結合弱點掃描和滲透測試之自動化 Web 安全檢測系統設計與實現

An Automated Web Application Security Testing System Combined with Vulnerability Scanning and Penetration Testing

柯鈞凱
國立高雄師範大學資訊教育研究所 研究生
outsidecastle66@gmail.com
楊中皇
國立高雄師範大學資訊教育研究所 教授
chyang@computer.org

摘 要

網路時代的來臨，網路建設也日益普及，使我國社會日益資訊化。但資訊化的結果除了帶來生活上的便利外，安全問題也越來越多。然而，越是依賴網路，網路安全範疇的問題越是不能忽視，各種利用網路進行攻擊的事件時時刻刻都在發生，作業系統和網站的漏洞抓不勝抓，然而這些威脅已是現今網路使用者最在意的議題之一。

本研究利用開放原始碼實作了一整合系統結合網路探測、弱點掃描及滲透測試等工具，針對 Web 安全做自動化的檢測，並製作一個 Live DVD/Live USB 環境，不限定任何作業系統環境，使用者只須要將光碟片放入光碟機，且不需安裝於硬碟上，即可快速進行自動化的 Web 安全檢測工作，也不會更動到原有系統及設定，對於初學使用者的門檻也大大降低，減少學習摸索的時間，加速使用者對 Web 安全檢測熟悉的程度，對於資安人員也可以減少檢測的時間，更於專心分析工作，並利用此環境做到快速使用安全工具來保護系統。

關鍵詞：網路安全、開放原始碼、網路探測、弱點掃描、滲透測試

一、 前言

在美國網站安全聯盟 (Web Application Security Consortium, WASC) 2008 年 9 月指出每個網站平均有 13.11 個漏洞(包括 8.91 個嚴重漏洞)[7]，因此我們可以透過 Web 安全測試來了解系統上的弱點、漏洞，藉此對該漏洞進行修補的動作。

在網路安全漸漸受到普羅大眾的重視，而各類的安全工具也在網路上相當快速的發展，但目前網路上的安全工具以執行於 Linux 環境為大多數，因此資訊安全人員必需要熟悉 Linux 環境才能順利使用，另外；各類型的安全工具皆有各自呈現報表的方式，可能會有 HTML、XML 亦或只是在終端機上面呈現，而要如何整合與統整是相當麻煩的問題，最後是平台的部署問題，當如果要在多種平台上操作，是否能夠順利運行。

為了解決這個不便，所以本研究建置一套可移動式的作業平台，本研究亦蒐集整理許多知名的安全工具，並分門別類與此平台整合，最後實作了一整合系統，針對 Web 安全做自動化的檢測，只須要輸入目標之 URL，並藉著 Live DVD/Live USB 的平台即可馬上使用自動化檢測工具來做掃描，藉著 Live DVD/Live USB 即可讓電腦成為一台自動化的 Web 安全檢測裝置[9]，可以馬上進行檢測工作，並產生統整報表。

二、 文獻探討

(一) 網路安全檢測

1. 網路掃描

網路安全掃描技術是一種基於 Internet 遠端檢測目標網路或本地主機脆弱安全性的技術。通過網路安全掃描，系統管理員能夠發現所維護的 Web 伺服器各種 TCP/IP 埠的分配、開放的服務、Web 服務軟體版本和這些服務及軟體呈現在

Internet 上的安全漏洞。

網路安全掃描技術[3]是採用積極的、非破壞性的辦法來檢驗系統是否有可能被攻擊崩潰。它利用了一系列的腳本類比對系統進行攻擊的行為，並對結果進行分析。這種技術通常被用來進行模擬攻擊實驗和安全審計。網路安全掃描技術與防火牆、安全監控系統互相配合就能夠為網路提供很高的安全性。

2. 弱點評估

弱點評估會根據網路掃描後所得到的資訊做更進一步的檢測，在前一階段所得到的報表資訊，比如開啟的埠號、服務的版本或是作業系統等資訊，來做更深入的探測，與掃描階段不同的是弱點評估會藉著自己所維護的弱點資料庫，來對受測系統進行掃描，弱點掃描器會依據弱點資料庫比對出潛在的弱點或是可能的風險，以達到弱點掃描的目的，在弱點評估結束後，系統管理者可以依據報表進行修補的動作，以避免遭受外在攻擊者的威脅[5]。

3. 滲透測試

由於弱點掃描只能做為一般性的弱點風險偵測，但系統在現實環境中所遭受的風險更為複雜，為了補足弱點掃描的缺陷，因此需要滲透測試來彌補這方面的不足[2]。

在完整的滲透測試過程中[6]，通常測試人員會盡可能的收集資料來得知目標系統的相關資料，測試者首先可以利用像 Nmap、Nessus 等掃描工具，先對目標主機進行掃描來得知目標主機的相關資訊，之後，在進一步針對這些資訊來做進一步的偵測，藉由於此，可以找到在弱點評估階段檢測出的漏洞。

