中文化網路安全工具可移動系統設計與實現

吳佳寰
高雄師範大學資訊教育所
willie@ice.nknu.edu.tw
楊中皇
高雄師範大學資訊教育所
chyang@nknucc.nknu.edu.tw

摘要

現今網路上已有許多弱點評估的工具，但是一來這些工具佈署需要時間，二來其提供的中文環境通常都不夠友善，種種因素皆對網管人員在管理的工作上，造成不小的負擔。所謂工欲善其事，必先利其器，本研究所探討的即是製作一個中文化的Live DVD/USB環境，並蒐集知名的安全工具，將這些工具整合到Live DVD/USB之中，成為一個強大的快速佈署平台。藉由Live DVD/USB先天的特色以及中文化的環境，除了可提升資安人員檢測的速度，更降低了系統佈署的門檻與提高可攜性，達到快速評估弱點的目的。

關鍵字：弱點評估、滲透測試、Live DVD、Live USB、安全工具。

一、前言

近年來由於網路的普及以及迅速發展，資訊安全的議題也越來越受到普羅大眾的檢驗與重視。資訊爆炸的結果，造成網路上充斥著各種病毒以及木馬程式，而不懂技術的人也可以藉由網路上隨手可得的入侵工具，找到有漏洞的系統進行入侵攻擊。面臨著這些隨時可能入侵的攻擊以及風險，除了必須具備相當程度的網路安全概念以及危機意識之外，如何快速佈署可進行風險評估[23]的平台也是需要關注的問題[5, 9, 10]。

Live DVD是利用Linux所製作而成，植基於DVD上的唯讀作業系統。此系統的優勢在於不用安裝於硬碟上，開機時即時偵測系統硬體並自動設定。除此之外，我們也可以將系統安裝於USB隨身碟上，除了有快速的讀取能力，由於USB隨身碟可寫入的特性，更可以將變更的異動寫回隨身碟上，成為一個可快速佈署與高可攜性的完整作業系統。

本研究將網路上常見的安全工具整合至Live DVD/USB中，除了提供友善的圖形介面可方便執行之外，也將介面中文化，降低網管人員在操作上的負擔與不便性。

二、安全工具軟體

隨著網路的發達以及資訊的流通，資訊安全相關的議題也越來越受到大家的重視。層出不窮的網路入侵、機密竊取的事件，造成了組織內部重大的損失。因此，找出一套有效的評估或是偵測的方案，以杜絕各式的風險已是重要的課題[13, 15]。靠著主動的弱點評估與滲透測試[11]、以及被動的入侵偵測[18]，才有辦法及時的監控組織內部服務的狀態，並於第一時間修補或是通報系統的漏洞。以下介紹網路上常見的安全相關工具。

2.1 Nmap

在進行弱點評估的過程中，網路探測為首先必須先進行的工作，諸如上線的主機列表、對外開放的服務與埠號、甚至是主機所運行的作業系統，

都是弱點評估所需之重要資訊。其中，Nmap [20]是專用於資訊蒐集的強大工具,除了可以快速的蒐集弱點評估所需的資訊,其還有眾多的掃瞄參數可以設定，比如指定封包的類型、判別對外的服務軟體版本等強大功能。

2.2 Nessus

Nessus [17, 19]為目前知名的弱點評估軟體之一，不同於市面上其他弱點評估軟體，Nessus的架構為Server-client架構，藉由Nessus圖形化的client介面，來達到操控Nessus server進行弱點評估掃瞄的目的。Nessus具有諸多特色，除了有獨立的權限控管機制、Server-client架構之外，NASL語言的發明是Nessus之所以如此快速發展的因素之一。NASL為Nessus所發展的一套專門用於撰寫弱點掃瞄的高階語言。藉由NASL語法，可讓有需要的單位自行開發客制化的弱點掃瞄模組,而無需理會或是更動Nessus的程式碼。也因為此NASL的設計，讓開放原始碼社群貢獻了許多弱點評估的模組，使得Nessus的弱點資料庫快速的擴充以及完備。

