



檢視網路系統安全

掃描工具

技術組 林岳生

系統安全

現在網路安全相當受到重視，因為網站最怕的就是遭受入侵或是攻擊，遭受攻擊損失往往不是輕易可估算的。服務暫時停止，使得網站客戶流失、盡失顏面，更糟的可能是客戶資料、商業機密的竊取，造成網站信譽損失，甚至成為攻擊者的跳板，發動更大規模的攻擊。為了儘量預防這些問題，系統管理者不外乎努力設置各種防護措施，嚴密監控系統的狀況，但是這些都是站在城牆內不斷地把城牆逐高，努力守著城池，或許該換個角度，站在城牆外面試著測試自己所架設的服務。

由系統外部來測試系統的安全狀況

可以試著站在攻擊者的角度，假想要入侵攻擊某個目標，會如何蒐集資訊？該怎樣探測主機上的狀況？會發動什麼攻擊？以模擬攻擊的方式來尋找自己主機上的弱點，測試自己系統的安全狀況。或許不少系統管理者都想過，但是卻又不知該如何下手，該找破解程式？攻擊程式？去哪找？怎麼用？管理好多台機器，每台都跑了好多服務，這麼多機器和服務該如何一個個測試呢？就算能找到問題，但是該如何解決呢？

使用掃描工具

利用免費或是商業化的掃描工具，就算你不是入侵高手，你也可以像入侵者一樣使用各種方法來測試自己的機器，利用安全掃描軟體，可以幫你掃描一台機器上所開的所有服務。甚至可以一次掃描測試許多台電腦的所有服務，只需檢查掃描軟體測試結果上顯示的警告訊息，適當地調整系統上的服務，即可避免系統管理的疏失所造成的漏洞。

常見的掃描工具

目前比較常見的網路安全掃描軟體有 Nmap、Nessus、Saint 及 CyberCop Scanner

等等， nmap 是一般大家常拿來做 port scan 的軟體，nessus、Saint 和 CyberCope scanner 詳細功能各有不同，但是皆為類似的安全掃描軟體，有的可以增加模組，針對不同的弱點進行測試，甚至實施攻擊的行為。

使用這些類似的掃描工具，可以減少系統管理員管理主機上的疏失，在入侵者未發現漏洞之前先解決，達到偵測漏洞增加安全的功能。

掃描工具簡介

在此，我們將介紹兩套功能強大且免費的掃描軟體，以供以工系統管理員參考使用。

1. nmap – The Network Mapper

nmap 是一個在 unix 上的 port scanner 軟體，藉由 nmap 的掃描，可以輕易迅速的得知遠端主機上所執行的服務，甚至可以猜測遠端主機的作業系統以及版本，也可以針對子網路進行掃描，偵測子網路上有哪些主機存在，並一一探測其服務。

Nmap 的支援的功能包括：

- Vanilla TCP connect() scanning
- TCP SYN (half open) scanning
- TCP FIN , Xmas , or NULL (stealth) scanning
- TCP ftp proxy (bounce attack) scanning
- SYN/FIN scanning using IP fragments (bypasses some packet filters)
- TCP ACK and Window scanning
- UDP raw ICMP port unreachable scanning
- ICMP scanning (ping-sweep)
- TCP Ping scanning
- Direct (non portmapper) RPC scanning
- [Remote OS Identification by TCP/IP Fingerprinting](#)
- Reverse-ident scanning

Nmap 也支援動態延遲時間計算，封包逾時重傳，藉由同時 ping 來測試大量機器 up or down ， nmap 也提供彈性的目標和埠號選擇，假造 IP 來 scan ，判斷 TCP Sequence 預測特性，等等。

詳細的安裝及使用說明請到 <http://www.insecure.org/nmap> 查詢取得。

例如，我們選擇一台未裝設防火牆的測試主機，進行測試在 unix 上執行 nmap 程式，使用參數-O 進行掃描。

nmap -O 192.168.0.5

Starting nmap V. 2.53 by fyodor@insecure.org (www.insecure.org/nmap/)

Interesting ports on test.tw (192.168.0.5):

(The 1502 ports scanned but not shown below are in state: closed)

