行政院及所屬各機關出國報告
（出國類別 ：實習 ）

「實習 PKI 維運管理技術」報告

服務機關： 中華電信股份有限公司
數據通信分公司
出國人 ： 職 稱 姓 名
助理工程師 陳立群
助理工程師 趙文昌

出國地點：美國
出國期間：92 年 11 月 13 日 92 年 11 月 21 日
報告日期： 92 年 1 月 6 日

系統識別號:C09204482

公 務 出 國 報 告 提 要

頁數: 77 含附件: 否

報告名稱:

實習PKI維運管理技術

主辦機關:

中華電信數據通信分公司

聯絡人／電話:

／

出國人員:

陳立群 中華電信數據通信分公司 加值系統處 助理工程師
趙文昌 中華電信數據通信分公司 加值系統處 助理工程師

出國類別: 實習

出國地區: 美國

出國期間: 民國 92 年 11 月 13 日 -民國 92 年 11 月 21 日

報告日期: 民國 93 年 01 月 16 日

分類號/目: H6／電信 H6／電信

關鍵詞: PKI,植基於時間的安全,稽核,SANS研究院,資訊安全管理

內容摘要: 此次赴美實習PKI維運管理技術，習得先進國家稽核PKI或電子商務所需之稽核原則和基本概念、「植基於時間的安全」、稽核週界、防火牆、路由器、稽核網站與相關應用、網路稽核、Windows進階系統稽核、UNIX進階系統稽核之技術與工具運用，並針對訓練單位SANS研究院所提供的資安教育訓練及服務提出心得。

本文電子檔已上傳至出國報告資訊網

報告摘要

此次赴美實習 PKI 維運管理技術，習得先進國家稽核 PKI 或電子商務所需之稽核原則和基本概念、「植基於時間的安全」、稽核週界、防火牆、路由器、稽核網站與相關應用、網路稽核、Windows 進階系統稽核、UNIX 進階系統稽核之技術與工具運用，並針對訓練單位 SANS 研究院所提供的資安教育訓練及服務提出心得。

目錄

1. 前言 3
2. 目的 3
3. 行程 5
4. 研習內容 5
4.1 研習師資及內容安排 5
4.2 稽核原則和基本概念 6
4.3 稽核週界 10
4.4 稽核網站與相關應用 22
4.6 進階系統稽核-Windows 36
4.7 進階系統稽核-UNIX 46
5. 建議與心得 63
5.1 SANS 研究院舉辦之資安教育訓練、證照考試及服務值得借鏡 63

1. 前言

職奉派至美國實習 PKI 維運管理，針對稽核公開金鑰基礎建設、電子化政府網站、應用與電子商務所需之稽核網路、防火牆、路由器、作業系統、網站與應用程式的技術進行深入而緊湊的研習。對網路申辦或交易安全關鍵性的稽核議題，有通盤之瞭解，期望此次研習對於本公司經營 PKI 平台、核心與應用服務，提供高信賴、安全及可用度高之資料及應用系統的服務，爭取電子簽章法通過後的商機有所幫助。

2. 目的

「電子簽章法」在民國九十年十月三十一日由立法院通過，並由經濟部在九十一年四月一日宣布施行，賦予電子簽章與電子文件法律效力，代表電子交易獲得相當程度的保障，有效帶動電子化政府及電子商務之發展。

本分公司自八十七年接受研考會委託，與中華電信研究所規劃、開發、建置、營運「政府憑證管理中心(Government Certification Authority， GCA)」系統，開創國內網路認證服務之先河，奠定我國公開金鑰基礎建設(Public Key Infrastructure，PKI)之發展基盤。本分公司與中華電信研究所(以下簡稱本團隊)於九十年九月取得經濟部電子工商委外服務案，規劃及建置經濟部電子工商憑證中心，九十年十月標到研考會政府憑證總管理中心及政府憑證管理中心委外服務案，九十一年十二月標到內政部憑證管理中心委外服務案，提供自然人憑證之簽發服務，積極建設我國政府公開金鑰基礎建設。目前上述三個憑證管理中心都已經開始營運，簽發以 IC 卡、保密器等為私密

金鑰符記之憑證。

此次參加由美國系統管理、網路和網路安全研究院(System Administration，Networking and Security，Institute，縮寫為 SANS)在紐奧良所舉辦之 SANS Network Security 2003 Conference Track 7 Auditing Network Perimeters and Systems 課程，為期六天，並包含 Lab 實做課程，在 PKI 維運管理之系統管理與稽核技術方面有所收穫。參加此課程係基於以下幾個理由：

(1) 政府憑證總管理中心及政府憑證管理中心已經於民國九十二年七月通過 BS 7799 Part 2 2002 年版稽核認證。經濟部工商憑證管理中心則通過符合SAS 70標準之CA稽核，內政部憑證管理中心則積極建置 BS 7799 資訊安全管理體系，不過政府憑證總管理中心仍有通過更高安全等級之 WebTrust 認證之需求，政府憑證總管理中心、政府憑證管理中心、工商憑證管理中心必須接受持續性的資通安全內外部稽核。中華電信憑證管理中心依照憑證實務作業基準必須接受每兩年一次的稽核。

(2) 我們所熟知的 BS 7799 偏重於資安管理體系的建立與稽核，而不是著重於技術面的稽核，需要補足一些技術方面之稽核技能，來發掘問題，確保資通訊的安全。

(3) 構成政府公開金鑰基礎建設及中華電信憑證管理基礎建設的憑證資訊系統、註冊管理系統、目錄服務系統、發卡系統都牽涉到網路、防火牆、數位簽章及加解密機制、路由器、Windows 及 UNIX 等作業系統，這些都是本次課程的重點。

(4) 為使本分公司在 PKI 業務的營運技術及客戶服務，能參考國際經驗，符合最新國際標準，藉由最新稽核技術與產品，在高安全及可信賴的營運環境以及健全的稽核制度下，滿足電子化政府及電子商務應用需求，以利規劃

建置全方位、最佳的政府及企業解決方案，建立安全及可信賴的電子認證制度，做好網路認證之客戶服務、維運服務及營運推廣工作，故安排此項實習課程。

3. 行程

本次出國實習行程摘要如下：

日次	日期	地點	主要行程概述
1	90/11/13	台北-洛杉磯-紐奧良	行程，於洛杉磯轉機
2	90/11/14-11/19	紐奧良	實習 PKI 維運管理技術
3	90/11/20-11/21	洛杉磯-紐奧良-台北	行程，於洛杉磯轉機

4. 研習內容

4.1 研習師資及內容安排

本次研習共六天，授課老師為 Tanya Baccam，她目前擔任 Vigilar 的保證服務經理 (Manager of Assurance Services)，負責提供用戶端的滲透測試、弱點和風險評估，也負責設計安裝及設定入侵偵測系統與防火牆。她先前的經驗包括負責醫療組織的基礎建設安全，也在 Deloitte & Touche 擔任安全服務實作的經理而有機會對許多顧客提供週界安全、網路基礎建設設計與資料庫安全等安全架構的顧問服務也負責發展許多企業應用的整合角色。她目前具有 GCFW、GCIH、CISSP、CISA、CCNA、MCSE、CCSE、CCSA 和 Oracle DBA 等多張通資訊安全及電腦系統證照。

本次上課學員包含全球各地的電腦從業人員、諸如網際網路服務業者(Internet Service Provider，ISP)、網路資料中心 (Internet Data Center，IDC)、電腦顧問公司、美國國國防部的資訊人員，國籍遍佈美國、加拿大、瑞典、馬來西亞、盧森堡、英國、以色列、德國、波蘭、挪威、比利時、荷蘭、丹麥、波多黎各、奧地利、、等，但以美國學生為主，職是此門課唯二來自台灣的學生。本課程包含研習、討論、Lab 實做，上此課程的學員須具備電腦、網路及作業系統的知識。並自行準備筆記型電腦，透過 SANS 研究院準備的網路環境與系統進行實地指令操作，藉由本課程可習得經營 PKI 服務與電子商務等所需之稽核技術發展趨勢，對營運公開金鑰基礎建設以及電子商務，保持高安全與可信賴性的營運與客戶服務有很大的幫助。

4.2 稽核原則和基本概念

第一天上的課程為稽核原則和基本概念，定義本週課程會用到的術語與參數，提供常用到的良好稽核程序與檢查表產生方式，並清楚定義了稽核與評估之間的關係。本課程強調了稽核觀念對實際狀況的真實應用，幫助稽核人員決定如何使用不同的稽核策略以及哪些政策需要應用到。在本課程中提到高階使用到的控制與目標，接下來的每一天則會提到在第一天所提到的稽核目標如何落實與強調，老師要我們開始學習像稽核人員一樣思考，第一天課程主要的焦點集中在基準線(baseline)與植基於時間的安全(Time based Security，TBS)。植基於時間的安全對許多稽核人員來說屬於新觀念，將可幫助有效完成未知科技風險的度量，也能夠幫助組織精確識別如何投資安全與保證的金錢而能獲得最大的回饋。

在今天的課程我們瞭解到稽核員的角色和政策的創造以及政策

的符合還有緊急事件之處理的關係。同時也瞭解到幾種稽核標準與稽核證照，例如資訊安全稽核與控制協會(ISACA)與授證電腦稽核人員(CISA，Certificated Information System Auditor)之關係。美國常用的FISCAM與COBIT標準，同時也學習了基礎的稽核與評估策略，例如基準線(baseline)、以時間為基礎的安全、怎樣從稽核的角度來思考?從安全政策與程序發展出稽核檢查表，並由檢查表反思大框架的安全程序與政策等。最後並介紹稽核程序的六個步驟，步驟間如何相互相關，如何有效執行稽核?如何有效報告發現。

在此先對一些術語提供定義：所謂的「稽核」可視為一種度量(measurement)，尤其是相對於標準的一種度量。大致可分為符合性稽核(Conformance Audit)、安全稽核(Security Audit) 以及財務稽核(Financial Audit)。在資訊科技及資訊保證(information assurance)裡有三個地方最能稽核，也就是從政策的層次(Procedure level)、程序的層次以及系統的層次，系統的層次。所謂符合性的稽核是指系統究竟有多好來滿足組織內所訂的政策及程序。安全稽核是用來度量政策及程序如何實施或是以更一般的稽核方式用來度量與產業最佳實務(best Practice)間於高於系統層次方面有哪些需要改進。簡單定義稽核可說是回答這樣的問題:"你如何知道你...."(How do you know you....)

所謂的評估(Assessment)則是一種度量與估計，包含對於風險、威脅弱點或損失成本的量測。而所謂的範圍(scope)則是指所稽核或評估的責任區。目標(Objective)則是指政策或程序的目標，或是稽核與評估的目標。因此我們通常先定義稽核的範圍，再選擇稽核的目標。而所謂的控制、控制項或安控措施(Control)，係指如何吻合我們的目標。例如我們的目標為用戶鑑別，則控制項可以是NT的網域控制器或是事件記錄器(Event Logging)將登入、登出或是輸入錯誤密碼的情形紀錄下來。如果把目標當作什麼(What)，則控制項為如何(How)。

矯正(Remediation)則代表哪些我們將修正?例如依據最佳實務來做的建議，或是基於政策所做的建議，又如基於程序所做的建議。所謂的緩和、減輕(mitigation)係指我們所做以降低損失或傷害。

老師後續又談到稽核人員與系統管理者之間必須相輔相成，稽核者並非撒旦或魔王，針對系統管理來找麻煩，稽核者有如幫忙做健康檢查的醫生，希望能協助企業找出資訊安全問題所在。所謂的基準線(Baselines)係指度量系統的已知狀態，用於度量系統目前的狀態，是最佳的稽核工具與方法，並且用來描述系統的設定。

以「時間為基準的安全」是指稽核時將時間作為主要的基準，通常稽核量測 How you know，而「植基於時間的安全」測量 How Well/How Long，並量測潛在/真實的損失。「植基於時間的安全」具有量測「安全是否太超過」(Measurement of how much security is too much)，並且可以重製。植基於時間的安全和防禦縱深有關。假設

P=我們的防禦措施仍然有效的時間

D=偵測事件的時間

R=反應所需要的時間

植基於時間的安全其公式為

P＞D＋R 代表結果很好。意即我們的防禦措施在稽核或外來攻擊時持續有效的時間比偵測某一事件以及接著反應處置該事件來得長，則資料和系統將不會被破壞。以真實世界為例，若花十分鐘可以從藝廊破壞某系統而偷走藝術品，若經五分鐘小偷會被陷阱絆住而引起警報，而保全公司要兩分鐘才能通知警衛，而警衛要花兩分鐘配置好車子，車子開到藝廊需要兩分鐘，則

