

網路安全的理論與實務

楊中皇 著

第十二章 Nessus

<http://crypto.nknu.edu.tw/textbook/>

金 禾 圖 書

伴 您 學 習 成 長 的 每 一 天



# 第十二章 Nessus

- Nessus簡介
- Nessus的安裝方法
- Nessus的使用



# Nessus發展歷史

- R. Deraison成立一個計劃，命名為Nessus，在透過許多同好的協助與網路社群討論修改，於1998年4月首次發表Nessus
- 免費下載、功能強大、架構完整、更新迅速且相當容易使用的主機安全稽核掃描軟體
- 發展目的是幫助系統管理者搜尋系統主機的弱點所在，讓系統管理者對主機進行錯誤的更正或防護，以避免被入侵者攻擊
- Nessus的可延伸性使得掃描更具有發展空間，因為它隨意增加原本所沒有的偵測模式，而外掛模組(Plugins)就是對每個安全漏洞的描述和稽核，因此擴充外掛模組就可提升軟體的稽核能力



# Nessus主要特點

- 外掛**Plugins**：使用者可依需求修改外掛模組，而不需修改內部核心的程式碼
- **NASL**擴充語言：爲了迅速簡易撰寫測試掃描程式，系統業者設計一套**Nessus Attack Scripting Language**，不需修改**Nessus**的掃描引擎核心程式，即可自行達到各項要求
- 時常性更新弱點資料庫：**Nessus**的開發維護人員每天專注於檢查最新的安全漏洞



# Nessus主要特點(續)

- **Client-Server**架構：Nessus是由Nessus伺服器 and Nessus用戶端組成，而伺服器負責測試掃描，以外掛模組的方式來增加測試項目，將測試結果回報給用戶端檢視報告
- 同時測試多台電腦：此功能會為伺服器主機的能力而異，但Nessus系統可同時測試多台目標主機
- 聰明的通信埠識別能力：Nessus在測試目標並不會依循IANA所指派的通信埠編號。例：Nessus能辨別出一個開在port 6386的網頁伺服器



# Nessus主要特點(續)

- 重覆服務的檢測：如果一台主機同時架設兩個網頁伺服器，一個在port 80而另一個在port 8080，**Nessus**則會將兩個通信埠都測試出來
- 完整的報告：有多種輸出報表格式，分析報告包含系統所檢驗出的漏洞訊息、分級弱點的嚴重性與提供解決方案
- 完全支援**SSL**：**Nessus**可測試與**SSL**結合的服務，例如**HTTPs**、**SMTPs**、**IMAPs**等等
- 獨立的開發者：**Nessus**的開發者是完全獨立，跟商業軟體廠商沒有關聯，所以不會因與某些廠商有關而隱瞞任何的安全弱點





# Nessus操作平台

- **Nessus**由伺服器端與用戶端兩個部份組成，伺服器主要是負責測試執行，可安裝在所有的**Unix-like**作業系統
- 用戶端主要是一個前端介面，提供使用者登入**Nessus**伺服器，選擇要執行的測試與顯示測試結果。用戶端可以安裝在**X-Windows**、**Java**或是**MS-Windows**
- **Windows**版本分為**NessusWX**及**Tenable NeWT**，前者是免費的，而後者則是要付費的商業軟體
- 伺服器端的**Nessusd**預設**TCP**埠為**1241**，用戶端會談(**session**)時會使用以**E1Gamal**為基礎的公開金鑰方式做認證，以及每次連線傳輸資料都經過串流加密，避免資料被竊取後破解洩漏機密



# Nessus安裝-Linux

- **Nessus安裝方式有三種**
  - 網路直接安裝：這種方式最簡單，不過也是三種方式安全性最低的
  - **Script安裝**：安裝方式從<http://www.nessus.org>下載 **nessus-installer.sh**，script會自動安裝完成
  - 原始碼的安裝：需下載 **nessus-libraries.tar.gz**、**libnasl.tar.gz**、**nessus-core.tar.gz** 和 **nessus-plugins.tar.gz**這四支壓縮檔，再依此順序分別編譯執行安裝





- **nessus-libraries**
  - # cd nessus-libraries
  - # ./configure
  - # make
  - # make install
- **libnasl**
  - # cd libnasl
  - # ./configure
  - # make
  - # make install
- **nessus-core** 和 **nessus-plugins** 安裝過程同上述步驟即可完成安裝



# Nessus的使用

- 利用**nessus-adduser** 來增加新的使用者帳號
  - 允許多位使用者共用一部**Nessus**伺服器
  - 每位使用者帳號，只能依權限針對所設定的網路進行測試
- 建立一個**Nessus**伺服器憑證
- 編輯**nessusd**組態檔
  - 預設路徑於 `/usr/local/etc/nessus/nessusd.conf`
  - 使用者可以針對所需部份進行修改**nessusd**選項，選擇適合自己需求的組態



# Nessus用戶端-Linux

- Nessus用戶端分爲Unix-like及Win32兩種版本
- Unix-like啓動Nessus 用戶端程式
  - # cd /usr/local/bin
  - # nessus



# Nessusd host 設定

- Nessusd Host：設定連線的Nessus伺服器主機
- Port：設定與Nessus伺服器連線的通信埠
- Login：使用者登入帳號  
Password：使用者通行碼
- 輸入完畢後，點選「log in」，若登入成功會出現Connected，表示與Nessusd連線成功，「log in」會變成「log out」

Nessus Setup

Nessusd host | Plugins | Credentials | Scan Options | Target | User | Prefs. | KB | Credits

