出國報告（出國類別：其他）

赴美國參加「網路安全(戰)教育訓練」

服務機關：國防部參謀本部資電作戰指揮部
姓名職稱：劉定儞（中校副組長）
周世淵（上尉資參官）
派赴國家：美國
出國期間：99 年 3 月 6 日至 16 日
報告日期：99 年 4 月 15 日

摘要

爲瞭解國際網路安全(戰)訓練課程發展現況，藉以作爲規劃本部(資電作戰指揮部)部隊訓練之參據，特派專業人員赴美國參加於佛羅里達州奧蘭多市舉辦之 SANS 2010 大會，全程除參加「網路鑑識」與「駭客技術、行爲及事件處理」兩門課程外，並藉由參與課間研討會與產品發表，瞭解 SANS Institute 在網路安全(戰)訓練的全貌。派訓人員於完訓後，根據參訓過程提出八項心得與五項建議。心得包括：「訓練機構規劃之課程具整體架構」、「課程內容結合理論與實務」、「課前預習方能掌握授課內容」、「綜合演練提升學習成效」、「完善的教學與行政支援編組」、「與法律面有關的實務尚待加強」、「實務研討及廠商展覽有助於理論與實務結合」及「參訓經驗有助於規劃本部部隊訓練」；建議包括：「訓練必須以單位任務爲核心」、「訓練必須有全盤構想與規劃」、「自訓與委外訓練兩者兼施」、「加強與民間機構交流」及「建立組織間交流機制」，未來期能透過整體性且妥善設計的訓練規劃，提升本部在網路安全(戰)的戰力，有效防衛我「數位疆土」。

目次

一、目的

資訊與網路科技發展快速，現今我們已進入數位化社會，對資訊與網路科技的仰賴日益加深；由於網路無遠弗屆，加速資訊傳播的速度與其影響的範圍，人類的文明也藉著數位化而提升。當然，凡事均有光明面與黑暗面，在黑暗面方面，近年來資安事件與電腦犯罪案件不斷增加，駭客入侵造成個人資料外洩、企業重大財務損失及國家重要資訊系統遭破壞等類似事件層出不窮，這讓我們警覺到「數位疆土」的固守將日趨重要。

本部(資電作戰指揮部)擔負國軍網路的固守任務，面對駭客與敵人網軍日益精進的技術，要有效反制則必須瞭解此領域的專精技術。爲提升本部資訊(網路)安全作業人員素質，除積極透過自訓、委外訓練及鼓勵進修學位外，本(99)年度特別派員赴國外著名資訊安全訓練組織 SANS Institute，參加該組織舉辦的 SANS 2010 年會，藉由參與其訓練課程學習先進的資安技術，同時也藉由參觀會場中廠商展覽之機會，蒐集資安設備相關資訊。

此行主要目的是參與兩門資訊安全專業訓練課程，期能掌握網路安全(戰)技術發展趨勢，以作爲本部培育網路安全(戰)人員訓練方向與內容之參據。在參訓課程選擇方面，由於 SANS 2010 提供 5 大類、超過 30 門的訓練課程，爲符合「爲用而訓」的原則，在結合本部核心任務之前提下，選擇參加「Network Forensics (網路鑑識)」及「Hacker Techniques, Exploits, and Incident Handling (駭客技術、行爲及事件處理)」兩門課程，並選派具專業背景與英文能力之人員前往，俾能吸收國外之專業訓練經驗，作爲本部未來培養執行網路防護及資訊確保專業人才之參考。

二、過程

本次參加 SANS 2010 訊練課程之期程自 99 年 3 月 6 日起至 3 月 16 日止，共計 11 日，會議地點爲美國佛羅里達州奧蘭多市。行程概述如後：

(一)99 年 3 月 6 日：搭乘長榮航空班機赴美國洛杉磯，並於當日轉搭達美航空(Delta Airlines)美國國內班機，於 3 月 7 日清晨抵達佛羅里達州奧蘭多市。

(二)99 年 3 月 8 日：上午 08:00 至會場完成報到手續(如圖一、二)。

(二)99 年 3 月 8 日至 3 月 12 日(每日 09:00 至 17:00 時)：由劉定衢中校參加「Network Forensics (網路鑑識)」課程。

(三)99 年 3 月 8 日至 3 月 13 日(每日 09:00 至 17:00 時)：由周世淵上尉參加「Hacker Techniques, Exploits, and Incident Handling (駭客技術、行爲及事件處理)」課程。

