

保安漏洞掃描軟件概覽

2008 年 2 月

©香港特別行政區政府

這份文件的內容為香港特別行政區政府的財產，未經香港特別行政區政府的明文批准，不得轉載全部或部份文件內容。

免責聲明：政府盡力確保本文資料準確，但不明示或隱含保證資料準確無誤。對於因使用本文資料而引致或與之有關的任何錯誤或遺漏，香港特別行政區政府概不承擔任何法律責任。

目錄

摘要.....	2
I. 保安漏洞掃描軟件的基本概述.....	3
什麼是保安漏洞掃描軟件？	3
保安漏洞掃描軟件的好處	3
保安漏洞掃描軟件的限制	3
II. 保安漏洞掃描軟件的結構	5
III. 保安漏洞掃描軟件的種類	7
網絡掃描軟件	7
主機掃描軟件	7
IV. 考慮事項	8
選擇保安漏洞掃描軟件	8
操作事宜	8
一般保安漏洞掃描軟件的例子	10

摘要

保安漏洞掃描軟件（**vulnerability scanner**）評估網絡或主機系統的保安漏洞，並得出一套掃描結果。因為管理人員及攻擊者都可以採用同樣的工具去糾正或入侵系統，所以管理人員要在攻擊者掃描及攻擊保安漏洞前，先行掃描及糾正問題。本文將概覽保安漏洞掃描軟件。

I. 保安漏洞掃描軟件的基本概述

什麼是保安漏洞掃描軟件？

保安漏洞掃描軟件可以偵測到資訊系統（包括電腦、網絡系統、操作系統以及應用軟件）各種保安漏洞。這些保安漏洞可能源於軟件生產商、系統管理活動或用戶一般日常活動：

1. 源於生產商：包括軟件錯誤、操作系統欠缺修補程式、服務出現保安漏洞、不安全的預設配置以及網上應用系統保安漏洞。
2. 源於系統管理：包括不正確或未經授權改變系統配置、欠缺密碼保護政策等。
3. 源於用戶：包括跟未經授權方分享目錄、沒有執行掃描電腦病毒的軟件、以及故意引入系統後門等惡意活動。

保安漏洞掃描軟件的好處

首先，保安漏洞掃描軟件可以及早偵測到已知的保安問題及加以處理。利用保安漏洞掃描軟件持續作保安評估，可以很容易辨認出網絡內外的保安漏洞。

其次，新的設備甚至是新系統可能未經批准便跟網絡連接。保安漏洞掃描軟件便可以協助辨認出有可能危及整體系統及網絡保安的虛假機器（**rogue machine**）。

第三，保安漏洞掃描軟件可以驗證網絡上所有設備的清單。這清單包括設備類別、操作系統版本及程式修補程度、硬件配置及系統其它相關資訊。這些資料對保安管理及追蹤是很有用的。

保安漏洞掃描軟件的限制

保安漏洞掃描軟件的缺點包括：

1. 只能提供快照（**snapshot**）：保安漏洞掃描軟件只能夠評估一個短時期內有關係統或網絡保安的狀況。由於新的保安漏洞的不斷出現，以及改變系統配置亦可能導致保安漏洞，所以定期執行掃描是必須的。
2. 需要人為判斷：保安漏洞軟件只能根據數據庫預裝的插件（**plug-in**）來報告保安漏洞。它們不能決定掃描結果是假陰性（**false negative**）或是假陽性（**false positive**）

