行政院各機關因公出國人員報告書
(出國類別：研究)

赴美國參加 SANS 資安課程研習報告

服務機關: 內政部警政署刑事警察局
出國人員: 警務正 林芳如
偵查員 張文欣
偵查員 余厚萱

出國地區: 美國
出國期間: 106 年 7 月 21 日至 8 月 1 日、8 月 11 日至
8 月 22 日間、9 月 8 日至 9 月 18 日
報告日期：106 年 12 月 4 日

目錄

壹、摘要

本科為拓展資訊安全專業領域，培訓資安鑑識專業人員，於本年度分 3 梯次派員赴美國參加 SANS(System Administration, Networking and Security)相關課程，SANS 為合作研究及學術教育組織，提供超過 165,000 名以上的資訊安全專家、稽核員、網管系統管理人員及首席資訊長等相關人士，分享其資訊安全教育課程，同時能為其所遭遇的問題提供解決方案。

透過方法及技術的學習，期望能建立資安事件處理規範，運用於未來資安事件偵查、數位跡證蒐集與分析技術之實務運用，並強化專業人才培育，推廣相關偵查技巧至各警察機關科技偵查人員，強化科技犯罪預防及偵查能量，有效提升執法效能。

貳、目的

本次行程為參加美國 SANS 資訊安全相關課程，內容包含駭侵事件電腦蒐證與調查、事件日誌檔分析、網站滲透測試、駭客工具與技巧及電腦鑑識等資安事件調查技術，提升網路犯罪調查人員、資安鑑識分析人員及網路安全管理人員對於最新犯罪偵查技術的認知，並促進各國執法人員、資安專家與高科技犯罪調查產業間的互動、交流與知識分享。

參、行程

一、 106 年 7 月 21 日至 8 月 1 日，FOR508 進階數位鑑識、資安事件處理與威脅狩獵課程。

106 年		預定行程	任務	備註
日期	星期			
7 月 21 日	五	臺灣前往美國華盛頓	飛往美國	

7 月 22 日	六	美國華盛頓	於洛杉磯國際機場轉機	
7 月 23 日	日	美國華盛頓	抵達美國華盛頓	
7 月 24 日	一	美國華盛頓	至 SNAS 上課地點報到，並領取 SANS 上課徽章、上課教材及上課需知。	
7 月 25 日	二	美國華盛頓	進階資安事件調查與網際威脅狩獵課程第 1 堂	介紹進階資安事件調查與網際威脅狩獵並實機操作
7 月 26 日	三	美國華盛頓	進階資安事件調查與網際威脅狩獵課程第 2 堂	學習記憶體擷取技術、記憶體鑑識與相關鑑識工具
7 月 27 日	四	美國華盛頓	進階資安事件調查與網際威脅狩獵課程第 3 堂	執行痕跡偵測、作業系統備份調查、Event Log 分析
7 月 28 日	五	美國華盛頓	進階資安事件調查與網際威脅狩獵課程第 4 堂	時間序列分析、記憶體分析時間序列、作業系統分析時間序列
7 月 29 日	六	美國華盛頓	進階資安事件調查與網際威脅狩獵課程第 5 堂	資安事件調查腳本撰寫、惡意程式與反鑑識技術偵測

7 月 30 日	日	美國華盛頓	進階資安事件調查與網際威脅狩獵課程第 6 堂	進階資安事件調查與網際威脅狩獵總複習與APT攻擊之挑戰
7 月 31 日	一	美國華盛頓	搭機返臺	搭乘當地時間 7 月 30 日 18 時 55 分班機(臺灣時間 7 月 31 日 6 時 55 分)自美國華盛頓起飛，於舊金山國際機場轉機。
8 月 1 日	二	美國華盛頓返回臺灣	抵達臺灣	8 月 1 日 5 時 25 分抵達桃園國際機場。

二、 106 年 8 月 11 日至 8 月 22 日，SEC504 駭客工具、技術、攻擊及事件處理課程

106 年		預定行程	任務	備註
日期	星期			
8 月 11 日	五	臺灣前往美國紐約	飛往美國	搭乘華航機 23 時 35 分班起飛。
8 月 12 日	六	美國紐約	抵達美國紐約	預定當地時間 8 月 12 日 07 時 50 分抵達紐約(臺灣時間 8 月 12 日 19 時 50 分)，並前往飯店。
8 月 13 日	日	美國紐約	抵達住宿飯店	
8 月 14 日	一	美國紐約	至 SNAS 上課地點報到，並領取 SANS 上課徽章、上課教材及上課需知。	

8 月 15 日	二	美國紐約	現場事件處理及網路犯罪偵查	本次課程綜合介紹，包含事件處理流程及因應，學習處理步驟及證據鏈，並利用小組討論方式進行。
8 月 16 日	三	美國紐約	電腦網路駭侵漏洞利用課程第 1 堂	學習如何進行駭侵事件偵測及偵查，認識 IDS 系統的運作及如何繞過 IDS 系統。
8 月 17 日	四	美國紐約	電腦網路駭侵漏洞利用課程第 2 堂	學習 OSI 七層中網路層的攻擊，包括中間人攻擊、ARP 欺騙等手法。
8 月 18 日	五	美國紐約	電腦網路駭侵漏洞利用課程第 3 堂	學習密碼破解、跨網站腳本攻擊、SQL injection 及 DDoS 攻擊。
8 月 19 日	六	美國紐約	電腦網路駭侵漏洞利用課程第 4 堂	利用腳本學習攻擊者如何運用工具進行駭侵，如後門工具 Poison Ivy、Ghost RAT 等。
8 月 20 日	日	美國紐約	使用駭侵工具研習課程，課程結束	利用本次課程所學駭客工具進行練習，對於特定供教學使用之網站發動實際攻擊。
8 月 21 日	一	美國紐約	搭機返台	自美國紐約起飛。
8 月 22 日	二	美國紐約返回台灣	抵達臺灣	抵達桃園國際機場。