(二) Web 安全工具

1.Nmap 網路探測程式

Nmap[8]為一款知名的網路掃描程式，全名為 Network Mapper，由 Fyodor Vaskovich 於 1997 所開發的一套開放原始碼軟體，可用於檢測本機或網路遠端主機服務的相關資訊。開發 Nmap 的原意是希望藉由此軟體來協助進行伺服器的安全性稽核與弱點分析，進而有助於增強系統及網路安全。

Nmap 主要功能是針對 TCP/IP 通訊協定掃描，不僅可以檢測出目標主機所開放的 TCP 埠號，還可以取得對應的網路服務類型，以及應用軟體名稱與版本。Nmap 除了可以偵測出目標主機所使用的作業系統，還可以偵測出封包過濾器、及防火牆種類等資訊。

2.Nikto 弱點掃描系統

Nikto 是一個開放原始碼的 Web 漏洞掃描軟體，可以掃描具潛在危險的檔案和 CGI 程式等。Nikto 的設計理念是為了縮短 Web 伺服器的測試時間，最重要的是使用者可以自訂掃描語法資料庫。

Nikto 是一個強大的 CGI 掃描程式，不僅可以檢查 CGI 程式碼的安全弱點，還可以以規避的方式來做檢查，以用來規避入侵偵測系統。Nikto 含有完整的說明文件，強烈建議使用者在執行程式之前要仔細的閱讀。如果使用者的網頁伺服器執行 CGI 程式碼，Nikto 將會是用來檢查這些伺服器安全性的最佳資源。

3. W3af Web 應用程式攻擊與評估框架

W3af 是 Web Application Attack and Audit Framework 的縮寫，提供了滲透測試和稽核的平台，主要是針對 Web 的服務做檢測，W3af 是一款非常強大的開放原始碼安全漏洞檢測工具，並可提供一系列的 Web 檢測模組。

由於 W3af 是免費的工具，因此安全工作人員常用 W3af 工具來檢測系統的安全性。該 W3af 核心和它的 plugin 都完全用 Python 撰寫。所以此架構可以在所有安裝 Python 的作業系統平台下運行，W3af 該項目已超過 130 個 plugin，包括檢查 SQL Injection，跨站腳本攻擊 (XSS)。

(三) Live CD

1. Live CD 介紹

Live CD 是一種不需要安裝在硬碟上[1]，利用光碟即可馬上啟動作業系統的一種方式，因此也不會影響到硬碟中原有的系統，可免去一切安裝作業系統的複雜程序，由於 Live CD 的作業程序皆是由光碟機開機，所以並不怕網路上病毒的攻擊，

除了作業系統本身項目以外，還可以安裝其他的應用程式，讓使用者可以在自己熟悉的環境當中來作業，而不會有在陌生地方使用陌生作業系統之困擾，目前最廣泛使用的 Live CD 是 Knoppix。

2. Security Live CD 介紹

在 2006 年網路對於 Security Live CD 進行了排名，共列出了十大資安 Live CD 套件。

(1) Helix：有別於其它的 Security Live CD，主要專注於電腦鑑識 (Computer forensics) 與事件應變 (Incident response)[10]，由於 Helix 主要是做為鑑識工作的工具，所以 Helix 並不會改變電腦主機的系統、環境，亦不會主動掛載 swap 置換空間或其它的附加裝置，目的即是保持資料的完整性，以讓後續的鑑識工作能順利完成。

(2) BackTrack：BackTrack[4]是目前在滲透測試當中擁有最高評價的 Live CD，完全不需要安裝，只要從光碟機讀取，即可進行滲透測試的工作，目前此套件已收集了超過 300 種的安全工具，而在 2006 年 insecure.org 的票選，BackTrack 已成為全球最受歡迎的 Security Live CD。

(四) Web 弱點掃描工具

1.開放原始碼軟體

(1) Paros Proxy

Paros Proxy 是一個對 Web 應用程式的漏洞進行評估的代理程式，以 Java 撰寫的 Web 代理程式，可以評估 Web 應用程式的漏洞。Paros Proxy 支持動態地編輯/查看 HTTP/HTTPS，進而改變 Cookies 和表單字段等項目。Paros Proxy 還可以測試一般 Web 網站常見的弱點，如：SQL Injection 和 Cross-Site Scripting。

