資訊安全實習 ③

實驗名稱 – John the Ripper 密碼分析工具



本實驗之目的主要讓學員瞭解 SAMInside 以及 John the Ripper 之實際操作。學員可 由操作過程中瞭解如何利用 SAMInside 這套軟體取出 Windows 中現有的帳號密碼表(密 碼已 Hash),再透過 John the Ripper 密碼分析工具分析經由 SAMInside 取出的密碼檔。

實驗測試步驟

1. 安裝及操作 SAMInside

SAMInside - Windows Internet Ex	plorer								×
▲家田 編輯匠 被視(V) 我的最	om/eng/sammate.shtml 慶仏) 工具(D) 説明(H)					Y 🖾 🦘	K Google		
🚖 我的最爱 🍰 遠談的網站 -	🩋 自訂連結 🧧 発費的 Hotmail	🧧 網頁快訊圖庫 🔹							
18 SAMInside						💁 • 🖾 ·	- 🖶 • 網頁化	 安全性⑥、 工具〇、 Ø、 	~
	Site News 04/3/02/32 Extreme GPU Bruteforer has been updated to version 2.1 (comments: 3) 03/04/2012 Extreme GPU Bruteforer has been updated to version 2.0.2 (comments: 1) 02/12/2012 PassvordsPro has been updated to version 3.1.2.0 (comments: 8)			ICQ: 285429551 support@insidepro.com	-				
SAMInside Doveland					SAMInside				
PasswordsPro Version 3.1.2.0 (05/01/2012)		IMPORTANTI Yo	u may us	e this software fo	r the recovery of	f your own forgotten pas	sswords only.		
Extreme GPU Bruteforcer	Program Description Data Import								
Download Download (64-bit)	Password Recovery Command Line Param Additional Features	eters							
Buy Software	Demo Version Restric License Agreement FAO	ions							
Posts: 86099				Prog	ram Description	1			
Files: 89 Rainhow Tables		SAMInside							
Tables: 132 Hash Generator		Ele Edit View	ools <u>A</u> udit	Service 2		n o o o			
Algorithms: 345		User ·	RID	LM-Password	NT-Password	LM-Hash	NT-Hash		
Subscribers: 1517 Visitors today: 6240		BillG Administrator	1010 500	7777777A 7777777IS	7777777777777777 7777777777777777	5ECD9236D21095CE 73CC402BD3E791756	C04EB42B9F5 C7E2622D76E		
Total visitors: 7533466		v fredc twoa v william	1011 1000 1012	7777777T AA 277272727	27777777777777777777777777777777777777	3466C2B0487FE39A4 89D42A44E77140AAA DBC5E5CBA8028091	80030E356D1 C5663434F96 686E0F82ED2		
		threea	1001 1002	AAA	000 0000	1C3A2B6D939A1021 DCF9CAA6DBC2F2DF	E24106942BF: FA5664875FF/		
		Users: 7. Passwo	rds found:	3 (42.86%).	Curre	nt password: NQHXI	>		
		Ready)			
	SAMInside is designated for	he recovery of Windo	vs NT, Win	dows 2000, Window	s XP, Windows 200	3, Windows Vista, Windows	7 user passwords.		
	Some of its outstanding feat	res include:							M
							😜 病際網路	🖌 🗸 🔍 100% 🔸	•