三、 106 年 9 月 8 日至 9 月 18 日，SEC560 滲透測試及道德駭客課程

106 年		預定行程	任務	備註
日　期	星期			
9 月 8 日	五	臺灣前往美國拉斯維加斯	飛往美國	搭乘華航 18 時班機，於舊金山國際機場轉機
9 月 9 日	六	美國拉斯維加斯	抵達美國拉斯維加斯	當地時間9月8日20時 30 分抵達美國拉斯維加斯機場(臺灣時間 9 月 9 日 11 時 30 分)，並前往飯店。
9 月 10 日	日	美國拉斯維加斯	至 SNAS 上課地點報到，並領取 SANS 上課徽章、上課教材及上課需知。	
9 月 11 日	一	美國拉斯維加斯	網路滲透測試及道德駭客首日課程	滲透測試綜合規劃
9 月 12 日	二	美國拉斯維加斯	網路滲透測試及道德駭客課程第二日	利用工具進行深度掃描
9 月 13 日	三	美國拉斯維加斯	網路滲透測試及道德駭客課程第三日	弱點偵測
9 月 14 日	四	美國拉斯維加斯	網路滲透測試及道德駭客課程第四日	成功攻擊後之利用及橫向轉移

9 月 15 日	五	美國拉斯維加斯	網路滲透測試及道德駭客課程第五日	深層密碼測試及 APP 滲透測試
9 月 16 日	六	美國拉斯維加斯	網路滲透測試及道德駭客課程第六日	實作課程
9 月 17 日	日	美國拉斯維加斯	搭機返臺	搭乘當地時間 9 月 16 日 17 時班機(臺灣時間 9 月 17 日 8 時)自美國拉斯維加斯起飛，於洛杉磯國際機場轉機。
9 月 18 日	一	美國拉斯維加斯返回臺灣		9 月 18 日 5 時 30 分抵達桃園國際機場。

肆、課程內容重點

一、 FOR508 進階數位鑑識、資安事件處理與威脅狩獵：

(一) 課程簡介

本次研習課程為 FOR508 進階數位鑑識、資安事件處理與威脅狩獵課程(Advanced Digital Forensics, Incident Response, and Threat Hunting)，講師為資安專家 Chad Tilbury。

課程大綱為：

1、 進階資安事件處理與威脅狩獵(Advanced Incident Response & Threat Hunting)

2、 資安事件記憶體鑑識(Memory Forensics in Incident Response)

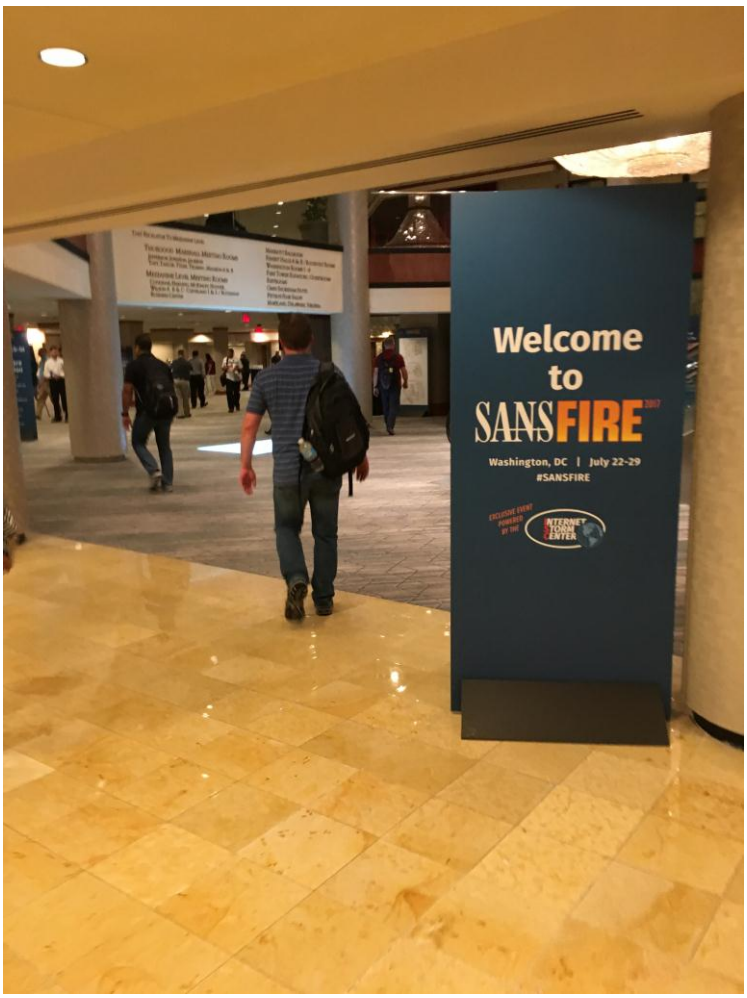
3、 駭侵事件鑑識技術(Intrusion Forensics)

4、 駭侵事件時間軸分析(Timeline Analysis)

5、 企業規模事件處理、進階攻擊與反鑑識技術偵測(Incident Response & Hunting Across the Enterprise | Advanced Adversary & Anti-Forensics

Detection)

6、 進階持續性威脅事件處理挑戰(The APT Incident Response Challenge)



圖片說明：SANS 課程會場照片

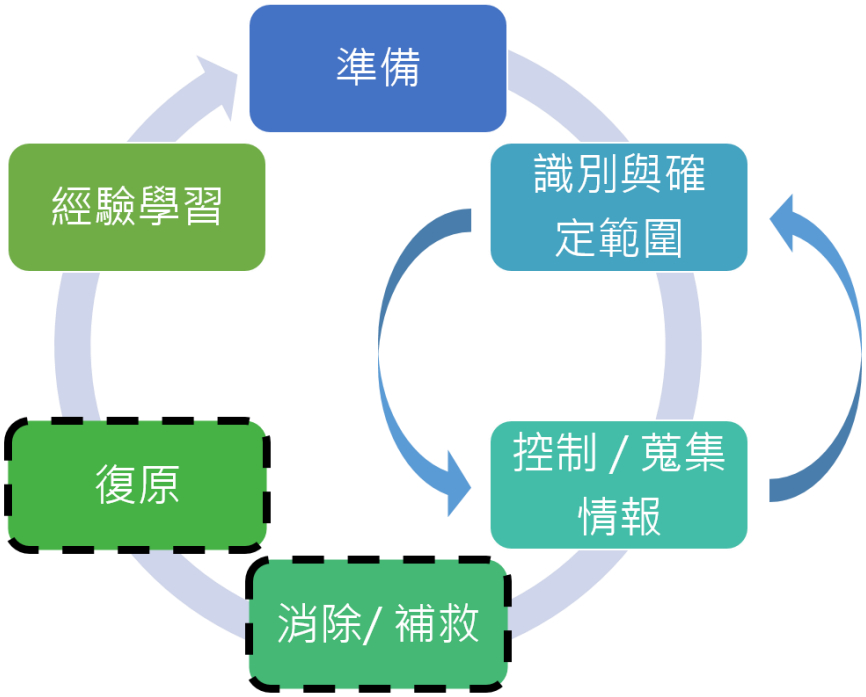
(二) 進階資安事件處理與威脅狩獵：

1、 介紹 SIFT Workstation：

SIFT Workstation 為 SANS 建立之 Linux based (Ubuntu)鑑識調查虛擬環境工作站，提供民眾免費下載使用，安裝多種開源套件，具有彈性，可針對不同跡證進行廣泛或深度調查，其指令式工具雖對於使用者操作較圖形化介面工具困難，但於面對大量證物時運算能力較佳，對於現今多跨系統、跨版本與大規模調查時，展現較好的相容性，可相容 E01、AFF 及 dd 等常見證物格式。另以 Linux based 建立之調查工作站，可於檢視 Windows 系統相關證物時，因作業系統運作方式不同，可確保證物內容不被更動。

2、 資安事件處理程序

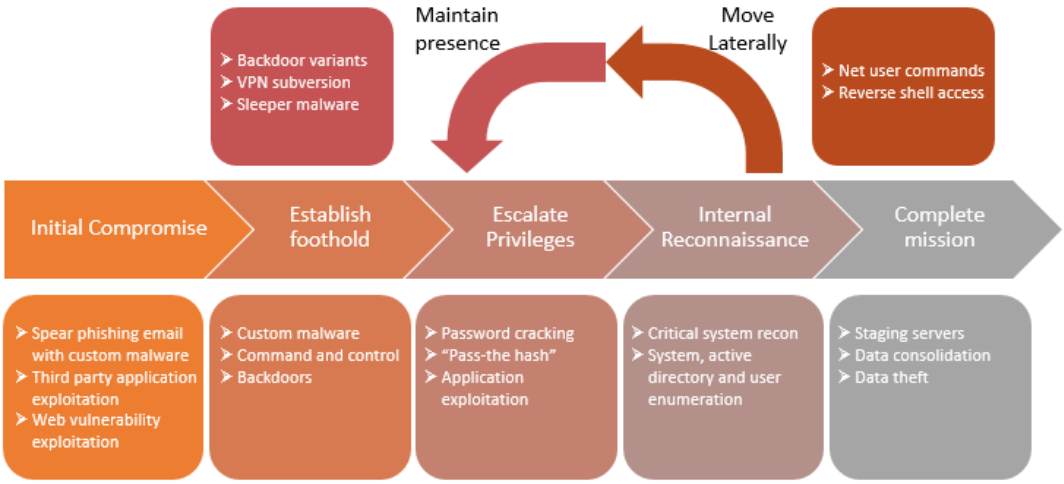
資安事件處理程序可分為準備、識別與確定範圍、控制/蒐集情報、消除/補救、復原、經驗學習等階段。



圖片說明：資安事件處理程序

3、 駭客攻擊生命週期－狙殺鍊(Kill Chain)

身為資安事件調查人員，亦須瞭解駭客想法與攻擊模式，阻斷其狙殺鍊(Kill Chain)，甚至進行反制。駭客攻擊生命週期可以劃分為七個步驟，但這些步驟都並非是必須的，且有些步驟會反覆的進行。



圖片說明：駭客攻擊生命週期－狙殺鍊(Kill Chain)

(三) 資安事件記憶體鑑識

1、 記憶體分析

因電腦作業系統中所有東西運作都必須透過記憶體，故其中含有大量

之數位跡證可供調查人員分析，包含行程、執行緒、惡意程式、網路資訊、開啟檔案、使用者密碼、系統設定檔等等。

2、 記憶體鑑識分析流程

(1) 找出可疑 Processes

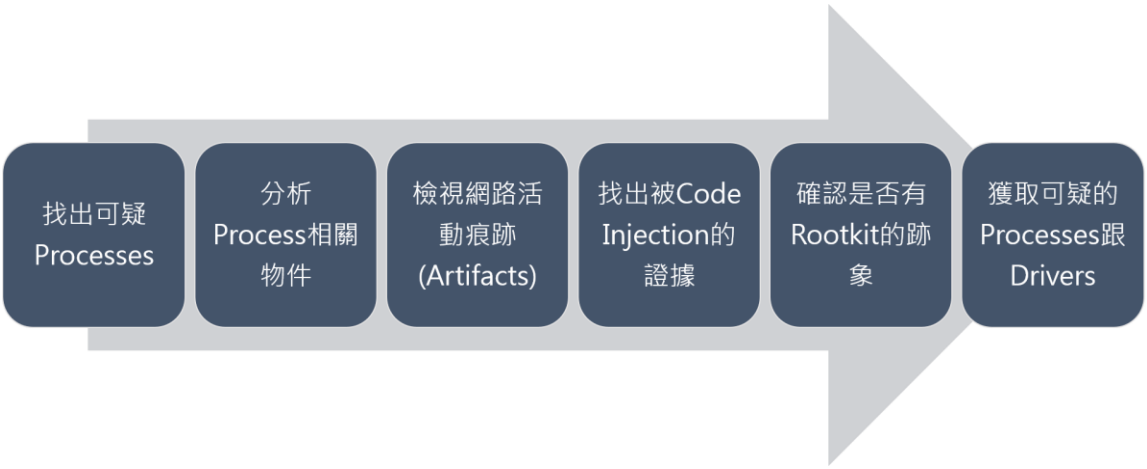
(2) 分析 Process DLLs 與 Handles

(3) 檢視網路活動痕跡(Artifacts)

(4) 找出被程式碼注入(Code Injection)攻擊的證據

(5) 確認是否有 Rootkit 的跡象

(6) 獲取可疑的 Processes 跟 Drivers



圖片說明：記憶體鑑識分析流程

(四) 駭侵事件鑑識技術

1、 執行檔執行過的進階證據(Advanced Evidence of Execution)：如 Windows prefetch、Application Compatibility Cache 等。

2、 Volumes Shadow Copy Service(VSS)

VSS 是整個磁區特定時間點的備份，類似虛擬機的快照功能，其可協助調查人員復原重要檔案 (event logs, registry 與遭刪除的檔案等)

3、 駭客橫向移動策略 Lateral Movement Adversary Tactics

駭客橫向移動策略可以簡化成三件事：取得系統權限、複製惡意程式、執行惡意程式或指令。

4、 事件日誌(Event Log)分析

事件日誌記錄著系統運行時所留下的事件紀錄，可用於剖析帳戶使用行為、追蹤駭客橫向移動、調查可疑的服務、可疑應用程式的安裝、惡意程式的執行等行為。

(五) 駭侵事件時間軸分析

1、 介紹檔案系統時間戳記：

檔案系統包含重要的 4 個檔案時間戳記：M(修改)、A(存取)、C(建立)、E(metadata 修改時間)，可以協助釐清事件經過。

2、 時間軸分析：

將調查資安事件時所蒐集之所有跡證相關時間戳記匯入超級時間軸(Super Timeline)，可協助調查人員釐清資安事件發生經過及事件、跡證間之關聯性。

(六) 企業規模事件處理、進階攻擊與反鑑識技術偵測

1、 介紹進階攻擊與反鑑識技術偵測

許多具有較高技術之駭客會針對受害對象進行資訊蒐集，並擬定專門的攻擊手法，並配合反鑑識技術阻撓鑑識與調查人員蒐集相關跡證，課程中介紹了相關反鑑識的偵測方式，如異常 MFT 表內容、異常時間序列、遭刪除之檔案、Registry Keys、資料抹除(File Wiping)、竄改時間戳記等。

2、 無惡意程式活動之遭感染系統調查

為了調查惡意程式已不存在之感染系統，可透過快速資料檢傷分類分析(Rapid Data Triage Analysis)、網際威脅情資蒐集與感染指標搜尋、系統日誌檔分析等偵測方式協助調查人員判斷系統是否遭感染或入侵：

(七) 進階持續性威脅事件處理挑戰

透過小組合作，以講師提供實際調查情境演練方式，分工合作完成完整之事件調查，分析鑑識系統包含伺服器、多種版本之作業系統等，其過程必須運用課程所學以分析相關電子跡證，釐清資安事件發生之過程、來源，其最快完成調查之優勝隊伍可獲得 SANS 講師頒發之 DIFR 徽章。

圖片說明：講師頒發 DIFR 徽章予優勝隊伍

(八) NetWars 挑戰

本次課程提供學員免費體驗 NetWars 挑戰活動，NetWars 有三種類別，包含：CyberDefense、Core 跟 DFIR。CyberDefense 防禦方的模擬實境競賽；Core 是攻擊方、滲透測試方模擬實境競賽；DFIR 則是 IR 與數位鑑識人員調查模擬實境競賽。

其挑戰活動採限時問答搶分方式，並於活動現場提供即時分數看板營造緊張的競爭氛圍。

本次出席學員選擇與所學相關之 DFIR 類別，活動分為 3 個階段，每個階段約有 40 至 50 題題目，依題目難度給予不同分數，必須將前一個階段都解答完才能進入下個階段。而每答錯 1 次扣 1 分，錯 3 次該題將被鎖住無法回答，不限使用任何工具軟體，商業軟體也可，其答案以開源工具亦可以找到。該活動不僅讓學員有機會實作、練習所學，答題過程必須知道各種數位跡證隱含的意義為何、儲存於何處，且題目領域廣泛，含括 Windows 數位鑑識、Unix 及 Linux 鑑識、網路鑑識、記憶體分析、惡意程式分析與反組譯、手機鑑識，非常具有挑戰性。

圖片說明：偵查員余厚萱參與 NetWars 挑戰得分情形(紅框處)

二、 SEC504 駭客工具、技術、攻擊及事件處理

(一) 課程簡介

SANS 504 課程為駭客工具、技術、攻擊及事件處理課程(Hacker Tools, Techniques, Exploits, and Incident Handling)，課程為期 6 天，課程的進行方式為以簡報講解觀念技術及工具，並輔以 Windows 系統和 Linux 系統的兩個實驗室環境進行實際操作，以供學員了解並熟悉工具的操作。

(二) 現場事件處理(Incident Handling)及電腦犯罪偵查

有鑑於科技犯罪案件在未來可能日益增加，機關內部應有現場事件處理的標準作業流程供處理人員(handler)參照，並製作成 cheat sheet 供出勤人員使用。現場勘查的主要可分為六個階段：準備(Preparation)、識別(Identification)、遏制(Containment)、清除(Eradication)、復原(Recovery)及經驗學習(Lessons Learned)，其主要目的是察覺駭客使用的指令或技術，並釐清已遭駭侵的內部機器。在準備(Preperation)階段並須成立事件處理小組，小組必須訓練至熟練操作軟硬體設備及了解程序，平日並準備好 Jump Bag，供事件發生時使用，並建立回報時間軸，依事件敏感度在不定的時間內做回報。識別(Identification)製作 Windows 及 Linux 兩個系統的 Cheat Sheet 供參；識別為證據鏈(chain of custody)的一環，最好可以全程攝影。遏止(Containment)主要目的是停止破壞(stop bleeding)，並需判斷事件的類型、嚴重性及敏感程度。清除(Eradication)主要是清除受駭設備上的可能作為駭客入侵的方式，包括帳

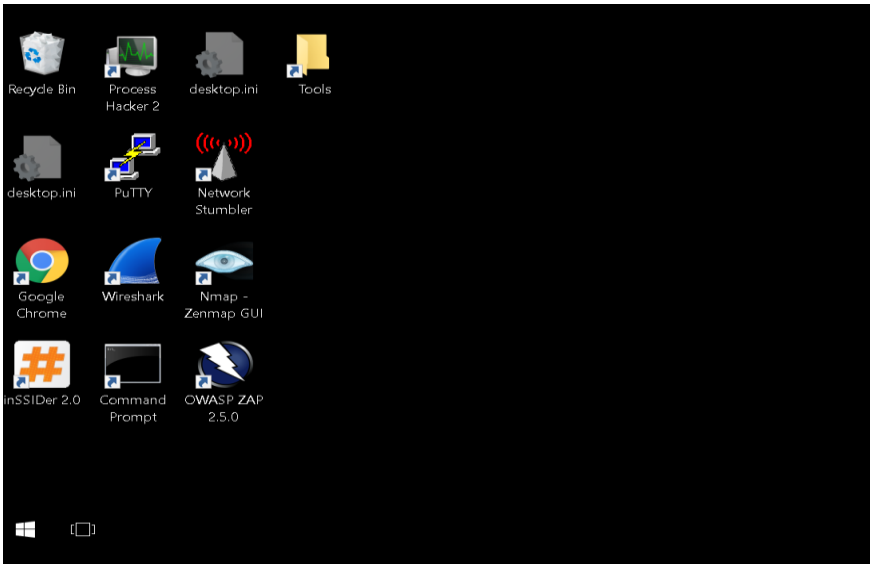
號、惡意程式碼等。復原(Recovery)是回復系統功能正常使用，並且要避免再次遭受駭侵。經驗學習(Lessons Learned)包括產生報告、召開會議及將案件作成附錄供以後參考。通常駭客入侵的程序通常可分為以下階段：偵查(Reconnaissance)、掃描(Scanning)、攻擊(Exploitation)、保持存取(Keeping Access)及清除軌跡(Covering Tracks)，各階段均已有相應的工具，於網路上供免費下載使用。現場事件處理(IR)需勘查的項目眾多，包含 DNS、Web Proxy、Firewall 等，不同端點間的傳輸紀錄，為了解駭客活動的重要勘查項目，尤其現今攻擊的手法日益多元且相互結合，如 DDoS 工具結合蠕蟲等，增加現場事件處理的困難度，機關或企業內部存有大量機器設備及使用者，導致釐清駭客的入侵點亦十分困難。

圖片說明：課程主要在紐約的 Millennium Broadway Hotel 舉行

(三) 駭客攻擊的偵查(Reconnaissance)及掃瞄(scanning)階段

以較中性的單字 attacker，取代使用 hacker 或 cracker。課中並強調若要將課堂所學的工具應用到真實的環境中，務必取得書面的許可。偵查(Reconnaissance)可使用的工具包括 whois lookups、DNS interrogation(使用 nslookup 指令，部分 Linux/Unix 版本使用 dig 指令)，為了安全，應該關閉 DNS zone transfer 的功能，或分別建置 external DNS 及 internal DNS。Attacker 也可能由網站或搜尋引擎蒐集資訊，包括求職、社交網站或 google，如 GHDB 或 google hacking，工具 FOCA 可協助從檔案的 metadata 中找出對攻擊者有用的資訊。掃瞄(scanning)包括 War Dialing、War Driving 及 Network mapping，其中 Network mapping 常使用的工具為 Nmap，並可做 port scanning 及 Active OS

Fingerprinting。攻擊者知道開啟的 port 之後，使用弱點掃描工具，並利用已知的弱點進行攻擊，弱點掃描工具包括 Rapid7、Nessus 及 Open VAS 等。課堂上主要介紹 Nessus，分為商業版及免費版，為 client-server 架構，課堂上並以實驗室情境操作 Nessus。



圖片說明：Windows 實作實驗室環境

(四) 保持存取(Keeping Access)

本天課程為保持存取(Keeping Access)，包括竊聽(sniffing)及 session hijacking。攻擊者可用實體方式保持存取，如使用 Rubber Duckie、Kon-boot 等。Netcat 則是目前最常用的駭侵工具，他可以在利用網路傳輸資料、對 open ports 建立連線、作為後門使用及具有 relay 功能，且可以跨平台操作，包括 Linux、Windows、Mac OS X 等，並以實驗室操做 Windows 及 Linux 環境下的 netcat，包括拿到及放入檔案、利用 netcat 當作 Linux 環境下的後門、做 Linux Netcat relay 等。竊聽(sniffing)可分為兩種，主動及被動，常用的工具為 wireshark。Session hijacking 則是結合 spoofing 及 sniffing 兩種技術，可用的工具包括 Responder。另一階段的課程為攻擊(Exploitation)階段，包括 DNS Cache Poisoning 及 Buffer Overflows。在 DNS Cache Poisoning 中，以 Dan Kaminsky 設計的方法說明該攻擊手法的概念。Buffer Overflow 是一種古老的攻擊方式，但目前仍持續存在。課堂中以程式及記憶體的角度、實例說明來解釋 Buffer Overflows 的攻擊方法。Metasploit 是結合多種攻擊手法的工具，包括漏洞(如 Buffer Overflows)、利用 payload 及具有掃描的功能，可以跨平台操作，包括 Linux、Windows、Mac OS X 等。

圖片說明：Linux 實作實驗室環境

(五) 攻擊(Exploitation)

介紹如何獲得系統的存取權限、網站應用程式攻擊及阻斷服務攻擊，獲取系統存取權限的方式包括破解帳號密碼、盜用 cookies、惡意程式、利用網站漏洞攻擊及中間人攻擊等；常見的阻斷服務攻擊等。破解帳號密碼為介紹「Cain and Abel」及「John and Ripper」等破密工具，並實際操作破解 Windows LM 及 NTLM 的 HASH 加密，其中因為 Linux 的加密有 salt 值，破密難度較高；盜用 cookies 部分，介紹免費的 proxy 工具如 Burp；惡意程式介紹蠕蟲、病毒及木馬，現今的攻擊多會夾帶惡意程式，惡意程式的威脅性將與日俱增；利用網站漏洞攻擊包括 XSS 及 SQLi，XSS 係上傳惡意的 Java Script，分為 Stored 及 Reflect 兩種類型；SQLi 係攻擊者上傳特殊的 SQL 字元，並因系統程式自身存在邏輯錯誤，達到入侵的目的，課堂並以 Linux 實驗室環境實際操作兩種攻擊手法；常見的阻斷服務攻擊有 DDoS 及 DNS 放大攻擊等，並使用工具 LOIC 進行實作。

(六) 保持存取(Keeping Access)及清除軌跡(Covering Tracks)

保持存取的方式包括使用應用層的木馬或後門、wrapper 及加殼(packer)及 rootkits。攻擊者使用應用層的木馬或後門，如 Poison Ivy、Ghost Rat，遠端操控被害者電腦；攻擊者可能利用 wrapper 將後門工具與正常程式包在一起，或使用加殼(packer)方式避免被逆向工程找出惡意的程式碼。記憶體分析是找出攻擊者活動的重要方法，首先亦須先傾印記憶體(memory dump)，可使用工具如 Google’s Rekall，並以 Linux 實驗室環境操作 Rekall 工具。Rootkit 可分為兩種類型，分別為 User-Mode 及 Kernel-Mode，其中又以 Kernel-Mode Rookit 特別重要。Rootkit 會隱藏自己的軌跡，包括登入紀錄、檔案、網路行為及程序。有別於應用層的木馬或後門，Rooktit 會隱身在已存在的程式中，更不易被查覺。有名的 rootkit 包括 Rooty、the Avatar Rookit 等，

免費的 Linux/Unix Rootkit 偵測工具有 Chrootkit、Rootkit Hunter 等；Windows 環境的偵測工具有 Sophos Anti-Rootkit 等。

隱藏軌跡，在 Unix/Linux 環境下，可以是單純的隱藏檔案或是將檔案放在不容易引起注意的資料夾，如/dev 或/tmp。修改 log 紀錄亦是一種方法，可以從/etc/syslog.conf 知道 log 檔案存放的位置，並且特別注意 error_log 及 access_log，這些 log 檔案多以 ASCII 存放，故很容易被修改。除了 log 檔案外，另外要注意 bash history file，該檔案會存放最近執行過的指令。在 Windows 環境下，隱藏軌跡的方法有使用 ADSs(Alternate Data Streams)技術，此為 NTFS 檔案系統特有的功能，要偵測電腦中是否有 ADSs 的檔案，可以使用微軟的工具 Streams；另一個方法同為修改 log 紀錄，在 windows 環境下，log 多存放在 system32 資料夾下的\winevt\Logs 資料夾，可以使用 Event Viewer 工具進行編輯。在網路環境下，隱藏軌跡的方式為使用 tunneling 的技術，將 A 通訊協定的內容封裝(encapsulate)在 B 通訊協定中，常用的技術包括 Reverse HTTP Shells，可用的工具包括 Ptunnel 及 Loki 等。

(七) CTF(Capture the Flag Event)搶旗活動

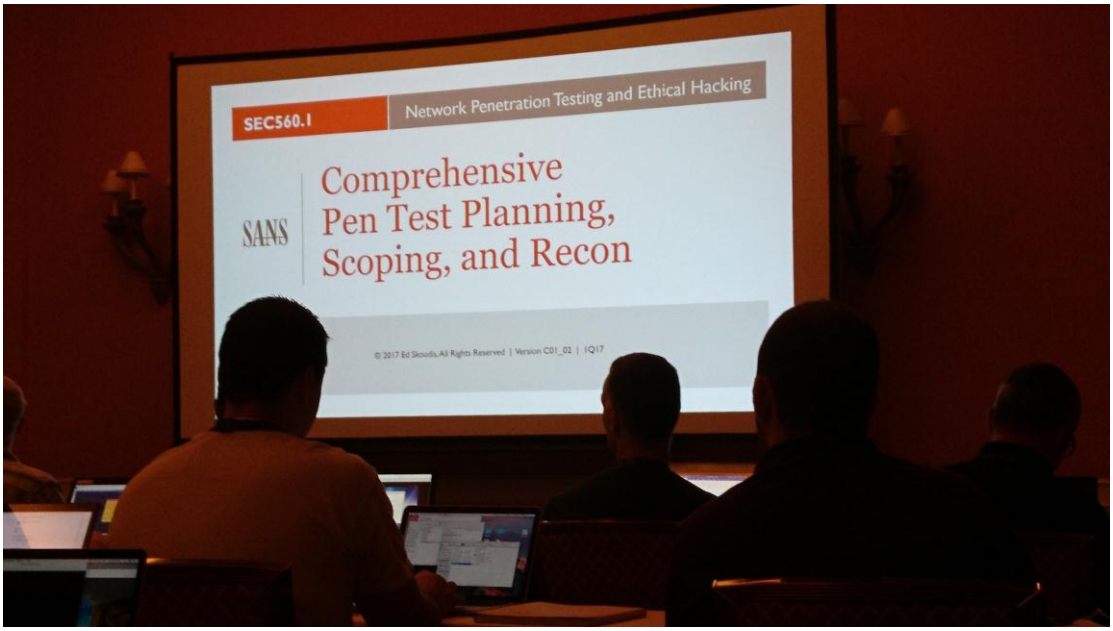
將前述的技術及工具使用，應用到搶旗活動中。由參訓學員各自分組，老師提供 5 個實驗室情境題，分別有 windows 及 linux 兩種環境，成功駭侵該實驗室並取得指定的 flat 檔案(如 flag1.txt)，則代表答題成功，在 windows 環境，flag 檔案放於 c 目錄，linux 環境放於根目錄。第一個完成所有情境題的小組，將獲頒 SANS 課程徽章。活動開始前，由老師講解搶旗規則，我們依指示設定實驗室環境，活動將由上午 9 時持續至下午 2 時 30 分，中途講師不會宣布休息，由小組自行運用所有時間，活動結束後，講師並將逐題講解。搶旗活動的目的是希望透過小組分工的方式，在最短時間內，達成所有任務，呼應課程反覆提到的小組合作的重要性，小組成員間應充分討論。本組共有 5 位成員，分別來自美國、台灣及中南美洲，我們每人負責一道題目，我想辦法找出我所分配到 linux 情境實驗室的可作為進一步駭侵的可用資訊，先進行偵查(Reconnaissance)及掃瞄，使用 Nmap、Nessus，並使用 Metasploit 工具嘗試進行攻擊及植入 netcat 作為後門到目標 IP 上。本小組最終因無法解答一 linux 情境實驗題，無法成功對該 linux 實驗室做提權而未能贏得活動，但亦完成解答其他四道情境題，過程中並充分討論及積極爭取贏得活動的精神，讓我獲益良多，亦讓我對於本次課程所學做一次整體性的實務運用，加深對於本次課程所學的技術及知識。從討論過程中，可以了解其他人的駭侵思維及切入點，並藉由討論，得到其他小組成員的建議，更快解

