

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

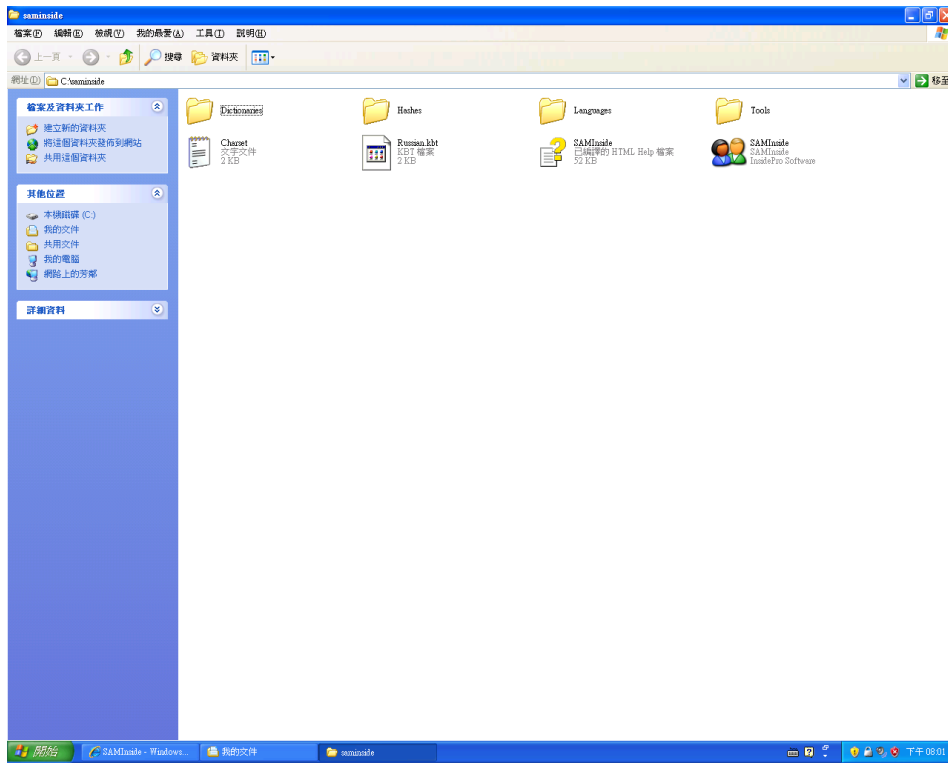
Step 1

開啟瀏覽器，連結至 <http://www.insidepro.com/eng/saminside.shtml> 並選取左上角的 SAMInside Download.

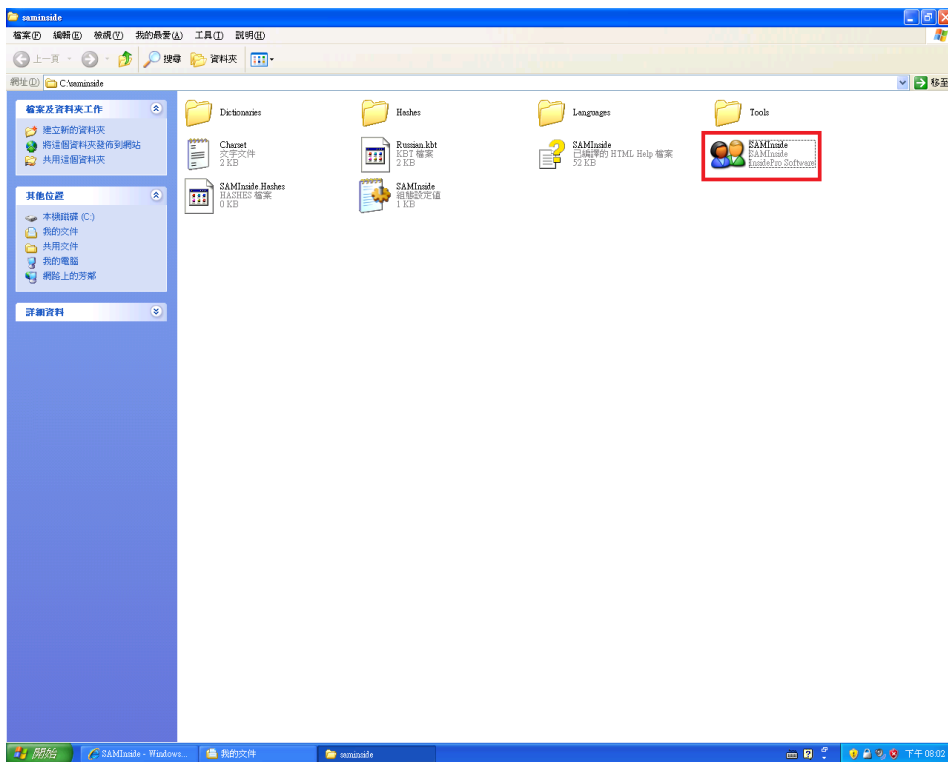
The screenshot shows the SAMInside website in Internet Explorer. The main content area features a table titled "Program Description" with columns for User, RID, LM-Password, NT-Password, LM-Hash, and NT-Hash. The table lists several users, including Administrator, fredc, twoa, william, threaa, and foura. Below the table, it indicates "Users: 7. Passwords found: 3 (42.86%)." and "Current password: JQHXKI".