(四)99 年 3 月 8 日至 3 月 13 日：參加人員利用午間或課後時段，參與大會或贊助廠商舉辦之展覽、產品發表或研討會(如圖三)。

(五)99 年 3 月 14 日出發返國，自奧蘭多市搭乘達美航空(Delta Airlines)美國國內班機抵洛杉磯，再轉搭長榮航空班機返回台灣，並於 3 月 16 日清晨返抵桃園國際機場。

圖一 SANS 2010 大會會場資訊

圖二 SANS 2010 大會報到櫃台

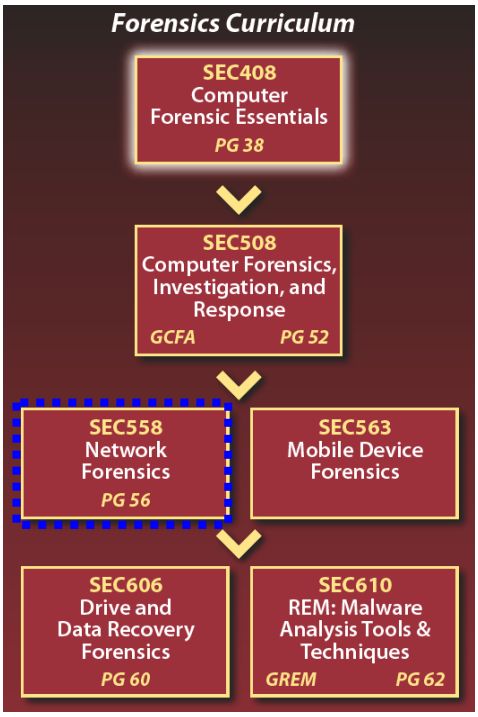

圖三 SANS 2010 大會辦理之廠商展覽

以下分別說明兩門課程的授課過程與課程重點：

(一)網路鑑識(Network Forensics)

網路鑑識(Network Forensics)課程上課日期自 3 月 8 日至 12 日(共計 5 天)，講師爲 Jonathan Ham，現職爲 Lake Missoula Group 之資深安全顧問。在 SANS 2010 的課程架構中，本課程屬鑑識課程中的進階課程(如圖四)，參加人員必須有電腦鑑識的基礎知識；上課期間講師針對 DNS 分析、DHCP 紀錄檔及使用鑑識

工具運用於各類數位證據之蒐集、分析與保存等內容，訓練學員如何建立網路鑑識環境與具備初級鑑識能力，並強化網路鑑識人員執行鑑識作業時資料之完整性與正確性。



圖四 SANS 2010 鑑識課程架構圖

網路鑑識五天課程內容涵蓋了網路鑑識(Network Forensics)、調查(Investigation)、回應(Response)、事件獲得與分析(Evidence Acquisition & Analysis)以及案例演練(Real World Exercises)等課題，各日的授課內容要點分述如下：

1.第一天：主題爲「被動的證據獲得與分析(Passive Evidence Acquisition and Analysis)」，針對「網路分析」、「事件獲得」以及「封包分析(第一部份)」做深入介紹。

課程從 DHCP 及 Proxy 的紀錄分析開始，因爲網路上的惡意使用者通常必須透過 DHCP 伺服器取得網址(IP Address)，而許多入侵事件係透過 Proxy 爲媒介。課程中，講師深入介紹如何從網路設備中側錄封包資料(包含：Wire, Hub, Switch, Tap, Wireless Access Point)、如何使用 tcpdump 捕捉網路封包、如何使用 ngrep 與 tcpxtract 進行封包分析。

2.第二天：主題爲「主動的證據獲得與傳輸通道(Active Evidence Acquisition and Covert Tunnels)」，針對「封包分析(第二部份)」、「鑑識方法(Forensic Methodology)」及「網路安全通道(Network Tunneling)建立」等內容作深入介紹。

在封包分析方面，使用 Wireshark 爲工具進行封包的深入分析，Wireshark 的功能涵蓋封包捕捉、資料搜尋與分析，其較 tcpdump、Snort、ngrep 及 tcpxtract 等工具更爲健全；另外也介紹命令列模式(Command-line)的 tshark、pcapcat、oftcat 等工具之使用方式。

