Open VAS 弱點掃描講義

一、常見弱點與分析

滲透性測試(模擬駭客進行「合法」的網絡入侵測試)

最新攻擊趨勢

- 戰術化滲透測試(Advanced Persistent Threats, APT)

  傳統滲透測試

  - 針對特定服務或弱點
  - 通常無事先規劃測試方針
  - 測試效能與效率較不顯著

  戰術化滲透測試

  - 測試前蒐集目標資訊
  - 根據目標資訊擬定測試方針
  - 測試效能與效率較高

- 戰術化滲透測試流程

  研究與偵查目標(分析目標)

  - 盡可能地取得受測目標的資訊

  準備滲透工作

  - 根據所蒐集的資訊擬定測試方針

  進行滲透

  - 根據測試方針執行滲透測試

  弱點利用

  - 利用滲透測試過程中所發現的弱點

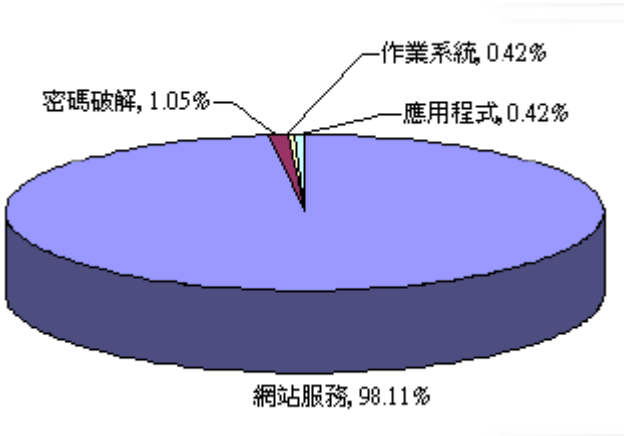
- 研究與偵查目標(分析目標)

  受測目標資訊

  - IP、作業系統、伺服器版本及實體位置等資訊
  - 相關人員資訊，如管理者姓名、職稱及電話等資訊
  - 信賴關係

- 利用網際網路資源

  - 低成本，多爲免費資源
  - 低風險，受測目標不易察覺
  - 高價值，可取得大量資料
- 2010 中國企業安全報告
  - 25 萬個網站遭植入病毒或木馬
  - 90%的傳統企業內部網路曾被入侵
- 2010 年 12 月資安人雜誌
  - 某網路銀行遭駭客入侵，外洩超過 16,000 筆客戶資料
- 2011 年 3 月 CNCERT 報告
  - 有 4,635 個政府網站遭入侵
- 資料來源(來自國家資通安全)
  - 98 年 4 月~ 100 年 3 月
  - 73 個網站，474 個弱點



測試類型	數量	百分比
網站服務	465 個	98.11%
密碼破解	5 個	1.05%
作業系統	2 個	0.42%
應用程式	2 個	0.42%

- 弱點分類

測試類別	說明	測試類別	說明
設定管理	・顯示錯誤資訊弱點 ・網站結構資訊洩露弱點	邏輯漏洞	網站功能設計缺失弱點 附件上傳弱點
使用者認證	帳號列舉弱點	輸入驗證	XSS 弱點 SQL Injection 弱點
連線管理・	連線管理機制弱點	Web Service	XML 資料處理弱點

測試類別	說明	測試類別	說明
使用者授權	網站授權機制弱點 目錄跨越弱點	Ajax	Ajax 弱點

- 弱點分類統計

測試類別	數量	百分比
輸入驗證	220 個	47.31%
設定管理	170 個	36.56%
使用者授權	46 個	9.89%
邏輯漏洞	23 個	4.95%
使用者認證	5 個	1.08%
連線管理	1 個	0.22%

- 98 年與 99 年弱點差異分析

98 年 4 月~99 年 3 月
50 個網站(408 個弱點)

測試類別	數量	百分比
輸入驗證	197 個	48.28%
設定管理	156 個	38.24%
使用者授權	34 個	8.33%
邏輯漏洞	17 個	4.17%
使用者認證	4 個	0.98%

99 年 4 月~100 年 3 月
23 個網站(57 個弱點)

測試類別	數量	百分比
輸入驗證	23 個	40.35%
設定管理	14 個	24.56%
使用者授權	12 個	21.05%
邏輯漏洞	6 個	10.53%
使用者認證	1 個	1.75%
連線管理	1 個	1.75%

- 98 年與 99 年弱點差異分析

蒐集 73 個台灣網站的 465 個網站服務弱點

– 仿照 OWASP Testing Guide 分為 8 個類別

– 主要分布於輸入驗證類別、設定管理類別及使用者授權類別等 3 個類別，約占網站服務弱點的 93.76%

- 探討 98 年與 99 年弱點差異探討

測試類別	98 年	99 年
設定管理	38.24%	24.56%
輸入驗證	48.28%	40.35%
邏輯漏洞	4.17%	10.53%
使用者授權	8.33%	21.05%

二、滲透測試軟體介紹

(資料取自行政院國家資通安全網站)

- Burp Suite

  優點

– 利用 proxy 對網站做 spider，所以只要瀏覽到網頁，就能獲得網頁資訊，不易被檔住

– 檢測深度可透過 proxy 自行加深

缺點

– 須付費才能使用 scanner 功能進行自動檢測，否則只能使用 intruder 功能以人工方式進行判斷弱點

工具與環境限制

– 需安裝 Java JDK/JRE 才可執行 burp suite

檢測項目

1. Cross Site Scripting
2. Injection Flaws
3. 資訊揭露與不適當錯誤處置

- THC-Hydra

優點

– 此工具破解密碼十分快速

– 可由 output 檔案得知是否正確解得帳號密碼

缺點

– 在使用數次後，工具操作上會有些錯誤情形發生，可重新啟動再次檢測

檢測項目

弱密碼

- Nikto

優點

–此工具檢測網站伺服器與應用程式的版本及設定不當相關弱點之功能極佳

–檢測速度快

–可自動更新套件

–操作簡單

缺點

－檢測深度較淺

工具與環境限制

－需安裝 Perl 環境才可執行 Nikto

－可能無法檢測有 IDS/IPS 或應用層防火牆之網站伺服器

檢測項目

1. Cross Site Scripting (XSS，跨網站腳本攻擊)
2. Injection Flaws (注入碼攻擊)
3. 資訊揭露與不適當錯誤處置
4. 不安全的伺服器設定
5. 不安全的伺服器版本
6. 不安全的應用程式套件

- Grendel-Scan

優點

－ 操作簡單，需輸入目標網站 URLs 與選擇所需之弱點檢測項目，即可完成掃描

－ 弱點檢測項目之描述十分詳盡

缺點

－ 檢測時產生大量 Log 檔，須準備大量硬碟空間以存放檔案

－ 掃描時間較一般工具久

檢測項目

1. Cross-Site Scripting (XSS，跨網站腳本攻擊)
2. Injection Flaws (注入碼攻擊)
3. 資訊揭露與不適當錯誤處置
4. 備份檔案
5. 不安全的伺服器設定

- w3af

優點

– 操作簡單，易於上手，plug in 功能說明詳細

– 可自行透過勾選 plug in 之方式選擇預測試之項目

– 檢測結果說明詳細(含 Cross-Site Scripting 不安全的伺服器設定弱點 url、測試字串與風險評估等等)

缺點

– Plug in 太多會造成檢測時間過長

– 有些 plug in 須互相搭配使用才有檢測效果工具與環境限制

– 需安裝 python 才可執行 w3af

檢測項目

1. Cross-Site Scripting
2. Injection Flaws
3. 資訊揭露與不適當錯誤處置
4. 疏於限制 URL 存取
5. 弱密碼
6. 不安全的伺服器設定

- Wikto

優點

– 圖形化介面操作方便

– 可以自行修改比對資料庫的字串

– 檢測報告說明清楚易懂

缺點

– 檢測時間較長

工具與環境限制

– 需要先註冊後才可下載，Windows 作業系統下需要安裝.NET framework，程式才可以使用

檢測項目

1. 資訊揭露與不適當錯誤處置

2. 疏於限制 URL 存取
3. 備份檔案
4. 不安全的伺服器設定

- Nessus

優點

– 圖形介面，容易上手
– 掃瞄速度快速
– 弱點檢測報告明確
– 提供大量 Plugins 檢測弱點

缺點

– 從 3.0 版開始，Nessus 改採專有軟體授權，但 2.x 系列仍會採用 Open source 授權

檢測項目

1. Cross Site Scripting (XSS，跨網站腳本攻擊)
2. Injection Flaws (注入碼攻擊)
3. 不安全的伺服器設定
4. 不安全的伺服器版本
5. 不安全的應用程式套件

三、OPEN-VAS 概念介紹與安裝

1.OPEN-VAS 概念

OpenVAS 代表 Open Vulnerability Assessment System(開放式弱點評估系統)表示全面性網路安全掃描的工具鏈，包含使用者圖形介面聯合各種第三方(third-party)安全測驗程式。因此整個伺服器核心是由一組網路弱點測試(etwork Vulnerability Tests (NVTs))來偵測遠端系統安全上的問題。

OpenVAS 是 GNU GPL (GNU General Public License)的自由軟體。OpenVAS 來自 Nessus 計劃，但 Nessus 變成一個專有產品，但 OpenVAS 自那時以來進展自身系統，雖然它的偵測程式部份仍沿用 Nessus 的寫法(NASL Nessus Attack Scripting Language)。

OpenVAS 軟體有五個部份所組成，都是由 OpenVAS 計劃所維護

主要有：

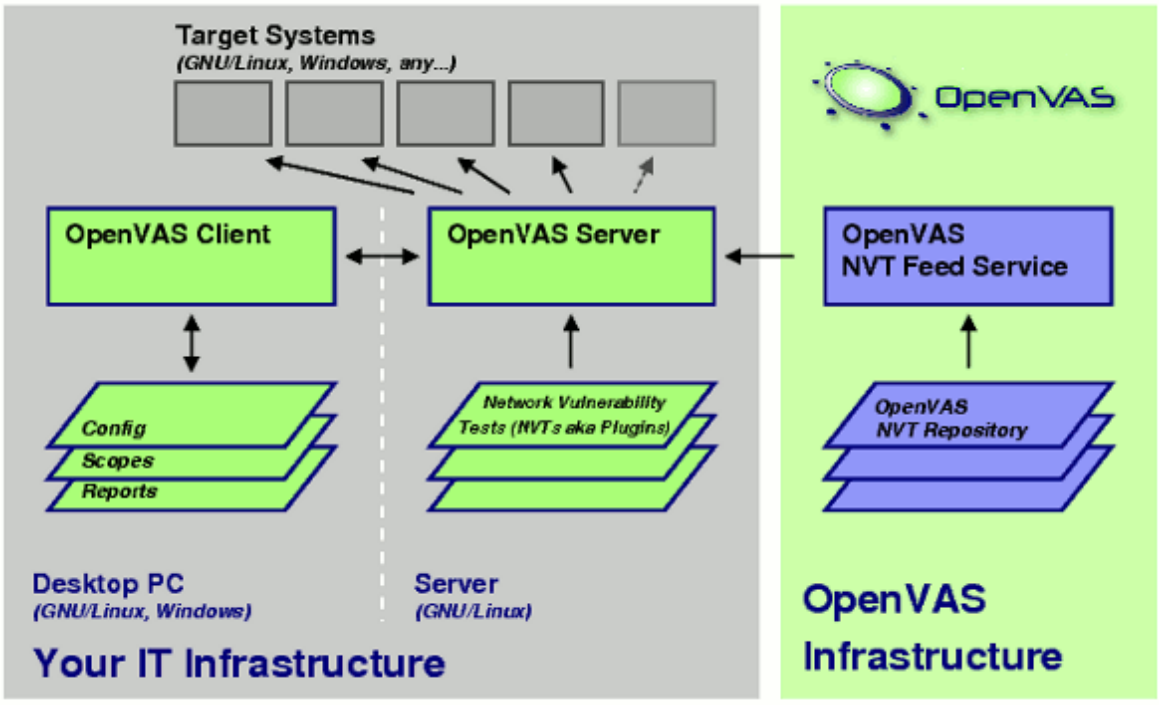
- OpenVAS-Server:OpenVAS 核心的部份，包括掃描目標的功能性的使用，掃描將始終來自正在運行 OpenVAS 伺服器的主機，因此主機必須能夠到達所要掃描目標。

  伺服器有三個模組：

  1. OpenVAS-Libraries: OpenVAS-Server 的功能函式庫。
  2. OpenVAS-LibNASL: 作為 OpenVAS-Server 與“Nessus Attack Scripting Language” (NASL)中介函式庫。
  3. OpenVAS-Plugins: 包含許多弱點測試小程式，注意此模組的更新週期是不保證提供最新的弱點測試小程式的。

- OpenVAS-Client: 控制 OpenVAS 伺服器, 處理掃描結果與顯示結果。是可以連到伺服器上任一主機，它也可以控制多台主機。
- openvas 處理方式：

  Client 向 Server 提出掃瞄請求，其設定(Config)工作目標主機(Scope)掃瞄報表(Report)均存在 Client 端，Server 接到請求，經過認證無誤後根據弱點測試開始掃瞄，其測試是 plugin 相關服務來測試。



掃瞄前要先思考：

1.我要偵測什麼弱點？我的目標是什麼？

2.是永久性監測或是單一個案，弱點偵測程式要如何持續？

3.要採用哪一種認証模式？

4.伺服器擺放位置？在網段內/外？

5.目標主機的位置？在 internet 公開主機或是 intrnet 主機?