(2) Web Scarab

Web Scarab 為 OWASP 元老級的計畫之一。Web Scarab 則是一個 HTTP-Proxy 為主的應用程式集，用來分析 HTTP 和 HTTPS 的通訊協定，Web Scarab 的目標是成為一個可用於自動或互動測試 Web 應用的安全工具。

2.商業軟體工具

(1) Acunetix WVS

Acunetix Web Vulnerability Scanner 是一款網路漏洞掃描且功能強大的工具，可以檢查網站的安全性，如 SQL Injection 或 Cross Site Scripting 攻擊等，適用平台有 Windows XP、2000、Vista 或 2003 sever。75% 的網路攻擊目標是基於 Web 的應用程式，因為網站內容可能涉及到公司的敏感資料，例如信用卡資料和客戶名單資料。Acunetix Web Vulnerability Scanner 是以駭客攻擊的方法來檢測用戶的 Web 應用程式安全，主動找尋 Web 應用的漏洞。

(2) N-Stalker

N-Stalker Web Application Security Scanner 是由 N-Stalker 公司所研發的一個安全評估工具。透過與知名的 N-Stealth HTTP Security Scanner 掃描工具及其 35,000 個 Web 攻擊簽名資料庫合併，使得 N-Stalker 能為使用者的 Web 應用程式消除常見的安全隱患，包括 Cross-Site Scripting、SQL Injection、Buffer Overflow、Parameter Tampering 以及更多的攻擊等。

三、 設計與實作

(一) 系統流程

本研究建構一 Security Live CD，讓資安人員可以利用一片 Live DVD 或 Live USB，使得任何作業系統環境皆可以成為自動化 Web 安全檢測裝置，進而透過網路針對受測主機進行自動化的檢測，最後可以呈現完整的 Web 報表 (詳見圖1)。

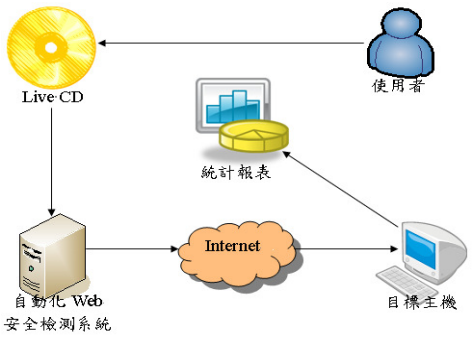

圖1 系統流程圖

(二) 自動化 Web 安全檢測系統架構

本研究以自動化快速檢測 Web 弱點為目的，建構一個可簡單輸入檢測目標的介面以快速檢測出弱點，以減少資安人員檢測弱點的時間。本研究結合 Nmap、Nikto、W3af 等弱點掃描和滲透測試工具 (詳見圖2)，整合不同的資料格式，對 Web 安全作自動化的掃描檢測，最後再利用網頁介面顯示掃描後的整合資訊，讓管理者可以迅速了解到 Web 弱點，以及盡速修補漏洞。

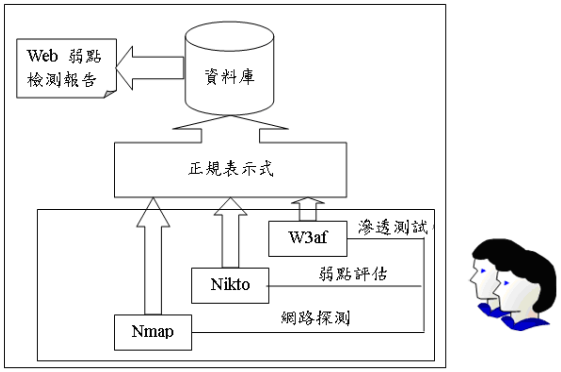

圖2 自動化 Web 安全檢測系統架構圖

(三)系統架構

本研究架構 (詳見圖3)，是基於 xubuntu 的作業系統來做發展。並利用輕量級的桌面選單 Xfce4，此設計理念是為了減少使用系統資源，利用 Xfce4 將所有安全工具分門別類放置，點選分類選單的自動化工具後即可馬上啟動自動化 Web 安全檢測工具，並利用簡單的視窗介面做為使用者提示，而讓測試人員可以僅輸入目標之 URL 而完成自動化安全檢測，最後得到掃描結果，以利於分析網頁的漏洞、弱點。

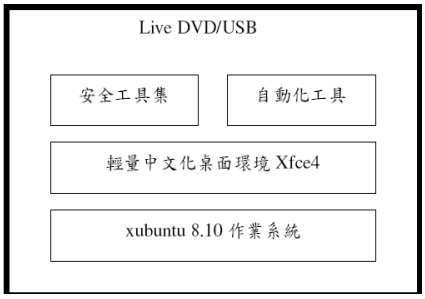

圖3 系統架構圖

當點選自動化 Web 安全檢測工具之後，馬上會跳出使用者提示的對話視窗，此時只要輸入所須測試網頁的 URL，即可自動進行 Web 安全檢測工作。當輸入 Web 之 URL 後會馬上自動執行檢測動作。