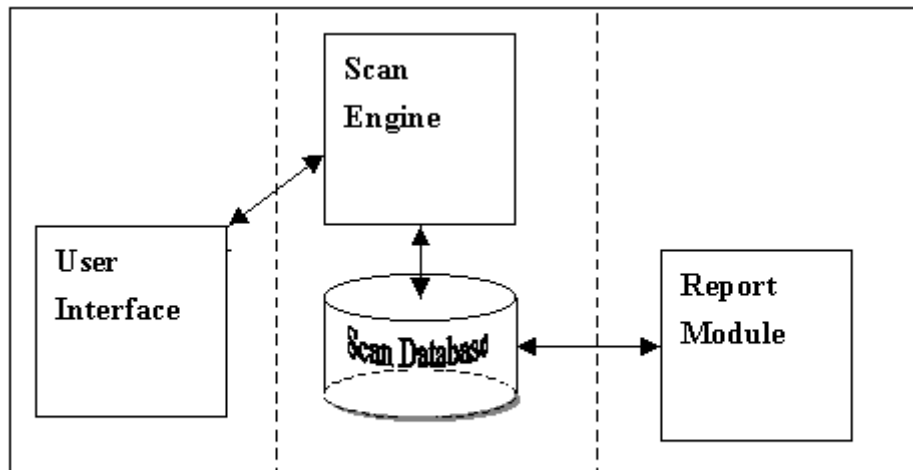
- ¹。每次掃描完成後，數據都要經人為判斷。
3. 其它：保安漏洞軟件只能發現已知的保安漏洞，它不能辨認出其它保安威脅，例如那些實體、操作或程序上的威脅。

此外，很多保安漏洞掃描軟件都要靠插件來找出潛在的保安漏洞。插件是掃描軟件所能偵測到的漏洞知識數據庫（或掃描數據庫）其中一部份。不同掃描軟件產品的數據庫可能有不同的名稱（例如「掃描配置檔案」(Scanning Profile)），但本文將一律稱之為「插件」。保安漏洞掃描軟件有限的插件數目可以是另外一個缺點。掃描軟件只能根據所安裝的對應插件組為參照，檢查其「所知」的保安漏洞。它不能辨認出那些欠缺對應插件的保安漏洞。然而，並非所有掃描軟件都需要插件的，比如說，埠掃描軟件便不需要插件，因為掃描只是以一定範圍的埠為目標。

¹ 就着保安漏洞掃描來說，「假陰性」指的是，未能辨認出所評估的系統或網絡的弱點；而「假陽性」所指的是，錯誤指出存有漏洞。前者可能因基於掃描數據庫欠缺某些插件，而後者則有待人工判斷加以確認。

II. 保安漏洞掃描軟件的結構

一般而言，保安漏洞掃描軟件由四個主要部份所組成，即掃描器（Scan Engine）、掃描數據庫（Scan Database）、報告模組（Report Module）、以及用戶界面（User Interface）。



Components of Scanner

1. 掃描器根據所安裝的插件，執行保安檢查，以辨認出系統資訊及保安漏洞。它可以同時間掃描多個主機，並將結果跟已知的保安漏洞加以比對。
2. 掃描數據庫儲存了有關保安漏洞的資料、掃描結果以及其它掃描器用到的資訊。插件數目以及更新頻率視乎軟件售賣方而定。每一個插件除了包括所測試個案外，也包括保安漏洞的描述、以及通用保安漏洞(Common Vulnerabilities and Exposures (CVE))² 辨識，甚至包括如何修補偵測到的保安漏洞指引。擁有自動更新功能的掃描軟件可以自動下載並將最新的插件安裝到數據庫。
3. 報告模組對掃描結果提供不同程度的報告，例如包括對系統管理員建議糾正方法的詳盡技術報告；以保安主管為對象的摘要報告；以行政人員為對象的高級圖表及趨勢報告。
4. 用戶界面則讓管理人員操作掃描器，那可以是圖像用戶界面，或只是指令界面。

大部份的掃描軟件的構成都如上所述。但亦有一些原始的掃描軟件，基本上只是一套程式或 C-code，掃描結果只是簡單的純文字檔案，這類軟件的更新並不頻密，有需要人手介入。

² <http://cve.mitre.org/>

另外，現時分佈式網絡掃描軟件的結構更為複雜。當企業網絡分佈範圍甚廣時，便會用到分佈式網絡掃描軟件，這類軟件由遠程掃描代理程式、代理程式的插件更新機制，以及中央管理點所組成。它們能夠從中央管理控制點，評估分佈不同地點網絡的保安漏洞，更新掃描代理程式，調校所有掃描器的設定，以及為整個企業定期測試。中央數據庫會從所有掃描代理程式收集掃描結果，加以分析及報告。

III. 保安漏洞掃描軟件的種類

保安漏洞掃描軟件大致可分為兩種：應用於網絡的網絡掃描軟件，其次為應用於主機掃描軟件。

網絡掃描軟件

網絡掃描軟件通常安裝在一部電腦上，掃描網絡上其它主機。它可以偵測重大的保安漏洞，例如配置不當的防火牆、有保安漏洞的互聯網伺服器、供應商提供的軟件所附帶的風險，以及網絡及系統管理附帶的風險等。