在鑑識方法(流程)方面，課程中提出並介紹了「獲得資訊」、「擬定策略」、「蒐集證據」、「分析」與「報告」等五個步驟。

在網路安全通道方面，實作使用 Secure Shell(SHH)建立資料加密的安全通道。至於如何檢視是否有利用合法網路流量隱藏非法資訊部份，授課講師以 ICMP 及 DNS 兩個協定爲例進行說明。

3.第三天：主題爲「防火牆、入侵偵測系統、代理伺服器及資料重建(Firewalls, IDS, Proxies, and Data Reconstruction)」，針對防火牆與路由器的證據蒐集、集中式紀錄伺服器(Central Logging Server)的紀錄分析等內容進行深入介紹。

在工具方面，Splunk 是以 Web 爲介面的紀錄分析與統計軟體，可對大量的紀錄進行統計並以圖形方式呈現分析結果，此方式協助鑑識人員快速瞭解大量紀錄中所隱藏的訊息或趨勢。

在網路型入侵偵測系統(NIDS)方面，則介紹了 Snort 的相關功能；網頁代理伺服器方面，介紹如何從 Squid (一種代理伺服系統)的暫存檔中萃取鑑識所需的網頁，以及如何進行紀錄分析。

4.第四天：主題爲「在無線網路中進行鑑識(Network Forensics Unplugged)」，針對無線網路鑑識的相關課題，包括在無線存取點(Wireless Access Points)的證據蒐集與流量分析進行深入介紹。

本日課程結束前也對於網路證據的議題，包括獲得、內容、儲存、隱私、捕捉與容許性等議題作說明；其他對於與證據獲得相關的法律，如：The Wiretap Act、The Electronic Communications Privacy Act (ECPA)，也有概略介紹。

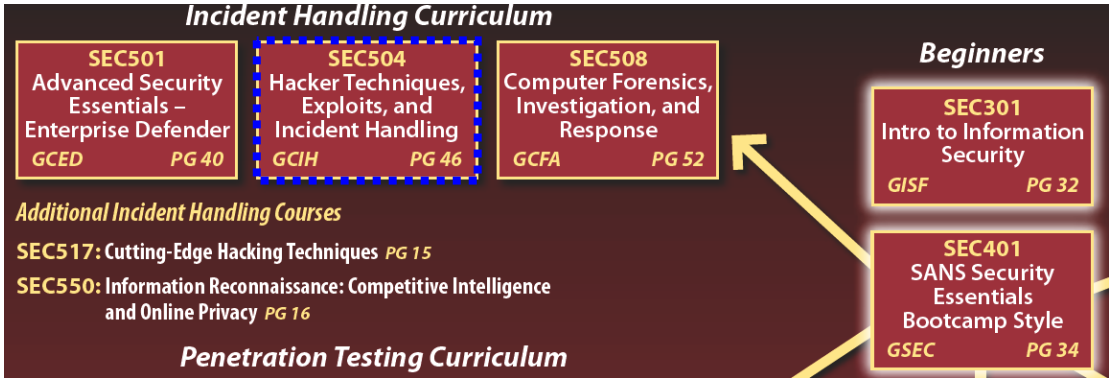
5.第五天：主題爲「網路鑑識案例探討(Capstone Investigation)」，針對課程中講師所設計的案例，分組以團隊合作的方式，利用前四天所講授的內容與各式工具，進行綜合演練(組合訓練)。

演練過程必須由分組的成員組成「鑑識團隊」，進行任務分工，鑑識步驟包括「驗證與獲得(Verification and Acquisition)」、「時間與關聯(Timelines and Correlation)」、「證據復原(Evidence Recovery)」、「證據與網路檔案重建(Evidence Reconstruction and Network File Carving)」與「呈現證據(Presenting Evidence)」等五個步驟。透過全程的演練，使學習者能充分瞭解鑑識過程，以及靈活運用課堂中所學的鑑識工具，尤其是呈現證據部份，因爲鑑識的結果要作爲法庭上定罪的依據，故其蒐證過程必須爲法官所採

信，內容呈現必須爲法官所認同與理解。

(二)駭客技術、行爲及事件處理(Hacker Techniques, Exploits, and Incident Handling)

駭客技術、行爲及事件處理(Hacker Techniques, Exploits, and Incident Handling)課程上課日期自 3 月 8 日至 13 日(共計 6 天)，講師爲 Bryce Galbraith，在 SANS 2010 的課程架構中，本課程屬事件處理課程中的進階課程(如圖五)，參加人員必須具備資訊安全的基礎知識；課程之進行均透過講師解說並搭配實務操作，研討現今駭客慣用技術、資安事件處置程序與復原機制等內容，期藉課程內容讓資訊維管與資安防護人員可先知悉駭客之網路偵蒐作爲與攻擊手法，進而針對其攻擊模式預先發展相對應之網路防護方法，俾確保單位內之資訊安全。



