臺灣大學計算機及資訊網路中心
Computer and Information Networking Center (C&INC) of National Taiwan University (NTU)

臺灣大學計算機及資訊網路中心電子報

投稿日期	民國 104 年 10 月 10 日	編號	請空白
投稿類別	□校務服務　■技術論壇　□專題報導		
題目標題	弱點掃描技術報告		
摘要	隨著網路技術的蓬勃發展，網路上的惡意活動愈來愈頻繁，不論是個人或是企業，都更加重視自身在網路世界的安全防護。而資訊安全防護，除了大家所熟悉的防火牆、防毒軟體及入侵偵測防禦系統等，弱點掃描技術也是資安的重要技術之一。		
姓名	李美雯		
服務機構/職稱	臺灣大學計算機及資訊網路中心		
聯絡電話	0233665010		
電子郵件信箱	mli@ntu.edu.tw		
聯絡地址	106 台北市羅斯福路四段 1 號		
備註			

弱點掃描技術報告

李美雯
臺灣大學計算機及資訊網路中心程式設計師
作者：轉載自臺灣大學計資中心北區學術資訊安全維運中心

引言

隨著網路技術的蓬勃發展，網路上的惡意活動愈來愈頻繁，不論是個人或是企業，都更加重視自身在網路世界的安全防護。而資訊安全防護，除了大家所熟悉的防火牆、防毒軟體及入侵偵測防禦系統等，弱點掃描技術也是資安的重要技術之一。

弱點掃描之重要性

正所謂「水可載舟，亦可覆舟」，這句話亦完美詮釋了弱點掃描技術的特性。對於資訊安全的管理人員來說，善用弱點掃描的技術可以幫助他們了解所管理的設備是否存在漏洞，進而修補漏洞並將漏洞所造成的風險降到最低。然而此技術對於一些惡意的攻擊者而言，卻也是一種得力的攻擊工具，攻擊者一旦取得了目標主機或設備的相關漏洞，後續便可以利用這些漏洞針對目標進行攻擊行為。

弱點掃描屬於一種網路探測技術。利用弱點掃描的技術，相關設備管理人員可以了解所管理的主機、伺服器或網路設備是否存在相關的漏洞，當中包含了設備上各個 Port 的狀態、相關的服務（如：FTP、HTTP、SNMP 等），甚至一些伺服器上較為常用的軟體版本與語法的相關漏洞（如：PHP 等）。其行為主要是偵測並掃描位於主機上的各個端口或節點的弱點資訊後，與自身的資料庫進行比對，並將分析出的相關弱點或漏洞資訊產生報表，供管理者快速瞭解並進行設備管理的修正決策。

對網路設備管理者或企業而言，妥善防護網路與資訊設備是他們所冀望的。如果能將防火牆、入侵偵測防禦系統與弱點掃描技術相互結合，可以更有效提高網路與設備之安全防護。通過對設備的檢測，我們可以瞭解所管理的設備目前所開放的服務資訊與相關漏洞，並及時發現需要修補的部分，或是在評估此風險的嚴重性後，根據相關的分析結果安排漏洞修補的優先順序，在惡意攻擊者出現前先進行防範。

正所謂預防勝於治療，若要說防火牆和入侵偵測系統屬於被動的防禦方法，

那弱點掃描就屬於一種主動的防禦方法，化被動為主動，就是為了可以更有效降低攻擊者入侵的機會。也可以說弱點掃描如同我們去醫院健康檢查一樣，預先瞭解自身健康狀況後，以便了解後續的相關治療方式。

如何挑選適合的掃描工具軟體也是管理者需要研究的重要課題之一，業界上提供了開源軟體與商用軟體供管理者選擇。其中，開源軟體雖提供管理者得以免費使用，但因維護成本的關係，更新頻率較商用軟體來的低，相對影響工具的效能與準確度。而 Nexpose 雖然是一套商用軟體，另外提供了 Community Edition 的免費版本，32 組 IP 可同時進行主機弱點掃描，漏洞資料庫也未因為版本之差異而有所不同，對於一般管理者而言這是個相當實用的工具。

而弱點掃描工具大多數與滲透測試工具相互搭配，原因在於當管理者利用弱點掃描工具取得漏洞資訊後，會利用多種方法進一步驗證漏洞的存在與危害程度。而這些方法中，滲透測試工具常為管理人員所採用。目前業界有多款弱點掃描與滲透測試工具，但大多各自掌握自己的強項，彼此間缺少整合性。

而 Nexpose 與滲透測試工具 Metasploit 可整合應用，在 Nexpose 進行弱點掃描的同時，滲透測試工具 Metasploit 可提供滲透測試的模組資訊，同一時間兩者可搭配運用。這種整合應用除了可節省管理者每個漏洞逐一測試的時間外，且同一家廠商開發的兩種工具的整合性也較高。另外，這兩種工具都支援 Web 的 GUI 介面，這對於管理者來說也增加了操作上的便利。當然此兩套工具並無限制必須搭配使用，管理者即便是利用 Nexpose 得知弱點的相關資訊，亦可利用其他的方式進行相關驗證，端看管理者需求決定。有關滲透測試工具將再另外撰寫技術報告詳加說明。

此報告後續將以 Nexpose 弱點掃描工具為範例說明其功能與操作方式。

簡介弱點掃描工具-Nexpose

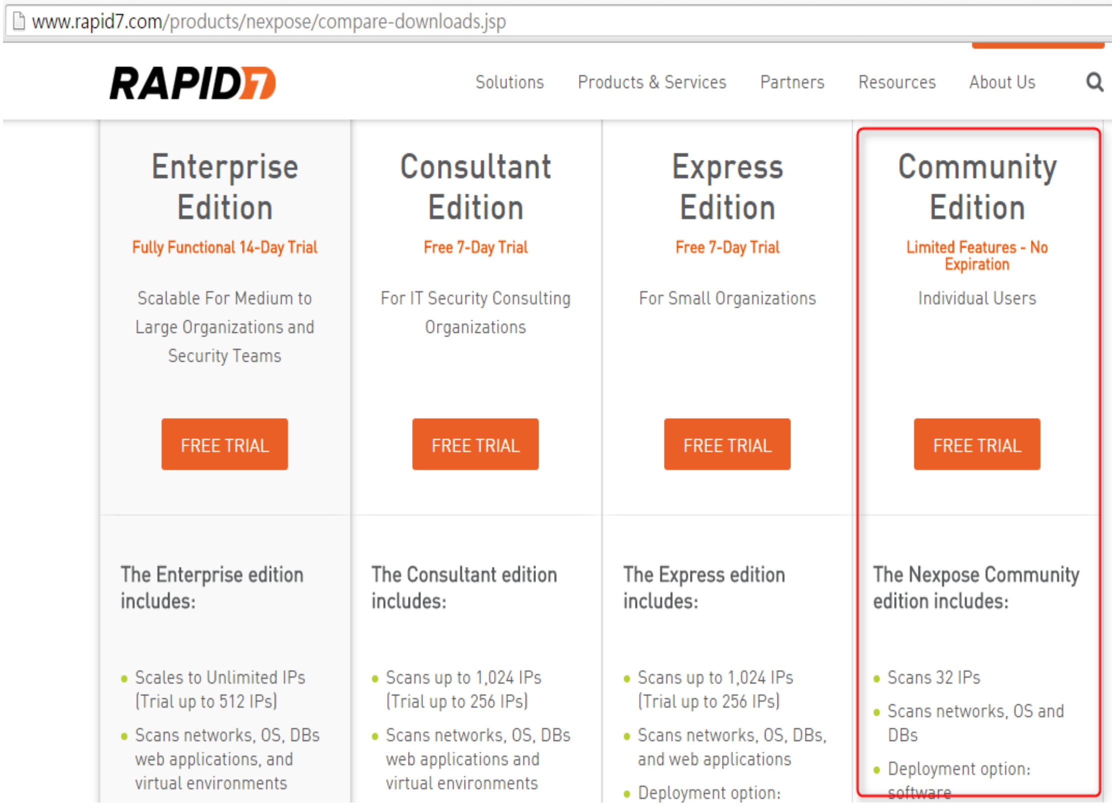
Nexpose 是一套弱點掃描工具，利用兩種風險指數評估，其一為 CVSS 的指數，另一種則是綜合主機重要程度、漏洞的嚴重程度與造成危害的程度，進行較精確的風險評估指數，並提供漏洞修補的建議方案。再者，也提供掃描排程的功能，讓管理者可精確的掌控掃描作業的時間以利漏洞修補。

Nexpose 為確保掃描時所需之弱點與漏洞的詳細資訊，與業界裡許多公認規模較大的弱點資料庫進行了整合，例如：BID[1]、CERT[2]、CVE[3]、IAVM、MS、MSKB、OVAL，接下來，以此工具為範例進行相關說明。