2.3 Snort

在開放原始碼的軟體中，Snort [24]是極負盛名的一款入侵偵測防禦系統[1]。此系統藉由不斷的監聽網路封包,並將之與預先配置好的資料庫做比對,來判斷是否有惡意的封包或是攻擊經由網路散佈進來。Snort依據不同類型的協定，比如SMTP協定、FTP協定等，分類成不同的資料庫模組。如此架構的設計,讓我們日後若需針對某特定服務額外的加入比對的樣式,則只需針對該類型的模組進行新增修改，而無需更動到全部的資料庫資料。除此之外，Snort也將規則的編寫語法透明公開化，搭配前述開放原始碼的特性，使得Snort的資料庫一直持續在更新與修正,降低誤判或是遺漏惡意封包的情況。

不少第三方廠商針對Snort提出了更加簡易的管理與設定方式。比如ACID計畫以及SnortCenter計畫，皆提供了Web介面的監控網頁，藉此降低操作門檻。

2.4 OpenSSL

OpenSSL [21]為一項開放原始碼的計畫，此計畫目標為提供一套商業等級的SSL/TLS加解密工具以及相關的開發套件,所有的原始碼皆公開於網路上可自由下載。此計畫支援了眾多加解密技術，諸如RSA、DSA等皆有完整的支援。OpenSSL以GPL授權發佈，這意味著任何人皆可取得原始碼，並自由的修改與散佈，唯一的限制是必須遵守GPL條款，所修改後的原始碼也必須開放給大眾，回饋給社群。也因為如此，現在常見的GNU/Linux、FreeBSD系統中都有提供可安裝的OpenSSL套件。除此之外，OpenSSL也廣泛的用於各式常見的服務之中，像是Apache網頁伺服器，也有取用OpenSSL的成果。沒有OpenSSL計畫，許多開放原始碼的計畫進展如今就不會如此活躍。

2.5 GPG

GPG(GnuPG) [12]是GNU遵照RFC2440 (OpenPGP) [3]標準所開發出的一套加解密軟體。在網路發達、資訊流通的現在，如何保有個人的隱私也越發越受到重視，而GPG正是因此原因而誕生。GPG支援非對稱式金鑰加密法，每一份金鑰分成一把公開金鑰以及一把私密金鑰,我們藉由私密金鑰將隱私的內容加密成密文,而唯有靠著成對的公開金鑰才能將密文還原，反之亦然。除此之外，我們也可將GPG應用在數位簽章，來確保訊息是否遭到竄改。GPG操作介面為文字模式，但由於開放原始碼，所以也有著第三方廠商的支援。在GPG官方網站上也有提供為數不少的圖形化介面，讓操作方式更為簡便。

2.6 RATS

RATS(Rough Auditing Tool for Security) [22]是用來評估程式原始碼潛在弱點的開放原始碼工具。它可以掃描C、C++、Perl、PHP還有Python的原始碼，並標記可能有弱點的程式碼位置(比如buffer over flow)，供程式人員之後進一步的檢查。RATS不但可以找出一些特定的弱點，更可以針對這些發現的弱點提出建議以及改進方式。

2.7 Honeyd

Honeyd [8]是一套知名的誘捕系統，我們可使用此系統來模擬常見的作業系統，放置於網路上來蒐集網路攻擊行為。Honeyd除了可以模擬常見的作業系統，其官方網站上也提供了諸多外掛模組，來用作於模擬常見的服務。比如我們可從官方網站下載模擬微軟 IIS 網頁伺服器的 scripts，來模擬正在提供網頁服務的Windows機器。如此模組化的設計，我們可以依照需求來客製化所需模擬的服務，使得模擬更加真實。企業可以設置一至多個Honeyd誘捕系統，並模擬企業對外開放的服務。Honeyd系統的價值在於，由於Honeyd誘捕系統並沒有真正的對外服務，所以所蒐集到的封包與攻擊行為皆可以作為企業的早期預警參考資訊，提前防範以降低網路攻擊對企業所造成的損害。

三、安全工具Live CD

德國程式設計師Klaus Knopper將Debian GNU/Linux系統移植至光碟上，取名為Knoppix [16]並散播至網路上。當時Knoppix是植基於CD此儲存媒介上，靠著一片CD就可以經由光碟開機直接使用已預先配置好的系統環境，故將此類產品命名為Live CD。隨著Knoppix各式各樣的應用以及衍生版本迅速的在網路上散佈開來，各種應用於Live CD上的技術也孕育而生，而在這之中Squashfs [25]以及Unionfs [4]此類技術的提出解決了原先CD唯讀不可更動的限制，也使的LiveCD的應用更加廣泛。