2.軟體安裝

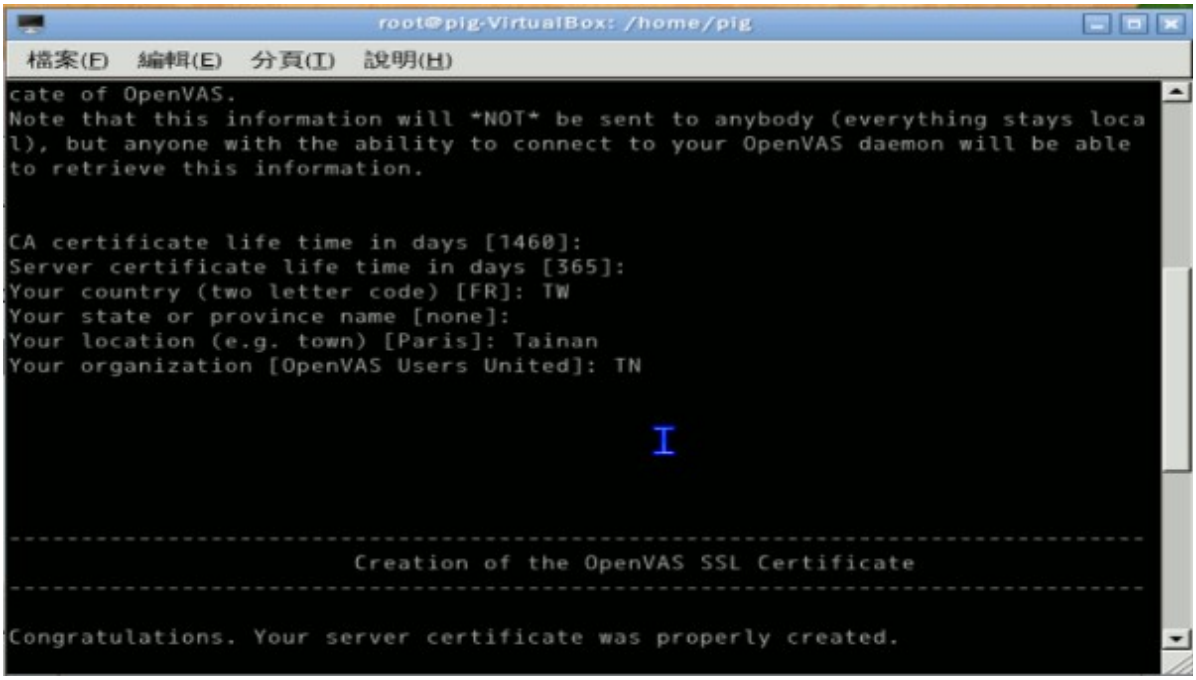
安裝伺服器：

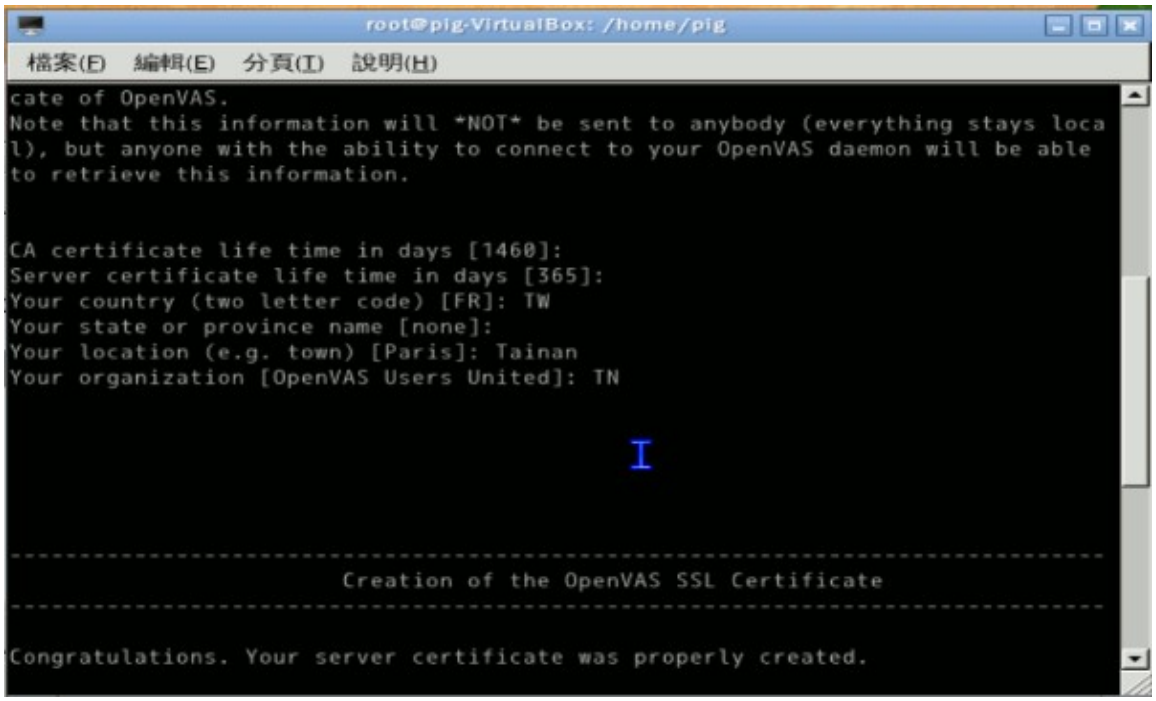
apt-get install openvas-server

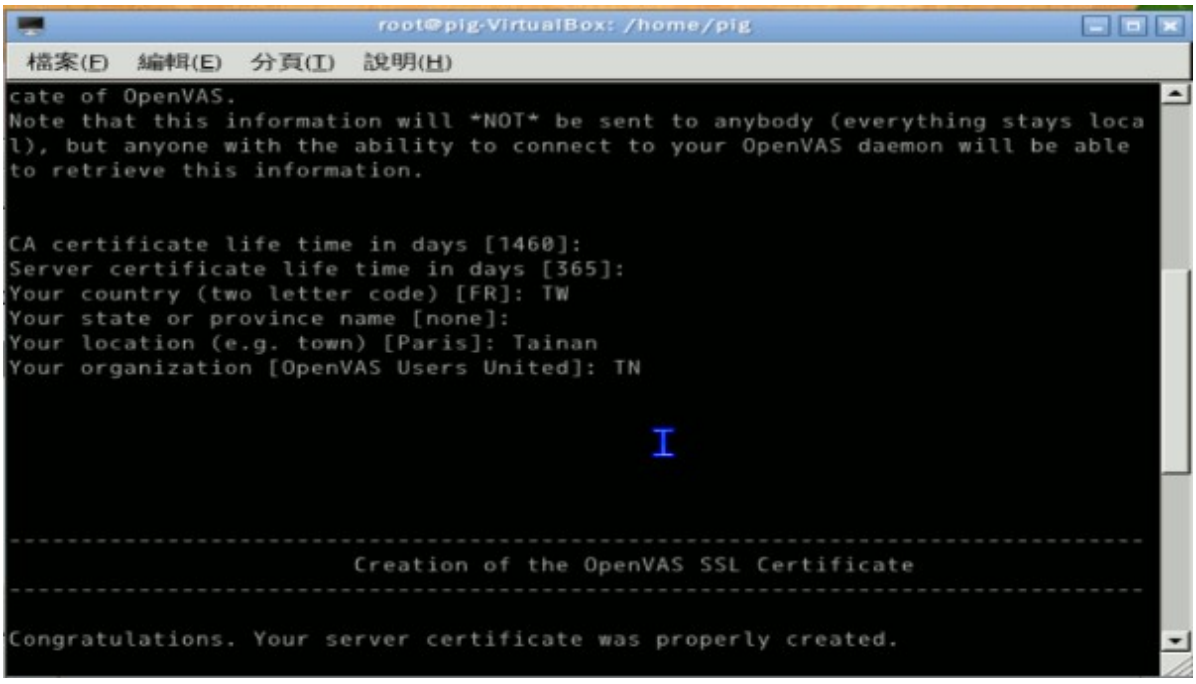
安裝客戶端：

apt-get install openvas-client

由於 client 與 server 溝通是透過 SSL 加密保護，需要安裝憑證
openvas-mkcert
出現如下畫面



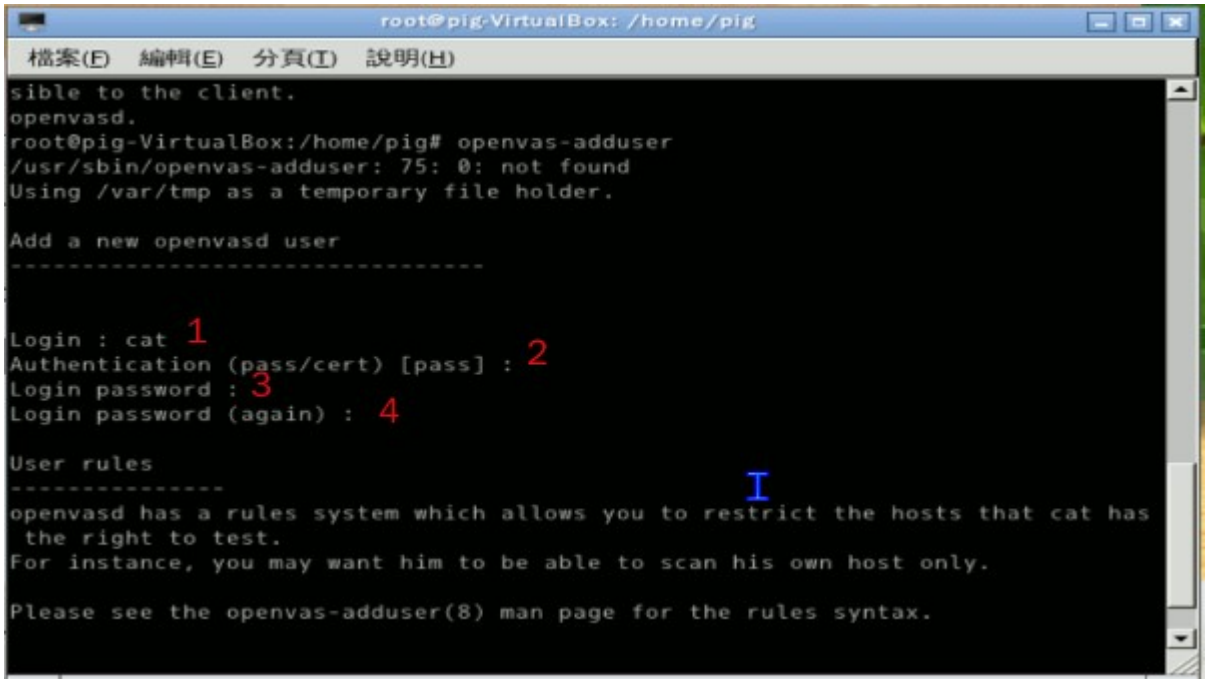




完成後按下 enter 離開

新增一位使用者

openvas-adduser



1：使用者名稱

2：驗證方式：數位憑證或是用密碼

3：指定密碼

4：確認密碼

指定登錄位置：(以 CTRL+D)做結束

規則是指限制使用者言(限制有三類：伺服器限制、使用者限制、目標限制)：

格式

accept|deny ip/mask

default accept|deny

例如：

accept 192.168.1.0/24

accept 192.168.3.0/24

default deny

上面的意義：至接受來自 192.168.1.0、192.168.3.0 等 C-Class 網段來源，其餘的拒絕。

deny 192.168.1.0/24

default accept

上面的意義：拒絕來自 192.168.1.0 之 C-Class 網段來源，其餘的則接受。

如果限制只能掃描他的系統(換言之：不可以掃別人)則

accept client_ip

default deny

啟動 OPENVAS

方法一：

#kill -l PID(指 openvasd 所執行的行程編號)