如何使用弱點掃描工具-Nexpose

Nexpose 的 Community Edition 可以免費使用（圖 1 紅框處），其他版本則需

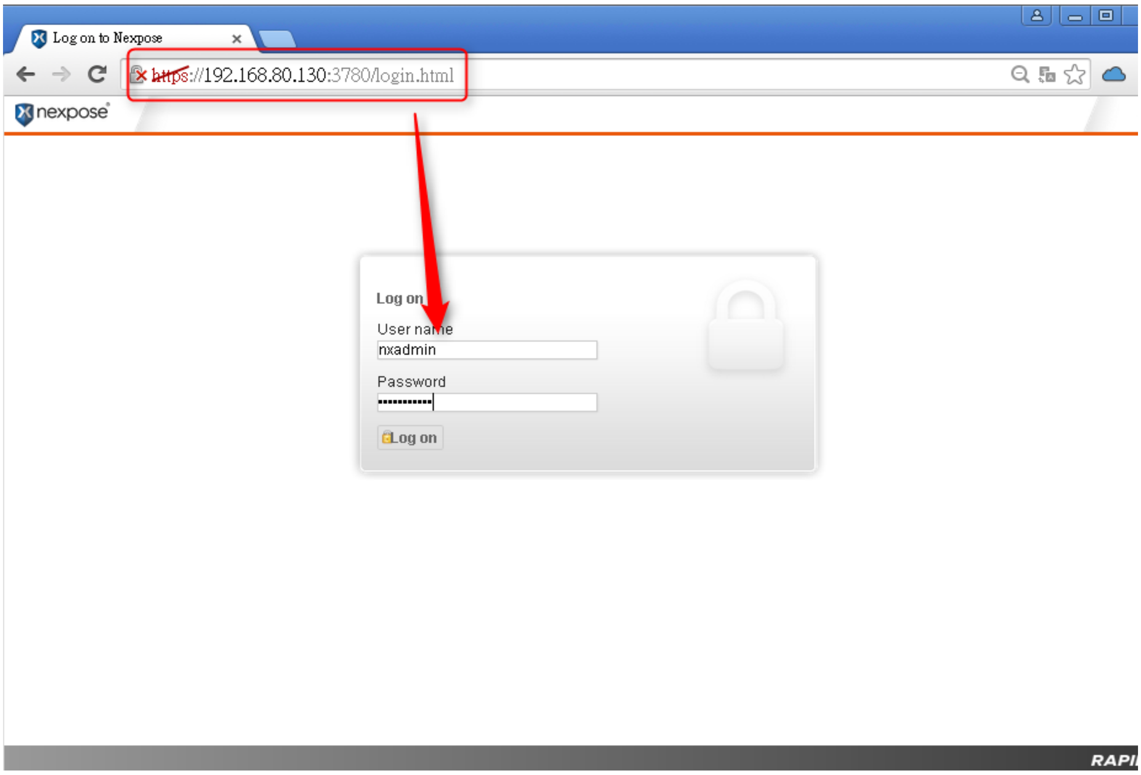
要收費。此版本雖然僅提供 32 組 IP 弱點掃描，但對於一般管理者而言綽綽有餘。



Enterprise Edition	Consultant Edition	Express Edition	Community Edition
Fully Functional 14-Day Trial	Free 7-Day Trial	Free 7-Day Trial	Limited Features - No Expiration
Scalable For Medium to Large Organizations and Security Teams	For IT Security Consulting Organizations	For Small Organizations	Individual Users
FREE TRIAL	FREE TRIAL	FREE TRIAL	FREE TRIAL
The Enterprise edition includes:	The Consultant edition includes:	The Express edition includes:	The Nexpose Community edition includes:
• Scales to Unlimited IPs (Trial up to 512 IPs) • Scans networks, OS, DBs web applications, and virtual environments	• Scans up to 1,024 IPs (Trial up to 256 IPs) • Scans networks, OS, DBs web applications and virtual environments	• Scans up to 1,024 IPs (Trial up to 256 IPs) • Scans networks, OS, DBs, and web applications • Deployment option:	• Scans 32 IPs • Scans networks, OS and DBs • Deployment option: software

圖 1

下載相關檔案並註冊完畢後，請連線 http://localhost:3780，並輸入帳密登入，如圖 2 所示。



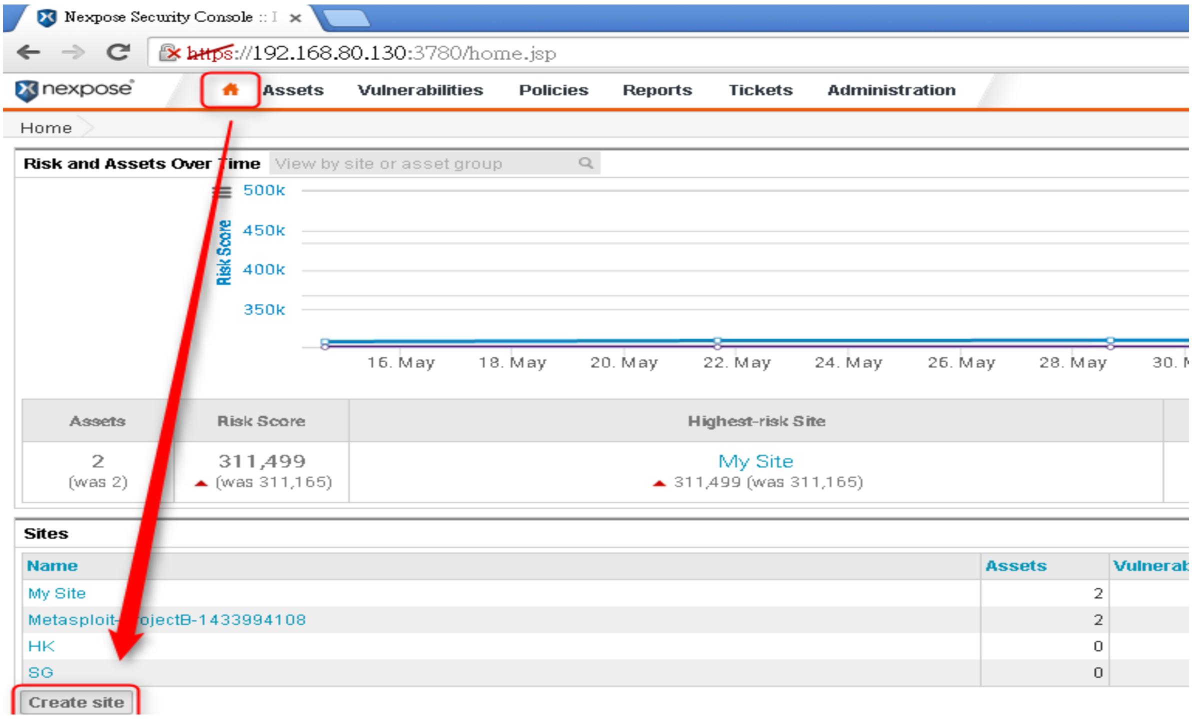
Log on

User name: nxadmin

Password: ••••••••••••

圖 2

在網站的主選單上點選一個「房屋」圖示(icon)後，點擊「Create site」按鈕，將顯示下一個「Site Configuration」的設置頁面。



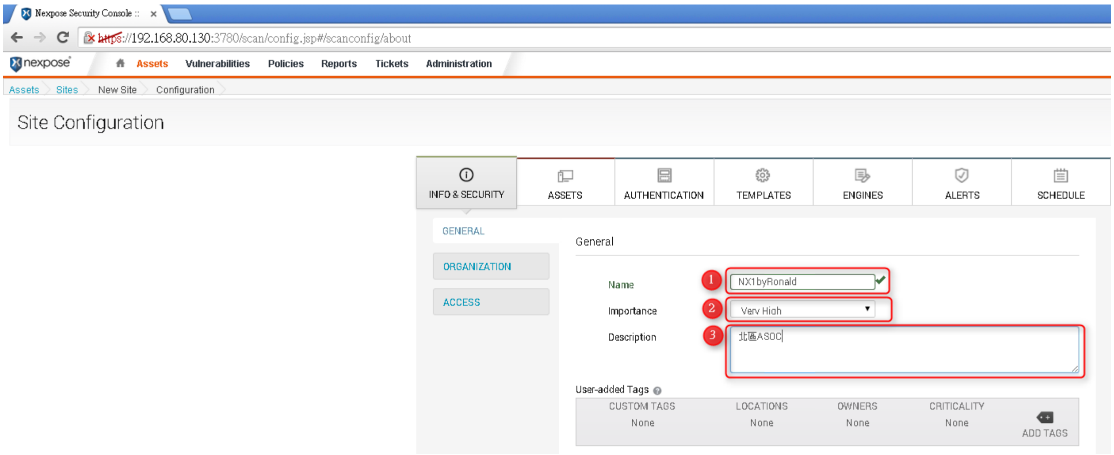
Assets	Risk Score	Highest-risk Site
2 (was 2)	311,499 ▲ (was 311,165)	My Site ▲ 311,499 (was 311,165)

Sites

Name	Assets	Vulnerat
My Site	2	
Metasploit-ProjectB-1433994108	2	
HK	0	
SG	0	

圖 3

在「Site Configuration」頁面，第一個「GENERAL」頁籤需填寫基本資訊，如 Name 與 Description（圖 4 編號 1&3 所示）。需留意的是 Importance 的部分（圖 4 編號 2），此設定將影響 Nexpose 對於漏洞風險評估分數的評分標準。



