

怎樣找到你最需要的 弱點工具



黃繼民 Jim Huang

創泓科技-資深技術顧問

jim@uniforcetech.com.tw

大綱簡介

- 前言
- 為什麼一定要掃描
- 防毒軟體、弱點掃描、滲透測試的差異性
- 我收到了弱掃報告，可是看不懂
- 怎樣找到最合適自己的弱掃工具
- Q&A

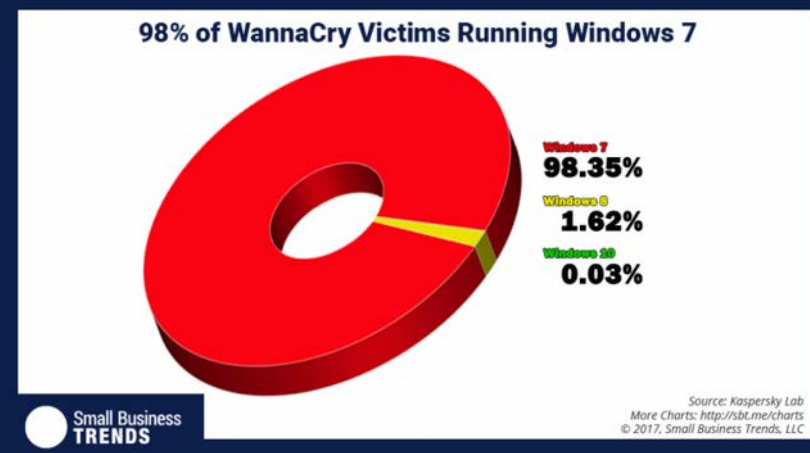
資安弱點武器化

- 美國安全單位NSA 遭到影子搨客組織入侵.
- 影子搨客釋出大量駭客工具於黑市.
- 針對Windows系統弱點的「永恆之藍」造成驚世攻擊WannaCry



永恆之藍 EternalBlue 效應

WannaCry's **EternalBlue** On Windows 10



- 2017年5月 爆發史上影響最大、傳播速度最快的全球性勒索攻擊WannaCry.
- 2017年6月 變種攻擊Petya 及 Not Petya 出現，針對主開機紀錄(MBR)，Win更新無效。
- 2017年6月 SambaCry 現身針對Linux系統設備(Server, NAS, IoT裝置)。
- 2018年 趨勢科技: 駭客利用「永恆之藍」入侵家用網路 台灣受攻擊次數連三週高居全球首位。

網路犯罪地下經濟

- # EternalBlue(永恆之藍)
- # SMB漏洞利用 (SMBv1)
- # Port 445
- # MS17-010
- # 跨平台的威脅
- # 從「勒索」到「奴役」



WannaMine

Wanna Decryptor 2.0

Ooops, your files have been encrypted!

我的電腦出了什麼問題？
您的一些重要文件被我加密保存了。
照片、圖片、文檔、壓縮包、音頻、視頻文件、exe文件等，幾乎所有類型的文件都被加密了，因此不能正常打開。
這和一般文件損壞有本質上的區別。您大可在網上找找恢復文件的方法，我敢保證，沒有我們的解密服務，就算老天爺來了也不能恢復這些文檔。

有沒有恢復這些文檔的方法？
當然有可恢復的方法。只能通過我們的解密服務才能恢復。我以人格擔保，能夠提供安全有效的恢復服務。
但這是收費的，也不能無限期的推遲。
請點擊「Decrypt」按鈕，就可以免費恢復一些文檔。請您放心，我是絕不會騙你的。
但若要恢復全部文檔，需要付款點費用。
是否隨時都可以固定金額付款，就會恢復的嗎，當然不是，推遲付款時間越長對你不利。
最好3天之內付款費用，過了三天費用就會翻倍。
還有，一個禮拜之內未付款，將會永遠恢復不了。
對了，忘了告訴你，對半年以上沒錢付款的窮人，會有活動免費恢復，能否輪

Payment will be raised on
5/15/2017 23:41:55
Time Left
02:23:55:59

Your files will be lost on
5/19/2017 23:41:55
Time Left
06:23:55:59

Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Check Payment Decrypt



SambaCry

WannaCry

可利用弱點持續增長變化

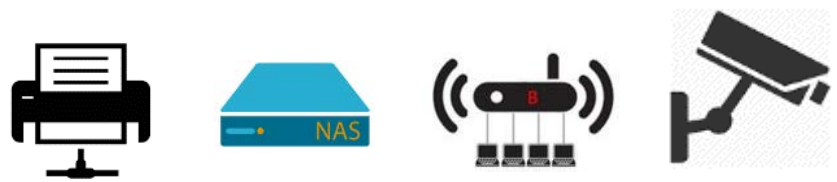


無線加密WPA2弱點揭露 智慧聯網裝置漏洞利用



假設:

1. 受駭裝置不只是“網路印表機”？
2. 同樣的問題是否會發生在其他系統裝置？
3. 是否會被利用作為“跳板攻擊”？
4. 攻擊目標會否針對校務系統及基礎服務？
5. 被視為“攻擊來源”的影響性？



Home Device is Attacker

Country	Percentage	Rank
Taiwan	21%	1
China	14%	2
Indonesia	14%	2
Thailand	11%	3
India	10%	4

資料來源: TREND 趨勢科技

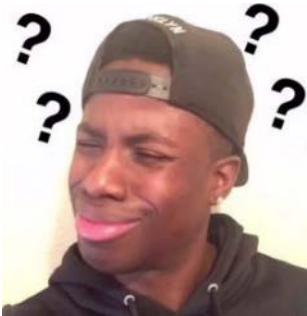
2018年 趨勢科技: 駭客利用「永恆之藍」入侵家用網路
台灣受攻擊次數連三週高居全球首位!

大綱簡介

- 前言
- 為什麼一定要掃描
- 防毒軟體、弱點掃描、滲透測試的差異性
- 我收到了弱掃報告，可是看不懂
- 怎樣找到最合適自己的弱掃工具
- Q&A

為什麼一定要掃描

WHY
NOT



因為害怕

怕多事

怕不懂

怕責罰

自我安慰

不曾出事

已有防護

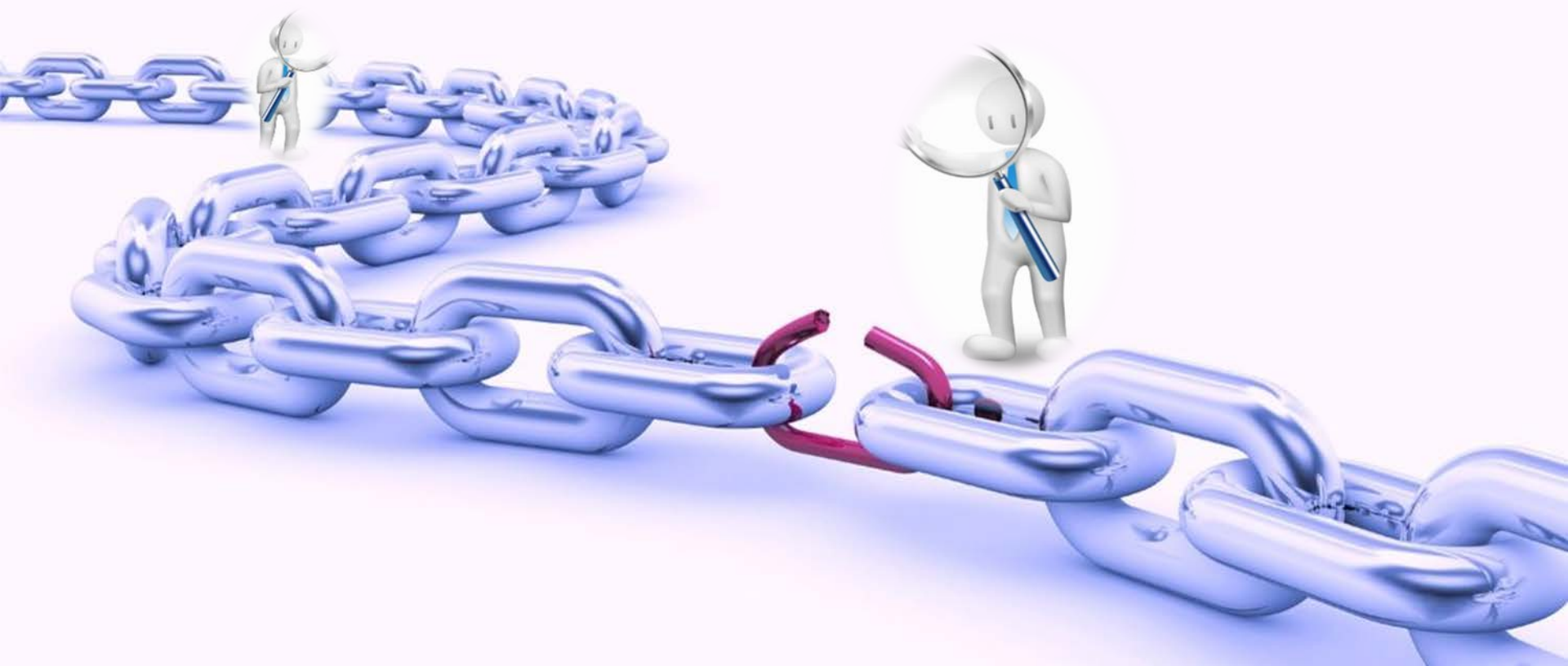
不是目標

已合規範

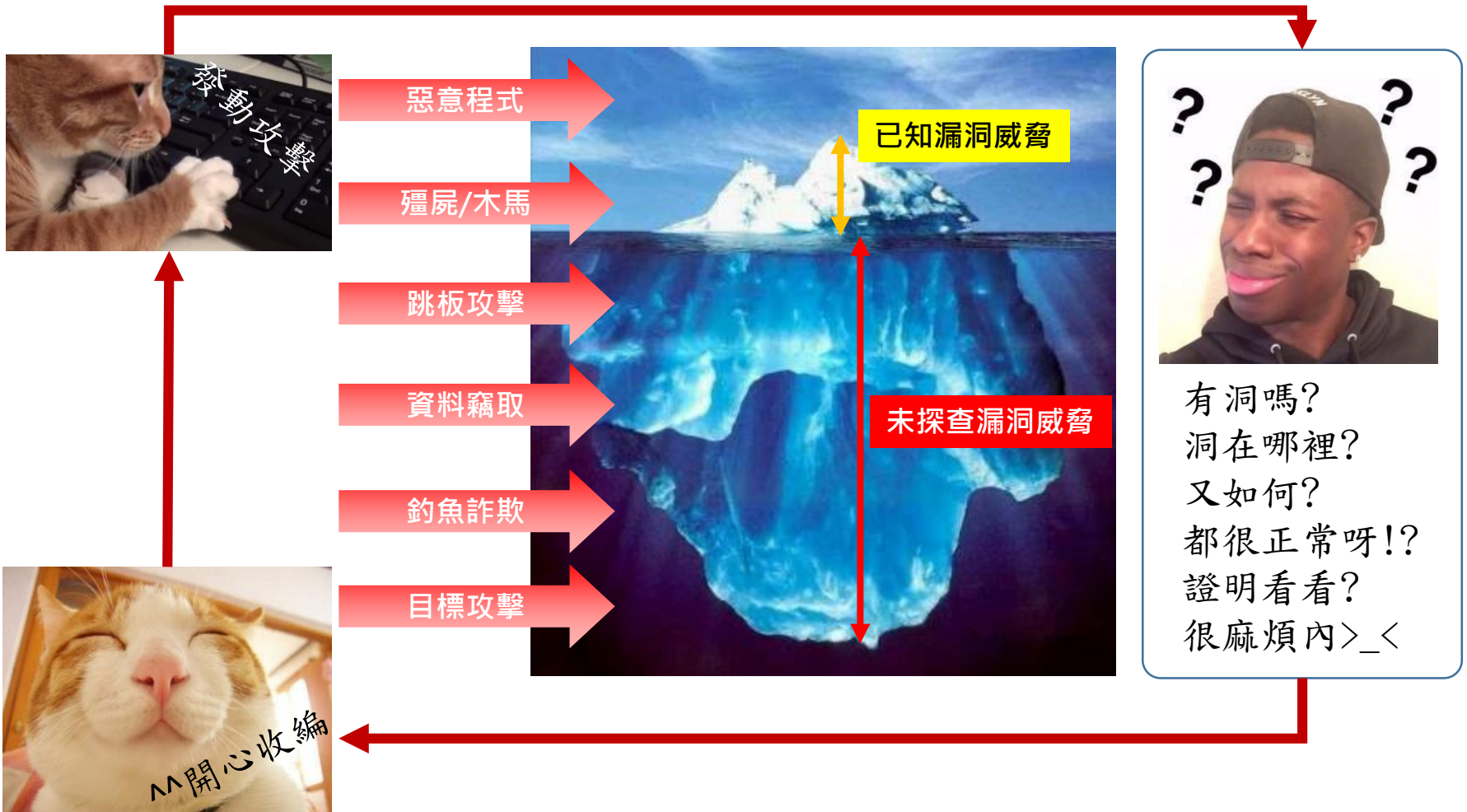
弱點掃描目的

<<<從資安的視角>>>

掌握存在的弱點，提早應對準備，避免風險暴露。



現今資安威脅有高達90%是利用漏洞！！



現今資安攻擊的「起手式」

FireEye Mandiant M-Trend Report 2017



侵入應用程式或OS
的漏洞 (Exploit)

回 Call 控制中心

下載惡意軟體本體

橫向散播

資料竊取



猜猜看，您認識以下哪些弱點？



Zip Slip目錄走訪漏洞



猜猜看，安全設備“安全”嗎？

iThome 新聞 產品評測 技術 專題 AI & Big Data Cloud DevOps GDPR 資安 研討會 社群

思科與Fortinet坦承防火牆漏洞遭「方程式」外流攻擊工具鎖定

駭客組織「影子搭客」釋出自稱源自「方程式」的300MB檔案，當中包括針對防火牆的各種攻擊工具。研究人員發現這些工具開發已有3年之久，而且針對防火牆漏洞進行攻擊是有效的。思科及Fortinet已證實某些工具可任意讀取防火牆檔案。

文 / 蘇嘉穎 | 2016 08 18 發表



TANET 花蓮區域網路中心

You are here: [Home](#) > [105 年公告](#) > [1050901] 【漏洞預警】Cisco與Fortinet防火牆產品存在多個安全漏洞

Main Menu

- 最新訊息公告
- 花蓮區域網路中心簡介
- 網路架構圖

[1050901]【漏洞預警】Cisco與Fortinet防火牆產品存在多個安全漏洞

Last Updated on Tuesday, 28 March 2017 03:12

iThome 新聞 產品評測 技術 專題 AI & Big Data Cloud DevOps GDPR 資安 研討會 社群

Google大爆26個Aruba產品資安問題，Aruba已緊急釋出更新修補漏洞

網路廠商Aruba日前收到Google通報指出，旗下的網路產品存有數十個軟體漏洞與安全瑕疵，包括了無線網路設備作業系統ArubaOS、AirWave管理平臺，以及Instant AP等。Aruba收到通報後不久也緊急發布軟體更新修補漏洞。

文 / 蘇嘉穎 | 2016-05-12 發表



SECLISTS.ORG

Aruba ArubaOS/Aruba Instant/AirWave Management - Multiple Vulnerabilities (CVE-2016-2031, CVE-2016-2032)

TAPT CERT

關於我們 資安情資 資安通報 民眾服務 資安資源



Palo Alto Networks發佈防火牆作業系統安全性更新

修補日期: 2017-12-22 / CVE 編號: CVE-2017-15940 CVE-2017-15942 CVE-2017-15943 CVE-2017-15944

摘要:

- 概況:
Palo Alto Networks 針對其防火牆作業系統 (PAN-OS) 存在數個漏洞，尤其其管理介面端 (server-side request forgery)，駭客已進入管理介面端防火牆操作攻擊並造成網路中斷。攻擊者利用GlobalProtect gateway 端之DOS攻擊，駭客可任意駭取網管功能，釋放PHOSSID cookie 駭取用戶ID。panAuthCheckByPass 駭取網管功能，取得對/ghp 資料庫與/ghp/fully/router.php、/usr/local/bin/gemindex_batch.sh 二個本地端輸入權力，使讓駭客root端執行命令；另駭取網管管理介面亦有RCE功能。Palo Alto 針對各款PAN-OS 提供相關更新。
- 建議:
(1) 建議在管理介面管理端增加防駭取管理功能，讓網管用戶可透過上面指令之字串，登入系統後執行在系統更新。
(2) 在GlobalProtect gateway或API端增加防駭取功能存在一部份，攻擊者必須驗證即可管理介面端。針對Denial of Service攻擊，請在GlobalProtect gateway或防火牆端設定限制。
(3) 建議在本地端駭取管理介面，駭客可management interface 進行管理駭取請求 (server-side request forgery、SSRF) 攻擊，先觀察駭取管理介面以瞭解外部管理，再將駭取管理。

iThome 新聞 產品評測 技術 專題 AI & Big Data Cloud DevOps GDPR 資安 研討會

駭客企圖開採思科ASA漏洞了，快修補！

思科上週才兩度修補自家ASA產品上的安全漏洞，思科的安全情報團隊表示已觀察到瞄準該漏洞的概念性驗證程式，其他安全研究人員也發現相同的情形，請用戶儘快修補。

文 / 陳國洲 | 2018 02 12 發表



Cisco Adaptive Security Appliance Remote Code Execution and Denial of Service Vulnerability

Critical	Advisory ID: cisco-sa-20180128-asa1	CVE-2018-0101	Download CVE/F
	First Published: 2018 January 29 17:00 GMT	CWE-415	Download PDF
	Last Updated: 2018 February 7 16:07 GMT		Email
	Version 2.2: Final		
	Workarounds: No workarounds available		
	Cisco Bug IDs: CSCvg35618		
		CSCvh79732	
		CSCvh81737	
		More...	
	CVSS Score: Base 10.0		

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

弱點已無處不在，所產生的威脅不斷攀升

資料來源: iThome 新聞剪輯

作業系統弱點

微軟修補了45個漏洞，包含5個已被開採的

從本月開始微軟首次採用新的Windows 更新政策，此次更新發布了10個安全公告，共修補45個漏洞，其中包含5個重大安全漏洞，可造成遠端程式攻擊，另外還包括5個已被開採的零日在漏洞。

文/ 陳瑋琦 | 2016-10-12 發表

按讚加入iThome粉絲團

微軟修補由Google揭露的安全漏洞

週二的例行更新中釋出了14個安全公告，涵蓋在 Microsoft Edge、Microsoft Office 辦公室產品、Windows 系統及 Windows 執行程式的龐大安全漏洞，以及由Google所揭露的漏洞。

文/ 陳瑋琦 | 2016-10-12 發表

按讚加入iThome粉絲團

Linux磁碟加密工具Cryptsetup爆重大漏洞

該漏洞存在於使用LUKS統一金鑰設定於Linux版本，LUKS為Linux操作系統標準機制，透過搭配Cryptsetup工具使用，安裝於Linux版本如Debian、SUSE Enterprise Linux、Red Hat Enterprise Linux、Ubuntu及Fedora。

文/ 陳瑋琦 | 2016-11-30 發表

按讚加入iThome粉絲團

重要商務系統弱點

iThome 新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安

甲骨文一次修補276個安全漏洞，寫下新紀

甲骨文上周一口氣修補下84個產品共276個安全漏洞，一舉超過第一季例行修補的248個漏洞，創下甲骨文漏洞修補的紀錄，這波漏洞中共有19個CVSS評分9.8分的重大漏洞，甲骨文呼籲用戶應儘快更新。

文/ 陳瑋琦 | 2016-07-26 發表

按讚加入iThome粉絲團

甲骨文修補308個安全漏洞，創新紀錄!

308個漏洞中有185個可能導致駭客程式攻擊，而123個漏洞存在於Oracle E-Business Suite，設備可能代客客戶層管理、金融管理、人力資源管理、供應鏈管理。

文/ 陳瑋琦 | 2017-05-24 發表

按讚加入iThome粉絲團

DB弱點導致伺服器淪陷

MySQL爆最高權限漏洞，MariaDB、PerconaDB

研究人員揭露了兩個MySQL漏洞分別為重大及高度風險漏洞，最嚴重可讓駭客取得資料庫最高權限，受影響的包含MySQL 5.5.51、MySQL 5.6.32及MySQL 5.7.14及之前的版本，還有基於這些版本的MariaDB與PerconaDB。

文/ 陳瑋琦 | 2016-11-03 發表



資安研究人員Dawid Golunski周二 (11/1) 揭露了兩個攸關MySQL開放資料庫的安全漏洞，將允許駭客取得系統最高權限，同時也殃及了基於MySQL MariaDB與PerconaDB。

相關的漏洞編號分別為CVE-2016-6664與CVE-2016-5617，前者屬重大漏洞，後者則是高度 (High) 風險漏洞，都屬權限擴張漏洞，皆影響MySQL 5.5.51、MySQL 5.6.32及MySQL 5.7.14及之前的版本，以及基於這些版本的MariaDB與PerconaDB。

Java SE重大漏洞

包括Oracle Database、MySQL、Solaris、Java SE Business Edition等，其中包含71個MySQL漏洞。

iThome 新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安 Video 研討會 社群

「黑護士」來襲! 資安業者以一台筆電癱瘓思科與合勤防火牆 (更新: 合勤緊急釋出更新)

資安業者TDC Security Operations Center展示一項名為「黑護士」的攻擊行動。駭客利用CMP發動攻擊，傳送少量CMP Type 3 Code 3，只利用少量流量，就能癱瘓包含思科、合勤、SonicWall及Palo Alto Networks的防火牆。

文/ 陳瑋琦 | 2016-11-14 發表

iThome 新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安 Video 研討會 社群

賽門鐵克防毒軟體爆漏洞，25項企業及消費安全產品可能受駭

由於賽門鐵克旗下多款安全產品採用相同核心引擎，影響到影響的安全產品包含17項企業產品及Symantec及8項消費品牌Norton防毒軟體，包括所有平台的Norton 360、Endpoint Protection、Email Security及Protection Engine等等。賽門鐵克已釋出更新修復漏洞。

文/ 陳瑋琦 | 2016-09-30 發表

IBM Cloud
雲端時代的IT新
選合架構下的
及服務交付線
我要報

iThome
新聞剪輯 iThome 社群

防毒軟體有漏洞已不是新聞。事實上，Google Project Zero就曾在Eset、趨勢科技PC-Cillin、卡巴斯基、FireEye、McAfee等發現有安全漏洞，甚至賽門鐵克自己出了漏洞。

新聞

看電影小心駭客利用惡意字幕接管你的電腦

Check Point發現駭客可利用惡意字幕檔案，結合媒體播放器或串流播放平台的漏洞，自遠端操控使用者的裝置，包含PC、手機或智慧電視，從而竊取裝置上的資訊。

文/ 陳瑋琦 | 2017-05-24 發表

資安系統弱點導致防護破壞

弱點已無處不在，所產生的威脅不斷攀升



OpenSSL Heartbleed 漏洞危機特別報導

政府網站安全未明 資安辦 4月底才能掌握

駭客利用Heartbleed 漏洞入侵VPN 多因素認證防

IT產品Heartbleed災情大清查



OpenSSL又爆1998年就存在的嚴重漏洞，SSL

CVE-2014-0195是屬於「DTLS無效片斷漏洞」，可能讓駭客得以遠端執行任意程式碼，因此被SANS列為重大漏洞。但這次公布的六個漏洞最受關注的是CVE-2014-0224，這項已存在超過15年的「SSL/TLS中間人攻擊漏洞」，可能讓駭客得以用來破解SSL及TLS流量，甚至修改其中內容。

文/ 林妍濤 | 2014-06-06 發表



Cisco及Juniper針對HeartBleed漏洞發布緊急安全通告

面對網路有史以來最嚴重的OpenSSL HeartBleed漏洞，IT廠商皆嚴陣以待，網路設備大廠Cisco及Juniper也雙雙公佈HeartBleed安全漏洞的安全警報。

文/ 林妍濤 | 2014-04-11 發表

Cisco表示，Cisco Registered Envelope Service (CRES) 及網路會議服務Webex Messenger Service已首先獲得修復，且其代管服務皆未受到影響。目前還在調查中的產品包括Cisco IOS、安全產品Identity Service Engine、Secure Access Control Server、Cloud Web Security、Catalyst 6500 Series 及7600 Series Firewall Services等，而Cisco也會持續更新評估狀況，一旦有修補程式也會立即發佈通知。

另一家網路設備大廠Juniper也發佈安全公告，列出受HeartBleed漏洞威脅的產品，包括作業系統 Junos OS 13.3R1、安全存取的用户端軟體Odyssey client 5.6r5以上、數個版本的Web存取軟體Network Connect (windows版本) 等，與SSL VPN連網產品Juniper SSL VPN (IVEOS) 7.4r1、SSL VPN (IVEOS) 8.0r1、以及桌面與行動終端軟體Junos Pulse (Android及iOS版本)等。其中有些已獲得修補。

弱點已無處不在，所產生的威脅不斷攀升

iThome 新聞 產品評測 CIO 技術 專題 專欄 主題頻道 研討會 社群

Unix /Linux 的Bash Shell 出現重大漏洞，危險等級可能超越Heartbleed

Errata Security執行長表示，Shell Shock漏洞可能與Heartbleed一樣嚴重，原因之一為大量的軟體與Bash Shell互動，如同大量的產品使用內含Heartbleed漏洞的OpenSSL一樣，因此根本無法估計可能受影響的軟體數量。

文/ 陳曉莉 | 2014-09-25 發表

讚 1.1萬 按讚加入iThome粉絲團 分享 3,345 8+1 98

iThome 新聞 產品評測 CIO 技術 專題 專欄 主題頻道 研討會 社群

資安

Bash驚爆Shellshock漏洞，全球半數網站伺服器陷危機

近日，國外爆出嚴重的資安漏洞危機，多家資安網站及Linux廠商發出警告，一個名為Shellshock漏洞，可能導致使用 Bash Shell的作業系統，包括Linux、Unix為基礎的平臺、Mac OS X系統等成為駭客遠端入侵的工具，甚至使得全球超過半數網站伺服器，皆可能身陷危機之中。

文/ 余至浩 | 2014-09-26 發表

讚 7,706 按讚加入iThome粉絲團 分享 1,128 8+1 18

iThome

新聞

羅馬尼亞駭客利用Shellshock漏洞入侵雅虎，不小心打中Web log 漏洞

羅馬尼亞駭客試圖利用Shellshock漏洞在Unix主機上建立傀儡網路，並用以入侵雅虎伺服器。原先雅虎以為是主機有Shellshock漏洞而遭受攻擊，雅虎資安調查之後發現，其實駭客打中的是該公司Web log除錯工具一個剛好與Bash Shell一樣有「指令插入」瑕疵的漏洞。

文/ 林妍蓀 | 2014-10-07 發表

讚 7,706 按讚加入iThome粉絲團 分享 120 8+1 0

註解: Bash是一個指令列shell（殼層）程式，廣泛存在於Linux、BSD和Mac OS X等UNIX-based的作業系統，使用者只要將指令輸入到一個簡單的文字式視窗，作業系統便會依指令運作。由於全球有超過半數的伺服器採用Linux，也讓這個漏洞的可能影響相當可怕，各方評估皆認為，嚴重程度可能超過Heartbleed。駭客一但成功攻擊一個網站或伺服器，特別是CGI網頁伺服器，幾乎可以為所欲為，例如可以隨意修改網站內容，變更程式碼、竊取資料庫中的使用者資料，或者安裝後門等惡意程式。而根據各個資安機構指出，目前已開始出現了利用Shell Shock的攻擊案例。

開源軟體(Open Source) 安全隱憂

OPEN SOURCE SECURITY ANALYSIS 2016 REPORT

Recent Black Duck On-Demand security audits of 200 commercial applications confirm the importance of open source in application development, and also highlight the persistent challenges organizations face in effectively securing and managing their open source dependencies.



67% of applications reviewed contained known open source security vulnerabilities



On average the companies were using 100% more open source than they originally believed

1,894 DAYS



Average age of known open source security vulnerabilities



Average amount of open source code in each application.



Average number of open source dependencies



iThome 新聞 產品評測 技術 專題 AI & Big Data Cloud DevOps GDPR 資安 研討會

新聞

Git爆任意程式碼執行漏洞，所有使用者皆受影響！

Git由於在處理子模組儲存庫的設置檔案存在漏洞，導致開發者可能遭受任意程式碼執行攻擊，多數程式碼託管服務皆已預設拒絕有問題的程式碼儲存庫，但使用者最好還是趕快更新，避免曝露在風險中。

文/ 李連興 | 2018-05-30 發表

讚 4.9 萬

按讚加入iThome粉絲團

讚 305 分字

G+



git --distributed-even-if-your-workflow-isnt

Search entire site...

Git is a **free and open source** distributed version control system designed to handle everything from small to very large projects with speed and efficiency.

Git is **easy to learn** and has a **tiny footprint with lightning fast performance**. It outclasses SCM tools like Subversion, CVS, Perforce, and ClearCase with features like **cheap local branching**, convenient **staging areas**, and **multiple workflows**.



Learn Git in your browser for free with **Try Git**.



資料來源: Black Duck Software

安全脆弱度，只需要一個正確的點

阿基里斯 vs. 阿基里德



你所認為的安全



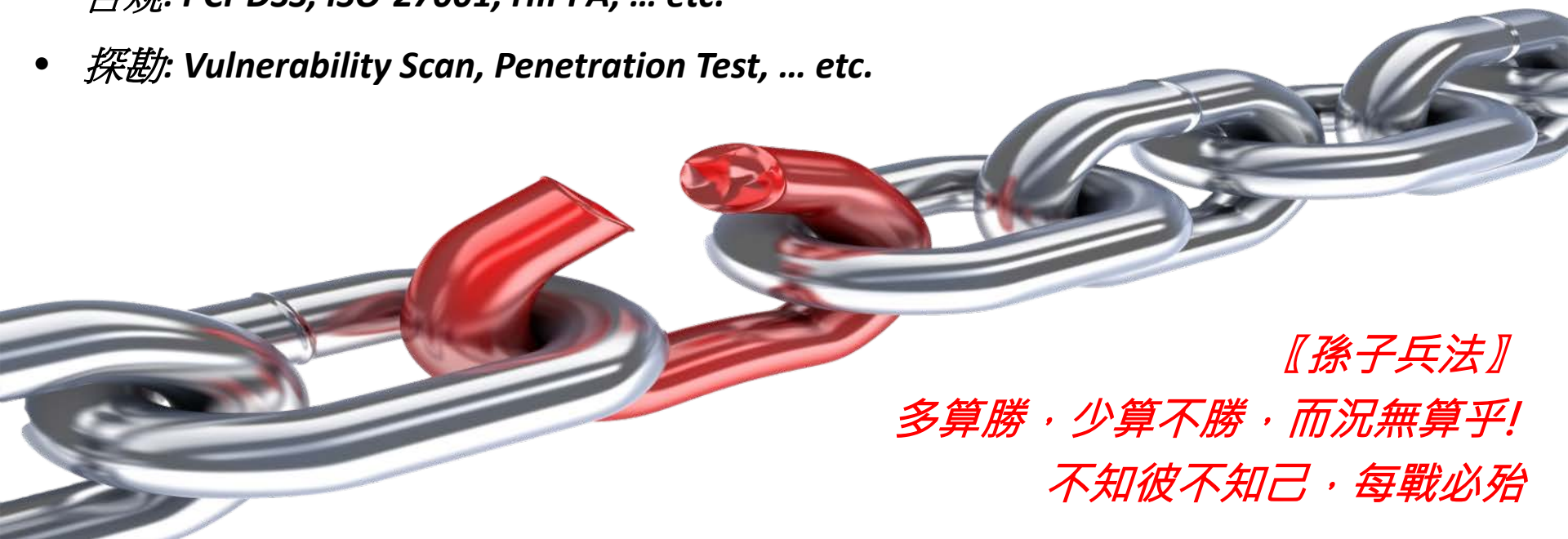
駭客

弱點

再問: 為什麼一定要掃描

資安防禦工事上的迷思

- **防護:** Firewall, IPS, Anti-Virus, Content Security Gate, Endpoint Security, WAF, NAC, ... etc.
- **檢測:** APT, Sandbox, Code review, ...etc.
- **分析:** Log Analysis management, SIEM, SOC, ...etc.
- **合規:** PCI-DSS, ISO-27001, HIPPA, ... etc.
- **探勘:** Vulnerability Scan, Penetration Test, ... etc.



【孫子兵法】
多算勝，少算不勝，而況無算乎！
不知彼不知己，每戰必殆

大綱簡介

- 前言
- 為什麼一定要掃描
- 防毒軟體、弱點掃描、滲透測試的差異性
- 我收到了弱掃報告，可是看不懂
- 怎樣找到最合適自己的弱掃工具
- Q&A

不同世代的安全威脅演進



Check Point
SOFTWARE TECHNOLOGIES LTD

第五世代安全與惡意威脅趨勢

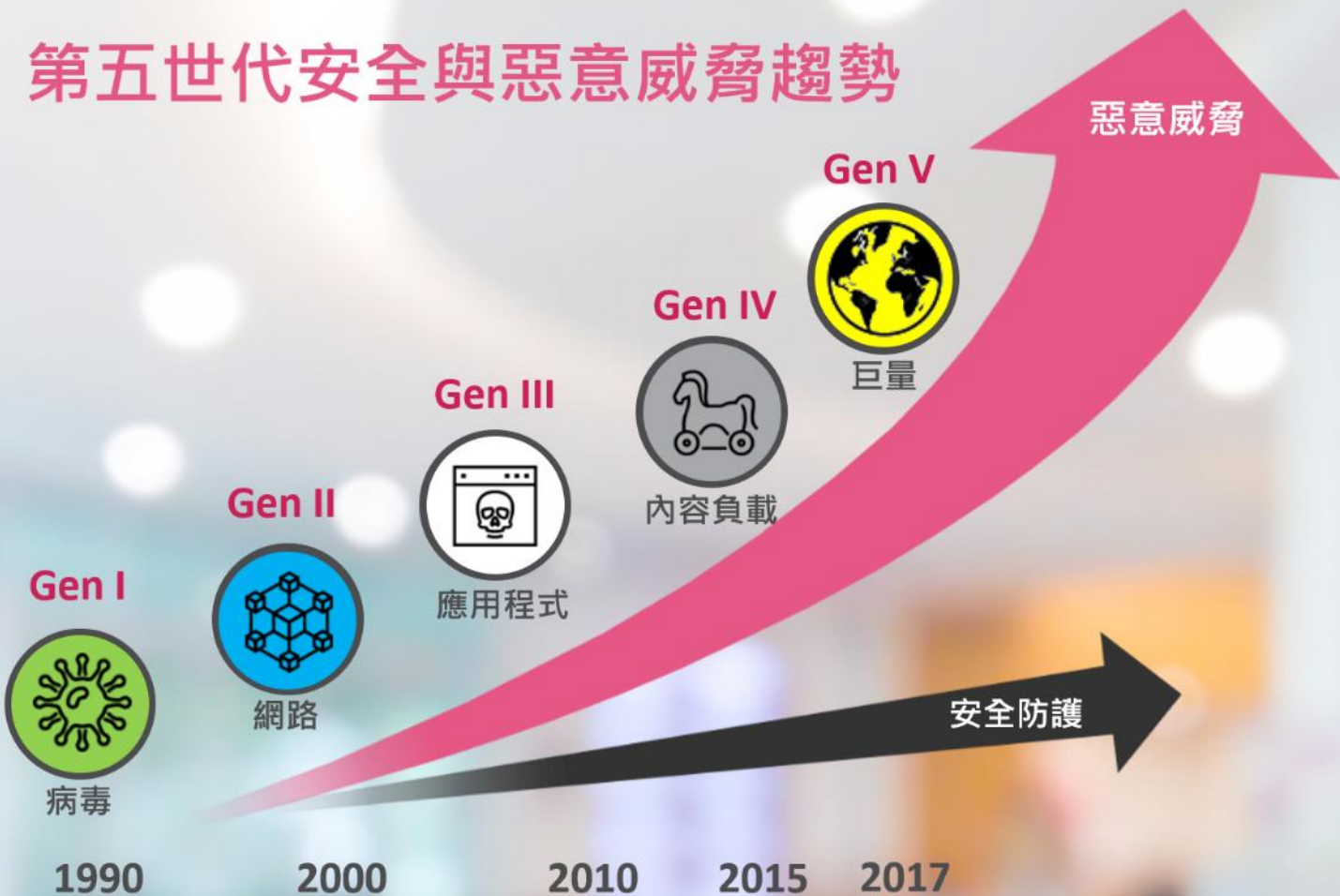
GRADE V

GRADE IV

GRADE III

GRADE II

GRADE I



不同世代威脅與安全防護對照

- Gen I**  1980'後期 – PC攻擊 – 單點破壞
病毒 防毒軟體
- Gen II**  1990'中期 – 外部網路攻擊
網路 防火牆
- Gen III**  2000s – 應用程式漏洞與系統弱點
應用程式 入侵偵測系統(IPS)
- Gen IV**  2010 – 多元型態惡意內容
內容負載 沙箱檢測與殭屍防護

Gen V



巨量

立即防禦威脅(不單僅是偵測威脅)

可即時反應與迅速回覆

全面防堵所有安全突破口:
雲、端點、網路、行動裝置

安裝防毒軟體 不等於 做好資安防護

iThome

新聞

產品評測

技術

專題

AI & Big Data

Cloud

DevOps

GDPR

資安

研討會

賽門鐵克疾呼防毒軟體已死

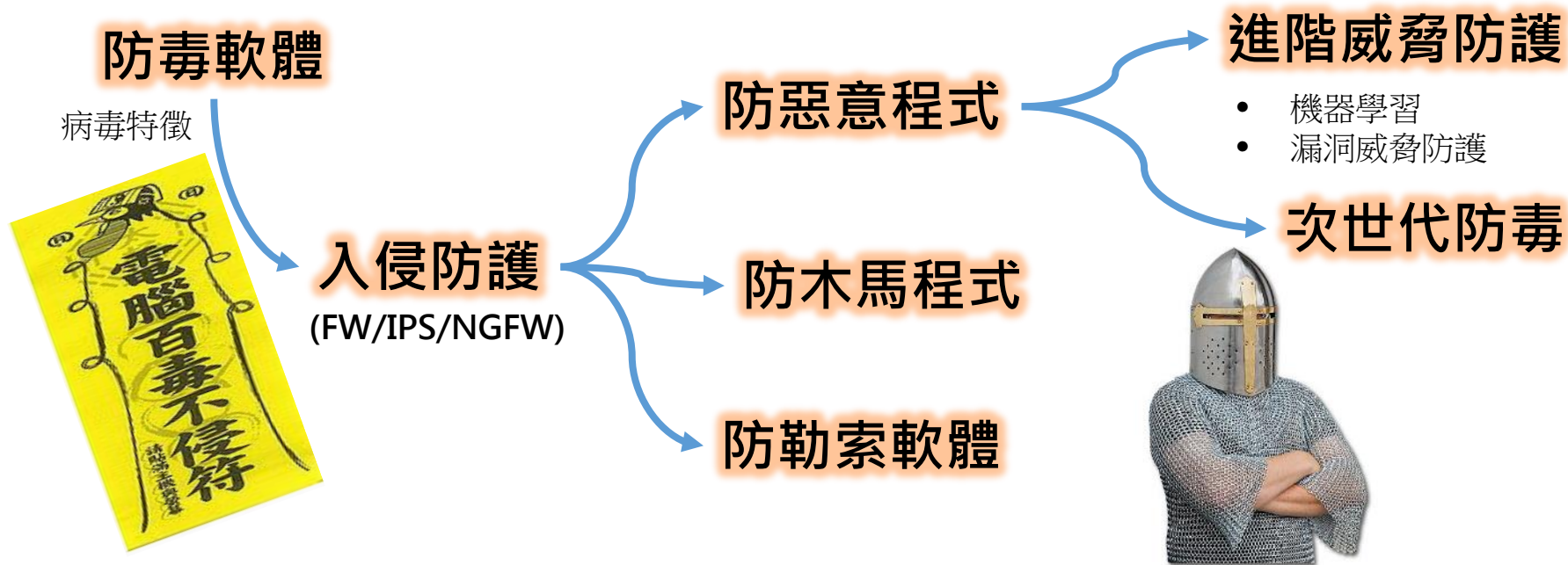
知名防毒軟體廠商賽門鐵克資深副總裁Brian Dye接受華爾街日報採訪時表示，80年代所發展出來的惡意軟體解決方案，現今已不再有效，惡意軟體攔截率僅剩45%，防毒軟體將不再是業者的搖錢樹

文/ 李建興 | 2014-05-21 發表

✓ 讚 4.9 萬 按讚加入iThome粉絲團

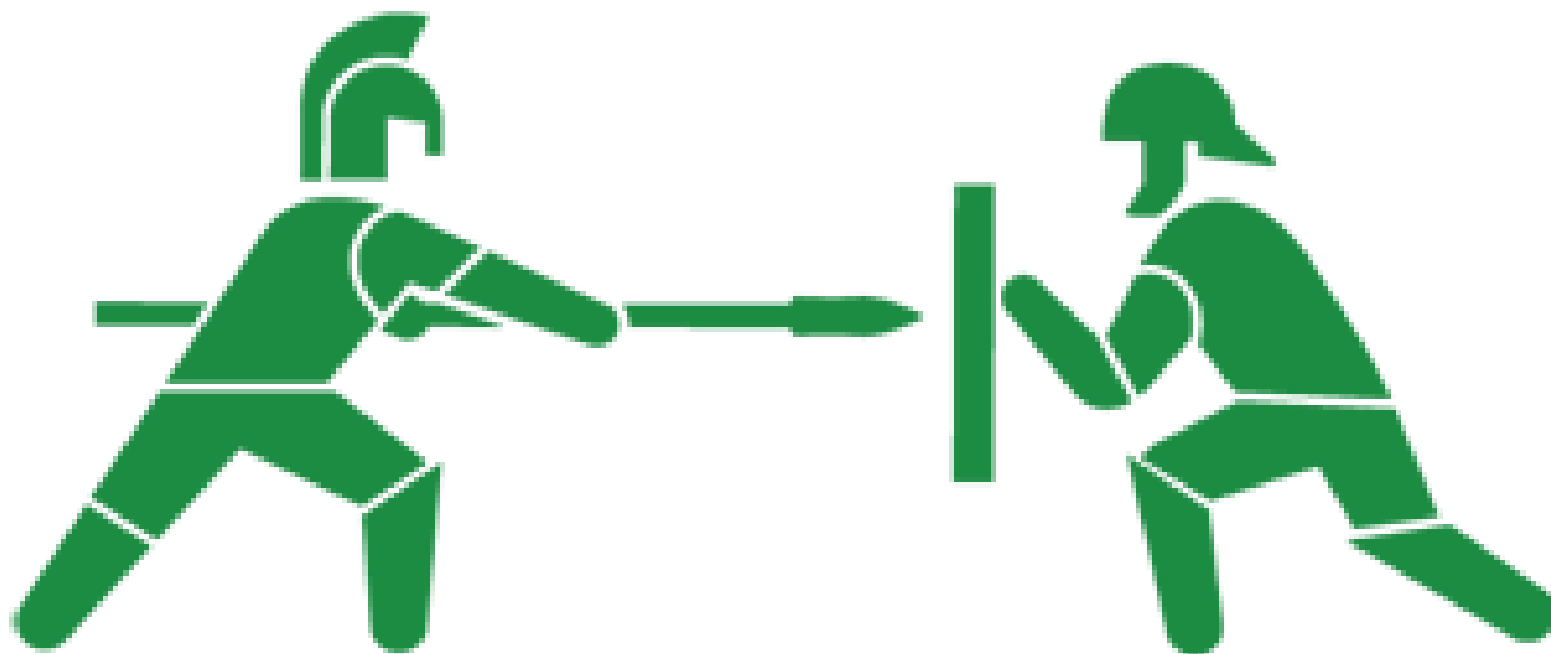
👍 讚 0 分享

G+



弱點掃瞄與滲透測試之間...?

對抗？演練？



弱點掃描與滲透測試 是相互合作搭配

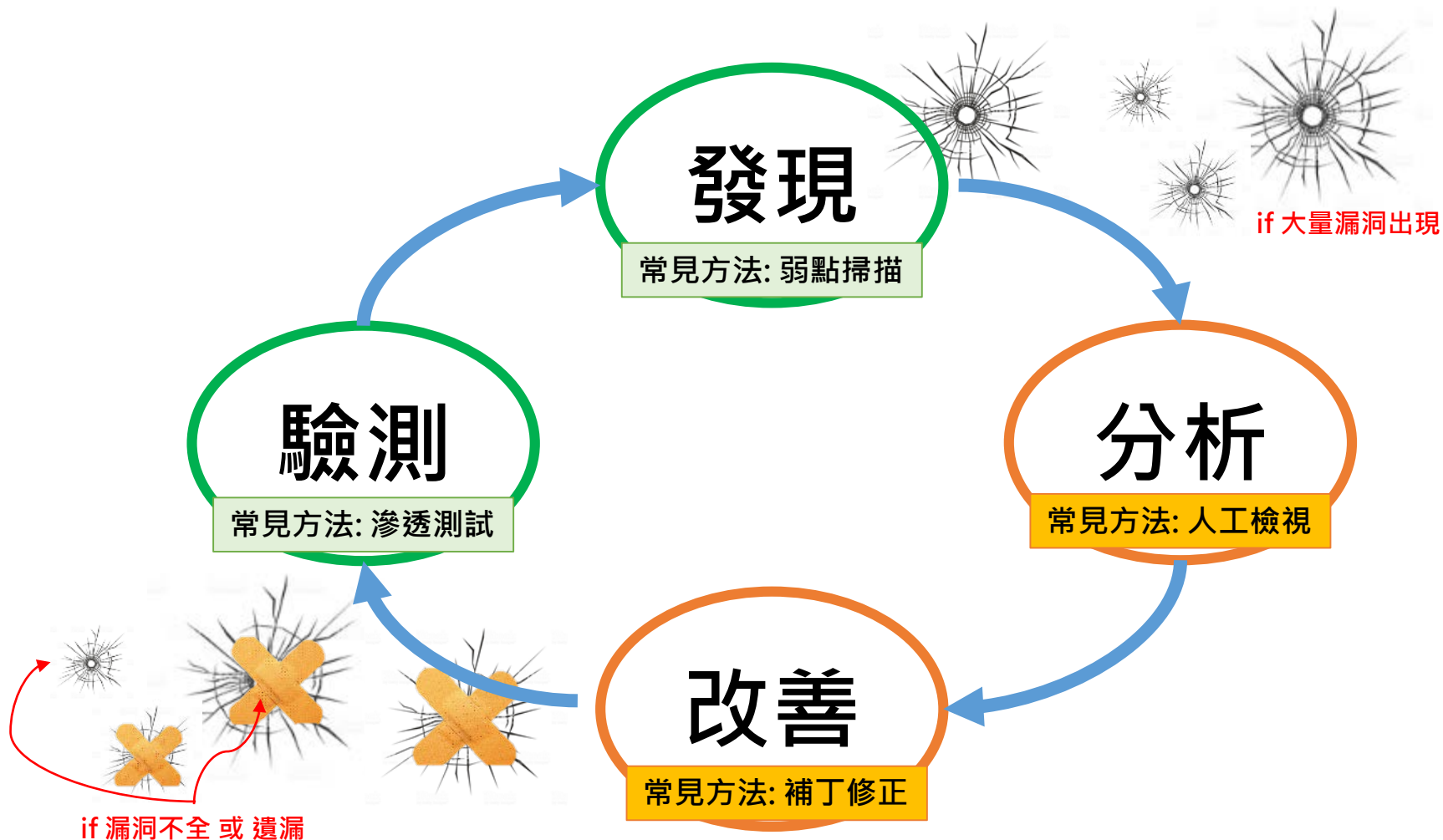
目的相同的 不同檢驗方式.

弱點掃描
Vulnerability Scanning

滲透測試
Penetration Testing



弱點掃描與滲透測試 是相互合作搭配



建立高效率的弱點安全管理

5 Best Practices for Building an Effective Vulnerability Management

1



SCAN

Perform weekly external and internal network scans

2



PLAN

Develop and implement an alert mitigation plan

3



PRIORITIZE

Make patches and fixes a high priority

4



VALIDATE

Test and validate patches and fixes before deployment

5



DEPLOY

Apply validated patches and fixes as soon as possible

資料來源 <https://www.acacompliancegroup.com/blog/5-best-practices-building-effective-vulnerability-management-program>

從資安怎麼看待「弱點(漏洞)」

弱點漏洞

不管嚴重等級是高(High)還是低(Low)

只要可以利用，就是好弱點

如果容易利用，那就是絕佳好弱點

受駭目標不管是高階或低階

只要可以利用，就是好目標！

弱點漏洞是怎麼發生？

- 不當的設計(Bad Design)
 - 例: 作業系統, 應用程式, 元件, 技術...
- 不當的實作(Bad Implementation)
 - 例: 網路規劃, 系統規劃, 存取控制...
- 不當的組態設定(Bad Configuration)
 - 例: 預設密碼, 未依循規範政策...
- 過時的組態設定(Stale Configuration)
 - 例: 沒有修補或更新...
- 被利用的方式
 - 例: Bypass, 加密通訊, 白名單, 社交工程...

資安趨勢部落格 > 漏洞攻擊 > 未來四年之內，零時差漏洞出現的頻率很可能提高到每天一次

未來四年之內，零時差漏洞出現的頻率很可能提高到每天一次

POSTED ON 2017 年 07 月 18 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

Share

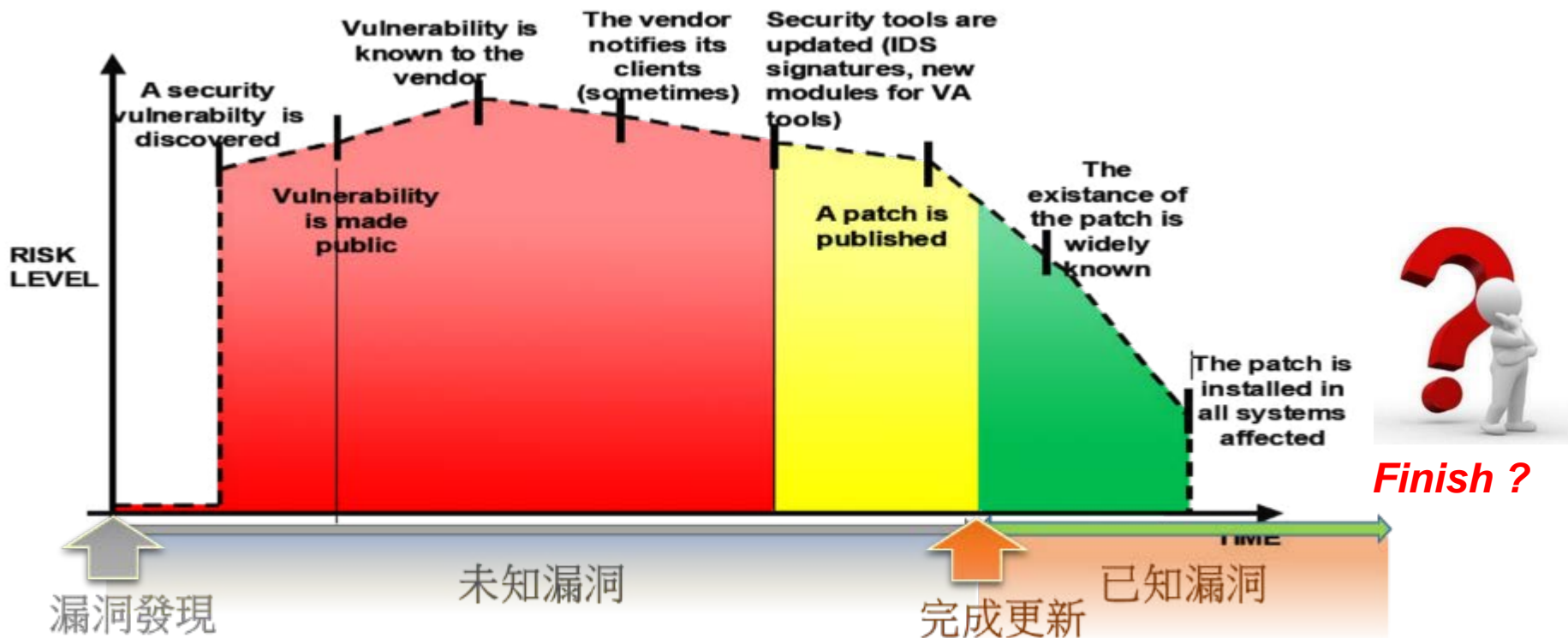
零時差漏洞 (也就是從未被發現的新漏洞) 最近出現的頻率越來越高，更糟的是，這些危險的漏洞經常都是在駭客攻擊事件發生之後，人們才知道漏洞的存在。

根據網路資安研究機構 Cybersecurity Ventures 創辦人暨總編輯 Steven Morgan 指出，零時差漏洞的出現頻率在未來四年之內很可能提高到每天一次 (在 2015 年時大約每週一次)。



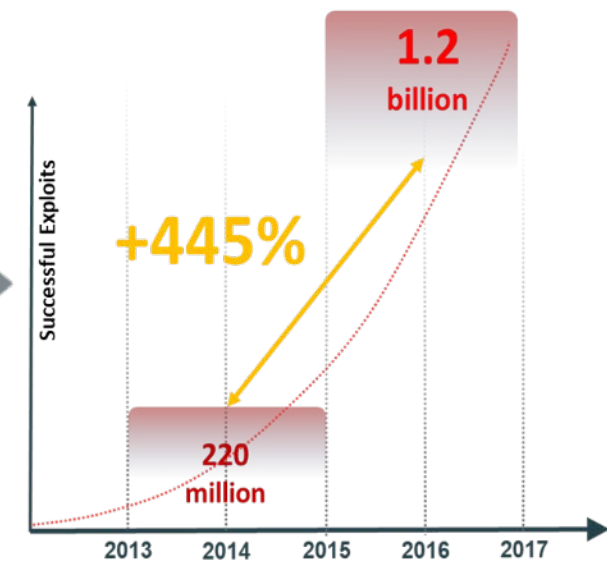
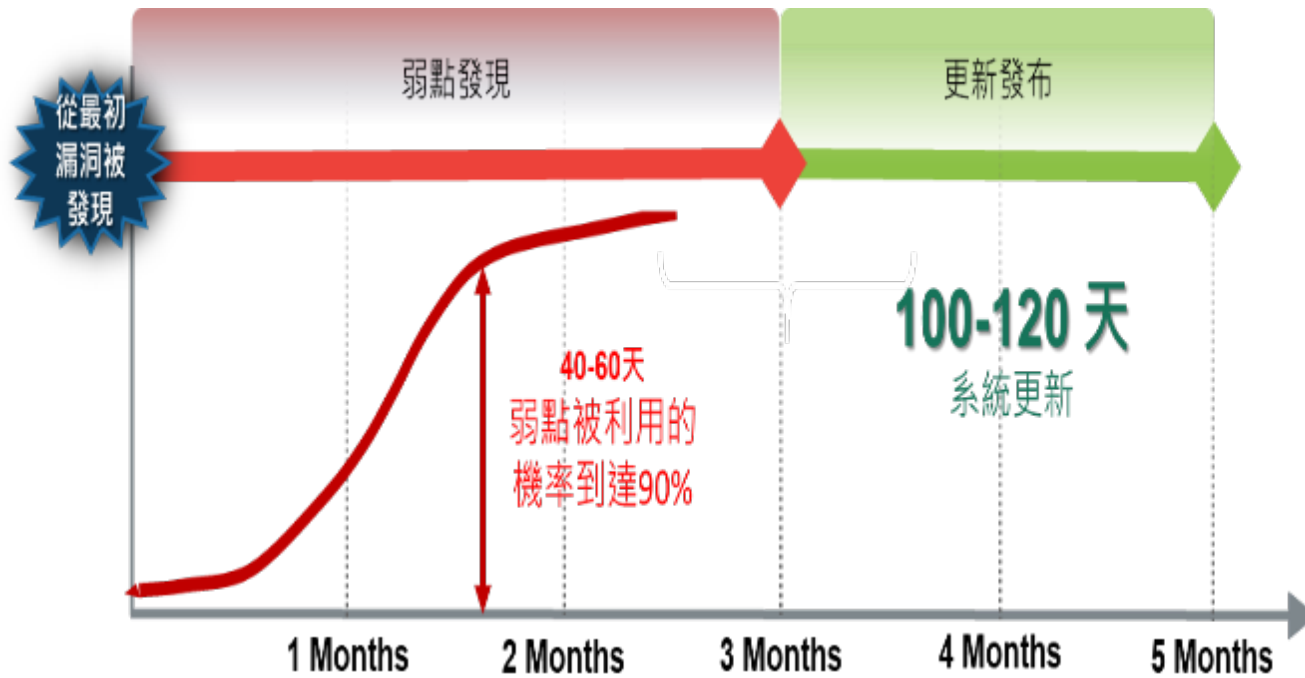
Zero-Day Attack 零日攻擊威脅

Window of Vulnerability



資料來源: https://www.owasp.org/index.php/Testing_Guide_Introduction

從漏洞揭露開始，攻擊威脅已然存在



Source: <https://www.infosecurity-magazine.com/news/companies-average-120-days-patch/>

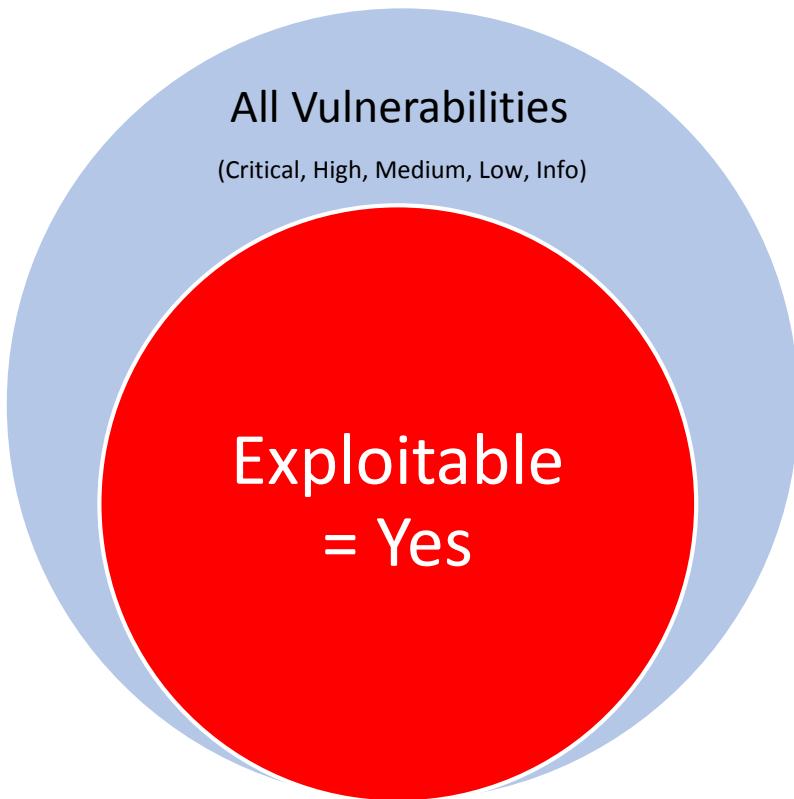
可利用的弱點漏洞 Exploitable

漏洞弱點不一定是絕對&立即威脅，必須搭配適當的條件才能被利用。

具備可利用性 (Exploitable) 代表該弱點漏洞已具可立即使用的攻擊程式碼 並被分享於相關滲透測試與漏洞工具包(Exploit Kits)。



2018年度網路安全報告

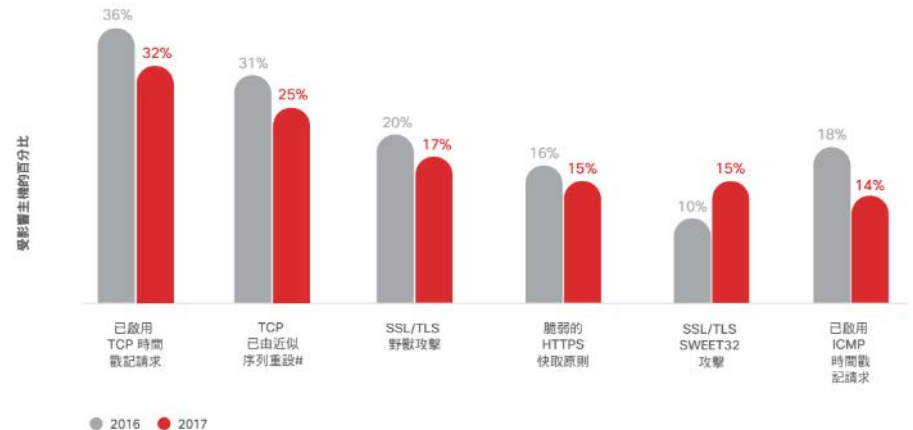


最常見的漏洞是嚴重性低但風險甚高

安全性解決方案公司和思科合作夥伴 SAINT Corporation 的資安專家表示，低嚴重性漏洞遺留多年，是因為公司不知道它們存在，或不認為它們存在重大風險。然而，這些微小安全缺口可能有著重大影響，讓惡意人士有機可乘，能夠入侵系統。

SAINT 研究人員研究 2016 年和 2017 年從 10,000 多台主機收集的漏洞暴露資料。該公司制定研究中所有組織最常偵測到的熱門漏洞列表，其表明最常發生低嚴重性漏洞（請參閱圖 39）。（請注意：研究中包含的一些組織有多個主機。）

圖 39 最常偵測到的低嚴重性漏洞，2016 年至 2017 年



來源：SAINT Corporation

關於「滲透測試」

定義：

滲透測試是指藉由具備資安知識與經驗、技術人員受僱主所託，針對僱主的目標系統模擬駭客的手法進行攻擊測試，藉以發掘安全漏洞並提出改善方法的善意行為。(By 維基百科)

目的：

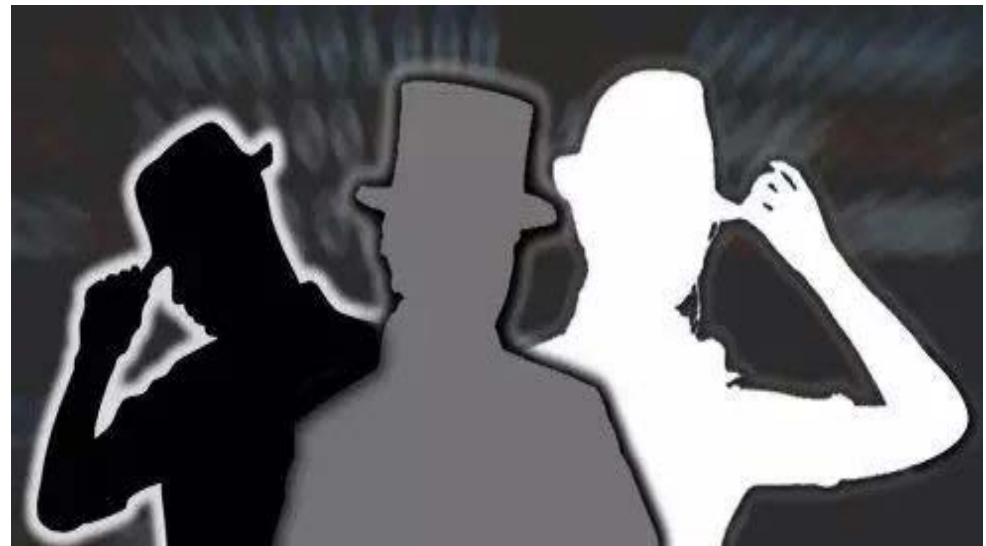
- 瞭解入侵者可能利用的途徑
- 瞭解系統及網路的安全強度
- 瞭解弱點並強化安全

方法論：

- OSSTMM
- OWASP Testing Guide
- SSDLC

方式：

- 白箱: 提供「檢測目標」的弱點資訊，由滲透測試者檢測；確認安全保戶強度。
- 黑箱: 只告知「檢測目標」，由滲透測試者自行發揮；模擬真實駭客攻擊。
- 灰箱: 上述二者的混和方式，常用在資訊不清楚的調查上。
- 雙黑箱: 授權合法的攻防演練。



白箱測試 vs. 黑箱測試 的優缺差異

以Web系統為例:

	優點	缺點
白箱測試	<ol style="list-style-type: none">1.弱點偵測正確率高2.提供較適當修正建議	<ol style="list-style-type: none">1.離線掃描2.僅能偵測程式碼上的弱點3.需提供程式碼
黑箱測試	<ol style="list-style-type: none">1.能偵測網站本身與程式碼的弱點2.弱點偵測範圍較為廣泛3.模擬駭客攻擊	<ol style="list-style-type: none">1.誤報率高2.需人工驗證3.需線上掃描4.耗時5.破壞性攻擊

防護架構檢測

網站系統檢測

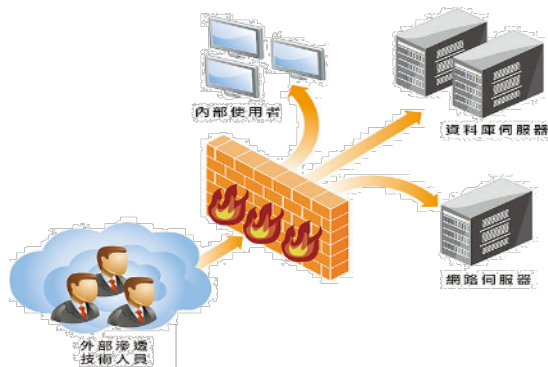
穿透檢測

原始碼檢測

周邊安全檢測

專業滲透測試服務的程序

注意！「甲方」與「乙方」必須達成共識與同意。
避免觸犯法律（刑法「告訴乃論」）



常見的滲透測試議題

□ 訊息蒐集

□ 目標探測

□ 弱點評估

□ Web掃描

□ 社交工程

□ 資料庫探測與攻擊

□ 密碼破解

□ 漏洞利用

□ 提權工具

□ 持續控制工具

□ 無線網路攻擊

□ 壓力測試

□ 測試報告

滲透測試的入門之法

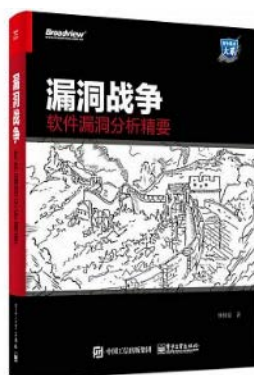
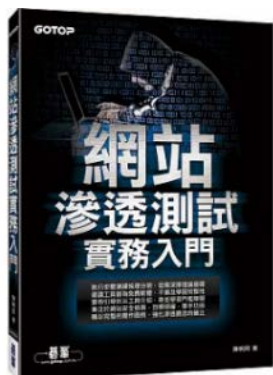
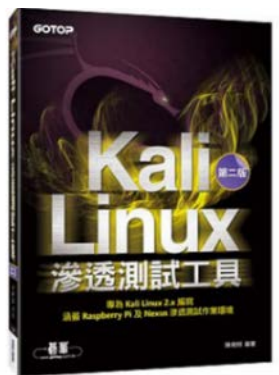
- 滲透測試技術 ≠ 駭客養成
- 駭客技術也不會像駭客任務的技能下載
- 知識: Domain Knowledge, Know-how
- 技術: 技術, 技巧, 工具
- 經驗: 新聞資訊, LAB實做, 實戰
- 想像力與好奇心

學習資訊參考



Kali Linux 2018.2 Release

<https://www.kali.org/>



大綱簡介

- 前言
- 為什麼一定要掃描
- 防毒軟體、弱點掃描、滲透測試的差異性
- 我收到了弱掃報告，可是看不懂
- 怎樣找到最合適自己的弱掃工具
- Q&A

OMG... 弱掃報告又來了.



看不懂報告

財務報告

醫療檢查報告

台灣積體電路製造股份有限公司及其子公司
高頻寬頻寬頻寬

民國 107 年 3 月 31 日 截至 106 年 12 月 31 日 及 3 月 31 日

單位：新台幣仟元

代碼	資產	107年3月31日 (經核實)		106年12月31日 (經核實)		106年3月31日 (經核實)	
		金	幣	金	幣	金	幣
1100	現金及約當現金 (附註六)	\$ 577,782,963	28	\$ 533,391,696	28	\$ 544,725,266	29
1110	透過關聯企業收購之金融資產 (附註七)	963,915	-	569,751	-	5,374,003	-
1120	透過其他綜合損益按公允價值衡量之金融資產 (附註八)	95,713,446	4	-	-	-	-
1125	透過損益按公允價值衡量之金融資產 (附註九)	-	-	99,374,153	5	71,083,797	4
1130	持有至到期日之金融資產 (附註十)	-	-	1,988,385	-	18,140,374	1
1136	按攤銷成本計量之金融資產 (附註十一)	9,888,741	1	-	-	-	-
1135	應收之利息及股息 (附註十三)	-	-	34,394	-	-	-
1139	應收之金融資產 (附註十三)	26,357	-	-	-	-	-
1170	應收票據及應收淨額 (附註十四)	106,691,372	5	121,133,348	6	106,532,829	6
1180	應收關係人款項 (附註三二)	1,175,312	-	1,184,124	-	494,839	-
1210	其他應收關係人款項 (附註三二)	130,070	-	171,658	-	135,051	-
1310	存貨 (附註十五)	85,215,899	4	73,880,747	4	50,389,022	3
1476	其他金融資產 (附註三三)	11,667,264	1	7,233,114	-	3,761,484	-
1479	其他金融資產 (附註三三)	39,587,321	2	4,222,440	-	3,052,168	-
11XX	流動資產合計	920,116,660	45	827,293,110	43	826,661,633	43
1517	非流動資產	-	-	-	-	-	-
1527	透過其他綜合損益按公允價值衡量之金融資產 (附註八)	6,035,904	-	-	-	-	-
1535	透過損益按公允價值衡量之金融資產 (附註九)	-	-	18,833,329	1	20,499,438	1
1543	按攤銷成本計量之金融資產 (附註十一)	10,033,241	1	-	-	-	-
1543	以成本衡量之金融資產 (附註十二)	-	-	4,874,257	-	4,079,292	-
1550	採用權益法之投資 (附註十六)	18,307,517	1	17,861,488	1	19,940,062	1
1600	不動產、廠房及設備 (附註十七)	1,895,366,207	51	1,862,582,322	53	1,897,364,143	54
1780	商標資產 (附註十八)	13,674,295	1	14,175,140	1	14,278,436	1
1840	遞延所得稅資產 (附註四)	12,987,042	1	12,185,643	1	10,644,401	-
1920	存出保證金	2,121,209	-	1,263,414	-	572,005	-
1990	其他非流動資產 (附註十九)	1,513,731	-	2,983,120	-	1,624,131	-
15XX	非流動資產合計	1,128,695,146	55	1,134,698,933	57	1,109,801,938	57
100X	資產總計	\$2,049,155,806	100	\$1,991,861,643	100	\$1,936,463,571	100
2100	短期負債	\$ 56,731,350	3	\$ 63,766,850	3	\$ 54,666,000	3
2120	透過關聯企業收購之金融負債 (附註七)	170,673	-	26,709	-	124,935	-
2125	透過損益按公允價值衡量之金融負債 (附註九)	-	-	15,562	-	3,908	-
2126	應付之利息及股息 (附註十三)	79,182	-	-	-	-	-
2170	應付帳款	27,817,670	1	28,412,897	1	23,081,567	1
2180	應付關係人款項 (附註三二)	1,224,307	-	1,656,356	-	1,171,195	-
2201	長期銀行借款	18,291,325	1	14,254,871	1	10,703,456	1
2206	應付員工酬勞及董事酬勞 (附註二四及二九)	29,929,609	1	23,419,135	1	28,857,495	1
2213	應付之股利及股款	47,828,289	2	55,723,774	3	57,671,953	3
2250	當期所得稅負債 (附註四)	44,096,800	2	33,479,311	2	52,874,433	3
2250	負債準備 (附註二一)	49,354,740	2	33,961,787	1	11,296,320	1
2320	一年內到期之非流動負債 (附註二二)	-	-	58,401,122	3	44,909,480	2
2399	應付費用及其他流動負債 (附註二五、三十五及三二)	75,119,897	4	65,588,396	3	36,217,252	2
21XX	流動負債合計	342,235,242	16	358,206,680	18	321,580,524	17
2500	非流動負債	-	-	-	-	-	-
2541	應付公司債 (附註二五及三十一)	83,400,000	4	91,800,000	5	134,198,769	7
2541	長期銀行借款	-	-	-	-	19,340	-
2573	遞延所得稅負債 (附註四)	285,644	-	302,205	-	90,944	-
2640	淨延遲所得稅負債 (附註四)	8,818,704	1	8,650,704	1	8,337,369	-
2645	存入保證金 (附註二三及三十一)	5,991,361	-	7,586,790	-	12,321,468	1
2670	其他非流動負債	1,819,825	-	1,855,621	-	1,605,260	-
25XX	非流動負債合計	100,315,530	5	110,995,320	6	156,773,212	8
200X	負債合計	442,550,772	21	469,102,000	24	478,353,736	25

癌症篩檢 Tumor Markers

人類絨毛激素【男】B-HCG <1.2 mIU/ml <5

放射線檢查 Radiology Examination

胸部正面X光 Chest X-ray 無異狀

腰椎骨質密度檢查之平均骨密度 BMD 0.88 (g/CM2)

腰椎骨質密度檢查之骨密度百分比 BMD 87 (%)

腰椎骨質密度檢查之結論 BMD 骨質流失(T-score: -1.1) >=-1.0

右髖骨骨質密度檢查之平均骨密度 BMD 0.85 (g/CM2)

右髖骨骨質密度檢查之骨密度百分比 91

右髖骨骨質密度檢查之結論 BMD 正常(T-score: -0.6) >=-1.0

靜態心電圖檢 ECG

十二導程心電圖檢查 12-lead ECG 正常(心跳次數: 65次/分)

腹部超音波 Abdominal Ultrasound

腹部超音波(肝臟) Liver 輕度脂肪肝; 肝臟數顆囊腫, 大小小於2公分

腹部超音波(膽囊) Gallbladder 無異狀

檢查項目	正常參考值	5/24	5/25	5/26	5/29	第二次 入院	6/24
WBC	4~10 10 ³ /μL	11.8		17.1	11.6		7.5
RBC	4.5~5.9 10 ⁶ /μL	4.41		3.88	3.53		4.09
Platelet	150~440 10 ³ /μL	467		397	359		296
Hgb	14~18 g/dL	14.2		12.2	11.2		13.1
BUN	7~20 mg/dL	16			19		12
Creatine	0.7~1.5 mg/dL	1.2			1.1		1.13
CK	≤171 U/L	1526	4550	3080			
CK-MB	≤16.0 U/L	207	490	197			
C.R.P	≤3.0 mg/L	11.5		97.3	154.9		
Cholesterol	≤200 mg/dL	204					
TG	≤150 mg/dL	301					
HDL-C	≥40 mg/dL	39					
LDL-C	≤130 mg/dL	122					
PT	8~12 sec	9.5	10.0				10
APTT	23.9~34.9	27.5	32.0	37.4			28.5

備註：紅色字體代表檢查數值異常

我不明白你的明白...@@

主要的問題

Total Protein	8.1	6.0-8.5	g/dl
Albumin	4.8	3.5-5.5	g/dl
Globulin	3.3	2.2-3.5	g/dl
A/G Ratio	1.5	1.2-2.0	
G.O.T(AST)	27	0-40	U/L
G.P.T(ALT)	52 高	0-40	U/L
Alkaline-P	71	32-92	U/L
Total bilirubin	0.8	0.0-1.5	mg/dl
Direct bilirubin	0.2	0.0-0.4	mg/dl
r-GT(GGT)	50 高	8-34	U/L
HBsAg(i)	0.00 陰性	≤0.05	IU/ml
Cholesterol Total	246 高	120-200	mg/dl
Triglyceride	185 高	35-150	mg/dl
Sugar AC	102 高	70-100	mg/dl
BUN	18	8-25	mg/dl
Creatinine	1.0	0.5-1.5	mg/dl
Uric Acid	7.8 高	2.0-7.5	mg/dl
C.P.K	153	0-250	U/L
L.D.H	134	80-285	U/L
a-Amylase	37	30-160	U/L
V.D.R.L(R.P.R.)	Non-React	(Non-React)	#24800

○文字語言問題

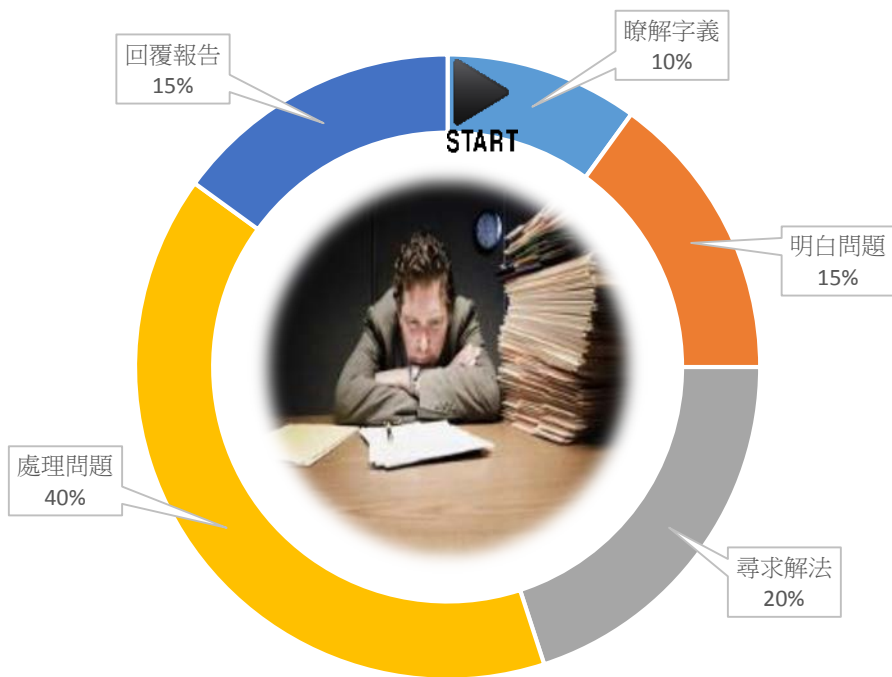
○字義解讀問題

○專業知識

○處理經驗

○急於尋求答案

弱掃報告 是幫助避免資安風險的基礎



資料

資訊

情報
分析

計畫

處理

減少
弱點曝光
(風險空窗期)

看懂弱掃報告的準備工作

● 弱掃的目的

- 系統弱掃 (系統漏洞, 應用程式漏洞, 服務漏洞, 密碼猜測, 組態設定 等)
- 網站弱掃 (系統弱掃, 網頁應用弱掃, 源碼檢測 等)

● 弱掃工具與方法

- 常見系統弱掃工具: Tenable/Nessus, Nmap/Zenmap, OpenVAS 等
- 掃描方式: 網路掃描 或 授權(深層)掃描.

● 必須認識的關鍵字

- CVE (弱點編號)
- CVSS (弱點風險評分)
- Severity (風險等級)
- Exploit Available (弱點可利用)
- Solution (修補解決方案建議)

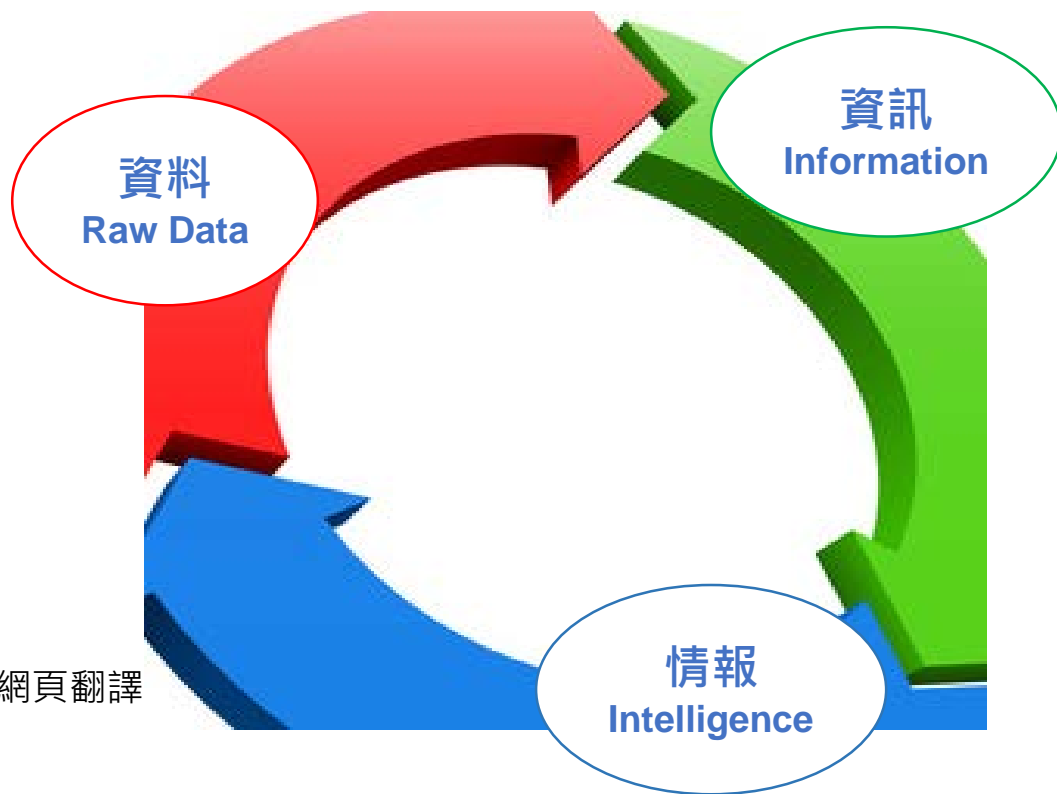
建立方便看懂的弱掃報告

● 定義報告結構化

- 目標資產資訊
- 掃瞄執行時間
- 整體狀態彙總
- 建立索引並階層排序
- 別吝於拆分報告內容

● 相關資源的幫助

- 翻譯工具, 例: Google Chrome 網頁翻譯
- 搜尋工具, 例: Google Search
- 弱點相關資訊網站, 例: [CVE Details](#), [Vuldb](#), [Exploit-db](#), [Tenable](#) 等
- 資安訊息相關網站, 例: [iThome security](#), [TW-CERT](#), [TACERT](#) 等





Nessus Scan Report

Fri, 14 Jul 2017 14:45:49 Eastern Standard Time

Table Of Contents

[Vulnerabilities By Host](#)

(例) 以主機(Host)排序方式

192.168.15.43

192.168.15.72

192.168.15.85

192.168.15.112

192.168.15.113

[Remediations](#)

[Suggested Remediations](#)

Vulnerabilities By Host

[-] Collapse All

[+] Expand All

192.168.15.43

Scan Information

Start time: Fri Jul 14 13:26:16 2017

End time: Fri Jul 14 13:48:20 2017

Host Information

DNS Name: fedora25.localhost.local

IP: 192.168.15.43

MAC Address: 00:15:5d:0f:c6:af

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	3	0	24	27



Nessus Scan Report

Fri, 14 Jul 2017 14:45:49 Eastern Standard Time

Table Of Contents

[Vulnerabilities By Plugin](#)

(例) 以弱點排序方式

97833 (2) - MS17-010: Security Update for Windows 8.1, Windows RT 8.1, Windows Server 2012 R2, Windows Server 2012, Windows Server 2016, Windows 10, Windows Server 2016, Windows 10, and Windows Server 2016

Vulnerabilities By Plugin

[-] Collapse All

[+] Expand All

97833 (2) - MS17-010: Security Update for Windows 8.1, Windows RT 8.1, Windows Server 2012 R2, Windows Server 2012, Windows Server 2016, Windows 10, Windows Server 2016, Windows 10, and Windows Server 2016 (WannaCry) (EternalRocks)

Synopsis

The remote Windows host is affected by the following vulnerability:

Description

The remote Windows host is affected by the following vulnerability:

- Multiple remote code execution (SMBv1) due to improper handling of these vulnerabilities, via 0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, and CVE-2017-0148.

- An information disclosure vulnerability due to improper handling of certain requests, via a specially crafted packet.

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

See Also

<https://technet.microsoft.com/library/security/MS17-010>

<http://www.nessus.org/u?321523eb>

<http://www.nessus.org/u?7bac1941>

<http://www.nessus.org/u?d9f568cf>

<https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/>

<https://support.microsoft.com/en-us/ku/2696547>

<http://www.nessus.org/u?8dca55e4>

<http://www.nessus.org/u?38fd3072>

<http://www.nessus.org/u?4c7e0cf3>

<https://github.com/stamparm/EternalRocks/>

<http://www.nessus.org/u?59db5b5b>

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.8 (CVSS:3.0/E:P/R:L/O:R/C:C)

CVSS Base Score

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

CVSS Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

報告範本(高階)

以階層式摘要表示

Table of Contents

掃描結果摘要
 所有主機弱點
 10.8.13.186
 10.8.13.195

掃描結果摘要

第一階 總覽整體狀態

弱點數量(依風險)

弱點數量(依主機)

IP Address
10.8.13.195
10.8.13.186

所有主機弱點

第二階

10.8.13.186

IP Address: 10.8.13.186
MAC Address: 34:99:71:00:fc:e2
Total: 35
Vulnerabilities: Critical: 0, High: 0, Medium: 3, Low: 0, Info: 32

各級風險弱點數量統計

Severity
Critical
High
Medium
Low
Info

第三階 顯示該主機弱點詳細資訊

嚴重風險等級弱點

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port	Exploit?
56998	Microsoft Office Unsupported Version Detection	Windows	Critical	10.8.13.186	TCP	445	No

Plugin Text:
Plugin Output:
 Installed product : Office 2007
 End of support date : October 10, 2017
 Supported versions : Office 2010 / 2013 / 2016

Synopsis: The remote host contains an unsupported version of Microsoft Office.
Description: According to its version, the installation of Microsoft Office on the remote Windows host is no longer supported.
 Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.
Solution: Upgrade to a version of Microsoft Office that is currently supported.
See Also: <http://support.microsoft.com/gp/lifeoffice>

CVE:

高風險等級弱點

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port	Exploit?
87253	MS15-124: Cumulative Security Update for Internet Explorer (3116180)	Windows : Microsoft Bulletins	High	10.8.13.186	TCP	445	Yes

Plugin Text:
Plugin Output:
 ASLR hardening settings for Internet Explorer in KB3125869 have not been applied. The following DWORD keys must be created with a value of 1:
 - HKLM\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_ALLOW_USER32_EXCEPTION_HANDLER_HARDENING\iexplore.exe
 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_ALLOW_USER32_EXCEPTION_HANDLER_HARDENING\iexplore.exe

Synopsis: The remote host has a web browser installed that is affected by multiple vulnerabilities.
Description: The version of Internet Explorer installed on the remote host is missing Cumulative Security Update 3116180. It is, therefore, affected by multiple vulnerabilities, the majority of which are remote code execution vulnerabilities. An unauthenticated, remote attacker can exploit these issues by convincing a user to visit a specially crafted website, resulting in the execution of arbitrary code in the context of the current user.
Solution: Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 8, RT, 2012, 8.1, RT 8.1, 2012 R2, and 10.
See Also: <https://technet.microsoft.com/library/security/MS15-124>
CVE: CVE-2015-6093,CVE-2015-6134,CVE-2015-6135,CVE-2015-6136,CVE-2015-6138,CVE-2015-6139,CVE-2015-6140,CVE-2015-6141,CVE-2015-6142,CVE-2015-6143,CVE-2015-6144,CVE-2015-6145,CVE-2015-6146,CVE-2015-6147,CVE-2015-6148,CVE-2015-6149,CVE-2015-6150,CVE-2015-6151,CVE-2015-6152,CVE-2015-6153,CVE-2015-6154,CVE-2015-6155,CVE-2015-6156,CVE-2015-6157,CVE-2015-6158,CVE-2015-6159,CVE-2015-6160,CVE-2015-6161,CVE-2015-6162,CVE-2015-6164

CVE (通用弱點披露)

Common Vulnerabilities and Exposures

- CVE 為全球主要的弱點資料維護組織，收集各種資安弱點並給予編號以便於公眾查閱。
- CVE 現由美國非營利組織MITRE所屬的National Cybersecurity FFRDC所營運維護。
- 每一個經CVE確認的弱點披露都會賦予一個專屬的編號(格式：CVE-YYYY-NNNN)。
- CVE 弱點資訊為現今全球所公認的弱點參考標準。

The screenshot shows the CVE website interface. At the top, there is a navigation bar with links for 'CVE List', 'CNAs', 'Board', 'About', and 'News & Blog'. On the right, there is a 'NVD' section with links for 'Go to for: CVSS Scores', 'CVE Info', and 'Advanced Search'. Below the navigation bar is a search bar with buttons for 'Search CVE List', 'Download CVE', 'Data Feeds', 'Request CVE IDs', and 'Update a CVE Entry'. A status bar indicates 'TOTAL CVE Entries: 105419'. The main content area includes a description of CVE as a list of entries with identification numbers, descriptions, and public references. Below this are three main sections: 'CNA Participation Growing Worldwide' with a world map, 'Latest CVE News' with recent news items, and 'Newest CVE Entries' with a list of tweets from @CVEnew.

CVE Numbering Authorities (CNAs)

<https://cve.mitre.org/>

CVE 的注意事項



TIP!

- CVE不是唯一的弱點資料來源! (其他組織或製造商公佈, 例: 微軟MS)
- 多數的弱掃工具 是依據CVE公佈弱點資訊, 建立掃描檢測方式, 但各家的方法不盡相同.
- 掃描發現的弱點不一定具有CVE編號! (可能已發現存在攻擊威脅但尚未完成驗證階段, 亦可視為「未知威脅Unknow Threat」).
- 發現的弱點並須經過CVE組織確認驗證程序後, 才會給予CVE編號.
- 零日漏洞(Zero-day exploit 或 0-Day) 通常指「還沒有修補程式方法的漏洞」.
- 同一弱點威脅可能具備有多個CVE, 需視修補建議方式評估達成.

SMB弱點

CVE-ID	
CVE-2017-0144	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	

CVSS (通用弱點評分系統)

Common Vulnerability Scoring System

The screenshot shows the NIST NVD website. The header includes the NIST logo and 'NATIONAL VULNERABILITY DATABASE'. The main content area is titled 'Vulnerability Metrics' and features a large 'CVSS' logo. The text describes the CVSS as an open framework for communicating the characteristics and impacts of IT vulnerabilities. It mentions that CVSS is used for prioritizing remediation activities and calculating the severity of vulnerabilities. A sidebar on the left contains navigation links: General, Vulnerabilities, Vulnerability Metrics, Products, Configurations (CCE), Contact NVD, Other Sites, and Search. Below the main text, there is a section titled 'Using CVSS support within NVD' with numbered steps: 1. NVD CVSS v3 Calculator or NVD CVSS v2 Calculator, 2. Click on a CVSS score while viewing a vulnerability detail page to customize that score using temporal and environmental metrics, and 3. Download CVSS scores for all the NVD vulnerabilities from the NVD CVE feed.

<https://nvd.nist.gov/vuln-metrics/cvss>

NVD Vulnerability Severity Ratings

CVSS v2.0 Ratings		CVSS v3.0 Ratings	
Severity	Base Score Range	Severity	Base Score Range
Low	0.0-3.9	None	0.0
Medium	4.0-6.9	Low	0.1-3.9
High	7.0-10.0	Medium	4.0-6.9
		High	7.0-8.9
		Critical	9.0-10.0

- CVSS 由美國國家基礎建設諮詢委員會 (NIAC) 委託製作。
- 為目前全球主要的弱點評分標準。
- CVSS的評分標準包含多種項目所訂出弱點的危險分數。
- CVSS 評分從0分到10分, 0代表沒有發現弱點, 而10則代表最高風險。
- CVSS v3為最新的評分方式, 將弱點風險分成五個等級。
- 弱掃工具將CVSS所公布各個弱點的風險等級作為預設標準, 但使用者可依實際環境調整*。

Exploit-DB (可利用弱點資料庫)

- Exploit-db 為全球主要的可利用弱點資料庫，由知名資安訓練組織Offensive Security維護。
- 收集來自全球白帽提交的各類漏洞訊息及利用代碼。
- 資料類型包括4大類: Remote Exploits, Web Application Exploits, Local & Privilege Escalation Exploits, Denial of Service & PoC Exploits.

The screenshot shows the Exploit-DB website interface. The main heading is "Web Application Exploits" with a sub-note: "This exploit category includes exploits for web applications." Below this, it indicates "23,077 total entries" and provides pagination controls. A table lists various exploits with columns for Date, D (Download), A (Download Vulnerable Application), V (Verification), Title, Platform, and Author. Three red arrows originate from the table and point to callout boxes:

- An arrow from the 'V' column points to a box labeled "Verification".
- An arrow from the 'A' column points to a box labeled "Download Vulnerable Application".
- An arrow from the 'D' column points to a box labeled "Download Exploit Code".

Date	D	A	V	Title	Platform	Author
2018-08-02	✓	✓	✓	ASUS DSL-N12E C1 1.1.2.3_345 - Remote Command Execution	Hardware	Fakhri Zulkifli
2018-08-02	✓	✓	✓	Universal Media Server 7.1.0 - SSDP Processing XML External Entity Injection	XML	Chris Moberly
2018-08-02	✓	✓	✓	CoSocys Endpoint Protector 4.5.0.1 - Authentication	PHP	Ox09AL
2018-08-02	✓	✓	✓	PageResponse FB Inboxer Add-on 1.2 - 'search_field'	PHP	AkkuS
2018-08-02	✓	✓	✓	TI Online Examination System v2 - Arbitrary File Do
2018-08-02	✓	✓	✓	WityCMS 0.6.2 - Cross-Site Request Forgery (Passwo
2018-08-02	✓	✓	✓	Chartered Accountant : Auditor Website 2.0.1 - Cross-site scripting
2018-07-30	✓	✓	✓	H2 Database 1.4.197 - Information Disclosure	...	owodelta

<https://www.exploit-db.com/>

值得關注的可利用弱點 (Exploitable)



可被利用的弱點，威脅度大於高風險弱點！

iThome 新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安 Video 研討會 社群 搜尋

比WannaCry更狠！新網路蠕蟲EternalRocks現身，駭客利用7種NSA駭客工具攻擊Windows電腦

研究人員發現，除了勒索蠕蟲WannaCry之外，5月初發現新網路蠕蟲EternalRocks，同樣鎖定SMB漏洞來發動攻擊，但是，其他攻擊者也可以植入其他惡意軟體到遭受EternalRocks感染的電腦

WannaCry所使用的EternalBlue和DoublePulsar兩種駭客工具之外，還使用了其他NSA開發的5種駭客工具，包括EternalChampion、EternalRomance、EternalSynergy、ArchiTouch和SMBTouch等。

這7種駭客工具具有3個不同的用途，第一、EternalBlue、EternalChampion、EternalRomance和EternalSynergy專門攻擊SMB漏洞。第二、ArchiTouch和SMBTouch則是偵測目標電腦是否存在SMB漏洞。第三、駭客利用DoublePulsar傳播蠕蟲到其他存有SMB漏洞的Windows電腦。

根據Bleeping Computer表示，EternalRocks可能會繞過電腦防毒軟體的偵測，造成受害者不易察覺遭入侵。而且，它沒有設置kill switch的功能，快速在網路上掃描易遭攻擊的電腦IP，隨機發動攻擊。不僅如此，駭客能夠利用EternalRocks和其他惡意程式結合，如勒索軟體、銀行木馬、RATs和其他攻擊程式。

Exploit-db公佈可利用code及方法

Date	D	Title
2017-08-01	🟢	[Hebrew] Digital Whisper Security Magazine #85
2017-08-01	🟢	[Hebrew] Digital Whisper Security Magazine #84
2017-07-16	🟢	How to exploit ETERNALROMANCE/SYNERGY on Windows Server 2016
2017-07-12	🟢	Hidden Network: Detecting Hidden Networks created with USB Devices
2017-07-03	🟢	[French] SYN FLOOD ATTACK for IP CISCO Phone
2017-06-29	🟢	How to Exploit ETERNALBLUE on Windows Server 2012 R2
2017-06-29	🟢	[Spanish] How to Exploit ETERNALBLUE on Windows Server 2012 R2
2017-06-28	🟢	[Persian] Xpath Injection
2017-06-26	🟢	How to Write Fully Undetectable Malware - English Translation
2017-06-21	🟢	Blind SQL Injection Attacks
2017-06-19	🟢	[Italian] How to write Fully Undetectable malware
2017-06-15	🟢	Web Application Penetration Testing Techniques

弱點資訊參考資源

CVE Details
The ultimate security vulnerability datasource

Search: Search

View CVE

Enter a CVE id, product, vendor, vulnerability type... Search

Current CVSS Score Distribution For All Vulnerabilities

CVSS Score	Number Of Vulnerabilities	Percentage
0-3	302	3.9
1-2	673	8.8
3-3	2469	4.1
3-4	2171	2.8
4-5	17013	20.7
5-6	18557	19.6
6-7	12827	12.4
7-8	20279	21.7
8-9	252	0.4
9-10	12430	14.8
Total	84263	

Weighted Average CVSS Score: 6.8

<https://www.cvedetails.com/>

VULDB

HOME RECENT ARCHIVE STATS EXTRAS SEARCH LOGIN

CVSS Current Top 5

Top vulnerabilities with the highest CVSS9 temp scores at the moment. The score is generated by separate values which are called vectors. These vectors define the structure of the vulnerability. They rely on attack prerequisites and impact. The calculated score ranges between 0.0 and 10.0 whereas a high value denotes a high risk. The main score is the base score which analyzes the structure of the vulnerability only. The extended score called temp score introduces time-based aspects like exploit and countermeasure availability. Our researchers usually worry only to generate a CVSS score as accurate as possible.

- QEMU Cirrus CLGD Sbox VGA Emulator Heap-based memory co...
- Panorai Display SDK: posixenva.exe privilege escalation
- Active Directory Plugin Certificate Validation Man-in-the-Middle
- DHC Online Shop App X.509 Certificate Validation Man-in-the-M...
- haxme Service Cookie Store Share privilege escalation

Exploit Price Current Top 5

Top vulnerabilities with the highest exploit price at the moment. These price estimations are calculated prices based on mathematical algorithm. The algorithm got developed by our specialists over the years by observing the exploit market structure and exchange behavior of involved actors. It allows the prediction of generic prices by considering multiple technical aspects of the affected vulnerability. The more technical details are available the higher the accuracy of the reproducible approximation.

- Linux Kernel RDX entry_34.5 memory corruption
- Linux Kernel Efs Image (vme.c truncate_image_node) ...
- Linux Kernel Efs Image segment c_remove_entry_seg...

<https://vuldb.com/?>

tenable

Support Community Downloads Documentation Education Login

Newest Plugins

ID	Name	Product	Family	Severity
TT3287	Wreshart 22x < 2.236 / 24x < 2A.5 / 25x < 2.6.2 Multiple Vulnerabilities	Kessus	Windows	High
TT3286	Whoare Horizon View Agent 7.x < 7.5.3 Local Information Disclosure Vulnerability (CVE-2018-2076)	Kessus	Windows	Low
TT3285	OnSSI Crawler Recorder Installed	Kessus	Windows	Info
TT3284	OnSSI Crawler's Recorder 3.5 < Patch 10 / 5.x < Patch 19 / 5.3 < Patch 19 Denial of Service (DoS) Vulnerability	Kessus	Windows	Medium
TT3283	Google Chrome < 68.0.3403.95 Multiple Vulnerabilities	Kessus	Windows	High
TT3282	Google Chrome < 68.0.3403.95 Multiple Vulnerabilities	Kessus	MacOS X Local Security Checks	High
TT3281	Iron Project Local Security Bypass Vulnerability (CVE-2018-2056)	Kessus	Misc.	Low
TT3280	Iron Project s85 Deleg Exception Handling Local DoS (CVE-2018-2051)	Kessus	Misc.	Medium
TT3279	Iron Project s86 Passwords/Session Local DoS (CVE-2018-2054)	Kessus	Misc.	Low
TT3278	Coreex XenServer: Multiple Vulnerabilities (CVE-2018-2056)	Kessus	Misc.	Low
TT3277	Realt Reader < 3.2 Multiple Vulnerabilities	Kessus	Windows	High

<https://www.tenable.com/plugins>

TW CERT

關於我們 政策與法規 政策與法規 異業認證 政策與法規

日期 標題

2018-08-02	美國政府對中國黑客組織駭客組織的一名單人入黨	2018-08-02	Redfish 警告用戶進行安全更新: 該警告人來自美國政府官員
2018-08-01	中國政府公佈其駭客名單, 包括黑客組織	2018-08-01	德國政府: 確保信息安全, 保護用戶隱私
2018-08-01	中國政府駭客名單: NCCIP 公佈其駭客名單安全情報與報告	2018-08-01	英國政府警告 KIDCCO 駭客安全威脅: 警告 720 萬英國的 KIDCCO 駭客...
2018-08-01	英國政府駭客名單: 英國政府公佈其駭客名單	2018-07-27	越南政府駭客名單: 越南政府公佈其駭客名單
2018-08-01	美國政府駭客名單: 美國政府公佈其駭客名單	2018-07-24	新加坡政府的駭客名單: 新加坡政府公佈其駭客名單

新聞資訊

日期	標題
2018-07-30	倫敦駭客 ClamAV 安全更新: 駭客 ClamAV 安全更新: 駭客 ClamAV 安全更新...
2018-07-25	倫敦駭客 (vul) Reader 安全更新: 倫敦駭客 (vul) Reader 安全更新...
2018-07-24	倫敦駭客 (vul) Reader 安全更新: 倫敦駭客 (vul) Reader 安全更新...
2018-07-23	倫敦駭客 (vul) Reader 安全更新: 倫敦駭客 (vul) Reader 安全更新...
2018-07-20	倫敦駭客 (vul) Reader 安全更新: 倫敦駭客 (vul) Reader 安全更新...

研安活動

日期	活動類型	標題
2018-09-19	研討會	107 年資訊安全學術研討會: 資訊安全學術研討會...
2018-09-13	研討會	107 年資訊安全學術研討會: 資訊安全學術研討會...
2018-08-29	研討會	107 年資訊安全學術研討會: 資訊安全學術研討會...
2018-08-24	研討會	2018 年資訊安全學術研討會: 2018 年資訊安全學術研討會...
2018-08-24	研討會	2018 年資訊安全學術研討會: 2018 年資訊安全學術研討會...

<https://www.twcert.org.tw/Default.aspx>

善用網路資源查找資安資訊

- 國內主要IT資安媒體

The screenshot shows the iThome website with a navigation bar at the top containing links for 新聞, 產品評測, 技術, 專題, AI & Big Data, Cloud, DevOps, GDPR, 資安, and 研討會. The main content area features several news articles:

- WannaCry** (Large blue header)
- 美國直指肆虐全球的WannaCry勒索蠕蟲幕後黑手就是北韓!** (2017-12-19)
- 中華電信：臺灣今年第二季DDoS最大攻擊流量已經達到111Gbps** (2017-12-01)
- 比特幣分支增加獲利，WannaCry作者領光價值逾14萬美元的比特幣贖金** (2017-08-04)
- 又見勒索蠕蟲Petya鎖定**
- 本田因WannaCry被迫暫**
- 資安一周[0603-0609]：**

- 全球主要的搜尋引擎

The screenshot shows a Google search for "wannacry smb". Red annotations highlight the search bar, the "工具" (Tools) button, and the "國家地區" (Location) filter set to "台灣". The search results include:

- Microsoft 資訊安全公告MS17-010 - 重大 | Microsoft Docs**
<https://docs.microsoft.com/zh-tw/security-updates/securitybulletins/2017/ms17-010>
2017年10月11日 - Microsoft Windows SMB 伺服器的安全性更新(4013389); 提要: 受影響的軟體和弱點嚴重等級: 弱點資訊: 多個Windows SMB 遠端執行程式碼弱點; Windows SMB ...
- 美國直指肆虐全球的WannaCry勒索蠕蟲幕後黑手就是北韓! | iThome**
<https://www.ithome.com.tw/news/119724>
2017年12月19日 - WannaCry利用美國國安局 (NSA) 所開發的EternalBlue攻擊工具針對微軟Windows作業系統的伺服器訊息區域 (SMB) 漏洞展開攻擊, 它在今年5月12日於歐洲市場 ...
- 勒索軟體FAQ 問與答懶人包12個你不知道的祕密! [WannaCry重要必讀 ...]**
newguest88.pixnet.net/.../341976147-勒索軟體-faq-問與答懶人包-12個你不知道的...
2018年5月14日 - 這是 Microsoft 於2017/3/12 推出的SMB 安全性更新(安全補丁), 也就是事先防堵近期WannaCry 所利用的資安漏洞, 支援 Windows Vista、Windows Server ...

善用工具(1) Google 網頁翻譯



MS17-010: Security Update for Microsoft Windows (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya)

CRITICAL Nessus Plugin ID 97737

Synopsis

The remote Windows host

Description

The remote Windows host

- Multiple remote code execution vulnerabilities due to improper handling of certain requests. An attacker can craft a specially crafted packet, to execute arbitrary code on the remote host.

- An information disclosure vulnerability exists in the handling of certain requests. An attacker can disclose sensitive information.

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE and ETERNALSYNERGY are worms that utilize the vulnerabilities and exploit the remote code execution vulnerability. WannaCry is a ransomware that utilizes the remote code execution vulnerability in Microsoft Office, and the

Solution

Microsoft has released a security update for Windows XP, 2003, 2008, 2008 R2, 2012, 2012 R2, and 2016. Microsoft has also released a security update for Windows XP, 2003, 2008, 2008 R2, and 2016.

See Also

- <https://technet.microsoft.com/library/security/MS17-010>
- <http://www.nessus.org/u2321523eb>
- <http://www.nessus.org/u77bec1941>
- <http://www.nessus.org/u2d9f569cf>
- <https://github.com/stamparm/EternalRocks/>
- <http://www.nessus.org/u259db5b5b>



MS17-010 : Microsoft Windows SMB服務器安全更新 (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya)

CRITICAL Nessus 插件ID 97737

概要

遠程Windows主機受多個漏洞的影響。

描述

遠程Windows主機缺少安全更新。因此，它受以下漏洞影響：

- 由於對某些請求的處理不當，Microsoft Server Message Block 1.0 (SMBv1) 中存在多個遠程執行代碼漏洞。未經身份驗證的遠程攻擊者可以通過特製的數據包利用這些漏洞來執行任意代碼。(CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)。由於處理不當，Microsoft Server Message Block 1.0 (SMBv1) 中存在信息洩露漏洞。未經身份驗證的遠程攻擊者可以通過特製的數據包利用此漏洞來洩露敏感信息。(CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE和ETERNALSYNERGY於2017/04/14由一個名為Shadow Brokers的團隊披露的多個Equation Group漏洞和蠕蟲中的四個。WannaCry / WannaCrypt是利用ETERNALBLUE漏洞的勒索軟件程序，而EternalRocks是一種利用遠程代碼執行漏洞的蠕蟲。Petya是一個勒索軟件程序，首先使用CVE-2017-0109，這是Microsoft Office中的一個漏洞，然後通過ETERNALBLUE進行傳播。

解

Microsoft已針對Windows Vista, 2008, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 2012 R2和2016發布了一組補丁。Microsoft還發布了不再支持的Windows操作系統的緊急補丁，包括Windows XP, 2003和8。

也可以看看

- <https://technet.microsoft.com/library/security/MS17-010>
- <http://www.nessus.org/u7321523eb>
- <http://www.nessus.org/u77bec1941>
- <http://www.nessus.org/u2d9f569cf>
- <https://github.com/stamparm/EternalRocks/>
- <http://www.nessus.org/u259db5b5b>

插件詳細信息

嚴重性: 嚴重

ID : 97737

文件名: smb_int_ms17-010.nasl

版本: 1.22

類型: 本地

代理人: 窗戶

系列: Windows : Microsoft Bulletins

發佈時間: 2017/03/15

修改時間: 2018/07/30

依賴關係: 93962, 13855, 57033

風險因素

風險因素: 惡意

CVSS2

基本分數: 8.7

時間分數: 10

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

時間向量: CVSS2 # E : H / RL : OF / RC : C

CVSS3

基本分數: 9.8

時間分數: 9.4

向量: CVSS : 3.0 / AV : N / AC : L / PR : N / UI : N / S : U / C : H / I : H / A : H

時間向量: CVSS : 3.0 / E : H / RL : O / RC : C

漏洞信息

CPE : cpe / o : microsoft : windows

必需的KB項目: SMB / MS_Bulletin_Checks / 可稱

漏洞利用: 真實

漏洞利用: 漏洞利用可用

補丁發布日期: 2017/03/14

漏洞發布日期: 2017/03/14

可利用的

帆布 (CANVAS)

核心影響力

Metasploit (MS17-010 EternalBlue SMB遠程Windows內核池噴霧)

參考信息

善用工具(2) 商業弱掃廠商的資訊資源

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow. WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalBlue is a ransomware program that first utilized seven Equation Group vulnerabilities. Petya is a ransomware program that first utilized in Microsoft Office, and then spreads via ETERNALBLUE.

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, and Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, and Windows Server 2012 R2. Microsoft has also released emergency patches for Windows operating systems that include Windows XP, 2003, and 8.

See Also

- <https://technet.microsoft.com/library/security/MS17-010>
- <http://www.nessus.org/u7321523eb>
- <http://www.nessus.org/u77bec1941>
- <http://www.nessus.org/u2d9f569cf>
- <https://github.com/stamparm/EternalRocks/>
- <http://www.nessus.org/u259db5b5b>

NIST
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE

NVD

VULNERABILITIES

CVE-2017-0143 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

QUICK INFO

CVE Dictionary Entry: CVE-2017-0143
NVD Published Date: 03/16/2017
NVD Last Modified: 06/20/2018

Current Description

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

Source: MITRE
Description Last Modified: 03/16/2017

CANVAS (CANVAS)
Core Impact
Metasploit (MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption)

Reference Information

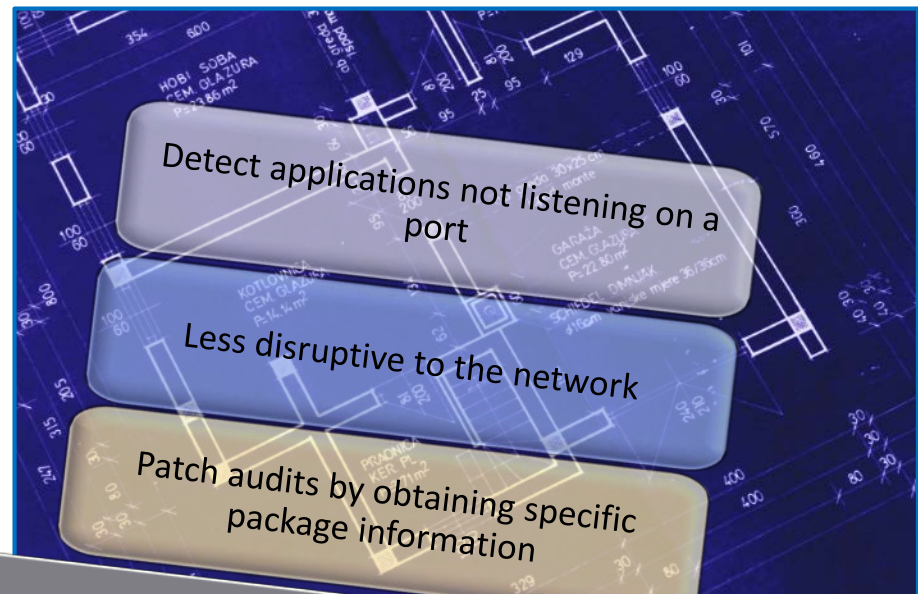
CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148
BID: 96703, 96704, 96705, 96706, 96707, 96709
MSFT: MS17-010
MSKB: 4012212, 4012213, 4012214, 4012215, 4012216, 4012217, 4012606, 4013198, 4013429, 4012598
IAVA: 2017-A-0065
EDB-ID: 41891, 41987

常見弱點掃描方式

網路掃描 (Network Scan)

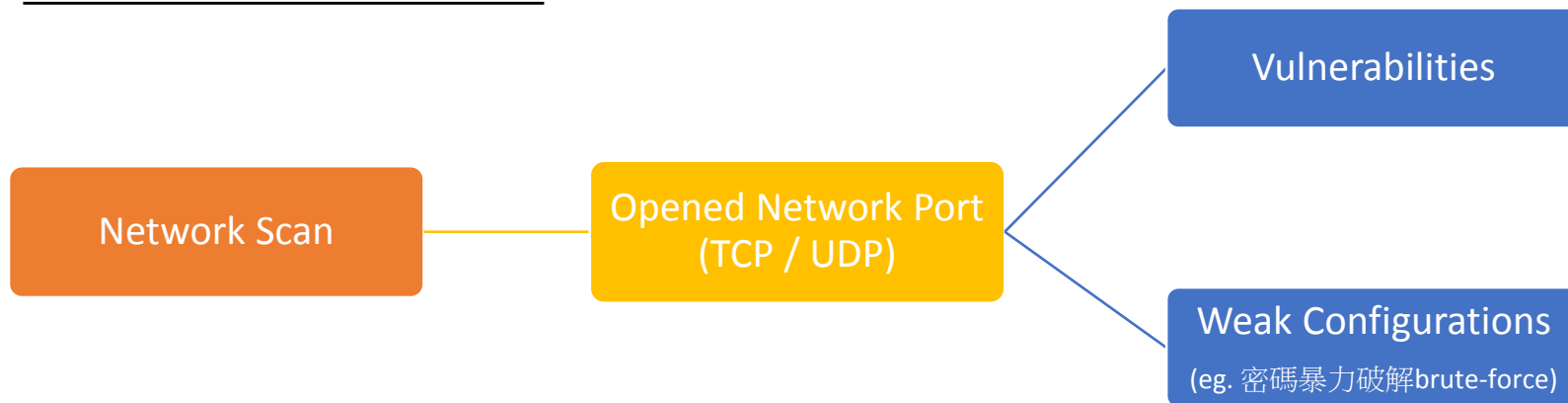


授權掃描 (Credential Scan)



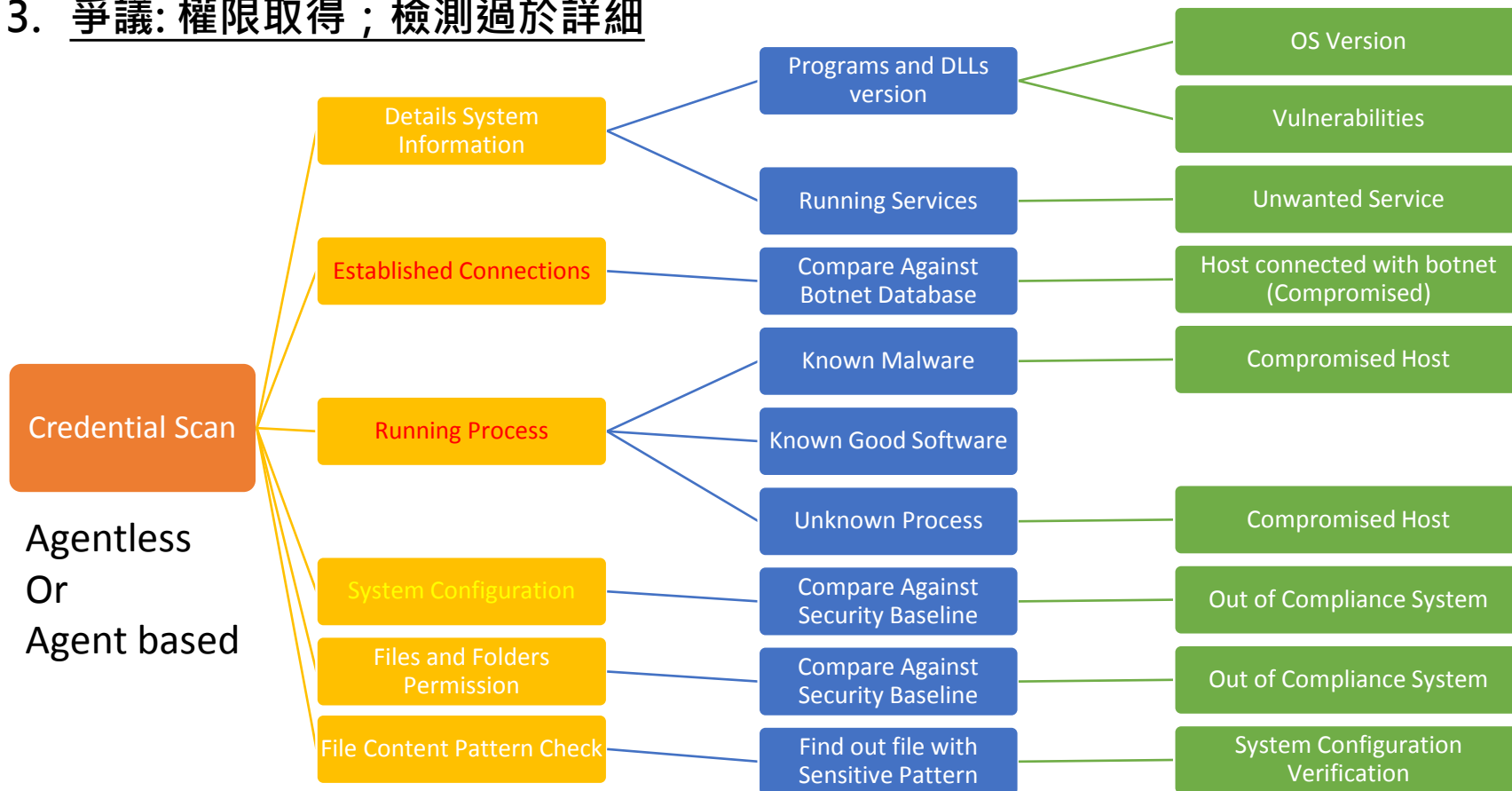
常見弱點掃描方式:網路掃描 (Network Scan)

1. 檢測目標系統存在使用的網路埠進行探測與比對
2. 也稱“基本掃描”
3. 爭議：識別的準確性問題



常見弱點掃描方式:授權掃描 (Credential Scan)

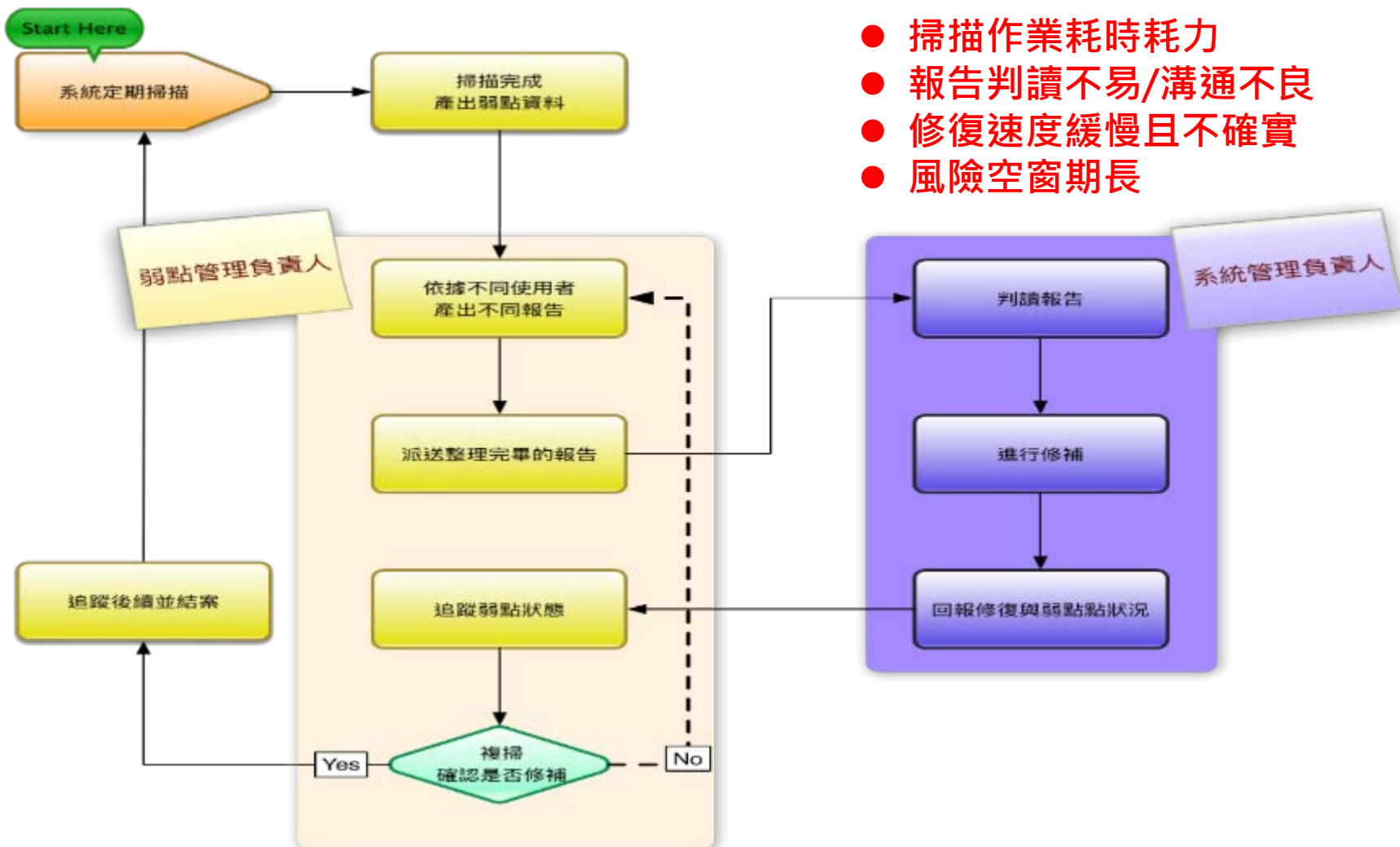
1. 授予權限登入目標系統進行檢測
2. 也稱 “深層掃描”
3. 爭議: 權限取得 ; 檢測過於詳細



大綱簡介

- 前言
- 為什麼一定要掃描
- 防毒軟體、弱點掃描、滲透測試的差異性
- 我收到了弱掃報告，可是看不懂
- 怎樣找到最合適自己的弱掃工具
- Q&A

弱掃執行的困擾



- 掃描作業耗時耗力
- 報告判讀不易/溝通不良
- 修復速度緩慢且不確實
- 風險空窗期長

合適自己的弱掃工具

● 弱掃的目的

- 任務導向: 系統弱掃 或 網站弱掃 或 更多類型 (應用程式, 網路設備, 資安設備, 聯網裝置 等)
- 需求導向: 資安管理需求? 資安事件需求? 一般合規需求? 合規稽核需求?

