忘記密碼不再煩惱

我們使用電腦的時候，經常會遇到一些尷尬的事情，而最嚴重的莫過於忘記了登陸密碼，這時候有條件的用戶會把他的硬碟當作從盤挂在其他的系統下，將重要的資料拷貝出來，那沒有條件的用戶只能無可奈何重裝系統？？答案是"不"!下面我就向大家介紹一款修改登陸密碼的利器：Offline NT Password & Registry Editor.

Offline NT Password & Registry Editor.是一個免費軟體，是由國外的編程愛好者開發出來的，我先向大家介紹這個軟體的安裝及使用方法，之後我會簡單介紹它的工作原理。

下載 Offline NT Password & Registry Editor

您可以從 http://home.eunet.no/~pnordahl/ntpasswd/官方網站下載最新版本的 Offline NT Password & Registry Editor，它會有三個下載提供：bd040818.zip，cd040818.zip，sc040818.zip,其中 bd040818.zip 是針對打算使用的用戶，cd040818.zip 是針對打算使用光碟作？該工具載體的用戶，sc040818.zip 則是？使用軟碟作？載體且使用的是 SCSI 硬碟的用戶提供 SCSI 驅動。在這裏我主要介紹如何使用軟碟作？該工具載體,其他情況的用戶可以參考官方的幫助文件。

安裝 Offline NT Password & Registry Editor

首先在用 WINRAR 或 WINZIP 將 bd040818.zip 解壓，它會生成名？ bd040818 的文件夾，內有三個文件 bd040818.bin，install.bat，rawrite2.exe.我們雙擊 install.bat，會自動打開一個執行視窗，顯示：

RaWrite 2.0 - Write disk file to raw floppy diskette

Enter target diskette drive:

選擇您的軟盤機的盤符，如果是 a,就輸入 a,是 b 就輸入 b，然後回車，接下來顯示：

Please insert a formatted diskette into drive A: and press -ENTER- :

插入一張格式化過的空白軟碟後回車，它會自動進行安裝。以下是安裝過程的顯示：

Number of sectors per track for this disk is 18

Writing image to drive A:. Press ^C to abort.

Track: 79 Head: 1

Done.

Done!

To run Offline NT Password and Registry Editor, leave the floppy in the drive an

d reboot.

Press any key to continue . . .

到這裏安裝就結束了。

使用 Offline NT Password & Registry Editor

將安裝好的軟碟插入您忘記密碼的主機的軟盤機內，開機進入 BIOS,設置軟盤機？第一啟動設備。然後保存重？。重？後軟碟會自動引導到一個 linux 環境下，對 linux 不熟悉的朋友也不用驚慌，這裏只需要您作簡單的選擇和輸入就可以了。首先第一個選擇是：

```
============================================================
. Step ONE: Select disk where the Windows installation is
============================================================
Disks:
/dev/ide/host0/bus0/target0/lun0/disc: NT partitions found:
1:          /dev/ide/host0/bus0/target0/lun0/part1 10001MB Boot
2:          /dev/ide/host0/bus0/target0/lun0/part2 80003MB
Please select partition by number or
a = show all partitions, d = load new disk drivers
l = relist NTFS/FAT partitions, q = quit
Select: [1]
```

這裏“/dev/ide/host0/bus0/target0/lun0/part1 10001MB Boot”代表您的 C 盤，也就是安裝 windows 的地方。“/dev/ide/host0/bus0/target0/lun0/part2 80003MB”代表您的 D 盤，我們這裏應該選擇 1,簡單的說您看哪個選項後有 Boot 的，就選哪個。選擇後回車進入下一個畫面：

```
============================================================
. Step TWO: Select PATH and registry files
============================================================
What is the path to the registry directory? (relative to windows disk)
[windows/system32/config] :
```

這裏是讓您選擇 SAM 文件所在的路徑，這個文件裏是放置的是加密過的用戶所有重要資訊。Winxp 下它的路徑？ windows/system32/config，Win2000 下它的路徑？ winnt/system32/config,這裏程式會根據您的作業系統自動確定路徑，所以您直接回車確認即可。進入下一個畫面：

```
-r--------  1 0  0  262144 Jan 12 18:01 SAM
-r--------  1 0  0  262144 Jan 12 18:01 SECURITY
-r--------  1 0  0  262144 Jan 12 18:01 default
-r--------  1 0  0  8912896 Jan 12 18:01 software
-r--------  1 0  0  2359296 Jan 12 18:01 system
dr-x------  1 0  0  4096 Sep  8 11:37 systemprofile
-r--------  1 0  0  262144 Sep  8 11:53 userdiff
```

Select which part of registry to load, use predefined choices
or list the files with space as delimiter
1 - Password reset [SAM system security]
2 - RecoveryConsole parameters [software]
q - quit - return to previous
[1] :