最後，在 Web 安全檢測掃描之後，會得到一份掃描結果 (詳見圖4)，利用此結果可以知道此網頁弱點的詳細資料，因而對此部分做補強的動作，而讓網頁的安全性可以提高，免於被有心人士入侵。

四、 系統開發與實驗測試分析

(一) 系統測試

本研究實際測試，以自動化的掃描檢測 Web 弱點，最後可以自動呈現 Web 弱點檢測報告，且有統計圖表，如：圓餅圖、直方圖可以統計出 Web 弱點個數及比例；另外，檢測報告可以轉成 PDF 格式，具備文件保密功能，以避免內容不會被修改。

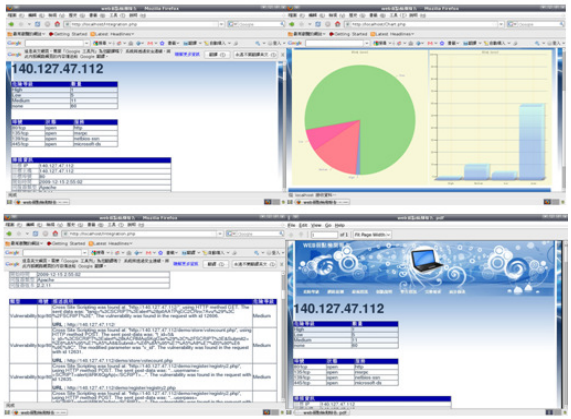

圖4 Web 弱點檢測報告

(二) 知名 Web 弱點檢測工具比較

本研究與目前現有知名的 Web 弱點檢測工具做比較，主要是以自動化執行、報表的呈現、統計圖表等方面來進行比較，如表一、表二所示。

表 1　與開放原始碼工具比較

類別	本研究	Paros Proxy	Web Scarab
自動化	O	X	X
中文報表	O	X	X
統計報表	O	X	X
GUI 介面	O	O	O
PDF 格式	O	X	X
Web 檢測	O	O	O

表 2　與商業軟體工具比較

類別	本研究	N-Stalker	Acunetix WVS
自動化	O	O	O
價格	免費	U.S.$359,00	U.S.$1445
統計報表	O	O	O
Web 檢測	O	O	O
GUI 介面	O	O	O
危險統計	O	O	O

五、 結論與未來展望

本文就開放原始碼的技術，提出一套針對 Web 安全的自動化弱點檢測工具，結合 Nmap、Nikto、W3af 等弱點掃描和滲透測試工具，由於此工具全部自動化，所以完全無門檻問題，只要輸入要檢測 Web 之 URL 即可馬上獲取掃描後的資訊。由於全部系統整合到一片 Live DVD 或 Live USB，所以在不同的環境皆可使用，且不必更動到原有的系統架構。

在未來發展方面，可考慮加上安全程式碼檢測工具，使其更為全面了解 Web 上之漏洞和弱點，以檢測潛藏的 Web 漏洞，另外；在自動化弱點檢測系統中傳輸連線並未加密，在未來可考慮連線安全性的方向作發展。

參考文獻

[1]. 王旭正、高大宇、ICCL-資訊密碼暨建構實驗室，資訊安全：網際網路安全與數位鑑識科學，博碩文化出版公司，2007年1月。

[2]. 陳政龍，軟體開發之資訊安全管理問題探討，資通安全專論，2008年4月。

[3]. 楊仁和譯，防駭超級工具，歐萊禮，2008年02月。

[4]. BackTrack,http://www.remote-exploit.org/backtrack.html, February 2010.

[5]. B. Skaggs, and B. Blackburn, Network vulnerability analysis, Circuits and Systems, 2002. MWSCAS-2002. The 2002 45th Midwest Symposium on, page 493-495.

[6]. D. Geer, and J. Harthorne, Penetration Test： A Duet. Computer Security Applications Conference, 18th Annual, pages 185-195, 2002.

[7]. K.J. Higgins, Web Application Security Consortium, Report： In-Depth Analysis Finds More Severe Web Flaws, October 2008.

[8]. M. Wolfgang, Host Discovery with nmap, Internet published, http://moonpie.org/writings/discovery.pdf, November, 2002.

[9]. P. Midian, How to ensure an effective penetration test, Information Security Technical Report, Volume 8, No 4, April 2003.

[10]. T. Grance, K. Kent, and B. Kim, Computer Security Incident Handling Guide. Retrieved January 11, 2008, from the World Wide Web: http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf.