財團法人國家實驗研究院
國家高速網路與計算中心
National Center for High-Performance Computing

# 網站安全攻防實務

## 弱點掃描與分析工具

蔡一郎

# 課程大綱

- 安全弱點
- 弱點評估
- Nessus簡介
- Nessus安裝
- Nessus使用與設定
- 弱點報表分析
- 弱點修正
- Web 弱點掃描工具

# 何謂安全弱點

- 系統或網路上的缺口所導致的未授權的使用資源或接取服務
- 因程式上或組態設定上的錯誤或忽略而導致的安全問題

# 安全弱點形成的原因

- 設計階段(Design Phase)
  - 脆弱的演算法，或設計時未考慮到的問題
- 實作階段(Implementation Phase)
  - 因疏忽或是錯誤導致的軟體漏洞
- 操作階段(Operation Phase)
  - 使用者的使用或是設定不良所導致
- 人性/習慣(Human Nature)
  - 人性上的弱點所導致

# 弱點運用的方式

- Bruce force
- Resource exhausting
- Buffer overflow
- Format string
- TCP Spoofing
- TCP Hijacking, …etc.

# 弱點造成的影響

- 造成程式錯誤
- 權限提昇
- DoS
- 資訊洩露/竄改
- 植入木馬/後門程式

# 安全弱點的修補

- 軟體
  - Apply patch form vendor
  - Apply safe configuration setup
  - Close unnecessary services
- 安全的使用習慣
  - Strong password
  - Password protect screen saver
  - Don’t open malicious email/files
- 要求軟體開發者進行弱點改善

# 弱點評估的定義

- 用來檢查網路或作業系統的安全性
- 模擬攻擊者所發出的攻擊動作
- 可提供網路管理人員做為弱點修補之依據，以提昇安全性
- 與防毒軟體的做法相似，依據所謂的「弱點特徵資料庫」來測試是否存在已知的漏洞

# 弱點掃描的重要性

- 無絕對安全的系統
- 攻擊手法日新月異，更新速度越來越快
- 使用弱點掃描工具
  - 協助管理人員掌握最新的弱點資訊
  - 提供弱點修補的資訊
- 需不斷地進行弱點掃描與漏洞修補

# 使用的限制

- 不可過份依賴弱點掃工具軟體
- 特徵資料庫必需持續更新
- 不正確的使用方式，有時候反而會更加危險
  - 入侵偵測系統
  - DoS測試
- 誤判率高：弱點評估報告不一定是正確的，必須要有探討及分辨真偽的能力

# 弱點評估軟體的比較

- 商業軟體
  - 優點：有廠商維護，支援性較佳，使用門檻較低，較具親和力
  - 缺點：所需成本高
- 免費軟體
  - 優點：免費
  - 缺點：功能與說明較簡略，誤判率高，支援較少

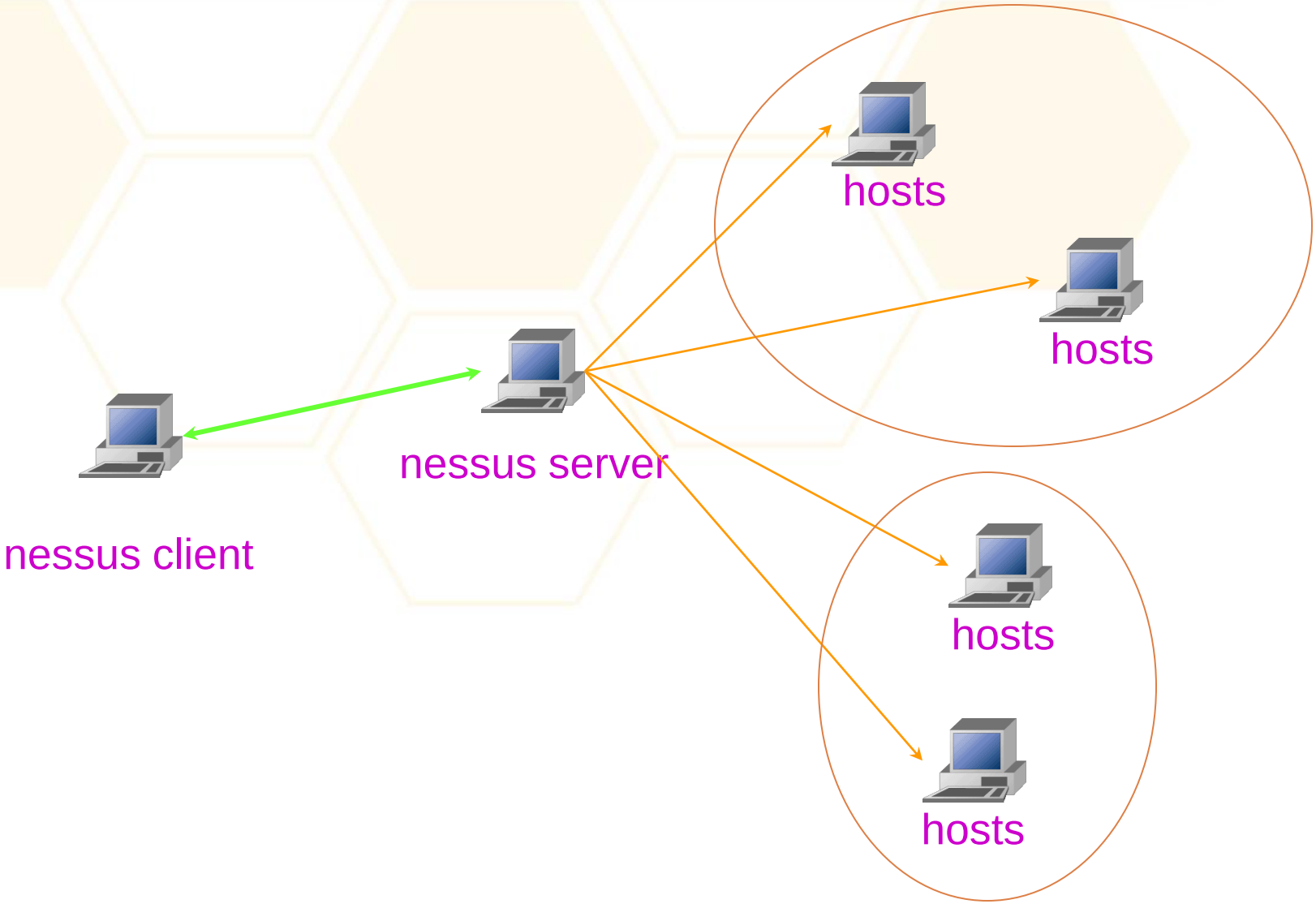
# Nessus軟體介紹

- 為一免費的網路安全檢測工具
- 它是在1998年，由法國的Renaud Deraison所發展的
- Nessus網頁：http://www.nessus.org/
- 目前最新的新版本為：*4.2.1*
  - 由3.0版本開始不提供原始碼
- 提供弱點資料庫更新
  - 免費下載版會慢7天

# Nessus軟體的特點

- 以Plug-in的方式組成
- 主從式架構
- 能同時檢測無限制的主機
- 能辨識主機上的服務
- 重覆服務的檢測
- 使用自附的直譯器及程式語言-- NASL
- 支援多種格式的報告結果
  - txt、html、pdf等格式

# Nessus架構



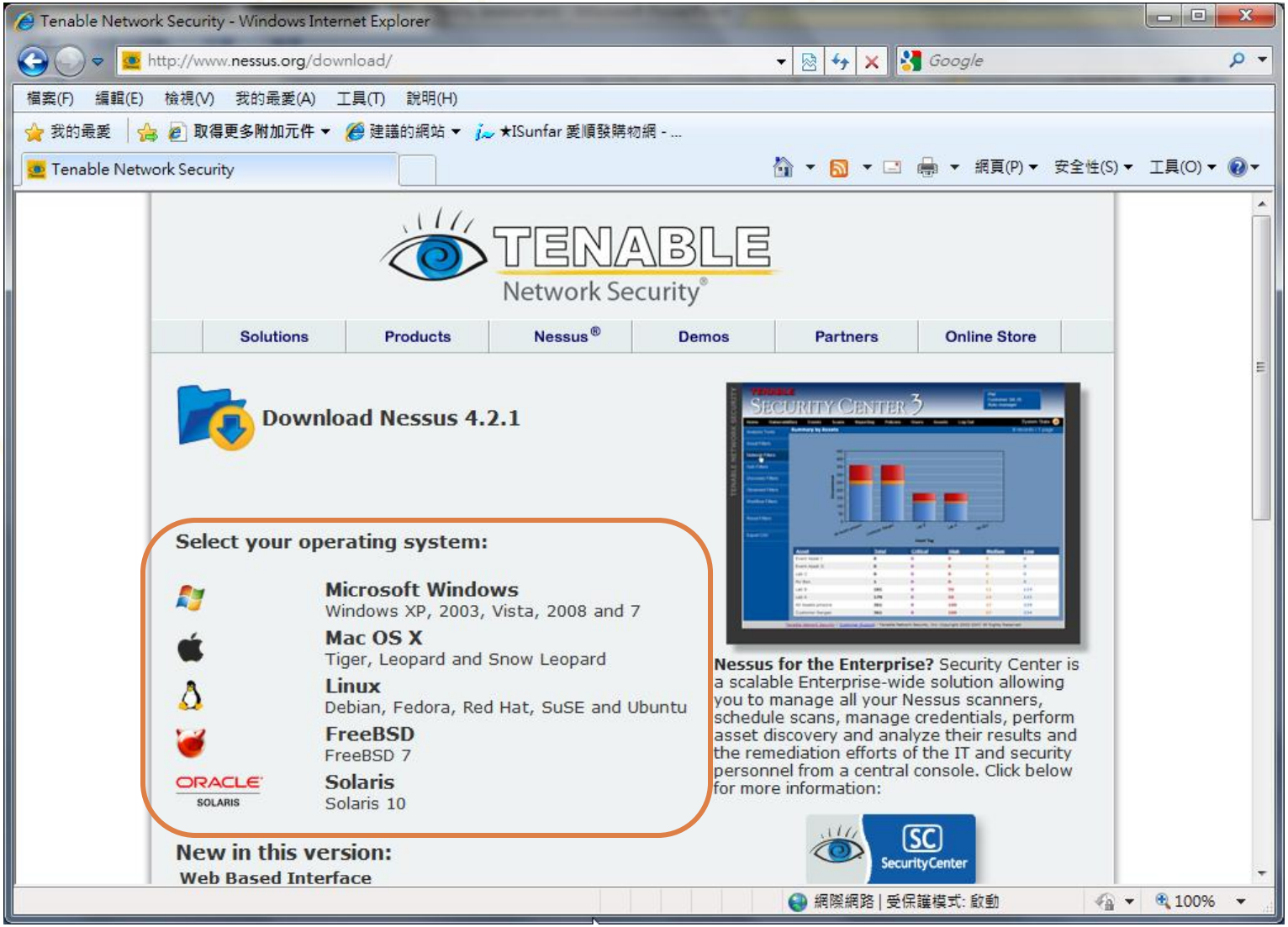
# Nessus server的安裝

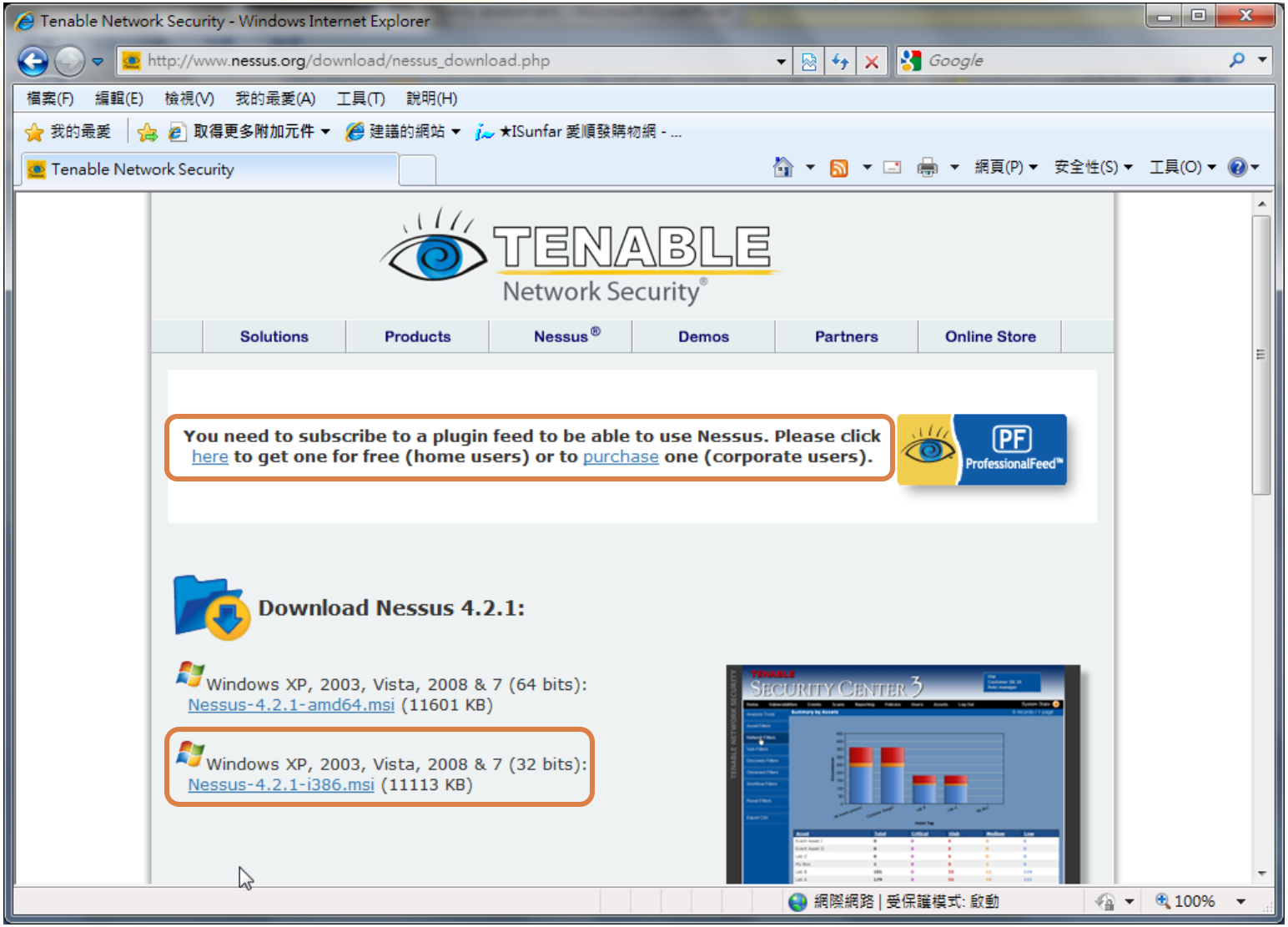
- 安裝：Nessus server 必需安裝在unix like的主機上，安裝方式有下列幾種：
  - 直接在網路上安裝，執行以下指令：
    lynx -source http://install.nessus.org | sh
  - 下載自動安裝程式：nessus-installer.sh
    #./nesshs-installer.sh
  - 下載nessus的原始碼後，個別編譯
  - 安裝RPM套件：3.0之後版本僅提供RPM套件，不提供原始碼

# 安裝步驟

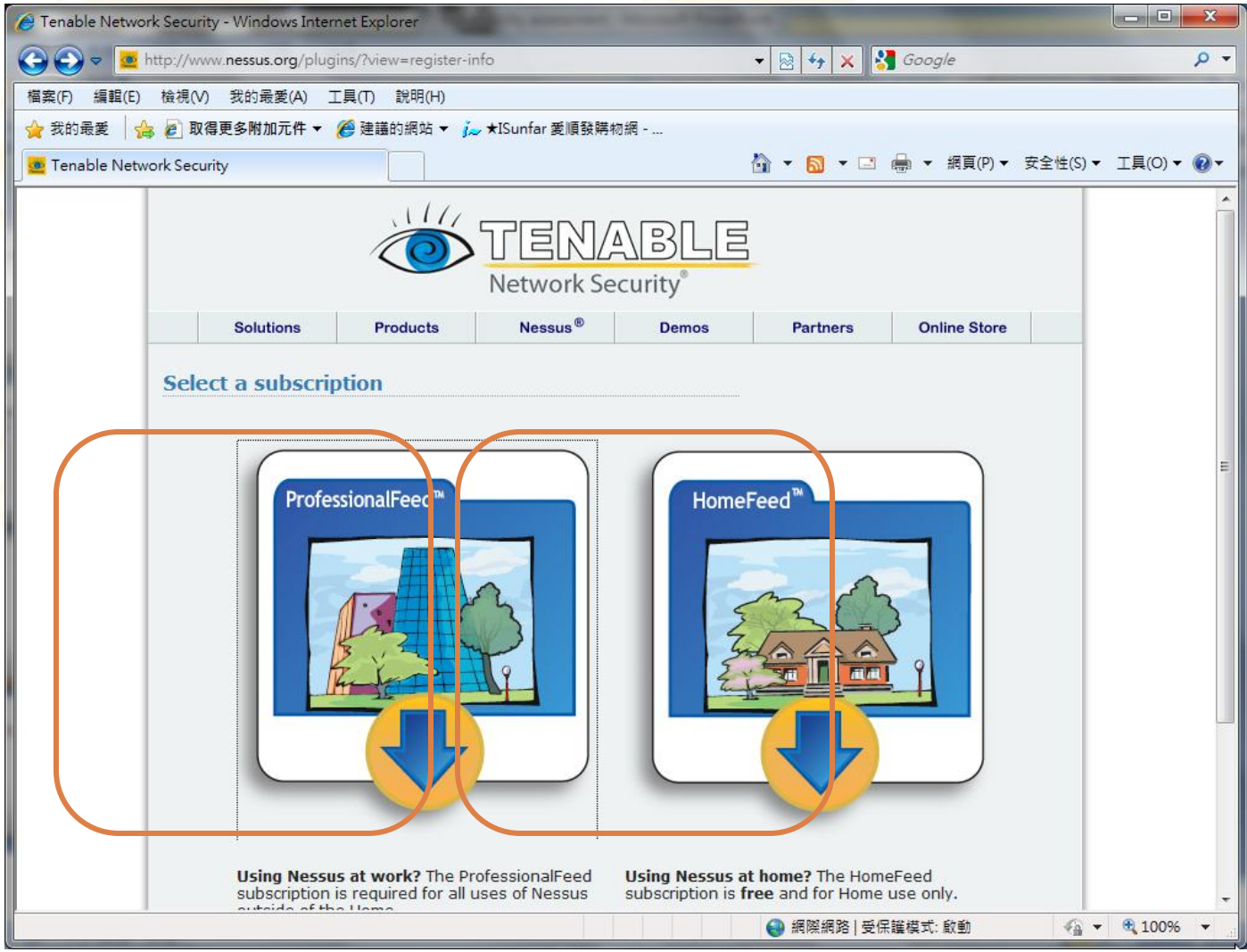
- 檢查系統需要的套件
  - gtk2、gtk2-devel(nessus client需要用的)
- 下載rpm套件
- 安裝rpm套件
- 建立第一個使用者
- 向nessus註冊：
  - 要註冊才能更新plugin
- 啟動nessusd

