经间 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 □專題葬	服導	
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 繁,不論是個人或是企業,都更加重視自 防護。而資訊安全防護,除了大家所熟悉 及入侵偵測防禦系統等,弱點掃描技術也 一。	的惡意活動 目身在網路 影的防火牆 2是資安的	愈來愈頻 世界的安全 、防毒軟體 重要技術之
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,

Computer and Information Networking Center (C&INC) of National Taiwan University (NTU) 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

Computer and Information Networking Center (C&INC) of National Taiwan University (NTU) 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。

www.rapid7.com/products/nexpose/compare-downloads.jsp



@
 @
 @
 @
 @
 @
 @
 @
 #
 @
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #

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。

		A - •
	20.27004 - 1.1.1	
← → C x https://192.168.80.1	30:3780/login.html	
Nexpose [®]		
	Log on User name nxadmin Password 	
		RAP

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。

V Mexpose Seco									
← → C	🖹 😹 🕅 😵 🕅 🖹	3 0.130: 3780/hor	ne.jsp						
🔉 nexpose"	Assets	Vulnerabilities	Policies	Reports	Tickets	Administ	ration		
Home	1								
Risk and Assets	SOver ime View by	site or asset group	Q						
	= 500k								
	₩ 450k								
	₩ ₩ 4001r								
	2 400k								
	350k								
	_==	15 14.00 10	l taux av		8		05 14-		20.4
		TO MAY TO	. Ivialy 20	. way	22. May	24. WHAY	20.1918)	20. May	30. I
Assets	Risk Score			Hi	ighest-risk S	ite			
2	311,499				My Site				
(was 2)	🔺 (was 311,165)			🔺 311	,499 (was 3	11,165)			
Sites									
Name							1	Assets	Vulnerat
My Site								2	
Metasploit- roje	ectB-1433994108							2	
нк 🚩								0	
SG								0	
Create site									

Computer and Information Networking Center (C&INC) of National Taiwan University (NTU) 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。



圖 4

「ORGANIZATION」頁籤填寫組織資訊,將顯示在輸出的報表上。

🕅 nexpose 🖌 👫	Assets Vulnerabi	ilities Policies Re	eports Tickets	Administration		🔎 ? nxadmin 🔻
Assets Sites New Site	e Configuration					🖓 Search 🔍
Site Configura	tion				SAVE & SCA	AN SAVE CANCEL
() INFO & SECURITY	ASSETS	AUTHENTICATION	() TEMPLATES	ENGINES	⊘ ALERTS	SCHEDULE
GENERAL	Organiz	ation 🕜				
ORGANIZATION		organization Name				
	F	Primary Contact				
	E	lob Title E-mail				
	T	elephone Business Address				
	c	City Country		¥		
	s	State/Province				

企业 前 臺灣大學計算機及資訊網路中心

1

Computer and Information Networking Center (C&INC) of National Taiwan University (NTU) 「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。

шБ'	生日日生川	1-1-74						
nexpo	ose 🕺 👫 Ass	ets Vulnerabilities	Policies Report	s Tickets Admi	nistration		?	nxadmin ▼
Assets	Sites New Site	Configuration					Search	, <u>a</u>
Site	Configuratio	n				SAVE	& SCAN SAVE	CANCEL
	() INFO & SECURITY	ASSETS		TEMPLATES	ENGINES	(2) ALERTS	E SCHEDULE	
	GENERAL	Access	ø					
	ORGANIZATION	Site A	cess (0 selected)			Filt	er Q	
	ACCESS	Use	Name	Full Name		User Role		
		Davi	d	d		system-admin		
		□ HK_	admin	hk admin		site-admin		
		micl	nael	michael		site-admin		
		SG_i	admin	SG		site-admin		
				। ष्रा ८				

