

第七章

入侵系統

入侵系統

入侵系統包含了幾個重要的動作：

- 破解密碼
- 提升權限
- 執行應用程式
- 隱藏檔案
- 掩蓋軌跡

密碼的組成

密碼組成的基本元件：

(1) 字元，A、B、C、D、a、b、c、d等。

(2) 數字，由0到9。

(3) 特殊符號，@、_等。

密碼的組成

這幾個元件組合而成的密碼，可以是：

- (1) 只有字元，例如：john。
- (2) 只有數字，例如：1314、8879576。
- (3) 只有特殊符號，例如：@#!!!。
- (4) 字元及數字組合，例如：john1234。
- (5) 字元與特殊符號組合，例如：john@home。
- (6) 數字與特殊符號組合，例如：@1234@。
- (7) 字元、數字與特殊符號組合，例如：John@1234。

強密碼 (Strong Password)

■ 讓攻擊者不容易破解成功的密碼稱為強密碼。

下面的規則可以建立強密碼：

- (1) 密碼不能包含帳號名稱的部份或者是全部。
- (2) 必須最少要八個字元。
- (3) 密碼中要包含符號、數字、大寫及小寫字元。

中文鍵盤產生強密碼

- 利用中文輸入法的特性。
- 例如：姓名「陳」「大」「維」，利用注音鍵盤但是不要切換到中文，就變成按下「tp6」「284」「jo6」，中間再用特殊符號連接，就變成「tp6+284+jo6」。
- 不同的中文輸入法會產生不同的密碼組合。

測試密碼是否為強密碼

- Password Checker1
(<http://www.passwordmeter.com/>)
- Password Checker2
(<https://howsecureismypassword.net/>)
- Password Checker3
(<https://blog.kaspersky.com/password-check/>)

密碼攻擊

■ 密碼的的攻擊方式有四種：

- (1) 被動線上攻擊。
- (2) 主動線上攻擊。
- (3) 離線攻擊。
- (4) 非技術性攻擊。

被動線上攻擊

- 線上嗅探：通常會改動實體線路，但是不需要去偵測受害者，受害者也不容易發覺，直接在網路上進行存取及記錄原始的網路流量，一直等到流量資料中出現認證的序列，就可以將其中的帳號及密碼提取出來。
- Man-in-the-Middle (MITM)：就是攻擊者借用工具程式，使受害者與伺服器端的資訊都會經過攻擊者的電腦，攻擊者收集的資料可以即時或事後進行破解密碼的動作。
- Replay攻擊：利用MITM的方法，擷取客戶端與伺服器端之間的認證序列，但是攻擊者並不破解密碼，等到將來要使用時，直接將這個認證序列送出即可完成認證程序，登入伺服器。

主動線上攻擊

- 這種方法其實就是「密碼猜測」，我們可以假設管理者用了一個非常糟的密碼設定，只要花一些時間，就有可能將密碼測試出來。
- 懶散的管理者可能會用admin，administrator、systemadmin...當做帳號，密碼可能用生日、分機號碼、英文名字...。
- 此種攻擊方式容易被察覺，因為在系統的記錄檔中會發現大量登入失敗的資訊。

離線攻擊

(1) 字典攻擊法

(2) 暴力攻擊法

(3) 混合攻擊法

非技術性攻擊

- 社交工程
- 背後偷窺
- 鍵盤監聽

手動攻擊與自動攻擊

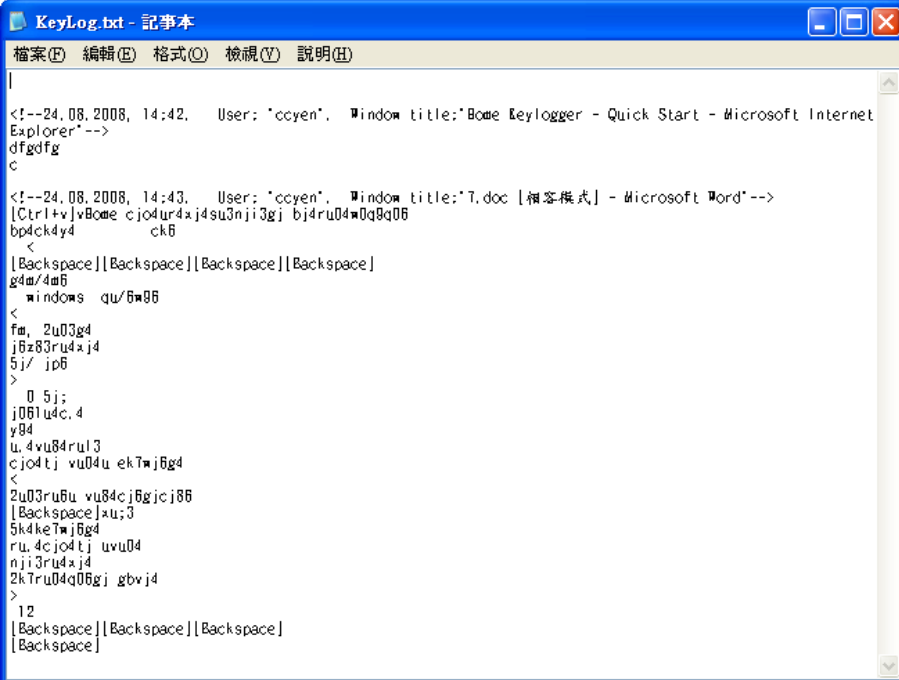
- 手動攻擊使攻擊者以手動方式，輸入帳號與密碼，如果不成功，就換下一個，手動攻擊通常會準備一個單字列表，列表嘗試完畢就不再輸入。
- 自動攻擊則是攻擊者必須先看看目標系統密碼加密的方法，然後利用工具程式自動進行輸入測試。

工具程式

■ Home Keylogger

■ Home Keylogger 會記錄你所輸入鍵盤的任何字，適用於 Windows 平台，缺點是無法記錄中文

○



```
KeyLog.txt - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

|
<!--24, 08, 2008, 14:42, User: 'ccyen', Window title: 'Home Keylogger - Quick Start - Microsoft Internet Explorer'-->
dfgdfg
c
<!--24, 08, 2008, 14:43, User: 'ccyen', Window title: '7.doc [相容模式] - Microsoft Word'-->
[Ctrl+v]vBome cjo4ur4xj4su3nji3gi bj4ru04m0q8q06
bp4ck4y4 ck6
<
[Backspace][Backspace][Backspace][Backspace]
g4m/4m6
<
windows qu/6m86
<
fm, 2u03g4
j6z83ru4xj4
5j/ jp6
>
 0 5j;
j061udc, 4
y94
u, 4vu84ru13
cj04tj vu04u ek7mj6g4
<
2u03ru6u vu84cj6gicj86
[Backspace]xu;3
5k4ke7mj6g4
ru, 4cjo4tj uvu04
nji3ru4xj4
2k7ru04q06gij gbvj4
>
 12
[Backspace][Backspace][Backspace]
[Backspace]
```

工具程式

■ ERD Commander 2005 Boot CD

- 利用ERD2005可以強行修改系統管理員密碼，方法簡單又易於操作，且在Windows 2000/XP/2003系統下均有效，這個工具應該算是線上攻擊的工具。

ERD Commander 2005 Boot CD

1. 下載ERD2005，解壓後將其映像檔燒成光碟。
2. 將主機改成以光碟啟動。
3. 重新開機，進入ERD2005桌面。
4. 接下來是最關鍵的一步：按「Start」，接著選「System Tools」，再選「Locksmith」，就進入修改密碼的介面，接下來的對話框中輸入修改密碼的用戶名（選擇Administrator），最後輸入密碼，然後按下NEXT。
5. 按下「Finish」之後就重新啟動，密碼就被修改完畢。