# 下載nessus套件

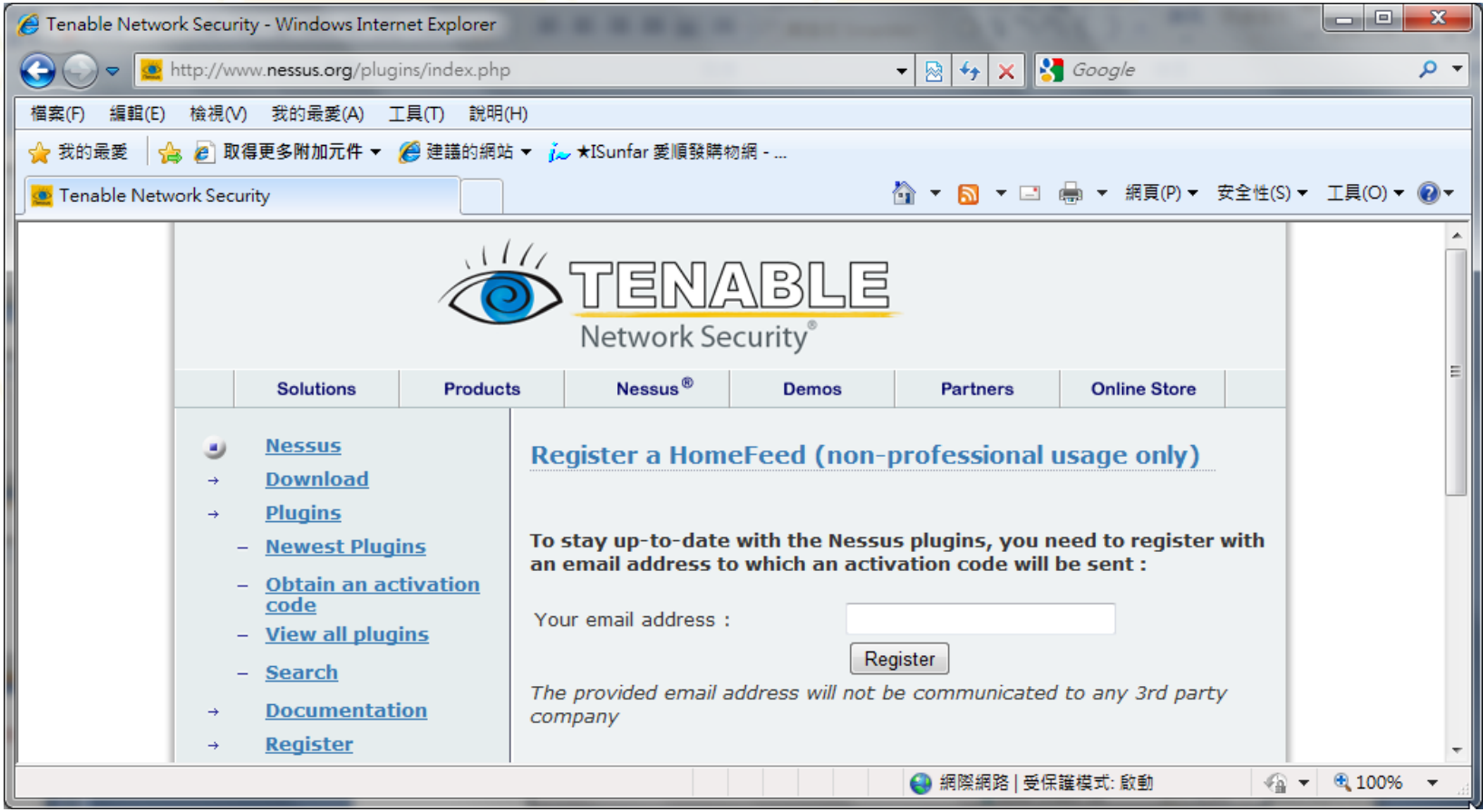

Tenable Network Security - Windows Internet Explorer
http://www.nessus.org/download/
Google
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
我的最愛
取得更多附加元件
建議的網站
★ISunfar 愛順發購物網 - ...
Tenable Network Security
網頁(P)
安全性(S)
工具(O)
TENABLE
Network Security
Solutions
Products
Nessus®
Demos
Partners
Online Store
Download Nessus 4.2.1
Select your operating system:
Microsoft Windows
Windows XP, 2003, Vista, 2008 and 7
Mac OS X
Tiger, Leopard and Snow Leopard
Linux
Debian, Fedora, Red Hat, SuSE and Ubuntu
FreeBSD
FreeBSD 7
ORACLE
SOLARIS
Solaris
Solaris 10
New in this version:
Web Based Interface
Nessus for the Enterprise? Security Center is a scalable Enterprise-wide solution allowing you to manage all your Nessus scanners, schedule scans, manage credentials, perform asset discovery and analyze their results and the remediation efforts of the IT and security personnel from a central console. Click below for more information:
SC
SecurityCenter
網際網路 | 受保護模式: 啟動
100%


Tenable Network Security - Windows Internet Explorer
http://www.nessus.org/download/nessus_download.php
Google
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
我的最愛
取得更多附加元件
建議的網站
★ISunfar 愛順發購物網 - ...
Tenable Network Security
網頁(P)
安全性(S)
工具(O)
TENABLE
Network Security
Solutions
Products
Nessus®
Demos
Partners
Online Store
You need to subscribe to a plugin feed to be able to use Nessus. Please click here to get one for free (home users) or to purchase one (corporate users).
PF
ProfessionalFeed™
Download Nessus 4.2.1:
Windows XP, 2003, Vista, 2008 & 7 (64 bits):
Nessus-4.2.1-amd64.msi (11601 KB)
Windows XP, 2003, Vista, 2008 & 7 (32 bits):
Nessus-4.2.1-i386.msi (11113 KB)
SECURITY CENTER 3
網際網路 | 受保護模式: 啟動
100%

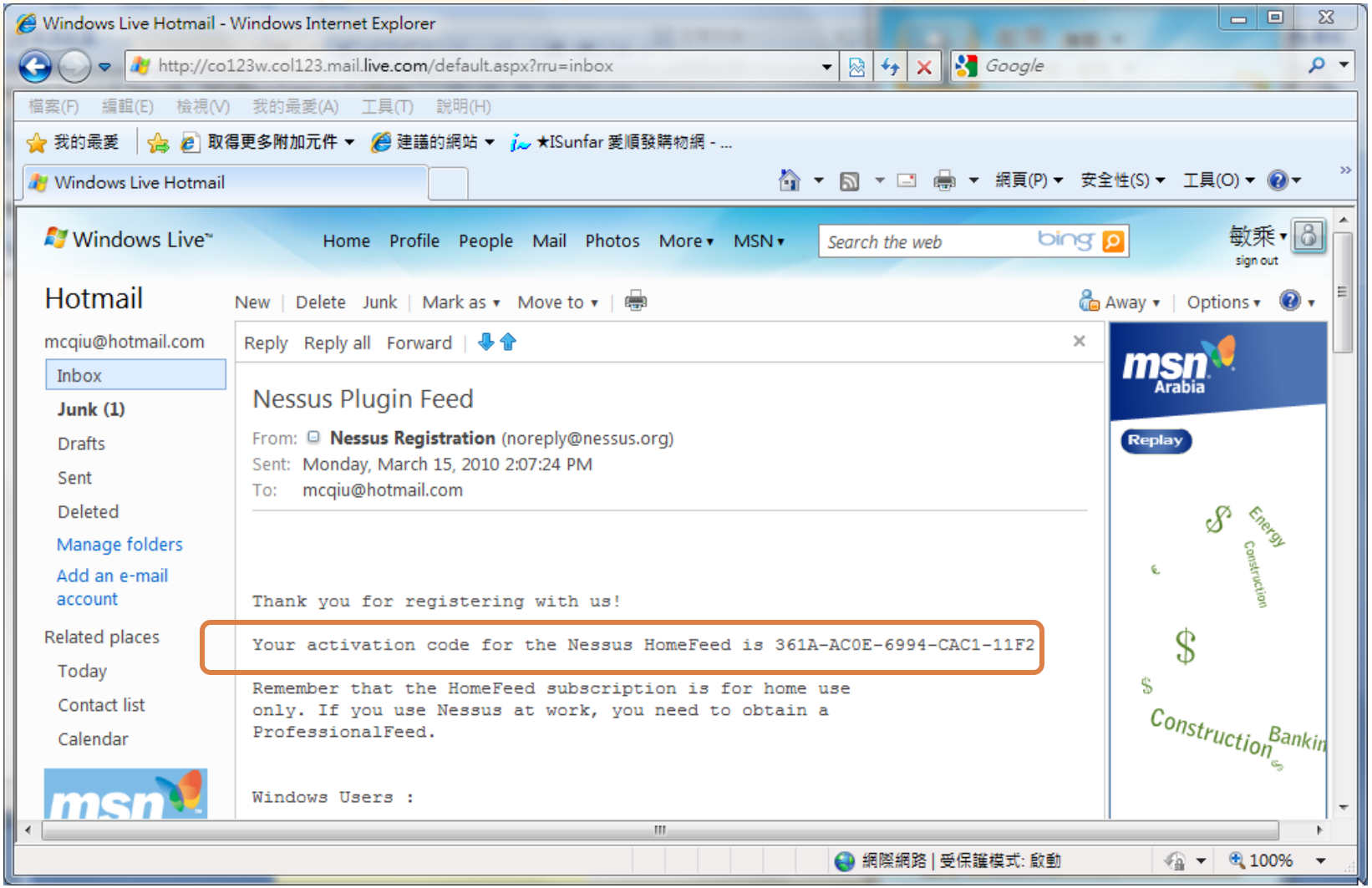
# Plugin Feed


Tenable Network Security - Windows Internet Explorer
http://www.nessus.org/plugins/?view=register-info
Tenable Network Security
TENABLE
Network Security
Solutions
Products
Nessus®
Demos
Partners
Online Store
Select a subscription
ProfessionalFeed™
HomeFeed™
Using Nessus at work? The ProfessionalFeed subscription is required for all uses of Nessus
Using Nessus at home? The HomeFeed subscription is free and for Home use only.

# HomeFeed Register



# Home Feed e-mail



# 安裝

```
# rpm -ivh Nessus-4.2.1-es5.i386.rpm
Preparing...                ########################################### [100%]
   1:Nessus                 ########################################### [100%]
 - Please run /opt/nessus//sbin/nessus-adduser to add a user
 - Register your Nessus scanner at http://www.nessus.org/register/ to obtain
   all the newest plugins
 - You can start nessusd by typing /sbin/service nessusd start
```

# 建立第一個使用者

**# /opt/nessus/sbin/nessus-adduser**

**Using /var/tmp as a temporary file holder**

**Add a new nessusd user**

**----------**

**Login : 帳號名稱**

**Login password :輸入密碼**

**Login password (again) :確認密碼**

# 設定使用者rule

```
# /opt/nessus/sbin/nessus-adduser
Login : student
Authentication (pass/cert) : [pass]
Login password :
Login password (again) :
Do you want this user to be a Nessus 'admin' user ? (can upload plugins, etc...) (y/n) [n]: y
User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that student has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser manual for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done :
(the user can have an empty rules set)
```

按空白鍵結束

# 使用者帳號管理

- 新增使用者
  /opt/nessus/sbin/nessus-adduser
- 刪除使用者
  /opt/nessus/sbin/nessus-rmuser
- 重設使用者密碼
  /opt/nessus/sbin/chpasswd
- 使用者資料
  - /opt/nessus/var/nessus/users/目錄下

# 向Nessus註冊

```
# /opt/nessus/bin/nessus-fetch --register 361A-AC0E-6994-CAC1-
    11F2
Your activation code has been registered properly - thank you.
Now fetching the newest plugin set from plugins.nessus.org...
Your Nessus installation is now up-to-date.
If auto_update is set to 'yes' in nessusd.conf, Nessus will
update the plugins by itself.
```