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。

Nexpose Security Console	• × 🗖					
← → C 🕑 https://	/192.168.80.130:37	80/scan/config.jsp#/	scanconfig/asset			Q Б ☆ 🗕
🕅 nexpose 👘	Assets Vulnerabi	lities Policies R	eports Tickets	Administration		🔎 ? nxadmin 🔻
Assets Sites New Si	te Configuration					Search Q
Site Configura	ation				SAVE	& SCAN SAVE CANCEL
0	Ē		502 102	₽	\bigtriangledown	
INFO & SECURITY	ASSETS	AUTHENTICATION	TEMPLATES	ENGINES	G ALERTS	SCHEDULE
Specify assets by If you enter a dupl entered range, it b INCLUDE 2 Assets [] [] 192.168.8 0 Asset Grou	Names/Addresses (icate host name or an IF ecomes part of that rany 對揮檔案 未選檔案 0.128 - 192.168.80.129 ps	connection address within a range re. x Enter name, address	that was already enter 2 ess, or range.	ed, it is not includ	 If you add an IP address EXCLUDE Assets 321 Enter name, Asset Groups 	ess that extends an × 0 assets ♥ 權權案]未證檔案 address, or range.
Enter an a	sset group name.				Enter an ass	set group name.
_			_	-	-	RAPID

CMIC 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)

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。

5					(
INFO & SECURITY	ASSETS	AUTHENTICATION	() TEMPLATES	ENGINES	(2) ALERTS	SCHEDULE
MANAGE	Add	d Credentials			CREAT	E CANCEL
ADD CREDENTIAL	S	Service 🕡	Microsoft Windo	¥		
Account Restrictions		Domain User Name				
ADD WEB AUTHENTICATION		Password Confirm Password				
		Test Credentials 👩				>
			CREATE CAN	CEL		

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。

e Configurat	Ion					SAVE &	SCAN SAV	E CANO
() INFO & SECURITY	ASSETS A		CONTRACTOR	ENGINES	3	() ALERTS	SCH	iii Hedule
SELECT SCAN TEMPLATE	Selected Sca	n Template: Full aud	lit					
CREATE SCAN TEMPLATE	Scan Temp Name DISA DISA Discover	acrivice y Scan y Scan - Addressive		Asset Discov ICMP, TCP ICMP, TCP, U ICMP, TCP, U	Service Disc. Service Disc. Custom TCP, Custom TCP, Custom TCP,	 Checks Checks Safe 0 Disabled Disabled 	Filter So Cop	Q y
	Exhaust FDCC Full aud Full aud	t		ICMP, TCP, U ICMP, TCP ICMP, TCP, U	Full TCP, Def. Custom TCP Default TCP,	Safe 0 Safe 0 Custom	8 8 8	
	 Full aud Full aud HIPAA c Internet 	t without Web Spide ompliance DMZ audit	r All Ports	ICMP, TCP, U ICMP, TCP, U ICMP, TCP, U Disabled	Default TCP, Full Default TCP, Default TCP	. Custom Custom . Safe 0 Custom	* % *	-

Celline 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) 「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。

	Configuration 2					Search
e Configuratio	on				SAVE & SO	CAN SAVE CANC
() INFO & SECURITY	assets	AUTHENTICATION	() TEMPLATES	ENGINES	(2) ALERTS	CHEDULE
MANAGE SCHEDULES	Set Sca	n Time 🥥				
CREATE SCHEDULE	Enable s	chedule				
MANAGE BLACKOUTS	Start dat	e and time	06/26/2015 HH MM	à <i>h</i> ∆ ▼	(CMT ±08:00) R	iiina Phona 🔻
CREATE BLACKOUT	Scan Ter	nplate	Full audit			¥
	Maximur	n scan duration	₩ee	ks 🔤 🖍 Days 🛛	✓ Hours	✓ Minutes
	🗷 Repea	t scan every	1	davs	¥	
	lf a scan duration	reaches the maximum	restart the so	an from the beginning		T
			SAV	E CANC	EL	

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。

ssets 🔿 Sit	es > NX_byRonald > Sca	ns > Full audit 🔌								Search	
Scan Progre	ess Ø										• :
Scan Type	Started	Assets	Vulnerabilities	ies Elapsed Assets Scanned						Scan Engine	Scan Log
Manual	2015/6/26 上午10:01:27	0	0	3 secor	ds A	Asset dis ctive: 0, Pending:	rv is in proare: omplete: 0	3S	Local scan engine		
Stop Scan	Pause scan										
Scan Engine	es Status										•
Scan Engin	e		A	ddress			87	Port		Engine Sca Status	m
Local scan	engine		1:	27.0.0.1				40814		In Progres	3
😌 Showing	1 to 1 of 1 🚔 Export to C	SV						Rows pe	erpage: 10 🔻	14 4 1	of 1 🕨
Completed /	Assets 😡										•
Address	U Name	Operating S	lystem	Vulnerabilities Scan Duration		Sca	n Status	Scan Eng	ine		
There are n	o completed assets.										
🖲 Showing	0 to 0 of 0 \mid 🚔 Export to C	SV						Rowspe	erpage: 1C 🔻	0	of 0 🕨 🖻
ncomplete	Assets 😡										•
Address		U Name			Operating Sy	/stem	Vuli	nerabilities	Scan Duration	Scan Statu	IS
There are n	o incomplete assets.										_
Chowing	0 to 0 of 0 Export to C	SV						Rowspe	erpage: 1C 🔻	0 + + +	of 0 + H