網路上已有一些以蒐集安全工具為訴求的Live CD計畫。藉由這樣的Live CD，我們可以在快速的佈署於不同的網路環境後，馬上使用這些已蒐集好的工具進行安全相關的評估與診斷。以下介紹幾個知名的安全工具Live CD，並比較其特色。

3.1 BackTrack

BackTrack [2]是基於SLAX，並整合Whax與Auditor Security Collection的優點而成。其蒐集了超過300種的安全工具，並將這些工具分門別類的放在選單中，以方便使用者選取使用。BackTrack是網路上少數幾個持續更新的安全工具Live CD，最新的2.0版包含了2.6.20的Linux核心，所蒐集的工具版本也是最新的版本。除此之外BackTrack也已內建了大部分無線網路晶片的驅動程式，這使得BackTrack非常適合用於無線網路安全的評估與檢測。

3.2 Helix

Helix [14]不同於BackTrack計畫，它專注於鑑識與事件應變(Incident Response)方面，所蒐集的工具也是以此兩者為主要目的。Helix是從Knoppix重製而來，所以舉凡Knoppix獨有的特色，比如將系統完全載入記憶體等特色，Helix也沒有缺少。由於Helix計畫專注於鑑識與事件應變的特色，國外許多鑑識的教學課程皆以Helix為教學示範的平台。

四、中文化安全工具可移動系統

上述的Live CD計畫皆有一個共通點，那就是其操作介面是英文語系，這對不熟悉外語的國人來說，上手使用會更加困難。這不但使得操作上必須習慣英文語系之外，當我們需要顯示中文或是輸入中文時，也會遇到問題。另外，如今CD儲存媒介漸漸的由DVD所取代，加上越來越便宜的USB隨身碟，我們即可將系統移植至DVD或是USB上，不僅可以存放更多的資料，也可以藉由DVD高速讀取的特性以及USB可讀可寫的媒介，來讓應用可以更加的多元化，達到可快速移動部署系統的目的。所以本研究將製作出完整中文環境的Live DVD/USB，不只是操作環境皆為繁體中文，常用的中文輸入法與相關字型也會含括於其中，以改善現有安全工具Live CD不易上手的缺點。

4.1 系統架構

圖一為本研究的系統架構圖，我們蒐集了各類知名的安全工具，將其分門別類後安裝至配置好的中文環境Live DVD/USB中，並挑選其中常用的圖形介面安全工具將其介面中文化，即可成為可移動之檢測平台。

圖一、系統架構圖

我們參考了弱點評估的步驟要項[7, 26, 29]與工具的特性，將工具分門別類。圖二為分類選單的畫面。

圖二、分類選單

4.2 中文環境建置

現今的 Linux 環境已包含完整的國際化(Internationalization)與區域化(Localization)支援，所以在設定中文環境的步驟上已簡化許多。我們只需將中文語系加入系統的locale並將之預設為zh_TW.UTF-8，再額外裝上相關的中文字型與輸入法，即可讓系統上的中文環境正常顯示與輸入。

中文字型我們所使用的是「AR PL New Sung」此套字型。此字型除了已含括大部分的繁體、簡體、日文字等之外，也內嵌了點陣字，使得字體大小即使在14點以下也不會模糊，可使得中文環境於顯示上更美觀。圖三為開機完成後的中文桌面環境。

圖三、中文桌面環境

4.3 Live DVD/USB製作

現在已有許多製作Live CD的方式與技巧，每種方式皆不太相同。有的需要從重編核心開始，一步一步的將環境建置起來，最後將系統製作成映像檔燒錄；有的則提供了一些建置的工具與命令稿，用來簡化製作的過程。不過這些方式不是步驟瑣碎，就是必須從現有的Live CD重製，降低了製作與客製化的彈性。所以本研究使用了Debian Live [6]計畫，其提供了以下特色：