Step 2	將下載下來的檔案解壓	縮至 C:\saminside		
	○ saminstide 宿業① 編輯匠 絵硯(① 我的最爱(込 工具(① 説明(①) (③) 上一页 · ② · ⑦ 20 提録 [② 資料來 [11]]•			
	#社①	Haches Dangung	▼ ● 8至 i Cools	
	 建立能的资料夹 第這個资料夹技術資源站 第這個资料夹 ● 共用這個资料夹 ● 218 	Russian kbt KBT 德家 2 KB	HTML Help 檔案 SAMInide Engle Pro Software	
	其他位置 ◆ 本規取罪(C) ◆ 発知文件			
	 ○ 共用文件 ○ 共用文件 ○ 我的電腦 ● 網路上的芳菜 			
	注意 (1997年1997年1997年1997年1997年1997年1997年1997			
<u> </u>	1 周治 の SAMInile - Windows. 本 1 (1) (1) (1) (1) (1) (1) (1) (1) (1) (in seminaise	🖮 🛛 🕺 🚺 🔔 🔍 🔮 T 🕇 0801	
Step 3	執行 SAMInside ▶ eminiate		-8×	
			~ □ 株平	
	 編末及資料夾工作 ● 建立新的資料夾 ● 建立新的資料夾 ● 建立新的資料夾 ● 第二第一次第二次第二次第二次第二次第二次第二次第二次第二次第二次第二次第二次第二次第二次	Hashes Languages	Tools	
	● 新活動資料交換所到時站 ● 共用這個資料交 工作 工作 工作 工作 工作 工作 工作 工作 工作 工作	Ruman kbt EF Wask 2 KB SAMInade SAMInade SAMInade	AL Help 衛家 EAMinade Englishing Eaving Eavi	
		TKB		
	 ● 新的電腦 ● 朝陰上的芳醇 			
	部資料 <u>(</u>)			
	🥶 附前的 🧹 SAMinide - Windows . 🖀 我的文件	arministife	m P ² 9 2 9 8 7∓0802	

Step 4	Windows\System32\Co	onfig\SAM 這路徑	图下可以找到 Wi	ndows 使用者的帳题	<i>虎與密碼檔</i>
	SAM,但這檔案我們	不能直接開啟,氰	壽用 SAMInside ź	言套軟體來開啟, 彪	動 SAMInside
	後,執行以下的操作				
	SAMInside Ede Edit Yew Icols Audit Service ?				
	Import SAM and SYSTEM Registry Files Ctrl+O Import SAM Registry and SYSKEY File Import Local Users via LSASS LM-Password	NT-Password LM-Hash	NT-Hash Description		
	Import Local Users via Scheiguler Import from PWDUMP File Alt+O Import from PWDUMP File				
	Import from *LC 2 File Import from *LC 2 File Import from *LC 2 File				
	Import from *LST File Import LM-Hashes from *.TXT File				
	Import MT-Hashes from *TXT File Export Users to PWDUMP File Export Selected Users to PWDUMP File				
	Export Selected LM-Hashes to EQB Format				
	Export Found Pesswords Export Statistics				
	Egit				
	Users: 0, Passwords found: 0 (0.00%).			Current password:	
	🛃 開始 🌈 SAMInuide - Windowe 👛 我的文件	😂 samincide 😫 SAMinside			
Step 5	執行後畫面如下:				
	👯 SAMInside				
	<u>File Edit View Tools A</u>	udit <u>S</u> ervice <u>?</u>			
	🧊 · 🔊 · 🞁	- 🌍 - 🌏 -	🔊 🍰 👔 -	🖒 🕨 🛍 🚺	
	User	RID	LM-Password	NT-Password	LM-Hash
	Administrator	500 501	<disabled></disabled>	<empty> <disabled></disabled></empty>	0000000000000000
	SUPPORT_388945a0	1002	<disabled></disabled>	7777777777777	000000000000000000000000000000000000000
	V XPMUser V HelpAssistant	1003 1004	7777777	7777777	01FC5A6BE7BC69 6E78A2ACF2A7AC
	CISLAB	1005	???????	???????	F6794AD6366E0E6
	<				>
	Users: 6. Passwords four	nd: 2 (33.33%).		Current password:	
	Ready].;;
	• 視窗中顯示的	User · LM-Passw	vord NT-Passwo	ord 為 Windows 的朝	影號與密碼檔
	・ 以 LM hash 為	例,以下為運作	方式:		