Port	State	Service
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
80/tcp	open	http
110/tcp	open	pop-3
111/tcp	open	sunrpc
113/tcp	open	auth
143/tcp	open	imap2
443/tcp	open	https
465/tcp	open	smtps
970/tcp	open	unknown
971/tcp	open	unknown
972/tcp	open	unknown
976/tcp	open	unknown
977/tcp	open	unknown
993/tcp	open	imaps
995/tcp	open	pop3s
1022/tcp	open	unknown
1023/tcp	open	unknown
2049/tcp	open	nfs

TCP Sequence Prediction: Class=random positive increments

Difficulty=11445 (Worthy challenge)

Remote operating system guess: FreeBSD 2.2.1 – 3.2

Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds

由掃描結果，可輕易且快速得知，這台主機上對外所有的服務名稱以及 port number。藉由-O 的參數，我們還得知這台主機的作業系統和版本，以及作業

系統實作 TCP 的可靠程度。入侵者藉由得知系統所開的服務、埠號、作業系統、版本等資訊，便可決定該如何對欲入侵的主機進行攻擊。系統管理員藉由使用 nmap 這類工具，便可以測試自己的主機，對主機狀況進行大略了解和初步檢視。

對於一般的系統管理者，藉由 nmap 也只能得知主機由外部看到的埠號，到底是否有問題呢？這時就要搭配其他安全掃描軟體來幫我們做檢測。

2. Nessus – Security Scanner

Nessus 是一套免費、功能強大、更新迅速、使用容易的遠端掃描軟體，在系統管理員使用 nmap 快速得知主機大略狀況之後，便可以針對想要進行詳細掃描的機器，使用 nessus 進行測試，nessus 可以依據其 plugin 進行弱點的測試及攻擊，並列出可能的問題，以及解決的建議方法，詳細特點歸類如下：

1. plug-in 的結構：每項安全掃描都是寫成在外部的 plug-in，用這種方法，你可以輕易的增減你所需做的測試，而不需要去修改 nessus 掃描引擎的程式碼，目前已有的 plugin 可分為以下幾類：

- Backdoors：各種後門程式
- CGI abuses：測試常見的 CGI 問題
- Denial of Service：阻斷停止服務
- Finger abuses：測試 finger 的問題
- Firewalls：測試防火牆的一些設定常有的疏失
- FTP：包括匿名使用者的權限、檔案權限、各種 ftp server 的漏洞
- Gain a shell remotely：測試某些服務可能造成遠端得到 shell 的問題
- Gain root remotely：測試某些服務可能造成遠端得到 root 的權限
- General：一般性問題的 plugin
- Misc：其他問題的 plugin
- NIS：測試 NIS 的問題
- Port scanners：使用 nmap 對遠端機器進行 ping、tcp connect scan、FTP bounce scan、TCP SYN scan
- Remote file access：遠端檔案權限存取測試
- RPC：遠端程序呼叫問題的 plugin
- SMTP problems：檢查常見 mail server 的問題，像是 sendmail 較舊版本遠端得到 shell，覆寫檔案，mail relay 等問題
- Useless services：檢查是否有一些並不一定需要，且容易造成系統可能的安全問題，像是以明碼傳送的 telnet、rlogin、rsh 等等
- Windows：測試 windows 上檔案分享服務，認證服務等問題

2. NASL：為了讓撰寫安全掃描程式迅速簡易，因此設計了 NASL(Nessus Attack Scripting Language)，使得不需修改 nessus 的掃描引擎核心程式即可達到各種掃描求。
3. 時常更新的弱點資料庫：nessus 的開發維護人員專注於檢查每天最新的安全漏洞，弱點資料庫更新的時間原則是天來計算。
4. Client-server 架構：nessus 是由兩個部分組成，nessus server 和 nessus client，nessus server 部分負責攻擊，client 則是一個控制和觀看訊息的介面，你可以在不同的系統跑 server 和 client，也就是可以在 PC 上稽核檢視整個網域主機的狀況，而執行攻擊的則是一台在機房的大型主機，目前 server 部分只能在 POSIX 系統上執行(Solaris、FreeBSD、GNU/Linux and others)，client 有 X11、JAVA 和 Win32 三種版本。
5. 可以同時測試無限多台電腦：依照 nessus server 那台主機的能力而定。
6. 不依照埠號來決定主機服務的項目：nessus 不會拘泥於 IANA 所定的埠號來決定服務的項目，也就是說當 FTP server 跑在 31337，當 Web server 跑在 8080 時，nessus 一樣可以辨別他們的服務項目。
7. 模擬入侵者的行為：nessus 不會依照相信 service 對外宣稱的版本資訊來決定這個版本是否安全，他依然會測試各種可能的問題，像是 version x.y.z 之類的，95%的安全測試依然會執行他們的測試，仍然會嘗試 overflow 你的 buffers，對你的 mail server 做 relay，甚至毀掉你的系統。
8. 完整的報告：nessus 不會指告訴你哪裡有問題，在大多數的情況下還會告訴你該如何預防入侵者的攻擊這些弱點，並會分級表示弱點的嚴重性。
9. 可轉換格式報表：可將掃描報告轉成 ASCII text LaTeX HTML "spiffy" HTML 這些格式。
10. 獨立的開發者：nessus 的開發者是完全獨立無顧忌的，跟商業軟體廠商毫無任何關係，所以決不會因為他們跟某軟體有關係而隱瞞任何的安全的弱點。