- 使用Debian官方維護套件：Debian官方套件數量截至目前為止已超過一萬八千多套，而我們可以選用這些套件，並利用Debian Live計畫所提供的工具製作成Live DVD/USB，這使得我們可以隨著Debian套件的更新，製作包含新版套件的Live DVD/USB。
- 保留原先的配置：許多Live CD的計畫，皆對原先的系統做了不少的修改與更動，這造成了後續的更新以及維護上需要花費額外的精力去作整合。Debian Live計畫有鑑於此，於製作的過程中不會更動原先套件的配置，日後更新的步驟上也會更加簡便。

- 彈性的客製化：Debian Live計畫可在安裝的過程中讓使用者介入，使用者可以額外的自訂所需的環境與套件，比如更動開機的流程、或是指定開機時所執行的指令等。我們也可額外的安裝所需的軟體，這麼一來就不會侷限於Debian官方的套件庫。

製作的步驟如下：

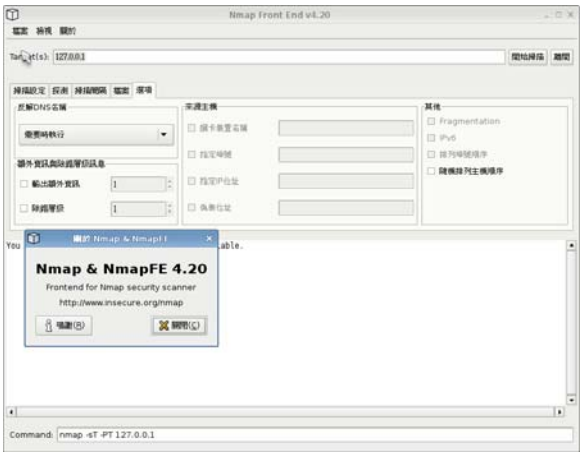
1. 使用make-live config指令建置基本環境，並修改相關設定檔配置，以符合所需。
2. 使用make-live開始建置相關的環境與套件。在製作的過程中由於需要一個乾淨的環境，所以我們需要使用debootstrap/cdebootstrap相關工具來chroot並配置好相關環境。
3. 待提示字元出現，我們就可開始自訂環境，並安裝額外所須的套件。要讓中文環境下的中文輸入法可以正常使用，也需於此步驟做設定。此步驟完成後，執行exit即可。
4. 最後使用mkisofs將相關的檔案與開機程式製作成ISO映像檔，我們只要將映像檔燒錄成DVD，即可藉由此Live DVD來開機並運行系統。除了製作成ISO映像檔，我們也可於步驟2中指定映像檔類型，如此一來我們可製作出安裝到USB隨身碟的映像檔，搭配設定相關參數後，即可使此Live USB發揮可讀可寫的特性。圖四是本研究所製作出來的Live DVD的開機畫面：

圖四、開機畫面

4.4 軟體介面中文化

本研究蒐集了許多安全相關的工具，其中有些安全工具提供額外的圖形介面可供操作。我們將這些工具所提供的圖形介面進行中文化，以降低操作的門檻。以下列出幾個有進行中文化的套件中，較知名的軟體：

1. NmapFE：新版的Nmap附帶了一英文前端圖形介面NmapFE，Nmap文字介面下大部分的參數皆可藉著NmapFE圖形介面來設定，使用者即使不熟悉文字介面以及Nmap的使用，也可以藉著NmapFE的圖形介面來達成資訊蒐集的目的。NmapFE目前只提供了英文介面，本研究遂將Nmap所附帶的NmapFE圖形介面中文化，如此一來即可讓操作門檻降低。圖五為中文化後的NmapFE圖形介面。

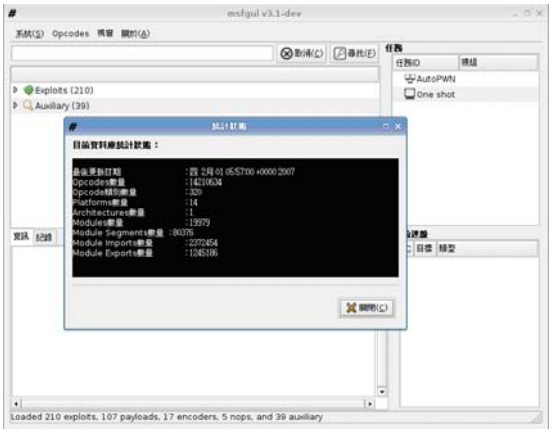


圖五、NmapFE中文化圖形介面

2. Nessus客戶端圖形介面：藉著Nessus先天上Server-client架構的優勢，我們得以操作圖形化的客戶端來進行弱點評估的任務，而無需瞭解Nessus背後運作的原理與流程。因此，本研究加入了客戶端圖形介面的中文語系，使得Nessus客戶端圖形介面得以在系統locale為zh_TW.UTF-8中正常的顯示中文，降低操作上的困難。圖六為Nessus客戶端中文化後的圖形介面。