歐洲 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)

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。

🔉 nexpose	👫 Assets Vu	Inerabilities Policie	es Reports	Tick	ets	Admii	nistratio	n			୍ବ	∅ ?	nxadmin 🔻
Assets Sites 1	/ly Site										[🗣 Searc	h
Site Scan Summary	,												* >
Defined Assets	Active Assets	Inactive Assets	Vulnerabilitie	s	Last	Scann	ed				Next Scan		
	2	2 0)	351	2015	5/6/24	下午11:25	5:22			2015/6/28下子	F1:00:00	
Manage site Cre	ate site report View	w scan history											
Trends Risk and A	ssets Over Ti 👻		• x	Ass	ets by	/Risk a	and Vulne	erabili	ties	0			▼ x
≡ 500k			- 5		≡	400 —							
₩ 450k					lities							•	
8			- 4 &		erabi	200 -							
2 400k			, sets		Vuln								
350k													
8			2 2			0 📍	50.00	0 100	nnn	150.0	00 200 000 250 00	ທ 300 ບເສ	0.000
	25. May	8. Jun 22. Jur	n				00,00		,000	100,0	Risk Score	0 000,044	0,000
Current Scans													• >
			There are r	no scan:	s to di	isplay.							
Scan Now													
Assets													- 1
View details about a	ssets, including those	no longer active. To def	lete an asset. s	elect a r	row. T	o delete	e all disp	laved	asse	ts. se	lect the top row an	d use Sele	ct Visible.
Cancel all selections	s using Clear All. Lean	n more.											
Delete assets Re	move asset from site	3	_					_			Tota	I Assets S	elected: 0 of 2
□ • Address		Name	OS					45	2 ²	D.	Vulnerabilities	Risk	Last Scan 🎚
192.168.80.12	9	PC-D9C81FC7B59A	Mic	rosoft W	√indov	vs XP			0	11	10	6,419	Fri Jun 26 2015
192.168.80.12	8	METASPLOITABLE	Ubu	intu Lini	ux 8.0	4			0	147	341	305,081	Wed Jun 24 2015
Showing 1 to 2 of 2	🛛 🔤 Export to CSV									Ro	ws 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。

Assets Sites 192.168.80.128		Search	
ADDRESSE 192.168.80.128 S	OS	∆ Ubuntu Linux 8.04	
HARDWAR 00:0C:29:85:51:9A E	CPE	cpe:/o:canonical:ubuntu_linux:8.04:::lts	
ALIASES METASPLOITABLE	LAST SCAN	Jun 28, 2015 5:07:43 AM (19 hours ago)	
HOST 🛃 Virtual machine TYPE	NEXT SCAN	Jul 5, 2015 5:00:00 AM	
SITE Global			
RISK SCORE		USER-ADDED TAGS 🔍	
original 152,611	CUSTOM TAGS None	DWNERS None	4
CONTEXT-DRIVEN 305,223	LOCATIONS Taipei x	CRITICALITY Very High x	Ati
Scan asset now Create asset report Delete asset			
Trends Risk Over Time -			•
≡ 306k			
80 305k			
303k			
11. May 18. May	25. May 1. Jun	8. Jun 15. Jun 22. Jun 29. Jun	

《》「「《 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) 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。