這裏顯示的是 windows/system32/config 下的文件，因? 我們的目的是重新設置登陸密碼，所以應該選擇 1,因? 預設值是 1,所以直接回車，進入下一個畫面：

<>========<> chntpw Main Interactive Menu <>========<>

Loaded hives: <SAM> <system> <security>

1 - Edit user data and passwords
2 - Syskey status & change
3 - RecoveryConsole settings
- - -
9 - Registry editor, now with full write support!
q - Quit (you will be asked if there is something to save)

What to do? [1] ->

這裏顯示的是該軟體的主功能表，除了更改密碼以外，我們還可以對 SAM 文件進行一些編輯。這裏我們選擇 1,因? 預設值是 1,所以直接回車，進入下一個畫面：

===== chntpw Edit User Info & Passwords ====

RID: 01f4, Username: <Administrator>
RID: 01f5, Username: <Guest>, *disabled or locked*
RID: 03e8, Username: <HelpAssistant>, *disabled or locked*
RID: 03eb, Username: <test>, *disabled or locked*
RID: 03ea, Username: <SUPPORT_388945a0>, *disabled or locked*

Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator]

這裏顯示的是您的系統所有用戶的一些資訊，我們可以看到這個系統內有五個用戶，用戶名分別？：Administrato，Guest，HelpAssistant，test，SUPPORT_388945a0，其中 Administrator ，Guest ，HelpAssistan，SUPPORT_388945a0？系統自動? 生的用戶，test？自己創建的用戶，我們只要獲得有最高許可權的 Administrator 用戶密碼就可以了，因? 預設值是就是

Administrator,所以直接回車，進入下一個畫面：

RID : 0500 [01f4]
Username: Administrator
fullname:
comment : Built-in account for administering the computer/domain
homedir :

Account bits: 0x0210 =
[ ] Disabled | [ ] Homedir req. | [ ] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account | [ ] NMS account |
[ ] Domain trust ac | [ ] Wks trust act. | [ ] Srv trust act |
[X] Pwd don't expir | [ ] Auto lockout | [ ] (unknown 0x08) |
[ ] (unknown 0x10) | [ ] (unknown 0x20) | [ ] (unknown 0x40) |

Failed login count: 0, while max tries is: 0
Total login count: 3

* = blank the password (This may work better than setting a new password!)
Enter nothing to leave it unchanged
Please enter new password:

這裏是顯示的是 Administrator 的註冊表資訊，我們不需要關心它。最後一行是要您輸入您的 Administrator 用戶的新密碼，我們看到有這？一句話：* = blank the password (This may work better than setting a new password!)，這裏要作一個說明：筆者經過多次實驗發現如果您設置一個新的密碼，它根本不起作用，登陸時還是會提示密碼錯誤，而您如果輸入*，即表示設置密碼？空，則登陸時不用輸入密碼直接回車就可以成功的進入系統。造成的這個現象的原因後面我會詳細說明。所以我們輸入*,讓它？空密碼,回車，進入下一個畫面：

Blanking password!

Do you really wish to change it? (y/n) [n]

這裏是讓您確認變更，我們輸入 y,回車，進入下一個畫面：

Changed!

Select: ! - quit, . - list users, 0x - User with RID (hex)
or simply enter the username to change: [Administrator]

這裏是讓您選擇更改其他用戶的密碼，我們不打算更該其他用戶所以輸入!,回車，回到主功能表：

<>========<> chntpw Main Interactive Menu <>========<>

Loaded hives: <SAM> <system> <security>

1 - Edit user data and passwords
2 - Syskey status & change
3 - RecoveryConsole settings
- - -
9 - Registry editor, now with full write support!
q - Quit (you will be asked if there is something to save)

What to do? [1] ->

這裏我們選擇 q 退出主功能表，進入下一個畫面

Hives that have changed:
Name
0 - OK

==========

. Step FOUR: Writing back changes

==========

About to write file(s) back! Do it? [n] :

如果您想放棄以前的操作，那這裏是最後一次機會。如果您選擇 y 那？所有的變更會寫入文件中，我們選擇 y 後回車。

Writing SAM

NOTE: A disk fixup will now be done.. it may take some time

Mounting volume... OK

Processing of $MFT and $MFTMirr completed successfully.

NTFS volume version is 3.1.