圖六、Nessus客戶端中文化圖形介面

3. Metasploit GUI：Metasploit [27]為知名的滲透測試工具，其提供了許多可用來入侵與攻擊的模組，供測試者使用。藉由Metasploit所提供的框架以及彈性的設計，我們可視需求選用不同的攻擊模組來達到滲透測試的目的。甚至我們也可遵循Metasploit所提供的API，快速的撰寫滲透測試的模組，來使得滲透測試更加逼真、完整。Metasploit於最新3.1開發版本中提供了可用的圖形介面msfgui程式，這讓以往Metasploit不易操作的問題獲得了改善，測試者可經由此圖形介面來更簡易的進行測試的操作，而無需花費額外時間去習慣文字介面的操作與設定。本研究亦將msfgui完整中文化，如此可降低語言上的隔閡，也更符合國人的習慣。圖七為中文化後的msfgui圖形介面。



圖七、msfgui中文化圖形介面

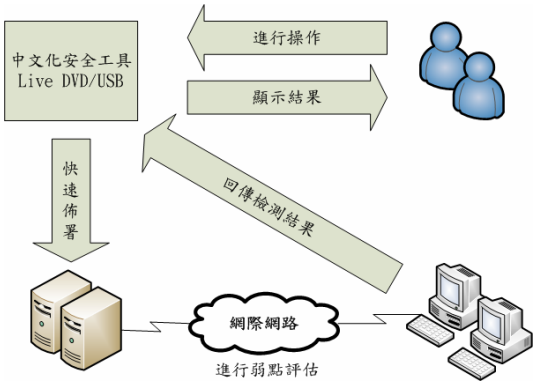
4.5 操作與使用

在資訊安全議題越發受到大眾重視的現在，如同安全工具Live CD此類的應用也越來越多。安全工具Live CD主要可以應用在以下幾個方向：

1. 資訊安全基礎教育：近年來國內已開始重視資訊安全的教育與訓練，如TWISC [28]等安全組織皆已計畫推出資訊安全的訓練與課程，來協助推廣國內對於資訊安全的認識。在這樣的訓練課程中，我們即可使用安全工具Live DVD/USB來協助課程的推動與模擬練習，藉由其中所蒐集的工具，來讓學員可以實際的操作，而不流於形式。
2. 協助網路管理人員評估與檢測組織內部網路：網路管理人員隨時需移動至不同的網路環境下進行工作除錯，這在越大的網路架構中愈容易發生。在這樣的情況下，一套可以快速移動並部署的工具環境即非常重要，而安全工具Live DVD/USB即可符合這樣的需求。安全工具Live DVD/USB不但具備實用性，更具備時效性，網路管理人員無需額外的佈署機器來進行檢測，即可在不同的環境中快速的佈署完畢並進行任務。

由於本研究已將常用的安全工具依其特性做了分類，所以使用者可以依照其需求取用不同分類

的安全工具來進行掃描、弱點評估、或是運用在其他資訊安全相關的領域上。例如，使用者可以選擇「資訊蒐集」分類中的工具來掃瞄目標主機資訊，之後可以端看需要選擇「弱點評估」或是「滲透測試」分類的工具來做更進一步的檢測。如此一來，工具的選擇與使用更加具有彈性，我們可以依任務的不同來將工具做不同的組合使用，使工作任務進行上可以更為順利。下圖為使用者使用本研究的平台進行弱點評估的使用流程圖，藉由彈性的工具選擇以及本研究快速部署的特性，使之可更適用於資訊安全相關的應用上。圖八即為運用在弱點評估的使用流程圖。