# 啟動nessus server

- 啟動nessusd

  # service nessusd start

  Starting Nessus services: [ OK ]

- 查看nessusd服務是否正常啟動

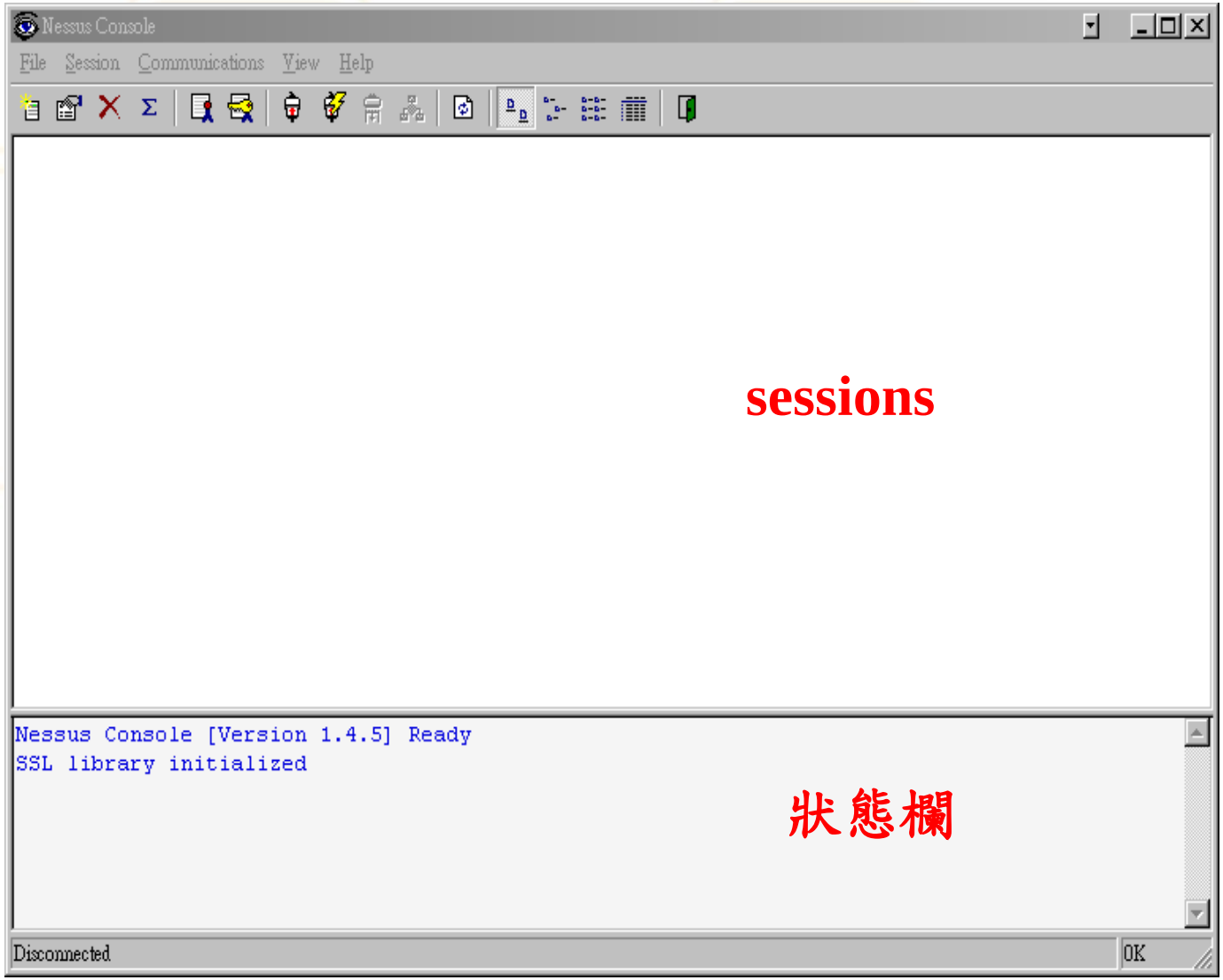
  [root@STATION40 ~]# ps -ef | grep nessus

  root 3369 1 0 18:13 ? 00:00:00 /opt/nessus//sbin/nessus-service -q -D

  root 3370 3369 0 18:13 ? 00:00:06 nessusd -q

  root 3453 3421 0 19:30 pts/0 00:00:00 grep nessus

# nessusWX

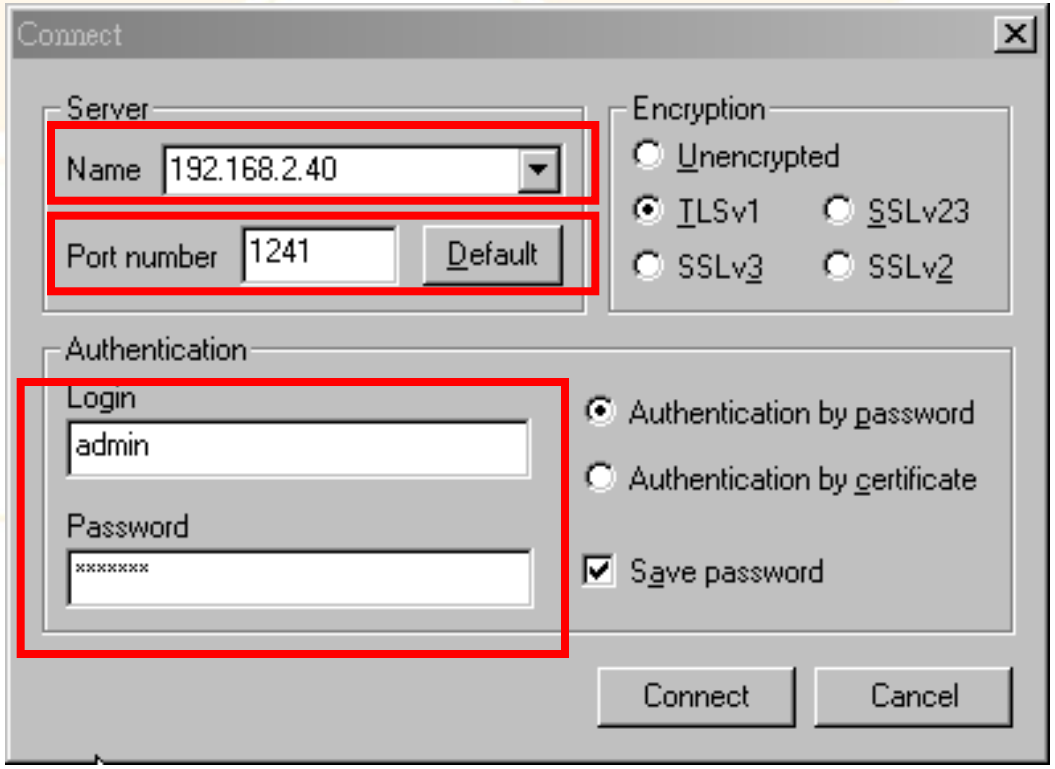

Nessus Console
File Session Communications View Help
sessions
Nessus Console [Version 1.4.5] Ready
SSL library initialized
狀態欄
Disconnected
OK