User	RID	LM-Password	NT-Password	LM-Hash	NT-Hash
<input checked="" type="checkbox"/> BillG	1010	??????A	??????????????	5ECD9236D21095CE...	C04E842B9F5
<input checked="" type="checkbox"/> Administrator	500	??????IS	??????????????	73CC402B03E791756...	C7E262D76C
<input checked="" type="checkbox"/> fredc	1011	??????T	??????????????	3466C2B0487FE9A4...	80030E356D1
<input type="checkbox"/> twoa	1000	AA	aa	89D42444E77140AAA...	C5663434F96
<input type="checkbox"/> william	1012	??????Y	??????????????	D0C5E5CBA8008091...	68669B2E2D2
<input type="checkbox"/> threaa	1001	AAA	aaa	1C3A286D939A1021...	E24106942BF
<input type="checkbox"/> foura	1002	AAAA	aaaa	DCF9CA65DBC2F2DF...	FA5664875FFF

Step 2 將下載下來的檔案解壓縮至 C:\saminside

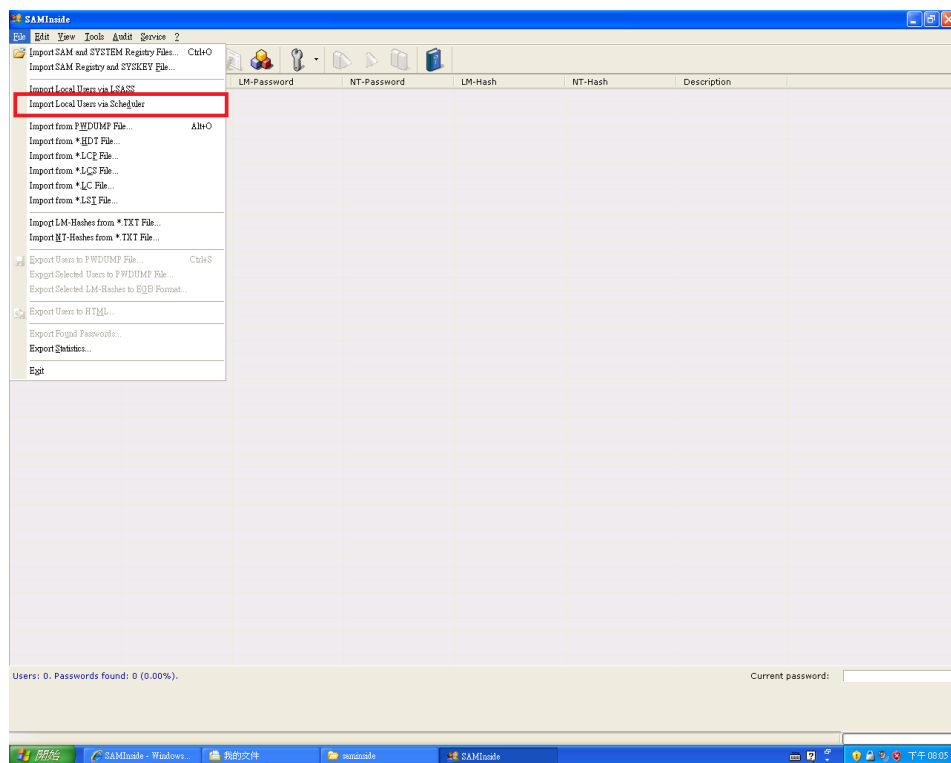


Step 3 執行 SAMInside



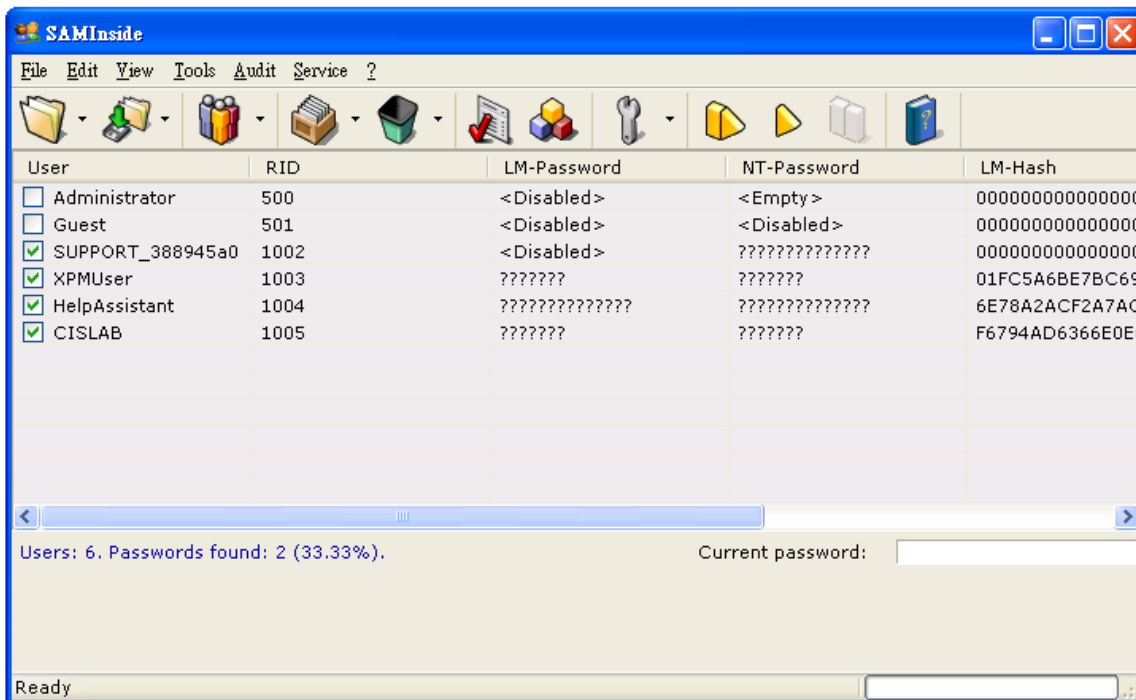
Step 4

Windows\System32\Config\SAM 這路徑下可以找到 Windows 使用者的帳號與密碼檔 SAM，但這檔案我們不能直接開啟，需用 SAMInside 這套軟體來開啟，啟動 SAMInside 後，執行以下的操作



Step 5

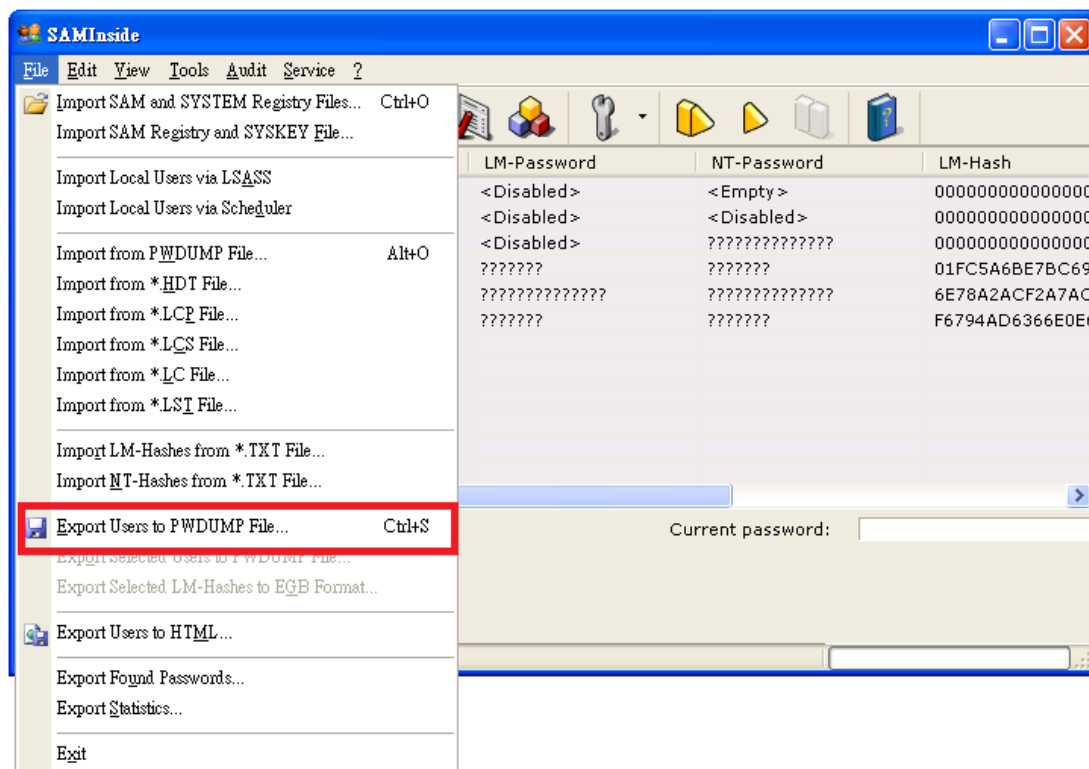
執行後畫面如下:



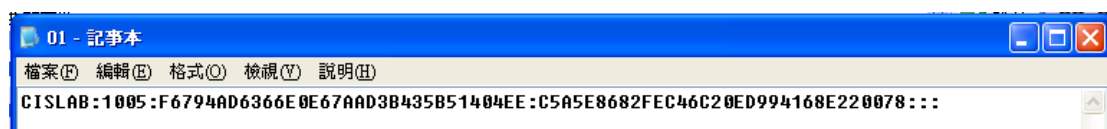
- 視窗中顯示的 User、LM-Password、NT-Password 為 Windows 的帳號與密碼檔
- 以 LM hash 為例，以下為運作方式：

將密碼中的所有小寫字元轉換成大寫。使用 NULL 字元填補密碼，直到密碼的長度正好是 14 個字元，分成各 7 個字元的兩個區塊，使用上述區塊作為 DES 機碼，來加密特定字串。將兩段密碼文字串連成 128 位元的字串，並儲存結果

- 使用者只需按下 File->Export Users to PWDUMP File(Ctrl+S)將這檔案轉存成下列的表格(ex.: 01.txt)，這格式即可使用 John the Ripper 破解工具來破解



匯出後檔案如下:



- 上圖中在把 LM-Hash 及 NT-Hash 欄位的文字轉存成文字檔時，分別為 User、LM-Hash、NT-Hash 及 Description 等對應欄位

