้สำเร็จ)

ข้อดี

- รหัสผ่านของผู้ดูแลระบบจะไม่ถูกเปลี่ยนแปลง
- สามารถใช้งานได้โดยไม่ต้องติดตั้งลงเครื่อง
- สามารถใช้งานได้ฟรี

ข้อเสีย

- หากมีการตั้งรหัสผ่านของผู้ดูแลระบบแบบซับซ้อนมากๆ อาจใช้เวลาในการถอดรหัสนานมาก

โปรแกรม Ophcrack สามารถถอดรหัสได้แค่ 4 ตัวเท่านั้น จึงมีการโหลด Rainbow tables มาเป็นตัวช่วยใน การถอดรหสได้มากกว่า 4 ตัว ซึ่งตัวที่เราใช้คือ XP free fast (703MB)

Rainbow tables มีให้เลือกดาวน์โหลดหลายตัวตามความต้องการในการใช้งาน มีทั้งแบบฟรีและเสีย ค่าใช้จ่าย



ความยาวรหัส 8 ตัว, ถอดรหัสที่เป็นตัวเลข ภาษาอังกฤษพิมพ์เล็ก-ใหญ่ได้ (เราใช้ตัวนี้)

Rainbow tables แบบต่าง ๆ





Success rate: 99.9% Charset: 0123456789abcdefghijkImnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

md5sum: f6f5536975b57c891ed5f2de702a02bd



Success rate: 96% Charset: 0123456789abcdefghijkImnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ !"#\$%&'()*+,-./:;<=>?@[\]^_`{{}~ (including the space character)



Success rate: 99%

Based on a dictionary of 64k words, 4k suffixes, 64 prefixes and 4 alteration rules for a total of 2³⁸ passwords (274 billion).

md5sum: 403cf58178d7272a48819b47ca8b2e6b



md5sum: e0718aaf085980e0884ea5d09c7b856e



Success rate: 99% Passwords of length 6 or less Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ !"#\$%&'()*+,-./:;<=>?@[\]^_`{|}~ (including the space character) Passwords of length 7 Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ Passwords of length 8 Charset: 0123456789abcdefghijklmnopqrstuvwxyz



Success rate: 99.9% Passwords of length 1 to 12 Charset: 0123456789



Success rate: n/a Passwords of length 5-12 Charset: 0123456789abcdefghijkImnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ !!"#\$%&'()*+,-,/:;<=>?@[\]^_`{}~ (including the space character)



Success rate: 99% Passwords of length 1-7 Charset: 0123456789abcdefghijkImnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ !"#\$%&'()*+,-./:;<=>?@[\]^_`{{}~ (including the space character)



Success rate: 99% Passwords of length 8 Charset: 0123456789abcdefghijkImnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!*



Success rate: 99% Passwords of length 8 Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ !"#\$%&'()*+,-./:;<=>?@[\]^_`{}~ (including the space character)



Success rate: 99% Passwords of length 8 Charset: 0123456789abcdefghijklmnopqrstuvwxyz with the first letter capitalized Passwords of length 9 Charset: 0123456789abcdefghijklmnopqrstuvwxyz

ขั้นตอนการติดตั้งและใช้งาน OPHCRACK USB

 เปิดเครื่องทำการกด F2 ย้ำๆแล้วจะขึ้นดังรูปที่ 1 แล้วคลิก boot กด internal optical disc drive เพื่อเซ็ตค่าคอมพิวเตอร์ให้ทำการอ่านจาก disc หรือ usb

Aptio Setup Ut Build Advanced Security Bo	ility – Copyright (C) 2010 American Megat not Exit	rends, Inc.
Boot Configuration External Device Boot Network Boot	[Enabled] [Disabled]	This setting is for the boot order of each device.
Boot Priority Select 1st Boot Priority Select 2nd Boot Priority Select 3rd Boot Priority	[Internal Hard Disk Drive] [Internal Optical Disc Drive] [External Device]	'Network' are available when each setting in 'Boot Configuration' is set to 'Enabled.'
	Select 1st Boot Priority Internal Optical Disc Drive Internal Hard Disk Drive External Device	
•	Network	<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version 2.01.	1204. Copyright (C) 2010 American Megatrer	dsi inclusion in