New session setup

Nessusd Host : localhost

Port : 1241

Login : joe

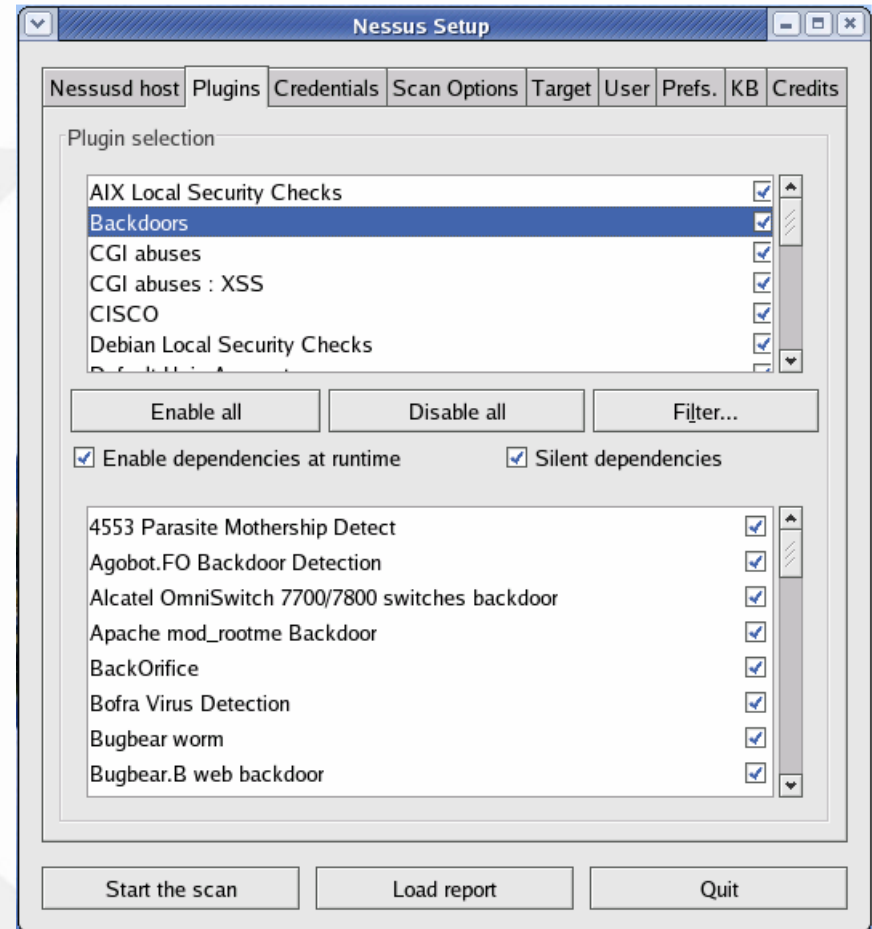
Password : \*\*\*\*\*

Log in

Start the scan | Load report | Quit

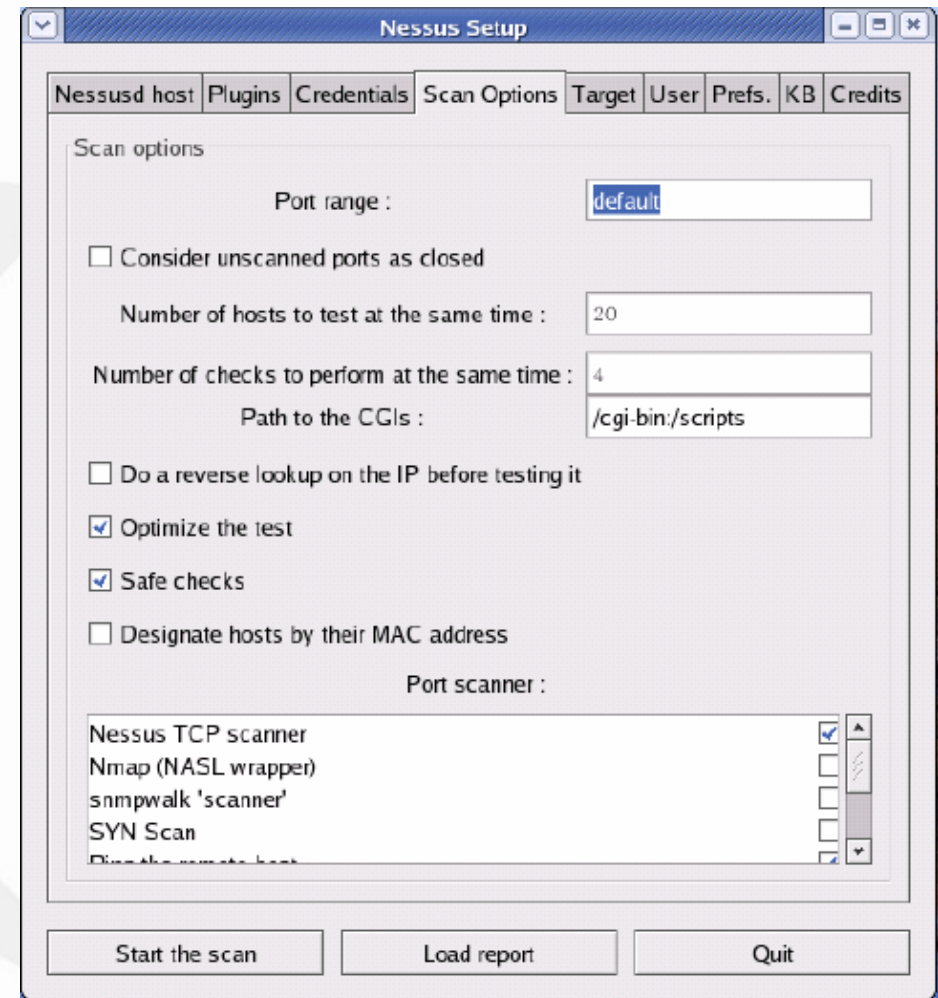


- 提供操作容易的搜尋頁面，供使用者搜尋特定的外掛模組
- 上半部視窗是Nessus掃描的種類
- 下半部是該種類的細項
- Nessus的各種測試程式均寫成外掛模組，使用者可隨意增加測試程式至Nessus程式內，而不需去修改核心的程式碼





