

# 第五章

## 列舉

# 入侵系統過程

- 列舉使用者名稱、機器名稱或SNMP...。
- 破解密碼。
- 升高權限。
- 執行應用程式。
- 隱藏檔案。
- 覆蓋蹤跡。

# 列舉

- 列舉是屬於Intranet環境的技術。
- 攻擊者會想要列舉的資訊項目包括：網路資源與分享、使用者及群組、應用程式、設定...等。

# 列舉的技術

- 使用系統提供的工具進行列舉。
- 獲取SNMP的使用者名稱。
- 獲得目標的預設密碼。
- 獲取E-mail的使用者名稱。
- 使用暴力法（Brute force）。

# 工具程式

## ■ Net Bios Null Sessions

- Null sessions使用CIFS/SMB（Common Internet File System/ Server Messaging Block）進行運作，主機必須安裝NetBIOS才能運作。

# Net Bios Null Sessions

- 攻擊者可以建立一個null session的連線到一個Windows（NT/2000/XP）主機上，並藉由null user name及password來登入。
- 任何使用NetBIOS連接到目標電腦的連線，都可能輕易的得到完整的列表，列表包括使用者名稱、群組、分享、權限、政策與服務。

# Net Bios Null Sessions

若使用這個null連接，可能會收集到目標主機的  
下列資訊：

- users及groups的列表。
- 主機的列表。
- 「分享」的列表。
- UIDs及SIDs（Security Identifiers）。

# Net Bios Null Sessions

假設目標的IP位址是192.34.34.2。

- Window版：`C:\>net use \\192.34.34.2 \IPC$ "" /u:""`
- Linux版：`$ smbclient \\\192.34.34.2\ipc$ "" - U ""`



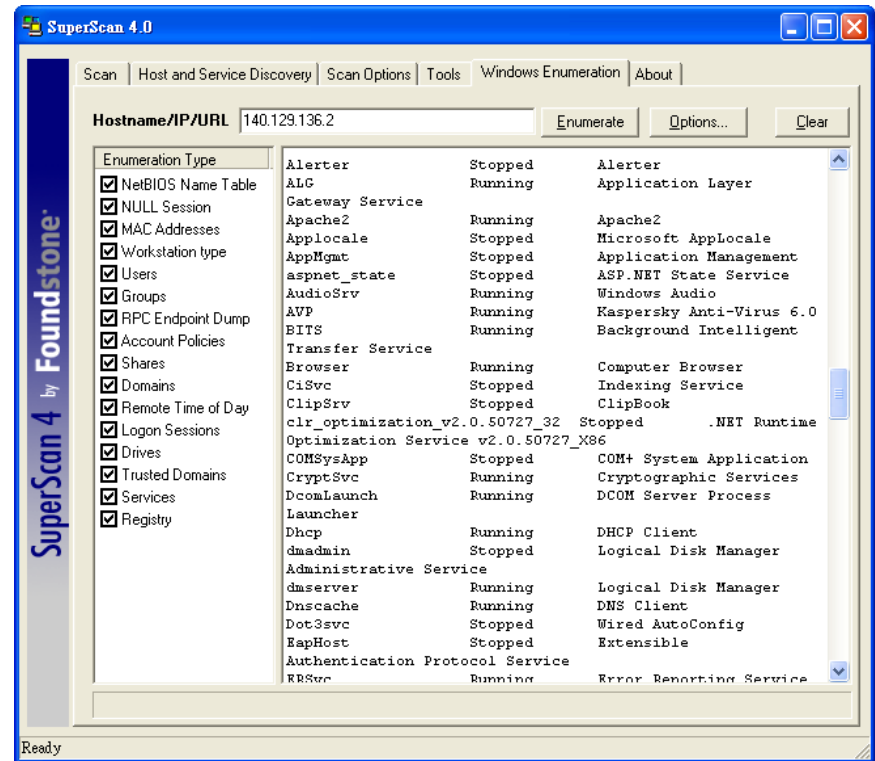
# 工具程式

## ■ SuperScan4

- SuperScan 是一個不需要安裝的掃描程式，這個程式包含了多個網路工具，當然也包括了列舉的功能。

# SuperScan4

- 使用時請點選「Windows Enumeration」頁籤，可以看到左邊的「Enumeration Type」中列出了許多這軟體可以列舉的項目，包括了NULL Session。接著輸入目標主機的名稱或IP，最後再按下「Enumerate」。