方法二：

step1:sudo su

step2:以 ROOT 身份進入後

/etc/init.d/openvas-server start|stop|restart

開始掃描：

step1:建立工作區(Task)

Task → New

New:加入新工作，內定名稱是『unnamed』

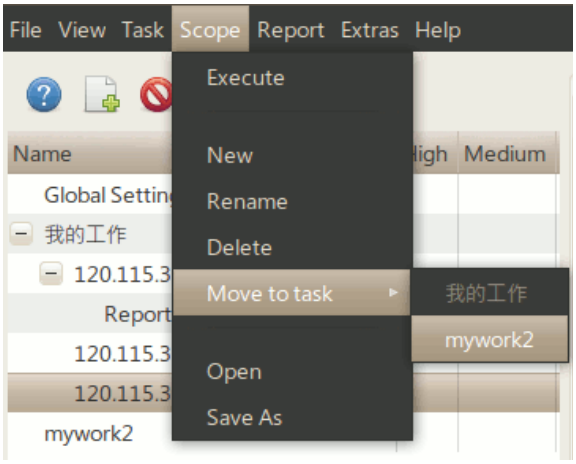
Rename：更改工作名稱，點選該名稱或是選取該項目

Remove：移走該工作之所有的 scope(範圍)，移走時會有確認方塊出現

step2:建立範圍(Scope)：

Scope 視為是一種子工作(sub-task)，定義一種目標範圍的掃瞄，其標題可以用來寫明掃瞄工作內容。註解也可以用來註明。不同的 scope 可以有不同的設定。當掃瞄完成後則會有一連串的報告。

- 執行：(Execute)當若連接到 open vas 伺服器時，Scope 設定存入並執行掃瞄
- 新增：(New)新增一個 unnamed ，新增內定設定可以經由改變 Global Setting 來決定
- 更名：(Rename):該改名稱
- 移除：(Remove):移除指定 scope 相關報告與設定檔
- 移至工作區(Move to task):將 scope 之報告從一工作區移到另一工作區
- 開啟(Open):可以開啟一個 scope 檔案至某一工作區，期間參數將會被覆蓋。可以將某一 scope 存入，再用此方式開啟
- 儲存(Save):儲存 scope 設定檔



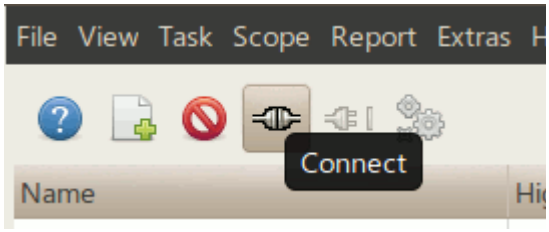
step3:連接與驗證：

驗證：Authentication

當 Open-vas client 連接到 OpenVas Server 時為了開啟可用的 plugin 來執行安全掃瞄，OpenVas-Client 2.0.0 將出先對話方塊表示 NVT 在伺服器端被發現。

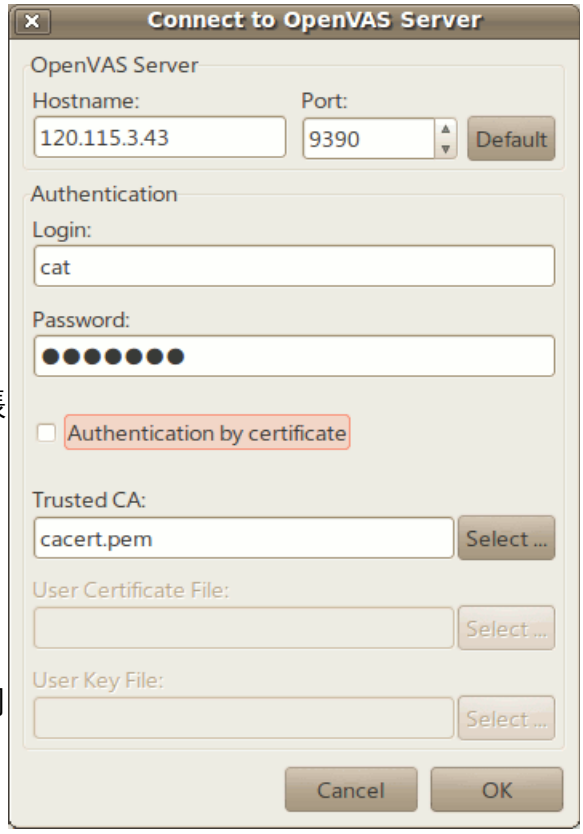
OpenVas-Client 可以管理多個不同伺服器，前述每一個 scope 可以擁有自己的連接方式。

連接方式：前述選單中的 Execute 或是用下圖



一開始連接將出現如下方塊：

連接伺服主機：

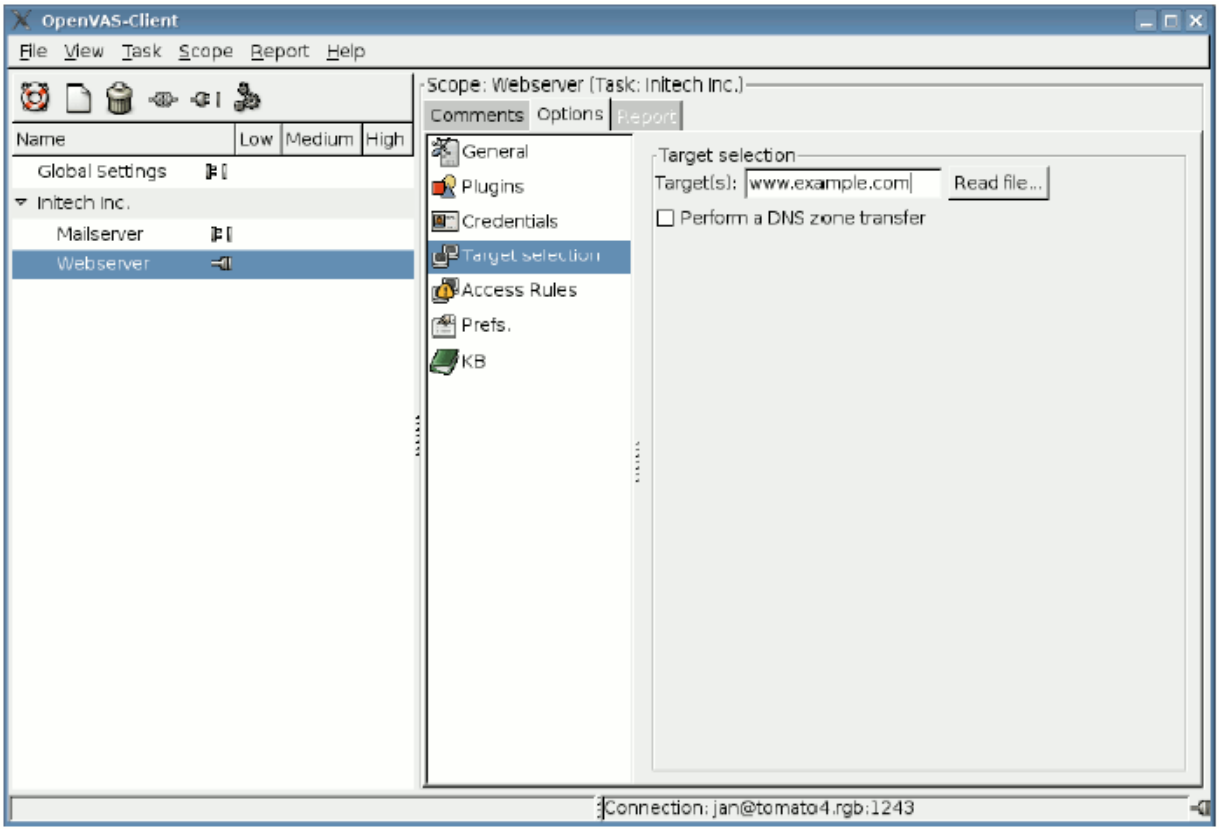


- Hostname:運作中的 OpenVas 伺服器之主機名稱或是 IP
- Port:OpenVas 伺服器連接 port 號內定值為 9390，可以按下 default 重新設定內定值
- Login:登錄 OpenVas 伺服器使用者之帳號，換言之在 OpenVas 伺服器必須有一個帳號。
- Password:同上為使用者密碼
- Authentication by Certificate:

勾選必須有一對 key/certificate，而 OpenVas 伺服器管理者必須給兩個檔案 User Certificate

File 與 User Key File，管理者可以用或者不用密碼產生一個 key，如果 User Key File 需要密碼，所以在連接 OpenVas 伺服器時則需要輸入密碼。

Step4:設定目標主機：



目標主機選擇：

Target(s)：OpenVAS 伺服器所要掃描主機，可依單一或是多台主機。

1. 定義方式如：“host1,host2”
2. 一種特殊語法如：“file:/some/where/targetlist.txt”，則由檔案列表中讀取。
3. Read from file：從檔案中讀取，主機與主機之間以逗號分隔，或是每一行表示一主機
4. Perform a DNS Zone transfer：OpenVAS 伺服器執行 AXFR 要求(區域 ZONE 轉換)至目標 DNS 取得 DNS 目標區域所有主機，然後做每一台主機的掃描。

192.168.1.0/24 :表示掃整個網段

- 使用 scan Assistant:

使用 scan 精靈協助建立工作與範圍，共有四個步驟

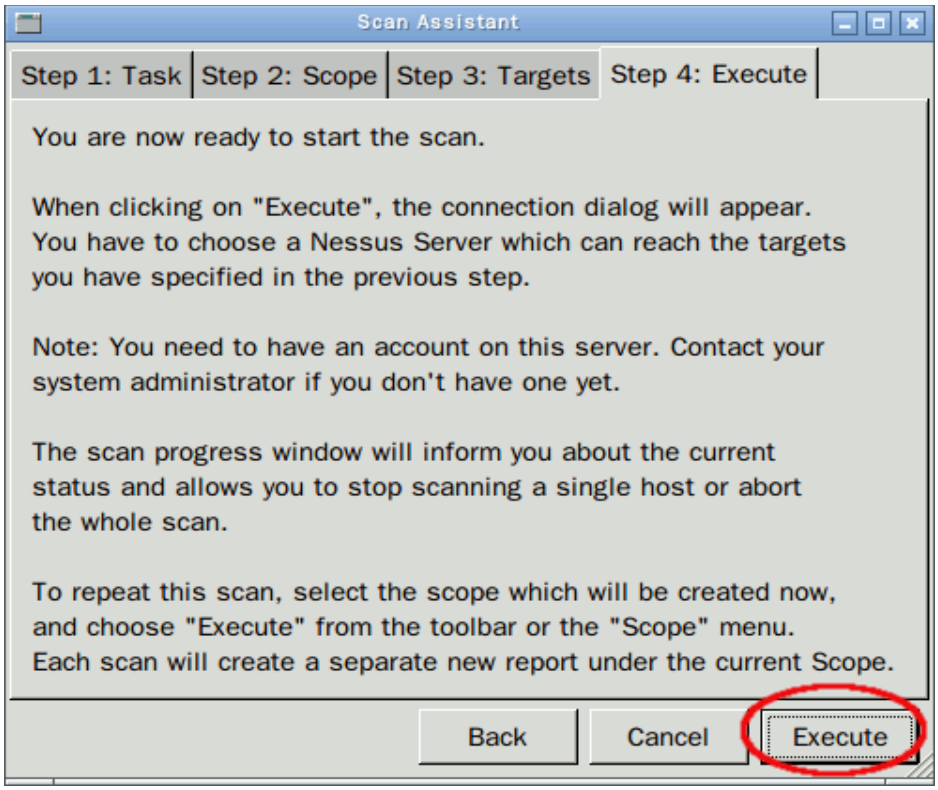
file→scan assistent

步驟一：建立 task

步驟二：建立 scope

步驟三：建立目標主機

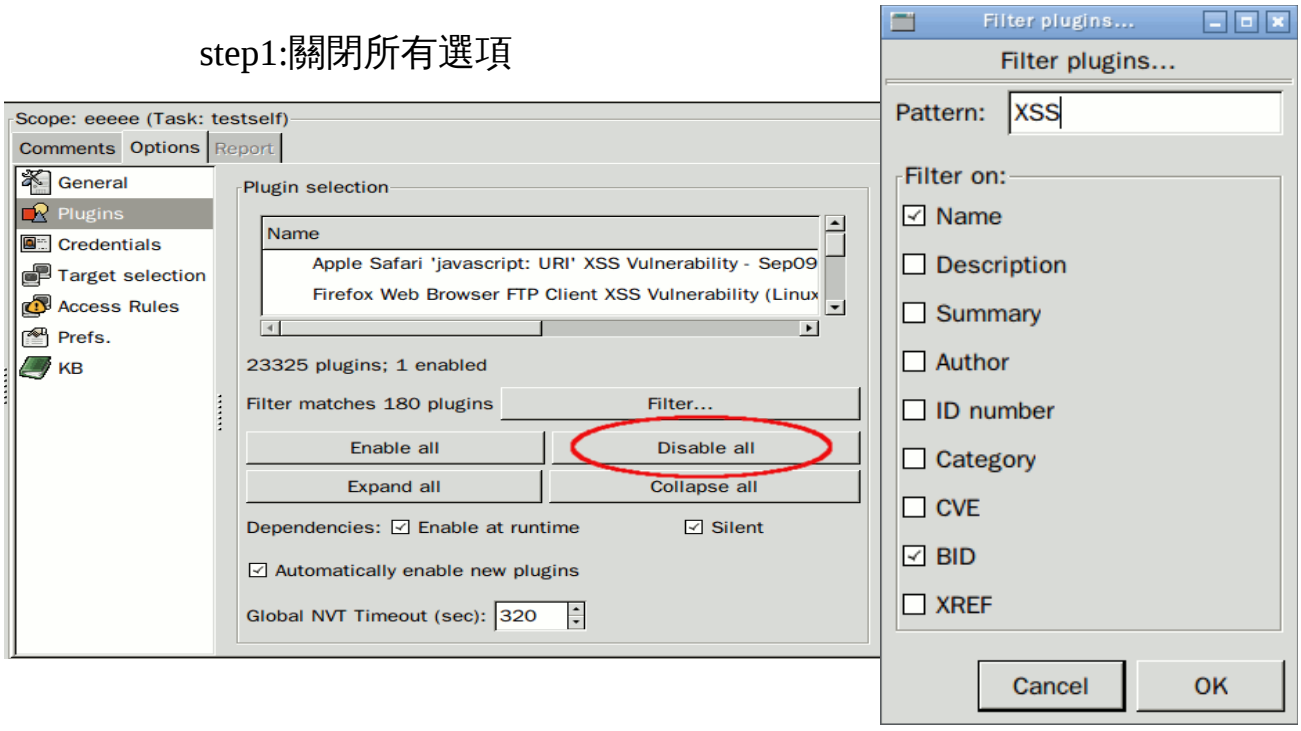
步驟四：開始掃描



四、OPEN-VAS 掃描應用

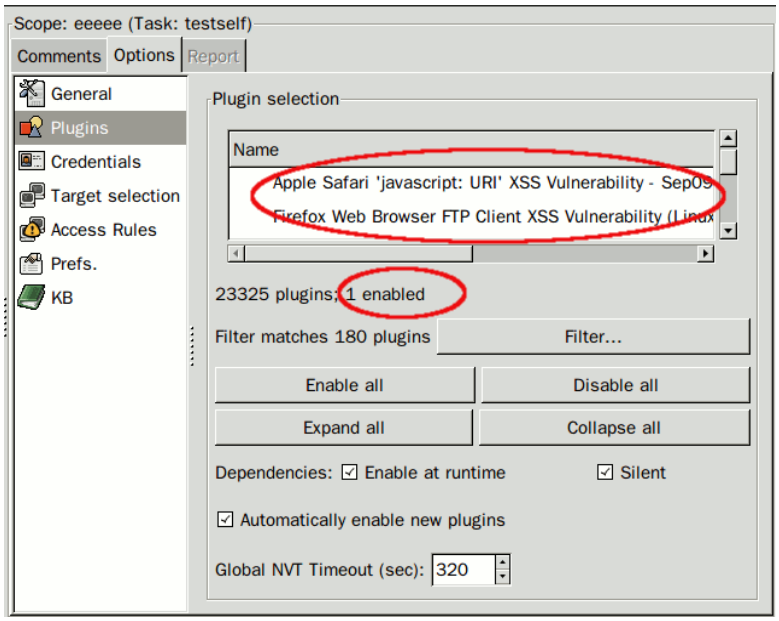
- 如何指定掃描，例如做 XSS 或是 SQL Injection

step1:關閉所有選項

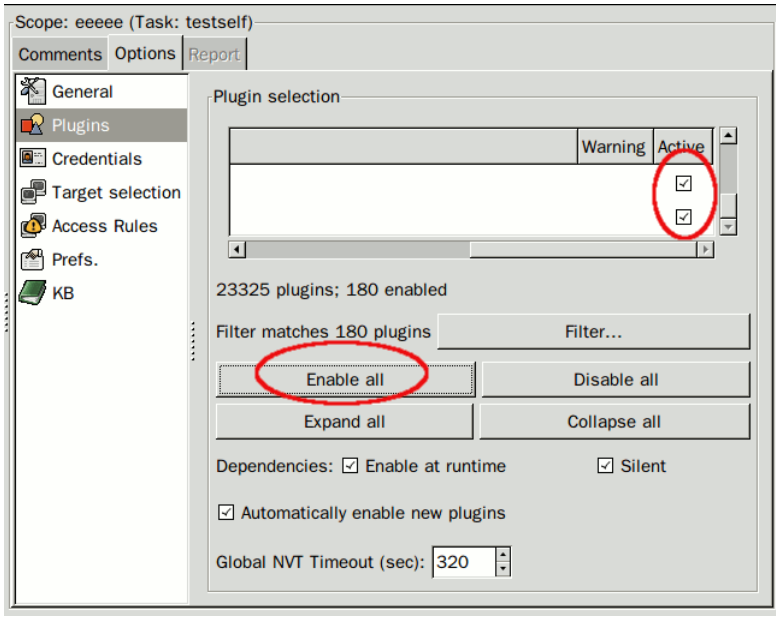


step2:選擇 XSS plugin

step3:查出有 XSS 的 plugin



step4：啟用(勾選 Enable all)

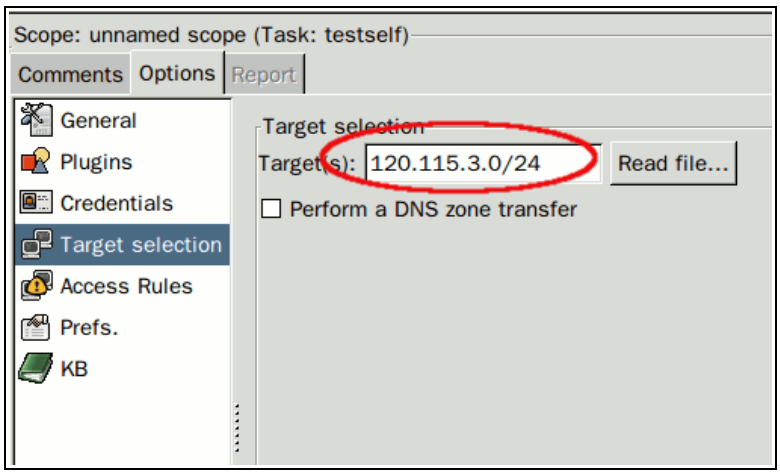


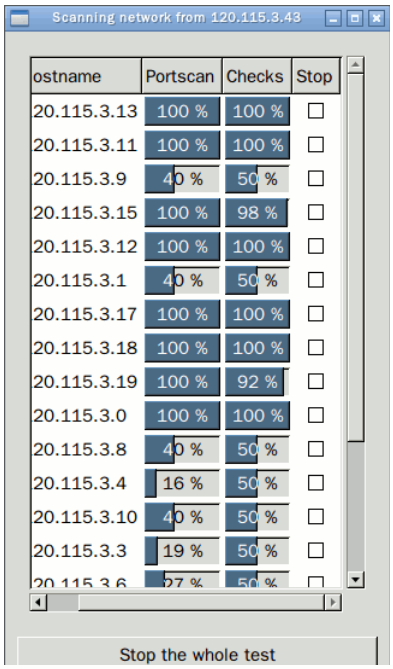
step5：掃描

- 全網段掃描(注意：內定掃描最大主機數為 255)

step1:設定(如下圖)

step2:執行掃描





- step3:報表輸出

Summary

This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

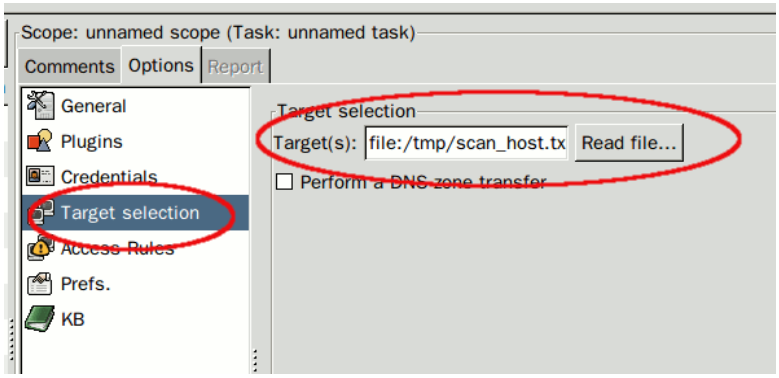
Scan started at: Thu Jan 12 18:12:58 2012
Scan finished at: Thu Jan 12 18:18:35 2012

Host	Possible Issues	Holes	Warnings	Notes	False Positives
120.115.3.0	Security note(s) found	0	0	1	0
120.115.3.1	Security note(s) found	0	0	1	0
120.115.3.2	Security hole(s) found	4	6	12	0
120.115.3.3	Security note(s) found	0	0	1	0
120.115.3.4	Security note(s) found	0	0	1	0
120.115.3.5	Security note(s) found	0	0	8	0
120.115.3.6	Security note(s) found	0	0	1	0
120.115.3.7	Security note(s) found	0	0	1	0
120.115.3.8	Security note(s) found	0	0	1	0
120.115.3.9	Security note(s) found	0	0	1	0

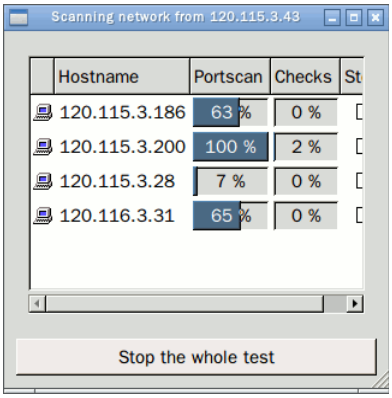
- 指定多台主機同時掃描

  step1:建立掃描主機檔，如下：
  120.115.3.200
  120.115.3.186
  120.116.3.31
  120.115.3.28

  step2:target section 選擇 Read Files

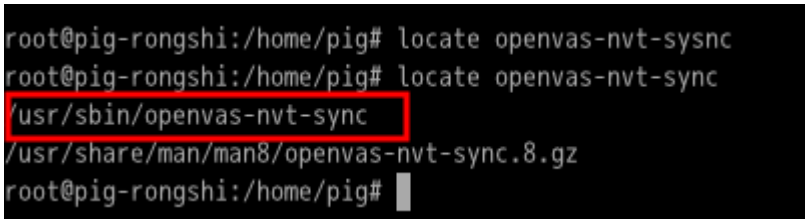


step3:開始掃描



- plugin 同步(偵測程式同步)

  執行 openvas-nvt-sync



- 增刪使用者

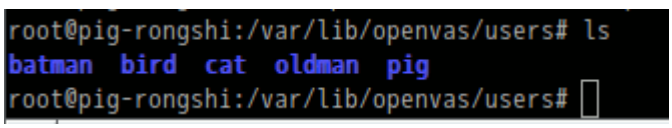
  使用者檔案位置：(可以查詢/etc/openvas/openvasd.users)