圖五 SANS 2010 事件處理課程架構圖

講師 Bryce Galbraith 於六天的課程中，著重於介紹現今網路駭客普遍行爲與攻擊手法，並分析網路攻擊事件逐漸上升之原因，主要爲駭客工具太容易於網路上獲得且操作容易，甚至有網站公開提供任人下載與教學使用；另外，由於現今網路科技的便利性，大多數人會運用電子郵件、網路銀行、股市交易等等網路服務，這更促使有心的駭客使用各式駭客工具以從中獲得利益，如鍵盤側錄器、後門及木馬等等。講師除說明現今普遍網路攻擊事件與趨勢，並解說資安事件基本處置程序及網路駭客行爲的 5 個主要步驟，藉以解析駭客行爲模式，講師授課重點如下：

1.資安事件基本處置程序：

講師在課程一開始，先針對單位的資安事件處置程序提出說明，處置重點爲預防準備(Preparation)、偵測識別(Identification)、封鎖圍堵(Containment)、移除(Eradication)及回復(Recovery)等五個階段，提供給資訊系統維管人員參考，單位內若發生資安事件，必須迅速處置，俾將風險降至最低，所以要透過政策的制定、標準化的處置程序及相關回報機制，才

能有效控制災損。

2.駭客攻擊行爲步驟一：偵察(Reconnaissance)

入侵者一般會利用第三方系統蒐集攻擊目標的基本資訊，例如：whois(如APNIC)、DNS 解析、Google 搜尋及部落格等網路上公開可獲得的資訊，並運用偵獲之資訊，分析出可攻擊之目標，上述的 whois 可獲得單位使用的 IP 網段、電話及電子郵件等，DNS 解析即是透過 DNS Zone Transfer 或者運用 nslookup 指令，可以列出或解析出目標相關的 IP 位址與單位的相關註冊網域名稱之系統(包含 Windows 及 UNIX 作業系統版本資訊)。

另外一項就是 Google，它具備強大的搜尋功能，是駭客最喜歡運用的搜尋引擎之一，某些網站會將網站架設的作業系統版本或是相關架構細節(如 FW、IPS 等等)透露於公開網頁，這使得駭客可透過搜尋工具，獲得相關資料，這些資料將可提供駭客進行相關弱點分析或刺探攻擊；此外，類似攻擊行爲也被運用於公開資料庫、部落格及社交網站(可針對單位的關鍵人物執行此類攻擊行爲)，因爲它可具有進階設定相關搜尋條件的功能(可針對目標個人資訊、街景地圖、特定搜尋條件設定、網站快取及系統弱點等等執行所需資料搜尋)，可濾除不必要之資訊，且可針對單一單位實施深度的搜尋。

所以，單位內的資訊系統維管人員必須注意，內部人員是否有在網路部落格中洩露單位之機密，或者是單位在網路上公開之資訊，是否合宜或有影響單位資訊安全之情事，如果不適宜公佈於公開網站上，可向 Google 公司反應，以維護單位機敏資訊安全。

3.駭客攻擊行爲步驟二：掃描(Scanning)

介紹駭客常用之掃描工具軟體(如 PortScan、Nessus 及 Nikto 等)，可針對目標主機之系統弱點、各埠號、作業系統、主機存活狀況及目標主機路徑上所經過之網路設備等實施掃描作業，獲得所需資訊。其主要運作原理爲對目標系統送出特定封包，藉由回應分析後獲取有用資訊，此步驟爲駭客入侵之重要前置作業，通常此階段所獲得的資訊將決定目標單位是否可被成功入侵。所以了解駭客在掃描作業階段所會運用之手段後，相對應的防護就是要關閉非必要的服務、設置防火牆或入侵預防系統(IPS)，透過防禦政策參數的設定，進而隔離內外部網路，濾除不必要的 ICMP 封包，而 DMZ 區域的伺服器更要落實漏洞修補與提升密碼設定強度，才可預防有心人士的掃描與刺探，降低資安威脅的風險。

4.駭客攻擊行爲步驟三：入侵破壞(Exploit Systems)