- 選擇欲掃描通信埠的範圍 (port range) : 1-1024表示掃描port 1 ~ port 1024 , -1則表示不做port掃描
- Consider unscanned ports as closed : 如果勾選此項, 表示假設未在掃描範圍內的port視為關閉的, 僅掃描所設定的通信埠範圍, 雖然會加速掃描速度, 但會遺漏部份弱點檢查, 所以不建議勾選此項
- 限制同一時間進行掃描的主機數目 (Number of hosts to test at the same time)





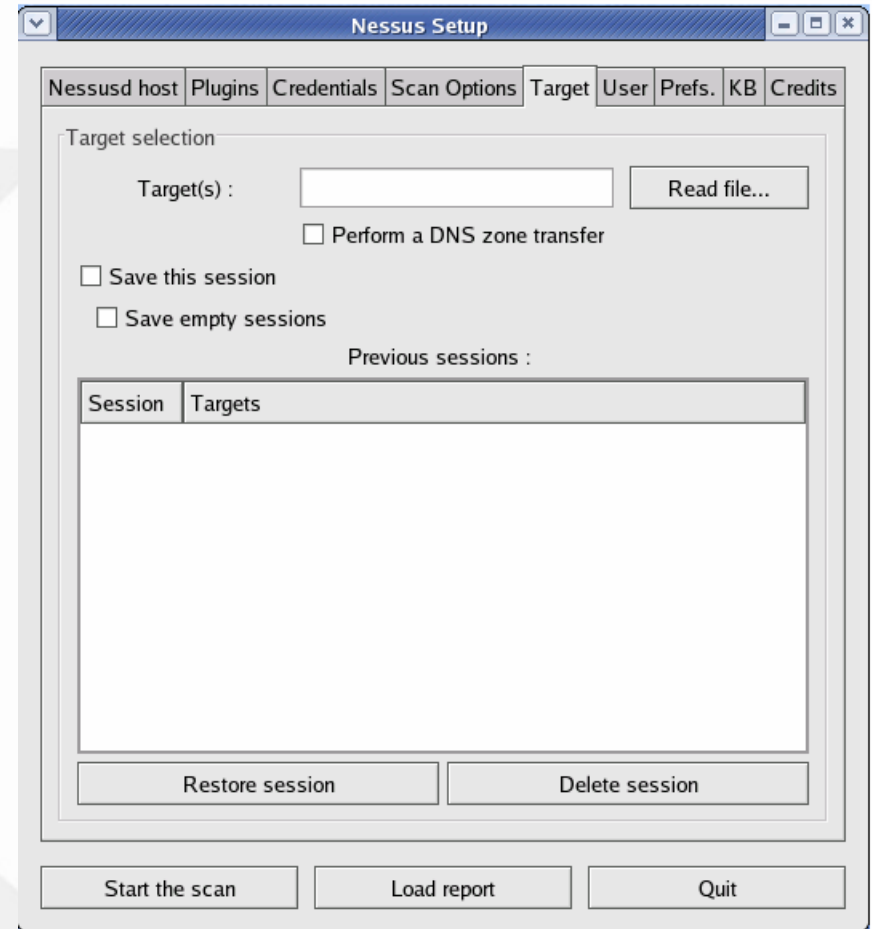


- 限制同一時間進行掃描的檢測次數 (Number of checks to perform at the same time) 設定掃描CGI程式之路徑 (Path to the CGIs)
- 是否使用DNS解析 (Do a reverse lookup on the IP before testing it)
- 設定最佳化測試 (Optimize the test)
- 安全測試 (Safe check) : 可避免掃描過程中去中斷目標主機的服務或破壞目標主機
- 依主機的MAC位址來測試 (Designate hosts by their MAC address)
- 進行port scan的工具選項 (Port scanner) : Nmap、tcp connection、ping及Port scan的逾時時間



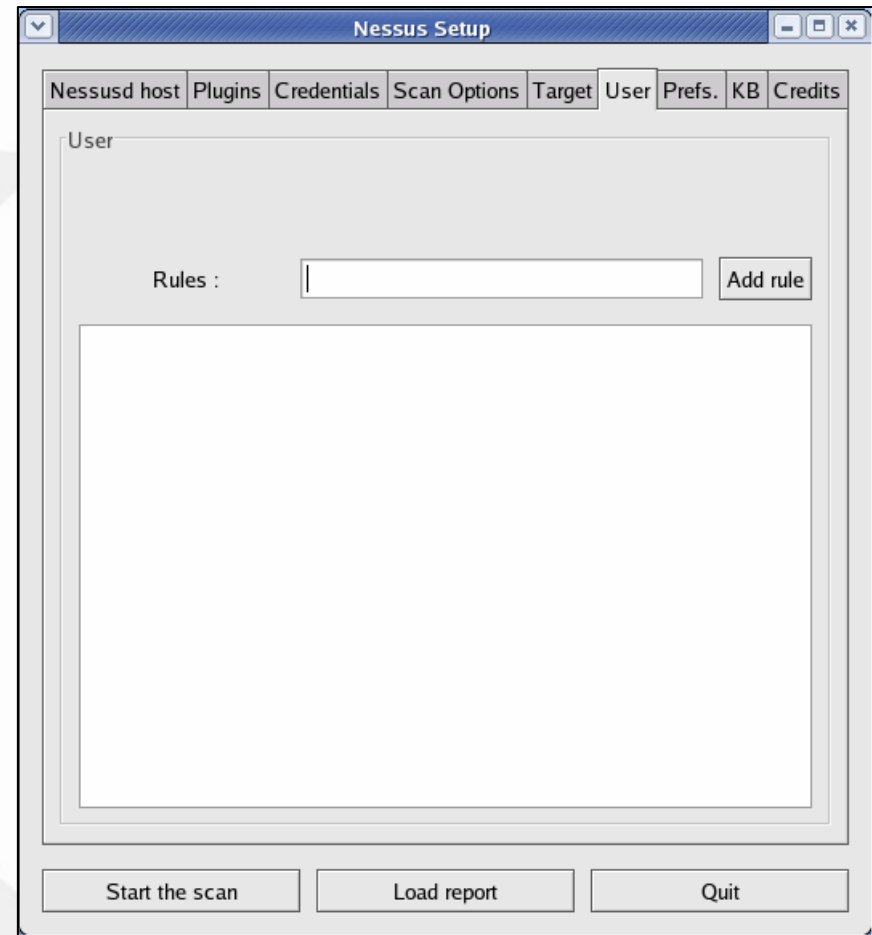
# 設定要掃描的主機範圍 (Target)