Setting required flags on partition... OK

Going to empty the journal ($LogFile)... OK

NTFS partition /dev/ide/host0/bus0/target0/lun0/part1 was processed successfully.
NOTE: Windows will run a diskcheck (chkdsk) on next boot.
NOTE: this is to ensure disk intergity after the changes

***** EDIT COMPLETE *****

You can try again if it somehow failed, or you selected wrong
New run? [n] : n

到這裏所有的步驟就結束了，它會再次提醒您是否有什？選擇錯誤的地方，如果有那就要把以上的動作再作一遍，我們確定沒有問題就選擇 n，回車，結束所有操作，然後取出軟碟並重？系統。

在登陸畫面中的用戶名一欄中輸入 Administrator，密碼不輸，直接回車。您會驚喜的發現，您成功的進入了系統。

Offline NT Password & Registry Editor 的基本原理

現在我簡單的解釋一下它的工作原理。在每一個 NT 作業系統下都會有一個叫 SAM 的文件(Winxp 下它的路徑？ windows/system32/config，Win2000 下它的路徑？ winnt/system32/config,). SAM文件即System Administration Manager---系統管理員程式。所有用戶的登錄名及口令等相關資訊都會保存在這個文件中。當我們登錄系統的時候，系統會自動地和 SAM 校對，如發現此次密碼和用戶名與SAM文件中的加密資料符合時，您就會順利登錄;如果錯誤則無法登錄。Offline NT Password & Registry Editor 就是通過直接修改 SAM 文件中的加密資料來達到目的的。

想更改SAM文件中的資料，我們就必須要先知道SAM文件中的資料結構資訊，因？MicroSoft從來沒有公開過相關的內容，所以這是個難點，幸運的是目前已經有一個德國高人B.D基本上確定這個文件的大部分registry structure資訊，如下：

```
/* This contains some policy settings for the account database */
struct accountdb_F
/* This is users F value, contains account type & state etc */
struct user_F
/* This is Users V data struct , contains password settings & state etc */
struct user_V
```

其中最重要的密碼資訊是在user_V中的，分別是：

```
int ntpw_ofs;           /* 0xa8 */
int ntpw_len;           /* 0xac */
```

ntpw_ofs放置的是加密密碼的偏移位址， ntpw_len放置的是加密密碼長度。我們

就是要通過修改這兩個變數的值來到達我們的目的。但是我們要知道這些資訊是經過加密的。這又是一個難點，讓我們首先看看一個明文密碼被加密過程：
首先輸入明文密碼
然後轉換明文密碼？UNICODE格式
再根據上一步得到的UNICODE string 製作出一個MD4 hash
最後根據DES這個資料加密標準加密MD4 hash,並且用userid(SID)的低位元元部分(RID)作？該資料的key值，然後把該資料放入V struct中。
我們要生成一個新密碼就必須嚴格按照這個步驟來進行，程式裏是通過這？幾個函數完成的：

```
/*轉換明文密碼？UNICODE格式*/
cheap_ascii2uni(newp,newunipw,pl);
/*根據上一步的UNICODE string 製作出一個MD4 hash*/
MD4Init (&context)
MD4Update (&context, newunipw, pl<<1);
MD4Final (digest, &context);
/*根據DES這個資料加密標準加密MD4 hash, */
des_ecb_encrypt((des_cblock *)digest,(des_cblock *)despw, ks1,
DES_ENCRYPT);
des_ecb_encrypt((des_cblock *)(digest+8),(des_cblock *)&despw[8], ks2,
DES_ENCRYPT);
```

但是遺憾的是,該程式的加密演算法同 Microsoft 的演算法似乎有些不同，舉例來說：我用這個軟體生成了 Administrator 用戶的一個新的密碼 123456,程式加密後的最終資料是：abcdefgh,並且將這個資料存入 SAM 文件中。但是當我在登陸視窗上輸入用戶名 Administrator，密碼 123456 時, Microsoft 用它的加密演算法得到的最終資料？ abcdabcd，顯然和 SAM 中對應資料 abcdefgh 是不一致的，所以導致最終登陸失敗。問題就出在程式的加密演算法和 Microsoft 的加密演算法是不同的。

不過不要緊，我們還記得有兩個重要變數：

```
int ntpw_ofs;          /*  0xa8  */
int ntpw_len;          /*  0xac  */
```

既然我們修改 ntpw_ofs 內容的嘗試失敗了，我們可以把修改 ntpw_len 作？解決問題的切入口，這裏就非常很簡單了。我們只要通過給 ntpw_len 賦值？ 0 來欺騙 SAM，告訴它密碼的長度？ 0，即密碼？空，那？就不再存在密碼加密的問題了，直接回車即可。程式裏是這樣完成的：

```
V->ntpw_len=0;
```

小結

目前更改登陸密碼的軟體有很多，不免讓人眼花繚亂，而今天介紹的這款軟體不敢說是最好的，但也說的上是其中的僥僥者，除了使用上非常方便有效外，還有一點：它是完全免費的。也許從今天起，你不會再擔心自己忘掉密碼該怎?辦，而是轉而擔心別人會不會改掉自己的密碼了。^_^

作者簡介

姓名：雷凱
工作單位：升技主板(蘇州)研發中心
聯繫地址：蘇州市新區馬運路羅禮科技有限公司研發中心 郵編 215000
E-mail: tigerleihm@yahoo.com.cn
“ 本文作者是雷凱 升技主板(蘇州)研發中心工程師。他目前在中國蘇州 升技主板(蘇州)研發中心工作。可以通過 tigerleihm@yahoo.com.cn 與他聯繫。 ”