(P)10 < (D)5+(R)6

藝術品會被偷走。我們如何降低偵測時間? 如何降低反應時間?非常重要。另一方面，我們可以假設 P=0，量測最佳與最壞的 D 與 R。其中 D+R=E，E 代表曝露時間(Exposure)。例如分析員正觀看

入侵偵測系統的螢幕，安全主管與網站系統管理員在他們自己的辦公室，稽核員可以用碼表紀錄，放一個測試攻擊於分析員所監看的網站伺服器，則 D=碼表從分析員看到入侵事件起算直到他驗證數據並發出警告。R=碼表從分析員呼叫安全主管一直到網站管理員將此漏洞修補起來。若 D+R=2 分鐘+3 分鐘=5 分鐘，這是最好狀況。假設是在聖誕節，安全主管在路上接到呼叫器顯示由分析員的告警，坐車花了十分鐘找到付費電話回撥給分析員，三分鐘後他確認這是一項攻擊要求分析員聯絡網站管理員，不巧網站管理員去度假，回來時已經過了三小時，則 D+R=13 分鐘+3 小時=3 小時 13 分鐘，這屬於最差情況。我們必須思考如何降低 D 與 R?需要多少花費?我們需要多少的 P?要花多少錢?又如處理緊急事件，(D+R)-P=Exposure，需要考慮 P 持續多久?決定 D 及 R。例如 Code Red 病毒造成邊界過濾器都有流量，P=0，D 和 R 是多少?又如稽核時檢查表必須包含最壞情況的的 D 與 R 之時間，以及量測到的 D 與 R 之時間，稽核報告應該包括改進 D 與 R 之建議。更多的細節，例如導入無線科技 802.11b，應付劫機事件等等風險時如何運用「植基於時間的安全」，老師希望我們能參考 Winn Schwartau 所寫的書 "Time Based Security"。

稽核者最主要的目標在量測和報告風險，其次在影響受稽者降低風險，通常可藉由量測和有效報告系統或流程如何對應最佳實務與相關政策。

稽核程序的六個步驟包括 1.稽核規劃(Audit Planning)，2.啟始會議(Entrance Conference) 3.現場稽核(fieldwork) 4. 準備報告(Preparing the Report) 5.結束會議(Exit Conference) 6.報告管理者(Report to Management)。其中稽核規劃是日常就開始準備，諸如研究、決定範圍、決定稽核策略、製作檢查表，將稽核程序化等等，啟始會議由稽核者面對被稽者(管理代表、系統管理者、系統用戶、系統安全人員

等)，結束會議後向更高層管理者做報告。今天課程的最後一部分，老師做一個稽核實例研討，並對各國辦公室使用電腦是否符合資訊安全政策情形做調查，其建議包括至少包含帳戶與密碼之 Proxy 存取，舉行資訊安全認知教育(Security Awareness Training)、對管理者進行資訊安全管理等等。而最後一張投影片半開玩笑地說對於稽核的衝擊為何?可能稽核報告會被受稽單位嗤之以鼻、將之拋棄。

4.3 稽核週界

稽核週界(Auditing Perimeter)著重在某些最敏感與重要的資訊基礎建設:路由器和防火牆。第二天的課程著重在瞭解路由器和防火牆作為控制措施(Controls)的功能。注意力集中在目前主流的非戰區 DMZ 架構，確認邏輯資訊流，瞭解 Cisco ACLS、防火牆規則以及最重要的一件事亦即如何有效地做稽核?

在第二天的課程，我們學習到路由器的功能、架構與組成，從 TCP/IP 之觀點看路由器，瞭解路由器的稽核問題，老師也舉出在大都會網路中的路由器範例。並提及路由器提供的安全存取控制、如何仔細稽核路由器、稽核的技術與來源、樣本稽核輸出、使路由器安全並稽核路由器的完整性，確認安全的弱點。在測試防火牆部分介紹作業系統的設定、防火牆的設定、系統的管理。也介紹測試防火牆的規則，如何確認防火牆設定錯誤?如何指出弱點?如何做變更控制?從所有網路來的封包流。給定由防火牆與路由器提供的大量資料，要如何使安全監視與稽核的策略獲得展現。在手動操作的課程，老師指導我們操作路由器稽核工具(RAT,Router Audit Tool)來評估路由器的設定檔案。

我們也測試了第三方的軟體，例如加密或鑑別的軟體、掃毒的軟體以及位置列(URL)的重新導向功能。我們也學習如何覆核入侵偵測

系統、防火牆 Logs 以及告警。此處我們學習了 Unix 及 NT 的掃瞄工具、UNIX 與 Window 的封包重建工具、資訊查詢工具以及監視器(Sniffers)。

在撥號入侵(War Dialing)介紹了於 ISDN、PBX、FAX 及類比電話中使用的手段，也介紹了一些駭客工具，例如 THC Scan、Phone Tag、PhoneSweep、TeleSweep Secure。在無線通訊部分也介紹了 802.11b 的一些安全問題、如何做預防措施?無線的稽核工具例如 WSA、Airopeek 以及 Net Stumbler。

今天上課，老師先針對稽核軌跡此一名詞作介紹，在電腦安全系統裡面，記載系統使用的資源並依照時間前後排列的紀錄稱為稽核軌跡。包含用戶登入、檔案存取或其他多變的活動，不論是實際或是嘗試性的、不管是未經授權或是合法的。

接著介紹 IP Header 以及 Static Packet Filtering，這是在多數路由器裡面提供的通訊控制，如果路由器允許流量至 220.10.5.0/24，則路由器評估在 IP header byte 16 是否包含 220、byte 17 是否包含 10、byte 18 是否包含 5，如果是的話，允許流量通過，如果不是的話將通訊鎖住。

防止進入過濾(Ingress Filtering)對於進入內部網路之通訊卻具有內部網路之來源位址(例如 10.0.0.0/8、172.16.0.0/12、192.168.0.0/16)進行過濾，以防止假冒，對於 127.0.0.1 之來源位址或是廣播位址必須加以禁止，對於路由表也要加以檢查。

外出過濾(Egress Filtering)只讓你所屬的位置空間可以向外、隔絕向外之假冒網址、記錄違反的來源之 MAC。對於進入/外出之過濾裡面有一些關鍵的服務例如 Windows 環境的 TCP 與 UDP 135-139 和 445 以及 UNIX 環境之 TCP 23，512-514，TCP 及 UDP 111，2049，6000-6255

等需要隔絕。並且記住要隔絕雙向。對於特殊之例子例如將網路監視委外給其他組織需要提供 SNMP 存取，建議透過 IPSec、SSH 或其他 VPN 技術提供隧道加密通道。

4.3.1 稽核路由器

在稽核路由器部分，總結來說，先確認路由器之功能究竟是網路裝置或是控制裝置，再決定想要的控制項。確認控制是否妥當以及能夠運作，再從功能層面以中間或臨時的報告提出建議。一些稽核路由器的工具及 benchmark 可以在 http://www.cisecurity.org 裡面找到。稽核路由器工具可以解決欠缺 Cisco IOS Benchmark、欠缺 IOS 稽核工具、困難無法維持之一致性、難以偵測改變、需要快速修正不正確設定、需要報告或客製化、需要檢查非 IOS 之裝置的問題。稽核路由器工具不能解決管理的、區域設定選擇、協定之弱點、主機方面問題(例如病毒、Code red) 、供應商程式碼、區域設定選擇等問題。

4.3.2 稽核防火牆

必須先定義的事情:

- 哪些資訊是你的防火牆所要保護的?
- 你對於防火牆的期望?
- 哪些風險將遭遇到?
- 哪些動作得到授權?

防火牆的環境包括:

- 安全政策(security policy):在稽核前先定義防火牆的目的，安全政策必須先定義。
  - 如果沒有安全政策，必須先告知管理階層定義防火牆之目的。
  - 如果你是管理階層，定義防火牆的目的。

- 許多管理者感覺政策是協在防火牆安全設定語言(ruleset language)所以這是用來定義政策的一個好地方。

- 防火牆政策(firewall policy):關於防火牆如何運作的特定需求，諸如:
  - 向內過濾(Inbound Filtering)
  - 控制向外存取(Control Outbound Access)
  - 加密
  - 病毒防護
  - Failover

- 變更控制(change control)
  - 誰必須得到授權對於架構進行變更?例如：
    - 增加或移除防火牆
    - 增加或移除路由器與交換器
    - 變更存取控制表列或路由
    - 何時這些變更得到授權?
    - 增加或移除主機
  - 變更要如何記錄?
  - 變更要如何取消(backed out)?

防火牆的系統管理必須留意:

- 密碼政策
- 增加或移除使用者帳號
- 修補程式更新
- Root/Admin 存取
- 標準化及安全建置防火牆平台

從上得知已經定義防火牆的目的，接下來要做的是覆核

(reviewing)防火牆的技術環境，記得一個關鍵字:SIMPLICITY!

技術環境:

- 防火牆架構
- VPN 設備
- 測試防火牆
- 測試防火牆規則
- 測試防火牆應用程式
- 告警(Alerting)與記錄(logging)

資訊敏感度分級可包括：

- 關鍵性資訊
  - 貿易資訊重要營運數據
- 維運資訊
  - 需要全部任務的操作
- 管理和設定
  - 內部操作及基礎建設

定義資訊將如何流動?那些資料留是得到授權的?哪些是沒得到授權的?所有的防火牆和週邊設備設計者傾向使用實體圖，因此稽核人員必須能夠從實體圖簡化資訊流動為邏輯圖。邏輯圖的目的是在顯示資訊的流動，因此允許擬定亦資料如何流向?安全政策定義哪些得到授權哪些沒有得到授權?防火牆的目的就是在控制資訊的流動。

資訊的流動可考慮

- 網際網路能連接 http 及 https 到網站伺服器
- 網站伺服器可查詢資料庫伺服器
- 管理站台可以藉由 SNMP 管理系統
- 協同資料庫和電子商務資料庫可以交換資料

防火牆架構的議題包括

- 實體的架構(switch)
- 網路位址轉換(Network Address Translation)
- 防火牆形式
- 週界(Perimeter)的設計
- Screened Subnet

防火牆的型態包括

- 封包過濾器(Packet Filter)-快速、低安全性、路由器就是一種封包過濾器
- 狀態檢查(State Inspection)-中等性能、中度安全，FW1 和 PIX 使用 State Inspection
- Proxy 和 Application Gateway-慢速、高安全性

防火牆介接形式有單一防火牆而沒有路由器(Single Firewall no router)、單一防火牆加上邊界路由器(Single Firewall border router)、一些通過 GCFW 證照者所設計的架構如 SFBR、DFF、雙重防火牆與邊界路由器(Dual Firewall Border Router)、雙重排列防火牆(Dual Inline Firewalls)、與 VPN 介接的防火牆、Firewall VPN 與 Border Router 等等。

防火牆架構的覆核必須考量:

- 你可能需要增加或移除防火牆?
- 你可能需要增加或移除網路裝置?
- 架構程序是否被遵循?

下一步你該考慮防火牆本身?首先防火牆平台的設定是否安全?

許多防火牆有如在已存在的作業系統頂端當作應用程式(例如 FireWall-1 或 SunScreen)，也有其他防火牆有如裝置(Appliance，例如 Nokia 或 Pix 裝置)，作業系統和防火牆應用程式緊密結合。

裝置式的防火牆其平台一般都完整地安全，從底端往上設計有如防火牆裝置。而裝置防火牆的缺點在於封閉或是專屬性。你必須相信製造商創造安全的平台給防火牆應用程式。

應用程式型防火牆其作業系統的好處在於你對於作業系統有極大的控制，有些如 Linux 或 Solaris 甚至提供 source code，你甚至可以提對於平台如何操作？牽涉哪些風險以及如何將風險減低等等有更好之瞭解。對於作業系統之安全有極大之控制也代表有很大的機會犯錯。

如果作業系統專屬於防火牆廠商的，那我們在這邊不談。如果作業系統屬於防火牆之平台，越少軟體安裝在上以及越少服務在上面執行越好。防火牆絕對不需要安裝或是執行的裝置不要安裝。確定防火牆保持最小之安裝軟體，如果你可以移除以下的軟體，則開始進行:

- X Windows 或圖形介面相關軟體
- NIS/NFS/RPC 相關軟體
- 編譯器、諸如 PERL 或 TCL
- 網站伺服器、管理軟體

大部分的作業系統提供其專屬的工具以決定哪些軟體已經安裝：

- Solaris: pkginfo
- Linux:rpm -q
- NT:控制台-新增/移除程式

最少的服務:

移除任何不需要的程式，這是你的防火牆，應該只要執行防火牆應用程式即可，你可以移除的服務包括：

- UDP(SNMP、DNS、Syslog、NTP)
- DNS 或網站伺服器
- 管理應用程式
- ICMP (Kernel 如何回應給 ICMP?)

有許多工具可以決定哪些服務在作業系統上執行，例如：

- UNIX:lsof-i、netstat –a、ps-aef
- NT:控制台->服務、netstat –a、Fport

也可以從網路層來確認服務，掃瞄網路平台，但把過濾功能關掉，可以評估當防火牆不再作業時，哪些危險存在?

掃瞄所有的埠號，從 UDP 及 TCP，確認所有打開的埠號，確認 Kernel 對於 ICMP 如何設定，例如：

- ICMP 要求(request)
- ICMP 網路遮罩要求(Netmask Request)
- ICMP .重導(redirect)
- ICMP 主機無法到達(Host unreachable)
- ICMP 廣播(broadcasts)

在 NT 上的掃瞄工具包括

- WS Ping Propack
- NTObjectives PacketX
- nmap NT

在 Unix 上的掃瞄工具包括

- Nmap
- hping2

ICMP 設定要確認系統沒有打開的 ICMP 設定：

- 未包含 ICMP 廣播路由
- 不對 ICMP 廣播回應
- 忽略 ICMP 重新導入
- 忽略時戳需求

同時要覆核系統之防禦工事，例如覆核作業系統之規格，像是：

- 檔案權限
- 使用者帳號/密碼
- 信賴關係(.rhost、domains)

將防火牆打開，類似你稽核作業系統時所用的工具，決定有多少服務在執行，使其他額外不需要的防火牆服務關閉。防火牆設定的準則應該是關閉所有的存取並確定掃瞄了每一介面。對於修補程式必須確保作業系統和防火牆應用程式已經使用最新的修補程式，例如 Linux up2date、Solaris patchdiag，NT 可參考微軟網站 www.microsoft.com。

對於防火牆的稽核，總結來說防火牆應該僅是防火牆而不該在防火牆上執行其他不必要的程式，消除所有不必要的軟體、應用程式和服務，覆核所有的防火牆平台和防火牆應用程式，注意程序書並且透過訪談檢視是否照程序書撰寫的執行。留意授權的經過、變更控制(Change Control)以及防火牆規則的備份。

稽核防火牆設定將在防火牆環境裏確認問題、錯誤設定以及弱點，一旦確認問題你可以修正這些問題並學得如何處理，因此創造出

更安全的環境。

建議留意以下幾個網站

- 防火牆系列

http://www.enteract.com/~lspitz/papers.html

- 工具/方法:

http://packetstorm.securify.com

http://www.insecure.org/

4.3.3 稽核與防止入侵撥接系統

侵入撥號系統的方法和其他入侵步驟非常類似：腳步拓印、掃瞄、列舉、進攻，這些工具會有計畫地去撥大量的電話號碼，然後將正確的資料連線記錄下來，然後企圖辨認電話線另外一端的系統，接著試圖以常見的使用者帳號與密碼登入該系統。侵入撥號系統的工具在稽核這邊的作用面則是找出組織或公司裡面有弱點的 Modem。

在這部分的介紹裡，描述如何有效稽核 modems 作為貴公司經常性的安全程序，介紹商用和免費軟體，描述如何保護你的基礎建設避免未經授權的 modem 存取。稽核的完整方法裡面，包括列出財產清冊，將所有使用中的 modem 建檔，建置預防性的控制措施，維護財產清冊。

對於想發起入侵撥接者，其思維一開始會考慮以下幾個問題:

- 權限: 在駭客和安全顧問之間的區別在於權限，在進行任何連線掃瞄前需得到書面的許可。
- 誰:定義範圍

避免緊急電話及分機

- 從那邊開始撥接
- 將入侵撥號裝置(war dialing)放在PBX之後以防止DID限制以及電話費
- 何時?連假三天最方便
- 多久?每月?

要入侵撥接系統需準備以下工作:

- Disable 電源管理及螢幕保護程式
- Disable 傳真軟體
- 和區域網路實體隔離
- Disable 語音電子郵件通知
- 不共用線路
- 將自動回覆關閉(一般設為內定，但必須確定)

入侵撥接系統的軟體在自由軟體部分包含

- THC-Scan(Dos/Windows):
  - 是由一個叫做 The Hacker's Choice(THC，http://www.infowar.co.uk/thc/)之駭客團體的前輩 Hauser 所寫。
  - 可在 http://www.securityfocus.com/tools/47 下載。
  - 達到所有功能再加上一些額外特色。
- PhoneTag(Windows)
  - 可在 http://www.securityfocus.com/tools/49 下載。
  - 透過圖形介面容易使用
  - 容易產生撥號表列產生器(可以輸出為 txt 檔案作為其他軟體之使用)

入侵撥接系統的軟體在商用軟體部分包含

- Sandstorm 的 PhoneSweep:http://www.sandstorm.net/

- SecureLogix 的 TeleSweep Secure:http://www.sandstorm.net/

在 http://www.networkintrusion.co.uk/wardial.htm 則有自由軟體和商用軟體之評選報告。

對於使用中的 Modem，要使用以下之稽核檢查表檢查各類狀況:

1	有無警告橫幅?(warning banner)警告橫幅是否違反民法或刑法等法律?
2	是否撥入之橫幅顯示任何系統資訊?
3	在斷線前的錯誤登入嘗試允許次數
4	是否錯誤登入嘗試會顯示資訊?例如有效的用戶名稱?
5	是否在鑑別前有任何功能可被使用(例如 help)
6	是否該 Modem 獲得授權可以進行官方之功能?

4.3.4 無線區域網路安全

對於無線區域網路通信而言 I.E.E.E. 802.11 是無線區域網路 Medium Access Control (MAC)及實體層的規格，其中資料加密可採用 WEP-Wired Equivalent Privacy(WEP)，身分鑑別可採用 Shared Key Authentication，這兩者都是選擇性的，目前仍有不少無線通信設備出廠時將此兩機制選項關閉。SSID(Service set identifier)其作用像是網路名稱，可以程式寫入每一個站(例如 Access Point 和每一個無線的用戶端，Access Point 是無線的站台，允許無線用戶端透過他與其他網路或用戶連接)。如果沒有 SSID，用戶端無法獲得存取若想取得免費的 IEEE 802 標準可到 http://standards.ieee.org/getieee802/下載 pdf 檔案。SSID 和 MAC 位址以明文傳遞、AP 在內部網路會避過網際網路防火

牆、以及 802.11b 標準遭受 shared key method 攻擊、在 Access Point 之 SNMP 大量打開、而未經鑑別的 Diffie-Hellman Key agreement 會令 Man-in-the-middle 攻擊顯示 session key、128bits WEP 則會受到不同的密碼攻擊，但還是比沒有 WEP 好、、、這些都是無線區域網路通信發展上的問題。

要解決相關問題可以更新你的資訊安全政策使得無線 AP 需要權限才能接取、使用，使用用戶端鑑別以及金鑰管理、對於無線區域網路裡面向內的通信設為非信任區或是使用點對點的 VPN、在無線用戶端使用個人防火牆、對於 AP 注意實體安全、調整 AP 信號強度以降低影響、使用 128 bit WEP 加密或是使用無線稽核工具裡面的一些免費軟體，例如 Net Stumbler。

4.4 稽核網站與相關應用

4.4.1 課程簡介

諸如政府網站首頁被攻破、機密資料被竊取、線上購物、訂閱或網路銀行等應用層之弱點或漏洞無法用前兩天課程介紹的免費的網路層工具找出來。第三天的課程展現如何找出遠端用戶可能發現的網站漏洞。老師展示了一張安全檢查表，涵蓋了使用易取得之軟體和手動技巧可以處理的問題。教材以 Step by Step 方式呈現，有助於學習。所有技術及工具使用 Windows 平台展現，但也包含在 Unix 上執行類似測試的註解。

在本日課程涵蓋了資訊聚集攻擊(Information Gathering Attacks) 、使用第三者軟體可能暴露用戶資訊、阻斷式攻擊、用戶簽退過程、緩衝區滿溢攻擊(Buffer Overflows)、連線追蹤(Session

Tracking) 、如何改進伺服器端邏輯、伺服器端技術以保護用戶資料和敏感性資料、網路瀏覽器安全性問題、交易層問題、Get vs. Post、JavaScript 過濾器、在 Server 端交談期與交易時的鑑別、用戶密碼蒐集與破解、作業系統和網站伺服器端弱點等等問題。

4.1.2 稽核網站伺服器

討論三大重點產品:Apache、Microsoft IIS (Internet Information Service)、iPlanet/Netscape 之稽核。在網站伺服器的稽核方面，高階的檢查表包括:

1	獲得官方公司的政策、程序以及標準/指引，為求完整性，將之與最佳實務(Best Practice)比較，記下差異之處。尤其必須注意作業系統、網站伺服器、第三方產品以及編碼的安全實務
2	對應相關安全政策與標準，稽核作業系統，記下其差異之處。
3	針對相關政策與指引稽核網站伺服器並記下其差異，尤其是不需要或有危險的檔案、網站伺服器的使用者帳號與權限、Log 檔案
4	以相關的政策、標準稽核第三方的軟體(例如 Application Server)。
5	記下相關補強(patch)程序與工具，如果遺失必須記下來。
6	使用掃瞄工具並記下結果
7	掃瞄預設及實質的目錄
8	根據使用的軟體或網站產生弱點的表列(例如透過 http://www.securityfocus.com/bid 弱點資料庫或是 根據供應商名稱、產品名稱以及關鍵字在 Cassandra 網頁 https://cassandra.cerias.purdue.edu/main/index.html 之入侵

	事件回應資料庫產生弱點剖繪檔案)

Cassandra 網頁使用 https 保護傳遞的資訊，因為可能牽涉到貴公司的設備與網路組態，怕被駭客有機可乘。Cassandra 的弱點資料來自美國國家標準與技術研究院(National Institute of Standards and Technology，NIST)的 ICAT Metabase。Cassandra 提供到 ICAT 良好的介面並且藉由輸入作業系統、供應商名稱、產品名稱以及關鍵字提供無數的剖繪。每當有新的弱點吻合 ICAT 資料庫中你所儲存的剖繪，則會以 e-mail 告知。

在 Web Server 廣泛用途的安全工具，在開放程式碼部分以 www.nessus.org 所提供的 Nessus 最有名。商用的則以 www.iss.net 之 ISS 以主機式弱點掃瞄工具、www.intrusion.com 之 Security Analyst 針對 windows based 系統及 www.rapid7.com 之 NeXpose，是最佳的網路弱點掃描器。對於 Web Server 必須留意某些廠商提供的特定資源，例如 Microsoft 可參考 www.microsoft.com/technet/security/default.asp；iPlanet 可參考 http://developer.iplanet.com/tech/security/；Apache 可參考
Tutorials: http://httpd.apache.org/docs/misc/tutorials.html
Security Tips: http://httpd.apache.org/docs/misc/security_tips.html
負載測試工具參考 http://httpd.apache.org/test/flood/

對於安全的安裝、設定及維護 Microsoft IIS 之檢查表可在 http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/chklist/default.asp 看到

例如對於 IIS 5.0 基礎的安全檢查表包括

1.	對於虛擬目錄設定適當的存取控制表(ACLs)

2	設定適當的 IIS Log 檔存取控制表
3	啟動 Logging
4	移除所有的範例應用程式
5	移除所有的 IISADMPWD 虛擬目錄
6	移除不用的 script mappings

這些步驟對於系統管理者安裝 IIS 網站伺服器很重要，同時也成為稽核人員安全檢查表一個很好的起點。詳細步驟則可以在 http://www.microsoft.com/technet/security/tools/chklist/iis5cl.asp 看到。

http://www.microsoft.com/technet/security/urlscan.asp 則有微軟的工具 URLScan 提供過濾所有進入 IIS 網站伺服器的需求(request)，必須吻合由管理者所設定的安全準則。

4.1.3 隱藏的內容(Hidden Content)

對於伺服器輸出必須留意隱藏的內容，其安全檢查表如下:

1.	分析用戶端程式碼是否有不需要的資訊，例如註解(Comments)或 Meta tags
2	從伺服器端分析 HTTP 協定是否有不需要的資訊，例如伺服器標頭檔 Server Header、用戶的標頭檔(X-)
3	分析位址列(URLs)及鑑別碼(authentication credentials)是否有可能 Java applets 等被反組譯?
4	從每一個已知的目錄擷取 robots.txt 檔案並做檢視

4.1.4 加密與鑑別

對於資料加密的稽核，我們採用以下的安全檢查表作為總結:

1.	驗證所有顯示敏感資訊的的網頁都使用加密送出
2	驗證所有需求敏感資訊的的網頁都使用加密送出(例如可見

	SSL 的加密鎖)
3	驗證所有需求敏感資訊的的網頁都將使用加密送出
4	執行加密模組清查，並以目前的最佳實務或政策確認

不過實際上若要完成本份檢查表，會花比你所想的還要久的時間，因為牽涉到檢查許多網頁以及每一個 form。

對於敏感性輸出的安全檢查表

1.	是否使用加密?
2	是否顯示瀏覽器加密鎖
3	是否對於伺服器使用反快取(anti-caching)技術
4	是否對於使用者下載安全資料檔案提供告警訊息

鑑別方法(Authentication Method)的安全檢查表

1.	用戶端憑證: 確保任何有 PKI Enabled 的系統都被稽核 測試被廢止之憑證能否被允許存取
2	Form-Based: 確保 form 方法為 Post 並使用加密
3	HTTP Basic Auth: 確保所有附帶信物的需求檔都被加密
4	所有的鑑別方法 參見 Sign-On 稽核方法

Sign-On 稽核方法

1.	經法律核准的告警橫幅(訊息,warning banner)
2	使用簡要的錯誤訊息避免用戶資訊洩漏
3	所有牽涉信物(credentials)的都經加密
4	密碼輸入數次以上強迫登出機制(Confirm Lockout Mechanism)

	降低暴力攻擊法
5	對於 DDos 之攻擊防範
6	登入程序若不活動則 timeout 以避免半開程序

另外有 rfc 於 ftp://ftp.isi.edu/in-notes/rfc2617.txt，可供參考。

Sign-Off 稽核方法

1.	建議使用簽退(Sign-off)過程
2	確認網頁使用反快取(anti-caching)技術
3	是否在某交易期(Session)內不活動會自動簽退?

Session IDs

用戶輸入敏感性資料之安全檢查表

1	記下所有的 Form 方法，對於敏感性輸入必須使用 post
2	參見 encryption 安全檢查表(SSL、frames 等)

用戶輸入測試的安全檢查表

1	測試每一個 form element --記錄使用的 permutation list --記錄每一個 verbose 錯誤訊息
2	測試所有作為輸出的 HTTP 標頭檔案 --記錄使用的 permutation list --記錄每一個 verbose 錯誤訊息

本部分課程的講義作者為 David Rhoades，他所開的資安顧問公司網站 http://www.mavensecurity.com/ 提供相關的資源。並且留有電子郵件帳號 drhoades@mavensecurity.com 歡迎大家提供意見回饋。

4.5. 網路稽核

第四日的課程展示了許多網路安全專家可以稽核或評估網路之技術，依照深度防禦之技術，本課程告知學生如何稽核周邊裝置，產生尚存活之主機與服務的圖形，並評估這些服務的弱點。具備 Windows 或 Unix 背景的學生可從這些 Step by Step 的範例與活生生的展示免費工具與觀念中獲益。

執行完整基礎建設網路稽核的七步驟方法(The seven-step method)可將原本大量的稽核與安全工作切分為有意義的範圍。這項方法首先設計於稽核或提升高風險區域的安全。將這部分的工作自動化可使您只要按一些鍵盤按鈕，弱點的輪廓乃至於任何新的威脅等等很容易可以發現出來。

本日課程的重點包括什麼是弱點評估?弱點評估為何如此重要?調查弱點評估工具。什麼是 Nlog?下載及安裝 Nmap 與 Nlog、瞭解 Nmap 的特色和功能、如何描繪網路、網路駭客想知道哪些訊息、如何從外部描繪出網路架構?稽核周邊防禦、將描繪結果組織起來、確認弱點。後續跟隨的活動包括滲透測試、使用 Nessus、排定弱點補強之順序、定期網路描繪之效益以及找尋被破壞之主機等等。

一開始老師先簡單複習 TCP/IP，然後進行背景介紹、描繪網路(Mapping your network) 、確認及降低弱點，最後則將所有東西整合在一起。在稽核裡面協定所佔的角色為弱點評估針對 TCP/IP 裡面的應用層，描繪網路針對傳輸層和網路層。總結來說 TCP、UDP 和 ICMP 是三種主要的通訊協定，RFC 768、791、792、793 詳加敘述協定規則，使系統可以在給定刺激下可預期地反應。稽核員可以善加利用來稽核。

nmap 是由 Fyodor 所撰寫的，能提供豐富的 TCP 與 UDP 掃瞄能力，用 nmap –h 可以看到其詳盡的用法與特色。例如 Nmap –o 可以允許我們輸入一個範圍例如 192.168.1.1-192.168.1.254，加上-o 讓輸出的結果儲存在指定的檔案中，而且產生方便人們閱讀的格式。Nmap 可以從 http://www.insecure.org/nmap/index.html 下載得到。

其他免費軟體的掃描器包括 Foundstone(http://www.foundstone.com/knowledge/scanning.html)提供兩種免費的工具，第一個是 ScanLine(之前稱為 FScan) ，類似 nmap 的命令列掃瞄工具，但不需要額外的驅動程式，安裝簡單。另一個 Foundstone 選項則是 SuperScan 公用程式，Superscan 只會執行 ping scan 以及 TCP scan，但它會產生簡單的安裝路徑並提供視窗圖形介面。

埠掃瞄器(Port Scanner)可執行許多不同種類的掃瞄，有些帶有危險性。標準的掃瞄例如 ping scans 或 TCP scans 頗為直接且無害。然而包括 nmap 在內的某些掃描器，會執行不同目的之掃瞄，包括會繞過防火牆(firewall)或入侵偵測系統。Nmap 也能執行堆疊指紋(stack fingerprinting)，以很高的成功率嘗試決定在目標主機執行的 OS 版本，例如透過傳送非有效的 TCP flag combinations)並觀察從目標系統傳回來的反應。堆疊指紋有可能使系統當機或掛掉。請確認你有權限執行掃瞄。

從掃瞄的結果我們必須決定哪些服務對應到那些埠號，內部掃瞄會協助你達到此目的。研究在內部或外部之描述，防火牆可能會干擾掃瞄，Windows 可能會執行一些自己說給自己聽的埠號。從掃瞄的結果決定必須使用的服務，將不需使用的服務關掉。

4.5.1 刺激與回應

4.5.1.1 通訊協定基礎

無庸置疑，通訊協定是網路稽核的基礎背景知識之一，稱職的稽核人員須了解 OSI 架構、TCP/IP 架構及各相關通訊協定。比較常見的通訊協定有：

- 應用層：FTP, HTTP, DNS,
- 運輸層：TCP, UDP
- 網路層：ICMP, IP
- 連結層：ARP, RARP

其中最重要的當然是 TCP/IP 通訊協定。雖然此次課程有列出幾本英文版的參考書目，但是，市面上已經有不少中文版的此類書籍可供參考，因此不再贅述。

另外，有個網頁值得一提，欲查詢各通訊埠的指定(assignment)情形，可造訪：

http://www.iana.org/assignments/port-numbers 。

4.5.1.2 刺激與回應

事實上，所有的通訊協定都適用「刺激與回應」模式，給予一個特定的刺激，將會得到一些預期的回應。稽核工具利用這個好處，稽核人員也該了解並運用它。

各通訊協定的 RFC 詳細定義了「什麼樣的刺激該給予什麼樣的回應」，如有疑義應以 RFC 為準。RFC 可於 www.rfc-editor.org 取得，常見的有：

- RFC 768: UDP
- RFC 791: IP
- RFC 792: ICMP
- RFC 793: TCP

有些通訊協定的回應異於常規(abnormal)，稽核人員也該具備這方面的知識，例如：

Active FTP: 主要的通訊埠為 port 20 而非 TCP 慣用的 port 21。

Traceroute: UNIX 的 traceroute 指令使用到 UDP 與 ICMP 兩個通訊協定。

大型 DNS: UDP 有 512 位元組的長度限制。所以超過 512 位元組的大型 UDP DNS，會動用到 TCP 通訊協定。

知名埠對知名埠: 一般 TCP 通訊協定是一個臨時產生的(ephemeral)通訊埠對應一個知名(well-known)的通訊埠，但有些通訊協定的兩端都是知名埠。例如 NetBIOS 或 bootp 等通訊協定。

4.5.2 專家用語與方法

4.5.2.1 術語

了解弱點評估的程序之前，須先確定一些術語。

查字典，字典會告訴我們「threat」這個名詞有「威脅」的意思。就弱點評估的領域而言，簡單講，所謂「threat」，是指對我們的系統「造成傷害的可能性」，它可能以各種形式存在，也可能發生於各個不同的地方。

所謂「threat vector」，是指這些 threat 從何種途徑進入我們的系統。主要有五種：

- 來自網際網路的外來攻擊
- 來自電話網路的外來攻擊
- 來自區域網路的內在攻擊
- 來自近端系統的內在攻擊
- 來自惡意程式碼 (malicious code) 的攻擊

所謂弱點(vulnerability)，是指這些 threat 入侵並造成傷害的管道。弱點遍佈各處，網路、系統、應用程式、政策、或作業程序 均有可能。

所謂弱點評估，是指找出系統或管理上的安全漏洞的一種嘗試(attempt)。弱點評估是決定風險等級的基本工作。

4.5.2.2 方法

駭客要能利用一個弱點入侵，必須三個條件缺一不可：

- 剛好主機上有個弱點服務在執行；
- 剛好防火牆允許存取這個服務；
- 剛好有利用該服務搞鬼的方法。

所以，對症下藥，降低風險的方法就是：執行弱點評估工具或稽核工具，仔細研究其產生的報表，再針對各弱點補救，修復有問題的地方。

弱點評估分為主動評估與被動評估兩種，前者主動測試系統，後者則被動檢查系統。

Nmap 可以用為主動評估弱點的工具程式，Nmap 發出網路封包，根據受測系統的回應，可以發現系統的弱點。當然，這些資訊也可以被駭客拿來攻擊系統。而且，用 Nmap 執行弱點掃描可能造成電腦當機或服務中斷，使用時不可不慎重！

美國 FBI 追蹤因為使用 Nmap 掃描弱點而當機的案例，並出版了一份名為 CyberNotes 的報告，可於下述網址取得：
http://www.nipc.gov/cyberarchive.htm 。

4.5.3 網路對應工具

4.5.3.1 工具箱

弱點評估或稽核的工具有很多種，可以大概分為 3 大類：

- 網路對應：偵察通訊埠產生對應表，例如 Nmap。
- 被動弱點評估：竊聽封包，例如 TCPDump 或 WinDump。
- 主動滲透測試：例如 Nessus。

每個工具都有其長處及不足之處，針對同一問題如果使用不同工具測試，再交叉比對其結果，必定更能發現問題。為了方便使用，最好是將它們收集成工具包(toolbox)，而且三大類工具都要包括。

4.5.3.2 安全掃描網路的 7 個 P

- 計畫掃瞄(plan the scan)
- 發展策略(Develop a policy)
- 獲得授權(Get Permission)
- 宣告掃瞄(Publicize the scan):讓管理者有時間適當修補
- 可接觸的(Be present):如果發生狀況，要找得到你
- 提供回饋(Provide pheedback) (其實是 feedback！)

4.5.3.3 Nmap 及其相關工具

Nmap 是個網路對應工具，它對各個通訊埠發出封包，收集回應，並據以了解各個通訊埠是否正在使用。這些動作同時也能得知主機、作業系統、網路服務、通訊協定等各式各樣的資訊。

Nmap 及其相關軟體可於下列網址取得：

- http://www.insecure.org
  (UNIX)
- http://www.eeye.com/html/Databases/Software/nmapnt.html

(WinNT/2K)