決自己遇到的瓶頸，為學習的加速器。講師於活動結束後，對於每到情境題做講解，課程結束後，本小組成員互道珍重再見，對我是難得的國際學習經驗。

三、 SEC560 滲透測試及道德駭客

(一) 課程簡介

網絡滲透測試的工具及原理，瞭解系統可能遭利用之漏洞及防禦方式等內容，並由實驗環境進行實機操作。



圖片說明：授課情形

(二) 前言：成功的滲透測試人員應有的心態

1、 在框架外思考、依實務情形嘗試不同的方法。

2、 同時，應審慎、方法化、詳盡記錄、讓工作方法具可重複性。

(三) 名詞定義

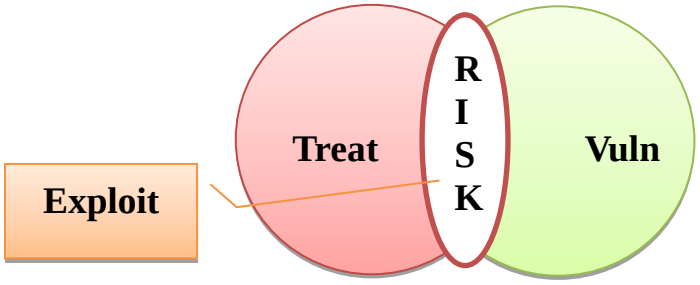
1、 威脅 VS 漏洞 VS 風險

(1) 威脅(Threat)：可能造成損害的人或行為。

(2) 漏洞(Vulnerability)：可能遭人利用以造成損害的漏洞。

(3) 風險(Risk)：威脅及漏洞重疊處。

(4) 弱點利用(Exploit)：威脅者用以利用漏洞的程式碼或技術。



圖片說明：威脅、漏洞、風險定義

(5) 滲透測試人員的工作：為了模擬真實世界的威脅來找到弱點，在一個受控的環境下，利用弱點測試來確定對組織所構成的業務風險，並提供可整合在目標組織營運中的適當防處建議。

2、 駭客、滲透測試、風險評估、安全稽核

(1) 駭客：

A. 傳統駭客：利用科技技術讓目標（系統、裝置等）做到原本未設計的功能。

B. 黑帽駭客：未經授權入侵電腦及網路系統。

C. 道德駭客（白帽）：在標的擁有者的同意下使用電腦攻擊技術來發現安全漏洞，目的在強化標的的安全等級。

(2) 滲透測試

A. 聚焦在尋找標的環境中可能被攻擊者用來滲透網路、電腦系統或竊取資料的安全弱點，滲透測試是道德駭客的一種。

I. 使用工具及技術來模擬犯罪者的行為。

II. 要能防止扒手，必須從扒手的角度來進行思考。

III. 目標在真正完成滲透，成功拿下目標系統並得以存取造成業務影響的資料。

B. 滲透測試的正式定義如下：滲透測試包含模擬真實世界的電腦攻擊技術。

I. 發現弱點。

II. 在可控的情況下利用弱點。

III. 利用專業且安全的方式實施，小心的設計實施的範圍及規則。

IV. 判斷業務風險及潛在影響，目的在幫助組織強化其安全實務。

(3) 紅隊(red team，一般指攻擊方)：

A. 利用滲透測試相關工具及技術來攻擊目標組織。

B. 目標在評估目標組織的偵測、應變處理規範及程序是否有效。

C. 滲透測試旨在發現弱點以更好的管理風險；而紅隊的目標在評估及強強化「藍隊」(防守方)的能力。

(4) 漏洞評估(Vulnerability /Security assessment)：與滲透測試相似，惟較滲透測試在進入目標系統並取得資料等技術性議題而言，風險評估更聚焦在發現弱點並具更明確的政策規範和程序審查。

(5) 安全稽核：就一套**嚴格的標準**進行檢測。

(四) 動機

1、 為什麼要進行滲透測試呢？

(1) 在壞人之前發現弱點。

(2) 幫助組織更好的了解並管理風險。

(3) 提供決策層級參考以決定資源分配優先度。

(4) 用滲透測試的方法真實地找到並利用弱點以說服決策層級往往比其他方式更有說服力。

2、 關於所發現的弱點處理

(1) 並非所有發現的弱點都會被處理，最終旨在風險管理，組織可以從業務角度來決定來接受某些風險而非消滅它。

(2) 所以如何從商業角度呈現滲透測試的發現也是很重要的。

(五) **滲透測試及道德駭客的種類**

1、 網路服務測試、使用者端測試、網路應用測試、社交工程測試（email、電話等）、無線安全測試、實體安全、竊取的設備或裝置(如透過失竊筆電竊取實驗室資料)、密碼分析攻擊(破解或繞過當地文件或攔截通訊的加密，或研析加密保護機制，應注意數位授權管理以免違法)、產品安全測試(針對測是環境所安裝的軟體進行安全測試)

2、 攻擊的各種階段：

(1) 惡意及道德駭客都會執行的階段：偵查、掃描、弱點利用。

(2) 惡意駭客更進一步實施：維護後門及管理員權限的存取、利用隱藏通道或日誌編輯進行滅跡。

(3) 在實務上可根據需求或實務情境跳過任何階段，但在實施滲透測試時應回頭再次檢驗分析跳過的步驟。

(六) **公開或免費的測試方法：**

網路上有數種釋出免費網路掃描季滲透測試方法的組織，提供有用的文件資源來構成客製化的測試計畫。

(七) 建置測試環境

1、 專用的測試用工作站(非日常私人或工作使用、無敏感資訊、耐操、通常無法使用防或牆保護)、掃描專用伺服器(配備高速網路)。
2、 虛擬測試機：易於複製、容易還原。
3、 網路架構：離主幹網路越近且越少過濾越好，注意部分 ISP 業者會偵測掃描或弱點利用型為並進行攔阻，最好可以事先知會你的 ISP 業者。
4、 考慮防火牆的影響。
5、 保護好你的測試用設備：避免第三方、測試方等的攻擊，關閉非必要的服務，在不影響測試的前提下加強安全設定。
6、 加密測試設備上的檔案系統。
7、 在不同測試工作間還原測試系統、抹除測試結果相關資料。

(八) 滲透測試程序概述

1、 準備
   (1) 簽訂保密協定。
   (2) 與目標進行會談，了解主要威脅及業務考量、同意實施規則、確認測試範圍。
   (3) 簽署同意書（注意執行測試之合法性、當地法規、諮詢律師），並示名測試風險。
   (4) 部屬測試小組成員。
2、 執行測試
3、 總結
   (1) 仔細分析並重複測試。
   (2) 報告撰擬及呈現。

(九) 訂定執行滲透測試之規則

1、 執行規則與範圍：兩者皆應事先訂定，通常先訂定範圍有助於測試規則的決定。
2、 未訂定規則可能造成：資源浪費、成效低落，讓目標、第三方等單位生氣。
3、 應與受測單位協議緊急聯繫管道，包括窗口名單、手機等聯絡資訊，應全天候保持練系管道暢通。
4、 透過加密管道交換資訊，如發現的弱點、測試報告等。
5、 進行每日工作報告，包括執行內容、重要發現、測試目標是否偵測到滲透測試等。

