



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

0

#### ■ 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

 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。

■ 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。

### 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) 。

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瞄程式, 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」。

#### 🗄 SuperScan 4.0 Scan Host and Service Discovery Scan Options Tools Windows Enumeration About Hostname/IP/URL 140.129.136.2 Enumerate Options... <u>C</u>lear Enumeration Type Alerter Stopped Alerter ✓ NetBIOS Name Table ALG Running Application Layer Gateway Service ✓ NULL Session Apache2 Running Apache2 MAC Addresses ston Applocale Stopped Microsoft AppLocale ✓ Workstation type Application Management AppMomt Stopped 🗹 Users aspnet state Stopped ASP.NET State Service Groups AudioSrv Running Windows Audio Found AVP Running Kaspersky Anti-Virus 6.0 RPC Endpoint Dump BITS Background Intelligent Running Account Policies Transfer Service Shares Browser Running Computer Browser Domains CiSvc Stopped Indexing Service ClipBook ClipSrv Stopped Remote Time of Day clr\_optimization\_v2.0.50727\_32 Stopped NET Buntime Logon Sessions uperScan Optimization Service v2.0.50727 X86 Drives COMSysApp Stopped COM+ System Application ✓ Trusted Domains CryptSvc Running Cryptographic Services Services DcomLaunch DCOM Server Process Running Launcher Registry Dhep Running DHCP Client dmadmin Stopped Logical Disk Manager Administrative Service dmserver Running Logical Disk Manager Dnscache DNS Client Running Wired AutoConfig Dot.3svc Stopped EapHost Extensible Stopped Authentication Protocol Service RRSVC Dunning Rrror Reporting Service Ready

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

0

 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

🖥 GelÅcet 📃 🗖 🔀									
<u>File</u> S	File Settings Help								
Rer	Remote Computer End of RID Domain/Computer Name								35
140.129.133.101 2000 Get Account WAKYE7UG5DX33XF						PIDAY	1.35		
		1						233	
User	Name	Full name	Comment	Usr commer	Passwor	Priv	Prima	Op Op	Op A
500	Administrator		管理電腦/約		343days	Administrator	513		п
501	Guest		供來賓存取	ł	0days 0	Guest	513		п
513	None		一般使用者	-					G
1000	TsInternetUser	TsInternet	這個使用者	4	343days	Guest	513		п
1001	NetShowServices	Windows Me	Windows Me	Windows Me	343days	Administrator	513		п
1002	NetShow Administ								A
1003	IUSR_WAKYE7UG5DX	Internet 3	匿名存取 ]	匿名存取	289days	Guest	513		п
1004	IWAM_WAKYE7UG5DX	啓動 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		п
1008	xoops123	xoops123			0days 0	User	513		n

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:

 打開regedit尋找 HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentC ontrolSet\Control\LSA\restrictanonymous。
 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 (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-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。

🗑 Getif [140.1	29.142.254]					
Parameters   Int	terfaces   Addresses   Routing Table   Arp   Gen. Table   Reachability   Traceroute   NSLookup   Ip discovery   MBrowser   Graph					
Host name DNS name IP Address	I40.129.147.073         SNMP Parameters <not dns="" in="">         Read community         public         Timeout         2000           I40.129.147.077         Write community         private         Retries         3</not>					
SysName	TNU-Core_A.tnu.edu.tw IfNumber 141					
SysContact	"" SysServices 78					
SysLocation	00					
SysDescr	Cisco Internetwork Operating System SoftwareIOS (tm) s72033_pp Software (s72033_pp-IPSERVICESK9-M), Version 12.2(18)SXF9, RELEASE SOFTWARE (fc1)Technical Support: http://www.cisco.com/techsupport.Copyright (c) 1986-2007 by cisco Systems, IncCompi					
SysObjectID	enterprises.9.1.534					
SysUpTime	67:17:08:24.98					
Configuration     Set as default     Load default     Factory settings       Telnet application     telnet exe     Browse						
SysInfo variables	OK Exit					

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。

🔖 Winfingerprint 0.6.2			
Input Options IP Range C IP List Single Host C Neighborhood IP Address: 140.129.140.14	Scan Options Domain C Active Win32 OS Version V Null IPC\$ Sessions V NetBIOS Shares V Date and Time V Ping Host(s) V Traceroute Host	e Directory C WMI API 7 Users ▼ Patch Level 7 Disks ▼ MAC Address 7 Disks ▼ Sessions 7 Groups □ Event Log 7 Bindings □ Show Errors	E <u>x</u> it <u>C</u> lear S <u>a</u> ve <u>H</u> elp
General Options Timeout for TCP/UDP/ICMP/SNMP Retries: 3 Max Conn No response from physiat packet	ि इ.ज. इ.dtions: 1024	7 TCP Portscan Range: 7 UDP Portscan Range: 7 SNMP Community String:	1 1024 1 1024 public
No response from histat packet No response from histat packet No response from histat packet 140.129.140.14 does not support Ne system.sysDescr : 144 140.129.140.14 www.tnit.ed 140.129.140.14 www.tnit.ed	BIOS over TCP. .129.140.14 www.tnit.edu.ti .1tw:80/top http Server: Mic .1tw:81/top .1tw 123 udp ntp .1tw 135 udp epmap .1tw 138 udp netbios-ns .1tw 138 udp netbios-dgm .1tw 138 udp .1tw 445 udp .1tw 445 udp microsoft-ds .1tw 500 udp isakmp	<u>₩:21/top</u> ftp 220 Gene6 FTP 3 rosoft-II\$/6.0	Server v3.7.0 (Build
Done. http://winfingerprint.sourceforge.net mailto:vacuum@users.sourceforge.n	<u>et</u>		~

### 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

#### 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

dpl

dpl

#### Search

Manufactor: d-link

Product:

#### Contribute to the default password list. Add your own experience

Manufactor:	Product:	Revision:
Protocol: Multi 🔽 Access		]
User ID:	Password:	dpl

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

0

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 脳。
- 5.使用http://www.defaultpassword.com/列舉預 設的帳號與密碼。



- 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。