圖八、弱點評估流程圖

五、結論

本研究除了提供完整的中文環境可降低操作難度之外，更蒐集了諸多常見的安全工具並中文化，可快速的平台佈署以及弱點評估，所以非常的適合個人、教育單位、甚至是企業資訊部門使用。網路管理者不需特地準備系統的建置與佈署，只需一片Live DVD或是一個Live USB，即可快速的移動到不同的環境進行弱點評估以及網路掃瞄。除此之外，我們不需更動到原有的系統架構，更可以將系統整合的成本降到最低，減少佈署的成本。

六、參考文獻

[1] R. Bace and P. Mell, Intrusion Detection Systems, NIST Special Publication 800-31, http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf, 2001.

[2] BackTrack, http://www.remote-exploit.org/backtrack.html.

[3] J. Callas, L. Donnerhacke, H. Finney, and R. Thayer, OpenPGP Message Format, RFC 2440, http://www.ietf.org/rfc/rfc2440.txt, 1998.

[4] P. W. Charles, D. Jay, G. Puja, K. Harikesavan, P. Q. David, Z. Erez, and Z. Mohammad Nayyer, "Versatility and Unix semantics in namespace unification." vol. 2: ACM Press, 2006, pp. 74-105.

[5] C. David, "Using VMWare and live CD's to configure a secure, flexible, easy to manage computer lab environment." vol. 21: Consortium for Computing Sciences in Colleges, 2006, pp. 273-277.

[6] Debian Live, http://debian-live.alioth.debian.org/.

[7] W. Charl Van Der, H. D. Moore, T. Roelof, M. Haroon, L. Johnny, H. Chris, and F. James, *Penetration Tester's Open Source Toolkit*: Syngress Publishing, 2005.

[8] Developments of the Honeyd Virtual Honeypot, http://www.honeyd.org/.

[9] C. Ed, "Developing "hands-on" security activities with open source software and live CDs." vol. 21: Consortium for Computing Sciences in Colleges, 2006, pp. 139-145.

[10] C. Ed, "Live CDs and security lab configuration," in Proceedings of the 2nd annual conference on Information security curriculum development Kennesaw, Georgia: ACM Press, 2005.

[11] D. Geer and J. Harthorne, "Penetration testing: a duet," 2002, pp. 185-195.

[12] GPG, http://www.gnupg.org/.

[13] T. Grance, K. Kent, and B. Kim, Computer Security Incident Handling Guide, NIST Special Publication 800-61,

http://csrc.nist.gov/publications/nistpubs/800-61/NIST-SP800-42.pdf, 2003.

[14] Helix, http://www.e-fense.com/helix/.sp800-61.pdf, 2004.

[15] R. IEONG and P. Consultant, "Freeware Live Forensics tools evaluation and operation tips," in *4th Australian Digital Forensics Conference*, Edith Cowan University, Perth, Western Australia, 2006.

[16] KNOPPIX, http://www.knoppix.org/.

[17] H. Moore, J. Beale, H. Meer, R. Temmingh, C. V. D. Walt, and R. Deraison, *Nessus Network Auditing*: Syngress Publishing, 2004.

[18] B. Mukherjee, L. T. Heberlein, and K. N. Levitt, "Network intrusion detection," *Network, IEEE*, vol. 8, pp. 26-41, 1994.

[19] Nessus, http://www.nessus.org/.

[20] Nmap, http://insecure.org/nmap/.

[21] OpenSSL, http://www.openssl.org/.

[22] RATS, http://www.fortifysoftware.com/security-resources/rats.jsp.

[23] R. Shirey, Internet Security Glossary, RFC 2828, http://www.ietf.org/rfc/rfc2828.txt, 2000.

[24] Snort, http://www.snort.org/.

[25] Squashfs, http://squashfs.sourceforge.net/.

[26] G. Stoneburner, A. Goguen, and A. Feringa, Risk Management Guide for Information Technology Systems, NIST Special Publication 800-30, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, 2002.

[27] The Metasploit Project, http://www.metasploit.com/.

[28] TWISC, http://www.twisc.org/.

[29] J. Wack, M. Tracy, and M. Souppaya, Guideline on Network Security Test, NIST Special Publication 800-42, http://csrc.nist.gov/publications/nistpubs/800-42/