6、 規則訂定注意事項：

(1) 不應包含價格、責任等（應訂於合約）。

(2) 應訂定開始及結束日期，協商可執行測試時間(如僅晚間或周末)。

(3) 協商是否讓測試對象的網管、資安部門獲知將執行測試，並注意不宣告之風險。

(4) 協商結束測試的定義，如發現弱點或成功拿下目標機器等。

(5) 黑箱（更貼近實際駭親狀況？）或白箱測試（更有效率、試可能的攻擊樣態、減少傷害目標系統的可能）。

(6) 閱讀受害系統內文件應當心：

A. 可能包含私人使用者資料或客戶資料

B. 或許可訂定測試樣品來確認駭侵是否德真正存取相關資料及對業務之影響

(7) 相關文件應由目標組織、測試小組主管、測試人員（非必要）簽署。

(十) 計劃執行範圍

1、 詢問測試對象最關注議題為何？

(1) 資訊洩漏

(2) 阻斷服務

(3) 網頁置換

(4) APT 攻擊等

2、 避免範圍擴張：討論威脅、風險及已知弱點，注意執行效率。

3、 建立簡單明的測試範圍：有哪些需被測試的標的，如特定網域名稱、網段、主機、應用服務等，有那些是特別需要避開的，在測試前製作測試範圍文件，並在測試中發現新項目時檢閱確認。

4、 第三方：測試涉及第三方設備時需取得明確書面同意書，如路由器、交換機、郵件伺服器、DNS 伺服器等。

5、 對雲端進行測試：與客戶訪談，有哪些設施與雲端運算有關，這是私有雲或公有雲？雲提供者為何？其他承租人為何？取得同意書或檢視和約是否規範安全評估、滲透測試相關內容。

6、 從雲端進行測試：利用雲端資源進行攻擊應確保雲端服務提供者的同意，利用運算資源可實施掃描、弱點利用、密碼解等。

7、 在測試環境或真實環境中實施：考量到對業務運作的影響，使用測

試環境為優，但多數組織並無測試環境，或測試環境相較真實環境存在差異。

8、 組織內部可能也存弱點，可實施現地測試或透過 VPN、SSH 等方式。

9、 測試的方式：掃網斷已發現主機、針對主機進行 Port Scan、弱點掃描、監聽網路服務、透過使用者軟體進行滲透、應用層的操作、實體滲透、設交工程等。

10、阻斷服務：

(1) 僅確認版本號來檢查是否存在弱點。

(2) 或真的實施阻斷服務攻擊來確認，具危險性，但總的來說，在可控環境中發現弱點總比真的遭遇攻擊來的好。

(十一) 滲透測試報告

1、 一定要寫報告：報告可用以歸檔存查，即使是針對自己組織內部的滲透測試也應撰擬報告，在測試當下便記錄操作情形、截圖、即時記錄發現狀況。

2、 不要僅表列弱掃結果：應檢視弱掃結果並協助目標組織瞭解相關重點內容，如弱點代表意義、如何修補、優先值等。

3、 報告應函內容：

(1) 摘要：最重要、包含總結、簡列重要發現及對業務的影響。

(2) 簡介：時間區段、執行範圍、關聯人員。

(3) 方法：程序、每階段執行結果、工具、執行標的等）。

(4) 發現：弱點存在位置、風險等級、被利用難易度、技術細節、建議，勿列入密碼資訊，最好配上編輯截圖凸顯重點。

(5) 建議：

A. 補丁、系統規劃、工作程序等。

B. 從問題成因考慮，以預防或避免相同情況再次發生。

C. 可能的話，不要提供唯一解。（考量資安等及需求、便利性、成本等）

(6) 結論：專案、範圍、整體資安陳述、發現、點等總結。

(7) 附錄：掃描結果詳細資料、專案相關文件備份及其他相關的項目資料。

伍、心得與建議事項

一、 學員經驗豐富且樂於分享：

本次課程之參訓學員來自各大廠商的資安人員、滲透測試人員，且超過三分之二參加過至少 1 場 SANS 課程、拿過多張資訊安全相關證照。學員經驗豐富，時常於課堂上與講師交流經驗。此外，因許多學員具有滲透測試相關背景知識或實務經驗，亦能於不同角度與其他學員分享攻擊方技巧與想法，帶給本次課程防禦方許多衝擊與知識交換。

二、 提供最新資安相關資訊分享：

講師每日會提供大量近期資訊安全最新之攻擊手法、威脅趨勢、鑑識與分析技術等情資，並介紹其他更深入之分析鑑識領域相關延伸閱讀資料、書籍，提供學員未來相關技術專長研究方向。

三、 建立資安事件處理標準程序：

目前國際上未針對資安事件處理訂定標準程序，各資安公司、學界所提流程多以企業資安團隊調查企業本身資安事件之相關處理程序，以企業確保資訊鐵三角政策：機密性（Confidentiality）、完整性(Integrity)、可用性(Availability)為出發點所設計，而缺乏證據保全、電子跡證證據力與證據證明力之相關設計，為確保資安事件調查品質與證據保全，我國執法機關應積極、盡速訂定相關資安事件處理標準程序。

四、 資安鑑識專業分工與人才養成

SANS 課程所介紹的資安事件調查架構係以團隊方式進行，事件發生後，先由現場初步處理人員進行勘查分析，再將所蒐集之數位跡證分交各專業團隊分析，再將分析結果合併、關聯進行討論以釐清案情。專業領域包含網路鑑識、Windows 主機鑑識、Unix 及 Linux 主機鑑識、記憶體分析、惡意程式分析與反組譯、手機與行動設備鑑識等，各領域專長培育不易，但透過有效專業分工並以團隊合作方式調查案件，可提高調查效率。

陸、結語

近年大規模駭侵資安事件頻傳，隨著資通訊設備普及與發達趨勢，加上網際網路無國界之特性，亦使查緝網路犯罪變得困難，加強國際間資安調查技術與威脅情資之分享與交流，乃能有效預防、遏阻駭侵事件攻擊。本次代表本局參加 SANS 資訊安全課程，獲益良多，講師提供許多詳盡、最新的資訊安全相關訊息，且在小組互動討論過程中，學員間也能大方交流調查技術與過往經驗，學習氛圍

極佳。講師於課程中提供之工具與技術之知識，我國警察機關可運用於未來資安事件偵查、數位跡證蒐集與分析技術之實務運用，期望未來能推廣相關偵查技巧至各警察機關科技偵查人員，強化科技犯罪預防及偵查能量，有效提升執法效能。