- http://sourceforge.net/projects/nmapwin
  (nmapwin)
- http://netgroup-serv.polito.it/winpcap/
  (Packet capture driver)

nLog 是 nMap 的輔助工具，可以將 nmap 的 ASCII 版的輸出轉為資料庫格式，可以以主機或通訊埠為條件做查詢(query)，也可轉為瀏覽器(browser)版本。NLog 可於以下網址下載：

http://www.secureaustin.com/nlog

NDiff 也是 nMap 的輔助工具，利用 nmap 的輸出檢查系統是否有變動，可於以下網址下載：

http://www.vinecorp.com/ndiff/

4.5.3.4 封包產生工具

Superscan 掃描 TCP 連線以找出開放的通訊埠。

Hping2 是個客製化 TCP/IP 封包的網路工具。

Nemesis 是一組封包產生工具，包括 nemesis-arp, nemesis-dns, nemesis-icmp, nemesis-igmp, nemesis-ospf, nemesis-rip, nemesis-tcp, 以及 nemesis-udp 等八個工具程式，分別產生對應的封包。

4.5.4 主動與被動稽核工具

TCPdump 與 WinDump 屬於被動的評估工具，TCPdump 是 Unix 版本，而 WinDump 是 Window 版本，它們是封包竊聽器，記錄流經該竊聽程式所在網路介面的所有封包的詳細資訊，這是絕大多數入侵偵測系統的基本功能。TCPdump 可於 http://www.tcpdump.org 取得；WinDump 可於 http://netgroup-serv.polito.it 取得。

Ethereal 可說是圖形界面版的 TCPdump，可於 Unix 上執行，也可於 Window 上執行。Ethereal 可於 www.ethereal.org 取得。

4.5.5 弱點稽核工具

Nessus 除了弱點掃描之外，還可執行滲透測試。Nessus 可於 http://www.nessus.org 取得，具有以下特點：

- 可以作為弱點掃瞄工具
- 比 Saint 還需要更多手動操作
- 採用 Cilent-Server 架構
- 可作為滲透測試
- 自由軟體

Nessus 是優秀的安全掃描器，和其他弱點掃描器相比，在大環境其特殊設計提供部署一致性的弱點掃瞄是很特殊的，大環境可能使用許多弱點掃描器，而得到的結果在不同的網路間不一致。藉由 Client 及 Server 組成之不同以及槓桿效應，解決上述問題。Nessus Client 端軟體可以支援 Windows 及 Unix，Server 則必須安裝在 Unix 環境。

Nessus 有四個套裝軟體必須下載以便安裝 Nessus，要安裝你必須依照以下順序來編譯軟體:nessus-libraires、libnasl、nessis-core 以及 nessus-plugins。Nessus 為模組化的架構，幾乎只要駭客團體寫了惡意程式碼來利用弱點時，稽核/弱點掃瞄社群就能創造 Nessus 所需之外掛程式供弱點掃瞄，自由軟體 Nessus 提供至少 1100 種弱點。

4.5.6 網路弱點稽核方法

- 決定責任區域
- 研究弱點和風險
- 將週界安全
- 使非戰區(DMZ)安全
- 減少外部存取之風險
- 減少內部存取之風險
- 找尋特洛伊木馬程式

4.5.7 課程總結

- 弱點掃瞄昂貴、困難而且花時間
- 作為管理者，網路設定管理可能是個惡夢;做為稽核者要瞭解網路設定管理可能有問題
- 網路掃瞄工具:Nmap
- 被動弱點評估工具:TCPDump
- 主動滲透工具:Nessus
- Nmap、Nessus 以及其他工具可幫助我們解決上述問題，並且可以在一些簡單步驟後應用

4.6 進階系統稽核-Windows

Windows NT 及 2000 機器構成多數典型 IT 基礎建設的大部分，不過很不幸地這些機器通常也是最難有效控制使之安全的部分。第五天的課程協助將第一天所討論的策略與高階控制及目標運用到實際工作上。

第五天的關鍵課程包括在遭受破壞之電腦系統裡面要找哪些東西出來要如何找?課程包括使用 Windows NT 與 2000 以及免費與商用

軟體來評估或稽核視窗作業系統。經過整天的課程，參加者有機會使用以網路為基礎之稽核工具來測量活躍之系統，因此而得到必要之手動操作經驗。學員在此課程也會學到一些鑑識(forensics) 的基礎，當你在稽核過程中發現某些事情需要更進一步調查(investigation)時。

第五天的課程內容重點包括建立自己的稽核工具，檔案完整性之評估、稽核以確保安全的設定，諸如讀取 Logfiles、密碼評估工具、風險評估、哪些工具可以使用等等。在稽核以決定哪些地方做錯的部分，諸如找尋隱藏的檔案空間、事件重建、鑑別後門、破解程式的詳細分析都做了詳盡的介紹。在電腦犯罪事件調查方面，如何建立調查工具、備份的工具以及證據保存鏈(Chain of Custody)等都有詳盡的介紹。密碼評估工具使我們很容易瞭解到過短的密碼、純數字的密碼、採用單字或生日的密碼極容易被破解。本日的課程內容主要提供 Windows 2000 和 XP Professional 之稽核為主，但有些內容一樣可以適用於 Windows NT。而除了提供稽核之用，也供系統管理者把系統維護得更安全與有效。

4.6.1 安全檢查表可參考的資源

在 Windows 之稽核方面，建議先決定範圍、是否有足夠之政策可以使用，是否和最佳實務一起共用，再來可將微軟 Microsoft、美國國家安全局、美國國家標準研究院等等之參考資源放在你的安全檢查表：例如

1. 微軟的安全工具和檢查表主要網頁包括大量微軟產品的檢查表以及許多不同的工具:
http://www.microsoft.com/technet/security/tools/tools.asp，例如 Microsoft Baseline Security Analyzer，

2.Securtiy Operation Guide:提供 Windows 2000 Server 安全安裝、操作和稽核詳細的指引，包含可下載的 scripts 來自動化不同的管理及

安全工作。可在
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/secwin2k/default.asp 線上瀏覽或下載 Adobe PDF 格式之電子檔。

3.經認證的設定:Windows 2000 曾被評估為符合通用規範(Common Criteria)，微軟提供許多在 Common Criteria 標準下操作文件及設定範本，例如:

Windows 2000 評估設定管理者指引(Windows 2000 Evaluated Configuration Administrator's Guide)

http://www.microsoft.com/technet/security/issues/W2kCCAdm/default.asp

Windows 2000 經評估設定安全設定檢查表(Windows 2000 Security Configuration Checklist for the Evaluated Configuration):

http://www.microsoft.com/technet/security/issues/W2kCCSCG/W2kSCGce.asp

Windows 2000 經評估設定用戶指引(Windows 2000 Evaluated Configuration User's Guide):

http://www.microsoft.com/technet/security/issues/W2kCCUG/default.asp

4.美國國家安全局 (US National Security Agency，NSA):
http://www.nsa.gov/snac/index.html

美國國家安全局出版一系列提供許多不同方面的 Windows 環境之免費指引 (從 OS 到 Active Directory 至 IIS 與 Exchange)

5.美國國家標準與技術研究院(US National Institute of Standard and Technology，NIST):其電腦安全資源中心於
http://www.csrc.nist.gov/提供使電腦系統安全之詳細指引

4.6.2 如何開始稽核 Windows?

若被要求針對微軟作業系統整體安全進行評估，可先確認系統的基礎資訊，例如怎樣的 OS(NT、2000、XP...)?怎樣的版本?怎樣的硬體設定?Service Pack 的程度?哪些 hotfixes 已經安裝?哪些服務正在執行?哪些應用程式已經安裝?

要知道最基本的系統資訊可在 Windows 命令提示工作列輸入 ver 或是使用圖形介面工具 msinfo32 由(開始->執行）可看到作業系統版本、環境變數、Internet Explorer 檔案檔名及變數等等，事實上 msinfo32.exe 在系統摘要的頁次資訊就很足夠。

4.6.3 基本的 OS 資訊

OS 的 Type 例如是 Win NT、Win2K 還是 Win Xp?OS 版本其 build (Kernel) number 或是 Service Pack Level?系統資訊裡面其 uptime、註冊用戶或公司是誰?都是稽核重點。請注意磁碟分割應該為 NTFS，因為只有 NTFS 支援檔案或目錄權限的使用、稽核和加密。

4.6.4 系統漏洞修補與更新

修補安全問題、軟體 bugs 極為重要，其中 Service Pack 是主要的更新，通常是將至今的所有修補程式(patches)累積包裝。大約半年到一年提供一次，通常包含對原始程式增強的程式以及新增的元件；Hotfixes 針對關鍵的(critical)安全與系統問題；QFE fixes(QFE 為 Quick Fix Engineering 之縮寫)則針對單一的問題，不管是廣泛但次要的問題或是只影響到某些特定系統的問題。QFE 修正可能未經過廣泛的測試，而僅是快速修正，暫時解決特定問題而已。因此 QFE 可能一般都沒有對外公開，而像微軟會出版知識庫文章描述問題及修正方式。要得到 QFE 修正者必須直接接觸微軟公司，而 QFE 修正會在經過更

多廣泛測試後包含在稍後的 Service Pack 裡面。

請注意在更新系統時必須測試，並注意未被支援的軟體。許多廣為人知和最易造成損害的攻擊係利用已知有提供修補的弱點。例如 IIS 有許多的弱點(對應的攻擊於下列行列之括號後面)，包含 Remote Data Services(RDS)、buffer overflows(Code Red)、Unicode directory traversal(Nimda)，又如預設的 SQL Server 安裝在 sa 帳號後面為空白的通行碼，因此造成了 Spida、SQLSnake 等蠕蟲攻擊。又如另一個關鍵的 SQL 弱點在 2002 年 7 月已經提供修補，但沒有修補弱點的系統在 2003 年 1 月遭到 SQL Slammer 蠕蟲攻擊。更有許多病毒利用 Internet Explorer/Outlook Express 之弱點使得用戶僅瀏覽受感染或是惡意的 HTML 電子郵件就中毒。

http://support.microsoft.com/default.aspx?scid=fh;[ln];lifecycle 提供了微軟新的產品生命週期政策，企業產品支援七年，消費者產品支援五年，稽核者必須注意一旦某產品未被支援，例如 Windows NT Workstation 在 2003 年 6 月起不再支援，代表不再提供任何產品修正。

安裝 hotfix 可藉由手動或是 Windows update，在安裝過程更新的二進位位元程式複製到磁碟，Registry entry 顯示 hotfix 已經安裝、反安裝之目錄寫到%windir%環境變數(代表 Windows 作業系統安裝的目錄)，通常還需要將系統重新開機。重開機多半是未了將原本將被修補程式取代而鎖定的二進位檔案釋放出來以便新版本能夠複製到硬碟空間。另一理由則是 registry 必須被修改但現在遭鎖定為且作業系統所用，因此需要重開機。再來則是修補程式已經修改檔案和 registry 但必須在系統重新開機後才生效。但是有些關鍵且已經在線上服務的程式不容許隨意重新開機，或是多個修補程式若逐一重新開機很麻煩，現在微軟提供 qchain.exe 將多重修補檔案鍊結起來方便安裝而不必為每一修補程式重新開機，可參見微軟之知識庫文章 296861

"How to Install Multiple Windows Updates for Hotfixes with Only One Reboot"。微軟之安全佈告(Security Bulletin)裡面 MS03-004 之 03 代表目前年份之最後兩位，004 代表今年第四個安全佈告。若用 Windows Update 可使用六位數知識庫文章(six-digit Knowledge Base(KB))例如 810030，要描述 KB 數目和 Security Bulletin 數目之間的關係並不容易，這些都造成用戶之困擾。

4.6.5 如何檢查修補之程度?