  增加使用者

  openvas-adduser

  新使用者可以在

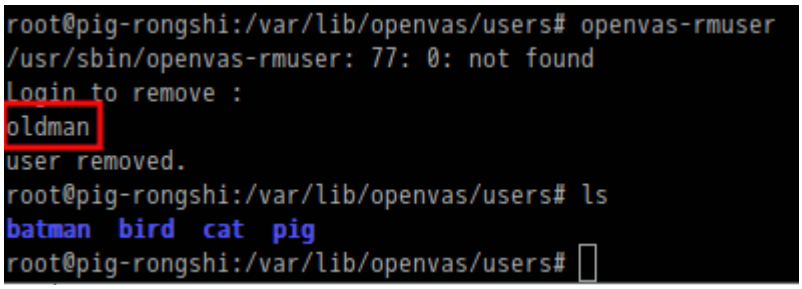
  /var/lib/openvas/users 目錄下見到



刪除使用者：

openvas-rmuser

則會詢問要刪除哪一使用者？



- 如何作規則訂定

  定義規則有三種

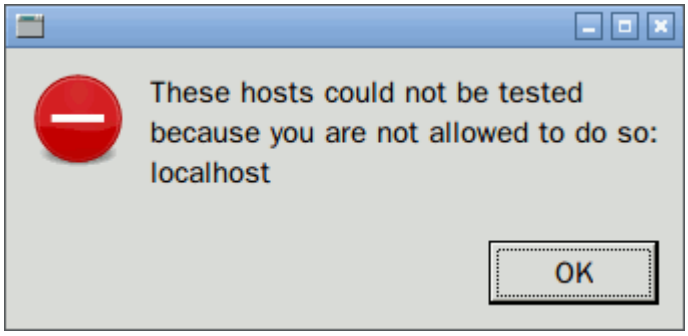
  規則設定：

- 伺服器規則設定：(適用整個伺服器上，會影響到已連接上來的使用者)。存在/etc/openvas/openvasd.rules

  格式：

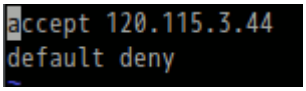
  accept|deny ip/mask 或者 default accept|deny

  基本上仍然會進入，但在做掃描主機則會跳出如下



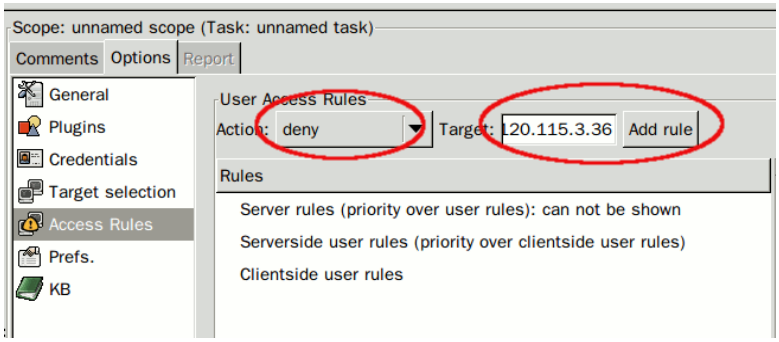
- 伺服器端使用者規則：指定給某一使用者，也只影響該使用者，此在加入使用中做設定，其設定檔存在/var/lib/openvas/users/yyy/auth

  修改其 rules 檔案

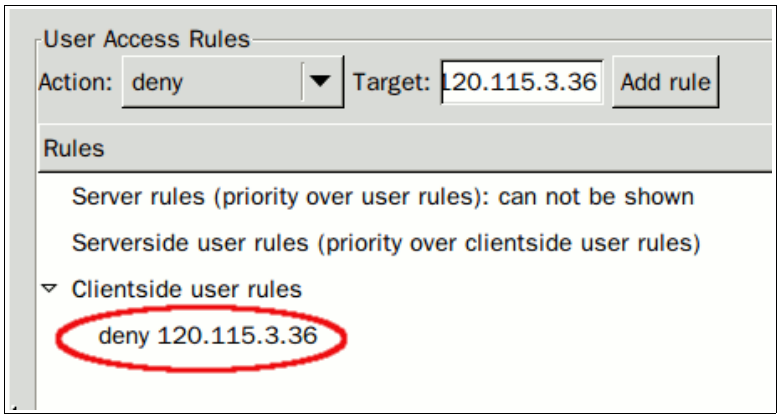


- 客戶端個人規則設定：(不管從哪裡來)

例如拒絕使用者 yyy 掃描 120.115.3.36，



按下『Add rule』後增加規則



舉例來說：

如果使用者 birdman 要求只能從 120.115.3.43 且只能掃 120.115.3.31

所以設定檔：

主機伺服器：accept

伺服器端使用者：(在 birdman 設定 rules)

accept 120.115.3.43

default deny

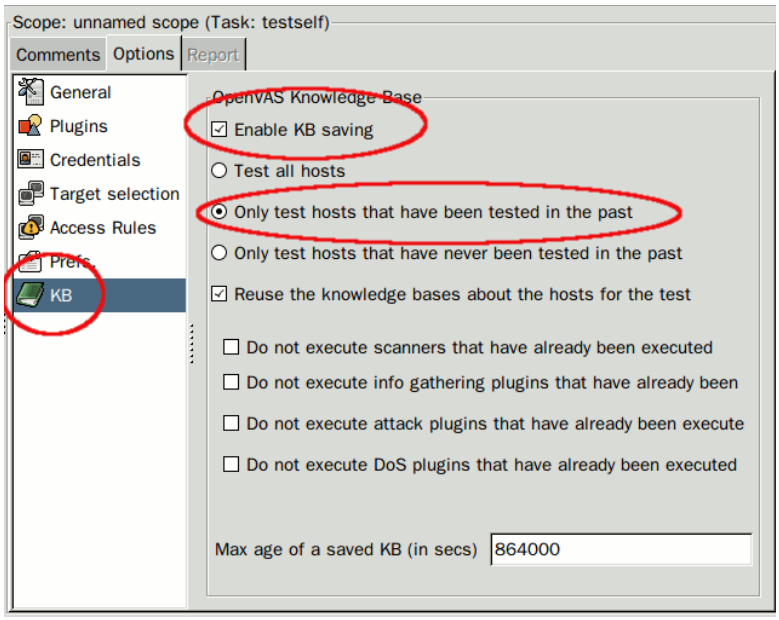
客戶端個人規則設定:

accept target:120.115.3.31

default deny

- 對已經掃描過的主機進行複掃

step1:開啟 KB

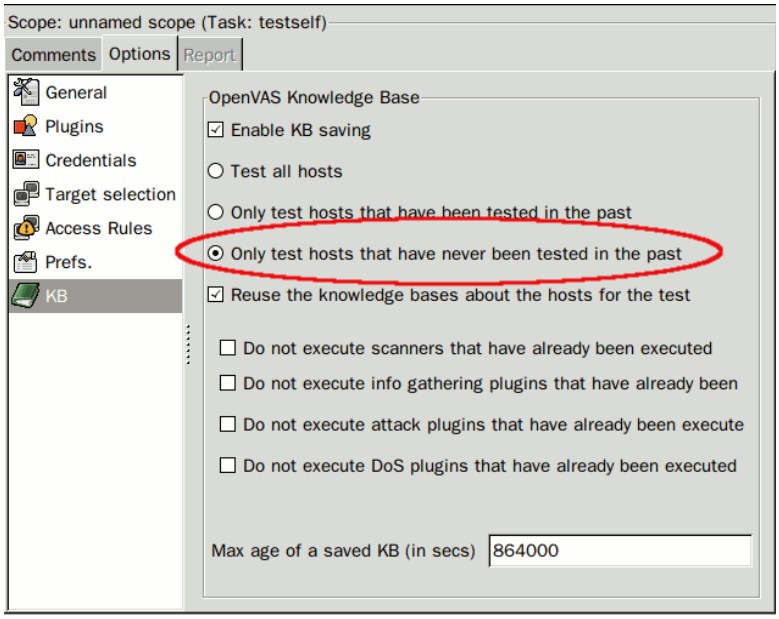


step2:設定條件

step3:進行掃描

同理對新主機也可採用此方式不過選第 3 項

step1：



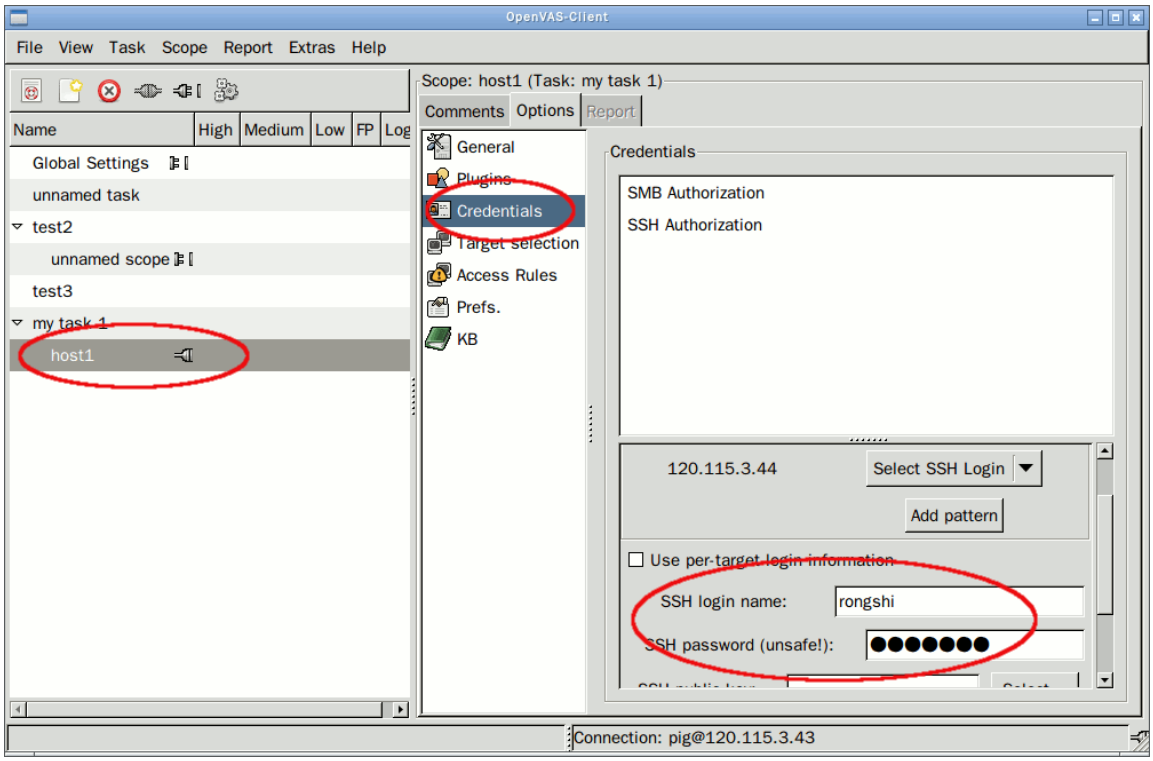
step2：設定主機

step3：開啟掃描

- 掃描 SSH 或是 SMB(掃描時有時需要以 SSH 或 SMB 之密碼進入主

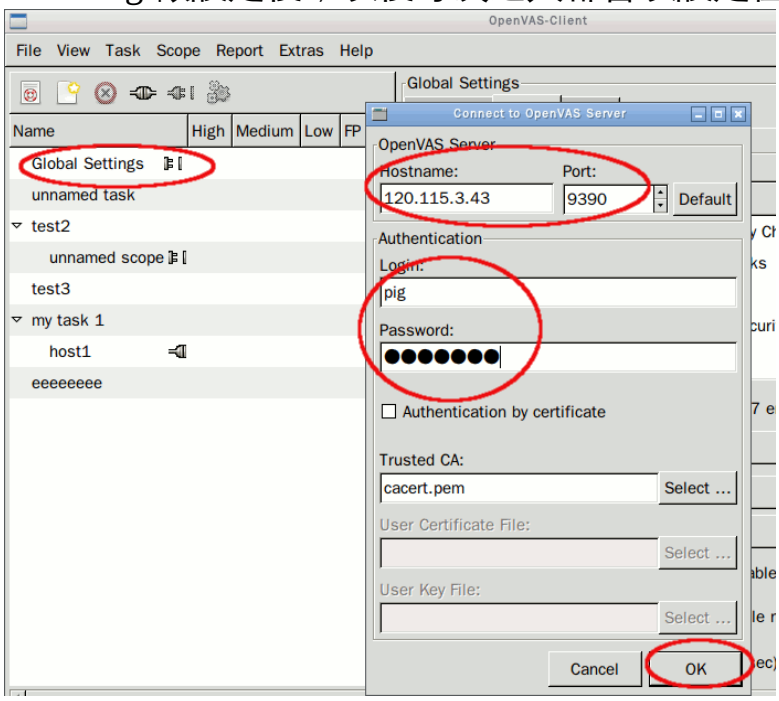
機做掃描，其準確度較高，但如何設定？

基本上需要連接 OpenVAS 伺服器，才能做設定，如果有 SSH 或 SMB 之密碼，填入視窗中。



- 如何每次開啟連接時都進入設定值

  在 global Setting:做設定後，以後每次進入都會以設定值出現

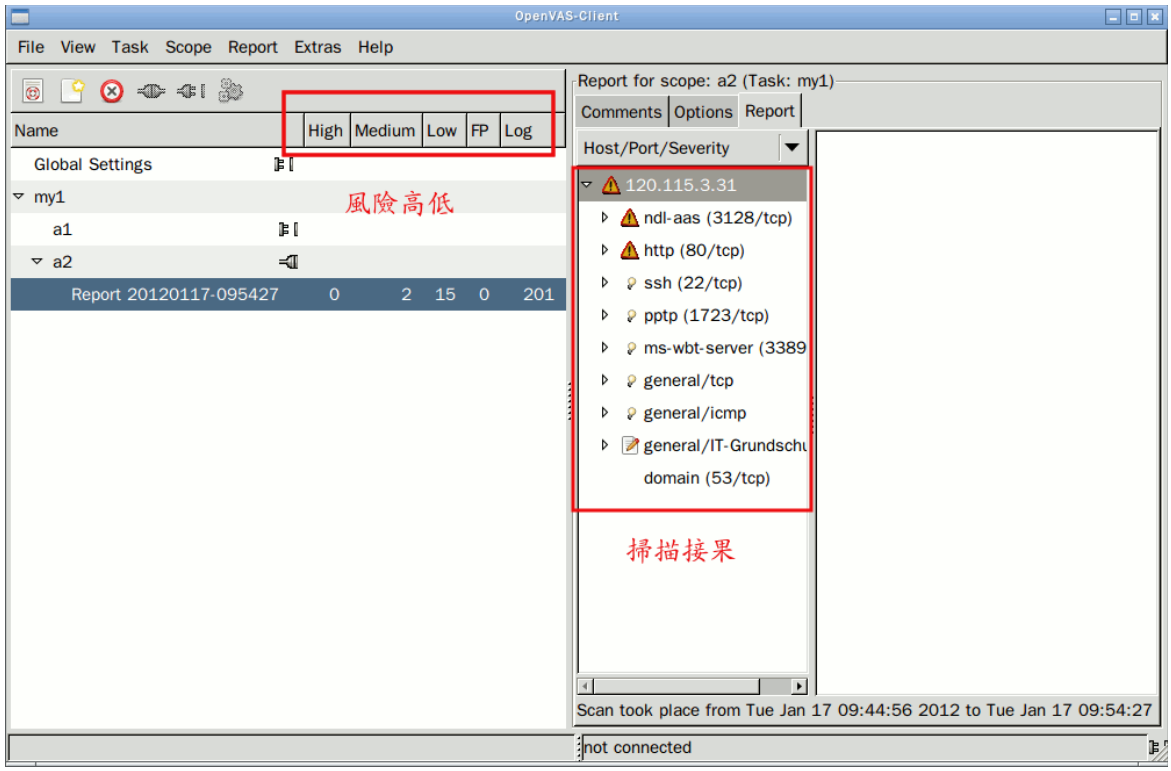


五、報告輸出與判讀

1.報表輸出

當掃描完成後，可以將結果做輸出。

通常掃描完成則出現如下：



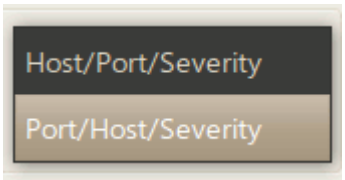
報表存在三個部份，左邊是樹狀串列可以瀏覽 hosts/ports/severity，右邊是報告區

- 報告的格式：

  有各種不同的格式，有三種類型：交換格式，可編輯文件與唯讀文件。最新的格式 PDF 格式。也可利用插入連結方式以瀏覽器來瀏覽。

利用 Report->Export 做輸出報表。

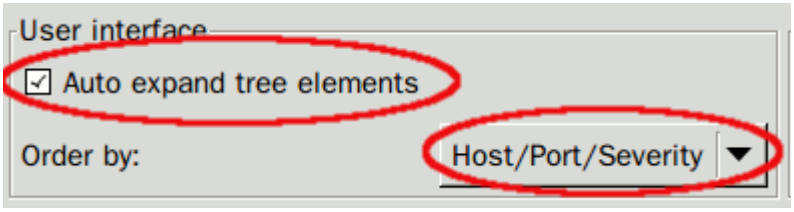
- 調整顯示格式：



設定掃描結果的編排方式，內定是 host 先，其次是 port，最後是 severity。

有兩種選擇，也可以在報表中做選擇。

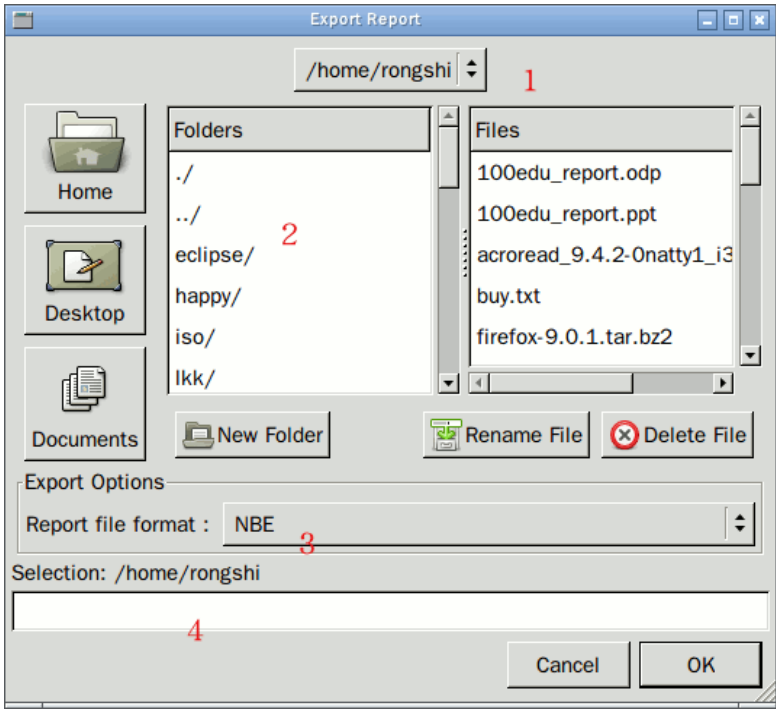
也在 file → Preferencess 中做調整



- 格式輸出

報表輸出：

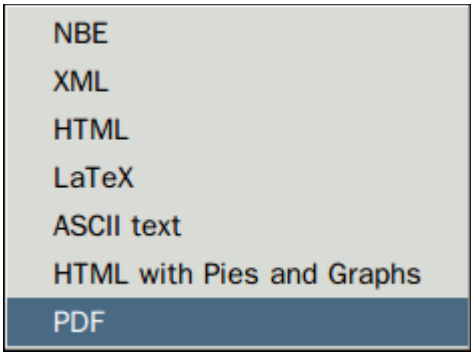
step1:點選掃描結果
step2:Report → Export
如下圖：



1.目錄位置

2.目前目錄下有哪些資料夾，右邊是檔案

3.輸出格式設定

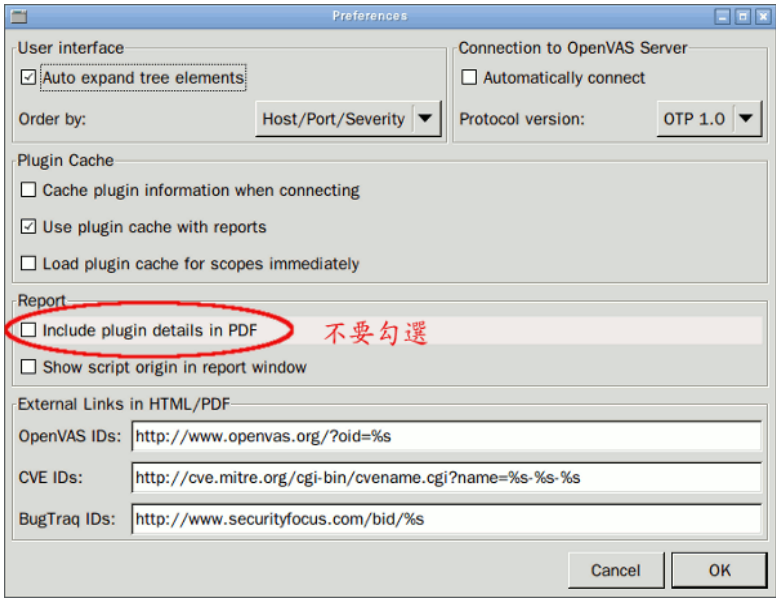


4.輸入輸出檔案位置

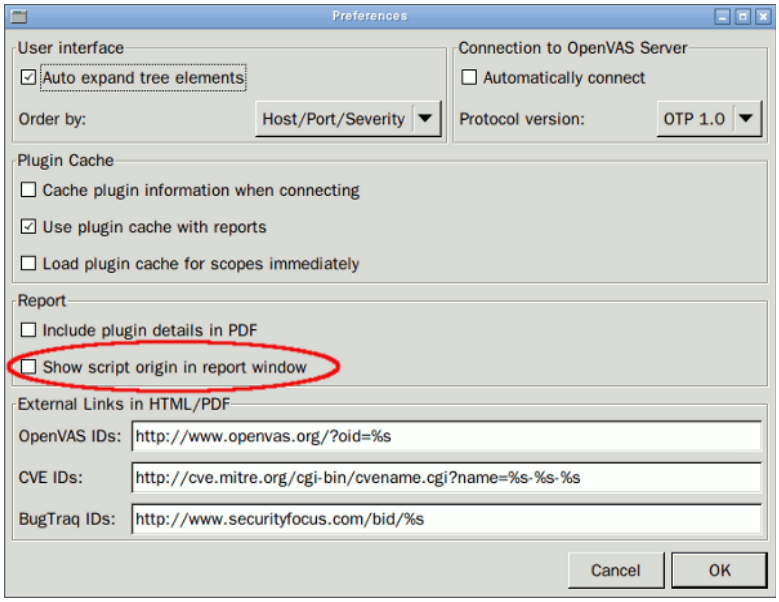
step3:選擇要輸出目錄→輸出格式→檔案名稱

- 精簡報表：

  由於報表輸出會附帶相關資訊，如果只要列出掃描結果，可以使報表精簡許多。



- 察看偵測程式來源：(下圖勾選)



- Plug-in Cache(Plug-in 快取)

  Cache plugin information when connecting ：

  OpenVAS-Client 將分別對個別的 Scope 建立快取，報存所有 plugin 的資訊，有下列三種功效：

  1.相同的 scope 將會更快速連接，因為 MD5 檢查是用來對新的 plugin 與改變。

只有在新的改變則才會下載在快取，當然連接到不同的 OpenVas 伺服器也會強迫下新的下載。

2.當客戶端與伺服端尚未連接時，這些 plugin 的資訊是可用的，可以檢視那一項 plugin 是被選取的與目前 plugin 的參數是什麼。注意所選擇也可能發生改變在連接後展開掃描時，因為新的 plugin 可能變成可用而其他 plugin 可能消失不見等種種變化。載入快取可能會花一些時間，如果不想這樣則關閉『Load plugin cache for scopes immediately』選項

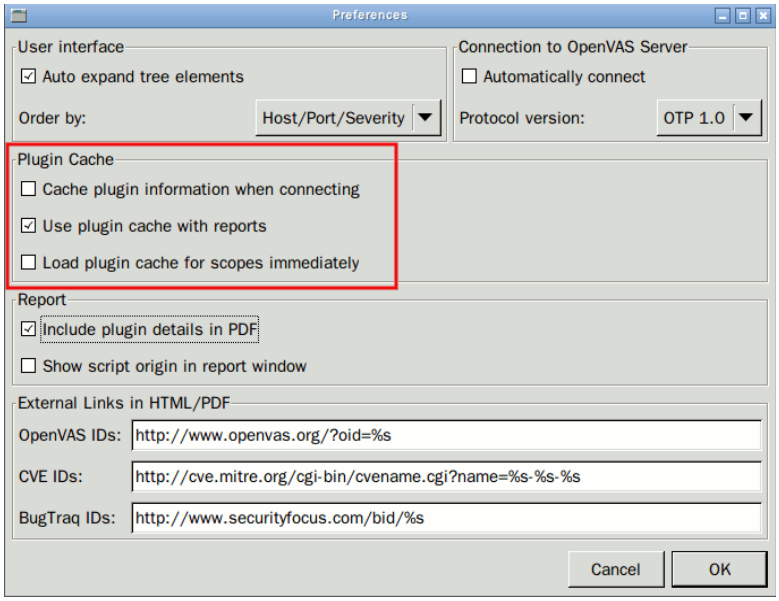
3.快取的缺點是對每一個 Scope 會耗去幾 megabytes 記憶體，如果空間不足則關閉此功能，如果移走快取則搜尋 OpenVas 路徑下『nessus_plugin_cache』(在家目錄下".openvas")，刪除之。

- Use plugin cache with reports ：

  OpenVAS-Client 加入所有 Plugin Information 到新建立的掃描報告，在 OpenVAS-Client GUI 可以重新檢視報告中 plugin 的選擇與 plugin 參數。因此此快取是增加透明度而非增加效能。缺點是產生報表時耗費幾 MB 記憶體，如果移走快取則搜尋 OpenVas 路徑下『nessus_plugin_cache』(在家目錄下".openvas")，刪除之。

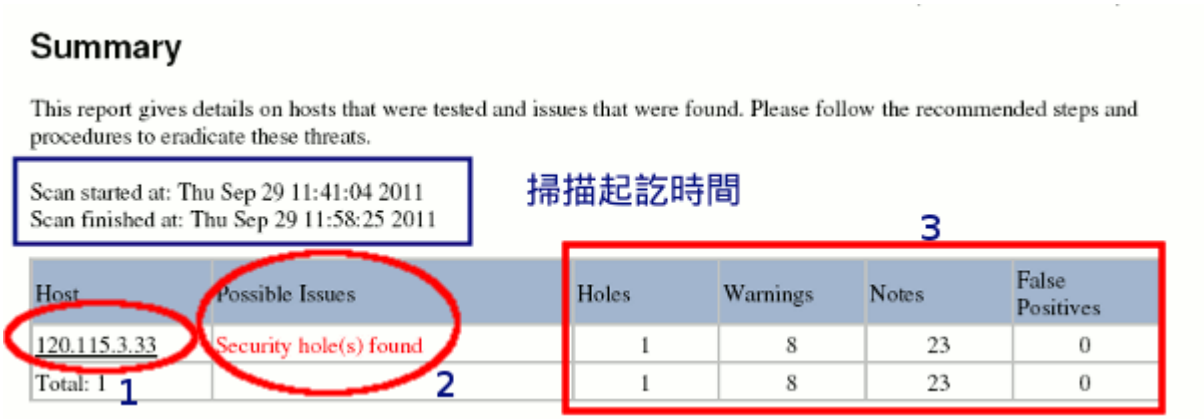
- Load plugin cache for scopes immediately ：

  取消此功能將產生 OpenVAS-Client 活動時無法自動載入 Scope 快取，無法看到選取的 plugin 與 plugin 參數，如果取消此功能則前述『Cache plugin information when connecting』是有利的，在點取 Scope 時避免載入更大的記憶體。



2.報表判讀

- 摘要



Summary

This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

Scan started at: Thu Sep 29 11:41:04 2011
Scan finished at: Thu Sep 29 11:58:25 2011

掃描起訖時間

3

Host	Possible Issues	Holes	Warnings	Notes	False Positives
120.115.3.33	Security hole(s) found	1	8	23	0
Total: 1		1	8	23	0

1 2

1:目標主機

2:出現弱點

3:種類：Holes(弱點)、Warnings(警告)、Notes(注意)

- 每台主機報告

Reports per Host

120.115.3.33

Scan of this host started at: Thu Sep 29 11:41:04 2011
Scan of this host finished at: Thu Sep 29 11:58:25 2011

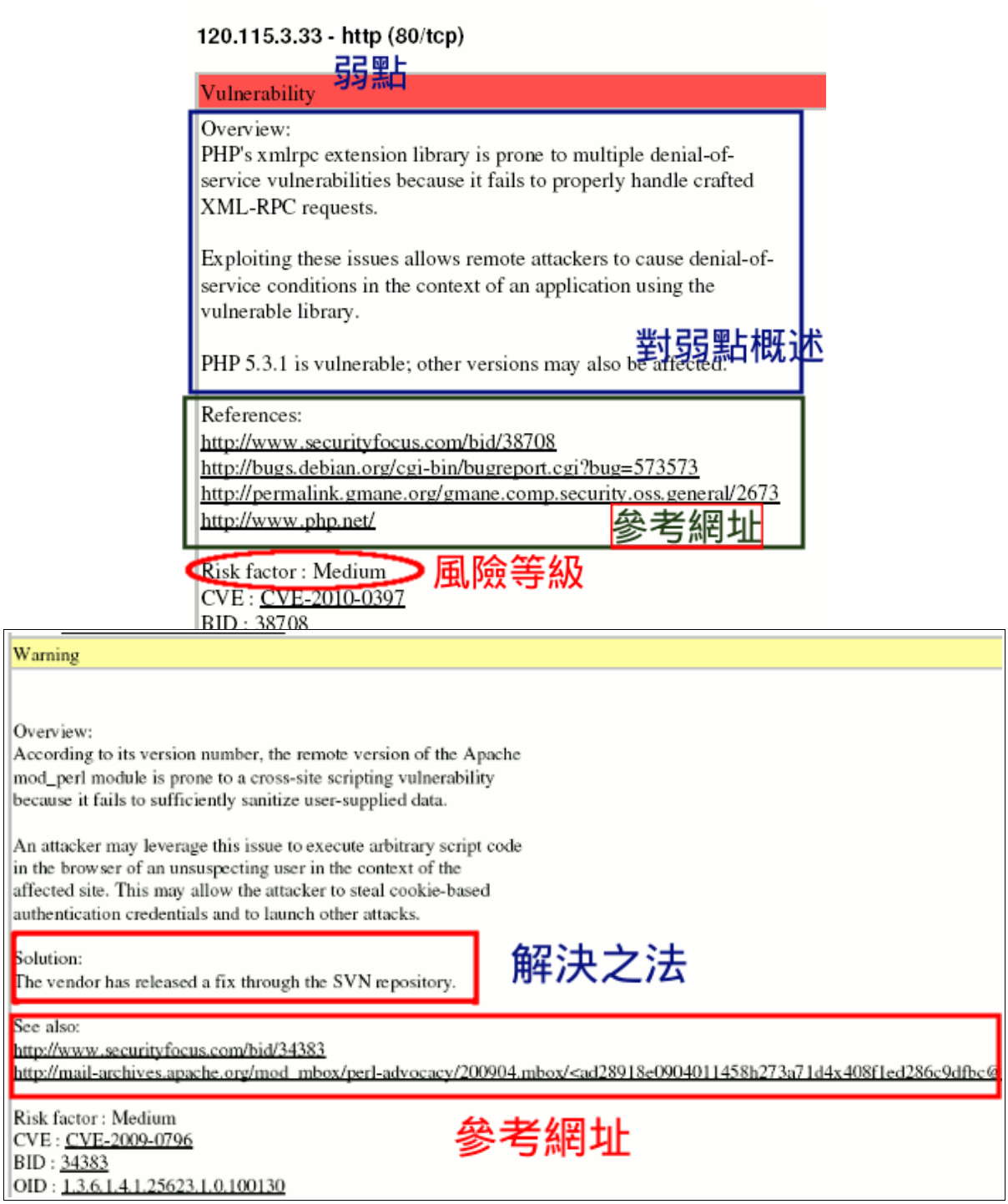
Service (Port)	Issue regarding port
http (80/tcp)	Security hole(s) found
epmap (135/tcp)	Security warning(s) found
netbios-ssn (139/tcp)	Security note(s) found
https (443/tcp)	No Information
microsoft-ds (445/tcp)	Security note(s) found
mysql (3306/tcp)	Security note(s) found
ms-wbt-server (3389/tcp)	Security note(s) found
general/tcp	Security warning(s) found
ssh (22/tcp)	No Information
netbios-ns (137/udp)	Security warning(s) found
unknown (49152/tcp)	Security note(s) found
unknown (49153/tcp)	Security note(s) found
unknown (49154/tcp)	Security note(s) found
unknown (49156/tcp)	Security note(s) found
unknown (49168/tcp)	Security note(s) found
general/SMBClient	Security note(s) found
general/CPE-T	No Information

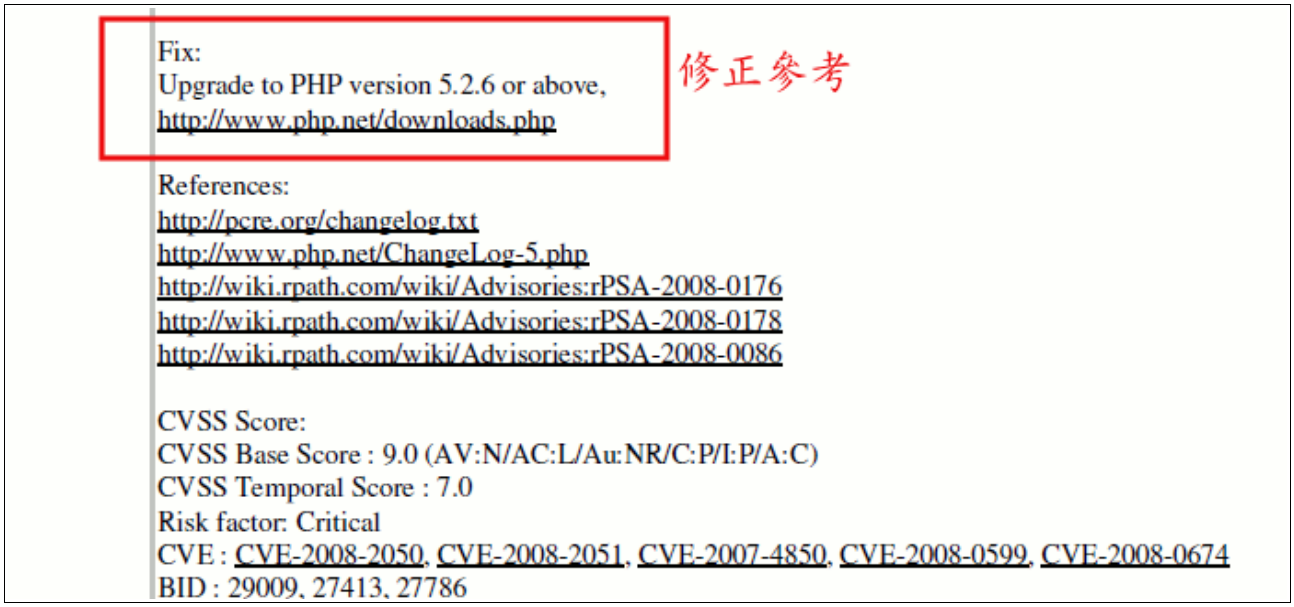
[return to summary]