Site Configuration

General

Name: NX1byRonald

Importance: Very High

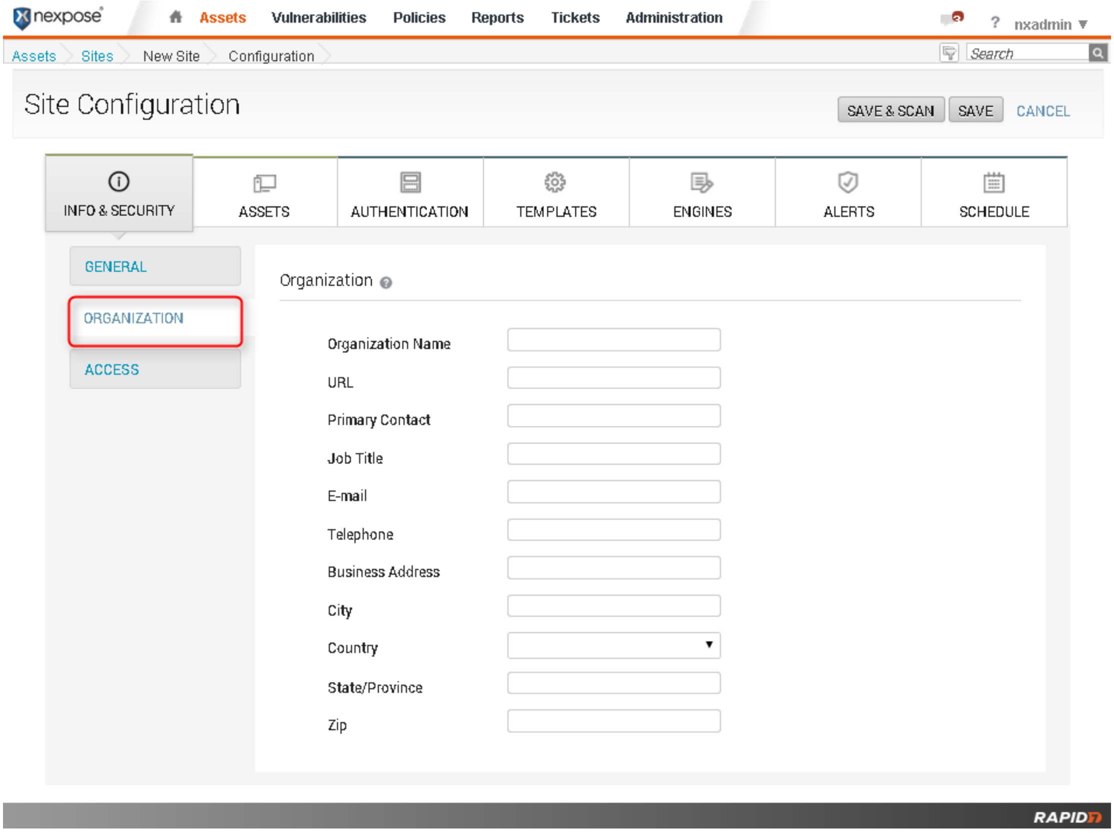
Description: 北區ASOC

User-added Tags

CUSTOM TAGS	LOCATIONS	OWNERS	CRITICALITY
None	None	None	None

圖 4

「ORGANIZATION」頁籤填寫組織資訊，將顯示在輸出的報表上。



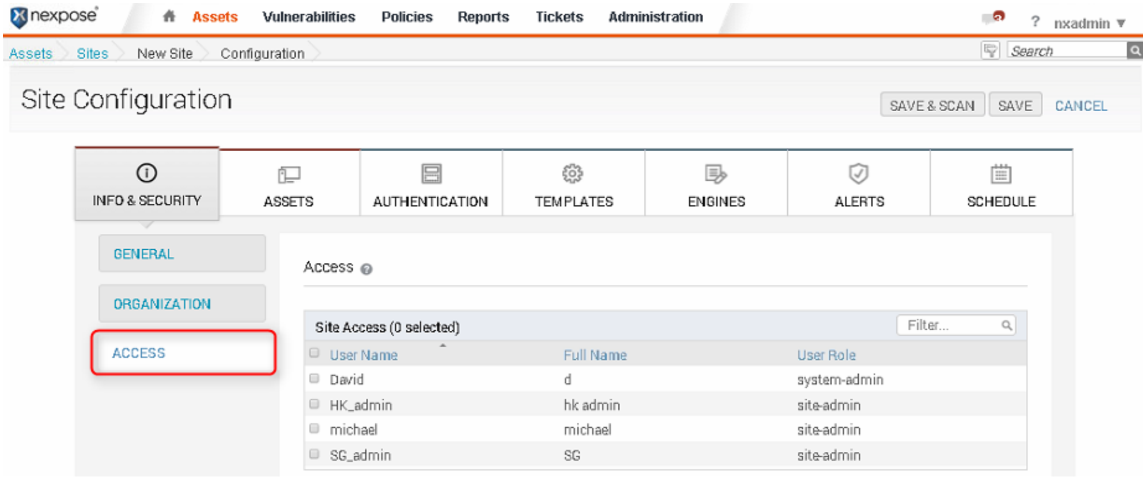
Site Configuration

Organization

Organization Name
URL
Primary Contact
Job Title
E-mail
Telephone
Business Address
City
Country
State/Province
Zip

圖 5

「ACCESS」頁籤是針對此 site 若有多位管理者，可以設定存取權限以便其他管理者管理此工具。

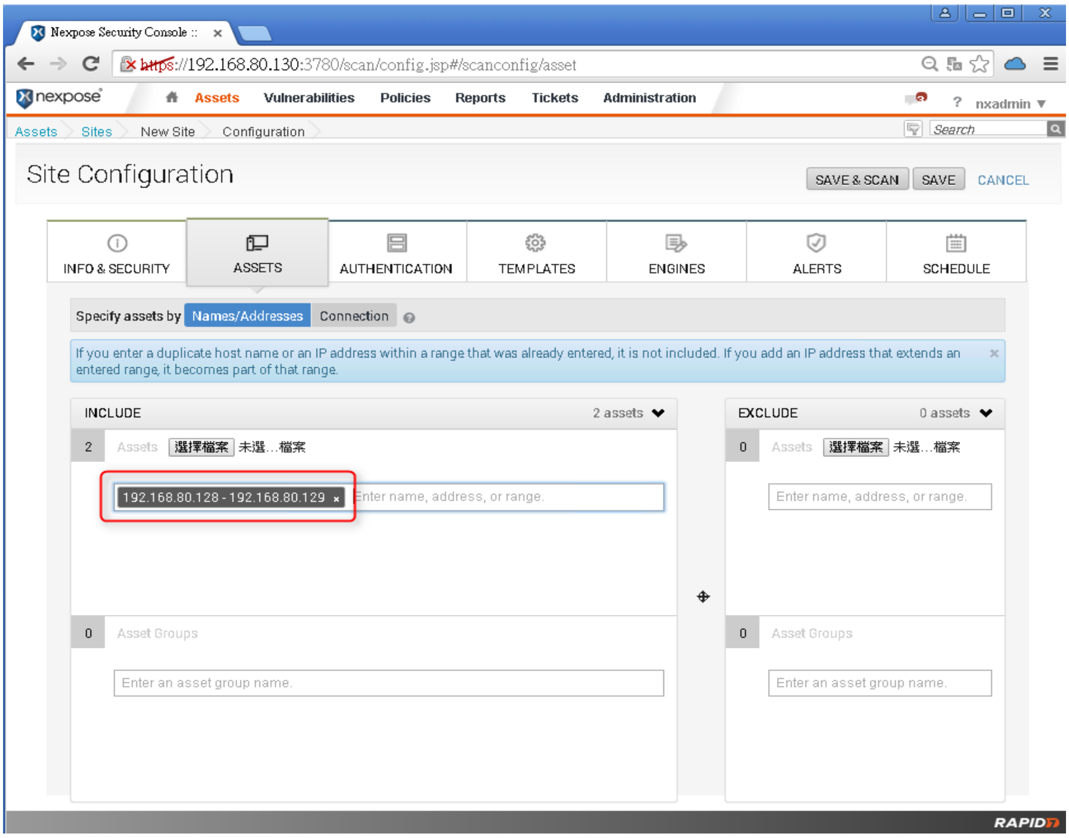


Site Access (0 selected)

	User Name	Full Name	User Role
□	David	d	system-admin
□	HK_admin	hk admin	site-admin
□	michael	michael	site-admin
□	SG_admin	SG	site-admin

圖 6

「Assets」頁籤有兩個部分，如圖 7 所示「Included Assets」和「Excluded Assets」。在「Included Assets」中我們以兩個目標 IP 位址作範例，在此欄位可以輸入一個網段或是個別的 IP。也可以利用匯入檔案的功能匯入 IP 列表檔。「Excluded Assets」是例外清單，可排除不需掃描的 IP。



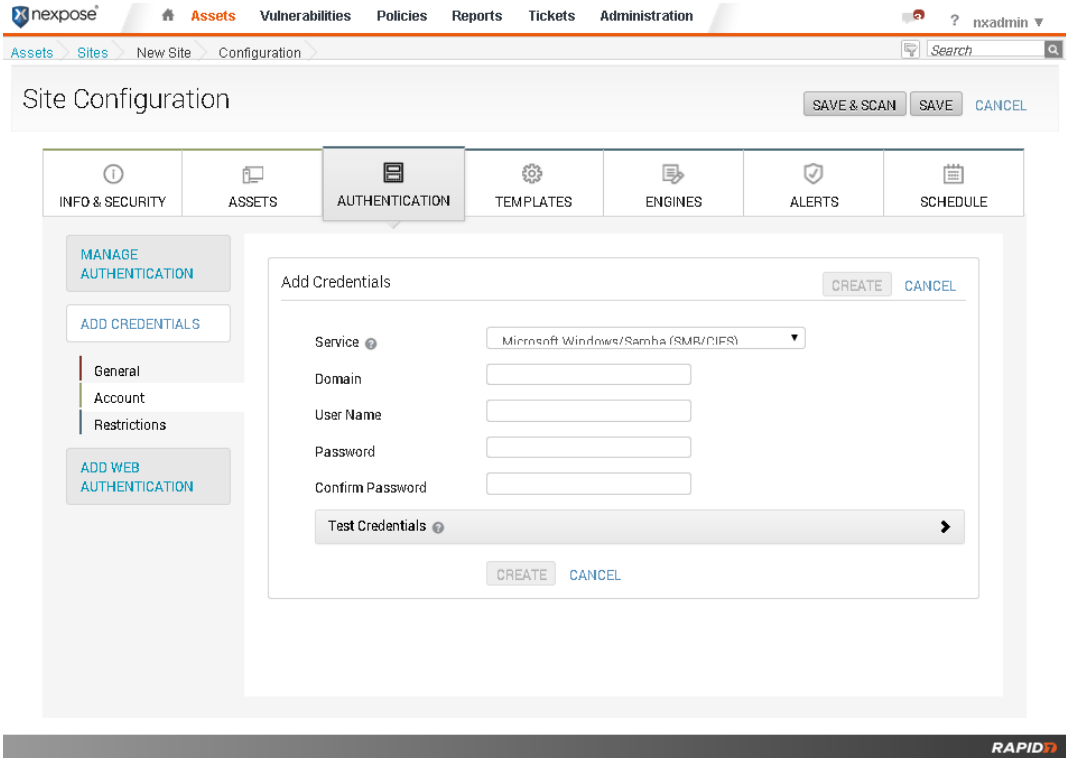
If you enter a duplicate host name or an IP address within a range that was already entered, it is not included. If you add an IP address that extends an entered range, it becomes part of that range.