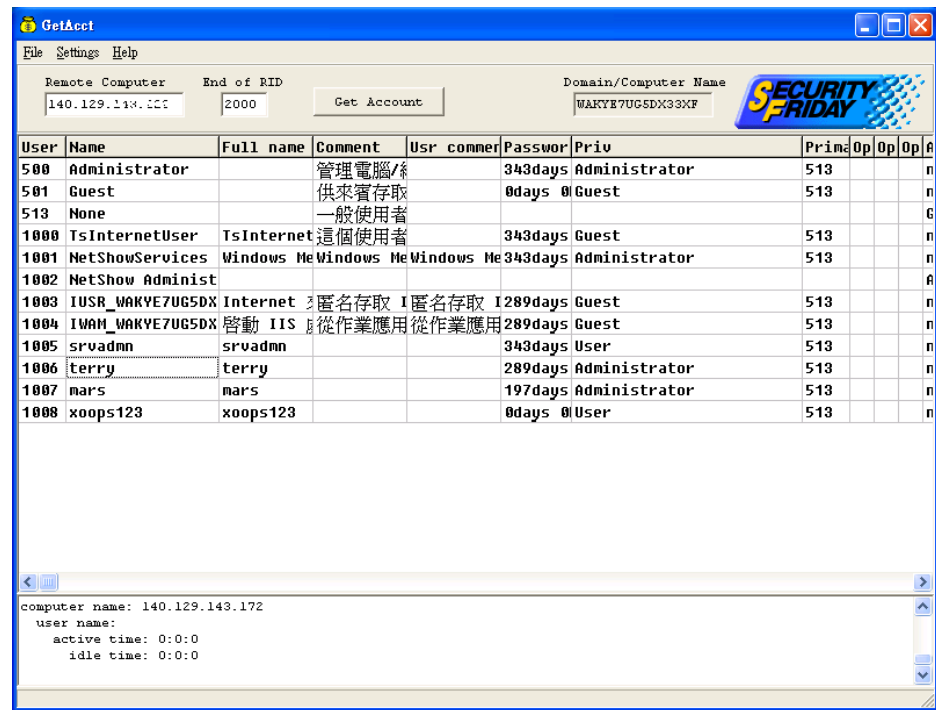
# 工具程式

## ■ GetAcct

- GetAcct可以獲得在Windows NT/2000/XP/2003機器上帳號的資訊。
- RID是當使用者建立時，作業系統給使用者的識別號。

# GetAcct

- 輸入IP位址或目標電腦的 NetBIOS名稱在「Remote Computer」欄位上，然後輸入1000以上的數字在「End of RID」欄位。
- 如果要檢查100個使用者，就輸入1100，預設值是2000，也就是檢查1000個帳號。最後按下「Get Account」按鈕。



The screenshot shows the GetAcct application window. The title bar is "GetAcct". The menu bar includes "File", "Settings", and "Help". The main interface has three input fields: "Remote Computer" (140.129.143.172), "End of RID" (2000), and "Domain/Computer Name" (WAKYE7UG5DX33XF). A "Get Account" button is located to the right of the "End of RID" field. A "SECURITY FRIDAY" logo is in the top right corner. Below the input fields is a table of user accounts.

User	Name	Full name	Comment	Usr commen	Passwor	Priv	Prim	Op	Op	Op	A
500	Administrator		管理電腦/		343days	Administrator	513				n
501	Guest		供來賓存取		0days	Guest	513				n
513	None		一般使用者								G
1000	TsInternetUser	TsInternet	這個使用者		343days	Guest	513				n
1001	NetShowServices	Windows Me	Windows Me	Windows Me	343days	Administrator	513				n
1002	NetShow Administ										A
1003	IUSR_WAKYE7UG5DX	Internet	匿名存取	I 匿名存取	I 289days	Guest	513				n
1004	IWAM_WAKYE7UG5DX	啟動 IIS	從作業應用	從作業應用	289days	Guest	513				n
1005	srvadmn	srvadmn			343days	User	513				n
1006	terry	terry			289days	Administrator	513				n
1007	mars	mars			197days	Administrator	513				n
1008	xoops123	xoops123			0days	User	513				n

At the bottom of the window, there is a status bar with the following text:

```
computer name: 140.129.143.172
user name:
active time: 0:0:0
idle time: 0:0:0
```

# Null Session 對策

- Null sessions 會去存取TCP 139與TCP 445 port，若不使用這兩個Port可以將其關閉。
- Null session無法在Windows 2003 Server上動作。
- 從Windows操作介面上關閉WINS Client TCP/IP，就可以關掉SMB服務。