	SAMInside le Edit Yiew Jools Audit Service ? Import SAM and SYSTEM Registry Files Ctil+O Import SAM Registry and SYSKEY File Import Local Users via LSASS Import Local Users via Scheduler Import from PWDUMP File Import from *LCP File Import from *LCP File Import from *LCP File Import from *LST File Import NT-Hashes from *.TXT File Import Selected Users to PWDUMP File Export Users to PWDUMP File Ctil+S Export Selected LM-Hashes to EGB Format Export Selected LM-Hashes to EGB Format	LM-Password <disabled> <disabled> <disabled> ??????? ???????????????????????????</disabled></disabled></disabled>	VT-Password <empty> <disabled> ????????????????????????????????????</disabled></empty>	LM-Hash 000000000000000000000000000000000000
匯出後 ● 01	後檔案如下: 139本 編輯(R) 格式(R) 絵環(R) 説明(R)			

2. 安裝 John the Ripper



Step 3	開啟命令提示字元:	開始→更多	→程式→附	蠆應用程式→	命令提示字元	
	★ 本提磁器 (C:) 檔案 (C:) 續報 (C:) 檢視 (V:) 我的最爱(▲) 工具 (D:)	说明(<u>H</u>)				
	🕞 上一頁 • 🕑 • 🏂 🔎 搜尋 🍋 資料夾	····				
	網址② 🗢 C.\	💼 協助工具 🔹 🕨				▶ 移至
	系統工作 🛞 🍎 Docu	□□ 姚栄 → >=	1386	Program Files	windows	
	陸	🔤 🔤 TrueType 造字程式				
	➢ 搜尋檔案或資料夾	17 🔄 Windows檔案總管 📝 WordPad				
	<u>榆家及资料来工作</u> (余)	₩ 小畫家				
	XPMUser	 □ 小算盤 ③ 同步處理 				
		▲ 命令提示字元				
		303 伯明子的病料工具 ■ 記事本				
	電子第件 Outlook Express Windows Catalog	2 2 通用輸入法編輯工具 (1) 通訊等				
	● Windows Update	 2010年 2010年 2010年 2010年 				
		 ・ 遠端点面連線 ・ ・ ・				
		💼 系統工具 🔹 🕨				
	Vindows Media Play 価格的 一 遊樂場	▶ 設値 ▶				
	Windows Messenger 💋 Internet Explorer					
	導覽 Windows XP ② Windows Media Player					
	雄業及設定轉移精 過 Windows Messenger 御堂はいい Marin Marin Mahan Windows Messenger 御堂はいい Marin Mahan Windows Messenger 和 和 和 和 和 和 和 和					
	所有程式(2) 🏓 🦾 遠端協助	þ				
		2 登出(1)				
	🔰 開始 🔒 PGP Desktop - All Keys 🖀 我的	这件 🔁 run	🤝 本機磁碟 (C:)	🖉 John the Ripper passw		🖮 國 🏅 🌖 🛆 下午 10.18
Step 4	輸入 cd c:\john179v 資料夾)	w2\john179\r	un(注意: 此	比路徑為先前的	解壓縮之路徑	,請確實指向 run
	□ mm 檔案(E) 續輯(E) 檢視(V) 我的最爱(人) 工具(E) 書	说明(H)				
	🕝 上一頁 • 🕥 · 🎓 🔎 搜尋 🌔 資料夾	····				
	網址 D 🗀 C.\john179w2\john179\run					▼ 🄁 移至
	檔案及資料夾工作 🉁 💋 pre-s	202	all.chr CHR 檔案 334 KB	alnum.chr CHR 檔案 227 KB	alpha.chr CHR 檔案 129 KB	
	建立新的資料夾 級 將這個資料夾發佈到網站	🖾 命令提示字元				_ 🗆 🗙
		(C) Copyright	dows XP [版本 5.1 1985-2001 Micros	.2600] oft Corp.		
	其他位置	C:\Documents	and Settings\XPMU	ser>		
	 john179 ① 我的文件 	omp C:\Documents	and Settings\XPMU	ser>cd U:\john1(9w2\jo	nn1 (9\run	
	● 共用文件	C:\john179w2\	john179\run>_			
	● 網路上的芳鄉 ● 和路上的芳鄉 ■ IKB	文件				
		☆母				
		<u> </u>				
	🛃 開始 👔 PGP Desktop - All Keys 📫 我的	交件 🍃 run	מת 🤤	6 John the Ripper passw	☑ 命令提示字元	CH 🌻 🏟 下午 10:24