防止密碼遭入侵的對策

1. 伺服器使用加密傳輸。
2. 不要使用預設的密碼。
3. 不要使用字典中可以找到的密碼。
4. 不要使用關於興趣、寵物或生日...。
5. 使用至少8 ~ 12字的密碼。
6. 每三十天改變密碼一次。
7. 監督系統的Log。
8. 不輕易讓不相干的人員靠近重要的機器。
9. 使用防止鍵盤側錄的程式。
10. 使用偵測軟體檢查系統。

工具程式

■ Anti Keylogger Shield

- 是一個防止鍵盤側錄的防護程式，程式本身並不需要進行更新或掃描的動作，但是可以讓鍵盤側錄程式都失效。



提升權限

- 將一般使用者的帳號權限提升成為管理者的權限。
- 通常攻擊者會設法先取得一般使用者的帳號，使用者帳號的權限比較低，但是有可能可以提升到管理者的階層。

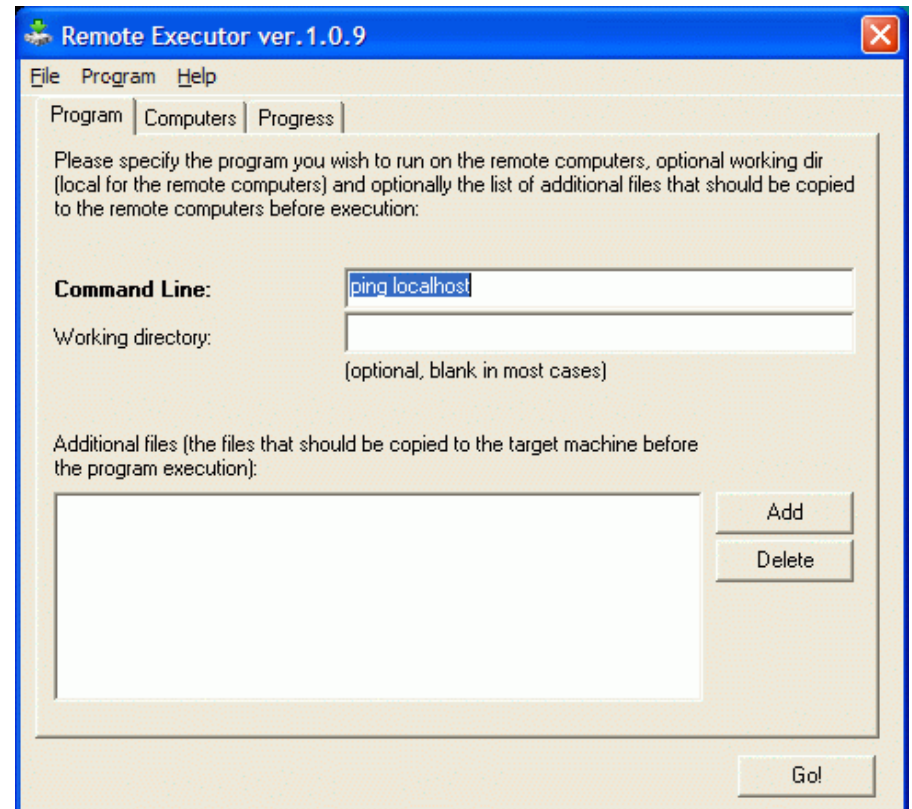
執行應用程式

- 當攻擊者取得管理者的權限後，接下來就是要在目標系統上執行應用程式。
- 執行應用程式的目的，可能是為了安裝「後門程式」、「鍵盤側錄」，也可能僅僅是為了複製檔案或破壞系統。