/uini	erabilities									•
iew	details about discovered vulnerabilities. To use one of the e	xceptio	n contr	ols on a	vulnerabilit	/, select a row. To us	e the control witi	n all displaye	d displayed vul	nerabilities,
Even	the top row and use select visible. Cancel all selections u	oloitak	lear All.	. ⊌ Islidated	with Motor	oloit x Exploit public	and & Validator	l with publich	ed evoloit	
Excl	ude Recall Resubmit	ipiortai	ле 40 и	aiuateu	with Hetas	рок 🔬 Ехрок рабія		Total \	ulnerabilities (Selected: 0 of 34
	Title	#	13 1 1	cvss	Risk	Published On	Modified On	Severity	Instances	Exceptions
	'rsh' Remote Shell Service Enabled		۵	7.5	750	Fri Jan 01 1999	Wed Dec 04 2013	Critical	1	O Exclude
0	USN-1259-1: Apache vulnerabilities		۵	5	511	Wed Oct 05 2011	Fri Feb 13 2015	Severe	1	O Exclude
	Tomcat Application Manager Tomcat Tomcat Password Vulnerability		۵	10	824	Mon Nov 09 2009	Fri Feb 13 2015	Critical	1	Ø Exclude
	USN-1789-1: PostgreSQL vulnerabilities		۵	8.5	398	Thu Apr 04 2013	Thu Jun 05 2014	Critical	1	O Exclude
	USN-1397-1: MySQL vulnerabilities		۵	8.5	665	Mon Jul 13 2009	Fri Feb 13 2015	Critical	1	Ø Exclude
0	USN-897-1: MySQL vulnerabilities		۵	8.5	665	Mon Jul 13 2009	Fri Feb 13 2015	Critical	1	Ø Exclude
	USN-1199-1: Apache vulnerability		۵	7.8	299	Mon Aug 29 2011	Fri Feb 13 2015	Critical	1	Ø Exclude
	USN-1437-1: PHP vulnerability		۵	7.5	633	Fri May 11 2012	Fri Feb 13 2015	Critical	1	O Exclude
	USN-1358-1: PHP vulnerabilities		۵	7.5	639	Fri Feb 10 2012	Fri Feb 13 2015	Critical	1	Exclude
0	USN-951-1: Samba vulnerability		۵	7.5	672	Thu Jun 17 2010	Fri Feb 13 2015	Critical	1	O Exclude

圖 14

《》 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) 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。



@
 @
 @
 @
 @
 @
 @
 @
 @
 @
 @
 #
 @
 #
 @
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #

Γ Vie	w reports」頁籤可查	后看產出報表的清單。	0	
🔉 nexpose	👫 Assets Vulnerabilities Policies	Reports Tickets Administration	1	nxadmin 🔻
Reports			E	Search Q
	Create a report	View reports	Manage report templates	
	New	Find reports Q	Rows 10 1 - 7 of 7	
	Report Name		Most Recent Report*	
	🔁 Demo		2015/6/28 9:09 PM	
	🖀 Metasploit Export ProjectB-143399	34108	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	