INCLUDE: 2 Assets — 192.168.80.128 - 192.168.80.129

EXCLUDE: 0 Assets

圖 7

在 Authentication 的頁籤裡，主要是針對欲掃描的目標主機或網頁，進行認證上的相關設定。在這裡我們可以添加目標主機的一些使用者資訊。若是使用的管理者權限來進行主機的掃描，亦會提升掃描的準確性與完整度。



Site Configuration

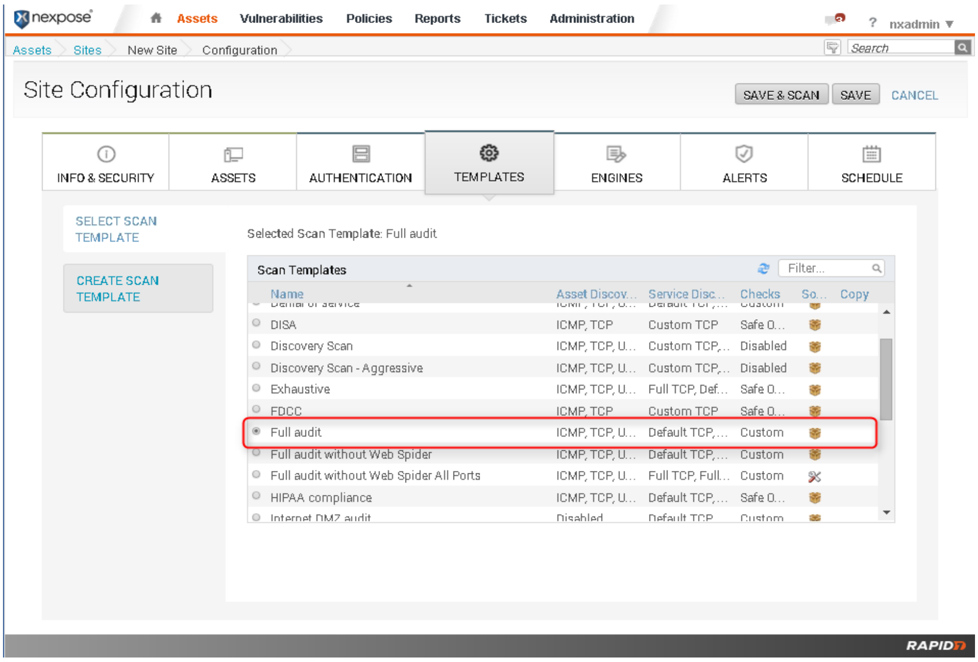
Add Credentials

Service	Microsoft Windows/Samba (SMB/CIFS)
Domain	
User Name	
Password	
Confirm Password	

Test Credentials

圖 8

「TEMPLATES」頁籤是選擇預計選用的掃描模組，每種模組有其定義的掃描方式與範圍，通常多選擇「Full audit」即可。



Site Configuration

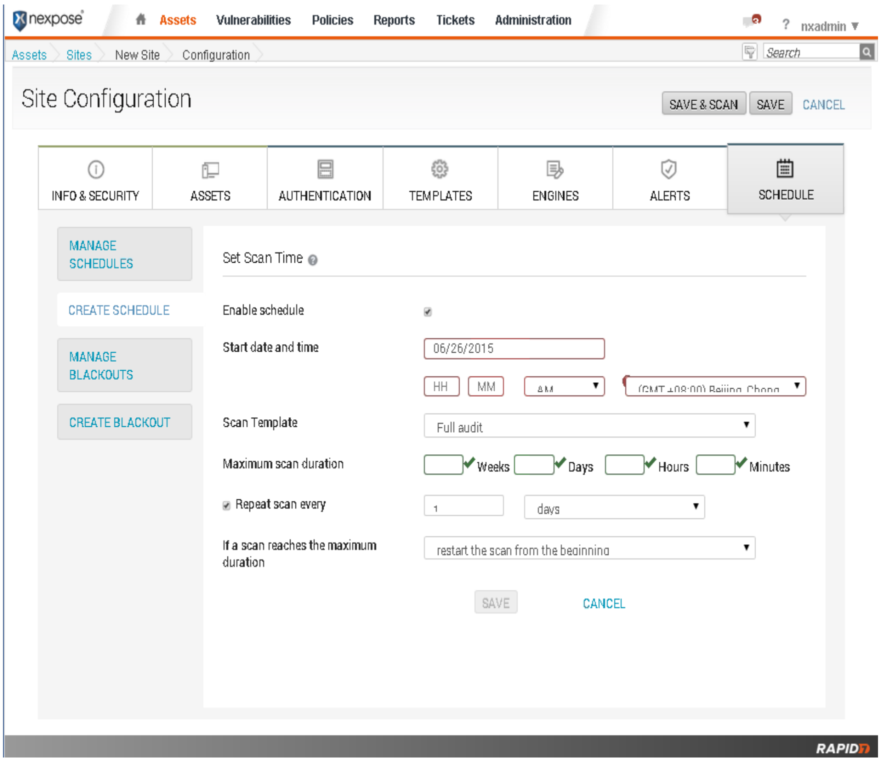
Selected Scan Template: Full audit

Scan Templates

	Name	Asset Discov...	Service Disc...	Checks	So...	Copy
○	Denial of service	ICMP, TCP, U...	Default TCP,...	Custom		
○	DISA	ICMP, TCP	Custom TCP	Safe O...		
○	Discovery Scan	ICMP, TCP, U...	Custom TCP,...	Disabled		
○	Discovery Scan - Aggressive	ICMP, TCP, U...	Custom TCP,...	Disabled		
○	Exhaustive	ICMP, TCP, U...	Full TCP, Def...	Safe O...		
○	FDCC	ICMP, TCP	Custom TCP	Safe O...		
●	Full audit	ICMP, TCP, U...	Default TCP,...	Custom		
○	Full audit without Web Spider	ICMP, TCP, U...	Default TCP,...	Custom		
○	Full audit without Web Spider All Ports	ICMP, TCP, U...	Full TCP, Full...	Custom		
○	HIPAA compliance	ICMP, TCP, U...	Default TCP,...	Safe O...		
○	Internet DMZ audit	Disabled	Default TCP	Custom		

圖 9

「Enable schedule」頁籤屬於 Nexpose 的掃描排程，讓管理者可掌控掃描時程以利後續修補工作。完成設置後先點選「Save」儲存相關設定，再點選「SAVE&SCAN」進行掃描。



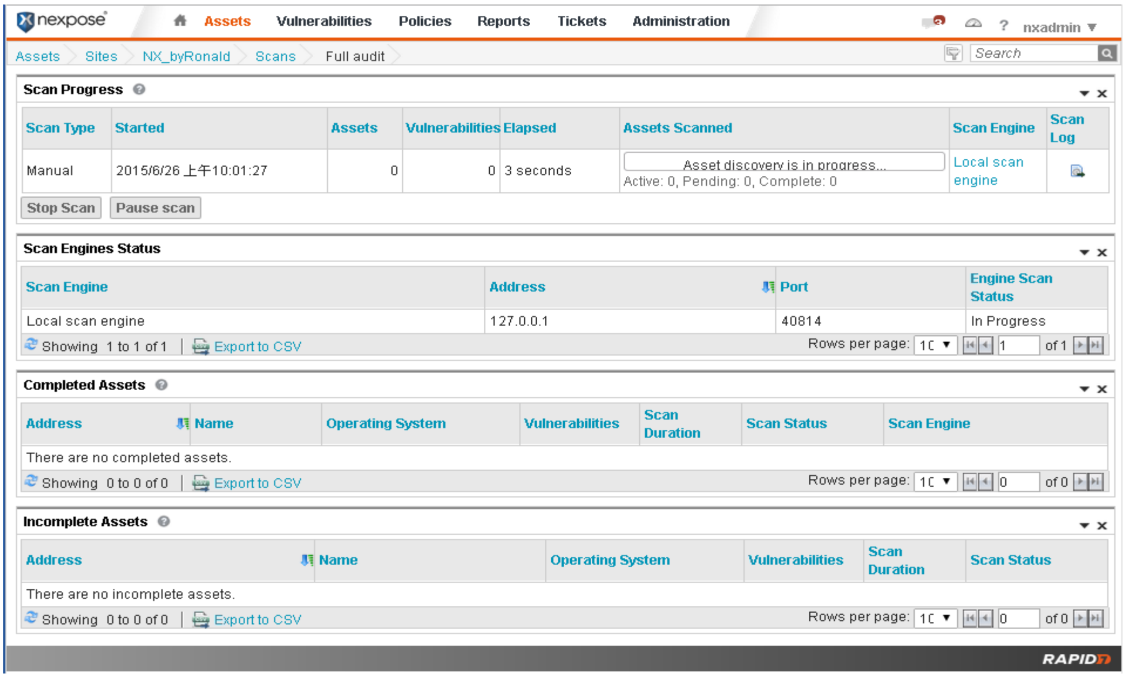
Site Configuration

Set Scan Time

Enable schedule	☑
Start date and time	06/26/2015 HH MM AM (GMT+08:00) Beijing, Chong...
Scan Template	Full audit
Maximum scan duration	Weeks Days Hours Minutes
☑ Repeat scan every	1 days
If a scan reaches the maximum duration	restart the scan from the beginning

圖 10

掃描開始後可以察看掃描進度與相關資訊，也可暫停或停止掃描。



Scan Progress

Scan Type	Started	Assets	Vulnerabilities	Elapsed	Assets Scanned	Scan Engine	Scan Log
Manual	2015/6/26 上午10:01:27	0	0	3 seconds	Asset discovery is in progress... Active: 0, Pending: 0, Complete: 0	Local scan engine	

Scan Engines Status

Scan Engine	Address	Port	Engine Scan Status
Local scan engine	127.0.0.1	40814	In Progress

Showing 1 to 1 of 1 | Export to CSV Rows per page: 10 1 of 1

Completed Assets

Address	Name	Operating System	Vulnerabilities	Scan Duration	Scan Status	Scan Engine
There are no completed assets.						