nessus 的運作過程：

1. 尋找有哪些 port 有服務正在進行，nessus 的 port scan 部分是依靠 nmap 來完成。
2. 測試這個 port 的服務有哪些可能的漏洞存在。
3. 產生測試報告。
4. 提出系統可能的漏洞。
5. 提出系統可能問題的解決方案。

詳細使用安裝說明可以到 nessus 台灣的 mirror 站 <http://www.tw.nessus.org> 或是到 <http://www.nessus.org> 總站取得。

使用 nmap 和 nessus

使用 nmap 和 nessus 必須要非常小心，這些工具發展的本意是要使得系統管理者能輕易快速的檢測自己的網路，但是在入侵者的眼中，這些工具就變成入侵破壞別人系統的最好工具，使用 nessus 的 NASL 就可以輕易地寫出非常強大的攻擊程式，所以當系統管理員使用這些工具時，千萬不要隨意掃描測試別人的網站，nessus 有許多 plugin 都會造成系統嚴重的毀壞，這比手裡拿一大串鑰匙在別人家門口一隻又一隻的測還嚴重，簡直就是直接把門撞迫近去別人家裡，用什麼心態來使用，nessus 就會變成如何，請自制使用時機。

nessus 的掃描速度會因選擇 plugin 的多寡以及網路狀況環境的不同，所以有時候相當耗時間，建議在做測試之前先使用 nmap 對系統進行概略的了解，使用 nessus 時就可以慎選所需要的 plugin 項目來節省掃描的效率，尤其針對大規模的主機進行掃描時，效果會非常明顯。

TW-CERT 也提供遠端安全掃描服務，是以 nessus 為主的自動化自我檢測系統。詳見 <http://www.cert.org.tw>。

網路安全掃描的迷思

透過網路安全掃描並不代表絕對安全，透過網路安全檢查的程式只能幫你從系統外部，使用掃描工具檢測已知的漏洞，已知的問題是死的，但入侵者可是活的，漏洞每天都不斷地在被找出來，而且根據統計，有超過六成的入侵事件都是系統內部的疏失所造成，所以單獨相信網路掃描工具比沒用還糟糕。

網路安全掃描只能當作是一個增進系統安全的參考，幫助管理者學習了解系統安全的重要，但增進網路系統安全還要靠很多事情才能作到。

網路安全掃描之外的其他安全技術

- 最基本的安全措施：使用防火牆。
- 系統管理員最基本的安全概念：使用經安全加密的連線程式，使用加密來傳送資料及文件。
- 建立系統內部掃描機制，確保系統內檔案的一致性。
- 督促使用者正確使用帳號密碼的習慣。

- 使用掃毒軟體，防止病毒或是後門程式。
- 常觀看並保留系統 log，注意並記錄系統服務不正常的狀況。
- 管理者應加強網路安全知識的收集，訂閱系統安全相關的 mailing list 等，隨時掌握 CERT、廠商發佈的安全訊息。
- 資料的完整備分。
- 評估系統備入侵後可能遭到的損害，建立完善的系統還原計劃。

網路安全永遠沒有做完的一天，因為問題不斷地被入侵者找出來，但光靠努力解決系統的問題也不夠，系統內部管理的問題更是需要仰賴教育訓練使用者才能完成，所以系統管理者應該要有高度的危機意識，正視網路安全的重要性。

台灣電腦網路危機處理中心 首頁：<http://www.cert.org.tw/>

假如您有任何建議與事件回報，請 mail 到 twcert@cert.org.tw

連絡電話：07-5250211 傳真：07-5250212