《資訊安全實務》

試題評析	本次命題除了典型亮點—數位鑑識之外，亦出現了行動裝置的安全議題，以及第一銀行 ATM 盜領案的時事。是以，學員在準備上除了基本分數要掌握外，近期資安事件新聞亦需多加留意。
考點命中	第一題：《高點．高上資訊安全實務講義》第一回，張又中編撰，上課補充。 第三題：《高點．高上資訊安全實務講義》第二回，張又中編撰，頁 2-3～21；第三回，頁 3-20。 第四題：《高點．高上資訊安全實務講義》第一回，張又中編撰，頁 1-7、11。

一、何謂駭客遠端遙控 ATM？（8 分）並請以第一銀行為例，說明國外駭客入侵該銀行 ATM 的做法。（17 分）

【擬答】

駭客藉由植入如木馬、後門等惡意程式至 ATM 系統，以獲得 ATM 的控制權限，並透過網路下達指令來遠端遙控 ATM 進行動作，例如：開啟出鈔口、吐鈔、執行特定應用程式等。

俄羅斯駭客入侵第一銀行 ATM 的做法如下：

(一)從分行入侵內部網路

駭客可能透過社交工程、釣魚郵件等方式，入侵第一銀行倫敦分行的行員個人電腦，藉此進入第一銀行的內部網路。

(二)建立內部網路潛伏基地

由於第一銀行的海外分行和總行系統間並無實質且明顯的區隔，故駭客可由第一銀行的內部網路逐步建立其潛伏基地。

(三)暗中蒐集入侵情報

駭客控制了一臺屬於第一銀行內部系統的錄音系統伺服器，以穿透防火牆進行存取連線。

(四)進行 ATM 入侵準備

駭客在 2016 年 7 月 4 日透過 ATM 軟體遞送伺服器，發送一可開啟 ATM Telnet 服務的遞送管理系統(Delivery Management System, DMS)更新，可將 Telnet 服務從手動模式轉為自動開啟模式。

(五)開啟 ATM 遠端控制

收到此更新的 ATM，自動按照例行系統更新程序執行，待下次重新開機後即會自動開啟 Telnet 服務，讓駭客可以遠端控制。

(六)植入木馬發動盜領

駭客於 2016 年 7 月 9 日再次從遠端登入，將木馬程式遞送到 ATM 並執行，讓 ATM 每次吐鈔 60 張。

二、何謂 ISO/IEC20000 標準？（5 分）並請詳述其中有多少功能？（20 分）

【擬答】

ISO/IEC 20000 是第一個 IT 服務管理的國際標準，描述如何建置非僅考慮技術需求，而是以企業目標導向並提供支援的 IT 服務。前身為 BSI Group 所發展的 BS 15000，ISO/IEC 2000 是最早發展為反映 ITIL 框架下的最佳實務指引，然其也支援其他的 IT 服務管理框架與方法，如 Microsoft Operations Framework 與 ISACA's COBIT 框架的元件。其中，ISO/IEC 20000-1:2011 敘述規劃和建置 IT 管理系統的指引；ISO/IEC 20000-2:2012 則說明服務管理的最佳實務。

ISO/IEC 20000 功能如下：

Parts	Content
20000-1	服務管理系統需求 Service management system requirements
20000-2	服務管理系統應用指引 Guidance on the application of service management systems
20000-3	服務提供者 Service providers

20000-4	流程評估模型 Process assessment model
20000-5	ISO/IEC 20000-1 導入計畫範例 Exemplar implementation plan for ISO/IEC 20000-1
20000-9	ISO/IEC 20000-1 雲端服務應用指引 Guidance on the application of ISO/IEC 20000-1 to cloud services
20000-10	概念與專有名詞 Concepts and terminology
20000-11	ISO/IEC 20000-1:2011 與 ITIL 服務管理框架的關係指引 Guidance on the relationship between ISO/IEC 20000-1:2011 and service management frameworks: ITIL®
20000-12	ISO/IEC 20000-1:2011 與 CMMI-SVC 服務管理框架的關係指引 Guidance on the relationship between ISO/IEC 20000-1:2011 and service management frameworks: CMMI-SVC

三、請試述手持移動裝置遭受惡意程式攻擊目標的原因。（10 分）並詳述惡意程式的種類有那些?（15 分）

【擬答】

手持移動裝置是一種小型計算機，具顯示螢幕、觸控輸入或是小型鍵盤，透過其網路連線功能以隨時隨地存取獲得各種訊息。例如：智慧型手機、平板電腦、攜帶型遊樂器等。

由於手持移動裝置在有無線基地台之處，可隨時隨地進行網路連線，加上與個人電腦相較，其資訊安全防護能力較弱，故易成為惡意程式攻擊目標。

惡意程式的種類如下：

(一)電腦病毒(Virus)
(二)電腦蠕蟲(Worm)
(三)後門程式(Backdoor)
(四)特洛伊木馬(Trojan Horse)
(五)惡意程式隱匿技術(Rookit)
(六)網頁惡意程式(Webpage Malware)
(七)間諜軟體(Spyware)
(八)廣告軟體(Adware)
(九)勒索病毒(Ransomware)
(十)SQL Injection

四、何謂數位鑑識？（7 分）並請以一個國內案例，說明數位鑑識的情況。（18 分）

【擬答】

數位鑑識為透過標準的數位證據採證流程，將電腦、網路設備中的數位證據加以保存，並整合相關數位證據進行分析、比對，還原事件發生的原始面貌。

數位鑑識流程如下：

(一)蒐集
(二)檢驗
(三)分析
(四)報告
(五)呈現

新北市張姓男子被楊姓前女友指控涉妨害性自主等罪嫌，檢警依兩人 MSN 對話紀錄起訴。張男筆電被台北市刑大查扣保管後，筆電內 MSN 紀錄疑遭警方竄改，經調查局資安鑑識實驗室鑑定後，發現於 2011 年 1 月 28 日下午，筆電被警方查扣期間 MSN 對話有竄改紀錄。新北地院因此認為該電腦紀錄已遭竄改無證據效力，楊女等人證詞也不足認定張男涉性侵、恐嚇，判決張男無罪，案經上訴高院遭駁回。法官另向檢方告發，要求追究是否有不肖警員涉嫌變造證據，張男並反控楊女與警方涉嫌誣告、妨害電腦使用等罪。