Network Hot Fix Checker(hfnetchk.exe)及 qfecheck.exe 都是命令列公用程式，使之容易執行。將之包含在 scripts，且可將之輸入重新導入至檔案中。Hfnetchk.exe 原本是由 Shavlik Technologies 發展(http://www.shavlik.com/)的免費工具，被微軟、the Center for Internet Security 等公司包含在其工具程式中。不過 Shavlik Technologies 仍在維護此工具，會從 XML 資料庫檔案(mssecure.xml)讀取目前的修補程式資訊。Hfnetchk.exe 可檢查 IIS、I.E.、Windows Media Player、SQL Server、Exchange、MDAC，檢查註冊檔、檔案版本和檔案 Checksums 等。

Windows Update 網站(http://windowsupdate.microsoft.com)為使用 Active X 之微軟網頁可以遠端掃瞄電腦並且提供一串哪些修補程式忘記附加之列表，並能自動下載和安裝修補程式(例如 IIS、I.E.、Windows Media Player)。唯一例外的是 http://office.microsoft.com/productupdates/提供微軟 Office 家族修補或元件之更新。另外可以使用 View Installation History 可以列出系列已安裝之修補程式。

微軟之 Microsoft Baseline Security Analyzer(MBSA)為免費可得之圖形化介面程式可執行許多基本作業系統和特定程式如 IIS、SQL

Server、Internet Explorer 之安全檢查。MBSA 也包含所有的 hfnetchk.exe 之功能，因此你可以整合你的修補程式做一個初步的弱點掃瞄。其他一些工具程式例如 Center for Internet Security's Scoring Tool 也有整合 hfnetchk.exe。

qfecheck.exe 可檢查安裝在 Windows 2000 和 Windows XP 系統的 hotfixes，與 hfnetchk 不同處在於 hfnetchk 會透過外部維護的資料庫檢查遺失的修補程式，而 qfecheck.exe 會檢查本地系統，列出已經安裝成功的修補程式。因此 qfecheck.exe 是一致性檢查器(consistency checker)，會確認你所安裝的修補程式確實被正確安裝，檔案沒有被意外刪除或是覆蓋，qfecheck 會留意存在 registry 的修補程式資訊，registry 包含和修補程式一起安裝的檔案及檔案版本。存在 registry 的資訊。

4.6.7 不需要安裝的元件

作業系統的預設安裝通常都不夠安全，元件(component)為特別的應用程式或公用程式，作為作業系統的模組部分，軟體供應商多半考慮方便管理者與用戶使用，而不會考慮對作業系統之安全性。某些元件包含內在的弱點，例如 SNMP(Simple Network Management Protocol)。有些則包含使軟體安全之元件，但卻沒有放在預設安裝裡面。也有些類似 IIS 以軟體臭蟲(bug)的方式帶來弱點，例如緩衝區滿溢 buffer overflow 的弱點，常常造成會自我傳播(self-propagating)的惡意程式碼(malicious code)例如 Code Red 和 Nimda 蠕蟲。而有些系統管理者甚至沒注意到有安裝網站伺服器，因此帶來許多困擾。

4.6.8 不需要的服務

許多預設的服務(Service)並非操作所需要的，有些服務可能包含

弱點--從資訊的洩漏到緩衝區滿溢，建議將不用的服務關閉。和元件採模組化可在作業系統裡面安裝及反安裝不同，Windows 的服務可類比如 Unix 的 daemon，是一種當系統開機後啟動並在背景執行的程序(process)，服務無法移除(除非將載入的應用程式反安裝)。然而他們可被 disabled 並避免執行。執行的服務可能為攻擊者帶來潛在的洞，如果某服務被 disabled 或不執行，將減少主機的洞開的門，同時也增進系統的效能。身為稽核員，必須知道被稽核的主機是否只執行必要的服務和元件。

4.6.9 如何檢查服務?

服務的狀態可被設定為以下三種

1.自動的(Automatic):服務載入並且在啟動時執行，當 OS 執行時也會執行。

2.手動的(Manual):服務在啟動時載入，但仍保持停止直到應用程式需要它時。

3.使不能(Disabled):服務在啟動時並未載入，沒有手動介入下不能啟動。

由於不需要的服務是最常見的弱點之一，先決定哪些服務正在執行，再決定哪些服務是必須的，最後再把不需要的服務關掉。至於要如何檢查服務呢?最基本的資訊來源來自於 Services MMC，從開始→程式->管理工具→服務選取。不過圖形界面資訊有時候並非最方便的格式，因此可用 Windows XP 裡面所附的 sc.exe 來查詢、啟始、關閉及設定服務。Sysinternals 包含一套免費公用程式稱為 psservice.exe，可在 http://www.sysinternals.com 網站下載。PSService 比 sc.exe 多了對於服務的描述。

當我們檢查系統所開的埠，因而檢驗可用的服務，從系統的內部-從本地系統(例如使用 netstat 指令)或是從外部-從外部系統(例如使用 port scanner)來檢查很好，因為基本上這是雙重檢查你的結果。

從內部檢查會顯示所有所有系統確認打開的埠，有可能系統會比從外面掃瞄顯示更多的埠，例如主機有回路回溯(loopback)連結或是藉由主機型防火牆防止外部窺視者看到內部的服務。也有可能掃瞄時從外部顯示的資訊比較多，例如主機被攻破，而負責報告埠情形之程式例如 netstat.exe 被特洛伊木馬取代，此時本地端的 netstat 會顯示假的訊息，而此時外部的掃瞄可以給你更精準的描繪。

4.6.10 從外部進行埠掃瞄

從外部進行埠掃瞄其選項包括 nmap/nmap NT，nmap(network mapper)是命令列工具，是至今最廣泛被使用的免費軟體。雖然 nmap 原本以 Unix、Linux 完成，但是已經有被放到 Windows 之版本。Nmap windows 版本需要你額外安裝 libcap 封包捕捉器，可能對於新手來講比較複雜些。不過 nmap 提供你最大的彈性與選項範圍，駭客也可能使用此種軟體掃瞄你的電腦，因此學會如何使用此種軟體對於進行防禦有極大之幫助。

4.6.11 埠列表

檢查必要服務通常不是那樣容易，記得和管理者討論。並進行自己的研究與實驗。將服務設定到 Disabled，如果設定到 Manual，服務可能仍然應需求啟動。記得檢查服務的相依性，對於 enabled 的服務記得檢查用來執行服務的帳號。

埠列表不是結論性的，但卻是一個很好的地方開始。要先將 process 與埠整合，可使用內部掃瞄透過 netstat –o、Foundstone 的命令列工具 Fport 和圖形界面工具 Vision、Sysinternals TCPView 等方式進行。許多 Windows 埠號會對應到可執行的 service.exe 或

svchost.exe，你可以賭這些服務為 Windows 之預設服務，但這可能不會太有幫助，如果你不能告知這些是哪些服務正在執行。對於 Win 2000，可使用 tlist –s 或是對於 XP，可以使用 tasklist/svc 你不妨參考微軟知識庫的文章 250320 "Description of Svchost.exe in Windows 2000" (http://support.microsoft.com/default.aspx?scid=kb;EN-US;250320) 或是微軟的知識庫文章 314056 "A Description of Svchost.exe in Windows XP" http://support.microsoft.com/default.aspx?scid=kb;EN-US;314056) 。此外並記得檢查 NetBIOS 協定。NetBIOS 協定也有"服務"。Nbtstat.exe 也會顯示有關 NetBIOS 服務相關資訊，例如 nbtstat –n 列出在本地主機之 NetBIOS 名稱，nbtstat –A <ip_address>在給訂 IP Address 之下列出遠端主機之 NetBIOS 名稱。

4.6.12 有關 Users 和 Group

系統只該有有效的用戶，群組有適當的會員，不要遺留空白的密碼，採用適當的密碼政策，使用強韌的密碼。

4.6.13 Windows 稽核總結-使用的關鍵工具

- 針對修補狀態，使用 HFNetChk
- 針對埠掃瞄以及服務，使用 Nmap 或其他類似工具
- 針對用戶、群組及權限，使用 DumpSec
- 針對密碼稽核使用 LC4 或類似工具
- 對於上述以外之其餘項目使用命令列工具
- 針對幾乎所有的事物，使用安全模版和安全設定與分析
- 針對稽核紀錄，使用事件檢視器(Event Viewer)以及日誌管理工具(log management tools)
- 盡可能自動化!

4.7 進階系統稽核-UNIX

第六天的課程類似第五天，但作業系統換為 UNIX、Linux、FreeBSD 及 Sun Solaris，並提供這些系統之基礎及內部工作原理的介紹。參與的人將藉由手動來探索、評估及稽核 Unix 及 Unix-Like 之系統。內容重點包括建立自己的稽核工具，檔案完整性之評估、稽核以確保安全的設定，諸如讀取 Logfiles、密碼評估工具、風險評估、哪些工具可以使用等等。在稽核以決定哪些地方做錯的部分，諸如找尋隱藏的檔案空間、事件重建、鑑別後門、破解程式的詳細分析都做了詳盡的介紹。在電腦犯罪事件調查方面，如何建立調查工具等都有詳盡的介紹。

第六天的課程著重在比較不同 UNIX 品牌間的差異與相似處，提供機會手動操作去經歷三種不同的 UNIX 環境，講課時逐步從標準 UNIX 系統不同的稽核控制談起，同時也會從存取控制和安全模型來談。

第六天課程其中一項重要的特色在於系統 Log 檔案之分析，在描述 Swatch 之使用後，有機會使用此優異之軟體去解析由 UNIX 系統產生之稽核軌跡。此外，也會學習到使用此工具搭配集中式系統 Log 以便產生安全事件告警並執行所有系統報告之有效稽核。

唯有真正了解 UNIX 才能深入稽核 UNIX。根據主辦單位的教學經驗，多數稽核人員對於 UNIX 比較陌生。所以本日課程先從基礎介紹起，先介紹 Unix 的一些基本觀念，包含各家 UNIX 的發展簡史，再循序漸進及於完整的 UNIX 主機分析。

4.7.1 UNIX 基礎

與微軟的視窗系統比較起來，UNIX 是命令列導向的系統，比較適合程式設計師及系統發展者，如果使用過 DOS 或 mainframe 主機，對於 UNIX 比較熟悉比較容易上手。

UNIX 有以下幾個特性：

- 幾乎所有的 shell 都具有可程式的能力，其安全模組都有簡單且公開的特性。
- 常用的功能多為外掛式而非內建於 UNIX 核心本身。
- UNIX 幾乎將所有東西都視為檔案，目錄、硬體設備、網路 socket... 檔案權限分為 Owner, Group, World 三個層次，各有讀寫執行等權限。(可用 chmod 來改變檔案權限。)
- 稽核人員至少必須熟悉以下幾個 UNIX 基礎指令：
  ls, cat, more, less, head, tail, man

UNIX 有以下標準服務(services)：

- Port mapper
- RPCs —— Remote Procedure Call 遠端程序呼叫，用於「分散式計算環境」，允許一個程序完全透通性的執行另一個系統上的功能。 (透過 Port mapper)，
- NFS —— 網路檔案系統
- NIS —— 網路資訊系統
- NIS+
- X —— X-視窗系統，一種網路導向的圖形介面視窗
- CDE —— 共通桌面環境
- Friends

4.7.2 從評鑑到稽核

要稽核 UNIX 系統，有一個很好的切入方法，就是將系統評鑑

(system accreditation)的程序轉化為稽核程序。每個組織在建構其UNIX 系統時都會有個組態控制(configuration control)的程序，良好的組態控制有助於順利建構各主機，也才有安全的系統，也比較容易稽核這些系統。

將評鑑程序轉為稽核程序是很簡單的。以下幾個網站有一些系統評鑑表(accreditation form)、安全檢查表(checklist)、或稽核程序可以參考：

- www.cisecurity.org
  （Windows 2000 及 Solaris 的 Benchmarks）
- www.nswc.navy.mil/ISSEC/Form/AccredForms/index.html
  （系統評鑑表、將政策轉為安全檢查表或系統評鑑表）
- www.nsa.gov
  （安全及組態指引）
- www.sans.org/giactc/gsna.htm
  （GSNA 實作）
- www.sans.org/giactc/gcux.htm
  （GCUX 應用及系統安全實作）

4.7.2.1 檔案完整性評估 (File Integrity Assessment)

檔案完整性評估有助於分析受監測的(monitored)檔案是否被篡改，也使損害評估(damage assessment)變得容易。建置「檔案完整性評估」必須是初始組態的一部份。

市面上有一缸子評估檔案完整性的稽核工具，可以參考www.securityfocus.com 網站，該網站蒐集了許多檔案完整性評估工具的資訊。點選【Tools】，再點選【Auditing】，再點選【File Integrity】即可。

比較受歡迎的檔案完整性評估工具有以下五種，

- Tripwire ASR 1.3.1
- Sherpa
- RIACS
- L5
- AIDE

4.7.2.2 Tripwire

最常見的檔案完整性評估工具應是 Tripwire ，商業版與 OpenSource 版都有。

Tripwire 的用法

1. 安裝所須版本。

如果是 OpenSource 版本，有詳細的指令，安裝之前必須先做 編譯、連結、測試 等工作。

2. 編輯 Tripwire 組態檔。

客製化(customize) Tripwire ，決定基準線，並決定資料庫及資料檔(組態檔、政策檔、指紋檔...)的存放位置。

3. 啟動 Tripwire 。

Tripwire 會根據組態檔對系統執行初始評估，並產生所有相關的指紋檔(指紋資料庫)。

4. 將資料移到安全的儲存媒體以防止被篡改。

指紋資料庫及政策檔(基準線)是最易受到駭客攻擊、篡改的資料，尤其須要注意其變更控制(change control)。保護這些資料的方法有以下幾種：

- 離線複製
- 燒到光碟
- 用 MD5 簽證

除了防範駭客攻擊之外，我們平常也需要控管我們對系統所做的更改、異動。Tripwire 及其同類工具程式，除了可做安全控管(Security Control)之外，也可以做變更控管(change Control)、稽核控管(Audit Control)等工作。其管理程序如下：