# Null Session 對策

■ 編輯機碼（registry）以限制匿名使用者（anonymous user）登入，其步驟如下：

1. 打開regedit尋找

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\restrictanonymous。

2. 選擇「修改」，Data Type: DWORD，Value: 2。

# SNMP列舉

- SNMP是簡單網路管理協定（Simple Network Management Protocol），管理者只要送出需求（Requests）給某個設備（Agents），這個Agents就會將回應送回。
- 需求的封包中包含了一些變數及設定的數值，Agents會依據變數中的數值傳回相對的回應。

# MIB

- MIB（Management Information Base）是SNMP的管理資訊庫。
- MIB提供SNMP Agent各種資訊的基本表現方式，是SNMP網路管理基本的元件。



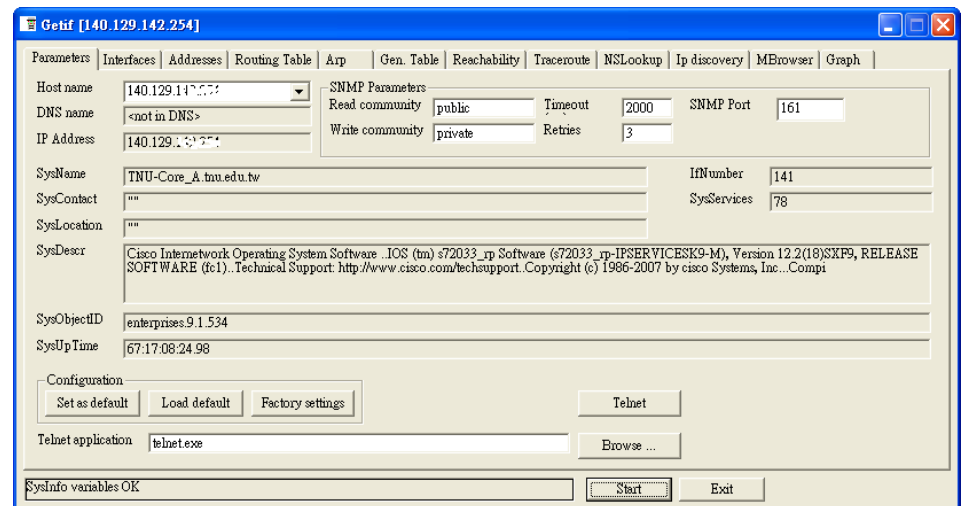
# MIB

- MIB-II是標準MIB的更新版本。
- MIB系統有一個稱為community string的變數，許多設備預設值是「public」且為「唯讀」屬性，這可能造成該設備的某些資訊外洩。

# 工具程式

## ■ Getif

- 是一個可以透過 SNMP 獲取有關 Agents 各項數值與設定的程式。



# 工具程式

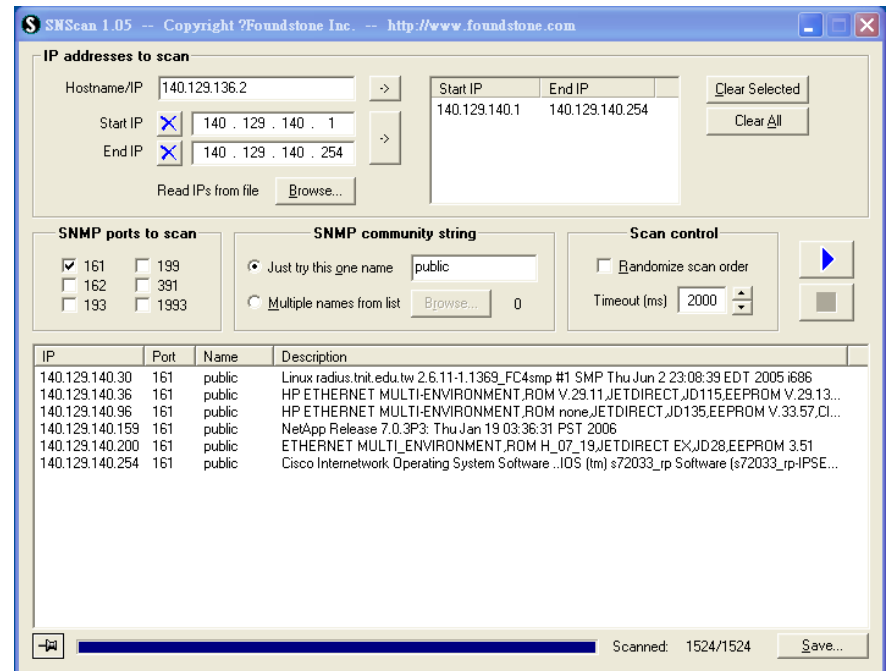
## ■ Solarwinds

- Solarwinds是一組網路管理工具，包含了Discovery、Cisco Tools、Ping Tools、Address Management、Monitoring、MIB Browser、Security、Miscellaneous。