● 付費專業軟體 或 開源免費軟體

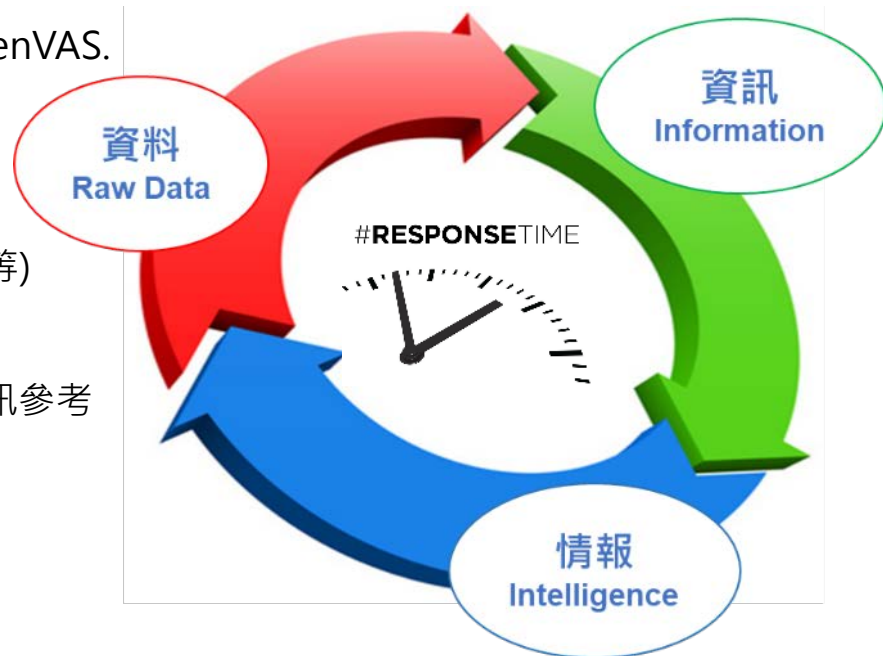
- 付費專業軟體: 例如 Tenable
- 開源免費軟體: 例如 Nmap/Zenmap 或 OpenVAS.

● 必須支援符合國際主要標準

- 具備最新且完整的CVE 弱點資料庫
- 支援 CVSS v3 評分標準資訊 及 風險等級(5等)
- 具備 Exploit Available (弱點可利用)資訊
- 具備Solution 修補解決方案建議 及 相關資訊參考

● 具有可自動化的管理方式

● 具有分析統計能力的報告方式



工具影響弱點管理方法的建立

資產群組建立:

- IP範圍型態
- 作業系統型態 (Windows, Linux, UNIX, 其他)
- 應用服務型態 (Web Application, Database, VM, 其他)
- 裝置類型 (Server, Network, IP Camera, NAS, Printer, 其他)
- 專案任務型態 (校務系統, 交易系統, 會員系統, 其他)

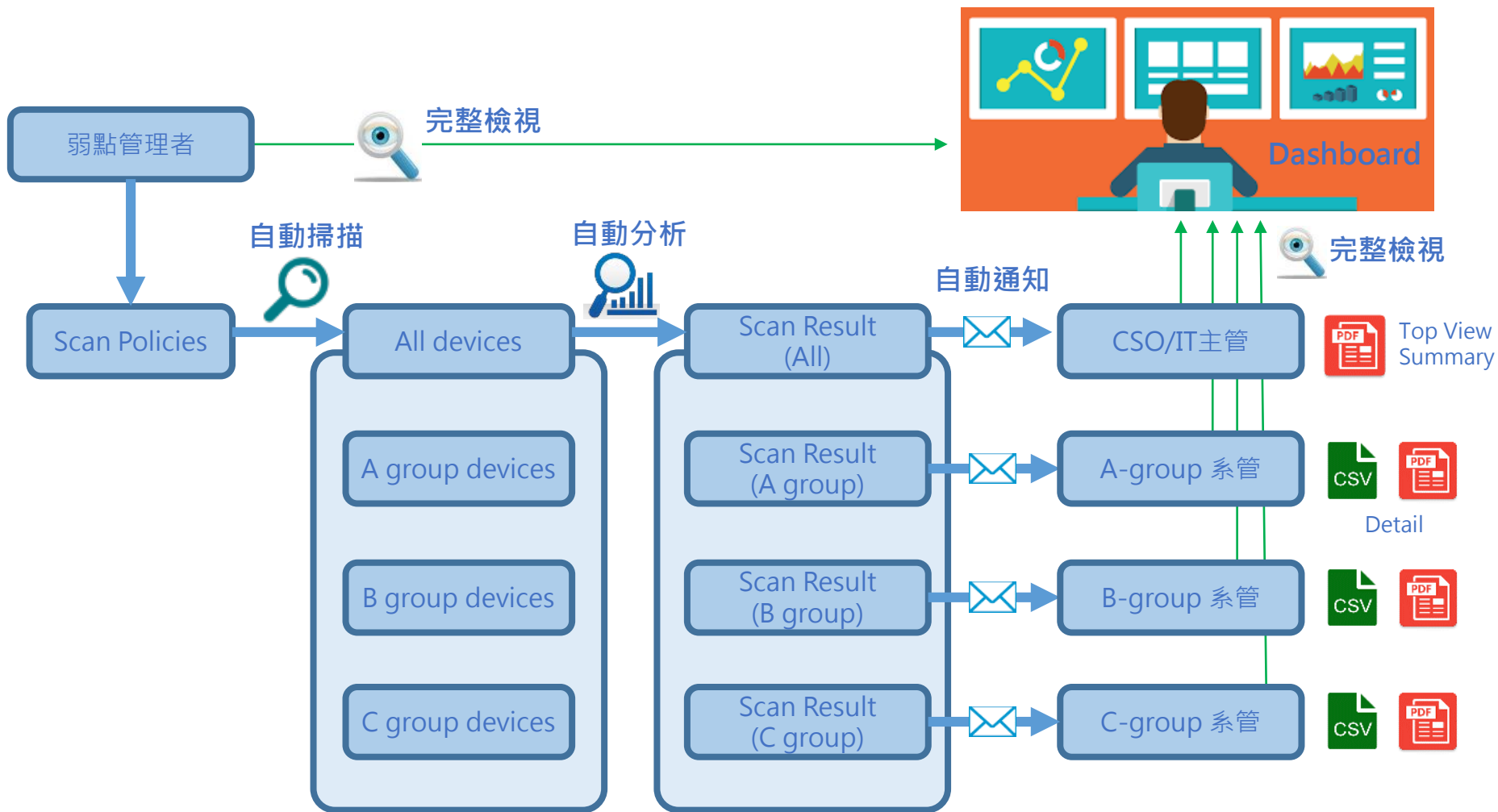
管理者群組建立:

- 群組: 網路(網段)、主機、系統、專案負責.
- 權限: 檢視權限、管理範圍、弱掃執行、風險管理

弱掃政策建立:

- 一般掃描政策.
- 進階掃描政策.
- 掃描頻率與週期

弱掃作業自動化

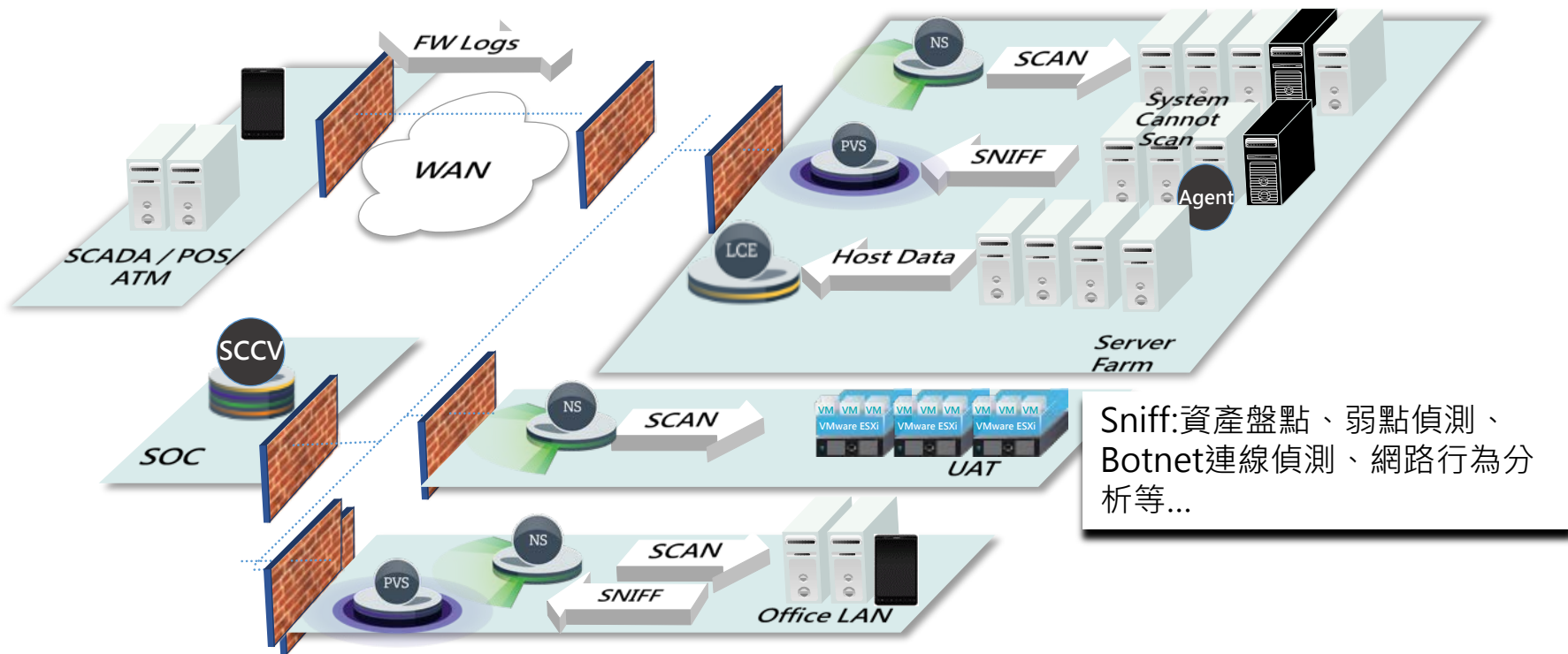


弱掃部署架構設計

分散式部署/集中化監控/分權管理模式

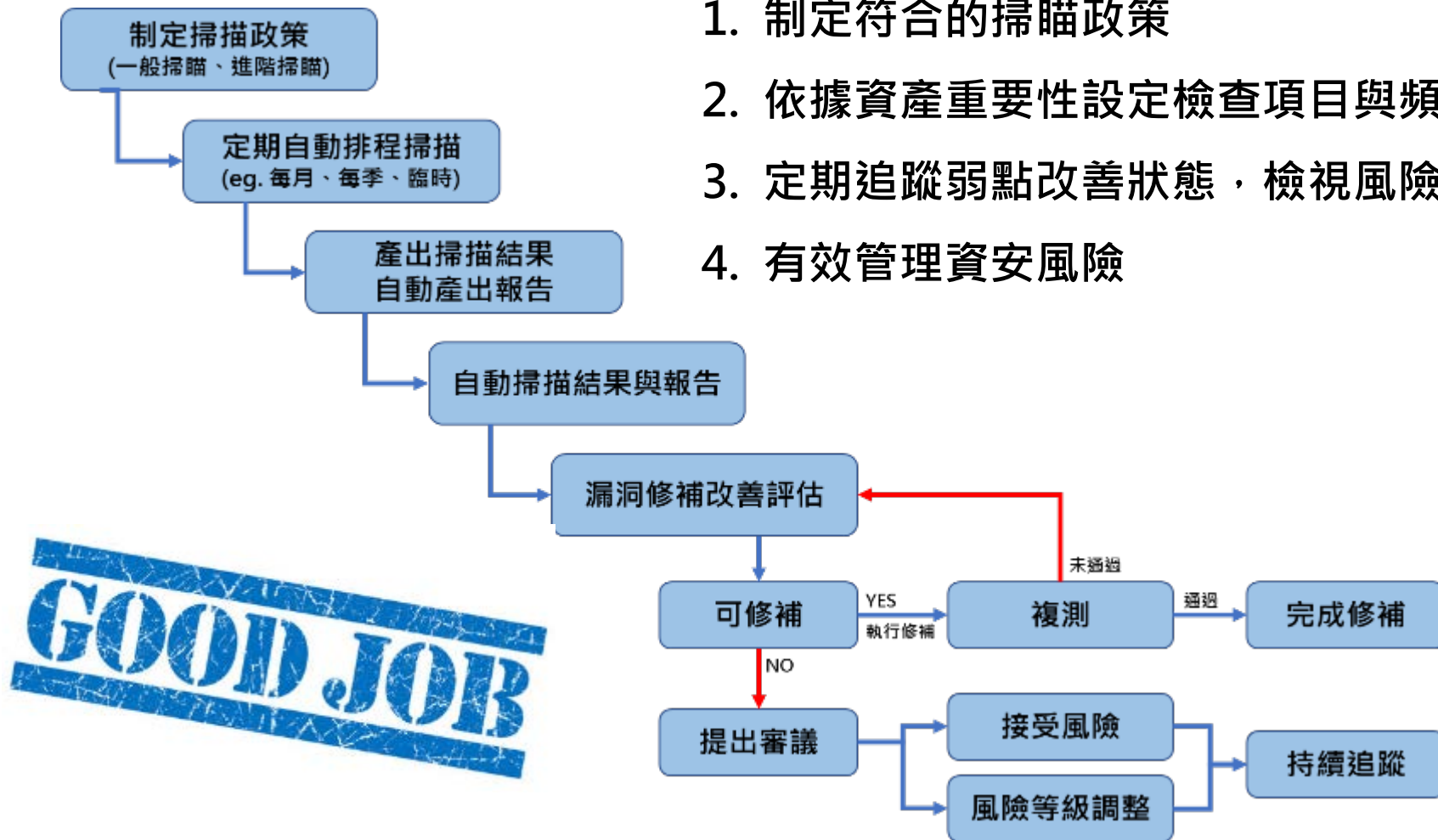
Host Data: 資產盤點、弱點偵測、主機活動等...

Scan: 資產盤點、弱點偵測、惡意程式偵測、設定檔稽核等...



配合資安治理政策，建立弱點風險管理機制

1. 制定符合的掃描政策
2. 依據資產重要性設定檢查項目與頻率
3. 定期追蹤弱點改善狀態，檢視風險程度
4. 有效管理資安風險



整體弱點狀態檢視

依風險等級統計

依嚴重等級的漏洞列表

依所有IP檢視漏洞列表

依所有漏洞列表

TopN 排行方式

Plugin ID	Name	Family	Severity	Tot
51192	無法信任 SSL 憑證	General	Medium	8
57582	SSL 自我簽署憑證	General	Medium	4
57608	需要 SMB 簽署	Misc.	Medium	3
85332	MS15-082: Vulnerability in RDP Could Allow Remote	Windows : Mi...	Medium	2

前10大IP列表

IP Address	Score	Repository	Total	Vulnerabilities
192.168.3.15	4112	DMZ	715	321 140 240
192.168.3.12	2046	DMZ	295	104 112
192.168.3.129	591	DMZ	154	90
192.168.3.132	140	DMZ	137	123
192.168.3.10	20	DMZ	90	82
192.168.3.1	18	DMZ	63	
192.168.3.2	3	DMZ	15	
192.168.3.254	1	DMZ	5	
192.168.3.3	0	DMZ	1	
192.168.3.4	0	DMZ	1	

Last Updated: 3 days ago

弱點分布情報快速檢視

SecurityCenter Dashboard Analysis Scans Reporting Assets Workflow Users

ibladmin

Switch Dashboard Options

整體漏洞趨勢

Vulnerability Trend - Severity Matrix

	Total
Past 24 Hours	0
Past 7 Days	1940
Past 30 Days	1940

Last Updated: 3 hours ago

Vulnerability Trend - New Vulnerabilities

Last Updated: 3 hours ago

可被利用比例

SecurityCenter Dashboard Analysis Scans Reporting Assets Workflow Users

ibladmin

Switch Dashboard Options

Vulnerability Trend - Vulnerabilities by Operating System

高風險漏洞檢視

Severity Trending

Last Updated: 2 hours ago

Vulnerability Trending

Last Updated: 2 hours ago

更精確的篩選出“嚴重”且“可被利用”的漏洞，應優先修補。

約26大可利用之嚴重及高風險等級漏洞排行

Plugin ID	Name	Family	Severity	Total
82826	MS15-034 ; HTTP.sys 中的漏洞可允許遠端程式碼執行 (3942563) (未經認證的檢查)	Windows	Critical	15
10295	ifcgi Service Detection	Service detection	High	11
79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (unauthenticated check)	Windows	Critical	7
69552	Oracle TNS Listener Remote Poisoning	Databases	High	7
87171	IBM WebSphere Java 物件遠端序列化 RCE	Web Servers	Critical	6
91896	PHP 5.6.x < 5.6.23 Multiple Vulnerabilities	CGI abuses	Critical	2
91442	PHP 5.6.x < 5.6.22 Multiple Vulnerabilities	CGI abuses	Critical	2
90921	PHP 5.6.x < 5.6.21 Multiple Vulnerabilities	CGI abuses	High	2
90361	PHP 5.6.x < 5.6.20 Multiple Vulnerabilities	CGI abuses	Critical	2
90008	PHP 5.6.x < 5.6.19 Multiple Vulnerabilities	CGI abuses	Critical	2