工具程式

■ Alchemy Remote Executor

- 是一個系統管理工具，可以讓系統的管理者在遠端網路的電腦上執行程式，同樣的如果是攻擊者擁有了密碼，也可以在遠端進行操作。



隱藏檔案

- 攻擊者安裝完應用程式後，可能會想要隱藏這些檔案，有兩種方法可以隱藏這些檔案：
 1. 使用 `attrib` 命令
 2. 使用 NTFS 檔案串流

attrib命令

1. 在Windows XP中，按「開始」及「執行」，輸入cmd按下Enter，這時會開啟命令視窗。輸入notepad test.txt按下Enter，將會使用記事本開啟檔名test.txt檔案，在記事本中隨便輸入一些文字然後存檔，並關閉記事本。
2. 輸入dir按下Enter，可以看到test.txt這個檔案。
3. 輸入attrib +h test.txt。
4. 輸入dir按下Enter，test.txt這個檔案不見了。

NTFS檔案串流

1. 在Windows XP中，按「開始」及「執行」，輸入cmd按下Enter，這時會開啟命令視窗。輸入notepad test.txt按下Enter，將會使用記事本開啟檔名test.txt檔案，在記事本中隨便輸入一些文字然後存檔，並關閉記事本。
2. 輸入dir可以看到這個檔案。
3. 在視窗中輸入notepad test.txt:hidden.txt並按下Enter。在記事本中隨便輸入一些文字然後存檔，並關閉記事本。
4. 輸入dir按下Enter，步驟三製造的檔案不會顯示。使用type test.txt:hidden.txt會出現錯誤訊息，但是再輸入notepad test.txt:hidden.txt檔案內容卻還在。
5. 輸入rm test.txt把test.txt刪除，再輸入notepad test.txt:hidden.txt，可以發現前面步驟三輸入的檔案不見了。

掩蓋軌跡

- 就是將所有攻擊過程中產生的痕跡予以消除，以免被偵測或檢查出在系統上曾經有攻擊者的存在。
- 攻擊者通常會刪除系統的訊息或與安全有關的事件記錄，這些記錄又可稱為日誌檔。

清除作業系統日誌檔

檢視Windows系統中的日誌檔：

執行「開始」→「設定」→「控制台」→「系統管理工具」→「事件檢視器」。

■ 主要有三項：

1. 應用程式日誌檔。
2. 安全性日誌檔。
3. 系統日誌檔。

工具程式

■ **elsave**

■ 語法：`elsave [-s \\伺服器主機] [-l log] [-F file] [-C] [-q]`

■ 如果要刪除遠端機器的應用程式日誌檔，命令格式如下：

```
elsave -s \\192.168.0.77 -l "application" -C
```

■ 同樣的要刪除安全性日誌檔和系統日誌檔，就在 `-l` 參數後面接著輸入「`security`」或「`system`」。

工具程式

■ clearlogs

語法：clearlogs [\\電腦名稱] <-app / -sec / -sys>

- 這裡的 -app 就是應用程式日誌檔， -sec 就是安全性日誌檔， -sys 就是系統日誌檔。

清除 IIS 日誌檔

- IIS 的日誌檔保存在

`%systemroot%\system32\logfiles\`下。

- 如果啟動了 IIS，就會在上述路徑下多出一個 W3SVC1 的資料夾，這就是用來儲存 web 的服務日誌檔的地方。
- 如果啟動了 IIS 內建的 FTP 服務，那麼還會多出一個 MSFTPSVC1 的資料夾，裡面放的就是 FTP 的日誌檔。

工具程式

■ cleaniis

`cleaniis c:\winnt\system32\logfiles\w3svc1\ 10.10.1.1`

就是清除IIS log中10.10.1.1此IP位址的所有訪問記錄。

`cleaniis c:\winnt\system32\logfiles\w3svc1\ /admin/`

就是清除IIS log中所有對/admin/此目錄的訪問記錄。

練習

- 寫出三組密碼，證明它們是強密碼，而且要「好記不易忘」。
- 使用中文輸入鍵盤及你的姓名，產生出一組密碼，並且輸入到微軟的測試網站，證明它是強密碼。