當完成上述兩個步驟後，入侵者已經獲得足夠的相關攻擊資訊，可進入第三個步驟，此步驟主要作法及目的爲「獲得存取權限」、「網頁應用程式攻擊」及「阻斷式服務攻擊」等三項。此步驟是利用所偵獲的目標系統各項弱點，

進而執行資料竊取、網頁置換、更改內容或實施阻斷服務攻擊等，直接使目標主機失去服務之功能，現今網路上均可找到許多現成的攻擊程式(如Metasploit、Cain 等軟體)，均能達成上述的功能。

(1)獲得存取權限：

主要是利用作業系統或套裝軟體設計之瑕疵，進而發展的攻擊行爲。應用此類型的攻擊有緩衝區溢位 (Buffer Overflow)、格式化字串攻擊(Format String Attacks)，緩衝區溢位是利用過長的字串重寫返回位址，而格式化字串攻擊則是利用程式中不正確的使用格式化字串，這將造成可以去讀取任意記憶體內容或重寫記憶體中的位址；另外還有連線奪取攻擊(Session Hijacking Attacks)，主要爲入侵者在使用者登入主機並完成身份確認後，即進行連線奪取，讓合法使用者跟主機間的連線中斷，入侵者的電腦取代合法使用者與遠端主機進行連結，入侵者可存取使用原合法使用者所有有權限存取的任何資源。

(2)網頁應用程式攻擊：

主要利用網頁程式漏洞，進而衍生的攻擊行爲，如：資料庫隱碼攻擊(SQL Injection)及跨網站攻擊(Cross Site Scripting) 爲主要的兩種攻擊模式。資料庫隱碼攻擊原理爲利用網站建置時撰寫的應用程式，未對使用者的輸入字串做妥善之過濾與處理，而將輸入的攻擊字串，直接傳送給後端的 SQL Server 執行，便可能獲得資料庫存取權限，讓入侵者有機會竄改資料庫系統參數，而造成損失或機敏資訊外洩；另有關跨網站攻擊爲當網站應用程式(如 PHP 程式)在還沒過濾使用者提供的資訊，將可能顯示在網頁中，這些內容有可能是嘗試要取得私人資訊的惡意程式碼，藉此入侵系統。

(3)阻斷式服務攻擊：

攻擊者利用各種方法，使提供服務的伺服器無法正常提供服務，攻擊者可能會透過一些路由表溢位或是針對伺服器的 CPU 及記憶體，耗盡其資源等攻擊方式來達成阻斷服務之目的。通常攻擊者透過發送大量僞造封包訊息來消耗網路頻寬，並阻礙合法節點建立連線，進而造成網路及伺服主機無法提供正常的服務。

因此，除了個人端用戶電腦要落實漏洞修補與定期掃描，避免成爲 DOS 或 DDOS 攻擊的利用平台之一，針對網路部份，需正確規劃網路架構，將內外網路分隔，並有效設定路由器存取控制列表(Access Control List, ACL)，濾除由外部介面進入含有內部網址之封包等相關資安參數設定，且可加裝網路型入侵偵測系統(NIDS)或網路型入侵預防系統(NIPS)，以提高此類型攻擊的偵獲率與防護強度。

5.駭客攻擊行爲步驟四：維持存取(Keeping Access)

當入侵者已成功的入侵目標主機或系統後，通常都會長期潛伏，俾從中獲得所需資訊或者使其成爲肉雞主機(類似傀儡主機，可被遠端操控並執行 DOS 之程式)，所以維持步驟四是很重要的。

通常入侵者會建立後門或安裝遠端管理程式(如 VNC、NetBus 及 Tini 等軟體)，以利再次進入系統，並可進一步安裝 rootkit、sniffer 等程式，讓使用者無法察覺入侵者的存在，且隱藏入侵者所開啓的埠、執行的惡意程式與暗藏的檔案及竊聽帳號密碼或其他有用資訊，以擴大攻擊面，就算已無利用價值，亦可轉運用爲跳板主機。

針對此類攻擊行爲，可以運用一些基本且免費的偵測軟體來檢驗自身主機是否已被入侵，像是 Netstat、Tcpview、Active Ports 及 FPort 等，均可在微軟網站下載，其可對網路連線狀態、程序執行狀態及目前埠號使用情況提供相關資訊，可做爲進一步分析之用；另外可運用防火牆設定記錄連線紀錄與不定期更新網站公佈的網站黑名單，即可定期分析單位內是否有可疑的連線，並可對已知的網站黑名單先期予以阻絕。

6.駭客攻擊行爲步驟五：匿蹤(Covering the Tracks)

本步驟主要說明當入侵者完成入侵行爲之後，如何使管理者無法發現攻擊者的入侵足跡。常見的模式爲刪除或修改紀錄檔或隱藏植入的檔案，像是木馬程式的植入常會僞裝成系統中正常執行的程式，使一般使用者不易察覺，故相關對應的方式有使用遠端檔案伺服器儲存紀錄檔等，或者運用檔案完整性檢查工具，均可協助單位內資訊人員查察新增或被修改的檔案，俾利早期發覺可疑跡象。

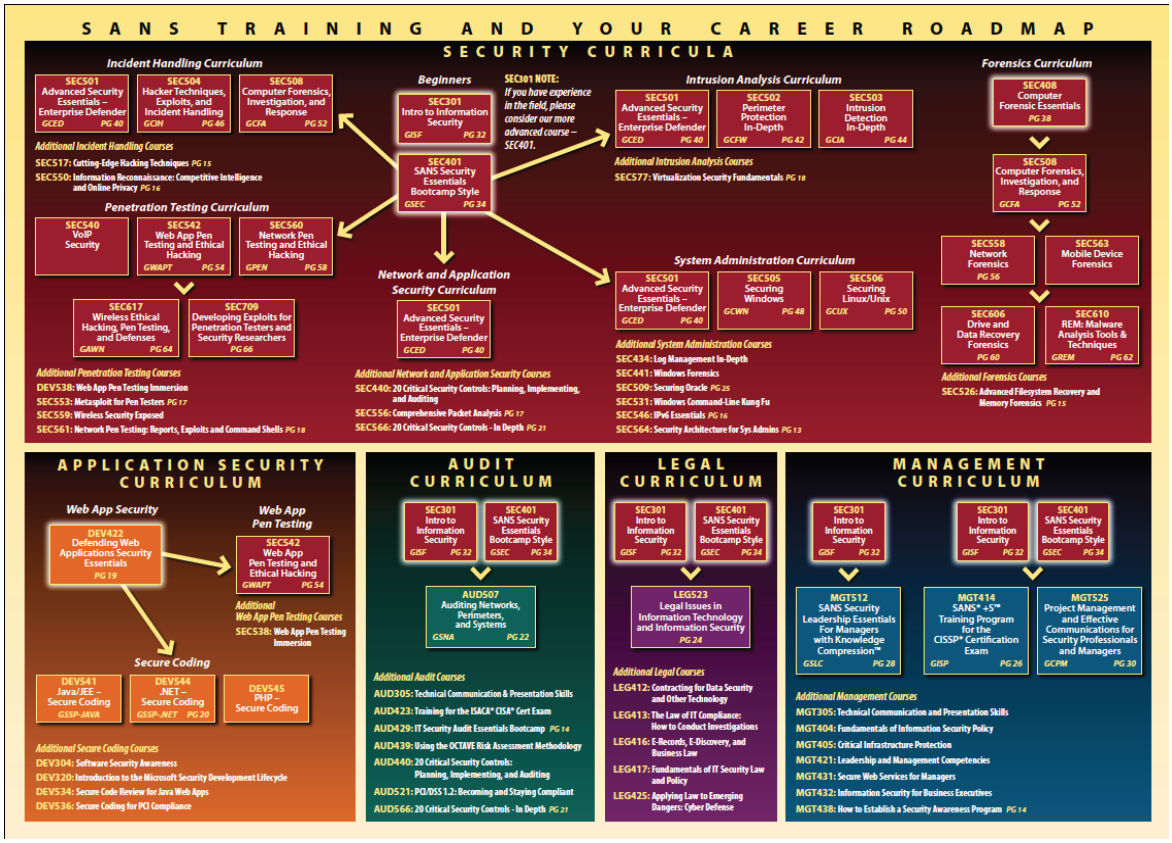
三、心得

本次奉派赴美國參加網路安全(戰)教育訓練，上課時間雖然只有短暫的六天，但是，透過實地體驗美國 SANS Institute 資訊安全專業訓練機構對於課程的整體規劃與進行過程(包括行政支援人員之服務)，可以感受到其與國內資訊專業訓練機構有許多差異之處。