รูปที่ 1

2. กด Exit แล้วกด yes



รูปที่ 2

- 3. โหมดของ Ophcrack ให้อยู่ 4 โหมด
 - Ophcrack Graphic mode automatic
 - Ophcrack Graphic mode manual
 - Ophcrack Graphic mode low RAM
 - Ophcrack Text mode

ซึ่งเราจะเลือกโหมดที่ 1 คือ Ophcrack Graphic mode – automatic เพื่อให้เข้าทำงานได้เลย



รูปที่ 3

4. จะได้หน้าต่างของดังรูปที่ 4 ขึ้นมาแล้วกด enter



5. โปรแกรมพื้นฐานจะทำการ Hack ได้สำเร็จได้แค่ password 4 ตัวเท่านั้น

rogress Stat	istics Prefi	erences	ck Help	Exit		Abou
User ∇	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd	
disabled* A disabled* benguin		31d6cfe0d1 31d6cfe0d1 31d6cfe0d1			empty empty	
rong rong2		1d95d51326 9cbef67993		2 1	aszx 1122	
rong3		700ec8a682		n n	iot found iot found	
			-			
Table	Directory	Status		Progra	255	
Table	Directory •	Status		Progra	955	
Table	Directory	Status	•	Progra	P55	
Table [Directory	Status		Progre	255	

รูปที่ 5

 จึงทำการเพิ่มในส่วนของ Rainbow Tables เข้ามาเพื่อให้ทำการ Hack password ได้มากขึ้นกว่าเดิม ให้ทำการคลิกที่ my document จะได้ดังรูป



รูปที่ 6

ทำการเลือก slitaz ophc -> เลือก table -> คือไฟล์ของ Rainbow Tables ที่จะใช้ทำการ Hack
 เลือก vista_proba_free แล้วลากมาไว้ Desktop



รูปที่ 7

8. จากนั้นมันจะทำการโหลดเพื่อใช้ไฟล์ในการ Hack



รูปที่ 8

9. คลิกtables



รูปที่ 9

10. ทำการ Install

Table	Directory	Married States	
XP free fast	Directory	all have	Status
XP free small			not instal
XP special			not instal
• XP german v1			not install
XP german v2			not install
Vista special			not install
Vista free			not install
Vista nine			not install
Vista eight			not installe
Vista num			not installe
Vista seven			not installe
XP flash			not installe
Vista eight XL	×		not installe
Vista special XL			not installe
Vista probabilist			not installe
Vista probabilist			not installe
Vista probabilist			not installe
A Real Property of the Property of the			mot matane
			in filling and friend
Market States And			And the second second
I see a supering the second second		Contraction of	••
= enabled = disabled	a = not installed		
- chooled - disabled	- not installed		

รูปที่ 10

11. คลิก Desktop



รูปที่ 11

12. คลิกชื่อไฟล์ดังรูปที่ 12 แล้วกด Chooes

OIL	Select the directory w	which contains the tables.	
Look in:	home/tux/Desktop		0007
Computer	Vista proba free		
Directory:	vista_proba_free		<u>C</u> hoose
Files of type:	Directories		Cancel

รูปที่ 12

13. คลิกที่ OK



รูปที่ 13

14. คลิกที่ Crack

User ∇	LM Hash	NT Hach			Law Provent
disabled* enguin est1 rong rong2 rong3		31d6cfe0d1 31d6cfe0d1 1d95d51326 9cbef67993 0a640404b5 700ec8a682		empty empty empty aszx 1122 not found not found	
Table	Directory	Status	Proc		

รูปที่ 14

15. ทำการประมวลผล และอ่านรหัสของ user

รูปที่ 15

16. ประมวลผลเสร็จได้รหัส

	interes interes	erences				
User V *disabled* A penguin iest1 irong rong2 rong3	LM Hash	NT Hash 31d6cfe0d1 31d6cfe0d1 31d6cfe0d1 1d95d51326 9cbef67993 0a640404b5 700ec8a682	LM Pwd 1	LM Pwd 2	empty empty empty aszx 1122 qwer1234 qwe123	NT Pwd
Table Vista p /// tabl tabl tabl	Directory /home/tux/	Status 100% in RAM 100% in RAM 100% in RAM 100% in RAM		Pro	gress	

รูปที่ 16

17. เลือก accout ที่จะใส่รหัส



รูปที่ 17

18. ทำการใส่รหัสที่ถอดมาได้



รูปที่ 18