2. 安裝 John the Ripper

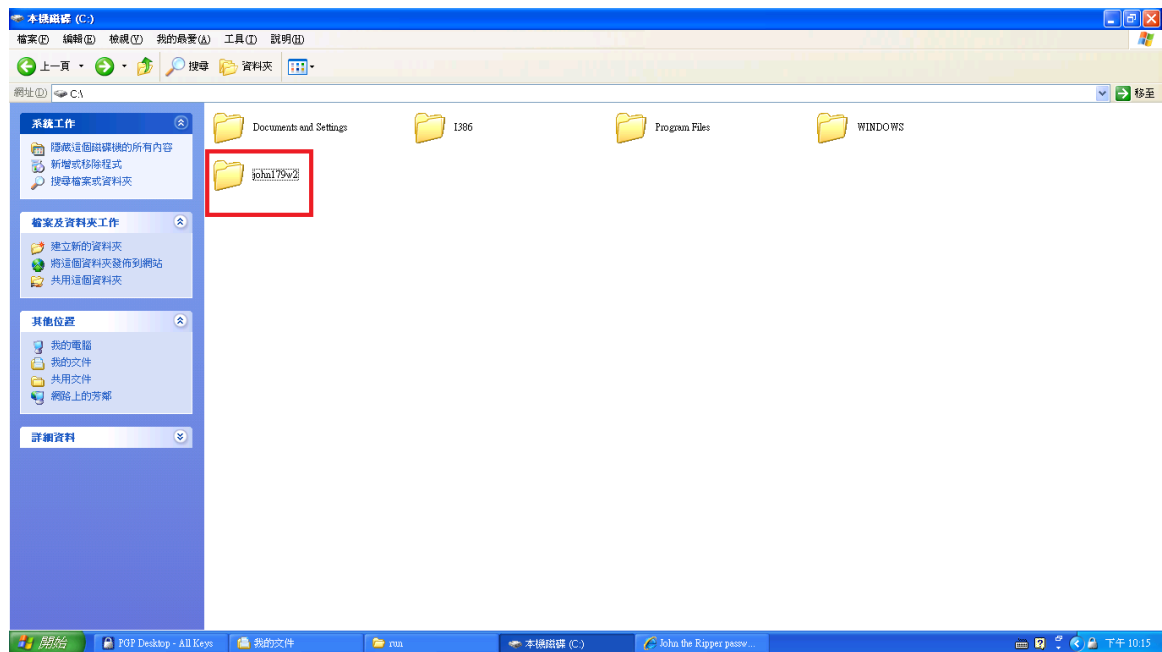
Step 1

開啟瀏覽器，連結至 <http://www.openwall.com/john/> 並選取 John the Ripper 1.7.9 (Windows - binaries, ZIP, 2029 KB)