- 單一主機
- 子網路(subnet)所有主機
- 一個範圍內主機，各主機以逗號隔開
- 可將目標主機編輯成一個檔案，直接選取該檔案，便可將檔案內的主機群設定為測試目標
- **Save this session**：儲存本次session掃描結果



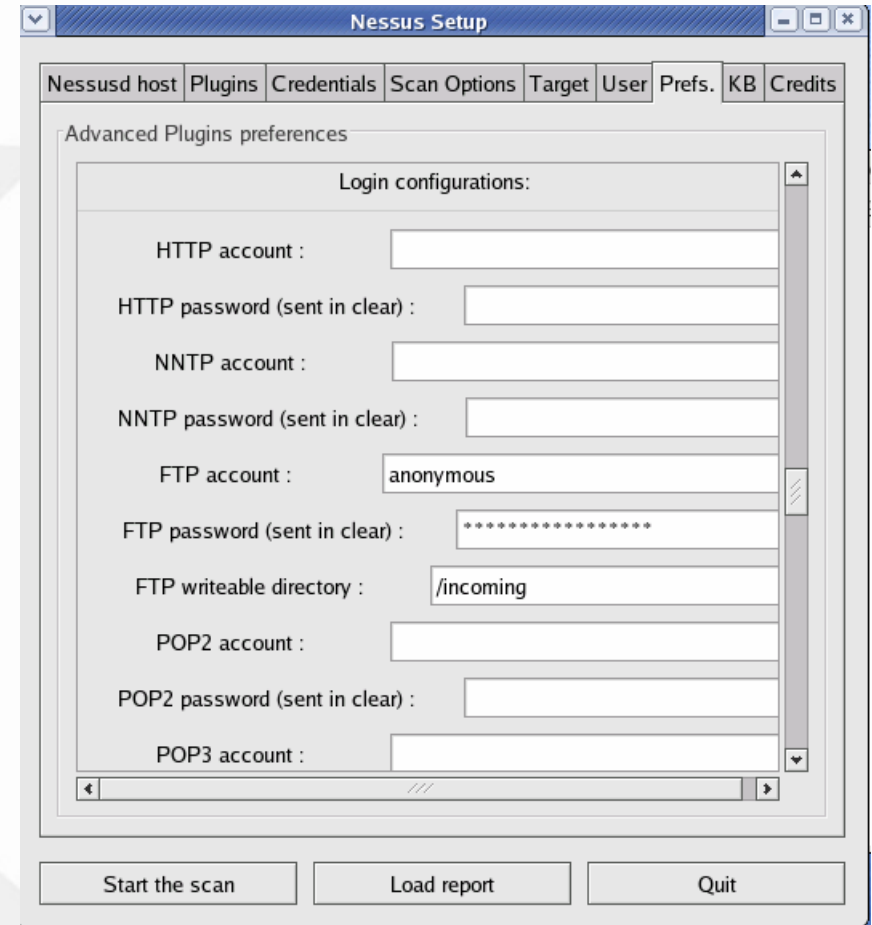


- **Rules**：設定對測試範圍作一些限制
- 例：要測192.168.10.1/24整個子網路的主機，除了192.168.10.32以外，可在「**Rules**」欄位裡輸入reject 192.168.10.32後按「**Add rule**」，這個規則就會加入到方框裡