1. 將「現行指紋資料」與「已知好的備份」做比對、驗證，
2. 執行管理性異動(administrative changes)，
3. 進行文件異動(document Changes)，
4. 重建指紋資料庫，
5. 產生安全備份，保存於專門處所。

4.7.2.3 RPM

如果是使用 RedHat Linux 系統，有另一種驗證軟體完整性的工具，叫做 RPM (RedHat Package Manager)。顧名思義，RPM 可用來安裝、升級、驗證軟體套件。有一篇名為〈Verifying Files with Red Hat's RPM〉的論文，作者是 Chris Brenton 君，針對使用 RPM 做檔案完整性評估工作有詳細的探討，可參考 www.sans.org/y2k/RPM.htm 網頁。

如果是使用 Solaris 系統，也有類似的工具，名為 pkginfo。

RPM 與 Tripwire 的差別在於，RPM 基本上只能管理經由 RPM 建置的軟體，不是經由 RPM 安裝的軟體完全無法掌控。而 Tripwire 則可驗證整個系統。所以，欲驗證軟體套件使用 RPM 之類的工具，欲驗證整個系統使用 Tripwire 之類的工具。

4.7.2.4 檢查網路服務

欲驗明網路服務可使用 netstat 工具程式，它列出使用中的網路連線(active connections)及其監聽的網路埠(listening ports)。

另一種工具程式 lsof 可列出開啟的檔案 (open files)，此有助於研究執行程序(process)、檔案(file)、及網路狀態(network status)。此工具可免費取得，網址為：
ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/lsof.tar.gz

啟動網路服務的方法有以下數種，

1. 經由 inetd 啟動。
   多數網路服務經由 inetd 啟動，inetd 是個 super daemon。所謂 daemon，是一種特殊的程序，啟動後沒有任何 user interaction，只是持續等待，定期執行某些動作或被動的等待網路連線、喚起其他程序。
2. 經由 xinetd 啟動。
   inetd 是傳統的 super daemon，沒有內建存取控制。xinetd 是改良版的 inetd，內建了存取控制。
3. 經由啟始 startup scripts 啟動。
   例如： /etc/rc.d、/etc/init.d、/etc/rc.local、/etc/inittab 等。

4.7.2.5 TCP-Wrappers

經由 inetd 執行的網路服務並未記錄於 syslog 中，TCP-Wrappers 及其同類程序補足了這個缺口，TCP-Wrappers 審查所有企圖存取這些網路服務的事件，並記錄對方的 IP 位址、以及存取成功或失敗。

經由存取控制清單 (ACLs -- Access Control Lists) 可以完成這個工作。系統管理者必須預先規劃所有這些網路服務的存取權限，並記錄於 /etc/hosts.deny 及 /etc/hosts.allow 兩個檔案，這兩個檔案的內容即是所謂的存取控制清單。TCP-Wrapper 依據存取控制清單決定准許或拒絕各存取事件。

4.7.2.6 UNIX 的記錄檔 (logs)

UNIX 的記錄檔 (logs) 對稽核工作很有幫助。

1. /var/run/utmp

   utmp 這個檔案記錄目前登入的使用者，登入時記錄，登出則刪除。以 who 指令可檢視其內容。

2. /var/log/wtmp

   wtmp 這個檔案記載登入登出事件的歷史記錄、以及一些系統事件。wtmp 為半永久性的資料庫，以 last 指令可檢視其內容。

3. /var/log/btmp

   btmp 這個檔案記載沒有闖關成功的登入企圖。

   btmp 為半永久性的資料庫，以 lastb 指令可檢視其內容。

4. /var/log/messages

   messages 這個檔案記載所有丟到主控台(console)的系統訊息，系統訊息顯示的同時都會保留一份副本於 messages 檔。

   messages 是文字檔，可以直接檢視其內容。

5. /var/log/secure

   secure 這個檔案記載一些與安全(security)及授權(authorization)有關的訊息，TCP-Wrappers 之類的工具程式會寫入這些資料。

   secure 是文字檔，可以直接檢視其內容。

4.7.2.7 檢查修補(patch)狀態

檢查系統的修補狀態可以知道系統安裝或沒安裝哪些修補套件。如果是 RedHat 系統可以用 up2date 工具程式檢查系統的修補狀態；如果是 solaris 系統可以用 patchdiag 工具程式檢查系統的修補狀態；另外，也可使用第三者提供的軟體套件。

4.7.2.8 整體評估工具

評估整個主機的評估工具如下：

- COPS 是一種 UNIX 安全狀態檢查程式，基本上它檢查各檔案及

軟體組態是否受到駭客攻擊。

- COPS_Perl 是較新版本的 COPS。
- Tiger 是 COPS 的加強版。

4.7.2.9 帳號密碼評估工具

評估帳號密碼的評估工具如下：

- Crack
- John the Ripper
- Monkey
- Nutcracker
- Passwd+
- 其他

4.7.2.10 檢查 NFS/RPC 服務是否正在執行

檢查 NFS/RPC 服務是否正在執行

- 檢視 /etc/exports 檔案
- 檢視 /etc/fstab 檔案
- 檢視 /etc/mtab 檔案
- rpcinfo -p 指令可以檢查 RPC 狀態。

4.7.2.11 匿名 FTP

匿名 FTP 也是稽核重點，guest 及匿名 FTP 帳號不應該允許其存取。

4.7.2.12 登入 Banner

登入 Banner 會洩漏不少訊息，給予有心人士可趁之機。應該檢查 /etc/issue、/etc/issue.net、/etc/rc.d/rc.local 等檔案，刪除不必要的訊息，以減少洩密的機會。

因為有很多 UNIX 系統在重新啟動時會重新產生登入 Banner，所以，可以考慮乾脆重新啟動 UNIX，再檢視新版登入 Banner。

4.7.2.13 檢查是否有監聽程式 (monitoring devices)

Sniffer 是一種用來收集帳號密碼組合的監聽程式。網路介面卡若處於 promiscuos 模式則表示有個 sniffer 正在執行。執行 ifconfig 指令並檢視其輸出，可以檢查網路介面卡是否處於 promiscuos 模式。

4.7.3 維護 UNIX 系統安全性與進行稽核

Bastille 是補強 Linux 系統安全性的稽核工具，適用於 Redhat 及 Mandrake 等系統。它可以提供各參數或選項的解釋供使用者參考，由使用者自行輸入來設定自己系統的安全，使用者親和性 (user friendly) 十足。而且，Bastille 可以設定成自動維持設定的基準線。Bastille 可於 www.bastille-linux.org 取得。

trojan.pl 可用於追蹤潛在的安全漏洞。它檢查可執行檔的搜尋路徑，找出在別人的帳號的搜尋路徑上擁有執行權的帳號，這是可以植入特洛伊木馬程式的安全漏洞。trojan.pl 可免費取得，網址是 ftp://ftp.uu.net/usenet/comp.sources.misc/volume43/trojan.pl 。

網路檔案系統 NFS 本身所提供的稽核資訊比較少，比較難稽核，普渡大學提供的 nfstrace 可以幫忙稽核 NFS。nfstrace 利用在網卡上的監聽程式 sniffer 蒐集所有與 NFS 有關的封包，藉由重組 NFS 交易 (transactions)可以達到稽核的目的。nfstrace 可免費取得，網址是 ftp://ftp.cerias.purdue.edu/pub/tools/unix/nfstrace 。

nfswatch 也是普渡大學提供的工具，它提供類似 nfstrace 的分析

資訊，但比較沒那麼詳細，其重點不在稽核而在監視 NFS 的產出(throughput)及反應時間(response times)。nfswatch 可免費取得，網址是 ftp://ftp.cerias.purdue.edu/pub/tools/unix/netutils/nfswatch 。

raudit 監視各使用者帳號的.rhost 檔，追蹤其異動情形，分析並舉報潛在的安全漏洞。raudit 可免費取得，網址是 ftp://ftp.cerias.purdue.edu/pub/tools/unix/sysutils.raudit 。

chkwtmp 及 chklastlog 檢查 wtmp 檔，並舉報異常記錄。這兩個工具可於下述網址取得，http://www.cert.dfn.de/infoserv/dsb/dsb-9404.html 。

UNIX 稽核工具可分為四大類：

- 檔案完整性評估工具： Tripwire, AIDE, rpm
- 稽核劇本(scripts)： COPS, Tiger
- 加強劇本(hardening scripts)： Bastille, Titan, YASSP
- 服務及通訊埠掃描者： Nmap, SAINT, Nessus, VLAD

以上稽核工具可以用來蒐集基準線資料，也可用於人工稽核。可以將各指令寫入劇本，利用 cron 定期執行。

4.7.4 偵測問題

關於鑑識(forensics)的四個步驟：

1. 準備
2. 蒐集並掌握證據
3. 檢查並分析證據
4. 重建事件

4.7.4.1 工具

稽核工作須求助於稽核工具、駭客入侵也有駭客工具，所謂知己知彼百戰百勝，稽核人員必須兩種都熟悉。

駭客使用的工具為 RootKits 駭客工具包，將各式各樣的駭客工具收集在一塊。

執行稽核工作所須工具可分 3 大類：

- 研究工具：一般指令，如 lsof, find, strings 。
- 收集工具：備份指令，如 tar, dd 。
- 分析工具：檔案完整性評估工具，如 Tripwire, RPM。

駭客將各式各樣的駭客工具收集在一塊，做成 RootKits ，身為稽核人員，最好也將各種稽核工具集合起來，弄個意外事件管理工具箱(Incident Handling Toolbox)，必要時才能方便而熟悉的執行稽核工作。

處理駭客入侵事件或意外事件的程序：

1. 法律研究的四個步驟
2. 犯罪現場快照(snapshot)
3. 收集的順序
4. 多種備份方式
5. 以時間為基準重建事件

稽核工作主要的挑戰在於：

- 迅速的行動
- 收集並管理合法的證據
- 採證但不要破壞現場
- 當軟體不值得信賴時研究可能的危害

4.7.4.1.1 RootKit 剖析

Lrk5 (Linux RootKit version 5) 是常見的駭客工具包。lrk5 可以

- 隱藏檔案、目錄、及網路連線；
- 掃除記錄；
- 存取後門；
- 監聽網路。
- 篡改重要的系統檔。

最糟糕的是 lrk5 可以篡改 tcpd，隱藏連線，避免被拒。如果連 tcpd 都不能信賴，那還有啥可以信賴？

4.7.4.2 步驟一　準備

要使稽核工作勝任愉快，稽核人員必須：

- 具備廣泛而良好的背景知識及訓練
- 擁有並使用適當的稽核工具
- 假設最壞狀況並據以管理系統

4.7.4.2.1 訓練

至少須具備下述訓練：

- UNIX 系統管理
- 網路
- 入侵偵測技巧
- 進階意外事件管理
- 實作、實作、再實作

4.7.4.2.2 工具

以下幾點要注意：

- 確認使用正確的工具
- 被駭系統的軟體已不值得信賴

- 使用靜態連結建立「意外事件管理工具包」
- 光碟是工具包的理想的儲存媒體

工具包至少應包含以下程式：

- shared libraries
- static system libraries
- netstat, lsof, top
- gdb, nm
- ps, ls, diff,su
- tar, dd, compress, gzip
- chown, chgrp, chmod
- passwd
- netcat
- strace/ltrace
- MD5
- fdisk/cfdisk
- who, w, finger
- dig
- find, df, du
- rm, mv, cp
- script
- gcc, ldd
- sh, csh

4.7.4.2.3 靜態連結

動態連結省空間因共用資源但易受入侵。所以必須使用 gcc -static 選項(靜態連結)重新編譯各程式。

如果因為 沒有程式原始碼、時間來不及、商業版 UNIX 未附編譯器...等原因，有部份模組或元件無法使用靜態連結，則重新編譯時把 LD_LIBRARY_PATH 環境變數指到光碟上的程式庫。(例如：setenv LD_LIBRARY_PATH=/mnt/CDROM/tools/lib)