Step 5	輸入 john.exe 查看相關指令說明
	6 John the Ripper password cracker - Windows Internet Explorer
	☆ 知的最要 (金) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2
	登 這個網站想要執行下列附加元件:來自 Xalobe Systems Incorporabel 的 Xalobe Flash Plaser': 如果您信任該網站及附加元件,而且要讓它執行,請按這種
	Products Ser C:\john179w2\john179\run>john.exe John the Ripper password cracker, version 1.7.9 Copyright (c) 196-2011 by Solar Designer Homepage: http://www.openwall.com/john/ Usage: john (OPTIONS) John the Ripper is a fast password cracker, currently availalsingle single single crack" mode single single crack" mode single single crack" mode
	Password Mash types most commonly found on various of all control various of all c
	OS passwords status[:NHME.] print status of a session [called NHME] Windows Proceed to John the Ripper 7P0 make-charsetsFILE make a charset, FILE will be overwritten Vindows NT/2000/XP/2003/Vista/7 make-charsetsFILE make a charset, FILE will be overwritten Vindows NT/2000/XP/2003/Vista/7 make-charsetsFILE make a charset, FILE will be overwritten Vindows NT/2000/XP/2003/Vista/7 make-charsetsFILE make a charset, FILE will be overwritten Vindows Status users[-]LOGINIUID[] [do not] load this (these) user(s) only users[-]CoUNT Unix Download one of the later shells=[-]SHELL[] load users with[out] this (these) shell(s) only salts=[-]COUNT Mdcroseb Office - John the Ripper 17 seare memory=LEUEL enable memory saving, at LEUEL 13 mable memory saving, at LEUEL 13 MS Word - John the Ripper 17 sformat-NAME force hash type NAME: des/bsdi/md/s/bf/afs/lm/trip/ Image: mable memory saving, at LEUEL 13
	Excel · John the Ripper 1. dummy 团团企業600大上市上都公司 团团企業600大上市上都公司 I
	● 1 開始 PoP Desktop - All Keys 🍙 発動文件 🍃 run 🍃 nun 🖉 John the Ripper passw
	 我們可以用 john [密碼檔.檔名]這簡單的指令來破密,也可以讓 John the Ripper 單獨 執行特定的模式來破密 單一解碼模式(Single crack mode) 字典模式(Wordlist mode) 暴力窮舉模式(Incremental mode) 單一解碼模式 針對密碼檔的帳號去做字詞變化破解
	 例如密碼檔內有 dragon 這個帳號, John the Ripper 會以此字串做變化, 如下 drago, nogard, 02dragon, dra567gon 指令形式: john -si [filename]
	字典模式
	 俗稱的字典檔攻擊, John the Ripper 可以指定字典檔 一般指令只有直接比對字典檔與密碼檔 john -w:[字典 filename] [密碼檔 filename] 進階指令,可將字典檔內的資料做有規則的排列或是重組等等,之後再來跟密碼檔 比對,在指令加入-rules 即可開啟此功能 john -rules -w:[字典 filename] [filename]