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。

	uldress				Name	05		₩.	ы	Vulnerabil	ties R	liek	Last Scar
	92.168.80.129				PC-D9C81FC7B59/	Microsoft Window	ws XP	0	11		10	6,420) Sun Jun 2
1	92.168.80.128				METASPLOITABLE	Ubuntu Linux 8.0	04	0	147		343	306,115	Sun May 3
nowing	1 to 2 of 2 🔤	Export to (osv						R	ows per pag	e: 10 🔻	14 4	1 of 1
	_												
/ulner:	abilities												
/iew.du	atails about discovere	ed vulnerat	bilities	To use o	ne of the exception (ontrols on a vulnerab	ility, select	a row. T	o use tr	e control wit	h all displa	ved dis	played vulne
electt	he top rov <mark>nd use S</mark>	elect Visit	ole. Ca	incel all se	elections using Clea	ir All. 🔞	,					,	
Expos	sures: 👌 Buscepti	ble to ma	lware	attacks 🕻	🗿 Metasploit-explo	itable 🐞 Validated w	/ith Metas	ploit 🔬	Exploit	published δ	😈 Validate	d with p	oublished ex
Exclu	de Rac Resu	bmit									Total Vu	Inerabil	ities Selecte
- .	Title	₩ 1	51	CVSS	Risk I	Published On	Modifie	d On	5	everity	Instances		Exceptions
1	MS08-067:) ×	•										
	Vulnerability in Server Service Could Allow		۵	10	841	Thu Oct 23 2008	Fri Feb	13 2015		Critical		2	🖉 Exclude
l	Remote Code Execution (958644)												
	MS09-001:												
	SMB Could All pw		m	10	939	Tue Jan 13 2009	Eri Foh	13 2015		Critical		2	O Evolution
	Remote Code Execution (958687)		Ť		000	10000011012000		10 2010				-	United and
	MS10-012:												
_	SMB Server C d			10	010	Tue Eeb 00 2010	Thus I are	10.004		Self-cal		2	O Contrad
	Allow Remote		æ	10	019	Tue Feb 09 2010	Thu Apr	10 2014	۱ ۰	znocar		2	S Excino
	(971468)												
olution													
Micr	asoft blindows Server	12003 SP	2089	P1 688)	Microsoft Windows	Server 2003, Standard	Edition SI	P2 0 R S	P1 696	MicrosoftV	Vindows Si	enser 20	03 Enternri
SP2	OR SP1 (x86), Micros	soft Windo	ws Se	rver 2003,	Datacenter Edition	SP2 OR SP1 (#86), Mi	crosoft Wir	ndows S	erver 20	03, Web Ed	tion SP2 0	R SP1 (x86), Micros
Wind	dows Small Business 8-067: Security Updai	s Server 21 te for Wind	003 SF Jows S	P2 OR SP1 Server 200	1 (x86) 13 (KB958644)								
Dow	mload and apply the p	patch from	c http://	go.micros	off.com/fwlink/?Link	dd=130719							
Micro	osoft Windows Server	r 2008 SP	1 () a64), Microso	t Windows Server 2	008 Enterprise Editio	n SP1 (ia6	4), Micro	softWin	dows Serve	r 2008 Star	idard E	sition SP1 (i
Micri (iaß)	asoft Windows Server	r 2008 Dat Server 20	tacente	er Edition	SP1 (ia64), Microsof (on SP1 (ia64), Micro	t Windows Server 200	8 HPC Ed	ition SP1 Server 21	(ia64),	Microsoft Wi (ia64) Micr	indows Ser	ver 200	8 Web Editi Servial Busi
Serv	er 2008 SP1 (ia64)	s oenier 20	106 01	urage Eur	1011 SF1 (1894), MICH	osul vanouvs sinain	ousiness i	activel 21	00 ar 1	(1004), MICI	oson (mina)	0W5 E5:	sermar busi
MSO	8-067: Security Upda	te for Wind	tows S	Server 200	I8 for Itanium-based	Systems (KB958644))						
Dow	nload and apply the p	patch from	c http://	(go.micros	soft.com//wiink/?Link	dd=130719							
Micri (x86) 2001	osoft Windows Server osoft Windows Server), Microsoft Windows 3 SP1 (x36)	r 2008 SP r 2008 Dat Server 20	1 (x86) tacenti 08 Sto	i, Microsof er Edition rage Editi	t Windows Server 21 SP1 (x86), Microsoft on SP1 (x86), Micros	008 Enterprise Edition Windows Server 2008 off Windows Small Bu	SP1 (x86) 3 HPC Edit Jsiness Se	, Microso ion SP1 erver 200	ift Wind (x86), M 8 SP1 (ows Server 2 icrosoft Wini x86), Microsi	2008 Stand dows Serve oft Window	ard Edit er 2008 s Esser	ion SP1 (x8 Web Edition htial Busine
MSO	8-067: Security Upda	te for Wind	iows S	Server 200	18 (KB958644)								
Dow	nload and apply the g	patch from	c http://	(go.micros	soft.com//wink/?Link	dd=130719							
Micre	osoft Windows Vista	< SP1 OR	SP1 ((86_64), N	licrosoft Windows Vi	ista Home, Basic Editi n < 9P1 OP PP4 6-02	ion < SP1 (OR SP1	x86_64), Microsoft V	Vindows Vi	sta Hor	ne, Basic N
OD1	OLCOL: 1 (100-04), MI	Enternrice	Editio	n < SP1 C	R SP1 (x86_64), Mi	crosoft Windows Vista	Business	Edition	< SP1 0	R SP1 086_	64), Micros	soft Win	dows Vista
SP1 Micro N Ec MS0	osoft Windows Vista & Jition < SP1 OR SP1 (8-067: Security Upda)	¢86_64), f te for Wind	Micros Sows V	oft Windov /ista for x6	ws Vista Starter Editi 4-based Systems (1	ion < SP1 OR SP1 (x8) (8958644)	6_64)						
SP1 Micro N Ec MS0	osoft Windows Vista I Jition < SP1 OR SP1 (8-067: Security Upda micad and apply the c	¢86_64), 1 te for Wind patch from	Micros Sows V c http://	oft Windov Asta for x6 Ago.micros	ws Vista Starter Edit i4-based Systems () soft.com/fwlink/?Link	ion < SP1 OR SP1 (x8) (8958644) dd=130719	6_64)						
SP1 Micro N Eco MS0 Dow	osoft Windows Vista B dition < SP1 OR SP1 (8-067: Security Updai miload and apply the p osoft Windows Server	¢x86_64), f te for Wind patch from r 2003 SP:	Micros Sows V c http:// 2 OR S	oft Windov Asta for x6 (go.micros 3P1 (ia64)	ws Vista Starter Edit i4-based Systems () soft.com/fwlink/?Link , Microsoft Windows	on < SP1 OR SP1 (x8) (B958644) (d=130719 : Server 2003, Slandar	6_64) d Edition S	P2 OR 1	3P1 (ja6	4), Microsof	Windows	Server 2	003, Entern
SP1 Mich N Ec MS0 Dow Mich Editi Mich MS0	osoft Windows Vista I Jillion < SP1 OR SP1 (8-067: Security Updal mload and apply the p osoft Windows Server on SP2 OR SP1 (a64 osoft Windows Small 8-067: Security Undal	ck86_64), f te for Winc patch from r 2003 SP: 4), Microso I Business te for Winc	Micros Jows V c http:// 2 OR S off Win/ Serve Jows S	oft Windov Asta for x6 (go.micros SP1 (ia64) dows Serv r 2003 SP Server 200	ws Vista Starter Edit 4-based Systems () soft.com/fwlink/?Link , Microsoft Windows ver 2003, Datacenter 20 OR SP1 (ia64) 3 for Itanium-based	ion < SP1 OR SP1 (x8) (8958644) (d=130719 : Server 2003, Standar : Edition SP2 OR SP1 Systems (KB958644)	6_64) d Edition S (ia64), Mic	IP2 OR 1	SP1 (ia6 indows	4), Microsof Server 2003	Windows ;	Server 2 on SP2	003, Enterp OR SP1 (jai