Showing 0 to 0 of 0 | Export to CSV Rows per page: 10 0 of 0

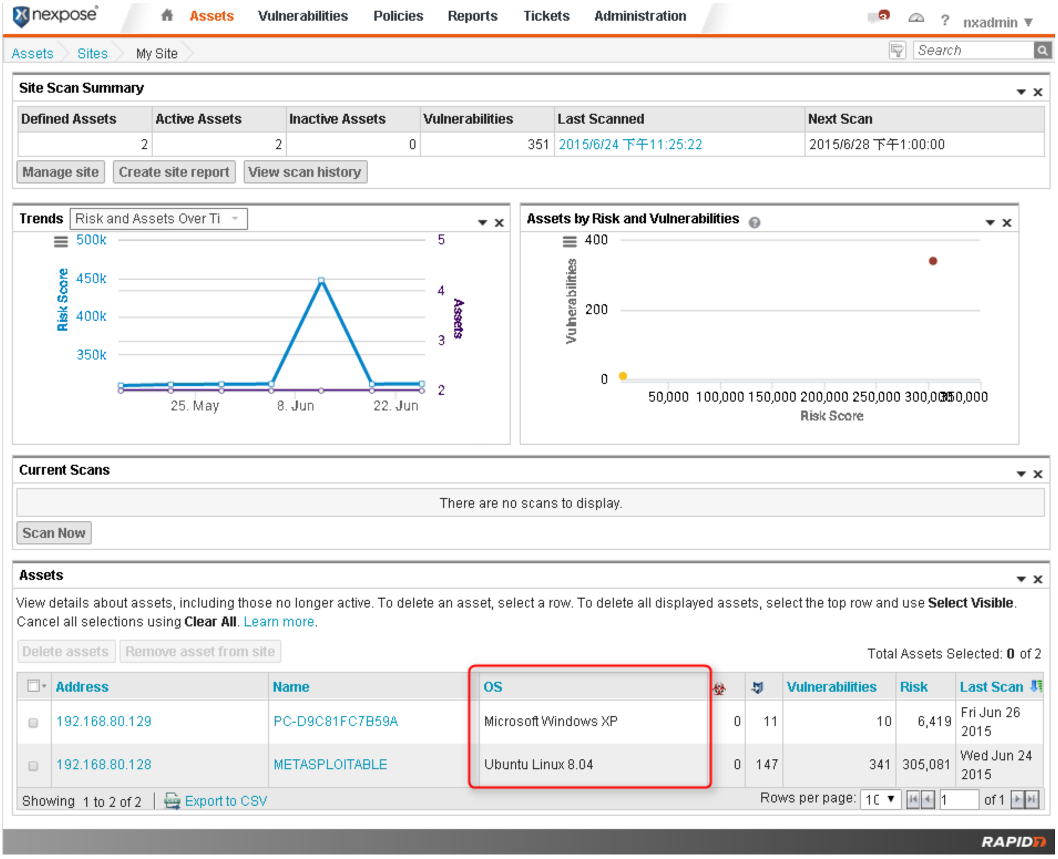
Incomplete Assets

Address	Name	Operating System	Vulnerabilities	Scan Duration	Scan Status
There are no incomplete assets.					

Showing 0 to 0 of 0 | Export to CSV Rows per page: 10 0 of 0

圖 11

掃描完成後可看到主機基本訊息。以範例設定的兩組 IP 為例，一台是 Windows XP，另一台則是 Ubuntu Linux 8.04。



Site Scan Summary

Defined Assets	Active Assets	Inactive Assets	Vulnerabilities	Last Scanned	Next Scan
2	2	0	351	2015/6/24 下午11:25:22	2015/6/28 下午1:00:00

Manage site | Create site report | View scan history

Current Scans

There are no scans to display.

Scan Now

Assets

View details about assets, including those no longer active. To delete an asset, select a row. To delete all displayed assets, select the top row and use **Select Visible**. Cancel all selections using **Clear All**. Learn more.

Delete assets | Remove asset from site

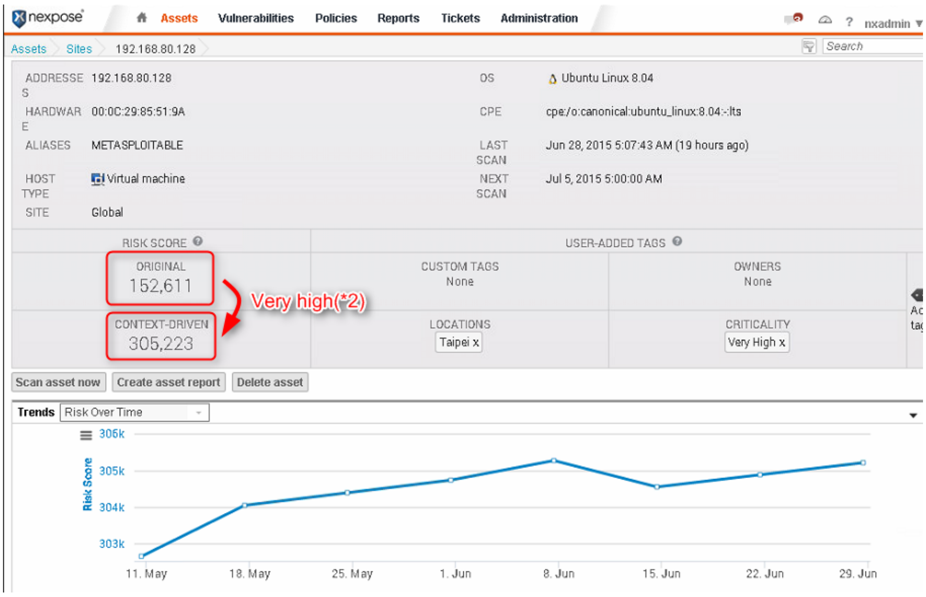
Total Assets Selected: **0** of 2

□	Address	Name	OS	☣		Vulnerabilities	Risk	Last Scan
□	192.168.80.129	PC-D9C81FC7B59A	Microsoft Windows XP	0	11	10	6,419	Fri Jun 26 2015
□	192.168.80.128	METASPLOITABLE	Ubuntu Linux 8.04	0	147	341	305,081	Wed Jun 24 2015

Showing 1 to 2 of 2 | Export to CSV   Rows per page: 10 ▼ 1 of 1

圖 12

點選主機名稱可以查看更詳細的資訊，如作業系統、風險指數等。CONTEXT-DRIVEN 分數的計算，是依照 Importance 設定的等級而來的。



ADDRESSES	192.168.80.128	OS	Ubuntu Linux 8.04
HARDWARE	00:0C:29:85:51:9A	CPE	cpe:/o:canonical:ubuntu_linux:8.04:-:lts
ALIASES	METASPLOITABLE	LAST SCAN	Jun 28, 2015 5:07:43 AM (19 hours ago)
HOST TYPE	Virtual machine	NEXT SCAN	Jul 5, 2015 5:00:00 AM
SITE	Global		

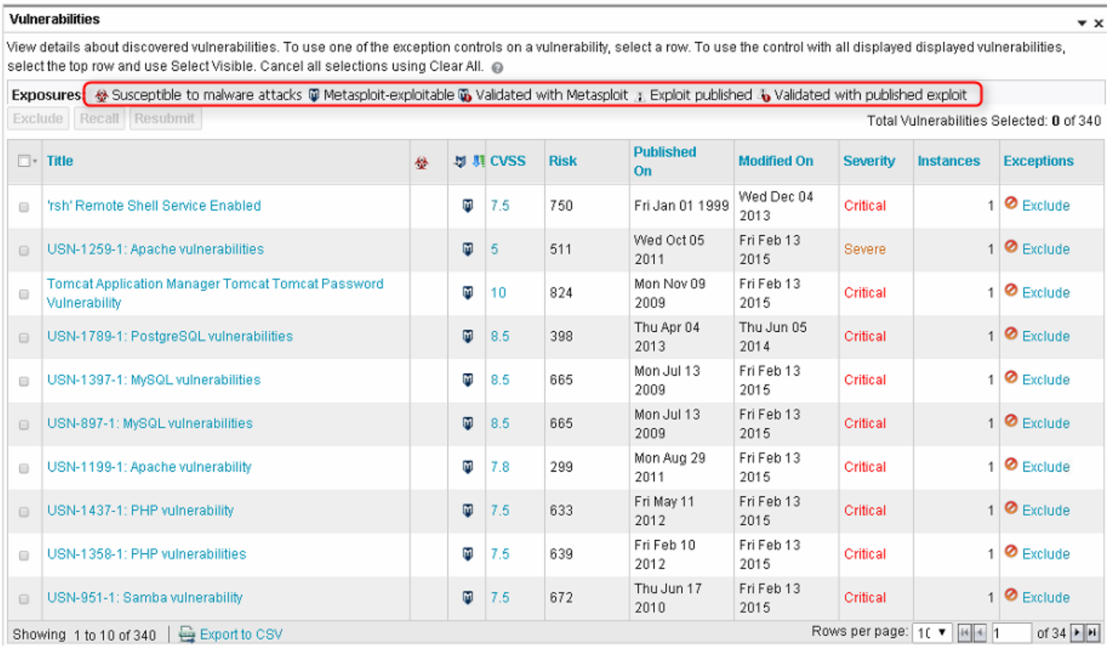
RISK SCORE
ORIGINAL 152,611
CONTEXT-DRIVEN 305,223

USER-ADDED TAGS
CUSTOM TAGS None
OWNERS None
LOCATIONS Taipei x
CRITICALITY Very High x

Scan asset now | Create asset report | Delete asset

圖 13

透過「Vulnerabilities」可查看主機被掃瞄到的漏洞。在「Exposures」的敘述中，如下圖紅色框內的 icon 所示，第一個 icon 圖示代表容易受到惡意軟體攻擊，第二個 icon 圖示代表漏洞可被 Metasploit 利用，第三個 icon 圖示代表已被 Metasploit 驗證可以利用。第四個 icon 圖示代表漏洞已經發布相關 exploit-db，亦即可以從 exploit-db 獲取漏洞相關訊息並可被有心人士利用，若被利用成功，則會顯示第五個 icon 圖示。



Vulnerabilities

View details about discovered vulnerabilities. To use one of the exception controls on a vulnerability, select a row. To use the control with all displayed displayed vulnerabilities, select the top row and use Select Visible. Cancel all selections using Clear All.