Last Updated: 2 hours ago

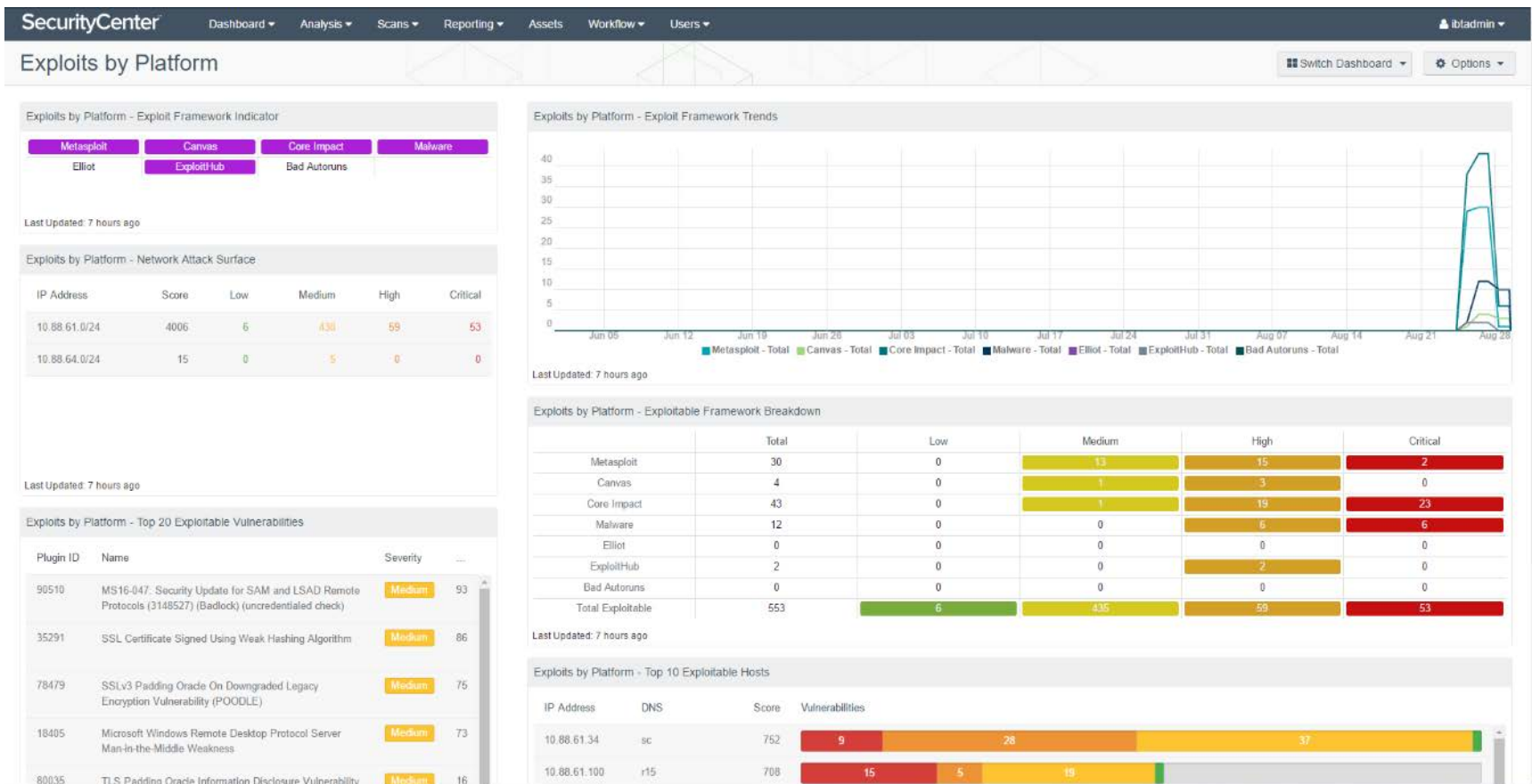
直接列舉風險度最高的IP主機，應優先檢視。

Top 10 IP Summary

IP Address	Score	Repository	Total	Vulnerabilities
10.88.61.100	650	IBT_Default	20	15 Critical, 6 High
10.88.61.34	640	IBT_Default	37	9 Critical, 28 High
10.88.61.87	90	IBT_Default	3	2 Critical, 1 High
10.88.61.64	80	IBT_Default	2	2 Critical
10.88.61.74	80	IBT_Default	2	2 Critical
10.88.61.81	80	IBT_Default	2	2 Critical

可利用弱點分析

可利用弱點套件(Exploitable)分析



弱點篩選過濾發現

內建多層的過濾條件, 直覺的操作介面, 加速各個管理者對於漏洞的分析與反應.

The screenshot displays the SecurityCenter interface for Vulnerability Analysis. The top navigation bar includes Dashboard, Analysis, Scans, Reporting, Assets, Workflow, and Users. The main content area shows a list of vulnerabilities with columns for Plugin ID, Name, Family, Severity, Host Total, and Total. Two filters are highlighted: 'Exploit Available' set to 'Yes' and 'Severity' set to 'Critical, High'. The vulnerability with Plugin ID 87171 is highlighted in red.

Filters:

- Exploit Available: Yes
- Severity: Critical, High

Vulnerability Table:

Plugin ID	Name	Family	Severity	Host Total	Total
82626	MS15-034 : HTTP.sys 中的弱點可允許遠端程式碼執行 (3042553) (未經認證的檢查)	Windows	Critical	12	15
79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (unauthenticated check)	Windows	Critical	7	7
87171	IBM WebSphere Java 物件序列化序列化 RCE	Web Servers	Critical	6	6
85887	PHP 5.6.x < 5.6.13 多個弱點	CGI abuses	Critical	1	2
88679	PHP prior to 5.5.x < 5.5.31 / 5.6.x < 5.6.17 Multiple Vulnerabilities	CGI abuses	Critical	1	2
88694	PHP 5.6.x < 5.6.18 Multiple Vulnerabilities	CGI abuses	Critical	1	2
91442	PHP 5.6.x < 5.6.22 Multiple Vulnerabilities	CGI abuses	Critical	1	2
91898	PHP 5.6.x < 5.6.23 Multiple Vulnerabilities	CGI abuses	Critical	1	2
76698	RHEL 6 : nss and nsspr (RHSA-2014.0917)	Red Hat Local Security Checks	Critical	1	1
81469	RHEL 6 : samba4 (RHSA-2015.0250)	Red Hat Local Security Checks	Critical	1	1
81470	RHEL 6 : samba (RHSA-2015.0251)	Red Hat Local Security Checks	Critical	1	1
81473	RHEL 6 : samba (RHSA-2015.0254)	Red Hat Local Security Checks	Critical	1	1
81474	RHEL 6 : samba4 (RHSA-2015.0255)	Red Hat Local Security Checks	Critical	1	1
84258	RHEL 6 / 7 : cups (RHSA-2015.1123)	Red Hat Local Security Checks	Critical	1	1
84788	RHEL 6 / 7 : java-1.7.0-openjdk (RHSA-2015.1229) (Bar Mitzvah) (Logjam)	Red Hat Local Security Checks	Critical	1	1

弱點資訊與建議取得

詳細的漏洞資訊、改建建議、及管理。

Critical IBM WebSphere Java 物件還原序列化 RCE (87171)

Synopsis
遠端 WebSphere Application Server 受到一個遠端程式碼執行弱點影響。

Description
遠端 IBM WebSphere Application Server 受到遠端程式碼執行弱點影響，這是因為未驗證的 Java 物件對 Apache Commons Collections (ACC) 程式庫進行不安全的還原序列化呼叫所導致。未經驗證的遠端攻擊者可惡意利用此弱點，傳送特製的 SOAP 要求，從而在目標主機上執行任意程式碼。

Solution
依照供應商公告，套用適當的過渡期修正。或者，確保 WebSphere Application Server 使用的所有暴露連接埠都會受到防火牆保護，免於來自任何公用網路的人侵。

See Also
Links:
[ibm.com](#)
[nessus.org](#)

Plugin Output
Nessus was able to exploit a Java deserialization vulnerability by sending a crafted Java object.

Discovery
First Discovered: 5 days ago
Last Observed: 5 days ago

Host Information
IP Address: 10.88.61.12 (8850 / TCP)
Repository: IBT_Default

Risk Information
Risk Factor: Critical
STIG Severity: I
CVSS Base Score: 10.0
CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:O/RC:N/D
CVSS Temporal Score: 8.3

Exploit Information
Patch Published: Nov 13, 2015
Exploit Available: Yes
Exploitability Ease: Exploits are available

Plugin Details
Plugin ID: 87171
Published: Dec 2, 2015
Last Modified: May 2, 2016
Family: Web Servers
Version: Revision 1.5
Type: remote

Vulnerability Information
Published: Jan 28, 2015

針對修補執行複測確認

Launch Remediation Scan Accept Risk Recast Risk

達到補強或補償性措施, 確保漏洞的威脅可獲得控制, 則漏洞風險可被接受(Accept Risk)或調整風險等級(Recast Risk).

漏洞問題描述, 將完全支援中文化.

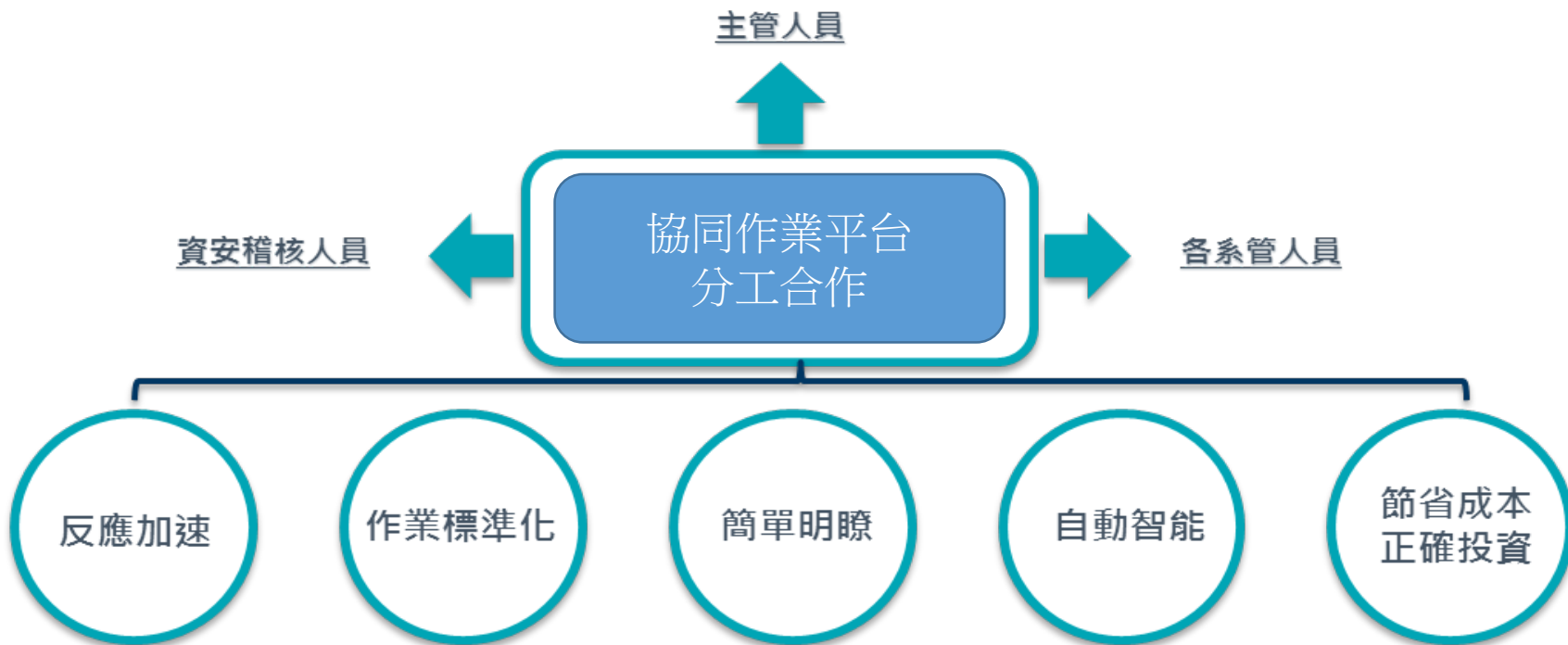
建議解決方案.

建議1. 漏洞修補
建議2. 利用防火牆保護

Plugin掃描執行結果

有助於發生具爭議或疑似誤判的掃描結果討論.

新型態弱掃管理的效益訴求



- ✓ 提升漏洞偵查速度
- ✓ 加快漏洞事件處理及回應速度

- ✓ 提供可標準化的漏洞管理方法
- ✓ 針對不同IT資產專案任務制定管理政策，並量化結果

- ✓ 將弱掃資料轉換成

- ✓ 提供自動化且具how-how方法
- ✓ 有效協助管理者漏洞修補順位及解決方法建議

- ✓ 節省處理作業的人力時間成本
- ✓ 準確的資安防護建設

**加速資安風險的處理回應
縮減風險空窗期**

Case Study

環境規模: 某金融單位國內外共計2000多台Server

傳統弱掃方式

WannaCry
事件通報

確認弱點資訊
(3天)

本次WannaCry事件的弱點資訊公布速度快，因此在設定漏洞掃描政策得以加快速度。但若以其他重大弱點未能有相關資訊可立即取得下，則必須耗費更多時間在弱點資訊的搜找與確認上。

執行弱點掃描作業
(15天)

現有弱掃工具為單一工作站，必須分區段逐一安排掃描作業，亦無法透過增派人力方式達到平行多工處理。由於掃描的主機數量多，容易拖緩弱掃工具本身的效能，或造成中斷。

弱掃結果彙整分析
(10天)

現行必須將各區段的弱掃結果透過人工方式個別彙整分析，並進一步依據資產規類比對後產出對應各系管人員的報告，再進行個別對應的案件通報。如需針對不同條件之統計分析，則所需耗費時間也會大幅增加。

弱點結果派送
(3天)

將弱點彙整的報告結果派送至各相關人員，並逐一通知及確認修補時程。

系統平台導入後弱掃方式

WannaCry
事件通報

確認弱點資訊
(1天)

本次專案弱掃系統廠商提供快速的情報資訊，弱點資料更新頻率為每日更新，可減少弱點資訊搜找的時間。

執行弱點掃描作業
(3-5天)

本次專案弱掃系統提供多個弱點掃描器的授權部署，並且可由中央管理設定排程自動執行掃描作業，並將掃描結果自動回報儲放於中央系統。並且可以僅針對指定的弱點項目(如本次WannaCry)進行指定盤查，可減少掃描作業對主機的耗能與時間。整體可加速弱掃速率，並減少作業所耗用的人力時間成本。

弱掃結果彙整分析
(1天)

本次專案弱掃系統於弱掃作業過程便已將結果回報儲放於中央系統資料庫，可直接套用相關的報告範本(如WannaCry)自動進行彙整及分析統計。可同時依據不同的管理者角色需求，產生對應的報告數據內容。具有專業的Know-How，大幅減少人工作業的時間，並且加速弱掃報告的提供。

弱點結果派送
(1天)

本次專案弱掃系統可針對資產對應建立弱掃結果派的規則，自動將弱掃報告透過email寄送給各相關人員。透過稽催功能可自動通知及確認修補時程，並進行追蹤與提醒。

縮減作業時間，加快反應速度
快速掌握弱點，降低風險空窗
提升資安效率，避免威脅損失



Case Study

提供重大威脅的弱點掃描政策，管理者可直接選用。

SecurityCenter SC Tenable SC PlayRoom

Dashboard ▾ Analysis ▾ Scans ▾ Reporting ▾ Assets Workflow ▾ Users ▾

Add Policy

Template

- Host Discovery
- Basic Network Scan
- Credentialed Patch Audit
- Web Application Tests
- Malware Scan
- Policy Compliance Auditing
- Internal PCI Network Scan
- SCAP and OVAL Auditing
- Dash Shellshock Detection
- GHOST (glibc) Detection
- PCI Quarterly External Scan
- DROWN Detection
- Badlock Detection
- Intel AMT Security Bypass Detection
- Shadow Brokers Scan
- WannaCry Ransomware Detection

影子擷客弱點掃描政策

WannaCry勒索掃描政策

提供相關的儀表板檢視範本，管理者可偵測已掃描結果進行快速過濾分析。

SecurityCenter SC Tenable SC PlayRoom

Dashboard ▾ Analysis ▾ Scans ▾ Reporting ▾ Assets Workflow ▾ Users ▾ Jim Huang ▾

Add Dashboard Template

影子擷客弱點偵測範本提供.

All ▾ shadow Q ← Back

- Shadow Brokers Vulnerability Detection
- Detecting WannaCry and EternalRocks

WannaCry及EternalRocks偵測範本提供.

Case Study

WannaCry及EternalRocks
偵測範本，自動針對已掃描
結果進行分析。

The screenshot shows the SecurityCenter dashboard with the following sections:

- WannaCry - Suspected and Confirmed Vulnerabilities:**

	Suspected	Confirmed (Ac)	Confirmed (Pa)	Confirmed (Ev)
Cumulative	4	2	0	0
Mitigated	2	2	0	-

Last Updated: Less than a minute ago
- WannaCry - Connection Summary:**

Source IP	Destination IP	Count
172.16.132.183	216.215.112.149	336
172.16.132.183	212.44.64.202	336
172.16.133.4	172.16.133.1	180
172.16.132.183	172.16.132.185	28
172.16.133.21	172.16.133.4	7
- Shadow Brokers - Codenamed Vulnerabilities and Exploits:**
 - DoublePulsar, EclipsedWing, EducatedScholar, EmeraldThread
 - EskimoRoll, Elomaf, Metasploit, PoisonIvy

Last Updated: Less than a minute ago
- Shadow Brokers - Unsupported and Outdated Products:**
 - Windows 2000, Windows XP, Windows Server 20, Windows Vista
 - Microsoft Exchange, SMBv1, IIS, Lotus Domino

Last Updated: Less than a minute ago
- Executive Summary - Outstanding Patches by Operating System:**

Family	Sc...	I...	Low	H...	T...
--------	-------	------	-----	------	------

自動套用WannaCry相關
的弱點項目進行過濾。

The screenshot shows the Vulnerability Analysis page with the following details:

- Filters:**
 - CVE ID: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148
 - Plugin Type: Active
 - Address: All
 - Plugin Name: (empty)
- IP Summary:**

IP Address	NetBIOS	Score	Total	Vulnerabilities
172.16.132.185	TESTLAB\DEMO2K3	80	2	2
172.16.132.186	WORKGROUP\AD-WIN8	80	2	2
- Options:** Jump to Vulnerability Detail List, Total Results: 2

自動比對過濾出存在WannaCry弱點的主機IP。

Case Study

效益

1. 透過WSUS 派送更新相關的修補程式.
2. 透過弱掃系統Tenable SC 稽核修補完整性，並發現存在弱點系統.
3. 結合資安防護系統，針對主要弱點加以偵測防護，防止內部橫向擴散.
4. 達成 提早預防、持續監測、全面防護的最大資安防護網.

The screenshot shows the Check Point SmartDashboard interface. The top navigation bar includes 'Install Policy', 'SmartConsole', and '593/593'. The main menu contains various security modules: Data Loss Prevention, IPS, Threat Prevention, Anti-Spam & Mail, Mobile Access, IPSec VPN, Compliance, and QoS. The 'Protections' section is active, displaying a search filter 'Look for: MS17-010' and a dropdown menu set to 'All'. Below the search bar, a table lists several protection rules for Microsoft Windows SMB vulnerabilities. The 'Default_Protection' and 'Recommended' columns for these rules are highlighted with a red box, showing 'Prevent' actions.

Protection	Confide...	Perf...	Industry Refere...	Relea...	?	?	?	Default_Protection	Recommended
Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-0143)	Medium	Med...	CVE-2017-0143	3/14/2017	?	?	?	Prevent	Prevent
Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-0144)	Medium	Med...	CVE-2017-0144	3/14/2017	?	?	?	Prevent	Prevent
Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-0145)	Medium	Med...	CVE-2017-0145	3/14/2017	?	?	?	Prevent	Prevent
Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-0146)	Medium	Med...	CVE-2017-0146	3/14/2017	?	?	?	Prevent	Prevent
Microsoft Windows SMB Information Disclosure (MS17-010: CVE-2017-0147)	Medium	Med...	CVE-2017-0147	3/14/2017	?	?	?	Prevent	Prevent
Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-0148)	Medium	Med...	CVE-2017-0148	5/16/2017	?	?	?	Prevent	Prevent

“天下武功无坚不摧，
唯快不破！”

—— 李小龍



Q&A