茲將本次與會及受訓的心得列舉如下：

(一)訓練機構規劃之課程具整體架構：

SANS 2010 Orlando 是 SANS Institute 於 2010 年度辦理一系列訓練課程中，規模最大的一個場次，其課程計區分有「安全(Security)」、「應用程式安全(Application Security)」、「稽核(Audit)」、「法律(Legal)」及「管理(Management)」等五大類，每一類的細部課程均依據深淺程度規劃學習路徑(如圖六)。此舉使參訓者易於瞭解並依學習路徑選擇適合個人參加的課程，或在參訓前即先期研讀必須具備的技術能力與知識；對組織而言，亦可據以規劃符合組織所需的訓練課程架構，使成員逐步具備更高的學能。這是國內許多資訊專業訓練機構待加強的部份。



圖六 SANS 2010 訓練課程類別與學習路徑圖

(二)課程內容結合理論與實務：

此次參加的兩門課均以「實作爲主、理論爲輔」爲課程設計原則，故除了介紹課程所需之基本學理外，相當著重於相關工具的實作，尤其是市面上可以找到的工具程式(包括開放原始軟體及市售軟體)，透過不同練習題的反覆練習，使與會參訓人員熟悉工具的操作，以提升學習成效；此外，因爲工具容易取得，故對於參訓人員而言，能於回到工作崗位後，立即以習得之技能遂行任務，達到「爲用而訓」之目標。

(三)課前預習方能掌握授課內容：

由於派訓人員參加的兩門課程在 SANS 2010 所規劃的學習路徑中，均屬於進階課程，且因內容豐富，講師授課速度非常快，故以五至六天的時間授課，事實上進行得非常緊湊；因此，參訓人員必須具備學習路徑中先修課程的基本知識，方能在既有的基礎下習得新知。爲提升學習成效，本部在派訓前已針對參訓人員進行「專業」與「語文」兩項能力評估，並擇優派訓，故初步評估參訓人員之學習成效良好。

(四)綜合演練提升學習成效：

在「網路鑑識」課程的最後一天，教材內容設計了一個情境題，學員依題目設計的動次，可以運用前四天所教授的鑑識觀念、流程、步驟與各式工具，實作一次完整的組合訓練。此外，由於情境題演練係以分組方式爲之，參訓人員被區非爲三人一組，透過分工賦予不同職責，共同完成鑑識工作，這對於從事鑑識工作之人員是很重要的，因爲在面臨實際狀況時，通常必須由一組鑑識人員共同遂行任務，方能爭取時效。

(五)完善的教學與行政支援編組：

本次參加的兩門課程在授課過程中，均編有助教及行政支援人員在課堂上協助授課，助教協助解決課程實作時學員遇到的問題，行政支援人員則是協助處理教室內軟體與硬體方面的問題排除。這樣的編組方式讓講師能專注於課程內容之講授，而不必分心於其他非課程核心的問題，對於學員的整體學習成效將有顯著之提升。

(六)與法律面有關的實務尚待加強：

由於「網路鑑識」的目的是要從數位證據中舉證，以作爲法官在法庭中判決案件的依據，故鑑識人員對法律面的觀念與認知也必須具備，由於課程較著重於技術面，對於法律面的知識著墨較少，如果學習者要了解鑑識的全般概念，必須再自行蒐集與研讀相關的書籍與資料。同樣的，「駭客技術、行爲及事件處理」課程所提及的各式駭客入侵手法，其結果與造成之影響，通常也涉及法律面的問題，因此如能加入一定程度有關法律面的內容，將更能建立參訓人員對此課

題的全般概念。

(七)實務研討及廠商展覽有助於理論與實務結合：

在訓練課程的空檔，如：午間休息及下午課後時間，大會辦理各式專題演講、專業研討會、以及新產品發表或展覽，這些活動均有助於參訓人員進一步瞭解業界發展現況，以及現今資訊安全技術。

(八)參訓經驗有助於規劃本部部隊訓練：

透過兩門課程的學習，可以得知美國具規模的資訊安全課程訓練機構，對於「網路鑑識」與「駭客技術、行爲及事件處理」課程的設計與授課方式；由於本部擔負國軍資訊安全監防任務，有效防範駭客入侵是首要的任務，而攻擊是最佳的防禦，瞭解駭客的攻擊手法則有助於提升反制成效；另單位如發生資安事件，事後依循著蛛絲馬跡還原事實真相是重要的工作，鑑識除能找到犯罪證據外，更能依此精進防範駭客攻擊的方法。因此，兩門課程的學習經驗，對於規劃本部未來的部隊訓練內容，均能提供正向的參據。