# 連結至伺服器端

- Communications ->Connect

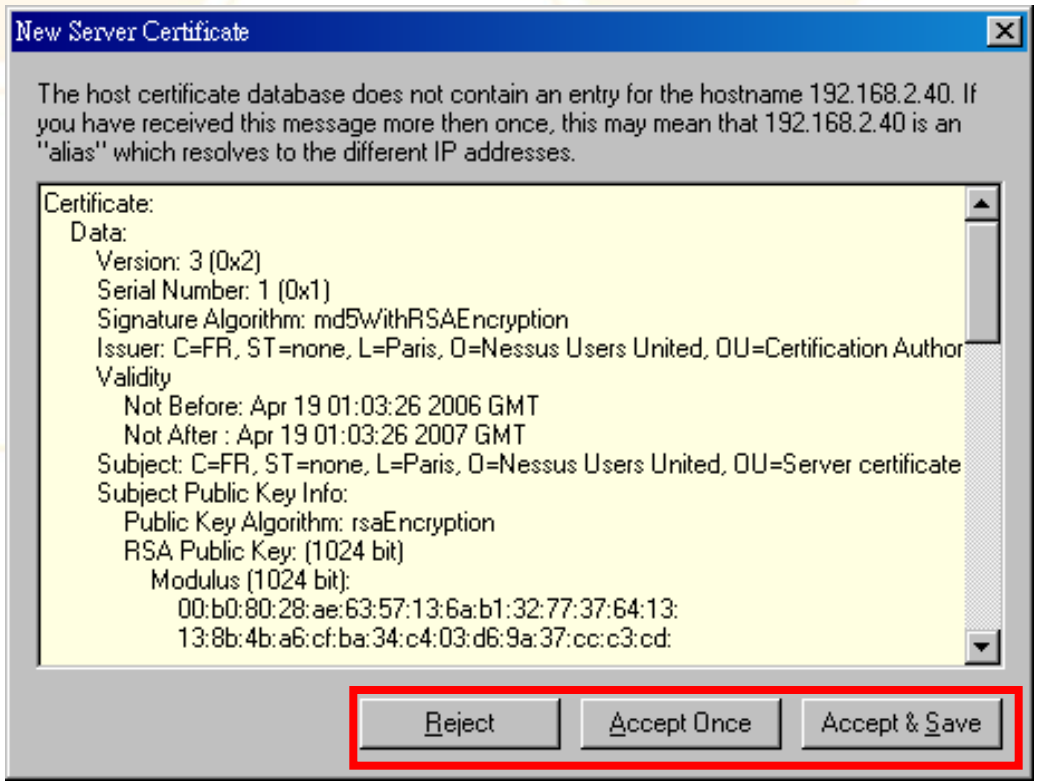
**Server IP and port**

**登入帳號及密碼**



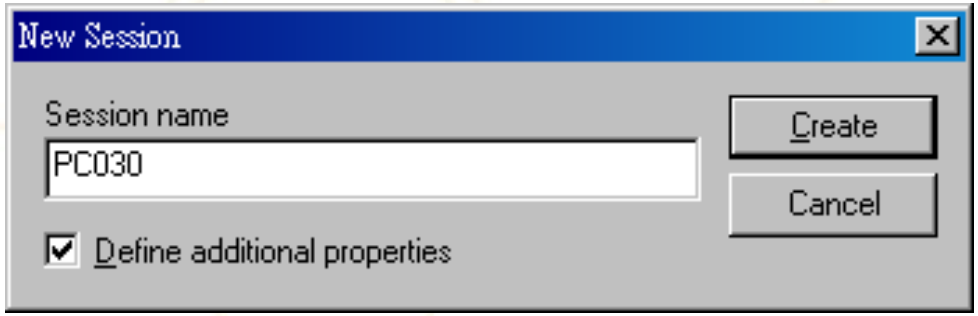
# Server certificate

- 第一次登入伺服器時會詢問是否接受伺服器憑證，需選擇「Accept Once」或「Accept & Save」才能繼續

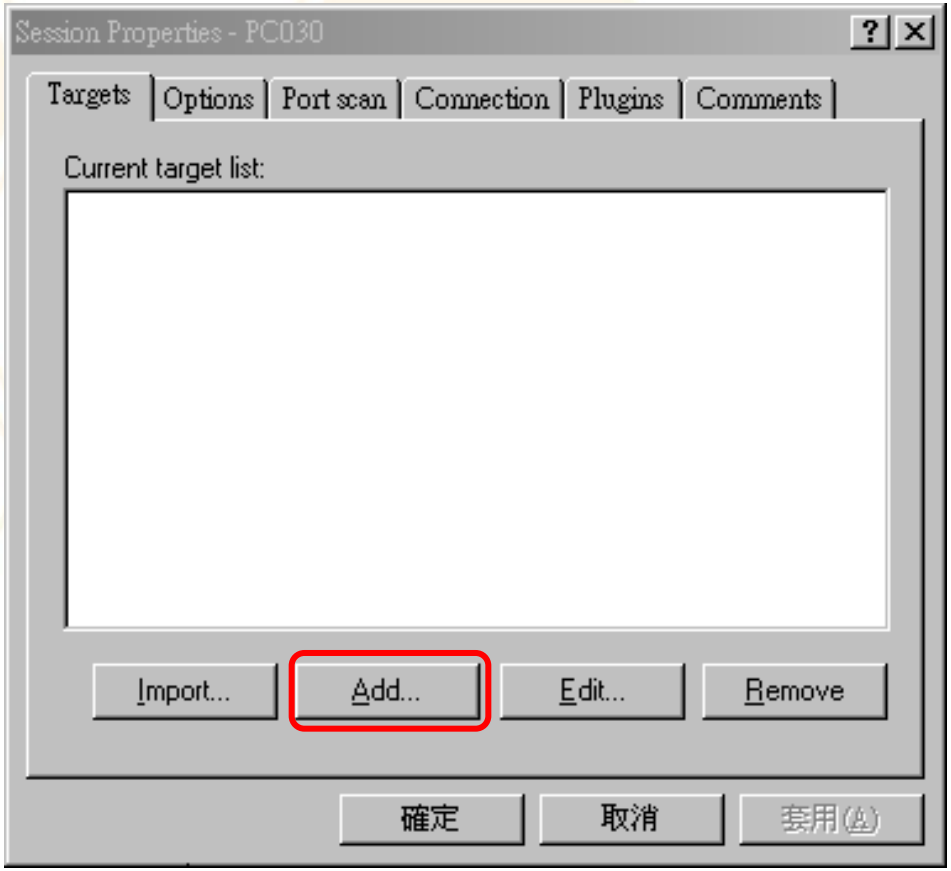


# 建立session

- 「Sessions」->「 New 」
- 輸入session名稱

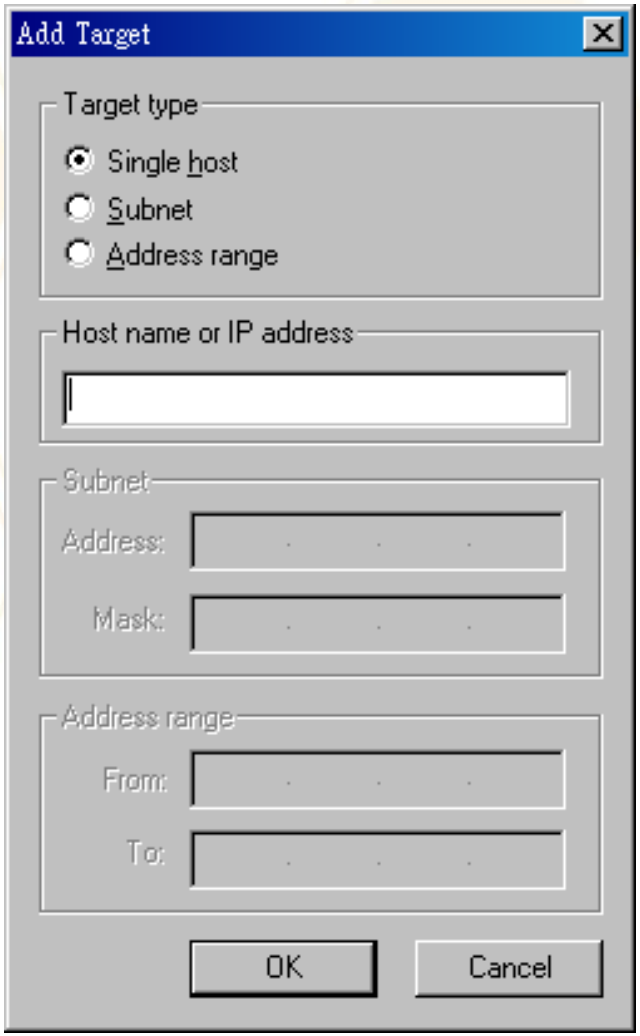


- Targets
- Options
- Port scan
- Connection
- Plugins
- Comments



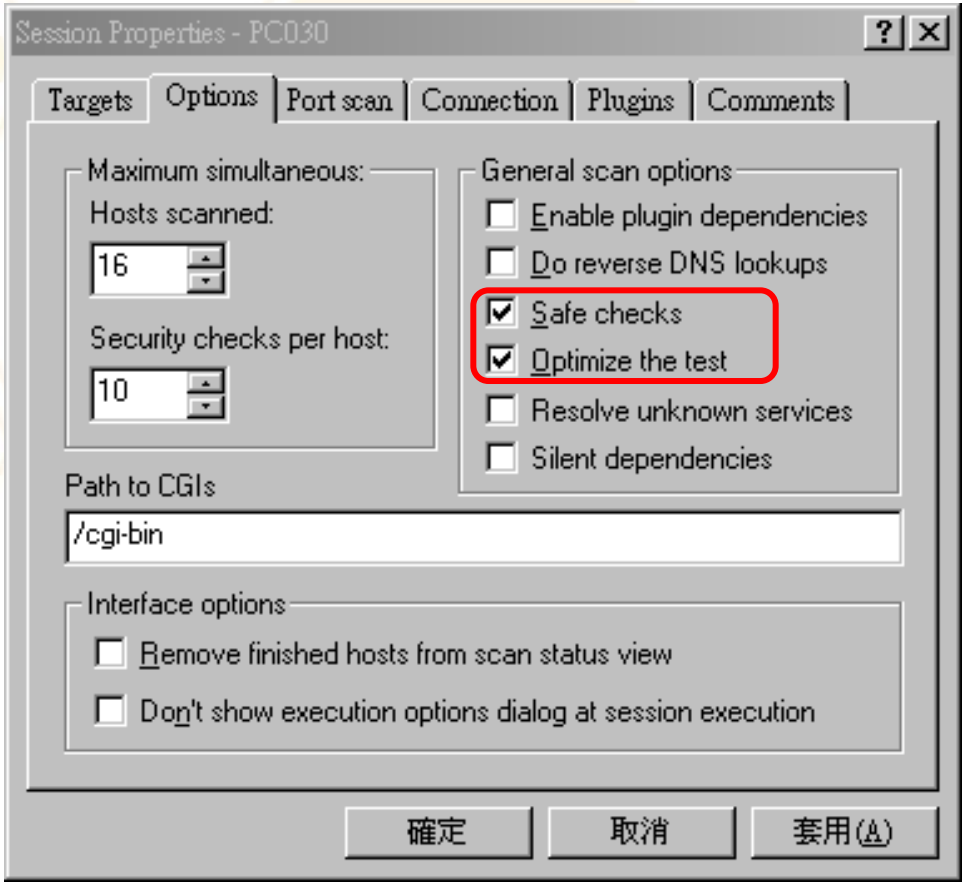
# 設定掃描目標

- Sigle host
  - 掃描單一主機
- Subnet
  - 掃描整個子網段
- Address range
  - 掃描特定IP範圍



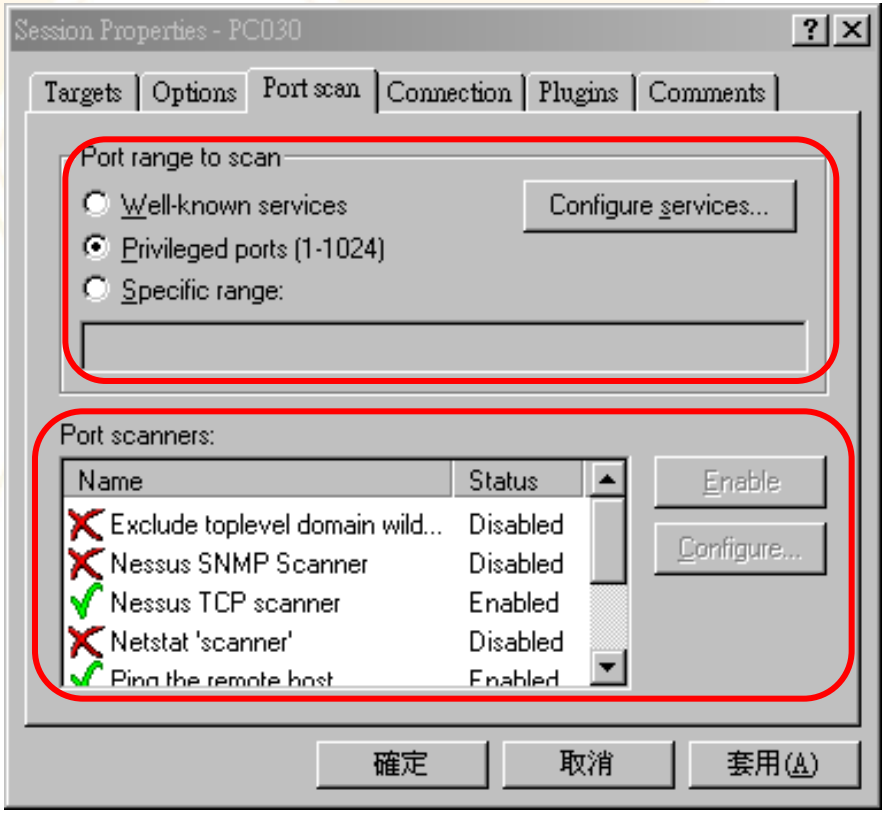
# 掃描選項

- Safe checks
  - 不實施危險性掃描項目，以避免造成系統受損

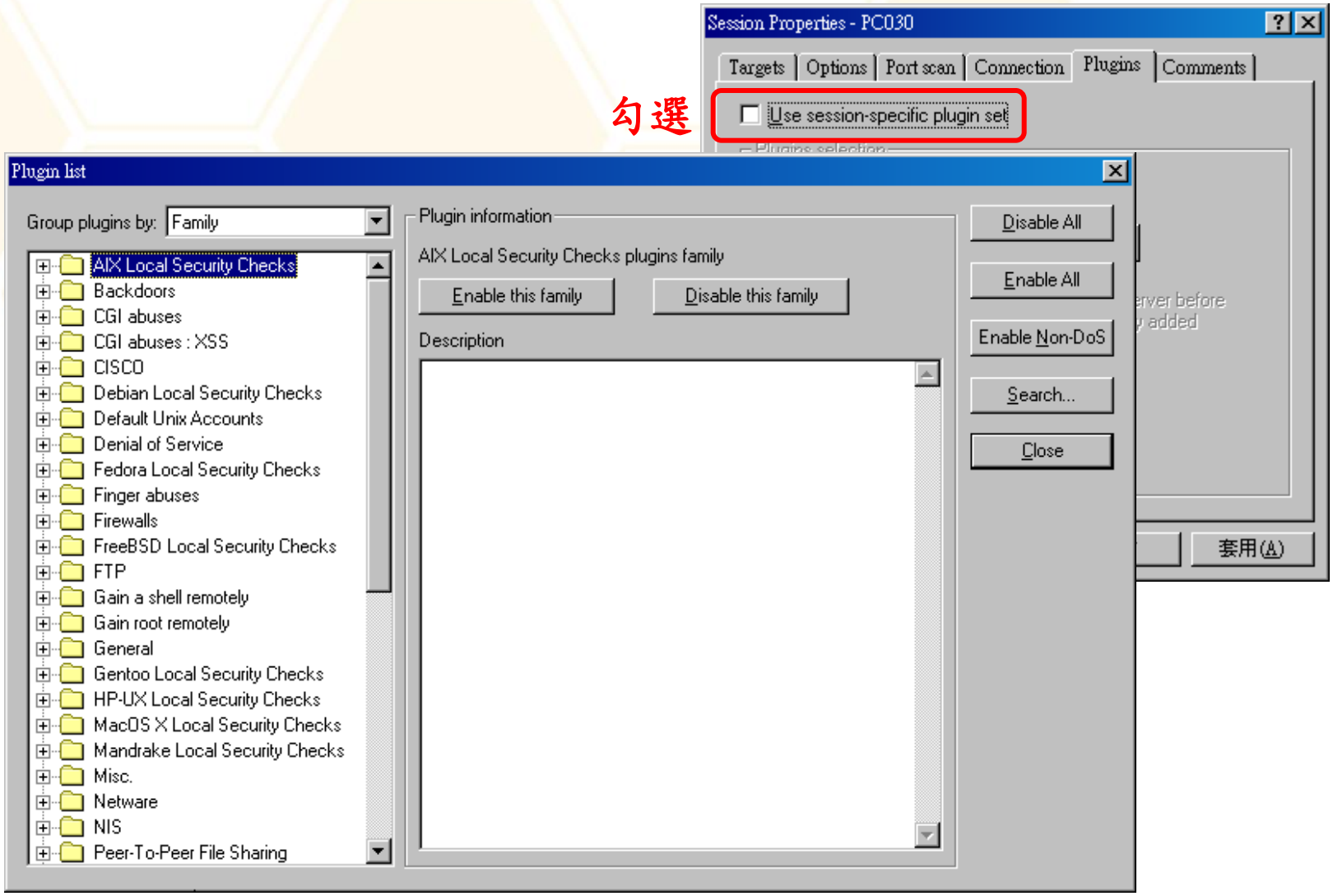


# Port scan選項

- 設定掃描通訊埠範圍
- 設定掃描方式

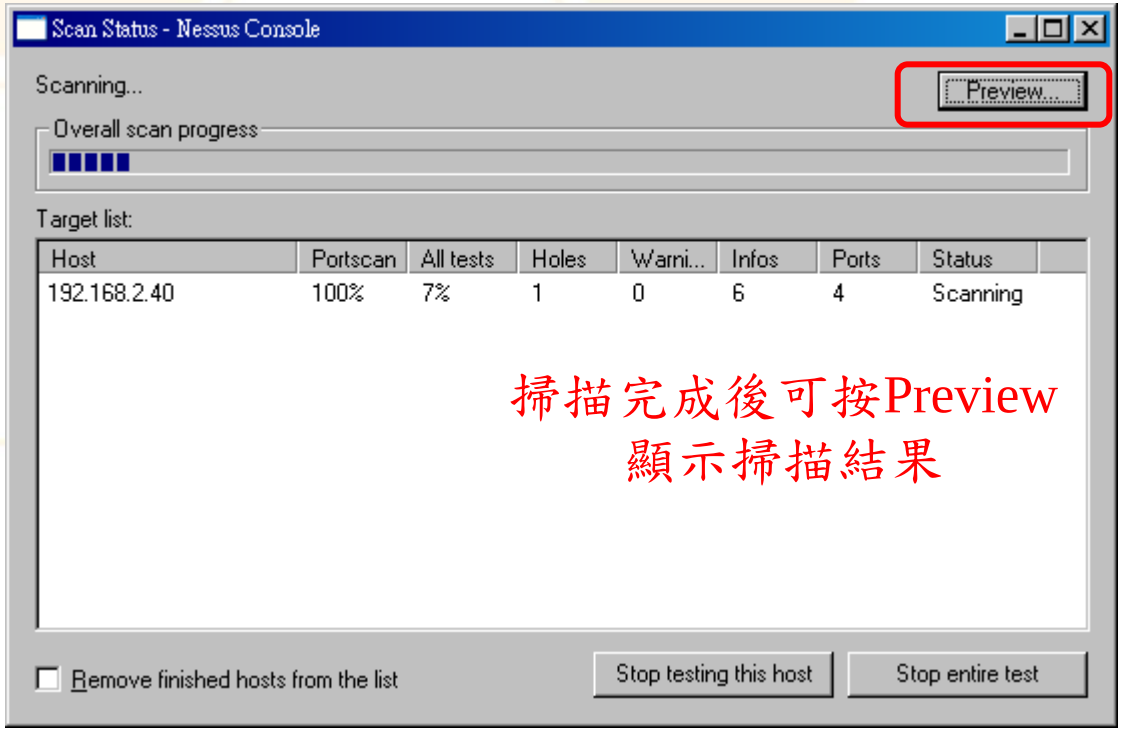