Exposures Susceptible to malware attacks　Metasploit-exploitable　Validated with Metasploit　Exploit published　Validated with published exploit

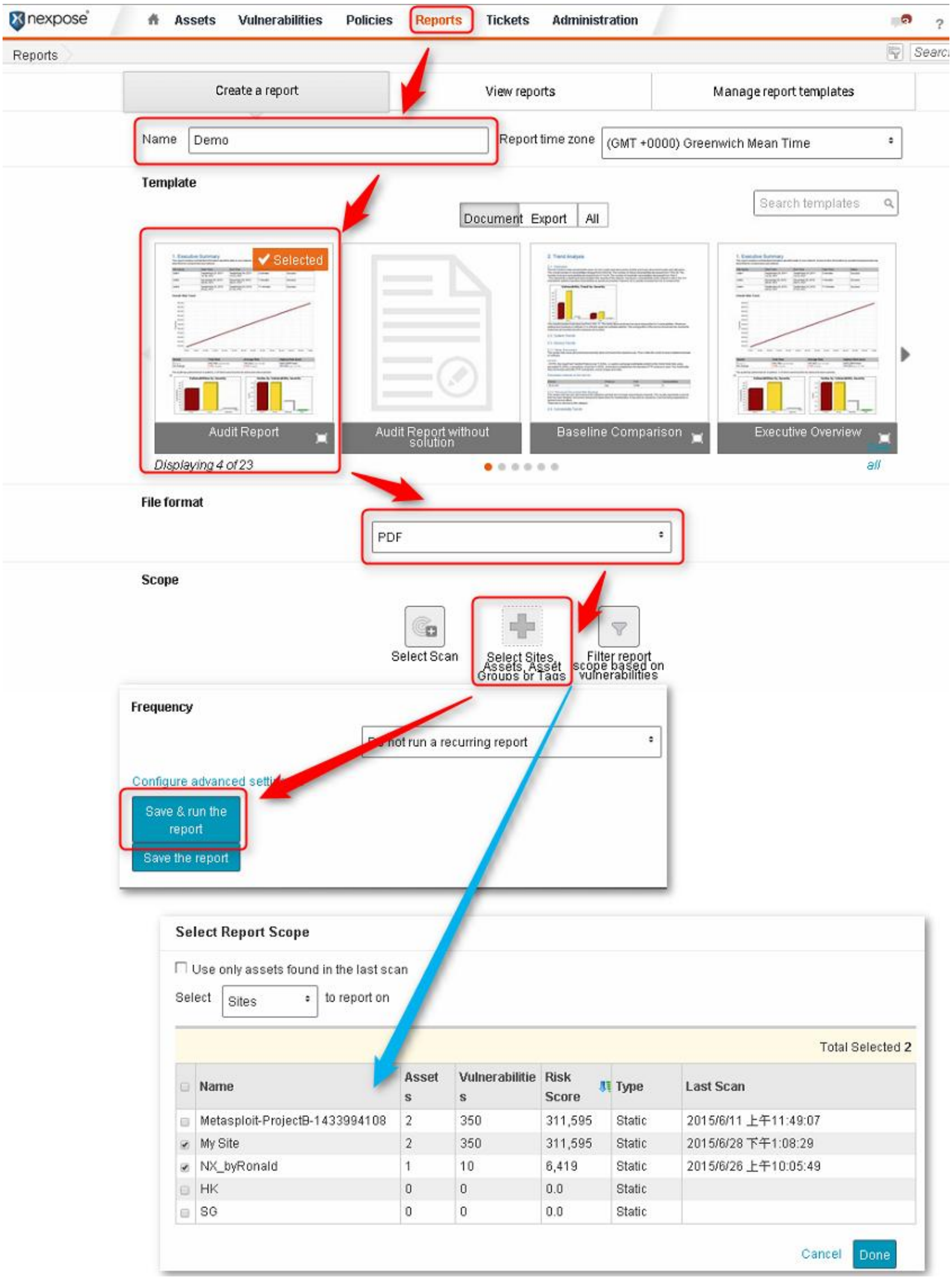
Total Vulnerabilities Selected: **0** of 340

☐	Title			CVSS	Risk	Published On	Modified On	Severity	Instances	Exceptions
☐	'rsh' Remote Shell Service Enabled		🛡	7.5	750	Fri Jan 01 1999	Wed Dec 04 2013	Critical	1	Exclude
☐	USN-1259-1: Apache vulnerabilities		🛡	5	511	Wed Oct 05 2011	Fri Feb 13 2015	Severe	1	Exclude
☐	Tomcat Application Manager Tomcat Tomcat Password Vulnerability		🛡	10	824	Mon Nov 09 2009	Fri Feb 13 2015	Critical	1	Exclude
☐	USN-1789-1: PostgreSQL vulnerabilities		🛡	8.5	398	Thu Apr 04 2013	Thu Jun 05 2014	Critical	1	Exclude
☐	USN-1397-1: MySQL vulnerabilities		🛡	8.5	665	Mon Jul 13 2009	Fri Feb 13 2015	Critical	1	Exclude
☐	USN-897-1: MySQL vulnerabilities		🛡	8.5	665	Mon Jul 13 2009	Fri Feb 13 2015	Critical	1	Exclude
☐	USN-1199-1: Apache vulnerability		🛡	7.8	299	Mon Aug 29 2011	Fri Feb 13 2015	Critical	1	Exclude
☐	USN-1437-1: PHP vulnerability		🛡	7.5	633	Fri May 11 2012	Fri Feb 13 2015	Critical	1	Exclude
☐	USN-1358-1: PHP vulnerabilities		🛡	7.5	639	Fri Feb 10 2012	Fri Feb 13 2015	Critical	1	Exclude
☐	USN-951-1: Samba vulnerability		🛡	7.5	672	Thu Jun 17 2010	Fri Feb 13 2015	Critical	1	Exclude

Showing 1 to 10 of 340 | Export to CSV　　Rows per page: 10　1　of 34

圖 14

在「Reports->Create a Report」頁籤中設定報表檔案名稱後，選擇報表範本類型與檔案格式並產出報表。範例中類型選擇「Audit Report」，格式為 PDF。接著選擇「sites」後，點選「+」圖示。從「Select Report Scope」選擇欲產生的報表 sites，並點選「Done」確認，最後就可以點選「Save & run the report」產出報表。



Name: Demo

Report time zone: (GMT +0000) Greenwich Mean Time

File format: PDF

Frequency: Do not run a recurring report

Select Report Scope

□ Use only assets found in the last scan

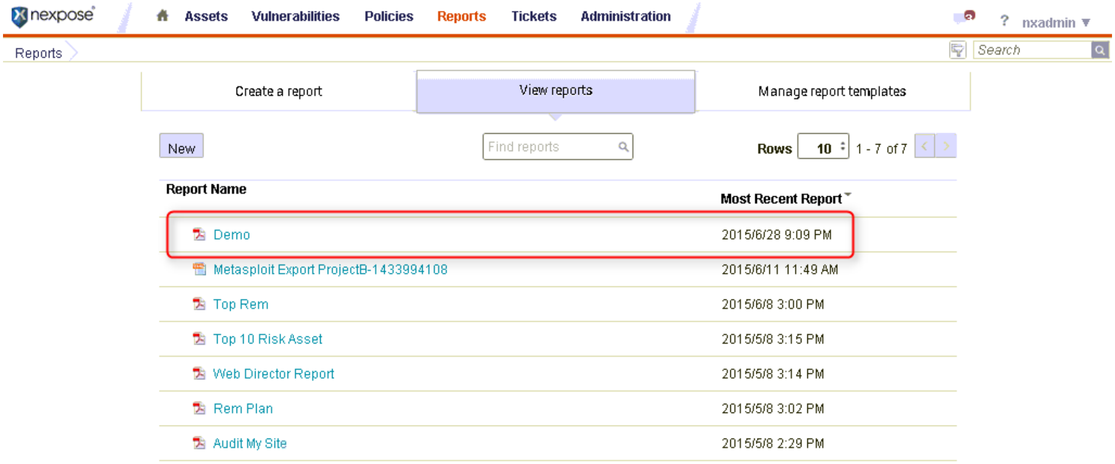
Select Sites to report on

Total Selected 2

□	Name	Assets	Vulnerabilities	Risk Score	Type	Last Scan
□	Metasploit-ProjectB-1433994108	2	350	311,595	Static	2015/6/11 上午11:49:07
☑	My Site	2	350	311,595	Static	2015/6/28 下午1:08:29
☑	NX_byRonald	1	10	6,419	Static	2015/6/26 上午10:05:49
□	HK	0	0	0.0	Static	
□	SG	0	0	0.0	Static	