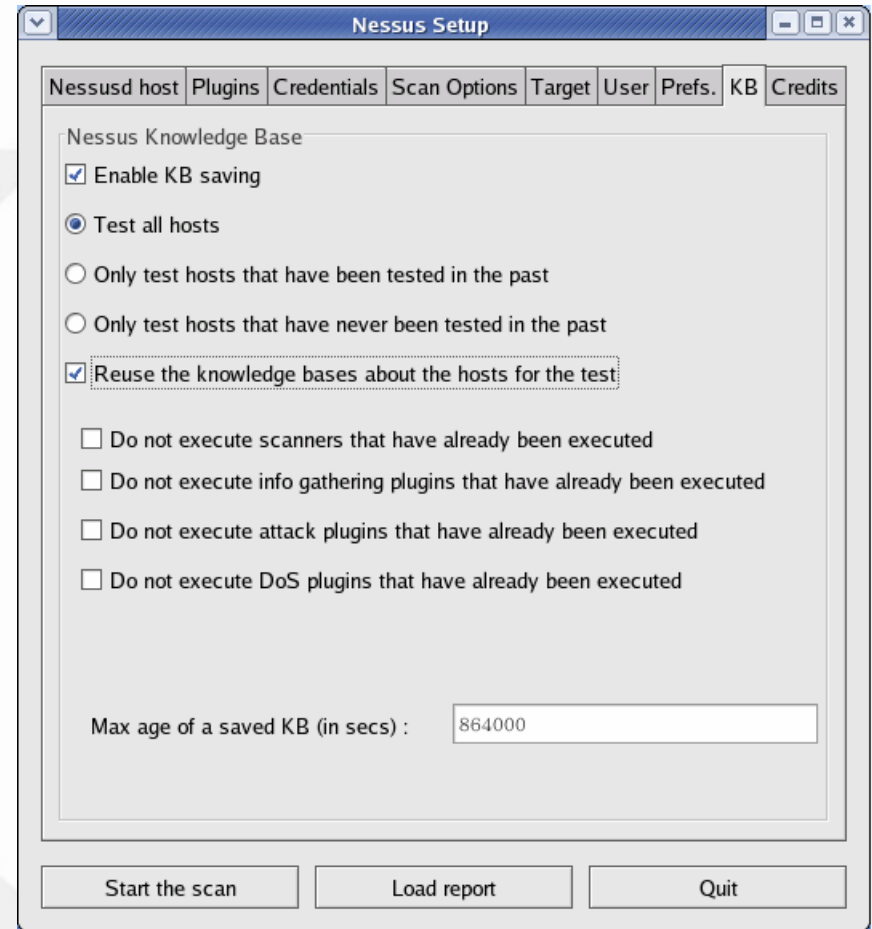


- 在執行某些測試項目時，需要輸入額外的參數才能執行
- 如果要ping 遠端主機，則可以在此設定用TCP或ICMP ping，也可以兩者都選擇
- 若選擇TCP ping，可設定其destination port
- 若選擇ICMP ping，則可設定重新嘗試的次數 (Number of retries)





- 保存已掃描主機所收集的資訊，包括主機開放哪些port、使用何種作業系統類型等，目的是為了減少不必要的測試
- 儘量利用其他已知的檢查結果，減少佔用網路資源，同時可以提高效率
- 測試結束後KB會從記憶體釋放，下一次掃描再重新開始，而按下視窗底部的「Start the scan」就開始掃描














- Test all hosts : 對全部主機進行掃描
- Only test hosts that have been tested in the past : 只對以前曾經掃描過的主機再進行一次掃描
- Only test hosts that have never been tested in the past : 對以前從未掃描過的主機或是超過指定時間未進行掃描的主機進行掃描
- Reuse the knowledge bases about the hosts for the test : 進行掃描時，nessusd會使用記憶體中的舊資料庫
- max age of a saved KB : 定義資料庫保存資料的有效期限，最大值是86400(單位：秒)，即為保存10天，過此期限，資料即作廢





# Nessus掃描狀態

 140.127.47.12	Portscan : Checks :	<div><div></div></div> <div><div></div></div>	Stop
 140.127.47.7	Portscan : Checks :	<div><div></div></div> <div><div></div></div>	Stop
 140.127.47.6	Portscan : Checks :	<div><div></div></div> <div><div></div></div>	Stop
 140.127.47.25	Portscan : Checks :	<div><div></div></div> <div><div></div></div>	Stop
 140.127.47.50	Portscan : Checks :	<div><div></div></div> <div><div></div></div>	Stop
 140.127.47.52	Portscan : Checks :	<div><div></div></div> <div><div></div></div>	Stop
 140.127.47.60	Portscan : Checks :	<div><div></div></div> <div><div></div></div>	Stop
 140.127.47.65	Portscan : Checks :	<div><div></div></div> <div><div></div></div>	Stop
 140.127.47.65	Portscan : Checks :	<div><div></div></div> <div><div></div></div>	Stop



# Nessus掃描結果報表

The screenshot displays the Nessus scan results interface. On the left, a list of hosts is shown under the 'Host' tab, with IP addresses ranging from 140.127.47.20 to 140.127.47.112. The host 140.127.47.101 is selected. The main panel shows the 'Port' list for the selected host, with 'ftp (21/tcp)' highlighted. The 'Severity' tab on the right shows a 'Security Warning' for the FTP service. The warning text states: 'This FTP service allows anonymous logins. If you do not want to share with anyone you do not know, then you should deactivate the anonymous since it may only cause troubles.' It also shows the content of the remote FTP root: 'drwxr-xr-x 2 0 0 4096 Oct 04 2004 pub'. The risk factor is 'Low' and the CVE is 'CAN-1000-0407'.

Subnet	Port	Severity
140.127.47	unknown (32769/tcp)	Security Warning
	sunrpc (111/udp)	Security Note
	sunrpc (111/tcp)	
	ssh (22/tcp)	
	omad (32768/udp)	
	mysql (3306/tcp)	
	https (443/tcp)	
	http (80/tcp)	
	general/tcp	
	general/icmp	
	ftp (21/tcp)	

This FTP service allows anonymous logins. If you do not want to share with anyone you do not know, then you should deactivate the anonymous since it may only cause troubles.