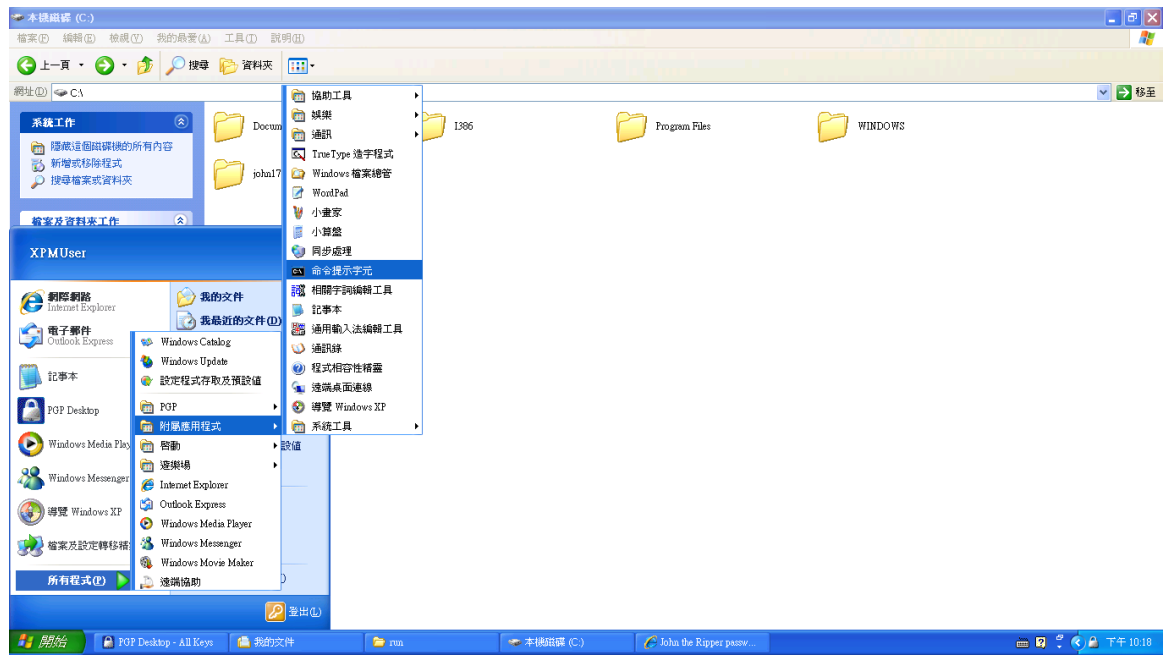
Step 2

將下載下來的檔案解壓縮至 C:\john179w2



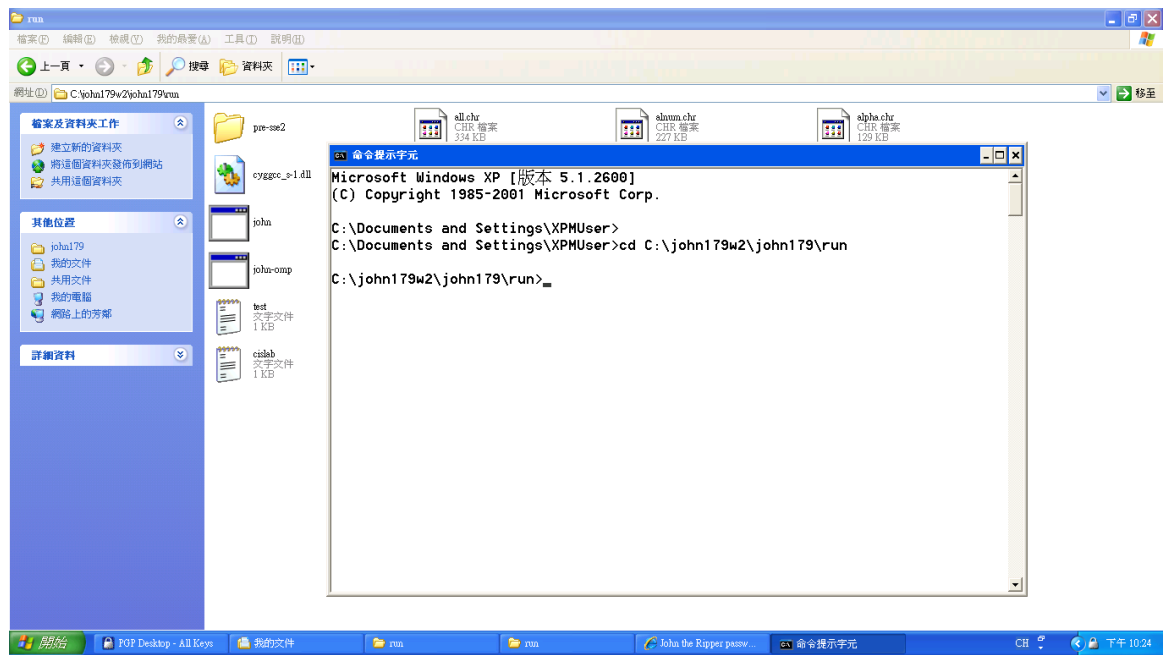
Step 3

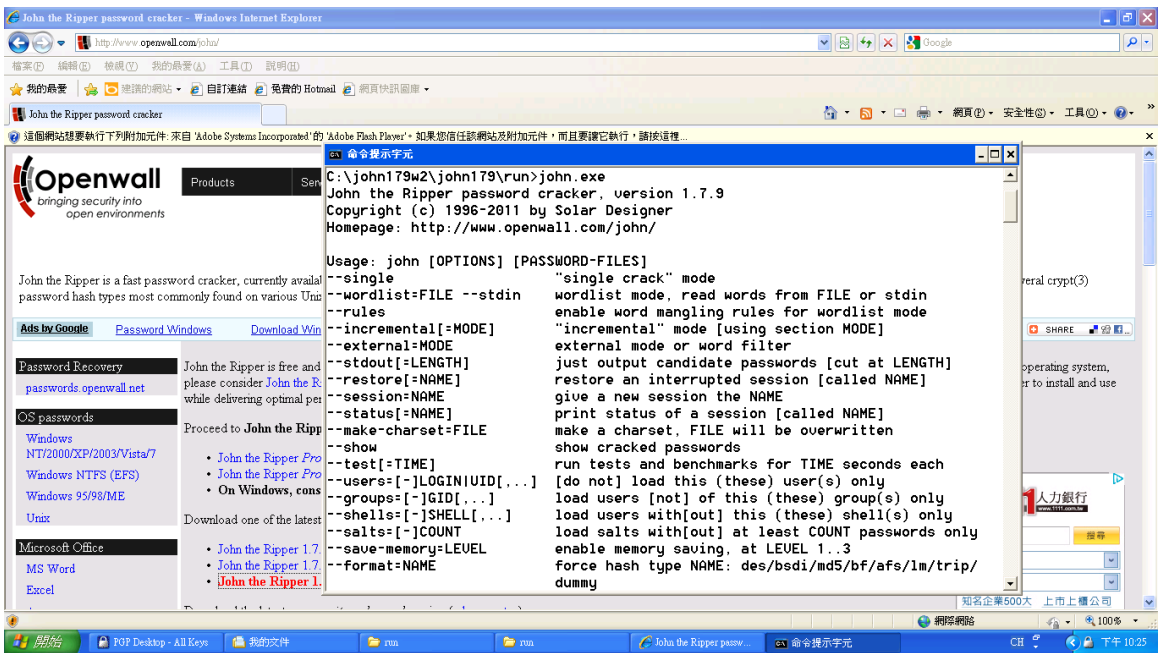
開啟命令提示字元: 開始→更多程式→附屬應用程式→命令提示字元



Step 4

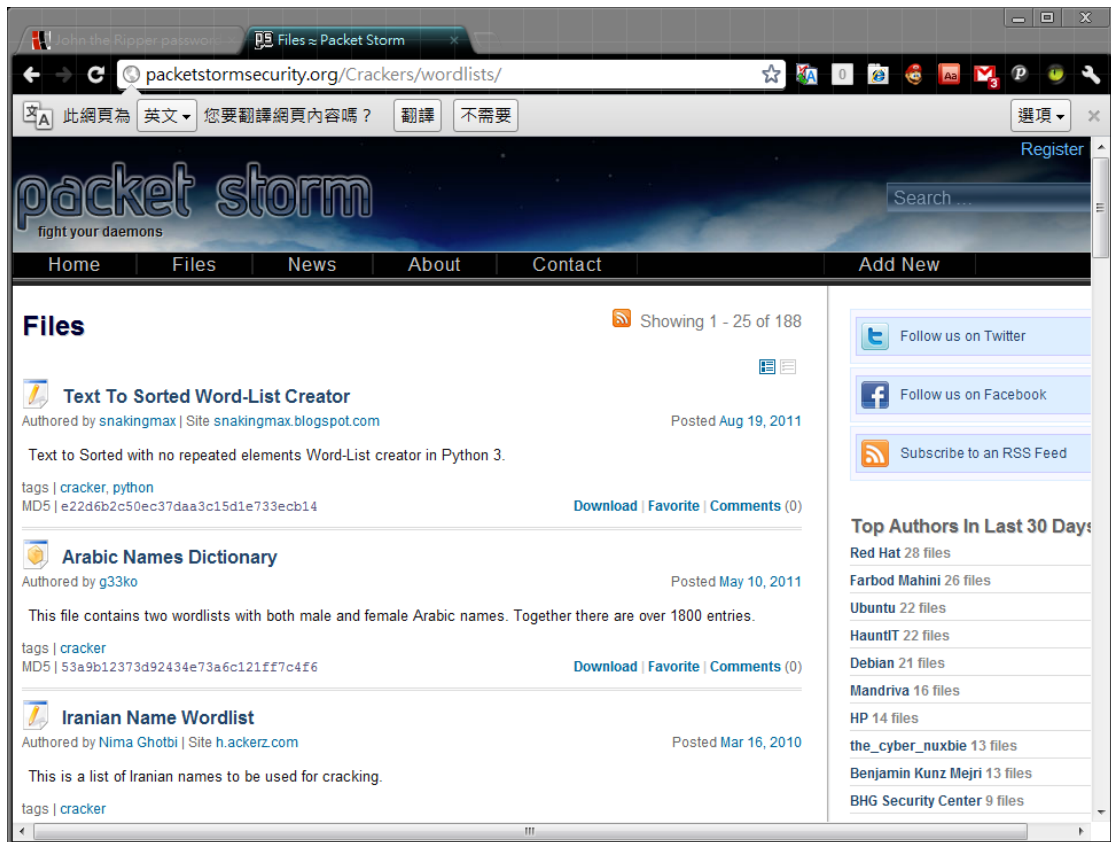
輸入 `cd c:\john179w2\john179\run`(注意: 此路徑為先前解壓縮之路徑, 請確實指向 run 資料夾)



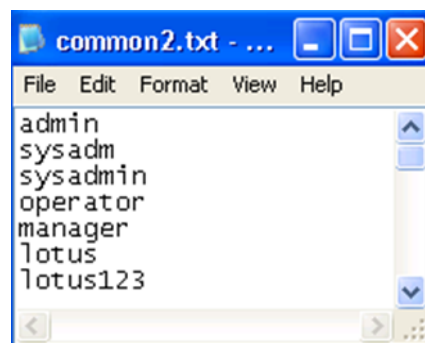
<p>Step 5</p>	<p>輸入 john.exe 查看相關指令說明</p> 
	<ol style="list-style-type: none"> 1. 我們可以用 john [密碼檔.檔名]這簡單的指令來破密，也可以讓 John the Ripper 單獨執行特定的模式來破密 2. 單一解碼模式(Single crack mode) 3. 字典模式(Wordlist mode) 4. 暴力窮舉模式(Incremental mode)
	<p>單一解碼模式</p> <ul style="list-style-type: none"> ● 針對密碼檔的帳號去做字詞變化破解 ● 例如密碼檔內有 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]
	<p>字典模式</p> <ul style="list-style-type: none"> ● 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]

字典檔取得

- 可至 <http://packetstormsecurity.org/Crackers/wordlists/> 抓取別人所建立的字典檔

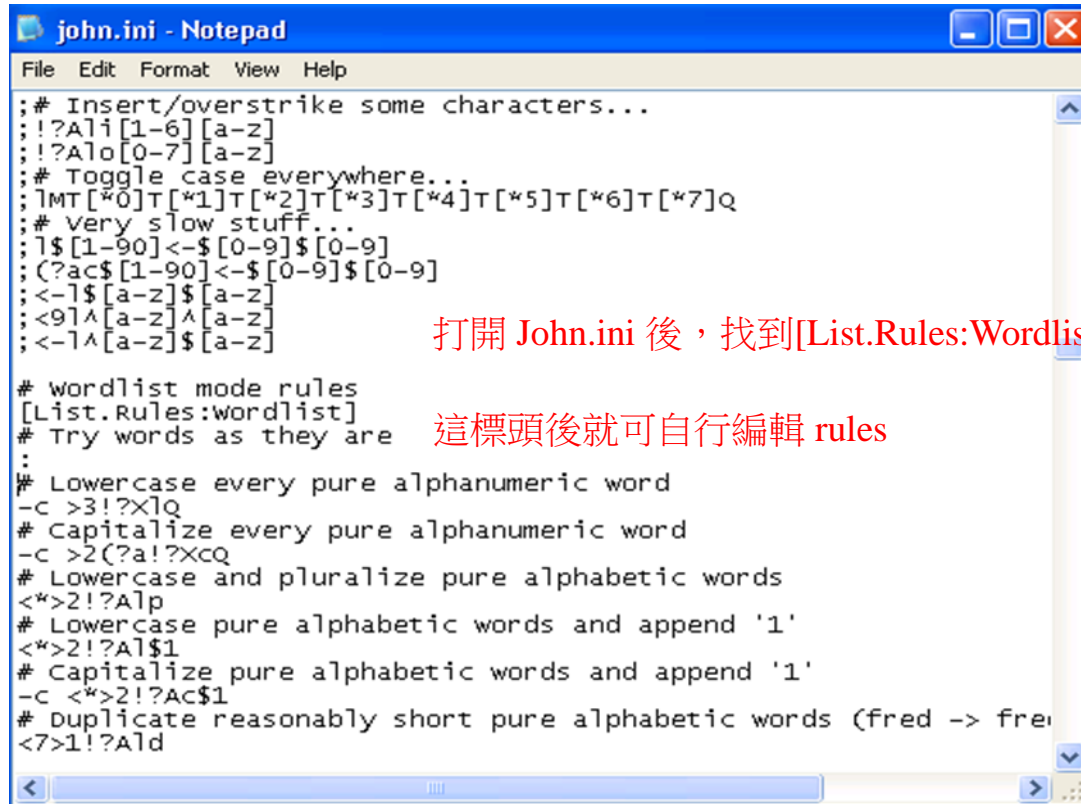


- 也可自行透過記事本編輯，將可能的密碼直接寫到檔案，每個密碼一行即可



字典模式中 rules 的編輯

Wordlist 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 Edit Format View Help
;# Insert/overstrike some characters...
;!?Al[1-6][a-z]
;!?Al[0-7][a-z]
;# Toggle case everywhere...
;!MT[*0]T[*1]T[*2]T[*3]T[*4]T[*5]T[*6]T[*7]Q
;# Very slow stuff...
;l$[1-90]<-$[0-9]$[0-9]
;(?ac$[1-90]<-$[0-9]$[0-9]
;<-l$[a-z]$[a-z]
;<9l^a[a-z]^a[a-z]
;<-l^a[a-z]^a[a-z]

# wordlist mode rules
[List.Rules:wordlist]
# Try words as they are
:
# Lowercase every pure alphanumeric word
-c >3!?!XlQ
# Capitalize every pure alphanumeric word
-c >2(?a!?!XCQ
# Lowercase and pluralize pure alphabetic words
<*>2!?!Alp
# Lowercase pure alphabetic words and append '1'
<*>2!?!Al$1
# Capitalize pure alphabetic words and append '1'
-c <*>2!?!Ac$1
# Duplicate reasonably short pure alphabetic words (fred -> freid)
<7>1!?!AlD
```

打開 John.ini 後，找到[List.Rules:Wordlist]，在

這標頭後就可自行編輯 rules

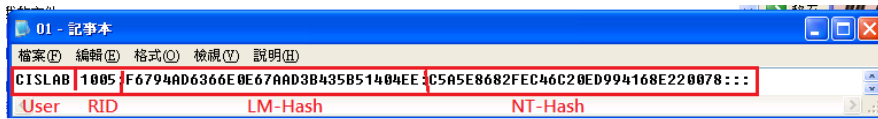
常用指令

- : 對 wordlist 不做任何動作
- C 將字首大寫，如：“crack” -> “Crack”
- c 將字首小寫其餘大寫，如：“Crack” -> “cRACK”
- r 反向，如：“crack” -> “kcarc”
- d 複製，如：“crack” -> “crackcrack”
- f 鏡射，如：“crack” -> “crackkcarc”
- { 往左 shift ，如：“crack” -> “rackc”
- } 往右 shift ，如：“crack” -> “kcrac”
- \$X 在字串後面串接一個字母，如： \$4: “crack” -> “crack4”
- ^X 在字串前面先置一個字母，如： ^4: “crack” -> “4crack”
- <N 字串大小必須大於 N
- >N 字串大小必須小於 N
- (X 只對第一個字是 X 的字串做 rule 的動作
-)X 只對最後一個字是 X 的字串做 rule 的動作
- p 複數，如：“crack” -> “cracks”
- P 過去式，如：“crack” -> “cracked”
- I 現在式，如：“crack” -> “cracking”

	<ul style="list-style-type: none"> - [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”
	<p>暴力窮舉模式</p> <p>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</p> <p>john -i [filename]</p>
	<p>John the Ripper 相關指令</p> <p>強制結束</p> <ul style="list-style-type: none"> - Ctrl^C <p>回復上次工作</p> <ul style="list-style-type: none"> - john -restore <p>在命令視窗顯示 test.txt 破解的結果</p> <ul style="list-style-type: none"> - john -show test.txt <p>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</p>

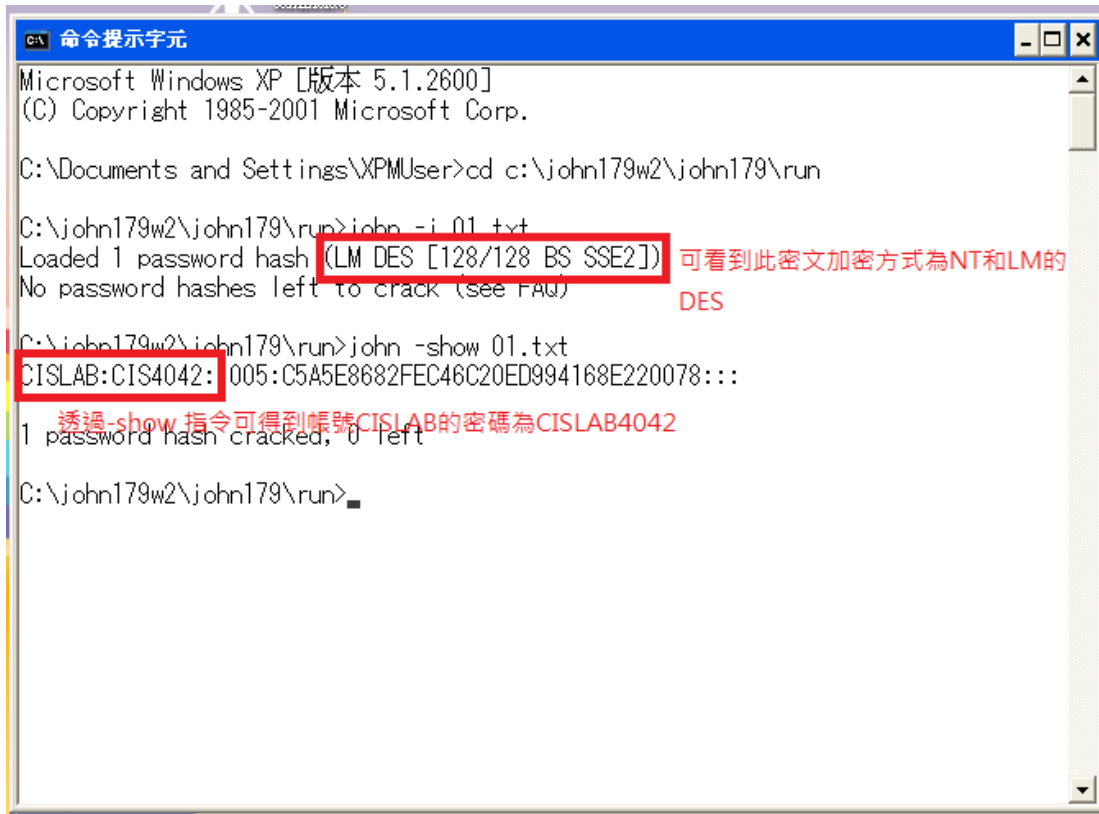
以 John the Ripper 破解 Window XP 密碼

SAMInside 所擷取出的密文貼成文字檔如下



```
01 - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
CISLAB | 1005 | F6794AD6366E0E67AAD3B435B51404EE | C5A5E8682FEC46C20ED994168E220078:::
User      RID      LM-Hash      NT-Hash
```

使用 John the Ripper 破解 windows 密文如下



```
C:\> 命令提示字元
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\XPMUser>cd c:\john179w2\john179\run

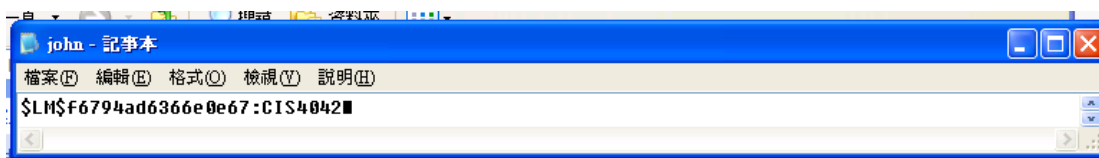
C:\john179w2\john179\run>john -i 01.txt
Loaded 1 password hash (LM DES [128/128 BS SSE2]) 可看到此密文加密方式為NT和LM的
No password hashes left to crack (see FAQ)          DES

C:\john179w2\john179\run>john -show 01.txt
CISLAB:CIS4042:005:C5A5E8682FEC46C20ED994168E220078:::
1 透過-show 指令可得到帳號CISLAB的密碼為CISLAB4042
password hash cracked, 0 left

C:\john179w2\john179\run>
```

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，這裡會記載所有解出的密碼與相對應的密文(如下圖)



```
john - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
$LM$F6794ad6366e0e67:CIS4042
```

問題：

假設一個字典檔的內容有{Kobe, Bryant, Odom, Derek, Fisher, Ariza, Trevor, Lamar, Paul, Jordan, Gasol, Andrew, Famar, Howard, LeBron}。若可能的密碼如下：TrevorTrevor, 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。

(1) 已知用戶**1 的密碼，可能為一男性名字，可利用

<http://packetstormsecurity.org/Crackers/wordlists/> 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, Trevor, Lamar, Paul, Jordan, Gasol, Andrew, Famar, Howard, LeBron}。若可能的密碼如下: TrevorTrevor, 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