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/passwordcheck/)

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。

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。



### (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

<pre>檔案(P) 編輯(E) 格式(Q) 檢視(Y) 說明(H)  </pre> (24, 05, 2005, 14;42, User; 'coyen', Window title; Bome Leylogger - Quick Start - dicrosoft Internet Explorer'> dfgdfg C  (24, 05, 2005, 14;43, User; 'coyen', Window title; T, doc [相念集式] - dicrosoft Word'> [Ctrl+V]vBome cjodurdajdsu3nji3gj bjdruD4mDd9006 bpdckdy4 ck6 [Backspace][Backspace][Backspace][Backspace] gdar/daf6 windows qu/6m96 fm, 2u03g4 jbz33ru4xi4 5// jp6 D 5;; jD6Tudc,4 y94 L 4vu84ru13 cjodtj vu04u etTmj6g4  2u03ru6u vu84cj6gicj686 [Backspace]au;3 StdeTmj6g4 zharu04q06gj gbvj4 > 12	🖡 KeyLog.txt - 記事本	$\mathbf{X}$
<pre>(!24.08.2008, 14:42. User: 'coyen'. Window title:'Bome Keylogger - Quick Start - Hicrosoft Internet Explorer'&gt; dfgdfg C (!24.08.2008, 14:43. User: 'coyen'. Window title:'T.doc [4W\$:44:4] - Hicrosoft Word'&gt; [Ctrl+v]vBome cjodurdajdsu3nji3gj bjdru004w0098006 bodck4y4 ck6 (Backspace][Backspace][Backspace][Backspace] gdar/du6 windows qu/6w98 ( fm, 2003g4 jbz83ru4xi4 5)/ jp6 D 5;; jD6]udc.4 y84 u.dvu84ru13 cjodtj vu04u ekTwj6g4 ( 2u03ru6u vu84cj6gjcj86 [Backspace]xu;3 StAteTwj6g4 ru.dcjodtj uvu04 nji3ru4xj4 2kTru04q06gj gbvj4 &gt; 12</pre>	檔案 (E) 編輯 (E) 榕式 (Q) 檢視 (Y) 說明 (E)	
<pre><!--24.08.2008, 14:43. User: 'ccyen'. Windom title:'7.doc [福客株式] - Wicrosoft Word'--> [Ctrl+ylyBome cjodur4xjdsu3nji3gj bjdruD4wD4BQBQD6 bodck4y4 ck6 {Backspace][Backspace][Backspace][Backspace] gdur4an6 mindoms qu/6w86 {     fm, 2003g4     j8z83ru4xj4     5// ip6</pre>	 24.08.2008, 14:42. User: "coyen". ™indom title:"Bome Keylogger - Quick Start - Microsoft Internet<br Explorer"> dfgdfg c	t
[Backspace][Backspace][Backspace] gdm/dm6 windows qu/6m96 < fm, 2u03gd j6z83rudxi4 5/7 jp6 > 0 5j; j06]udc. 4 y84 u. 4vu84ru13 cjo4tj vu04u ekTmj6gd 	24.08.2008, 14:43. User: 'ccyen'. Windom title:'7.doc [相容機式] - Wicrosoft Word' [Ctrl+y]vBome cjo4ur4xj4su3nji3gj bj4ru04m0g8q06 by4ck4y4 ck6 <	
[Backspace][Backspace][Backspace] [Backspace]	[Backspace][Backspace][Backspace][Backspace] gdm/dm5 windoms qu/6m96 < fm, 2u03g4 j6z83ru4×j4 5// jp6 > > 0 5; j051u4c.4 y94 u.4vu84ru13 cjo4tj vu04u ekTmj6g4 < 2u03ru6u vu84cj6gjcj86 [Backspace]×u;3 5k4keTmj6g4 ru.4cjo4tj uvu04 nji3ru4xj4 2kTru04q06gj 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 或掃瞄的動作,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。

Remote Executor ve	r. i. u. 9
e Program <u>H</u> elp	
Program Computers Pro	ogress
Please specify the program (local for the remote compu- to the remote computers b	a you wish to run on the remote computers, optional working dir uters) and optionally the list of additional files that should be copied efore execution:
Command Line:	ping localhost
Working directory:	 (optional, blank in most cases)
Additional files (the files tha the program execution):	at should be copied to the target machine before
	Add
	Delete

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

- 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

- 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。
- 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。
- 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删除,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-|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。



### ■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。