圖 15

「View reports」頁籤可查看產出報表的清單。

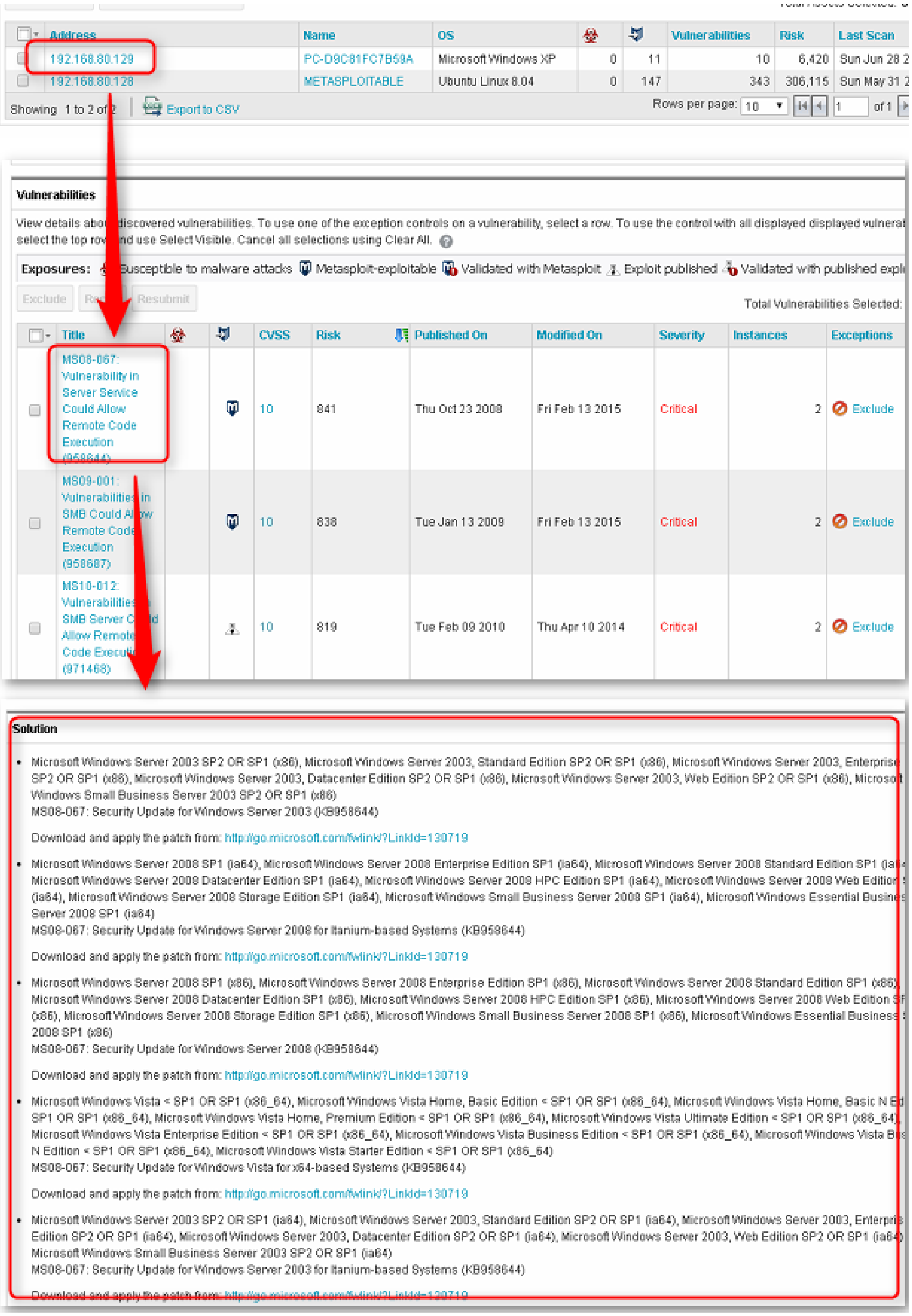


Report Name	Most Recent Report
Demo	2015/6/28 9:09 PM
Metasploit Export ProjectB-1433994108	2015/6/11 11:49 AM
Top Rem	2015/6/8 3:00 PM
Top 10 Risk Asset	2015/5/8 3:15 PM
Web Director Report	2015/5/8 3:14 PM
Rem Plan	2015/5/8 3:02 PM
Audit My Site	2015/5/8 2:29 PM

圖 16

如何進行漏洞修復

針對掃描工具掃出漏洞後應該作的修補工作，可參考圖 17，「Nexpose」在頁籤中提供漏洞修補資訊。



□ Address	Name	OS	☣	🛡	Vulnerabilities	Risk	Last Scan
□ 192.168.80.129	PC-D9C81FC7B59A	Microsoft Windows XP	0	11	10	6,420	Sun Jun 28 2
□ 192.168.80.128	METASPLOITABLE	Ubuntu Linux 8.04	0	147	343	306,115	Sun May 31 2

Showing 1 to 2 of 2 | Export to CSV   Rows per page: 10 ▾ 1 of 1

Vulnerabilities

View details abo discovered vulnerabilities. To use one of the exception controls on a vulnerability, select a row. To use the control with all displayed displayed vulnerat select the top ro nd use Select Visible. Cancel all selections using Clear All.

Exposures: Susceptible to malware attacks Metasploit-exploitable Validated with Metasploit Exploit published Validated with published expl

Exclude Re Resubmit   Total Vulnerabilities Selected:

□ Title	☣	🛡	CVSS	Risk	Published On	Modified On	Severity	Instances	Exceptions
□ MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)		🛡	10	841	Thu Oct 23 2008	Fri Feb 13 2015	Critical	2	⊘ Exclude
□ MS09-001: Vulnerabilitie in SMB Could Al ow Remote Code Execution (958687)		🛡	10	838	Tue Jan 13 2009	Fri Feb 13 2015	Critical	2	⊘ Exclude
□ MS10-012: Vulnerabilities SMB Server C d Allow Remote Code Executi (971468)		⚠	10	819	Tue Feb 09 2010	Thu Apr 10 2014	Critical	2	⊘ Exclude

Solution

- Microsoft Windows Server 2003 SP2 OR SP1 (x86), Microsoft Windows Server 2003, Standard Edition SP2 OR SP1 (x86), Microsoft Windows Server 2003, Enterprise SP2 OR SP1 (x86), Microsoft Windows Server 2003, Datacenter Edition SP2 OR SP1 (x86), Microsoft Windows Server 2003, Web Edition SP2 OR SP1 (x86), Microsoft Windows Small Business Server 2003 SP2 OR SP1 (x86)
  MS08-067: Security Update for Windows Server 2003 (KB958644)

  Download and apply the patch from: http://go.microsoft.com/fwlink/?LinkId=130719

- Microsoft Windows Server 2008 SP1 (ia64), Microsoft Windows Server 2008 Enterprise Edition SP1 (ia64), Microsoft Windows Server 2008 Standard Edition SP1 (ia Microsoft Windows Server 2008 Datacenter Edition SP1 (ia64), Microsoft Windows Server 2008 HPC Edition SP1 (ia64), Microsoft Windows Server 2008 Web Editio (ia64), Microsoft Windows Server 2008 Storage Edition SP1 (ia64), Microsoft Windows Small Business Server 2008 SP1 (ia64), Microsoft Windows Essential Busine Server 2008 SP1 (ia64)
  MS08-067: Security Update for Windows Server 2008 for Itanium-based Systems (KB958644)

  Download and apply the patch from: http://go.microsoft.com/fwlink/?LinkId=130719

- Microsoft Windows Server 2008 SP1 (x86), Microsoft Windows Server 2008 Enterprise Edition SP1 (x86), Microsoft Windows Server 2008 Standard Edition SP1 (x86), Microsoft Windows Server 2008 Datacenter Edition SP1 (x86), Microsoft Windows Server 2008 HPC Edition SP1 (x86), Microsoft Windows Server 2008 Web Edition S (x86), Microsoft Windows Server 2008 Storage Edition SP1 (x86), Microsoft Windows Small Business Server 2008 SP1 (x86), Microsoft Windows Essential Business 2008 SP1 (x86)
  MS08-067: Security Update for Windows Server 2008 (KB958644)

  Download and apply the patch from: http://go.microsoft.com/fwlink/?LinkId=130719

- Microsoft Windows Vista < SP1 OR SP1 (x86_64), Microsoft Windows Vista Home, Basic Edition < SP1 OR SP1 (x86_64), Microsoft Windows Vista Home, Basic N Ed SP1 OR SP1 (x86_64), Microsoft Windows Vista Home, Premium Edition < SP1 OR SP1 (x86_64), Microsoft Windows Vista Ultimate Edition < SP1 OR SP1 (x86_64), Microsoft Windows Vista Enterprise Edition < SP1 OR SP1 (x86_64), Microsoft Windows Vista Business Edition < SP1 OR SP1 (x86_64), Microsoft Windows Vista Bu N Edition < SP1 OR SP1 (x86_64), Microsoft Windows Vista Starter Edition < SP1 OR SP1 (x86_64)
  MS08-067: Security Update for Windows Vista for x64-based Systems (KB958644)