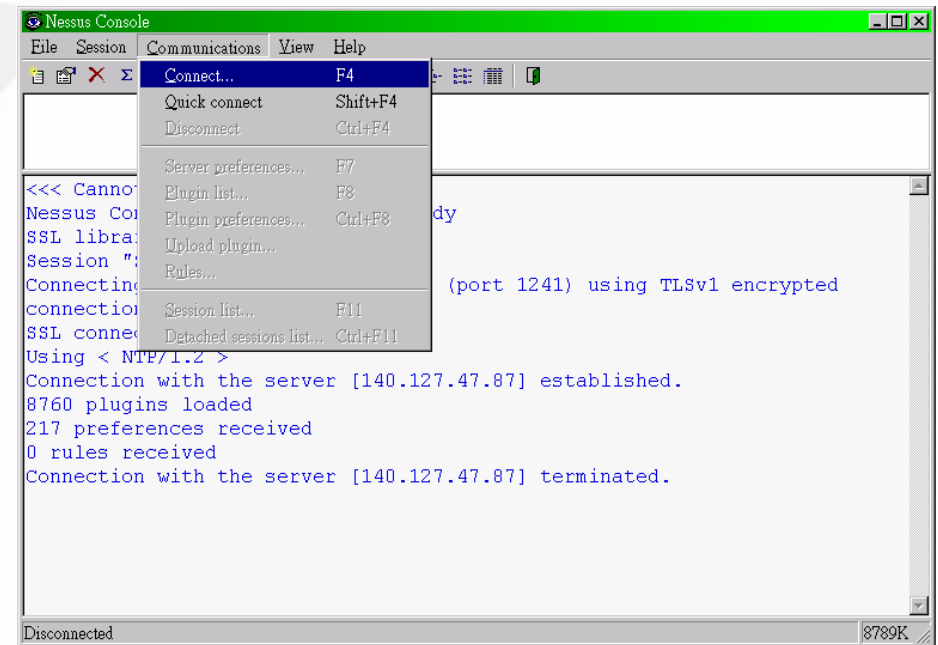
The content of the remote FTP root is :

```
drwxr-xr-x 2 0 0 4096 Oct 04 2004 pub
```

Risk factor : Low  
CVE : CAN-1000-0407



- 啓動NessusWX，且利用NessusWX連線至Nessus伺服器
- 選擇「Communications」選單的「Connect...」





# Nessus連接設定

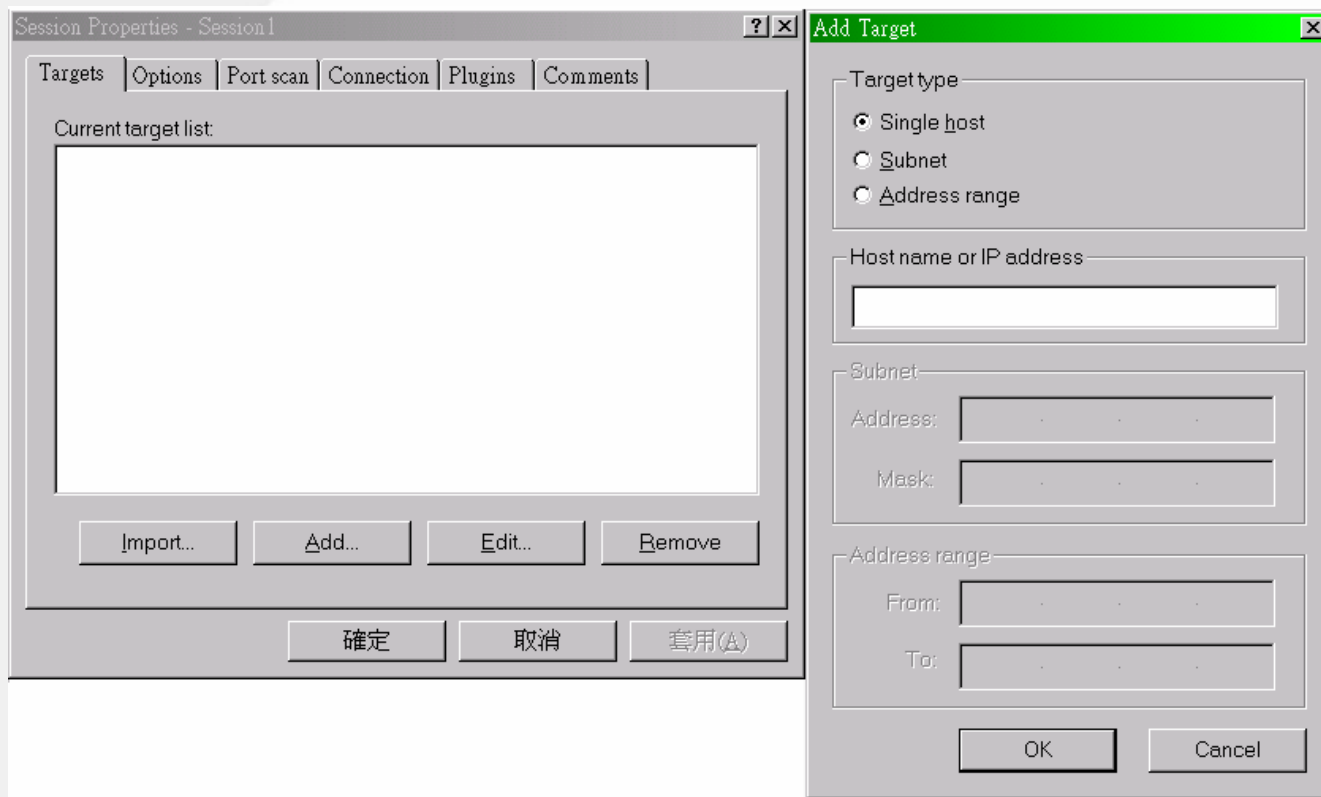
- 可設定欲連接Nessus伺服器的IP位址，預設通信埠為1241
- 輸入驗證的使用者帳號
- 如果是第一次連線，則會要求接受伺服器的憑證，接受後會從伺服器端載入plugins資訊到用戶端

The screenshot shows the 'Connect' dialog box in Nessus. It has a green title bar with the text 'Connect' and a close button. The dialog is divided into three main sections: 'Server', 'Encryption', and 'Authentication'. In the 'Server' section, the 'Name' field contains '140.127.47.87' and the 'Port number' field contains '1241', with a 'Default' button next to it. The 'Encryption' section has four radio buttons: 'Unencrypted', 'ILSV1' (which is selected), 'SSLv3', and 'SSLv2'. The 'Authentication' section has a 'Login' field with 'joe', a 'Password' field, and two radio buttons: 'Authentication by password' (selected) and 'Authentication by certificate'. There is also a checkbox for 'Save password' which is unchecked. At the bottom right, there are 'Connect' and 'Cancel' buttons.