網絡掃描軟件包括以下幾種：

1. 埠掃描軟件，確定遠程系統的網絡埠清單。
2. 互聯網伺服器掃描軟件，評估遠程互聯網伺服器是否有可能的保安漏洞（例如潛在危險的檔案或共用網間連接界面（CGI））。
3. 網上應用系統掃描軟件，用來評估在互聯網伺服器上運作的網上應用系統軟件的保安（例如跨網址程式編程攻擊及 SQL 插入攻擊（SQL injection））。應注意網上應用系統掃描軟件並不能為指定的網上應用系統作全面的保安檢查。為了測試網上應用系統，有需要作額外的手動檢查（例如多次登入嘗試無效後，登入戶口是否會被鎖上）。

主機掃描軟件

主機掃描軟件是安裝在需要掃描的主機上，可以直接接達低層次數據，例如主機操作系統的具體服務及配置細節。它能夠洞察用戶高危活動，例如使用容易被猜出的密碼甚至沒有密碼。它會偵測攻擊者已經危及系統的跡象，包括尋找可疑檔案名、出乎意料的新系統檔案或設備檔案，及高權限程式。主機掃描軟件亦可以進行基準（或系統檔案）檢查。因為網絡掃描軟件不能直接接達目標主機的系統檔案，所以不能進行這層次的保安檢查。

數據庫掃描軟件是主機掃描軟件的一種。它對授權、認證以及數據系統的完整性提供詳盡的保安分析，亦可以辨認出數據庫系統潛在的保安漏洞，包括簡單的密碼、錯誤的保安配置以及特洛伊木馬。

IV. 考慮事項

選擇保安漏洞掃描軟件

選擇保安漏洞掃描軟件時應考慮以下因素：

1. 更新頻率及插件更新方法

若欠缺相應的插件，保安漏洞掃描軟件通常無法辨認出有關保安漏洞。因此，軟件生產商若能及時提供更新及新插件，掃描軟件便越能有效偵測出新的保安漏洞。再者，有自動更新功能的掃描軟件能自動定期下載及安裝最新的插件，選擇保安掃描軟件時應加以考慮這一點。

2. 偵測漏洞的質和量

由於掃描軟件可能會把同一保安漏洞計算多次，軟件能否準確辨認出重大保安漏洞，比偵測出的保安漏洞數目更為重要。保安漏洞數目是否有效，可以參照通用漏洞（Common Vulnerabilities and Exposures (CVE)）³的標準保安漏洞及其他保安漏洞名單作比對。CVE的內容是CVE委員會的協作成果。

3. 掃描報告的水平

除了提供所偵測的保安漏洞資料外，一份有用的掃描報告要提供清楚簡明的糾正方法。若管理人員完成初步掃描或改變配置後要再作掃描，又或需要比較掃描結果，配備後端數據庫的掃描軟件便較為合適，因為它把掃描結果存檔作趨勢分析。

操作事宜

以下是進行保安漏洞掃描前要考慮的事宜：

部署的實務作業

掃描軟件的位置（適用於網絡掃描軟件）

掃描軟件處於防火牆之內還是外面，會影響掃描結果。自防火牆外對內部網絡進行掃描，只能偵測到外面可供使用的設備。因為防火牆的保護，內部網絡的漏洞並不能偵測

³ <http://cve.mitre.org/>

到。另一方面，由內部掃描 DMZ 主機未必可能提供全面的保安狀況。因此，爲了得到較完整的保安狀況，進行內外掃描是有需要的。

埠掃描的範圍（適用於網絡掃描軟件）

埠掃描能夠偵測出哪些埠是可供使用的（即服務正在聆聽的那些埠）。因爲公開的埠可能意味着保安弱點，埠掃描往往是攻擊者的一項偵察技術。因此保安漏洞掃描必須包括埠掃描。然而，一些保安漏洞掃描軟件已預設埠掃描範圍，例如只掃描 0 至 15000 的埠，系統管理員有需要知道預設埠掃描範圍，以確保所有必須被掃描的埠都包括在內。