四、建議事項

國軍資安監防與網路防護爲本部核心任務之一，鑑於先進國家(如：美國、英國、日本等國)莫不積極發展網路戰戰力，尤其是中國網軍對我之威脅與日俱增，爲有效防衛我「數位疆土」，並期於未來「不對稱作戰」中能取得優勢地位，擁有「高素質人力」爲網路作戰致勝的關鍵性因素。有別於傳統戰爭的槍砲與彈藥，網路作戰爲技術與知識密集的戰爭，作戰人員必須精研資訊安全與電腦網路的知識，瞭解戰場的全般狀況，更要因應戰況適時調整戰術戰法與製作有效的戰具，方能克敵致勝。因此，積極從事「網路安全(戰)人才培育」是從事網路防護與反制敵網路攻擊的重要工作。

本次有機會藉「赴美國參加網路安全(戰)教育訓練」之機會，參加於美國佛羅里達州奧蘭多市舉辦之 SANS 2010 大會及其網路安全(戰)訓練課程，除透過授課過程瞭解「網路鑑識」與「駭客技術、行爲及事件處理」兩門課程的內容與重點外，也透過參加廠商展覽與研討會之時機，提升資安產品新知與網路防護新概念，更瞭解現今主流網路攻擊種類與防護模式。爲提升本部網路防護與反制作戰人才培育成效，茲以本次參訓心得與所見所聞，對網路安全(戰)訓練提出下列建議：

(一)訓練必須以單位任務爲核心：

網路安全(戰)領域涉及的資訊專業知識與技術甚廣，惟在資源有限下，必須結合單位的核心任務，慎選訓練範圍，尤其是在委外訓練方面，單位必須投入相當的人力與預算，故不可不謹慎爲之。以本部而言，應以網路安全領域的技術爲主，法律與管理領域爲輔，以有效提升部隊整體戰力。

(二)訓練必須有全盤構想與規劃：

由於網路安全(戰)的訓練課程繁多，而且不同次領域的課程亦有所差異，故單位必須在釐清所需的訓練範圍後，設計出全盤性的訓練類別與學習路徑。尤其是在學習路徑的設計上，必須有梯度、有層次，由簡而難，逐次深入，使人員能按部就班，逐步由生手、半熟手到熟手，以具備遂行不同層次(難度)任務之能力。

(三)自訓與委外訓練兩者兼施：

委外訓練係快速獲得民間技術的捷徑，也是培養人員專業技能的必要手段，惟在國防資源有限下，必須選擇單位亟待加強或精進部分，且在人員結訓後，必須於單位內實施擴訓，以提升派訓成效。在人員派訓前，必須建立人員學習歷程資料(如：「個人能力分析表」)，包括：受訓經歷、具備證照及人員技能評估等資料，作爲擇優派訓之依據。

有關自訓部份，部隊訓練是戰力的倍增器，委外訓練人員必須將習得的技能，

於部隊訓練課表中排入課程並擔任教官，對單位人員定期實施授課，以傳承知識與技能。另外，單位也可挑選服義務役且具高素質之士官兵擔任教官，負責教授資訊基礎學能，提升部隊官兵之專業知識，以奠定日後接受委外訓練之基礎。

(四)加強與民間機構交流：

現階段民間網路安全技術發展已具相當程度，為提升本部網路安全(戰)專業技能，可與民間專業機構與大學實驗室建立交流管道，或參加國內外研討會(如駭客年會)，除從事技術交流外，更能掌握民間可資動員之人力與物力資源，必要時可大幅提升我作戰能力。

(五)建立組織間交流機制：

由於網路無遠弗屆，網路安全(戰)議題已非單純屬軍方任務，「數位疆土」包含軍網與民網，為達防衛固守，必須與相關單位有效協調與分工，整合軍、警、情等單位共同防禦，使組織間所獲情資及技術發展、教育訓練等資源，達成互相分享與交流，俾發揮整體綜效。

經由本次參與國際性訓練課程，可從中窺知在現今網路科技領域中，本部所需具備之網路安全(戰)能力，廣泛可區分「網路安全」、「應用程式安全」、「稽核」、「法律」及「管理」等五個面向，尤其是必須著重於前兩個面向的技能，方能掌握網路安全(戰)優勢，達到有效防範網路攻擊、降低資安事件影響的作戰目標，並能遂行「以小搏大、以寡擊眾」之不對稱作戰任務。