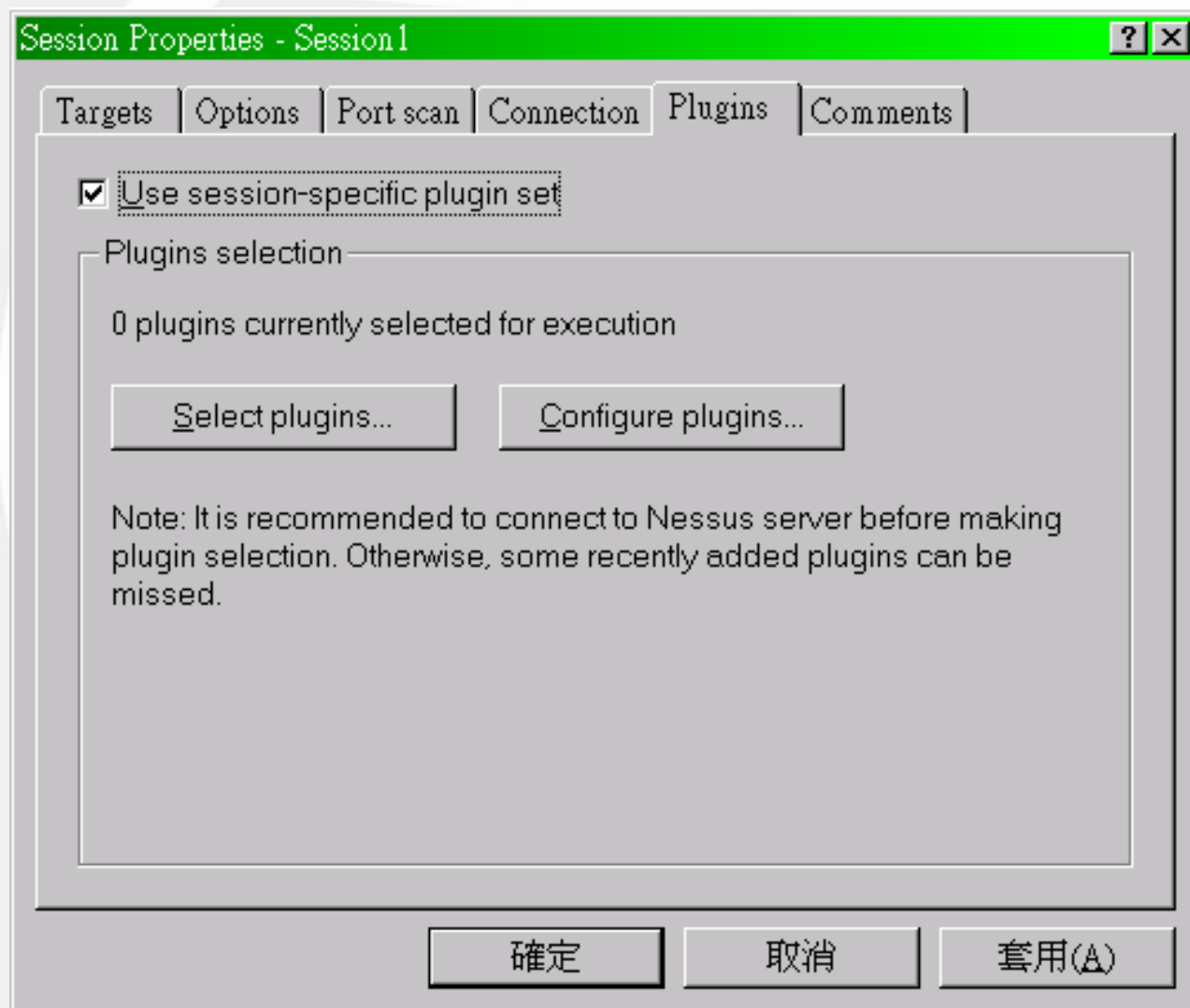
# 設定掃描目標

- 若要新增新的 **session**，設定欲測試的主機位址
- 可以是單一主機，子網路或是一個範圍主機IP





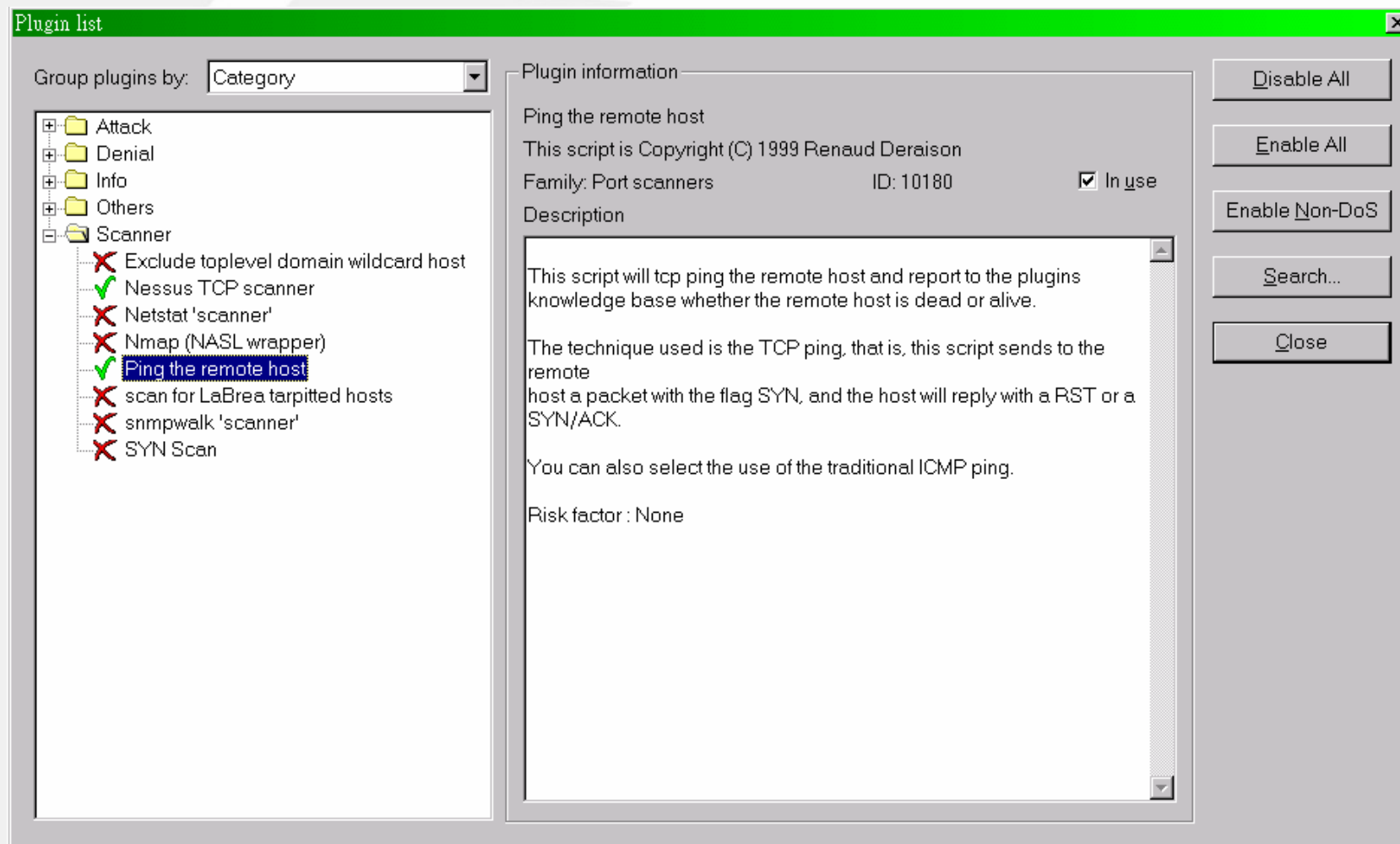
# Plugins選項頁面







# Plugin列表資訊





# 執行session掃描

- 離線掃描，只要輸入指定E-mail帳號或是session儲存，設定完成後則伺服器便會自動去執行
- 掃描結束後會自動寄到指定的電子郵件帳號，或是開啓已儲存的session來觀看掃描結果

Execute Session

Execution options

- ☐ Enable session saving
- ☐ Enable KB saving
- ☒ Detached scan

Detached scan options

- ☐ Continuous scan
- Delay between scan loops: 0
- E-mail address for notifications:

Execute

Cancel



## 掃描過程中狀態

Scan Status - Nessus Console

Scanning... Preview...

Overall scan progress

Target list:

Host	Ports...	All te...	Holes	War...	Infos	Ports	Status
140.127.47.70	0%	0%	0	0	0	1	Scann...
140.127.47.71	0%	100%	0	0	0	0	Finish...
140.127.47.72	0%	100%	0	0	0	0	Finish...
140.127.47.73	0%	100%	0	0	0	0	Finish...
140.127.47.74	0%	0%	0	0	0	0	Scann...
140.127.47.75	0%	100%	0	0	0	0	Finish...
140.127.47.76	0%	100%	0	0	0	0	Finish...
140.127.47.77	0%	0%	0	0	0	0	Scann...
140.127.47.78	0%	0%	0	0	0	0	Scann...
140.127.47.79	0%	0%	0	0	0	0	Scann...
140.127.47.80	0%	0%	0	0	0	0	Scann...
140.127.47.81	0%	0%	0	0	0	0	Scann...

☐ Remove finished hosts from the list

Stop testing this host Stop entire test



# 瀏覽session掃描結果

View Session Results - Session 1

Vulnerabilities:

140.127.47.12

- chargen (19/tcp)