設置底線

一般的保安漏洞掃描應包括初步評估、執行建議糾正，以及再次評估。爲確定糾正是否有效，較妥當的做法是保存所有掃描記錄（即制訂一個有效的準則），然後將每次的掃描結果跟準則比對，以進行趨勢分析。

掃描後及持續措施

掃描過程只是良好評估的一部份，正確詮釋掃描結果是重要的，因爲這才可以確保保安漏洞能獲辨認及修正。跟進行動的優先次序應同時予以制訂。

爲此，保安漏洞掃描及掃描後的跟進一定要有周全的保安政策配合，才能真正糾正發現的保安漏洞。此外，頻密掃描亦是關鍵。每當實施修補程式、改變配置，或安裝新軟件後，都應再掃描系統一次；或定期進行掃描。

預防措施

掃描過程的潛在威脅

掃描對資訊科技系統可以構成威脅，例如所有插件（包括高風險的插件，如拒絕服務掃描）都啓動時，掃描可能會令脆弱的伺服器崩潰。所以進行掃描前有需要作風險評估及周全計劃。通常，就一個未投入生產的系統而言，掃描時可以啓動包括高風險在內的插件；但若要對生產系統持續進行掃描，管理人員該考慮關掉一些高風險插件。

此外，利用網絡保安漏洞掃描軟件進行掃描時，會產生大量系統要求及網絡傳輸。進行掃描時，管理人員要注意若干群組的系統及的網絡的性能有沒有下降。

處理掃描結果

掃描結果包括系統漏洞的資訊，萬一外泄便會容許攻擊者直接針對漏洞發動襲擊。因此應把掃描結果保管在安全的地方，或予以加密防止未經授權的接達。若評估程序涉及第三者，機構有需要確保對方可信賴程度，而評估所發現的資料及專利的資訊便須安全地保存。

掃描過程的政策及程序

惡意或不恰當使用掃描工具對資訊系統可以構成重大威脅，甚或導致極大傷害。因此，有需要因應保安漏洞評估工具由誰使用、如何及何時使用而制定政策及程序。在進行掃描前，有關政策規定可能包括預先的安排或通知，獲得管理層批准甚至是法律批准。沒有人可以在未經批准下進行保安漏洞掃描。

一般保安漏洞掃描軟件的例子

開放源碼的免費軟件或商業保安漏洞掃描軟件可供下載或試用。以下是一些例子：

1. 網絡掃描軟件

- 埠掃描軟件
 - Nmap : <http://insecure.org/nmap/>
 - Superscan:
<http://www.foundstone.com/us/resources/proddesc/superscan4.htm>
- 網絡保安漏洞掃描軟件
 - Nessus : <http://www.nessus.org/nessus/>
 - GFI LANguard Network Security Scanner (N.S.S.) (commercial) :
<http://www.gfi.com/languard/>
- 互聯網伺服器掃描軟件
 - Nikto : <http://www.cirt.net/code/nikto.shtml>
 - Wikto : <http://www.sensepost.com/research/wikto/>
- 網上應用系統保安漏洞掃描軟件
 - Paros : <http://parosproxy.org/index.shtml>
 - Acunetix Web Vulnerability Scanner (commercial) :
<http://www.acunetix.com/>

2. 主機掃描軟件

- 主機保安漏洞掃描軟件
 - Microsoft Baseline Security Analyser (MBSA)
<http://www.microsoft.com/technet/security/tools/mbsahome.msp>
 - Altiris SecurityExpressions (commercial) :
<http://www.altiris.com/Products/SecurityExpressions.aspx>

- 數據庫掃描軟件
 - Scuba by Imperva Database Vulnerability Scanner:
http://www.imperva.com/application_defense_center/scuba/default.asp
 - Shadow Database Scanner
<http://www.safety-lab.com/en/products/6.htm>

重要事項：在任何網站登記，或下載及安裝任何軟件前，請先仔細閱讀相關條款及條件。此外，請注意執行掃描工具存有風險（例如當執行拒絕服務掃描時，脆弱的伺服器可能會崩潰）。掃描必須小心計劃及執行。掃描前應先預先安排及通知，例如取得管理層批准，甚或法律許可。顯然易見，切勿對非屬於你所管理的網絡進行掃描。