Lohn the Ripper password → 📴 Files ≈ Packet Storm	n ×	
C packetstormsecurity.org/Cracke	ers/wordlists/	🗛 🛛 🙍 🍮 🖪 🔀 🕑
这▲ 此網頁為 英文 · 您要翻譯網頁內容嗎?	翻譯不需要	選項▼
aadkat dtarm		Registe
Fight your daemons		Search
Home Files News	About Contact	Add New
Files	Showing 1 - 25 of 18	
		Follow us on Twitter
7 Text To Sorted Word-List Creator		Follow us on Facebook
Authored by snakingmax Site snakingmax.blogspot.com	Posted Aug 19, 20	11 Subscribe to an RSS Feed
tags cracker, python	ator in Fython 5.	
MD5 e22d6b2c50ec37daa3c15d1e733ecb14	Download Favorite Comments	Top Authors In Last 30 Da
Arabic Names Dictionary		Red Hat 28 files
Authored by g33ko	Posted May 10, 20	11 Farbod Manini 26 files Ubuntu 22 files
tags cracker	e Arabic names, rogenter mere are over 1000 entries.	HauntIT 22 files
MD5 53a9b12373d92434e73a6c121ff7c4f6	Download Favorite Comments ((0) Debian 21 files Mandriva 16 files
🚺 Iranian Name Wordlist		HP 14 files
Authored by Nima Ghotbi Site h.ackerz.com	Posted Mar 16, 20	10 the_cyber_nuxbie 13 files
This is a list of Iranian names to be used for cracking.		BHG Security Center 9 files
● 也可自行透過記事本編	輯,將可能的密碼直接寫到相	當案,每個密碼一行問
	📮 common2.txt 📃 🗖 🛃	×
	File Edit Format View Help	
	admin	~
	sysadm sysadmin	
	operator	
	manager	