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 Remediat Demo Applying 25 Top Remediations	will	Remediate 67% Inerabilities including:	•	Jun	e 28, 2015 13 Affec	:10:19 GM :ting 2 ets
	74% published exploits	<u>∲</u> 0	% ^{availab} malwai	ile re kits		
Remediations		Remediated Vulns	4	€	Affected Assets	Risk
Upgrade to the latest versi	on of PHP	69	13	0	1	57206
Upgrade to the latest versi	on of Oracle MySQL	42	2	0	1	20025
Upgrade libxml2 for Ubunt	u 8.04 LTS	12	1	0	1	11434
Upgrade samba for Ubuntu	18.04 LTS	8	7	0	1	9460
Upgrade php5-cgi for Ubur	ntu 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 lates	t version	10	0	0	1	7531
Upgrade php5-cli for Ubun	tu 8.04 LTS	6 토 10	28	0	1	7487

「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。

	Version of FITF		
Remediation Steps			
Download and apply the upgra	de from: http://www.php.net/down	loads.php	
The latest version of PHP is 5.6	3.8		
http://www.php.pet/downloads	oho		
napariti pripri de de midade.	<u>kuk</u>		
Affected Assets			
Name		Pite	
Name	IP Address	Site	
METASPLOITABLE	192.168.80.128	Mv Site	
		,	
2. Upgrade to the latest	version of Oracle MySQL	,	
2. Upgrade to the latest Remediation Steps	version of Oracle MySQL	,	
2. Upgrade to the latest Remediation Steps Download and apply the upgra	version of Oracle MySQL	mloads/mysql	
2. Upgrade to the latest Remediation Steps Download and apply the upgra http://dev.mysql.com/download	version of Oracle MySQL de from: <u>http://dev.mysql.com/dov</u> s/mysql	mloads/mysql	
2. Upgrade to the latest Remediation Steps Download and apply the upgra http://dev.mysql.com/download Affected Assets	version of Oracle MySQL de from: http://dev.mysql.com/dox s/mysql	mloads/mysql	
2. Upgrade to the latest Remediation Steps Download and apply the upgra http://dev.mysql.com/download Affected Assets Name	version of Oracle MySQL de from: http://dev.mysql.com/dov s/mysql	mloads/mysql Site	

(恐) 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)

「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-cye-2007-4887) •PHP Vulnerability: CVE-2007-4889 (nbn-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

- 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。