# 選擇plugin

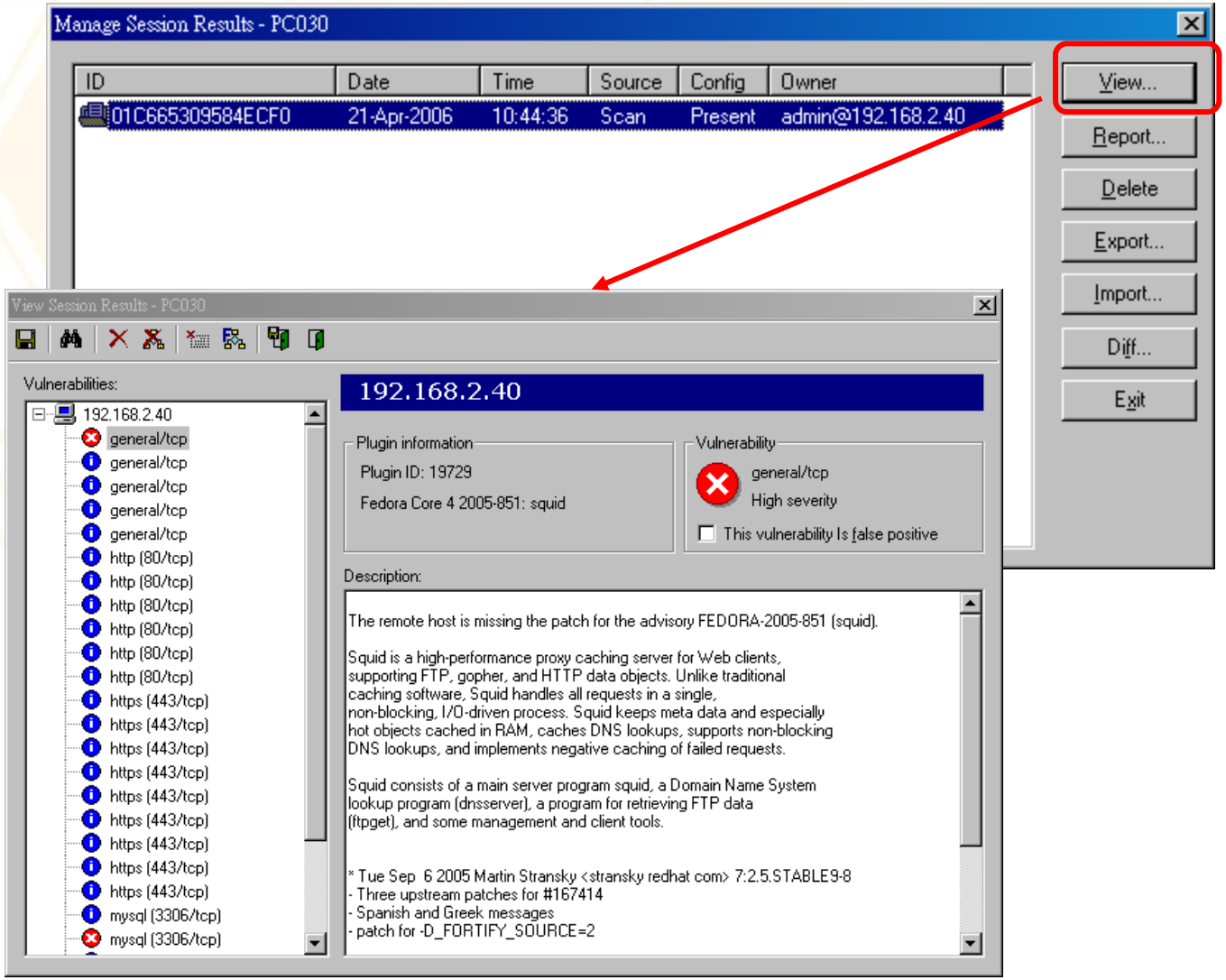

Session Properties - PC030
Targets
Options
Port scan
Connection
Plugins
Comments
勾選
Use session-specific plugin set
套用(A)
Plugin list
Group plugins by:
Family
AIX Local Security Checks
Backdoors
CGI abuses
CGI abuses : XSS
CISCO
Debian Local Security Checks
Default Unix Accounts
Denial of Service
Fedora Local Security Checks
Finger abuses
Firewalls
FreeBSD Local Security Checks
FTP
Gain a shell remotely
Gain root remotely
General
Gentoo Local Security Checks
HP-UX Local Security Checks
MacOS X Local Security Checks
Mandrake Local Security Checks
Misc.
Netware
NIS
Peer-To-Peer File Sharing
Plugin information
AIX Local Security Checks plugins family
Enable this family
Disable this family
Description
Disable All
Enable All
Enable Non-DoS
Search...
Close