字	典模	式中 rules 的編輯
Wo	ordlist	的 rules 會存放在 run 資料夾裡的 john.ini 中,下圖顯示的是 john.ini 的初始值
	john.	ini - Notepad 📃 🗖 🔀
File	e Edit	Format View Help
;# ;!	Inse ?Ali[ert/overstrike some characters
;! ;#	?Alo[Togg	0-7][a-z]]e_case_everywhere
; ;#	MT[*0 _Ver))]T[*1]T[*2]T[*3]T[*4]T[*5]T[*6]T[*7]Q / slow stuff
; (\$[1-9 ?ac\$[0]<-\$[0-9]\$[0-9] 1-90]<-\$[0-9]\$[0-9]
; <	9]^[a	[-2]》[a-2] [-2]^[a-2] [-2]*[a-2] 打開 John ini 後,找到[[ist Rules:Wordlist],在
, _` # \	word	[-2] $[a-2]$ $[b]$ $[$
[L #	ist.F Trv v	words as they are 這標頭後就可自行編輯 rules
: ₩ 1	Lower	case every pure alphanumeric word
-⊂ # (>3!? Capit	xlo alize every pure alphanumeric word
-⊂ # ∣	>2(? Lower	case and pluralize pure alphabetic words
<*: #	>2!?A Lower	case pure alphabetic words and append '1'
<**: # (>2!?A Capit	alize pure alphabetic words and append '1'
-⊂ #	<">2 Dupli	227AC\$1 cate reasonably short pure alphabetic words (fred -> free
<10	>1:??	v
1		
、 堂日	田指名	
《 常月 -	■ 用指令 :	₩ > 對 wordlist 不做任何動作
《 常月 -	用指令 : C	> 對 wordlist 不做任何動作 將字首大寫,如:" crack" -> "Crack"
< <	用指名 : C c	★ <
 	用指く : C c r	★ 梦 wordlist 不做任何動作 將字首大寫,如:" crack" -> "Crack" 將字首小寫其餘大寫,如: "Crack" -> "cRACK" 反向,如: "crack" -> "kcarc"
《 常月 - - -	用指< : C c r d	★ <
< < < <	用指⊲ : C c r d f	對 wordlist 不做任何動作 將字首大寫,如:" crack" -> "Crack" 將字首小寫其餘大寫,如: "Crack" -> "cRACK" 反向,如: "crack" -> "kcarc" 複製,如: "crack" -> "crackcrack" 鏡射,如: "crack" -> "crackkcarc"
< 常月 − − − − − − − − − − − − − − − − − − −	用指< C c r d f {	對 wordlist 不做任何動作 將字首大寫,如:" crack" -> "Crack" 將字首小寫其餘大寫,如: "Crack" -> "cRACK" 反向,如: "crack" -> "kcarc" 複製,如: "crack" -> "kcarc" 復製,如: "crack" -> "crackcrack" 鏡射,如: "crack" -> "crackcrack"
常月 常月 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	用指令 : C c r d f { }	★ 梦 wordlist 不做任何動作 將字首大寫,如:" crack" -> "Crack" 將字首小寫其餘大寫,如: "Crack" -> "cRACK" 反向,如: "crack" -> "kcarc" 復製,如: "crack" -> "crackcrack" 鏡射,如: "crack" -> "crackcarc" 往左 shift,如: "crack" -> "rackc" 往右 shift,如: "crack" -> "kcrac"
■ 常月	用指令 C c r d f { } \$X	★ <
■ 常月	用指< C c r d f { } \$X ^X	★ 對 wordlist 不做任何動作 將字首大寫,如:" crack" -> "Crack" 將字首小寫其餘大寫,如: "Crack" -> "cRACK" 反向,如: "crack" -> "kcarc" 複製,如: "crack" -> "crackcrack" 鏡射,如: "crack" -> "crackcrack" 镜射,如: "crack" -> "rackc" 往左 shift ,如: "crack" -> "kcrac" 在字串後面串接一個字母,如: \$4: "crack" -> "crack4" 在字串前面先置一個字母,如: ^4: "crack" -> "4crack"