# 工具程式

## ■ SNScan

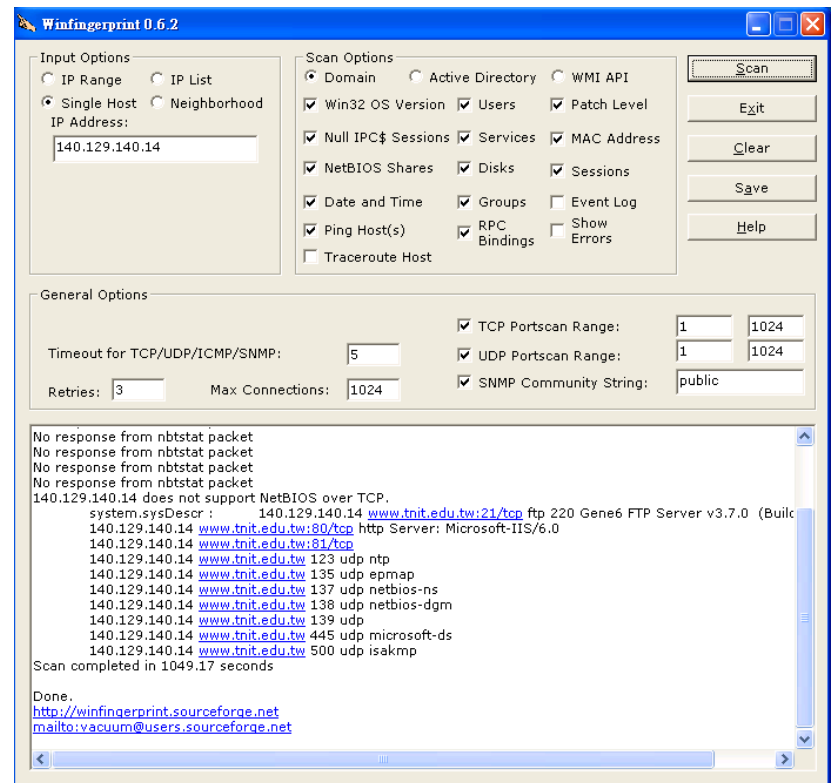
- 這是Windows-based SNMP scanner可以檢測網路上開啟了SNMP的裝置，它可以掃描特定的SNMP Ports，亦可使用public及使用者自定的community names。



# 工具程式

## ■ Winfingerprint

- Winfingerprint是視窗下圖形介面的工具程式，可掃描單一個主機或在連續的網路區塊同時進行列舉的動作。



# SNMP Enumeration 對策

- 最簡單的防治方法就是移除SNMP Agents或關閉SNMP服務。
- 如果一定要使用，而且設備也支援，可以使用SNMP v3，這會更安全。

# 預設帳號及密碼列舉

- 許多的裝置都會使用預設帳號及密碼，例如：交換器，路由器，分享器。列舉時可以嘗試使用預設帳號及密碼

○

## default password list

Browse by character: **A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0-9**

### Search

Manufacturer:

Product:

Contribute to the default password list.

### Add your own experience

Manufacturer:  Product:  Revision:

Protocol:   Access:

User ID:  Password:

Last updated 2006-08-22 16:54:16 (GMT+1)  
contact at defaultpassword dot com

## 列舉的步驟

1. 在主機上使用 null sessions 獲得資訊。
2. 使用 Super Scan4 等工具執行 windows enumeration。
3. 使用 GetAcct 等工具得到 users accounts。
4. 用 Getif、SNScan 等工具執行 SNMP port 的掃描。
5. 使用 <http://www.defaultpassword.com/> 列舉預設的帳號與密碼。



## 練習

- 先檢查電腦的設定，查出「閘道」的IP。因為閘道可能就是一台路由器，且其SNMP可能是開啟的。使用前述的Getif...等，看是否能列舉出閘道的相關資訊？
- 依據輸出，是否能推測出該設備的廠牌、型號...等相關資訊？
- 這個設備是否有預設的帳號及密碼？
- 嘗試尋找相關資料。