# 執行弱點掃描

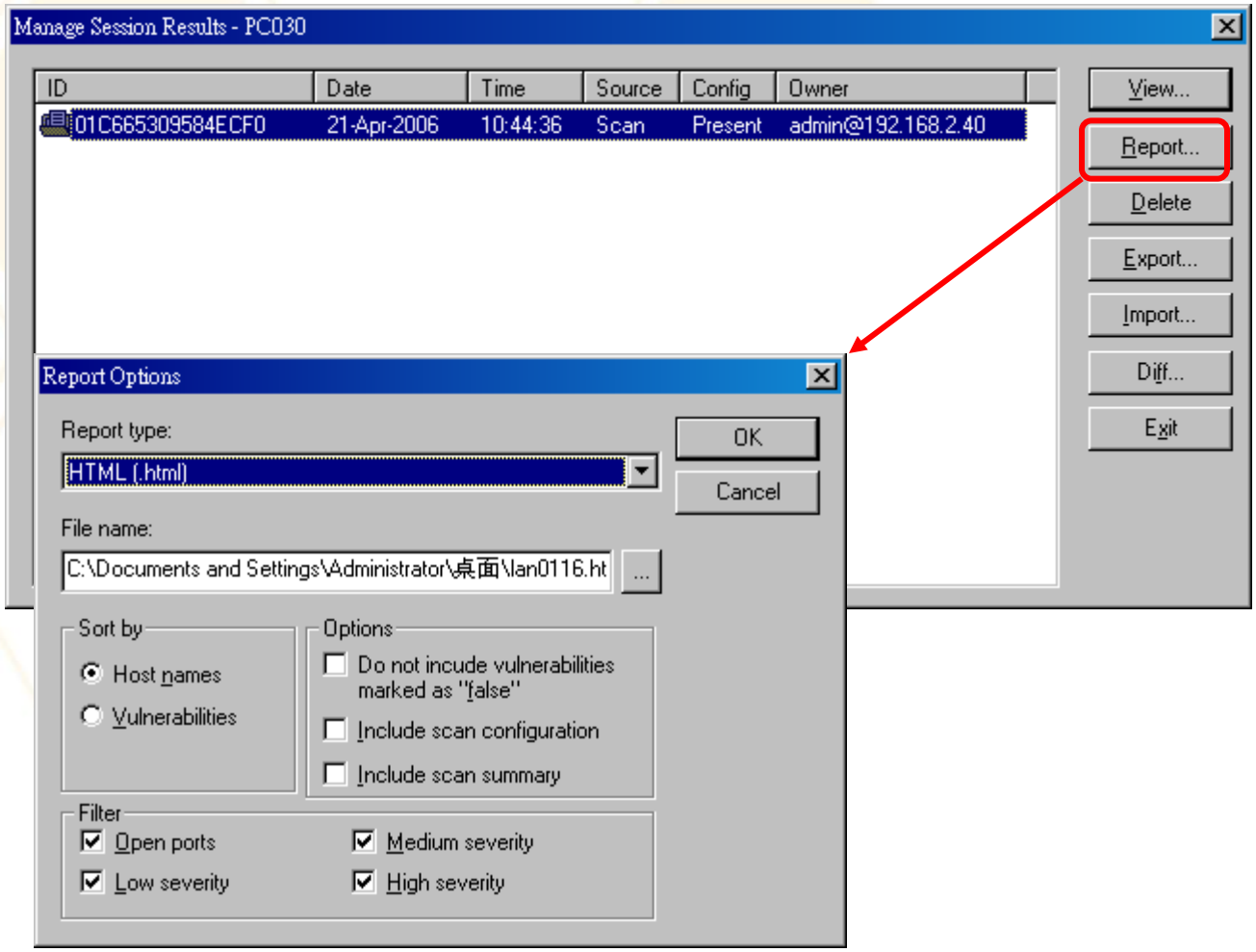
- 在面板上點選「session」=->「 Execute…」



# 觀看掃描結果


Manage Session Results - PC030
ID
Date
Time
Source
Config
Owner
01C665309584ECF0
21-Apr-2006
10:44:36
Scan
Present
admin@192.168.2.40
View...
Report...
Delete
Export...
Import...
Diff...
Exit
View Session Results - PC030
Vulnerabilities:
192.168.2.40
general/tcp
general/tcp
general/tcp
general/tcp
general/tcp
http (80/tcp)
http (80/tcp)
http (80/tcp)
http (80/tcp)
http (80/tcp)
http (80/tcp)
https (443/tcp)
https (443/tcp)
https (443/tcp)
https (443/tcp)
https (443/tcp)
https (443/tcp)
https (443/tcp)
https (443/tcp)
https (443/tcp)
mysql (3306/tcp)
mysql (3306/tcp)
192.168.2.40
Plugin information
Plugin ID: 19729
Fedora Core 4 2005-851: squid
Vulnerability
general/tcp
High severity
This vulnerability Is false positive
Description:
The remote host is missing the patch for the advisory FEDORA-2005-851 (squid).
Squid is a high-performance proxy caching server for Web clients,
supporting FTP, gopher, and HTTP data objects. Unlike traditional
caching software, Squid handles all requests in a single,
non-blocking, I/O-driven process. Squid keeps meta data and especially
hot objects cached in RAM, caches DNS lookups, supports non-blocking
DNS lookups, and implements negative caching of failed requests.
Squid consists of a main server program squid, a Domain Name System
lookup program (dnsserver), a program for retrieving FTP data
(ftpget), and some management and client tools.
* Tue Sep 6 2005 Martin Stransky <stransky redhat com> 7:2.5.STABLE9-8
- Three upstream patches for #167414
- Spanish and Greek messages
- patch for -D_FORTIFY_SOURCE=2

# 產生掃描報告


Manage Session Results - PC030
ID
Date
Time
Source
Config
Owner
01C665309584ECF0
21-Apr-2006
10:44:36
Scan
Present
admin@192.168.2.40
View...
Report...
Delete
Export...
Import...
Diff...
Exit
Report Options
Report type:
HTML (.html)
OK
Cancel
File name:
C:\Documents and Settings\Administrator\桌面\lan0116.ht
...
Sort by
Host names
Vulnerabilities
Options
Do not incude vulnerabilities marked as "false"
Include scan configuration
Include scan summary
Filter
Open ports
Medium severity
Low severity
High severity

# plugin更新

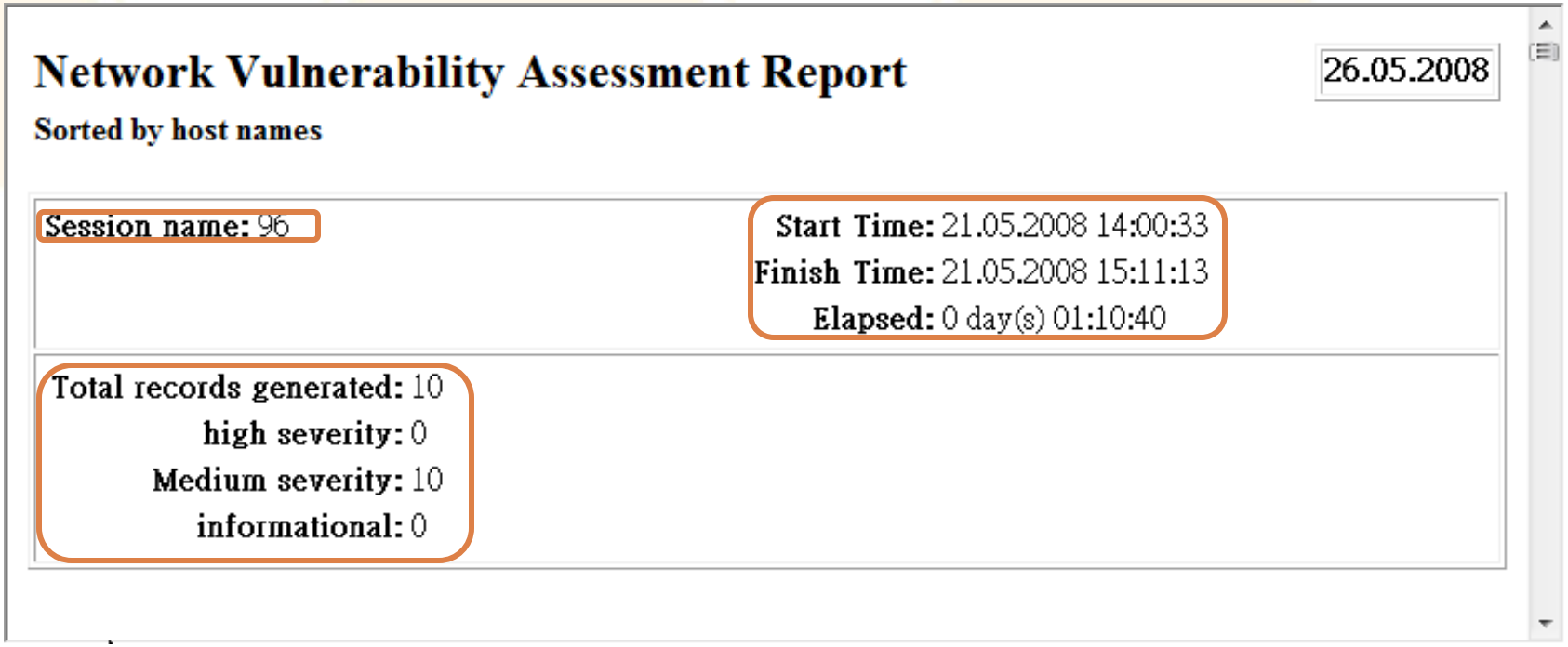
- Nessus 2.0版的更新方式：
  - /usr/local/sbin/nessus-update-plugins
  - 可以放到crontab中讓系統定期更新plug-in
  - Plugins的位置： /usr/local/lib/nessus/plugins
- Nessus 3.0版本之後
  - 可設定啟動nessusd服務後自動更新