■ 常務	用指< C c r d f { } \$X ^X <n< th=""><th>岁 wordlist 不做任何動作 將字首大寫,如:" crack" -> "Crack" 將字首小寫其餘大寫,如: "Crack" -> "cRACK" 反向,如: "crack" -> "kcarc" 複製,如: "crack" -> "crackcrack" 鏡射,如: "crack" -> "crackcrack" 镜射,如: "crack" -> "crackcracr" 往左 shift,如: "crack" -> "rackc" 往右 shift,如: "crack" -> "kcrac" 在字串後面串接一個字母,如: \$4: "crack" -> "crack4" 在字串前面先置一個字母,如: ^4: "crack" -> "4crack" 字串大小必須大於 N</th></n<>	岁 wordlist 不做任何動作 將字首大寫,如:" crack" -> "Crack" 將字首小寫其餘大寫,如: "Crack" -> "cRACK" 反向,如: "crack" -> "kcarc" 複製,如: "crack" -> "crackcrack" 鏡射,如: "crack" -> "crackcrack" 镜射,如: "crack" -> "crackcracr" 往左 shift,如: "crack" -> "rackc" 往右 shift,如: "crack" -> "kcrac" 在字串後面串接一個字母,如: \$4: "crack" -> "crack4" 在字串前面先置一個字母,如: ^4: "crack" -> "4crack" 字串大小必須大於 N
	用指 C c r d f { X ^X <n< p=""></n<>	★ <
	用指令 C C r d f { } \$X ^X ~X <n (X</n 	對 wordlist 不做任何動作 將字首大寫,如:" crack" -> "Crack" 將字首小寫其餘大寫,如: "Crack" -> "cRACK" 反向,如: "crack" -> "kcarc" 複製,如: "crack" -> "crackcrack" 鏡射,如: "crack" -> "crackcrack" 镜射,如: "crack" -> "crackcrac" 往左 shift,如: "crack" -> "rackc" 往右 shift,如: "crack" -> "kcrac" 在字串後面串接一個字母,如: \$4: "crack" -> "crack4" 在字串前面先置一個字母,如: ^4: "crack" -> "4crack" 字串大小必須大於 N 字串大小必須小於 N 只對第一個字是 X 的字串做 rule 的動作
 Image: State of the state	用指< C c r d f { } \$X ^X <n ×N (X)X</n 	★ 對 wordlist 不做任何動作 將字首大寫,如:" crack" -> "Crack" 將字首小寫其餘大寫,如: "Crack" -> "cRACK" 反向,如: "crack" -> "kcarc" 複製,如: "crack" -> "crackcrack" 鏡射,如: "crack" -> "crackcrack" 镜射,如: "crack" -> "crackcrac" 往左 shift,如: "crack" -> "rackc" 往右 shift,如: "crack" -> "kcrac" 在字串後面串接一個字母,如: \$4: "crack" -> "crack4" 在字串前面先置一個字母,如: ^4: "crack" -> "4crack" 字串大小必須大於 N 只對第一個字是 X 的字串做 rule 的動作 只對最後一個字是 X 的字串做 rule 的動作
< ■ 常 =	用指令 C c r d f { } \$X ^X <n >N (X)X p</n 	對 wordlist 不做任何動作 將字首大寫,如: " crack" -> "Crack" 將字首小寫其餘大寫,如: "Crack" -> "cRACK" 反向,如: "crack" -> "kcarc" 複製,如: "crack" -> "crackcrack" 鏡射,如: "crack" -> "crackcrack" 鏡射,如: "crack" -> "crackcarc" 往左 shift ,如: "crack" -> "rackc" 往右 shift ,如: "crack" -> "kcarc" 在字串後面串接一個字母,如: \$4: "crack" -> "crack4" 在字串前面先置一個字母,如: ^4: "crack" -> "4crack" 字串大小必須大於 N 字串大小必須大於 N 只對第一個字是 X 的字串做 rule 的動作 只對最後一個字是 X 的字串做 rule 的動作 複數,如: "crack" -> "cracks"
	用指令 C c r d f { } \$X ^X <n (X)X P P</n 	對 wordlist 不做任何動作 將字首大寫,如: " crack" -> "Crack" 將字首小寫其餘大寫,如: "Crack" -> "cRACK" 反向,如: " crack" -> "kcarc" 複製,如: " crack" -> " crackcrack" 鏡射,如: " crack" -> " crackcrack" 鏡射,如: " crack" -> " crackcarc" 往左 shift ,如: " crack" -> " rackc" 往右 shift ,如: " crack" -> " kcrac" 在字串後面串接一個字母,如: \$4: " crack" -> " crack4" 在字串前面先置一個字母,如: ^4: " crack" -> " 4crack" 字串大小必須大於 N 字串大小必須大於 N 只對第一個字是 X 的字串做 rule 的動作 只對最後一個字是 X 的字串做 rule 的動作 表載,如: "crack" -> " cracka"