開啟Port號

出現弱點

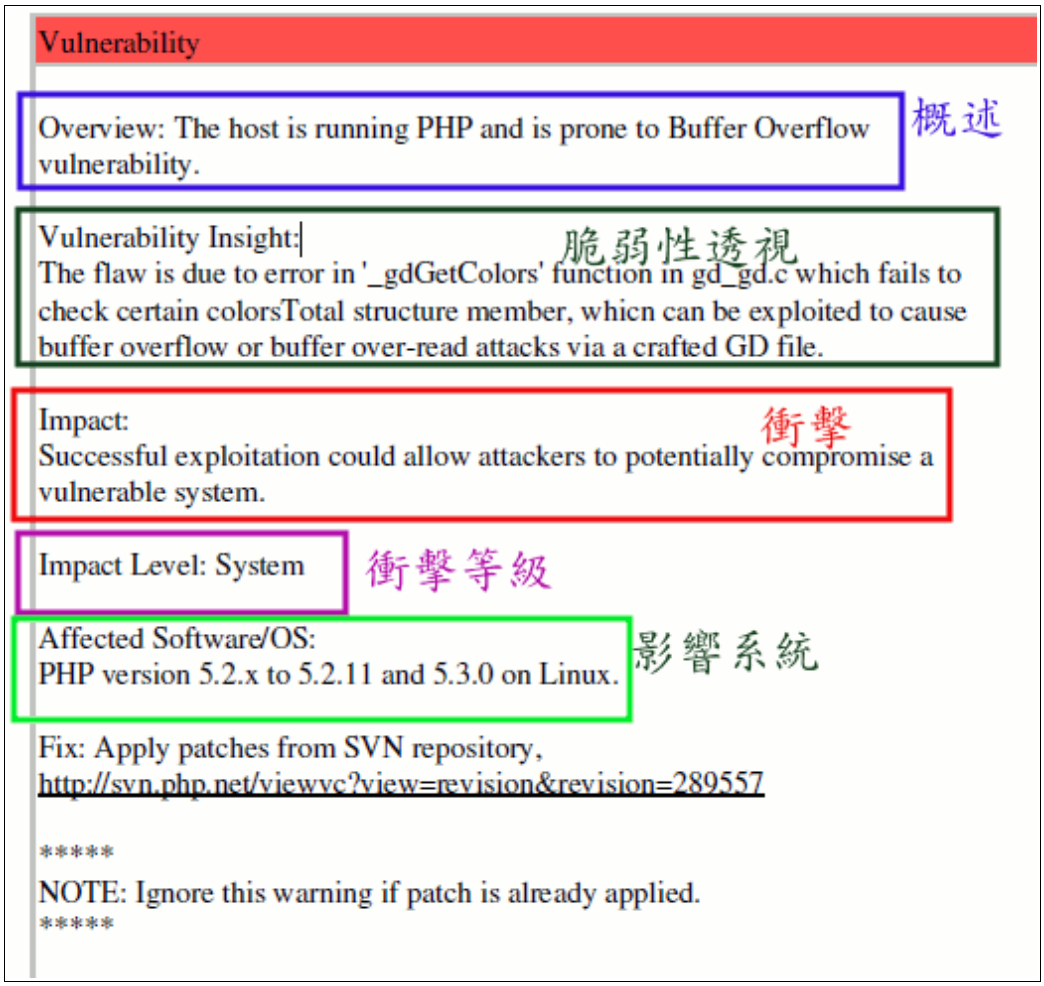
- 弱點修補

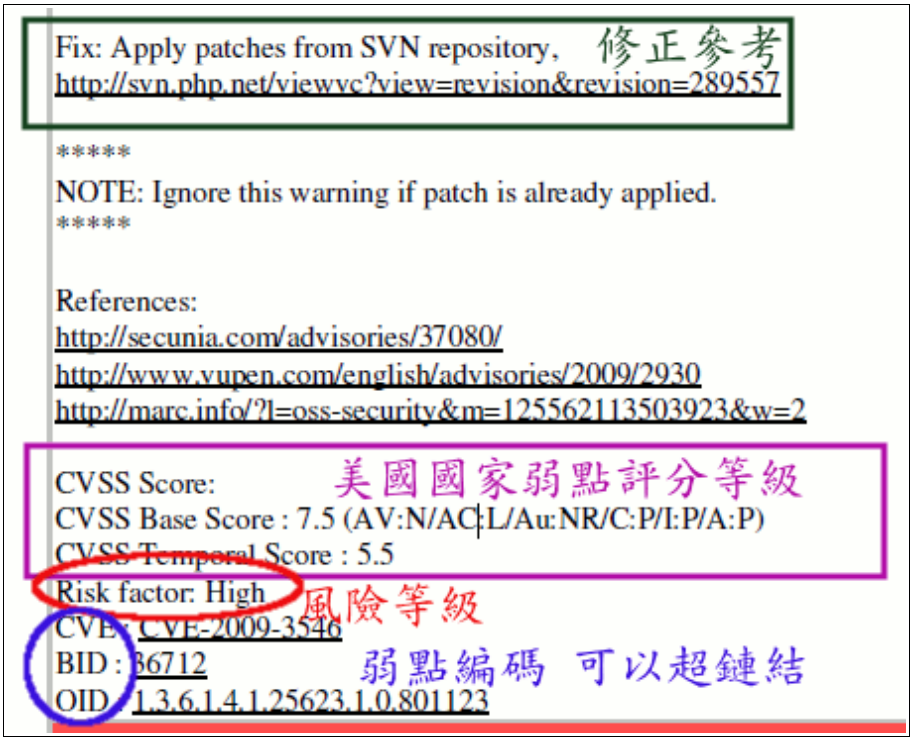

120.115.3.33 - http (80/tcp)
弱點
Vulnerability
Overview:
PHP's xmlrpc extension library is prone to multiple denial-of-service vulnerabilities because it fails to properly handle crafted XML-RPC requests.
Exploiting these issues allows remote attackers to cause denial-of-service conditions in the context of an application using the vulnerable library.
PHP 5.3.1 is vulnerable; other versions may also be affected.
對弱點概述
References:
http://www.securityfocus.com/bid/38708
http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=573573
http://permalink.gmane.org/gmane.comp.security.oss.general/2673
http://www.php.net/
參考網址
Risk factor : Medium
風險等級
CVE : CVE-2010-0397
BID : 38708
Warning
Overview:
According to its version number, the remote version of the Apache mod_perl module is prone to a cross-site scripting vulnerability because it fails to sufficiently sanitize user-supplied data.
An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks.
Solution:
The vendor has released a fix through the SVN repository.
解決之法
See also:
http://www.securityfocus.com/bid/34383
http://mail-archives.apache.org/mod_mbox/perl-advocacy/200904.mbox/
參考網址
Risk factor : Medium
CVE : CVE-2009-0796
BID : 34383
OID : 1.3.6.1.4.1.25623.1.0.100130



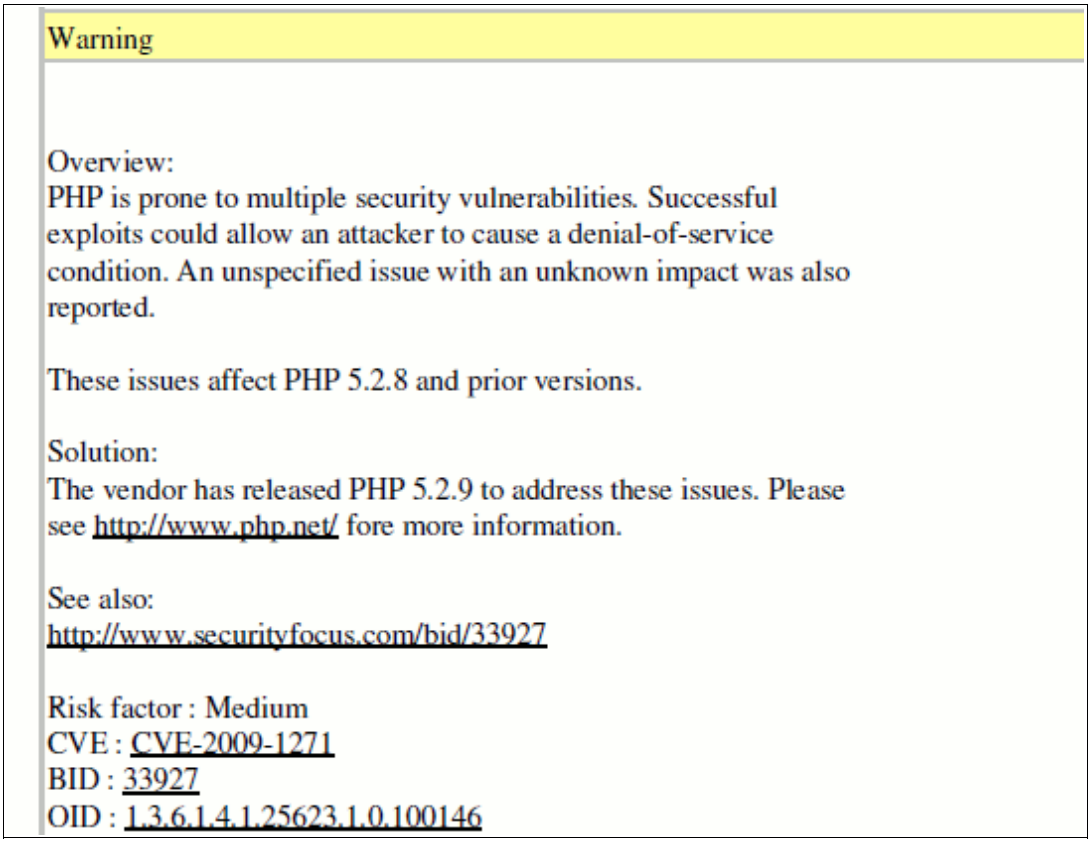
- 掃描結果分級:

  1.出現弱點(以紅色表示)

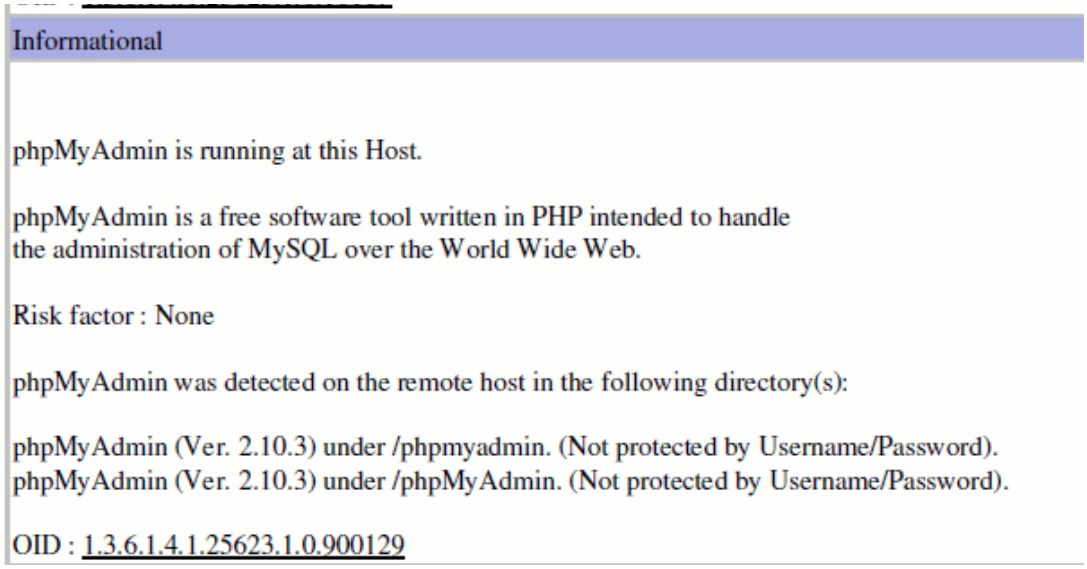



Fix: Apply patches from SVN repository, 修正參考
http://svn.php.net/viewvc?view=revision&revision=289557
*****
NOTE: Ignore this warning if patch is already applied.
*****
References:
http://secunia.com/advisories/37080/
http://www.vupen.com/english/advisories/2009/2930
http://marc.info/?l=oss-security&m=125562113503923&w=2
CVSS Score: 美國國家弱點評分等級
CVSS Base Score : 7.5 (AV:N/AC:L/Au:NR/C:P/I:P/A:P)
CVSS Temporal Score : 5.5
Risk factor: High 風險等級
CVE: CVE-2009-3546
BID : 36712 弱點編碼 可以超鏈結
OID : 1.3.6.1.4.1.25623.1.0.801123

2.警告(以黃色出現)


Warning
Overview:
PHP is prone to multiple security vulnerabilities. Successful exploits could allow an attacker to cause a denial-of-service condition. An unspecified issue with an unknown impact was also reported.
These issues affect PHP 5.2.8 and prior versions.
Solution:
The vendor has released PHP 5.2.9 to address these issues. Please see http://www.php.net/ fore more information.
See also:
http://www.securityfocus.com/bid/33927
Risk factor : Medium
CVE : CVE-2009-1271
BID : 33927
OID : 1.3.6.1.4.1.25623.1.0.100146

3.信息(以淺藍色表示)說明一些相關訊息



Informational

phpMyAdmin is running at this Host.

phpMyAdmin is a free software tool written in PHP intended to handle
the administration of MySQL over the World Wide Web.

Risk factor : None

phpMyAdmin was detected on the remote host in the following directory(s):

phpMyAdmin (Ver. 2.10.3) under /phpmyadmin. (Not protected by Username/Password).
phpMyAdmin (Ver. 2.10.3) under /phpMyAdmin. (Not protected by Username/Password).

OID : 1.3.6.1.4.1.25623.1.0.900129

- 檢查程式訊息說明