  設定檔：/opt/nessus/etc/nessus/nessusd.conf

  auto_update = yes
  - 手動更新

  # /opt/nessus/sbin/nessus-update-plugins

# Nessus報表：表頭



## Network Vulnerability Assessment Report

26.05.2008

**Sorted by host names**

**Session name:** 96

**Start Time:** 21.05.2008 14:00:33
**Finish Time:** 21.05.2008 15:11:13
**Elapsed:** 0 day(s) 01:10:40

**Total records generated:** 10
**high severity:** 0
**Medium severity:** 10
**informational:** 0

# Nessus報表：弱點描述

- 服務描述(Service)
  - 包含服務名稱及使用的通訊埠
- (危險等級)Severity
  - 三個等級：low、medium及high
- Description
  - 摘要(Synopsis)
  - 描述(Description)
  - 解決方案(Solution)
  - (風險級數)Risk factor

# samba版本漏洞

**Synopsis :**

It is possible to execute code on the remote host through samba.

**Description :**

The version of the Samba server installed on the remote host is affected by multiple heap overflow vulnerabilities, which can be exploited remotely to execute code with the privileges of the samba daemon.

**See also :**

http://www.samba.org/samba/security/CVE-2007-2446.html

**Solution :**

Upgrade to Samba version 3.0.25 or later.

**Risk factor :**

Critical / CVSS Base Score : 10.0

(CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVE : CVE-2007-2446

BID : 23973, 24195, 24196, 24197, 24198

Other references : OSVDB:34732

# php版本漏洞

**Synopsis :**

The remote web server uses a version of PHP that is affected by multiple flaws.

**Description :**

According to its banner, the version of PHP installed on the remote host is older than 5.2.5. Such versions may be affected by various issues, including but not limited to several buffer overflows.

**See also :**

http://www.php.net/releases/5_2_5.php

**Solution :**

Upgrade to PHP version 5.2.5 or later.

**Risk factor :**

High / CVSS Base Score : 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVE : CVE-2007-4887
BID : 26403

# 網路分享

**Synopsis :**

It is possible to access a network share.

**Description :**

The remote has one or many Windows shares that can be accessed through the Network.
Depending on the share rights, it may allow an attacker to read/write confidential data.

**Solution :**

To restrict access under Windows, open the explorer, do a right click on each shares, go to the 'sharing' tab, and click on 'permissions'

**Risk factor :**

High / CVSS Base Score : 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVE : CVE-1999-0519, CVE-1999-0520
BID : 8026
Other references : OSVDB:299

# SNMP使用預設community

**Synopsis :**

The community name of the remote SNMP server can be guessed.

**Description :**

It is possible to obtain the default community names of the remote SNMP server. An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allow such modifications).

**Solution :**

Disable the SNMP service on the remote host if you do not use it, filter incoming UDP packets going to this port, or change the default community string.

**Risk factor :**

High / CVSS Base Score : 7.5

(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

**Plugin output :**

The remote SNMP server replies to the following default community strings : private public

CVE : CVE-1999-0186, CVE-1999-0254, CVE-1999-0516,

CVE-1999-0517, CVE-2004-0311, CVE-2004-1474

BID : 11237, 10576, 177, 2112, 6825, 7081, 7212, 7317, 9681, 986

Other references : IAVA:2001-B-0001, OSVDB:10206

# Windows系統漏洞

**Synopsis :**

Arbitrary code can be executed on the remote host due to a flaw in the 'server' service.

**Description :**

The remote host is vulnerable to a buffer overrun in the 'Server' service which may allow an attacker to execute arbitrary code on the remote host with the 'System' privileges.

**Solution :**

Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://www.microsoft.com/technet/security/bulletin/ms06-040.mspx

**Risk factor :**

Critical / CVSS Base Score : 10.0
(CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVE : CVE-2006-3439
BID : 19409

# CVE

- CVE: Common Vulnerability and Exploit
  - is a dictionary of public known information security and explosures
  - http://cve.mitre.org/
- CVE-xxxx-xxxx (xxxx為四位數字)
  - 第一組數字表示年度，第二組數字表示該年度第組個被發現的安全弱點
- CAN-xxx-xxxx (xxxx為四位數字)
  - CAN為被發現但尚未通過CVE委員評估，為一弱點之候選
  - 當通過委員會評估後，CAN會改成CVE，但其後的數字不會改變

# CVSS

- CVSS：Common Vulnerability Score System
- 目的：
  - 在於提供一套檢查資訊系統安全漏洞的標準方式，並給予每個漏洞評分，可供修補漏洞的先後順序做為重要的參考，所有的漏洞評分皆透過資安專家嚴格的評量
- 是由美國國家基礎建設諮詢委員會(NIAC)委託製作，並且受到業界的支持

# 可能的誤判清況

- 應用系統判斷錯誤
  - 如在linux server上出現IIS或MS-SQL
- 已修補的弱點
  - Nessus利用banner判斷
  - 套件已修補但banner未改變
  - 不同系統之修補版本不同
- 自行開的服務
  - 使用自訂的通訊埠
  - 使用其它常用服務的通訊埠

# 系統安全強化的步驟

- 系統更新
  - 定期更新套件
  - 修改不安全的設定
  - 關閉不必要的服務
- 弱點掃描
- 根據弱點掃描報告進行修補
- 再次進行弱點掃描，以確認安全漏洞是否已修補

# Patch update

- Linux
  - 自行下載rpm套件或原始碼更新
  - 利用apt或yum進行套件更新
- Windows
  - Windows Update
  - Microsoft Update (Windows XP or late)
  - 「開始」→「程式集」→「Windows Update」
  - SMS (System Management Server)

# 結論

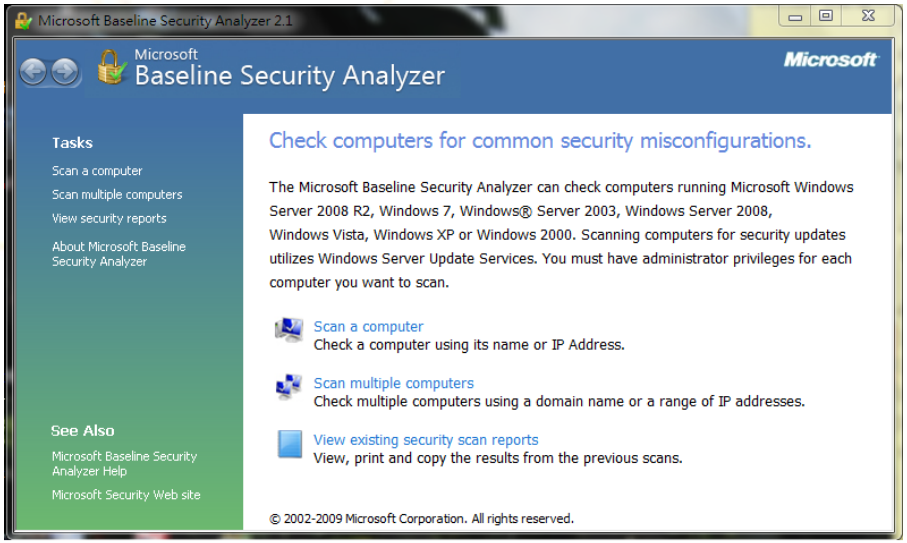
- 定期執行弱點掃描是資安工作的第一步，也是最重要的一步
- 需經常留意安全通報，發現自己安裝之軟體套件是否出現新的安全漏洞
  - 建議訂閱資安通報
- 發現安全漏洞應儘速進行修補，若不能修補應考慮進行接取控制或其它替代方案
- 未經同意對其它人的系統進行掃描是違法，進行掃描前最好有書面同意文件

# 安全通報網站

- 國內：
  - TWCERT/CC:http://www.cert.org.tw/
  - GSNCERT: http://www.gsn-cert.nat.gov.tw/
- 國外:
  - http://nvd.nist.gov/
  - http://www.kb.cert.org/vuls
- 系統/軟體官方網站
- 資安產品網站

# MBSA

- Microsoft Baseline Security Analyzer
- 微軟推出的簡易安全工具，用來檢查windows系統是否有未更新的安全漏洞
- 最後的release版本為2.1版
- http://technet.microsoft.com/en-us/security/cc184923.aspx



# Open source Web vulnerability scanner

- Nikto：http://cirt.net/nikto2
- Paros proxy：http://www.parosproxy.org/index.shtml
- Web Scarab：http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project
- Wikto：http://www.sensepost.com/research/wikto/
- Burp Suite：http://www.portswigger.net/suite/

# 商業版web vulnerability scanner

- Web Inspect：
  - https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11-201-200%5E9570_4000_100__
- AppScan
  - http://www-01.ibm.com/software/awdtools/appscan/
- Acunetix Web Security Scanner
  - http://www.acunetix.com/

# Nikto

- http://cirt.net/nikto2
- 開放源web 伺服器掃描工具
- 針對伺服器版本、檔案等進行快速掃描(非暗中掃描)
- 需求
  - SSL support the Net::SSLeay PERL module must be installed
- 安裝

  # wget http://cirt.net/nikto/nikto-current.tar.gz

  # tar -zxvf nikto-current.tar.gz

  # cd nikto-2.1.1/

- 進行更新

  # ./nikto.pl –update

- 基本的測試

  # perl nikto.pl –h host_IP

  # perl nikto.pl –h host_IP –p 443

  # perl nikto.pl –h https://host_IP/

  # perl nikto.pl –h host_IP –p 443 -ssl

# Paros proxy

- URL： http://www.parosproxy.org/index.shtml
- JAVA-based 網頁應用程式安全工具
  - XSS
  - SQL Injection
- 安裝
  - 安裝JRE(JDK)
  - 下載PAROS porxy： http://www.parosproxy.org/download.shtml

MileSCAN ParosPro

# Q & A