- [將第一個字刪除,如: "crack"-> "rack"
-] 將最後一個字刪除,如: "crack"-> "crac"
(由於"["和在"]" rule 裡有另外的用法,為了區分使用,
必須在之前加"\")
- R - 根據鍵盤上的位置往右移一格,如: "crack96" -> "vtsvl07"
- L 根據鍵盤上的位置往左移一格,如: "crack96"-> "xeaxj85"
暴力窮舉模式
暴力窮舉模式就是暴力破解法(brute-force attack),嘗試所有的組合,將全部的有效鍵盤 字符(大概 95 個)進行 1~8 位的隨機組合,去猜解密碼。這個模式可以解出簡單模式和 字典模式不能成功猜解的密碼,但是效率極低,非常耗費時間 john -i [filename]
John the Ripper 相關指令
強制結束
- Ctrl^C
回復上次工作
– john -restore
在命令視窗顯示 test.txt 破解的結果
– john -show test.txt
John the Ripper 會在 run 目錄中產生一個 "john.pot"檔案,這裡面保存著成功猜解出來的密碼

SAMInside 所	摄取出的密文貼成文字檔如下
▶ 01 - 記事本	
· 備楽(E) 編輯(E) 格式(CISLAB 1995 F679)	외 微純(1) 화명)[1] 4AD6366E ØE67AAD38435B51484EE <mark>(C5A5E8682FEC46C20ED994168E220878:::)</mark> 고
User RID	LM-Hash NT-Hash
使用 John t	he Ripper 破解 windows 密文如下
■ 命令提示字	元 _ O >
Microsoft W	indows_XP [版本 5.1.2600]
(C) Copyrig	nt 1985-2001 Microsoft Corp.
C:\Document	s and Settings\XPMUser>cd c:\john179w2\john179\run
C:\john179w	2\john179\rup≥iobpi_01_tyt
Loaded 1 pa	ssword hash <mark>(LM DES [128/128 BS SSE2])</mark> 可看到此密文加密方式為NT和LM的
No password	hashes felt to crack (see FAQ) DES
C•\iobo179w CISLAB•CIS4	2\iohn179\run>john -show 01.txt 042:_005:0545E8682EEC46C20ED994168E220078
。 透過-show	v 指今可得到帷號CTSLAR的変碼為CTSLAR4042
l password	nash crackéd, "U-Tertert a kiyw cischererz
C:\john179w	2\john179\run>_
1	
檢視.John	the Ripper 的破密結果
 可在 	預設目錄底下 run 資料夾中找到一個 john.pot 檔,這裡會記載所有意
碼與	相對應的密文(如下圖)
□ 10hm - 記爭卒 檔案(F) 編輯(E)	▲ □ □ ■ ▲ □ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■

問題:

假設一個字典檔的內容有{Kobe,Bryant,Odom,Derek,Fisher,Ariza,Travor, Lamar,Paul,Jordan,Gasol,Andrew,Famar,Howard,Lebron}。若可能的密 碼如下:TravorTravor,DerekkereD,domO,ArizaazirA,lamarramal,23jordan, Kobe24,Paul33,LebronJames,asolG,ndrewA,amaramar520,HowardHoward, bryantbryant,5566Fish}

(1)假如使用指令"f",上述那些密碼會被 John the Ripper 的字典模式找到

(2)假如使用指令"d",上述那些密碼會被 John the Ripper 的字典模式找到

(3)假如使用指令"{",上述那些密碼會被 John the Ripper 的字典模式找到

(4)若以 John the Ripper 的字典模式破解密碼檔,請寫一個可以搜尋到密碼 "5566fish"的 rule

(5)若以 John the Ripper 的字典模式破解密碼檔,請寫一個可以搜尋到密碼 "amaramar520"的 rule

總結測驗:

請利用 SAMInside 將電腦中的密碼檔輸出,並破解密碼。

- E知用戶**1 的密碼,可能為一男性名字,可利用 <u>http://packetstormsecurity.org/Crackers/wordlists/</u>網址所提供的字典檔的 名字之一後面加上 123 來破解密碼。
- (2) 已知用戶**2 的密碼與帳戶相關,可用單一解碼模式得出密碼。
- (3) 已知用戶**3 的密碼為 5 個數字的隨機密碼,可嘗試利用暴力破解法。
- (4) 已知用戶**4 的密碼為 4 個的隨機亂數(英文,數字,符號),可嘗試利 用暴力破解法。

問題:

假設一個字典檔的內容有{Kobe,Bryant,Odom,Derek,Fisher,Ariza,Travor, Lamar,Paul,Jordan,Gasol,Andrew,Famar,Howard,Lebron}。若可能的密 碼如下:TravorTravor,DerekkereD,domO,ArizaazirA,lamarramal,23jordan, Kobe24,Paul33,LebronJames,asolG,ndrewA,amaramar520,HowardHoward, bryantbryant,5566Fish}

(1)假如使用指令"f",上述那些密碼會被 John the Ripper 的字典模式找到

(2)假如使用指令"d",上述那些密碼會被 John the Ripper 的字典模式找到

(3)假如使用指令"{",上述那些密碼會被 John the Ripper 的字典模式找到

(4)若以 John the Ripper 的字典模式破解密碼檔,請寫一個可以搜尋到密碼 "5566fish"的 rule

(5)若以 John the Ripper 的字典模式破解密碼檔,請寫一個可以搜尋到密碼 "amaramar520"的 rule

Ans