使用 csh 進行。

4.7.4.2.4 其他

由 TCP-Wrappers 的輸出報表可以看出一系列的異常 telnet，在遠端主機的 syslog 上有記錄，但近端主機卻沒有記錄。(因為被入侵的駭客清除了)

入侵偵測系統 IDS (Intrusion Detection System) 會記錄 telnet, ftp

等連線的企圖。

使用多種工具，交叉比對其輸出，有助於早日發現問題。

4.7.4.3 步驟二　收集並管理

4.7.4.3.1 建立快照

務必記錄犯罪現場，但因為蒐集證據一定多多少少會破壞系統記錄，所以必須優先記錄容易消失的證據。

各種證據依其容易消失的程度排序如下：

記憶體 > 網路連線 > 程序 > 檔案系統 > 磁區

4.7.4.3.2 使用工具包的方法

將工具包的光碟 mount 到檔案系統，使用「乾淨」的 shell 工作，並設定搜尋路徑及程式庫連結路徑，以確保使用到正確的執行檔及程式庫。

4.7.4.3.3 script 指令

盡可能詳細記錄所有輸出輸入是非常重要的，可以幫助記憶並增加證據的可信度。執行 script 指令可以幫忙記錄所有顯示在螢幕上的任何輸入或輸出。

4.7.4.3.4 收集執行程序(process)的證據

要收集執行程序的證據，首先必須知道什麼程序正在執行，常見的有 ps 指令、lsof 指令、/proc 虛擬檔案系統 等途徑，茲分述如下：

執行 ps 指令是最簡單的方法，但不可百分之百信賴 ps，因為駭客可以操弄 ps 的輸出。執行 ps -auxww 或 ps -elf ，仔細看其結果，

推敲有無可疑之處。（此部份須仰賴稽核人員「功力」，即廣泛的背景知識、良好的訓練、以及實戰經驗。）

以某程序之編號(process ID)為參數執行 lsof 指令，可以顯示該程序開啟的檔案，及其他與該程序相關的詳細資料。

虛擬檔案系統 /proc 是抓取系統核心資料的一個介面。/proc 其實是個程序表(process table)，各個程序的程序編號是虛擬目錄，各種資訊則以虛擬檔案的型式呈現，因此，使用 cd, ls, more... 等基本 UNIX 指令就可以很容易地深入檢視各個程序的資訊。

4.7.4.3.5 收集網路證據

欲檢視近端的網路狀態，可以透過 netstat、IDS、防火牆的記錄、lsof 等途徑。

netstat 指令列出動作中(active)的連線，及其相關網路埠、程式等資料。lsof -i 指令顯示類似 netstat 的結果。但使用這些工具時必須知道，netstat, lsof, 及 nmap 等指令並不會百分之百顯示所有的網路服務。

欲檢視系統有哪些網路服務，可以檢查 inetd.conf 及 xinetd.d 檔案，但不可百分之百信賴。

欲尋找 sniffer 竊聽程式，可以執行 ifconfig 指令檢查網卡狀態，如果是在 promiscuous 模式，則表示有個 sniffer 竊聽程式正在執行。（基本上 ifconfig 指令是用來設定網路介面組態的，但未加任何參數時可以顯示介面狀態。）

4.7.4.3.6 收集檔案系統證據

執行 tar, dd 等指令，將檔案系統備份。

4.7.4.3.7 其他

執行 ls 指令時加上-lart 參數，可以讓輸出結果依時間排序，日期近者在前，有助於找出最近異動過的檔案。但是，不可百分之百信賴其顯示結果，因為駭客可以利用 touch 這個基本 UNIX 指令輕易篡改檔案的日期。

證據蒐集不易，必須小心處理：

- 儘量保留詳細的記錄
- 考慮對證據加密保存
- 封裝並註明日期
- 鎖起來
- 只分析複本

4.7.4.3.8 收集遠端記錄

駭客必須入侵系統才能做手腳。，而駭客必須同時入侵遠端系統，才能也對遠端系統做手腳，所以遠端系統上的記錄較難隱藏。

欲收集遠端記錄，可以利用 入侵偵測系統 (IDSs)、防火牆、路由器、以及遠端 syslog 伺服機...等途徑。

研究遠端系統的網路存取記錄，有助於迅速尋找是否還有電腦主機受到侵犯。考慮以下兩個問題：

1. 攻擊來源是否也存取其他系統？
2. 被駭電腦是否也存取其他系統？

4.7.4.4 步驟三　檢查及分析證據

事前準備越充分，事後追查越容易。以檢查證據的難易度而言，

「檢查檔案完整性資料庫」是最容易的；「檢查檔案系統」是最難的。

駭客入侵的證據何在？可考慮從以下三個方向尋找線索：

- 檢查 程序
- 檢查 記錄檔

  wtmp, utmp, btmp, messages, secure
- 檢查 檔案系統

  尤其須特別注意以下幾點：

  1. SUID 及 SGID 檔案
  2. 最近被修改過的執行檔
  3. 隱藏檔
  4. passwd 檔內異常的帳號
  5. 其他任何異於常軌的現象

執行 find 指令可以依設定條件搜尋整個目錄樹，非常有幫助。例如：find / \(-perm -004000 -o -perm -002000 \) -type f 可以找出所有 SUID 及 SGID 的檔案。

例如：touch -m 04220000 /tmp/tstamp

find / -newer /tmp/tstamp -type f 可以找出所有比 2000/04/22 還晚的檔案。

lsof +L1 可以找出失聯(unlink)的檔案，進而找出隱藏的磁區

4.7.4.5 步驟四 重建事件

詳細分析手邊所有的證據，以時間為基準，抽絲剝繭，重新組織駭客入侵的一連串事件，建構出完整的入侵過程。

可以檢查 shell 的指令歷史檔，運氣好的話，有時候可以找到一些線索。

5. 建議與心得

5.1 SANS 研究院舉辦之資安教育訓練、證照考試及服務值得借鏡

本次參加的課程資訊極為豐富，共領了七本講義，包含一本實做手冊(Lab Manual)，於六天之內上完，每本講義都厚達 200 多頁，實做手冊的網路環境事先由主辦單位 SANS 研究院(http://www.sans.org)之人員安排設定妥當，學員只需要自備筆記型電腦即可，實做課程補足上課理論之不足。主辦單位 SANS 研究院甚至事先發折頁提醒上課學員課程之內容極為豐富，將使學員強烈感受資訊超載(information overloading)，建議學員每天晚上回旅館或是住處時，不要看電視，能事先預習一下明天上課的講義內容。開課前一天傍晚也提供事先領取講義之服務。而所上課的內容在結束後另外提供帳號密碼，於六個月內隨時可以存取其中的上課內容影音檔案、講義 pdf 檔案，而這些研讀資料也提供 GIAC 認證考試(Global Information Assurance Certification Program)，準備時間也是六個月，除選擇題外，另需繳交一篇論文，交由相關領域的專家審查，亦即這些緊湊、豐富的資訊足足需要學員花六個月時間充分學習及消化。

GIAC 認證考試(http://www.giac.org)，以實用為導向，不僅測驗考生之知識，也考量實做。同時這也是一種對品牌保持中立的專業認證，於 1999 年開始，SAN 執行此項計畫，除了提供入門之 Security Essentials 課程外，也有進階的課程例如稽核、入侵偵測、緊急應變、防火牆及週界管理、駭客技巧、Windows 及 Unix 作業系統安全。換言之，考生要先參加線上或教室面授的課程，再參加線上考試(多數

為 75 題單選兩小時考完)前，然後花費五個月時間完成實做習題(Practical Assignment)發表論文(practical/research paper)於網站上讓大家公評，並且獲知通過之分數。如果線上考試或是實做論文沒有通過，必須花 USD 100 重新考過。GIAC 提供多種不同領域不同程度的驗證科目如下:

GIAC Security Essentials Certification (GSEC)
GIAC Certified Firewall Analyst (GCFW)
GIAC Certified Intrusion Analyst (GCIA)
GIAC Certified Incident Handler (GCIH)
GIAC Certified Windows Security Administrator (GCWN)
GIAC Certified UNIX Security Administrator (GCUX)
GIAC Information Security Officer (GISO)
GIAC Systems and Network Auditor (GSNA)
GIAC Certified Forensic Analyst (GCFA)
GIAC Security Leadership Certificate (GSLC)
GIAC IT Security and Audit Kickstart (GIAK)
GIAC Gold Standard Certificate (GGSC-0100)

有鑑於各領域的技術變化很快，這些證照的有效期限為 2 至 4 年，因此是一種顧及深度與時代演進的證照考試。在 2002 年有超過 16500 位安全、網路和系統管理專家參加由美國頂尖的安全專家所舉辦的多天深度訓練，其中有超過 4200 名學生取得 GIAC 證照，國內目前取得此項證照的人數尚在個位數，詳見 http://www.giac.org。

老師提供的實做手冊與區域網路環境，提供學員親手稽核老師提供的目標系統或自己自備的筆記型電腦。不過主辦單位也提醒實做課程應該不會損壞系統，但最好事先將系統備份，最好也裝置個人防火牆與防毒軟體，同時也警告學員若有駭客行為將被趕出此次課程。

由於本課程在深度、難度與廣度方面都份量足夠，因此順利完成此項課程者如果也是經過國際資訊系統安全授證協會(ISC)2(http://www.isc2.org) 於全球各地舉辦資訊系統安全專家認證考試(Certified Information System Security Professional，簡稱 CISSP)通過的學員，將可獲得 36 點的持續專業教育訓練點數(CPE)。依據 CISSP 考試規定，參加 6 小時、250 題 CISSP 考試的學員，每隔三年仍應該持續接受 120 點的專業訓練，並繳交證照維持費，否則證書在三年後就失效，必須重新參加考試。職陳員於 2002 年 9 月獲得中華電信首張 CISSP 證照，對於本分公司投標政府專案，因應建議書徵求文件有開立規格或是本團隊之加分深有幫助，藉由此次難得之研習機會，也獲得 36 點的持續專業教育訓練點數，深感慶幸有此機會奉派受訓並延續專業證照效力。

課程裡面不時聽到主要以美國籍為主的學員，發出問題或是對於老師的教材提出意見，老師對於認同的觀點也會加以讚賞。而主辦單位「系統管理、網路和網路安全研究院」(SANS 研究院)成立於 1989 年，知名度相當高，目前已經轉型為電腦安全教育與資訊安全訓練的服務單位，組織成員的核心份子包括政府機關、公司行號、大學及法人內有關網路安全從業人員、系統或網路管理者。在 2002 年，超過 16,500 位安全、網路及系統管理人員參加由美國頂尖的師資所舉辦之多天的深度專業訓練。SANS 與 FBI 合作提出的 Top 20 List of Vulnerability(http://www.sans.org/top20/)，包含 Windows 和 Unix 系統兩部分，針對系統上可能的漏洞作統計與排名，並加以描述漏洞與解決方案，成為相當具有參考價值的資料。SANS 也會每月邀請相關議題的專家在線上演講威脅以及如何阻擋的技術資訊，網站也有相關的資安每週重要訊息摘要(Newsbites)、GIAC 研究論文線上資料庫。教育訓練之出版物有許多都是深入之 step-by-step 指引。許多 SANS 之資源例如新聞摘要(http://www.sans.org/newsletters/newsbites/)、研究摘要(http://www.sans.org/rr/)、安全警報

(http://www.sans.org/newsletters/sac/)以及得獎論文、、、等免費提供社會大眾。SANS 研究院所舉辦之資訊安全感知(Security Awareness Training)或是深度教育(in depth education)及資訊服務可供本分公司 PKI 團隊、電信訓練所或是本分公司資通安全技術中心借鏡參考。

美國白宮於 2000 年正式執行「資訊系統保護國家計畫」，為因應資訊系統日益複雜的數位社會資訊安全議題，植基於防護 Protect、偵測 Detect、反應 React、回復 Recovery 四個動態環節，美國國防部提出「深度防禦」的概念與相關技巧，以

- 保護網路與基礎建設
- 保護區域資訊使用環境的邊界
- 保護資訊使用環境
- 支撐性基礎建設
  1. 公開金鑰基礎建設與金鑰管理基礎建設(Key Management Infrastructure)
  2. 偵測與反應

四個重點技術領域，整合技術、管理與治理等多方面內涵，實現資訊安全之多層防護，降低遭受攻擊之風險。本次實習對於本分公司 PKI 維運以及如何稽核與運用上述四個深度防禦重點技術有很大的幫助。