- chargen (19/tcp)
- chargen (19/udp)
- chargen (19/udp)
- daytime (13/tcp)
- discard (9/tcp)
- domain (53/tcp)
- domain (53/tcp)
- domain (53/tcp)
- domain (53/udp)
- domain (53/udp)
- domain (53/udp)
- domain (53/udp)
- echo (7/tcp)
- echo (7/tcp)
- ftp (21/tcp)
- ftp (21/tcp)
- ftp (21/tcp)
- general/icmp
- general/tcp**
- general/udp
- microsoft-ds (445/tcp)
- microsoft-ds (445/tcp)
- ms-term-serv (3389/tcp)
- ms-term-serv (3389/tcp)
- ms-term-serv (3389/tcp)

**140.127.47.12**

Plugin information

Plugin ID: 11618

Remote host replies to SYN+FIN

Vulnerability

general/tcp

Medium severity

☐ This vulnerability is false positive

Description:

The remote host does not discard TCP SYN packets which have the FIN flag set.

Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules.

See also : <http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html>  
<http://www.kb.cert.org/vuls/id/464113>

Solution : Contact your vendor for a patch

Risk factor : Medium

BID : 7487



1. 掃瞄位址：顯示目前掃描及狀況分析的主機IP
2. 訊息代碼(Plugin information)：顯示此弱點代表的ID碼，透過這個ID碼可以到Nessus網站找到此弱點更詳細的說明
3. 弱點(Vulnerability)：顯示風險等級，若是紅色狀況為嚴重，請立即處理相關安全問題
4. 狀況描述(Description)：描述這個弱點發生的原因
5. 解決方法(Solution)：提供管理人員解決上述弱點的解決方案與建議。



# 參考資料

- R. Deraison, et al, *Nessus Network Auditing* , SYNGRESS
- NESSUS, [http : //www.nessus.org/](http://www.nessus.org/)