  Download and apply the patch from: http://go.microsoft.com/fwlink/?LinkId=130719

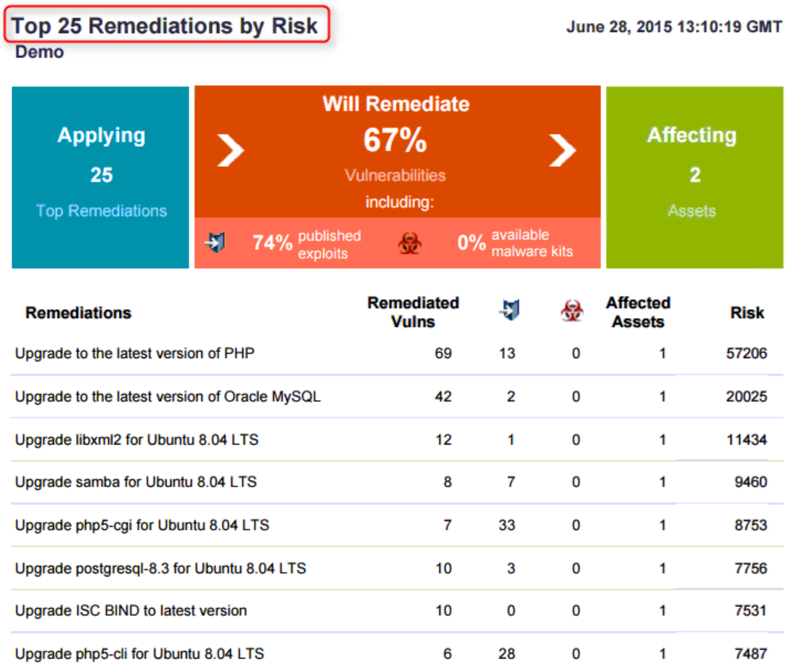
- Microsoft Windows Server 2003 SP2 OR SP1 (ia64), Microsoft Windows Server 2003, Standard Edition SP2 OR SP1 (ia64), Microsoft Windows Server 2003, Enterpris Edition SP2 OR SP1 (ia64), Microsoft Windows Server 2003, Datacenter Edition SP2 OR SP1 (ia64), Microsoft Windows Server 2003, Web Edition SP2 OR SP1 (ia64) Microsoft Windows Small Business Server 2003 SP2 OR SP1 (ia64)
  MS08-067: Security Update for Windows Server 2003 for Itanium-based Systems (KB958644)

  Download and apply the patch from: http://go.microsoft.com/fwlink/?LinkId=130719

圖 17

除了操作介面上的修補資訊外，建議管理者使用以下三種類型的報表進行漏洞修補評估。

Top Remediations（圖 18）會產生前 25 名風險指數最高的漏洞修補建議提供管理者參考，許多弱點掃描測試的案例中可以發現，許多高風險的漏洞修補後，許多相關的漏洞也一併被解決了。



Top 25 Remediations by Risk

June 28, 2015 13:10:19 GMT

Demo

Applying
25
Top Remediations

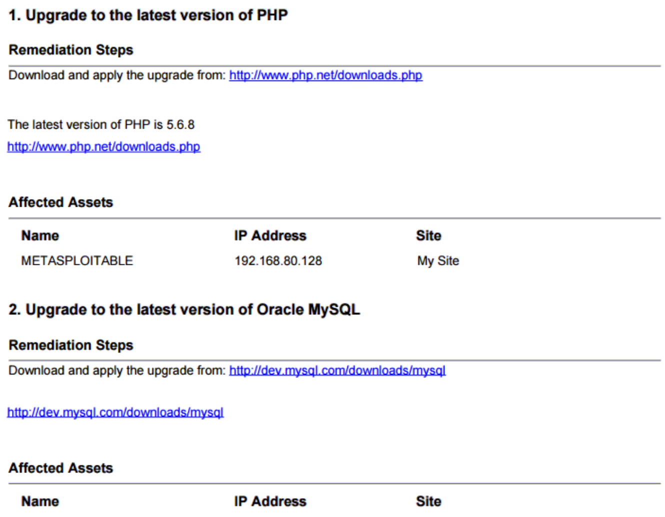
Will Remediate
67%
Vulnerabilities
including:
74% published exploits
0% available malware kits

Affecting
2
Assets

Remediations	Remediated Vulns		☣	Affected Assets	Risk
Upgrade to the latest version of PHP	69	13	0	1	57206
Upgrade to the latest version of Oracle MySQL	42	2	0	1	20025
Upgrade libxml2 for Ubuntu 8.04 LTS	12	1	0	1	11434
Upgrade samba for Ubuntu 8.04 LTS	8	7	0	1	9460
Upgrade php5-cgi for Ubuntu 8.04 LTS	7	33	0	1	8753
Upgrade postgresql-8.3 for Ubuntu 8.04 LTS	10	3	0	1	7756
Upgrade ISC BIND to latest version	10	0	0	1	7531
Upgrade php5-cli for Ubuntu 8.04 LTS	6	28	0	1	7487

圖 18

「Top Remediations with Details」在報告中增加了「Top Remediations」的修補細節，如圖 19 所示，包含漏洞修補的檔案下載連結。但是所提供的詳細資料量大，若是產生報表的主機數較多，需評估是否使用此類型的報表。



1. Upgrade to the latest version of PHP

Remediation Steps

Download and apply the upgrade from: http://www.php.net/downloads.php

The latest version of PHP is 5.6.8
http://www.php.net/downloads.php

Affected Assets

Name	IP Address	Site
METASPLOITABLE	192.168.80.128	My Site

2. Upgrade to the latest version of Oracle MySQL

Remediation Steps

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql

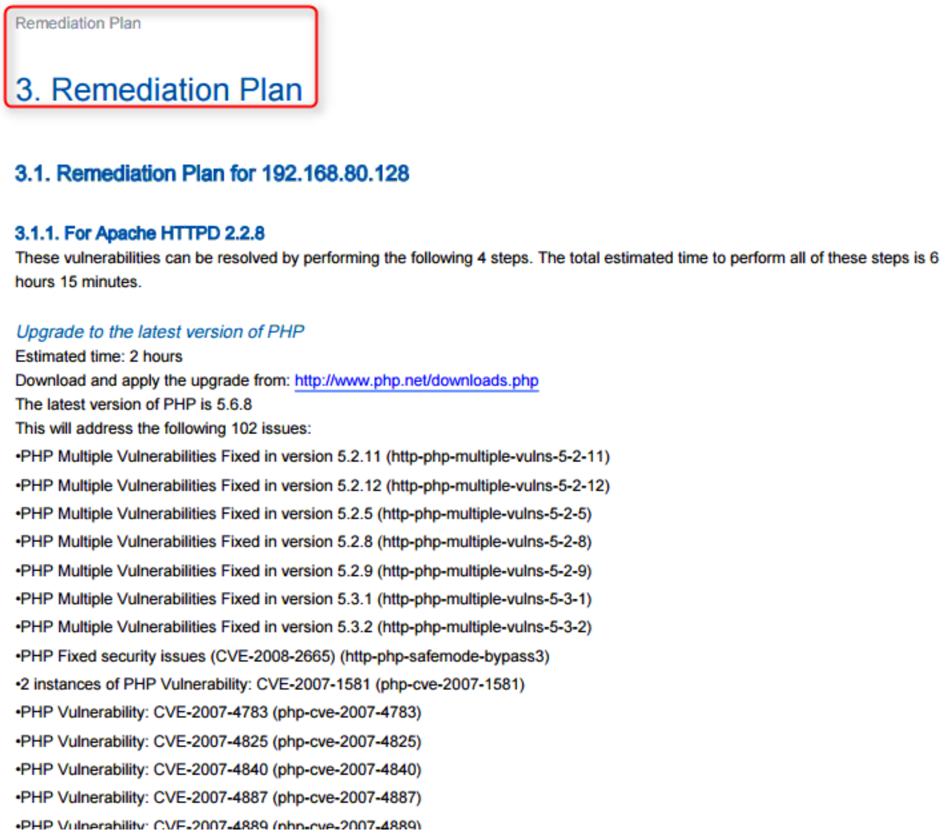
http://dev.mysql.com/downloads/mysql

Affected Assets

Name	IP Address	Site

圖 19

「Remediation Plan」可將漏洞與修補訊息一併整理成評估報表，如圖 20 所示。



Remediation Plan

3. Remediation Plan

3.1. Remediation Plan for 192.168.80.128

3.1.1. For Apache HTTPD 2.2.8

These vulnerabilities can be resolved by performing the following 4 steps. The total estimated time to perform all of these steps is 6 hours 15 minutes.

Upgrade to the latest version of PHP

Estimated time: 2 hours

Download and apply the upgrade from: http://www.php.net/downloads.php

The latest version of PHP is 5.6.8

This will address the following 102 issues:

•PHP Multiple Vulnerabilities Fixed in version 5.2.11 (http-php-multiple-vulns-5-2-11)

•PHP Multiple Vulnerabilities Fixed in version 5.2.12 (http-php-multiple-vulns-5-2-12)

•PHP Multiple Vulnerabilities Fixed in version 5.2.5 (http-php-multiple-vulns-5-2-5)

•PHP Multiple Vulnerabilities Fixed in version 5.2.8 (http-php-multiple-vulns-5-2-8)

•PHP Multiple Vulnerabilities Fixed in version 5.2.9 (http-php-multiple-vulns-5-2-9)

•PHP Multiple Vulnerabilities Fixed in version 5.3.1 (http-php-multiple-vulns-5-3-1)

•PHP Multiple Vulnerabilities Fixed in version 5.3.2 (http-php-multiple-vulns-5-3-2)

•PHP Fixed security issues (CVE-2008-2665) (http-php-safemode-bypass3)

•2 instances of PHP Vulnerability: CVE-2007-1581 (php-cve-2007-1581)

•PHP Vulnerability: CVE-2007-4783 (php-cve-2007-4783)

•PHP Vulnerability: CVE-2007-4825 (php-cve-2007-4825)

•PHP Vulnerability: CVE-2007-4840 (php-cve-2007-4840)

•PHP Vulnerability: CVE-2007-4887 (php-cve-2007-4887)

•PHP Vulnerability: CVE-2007-4889 (php-cve-2007-4889)

圖 20

結論

弱點掃描工具可以提供管理者漏洞的資訊，但仍須仰賴管理者修補漏洞才有實質的效益。漏洞的修補無法一勞永逸，設備的更新與漏洞的發布日新月異，建議管理者在修補漏洞完畢後，仍須定期執行弱點掃描與修補，才能發揮弱點掃描的最大效果。

參考資料

1. 資安人。RAPID7 弱點管理 NEXPOSE。網址：http://www.informationsecurity.com.tw/product/product_detail.aspx?pid=6145。上網日期：2015-06-29。

2. 夏克強。2008 年 5 月發行。弱點掃描技術與策略。麟瑞科技電子報。網址：http://www.ringline.com.tw/epaper/Forum970502.htm。上網日期：2015-06-29。