《資訊安全實務》

試題評析	本次出題攻守兼備，除了傳統考題如 SOC、數位鑑識外，熱門議題如勒索病毒亦現蹤跡。是以，學員在準備上除了傳統的資安議題需確實掌握外，資安新知也需有所涉獵，方能獲得高分。
考點命中	第二題：《高點資通安全總複習講義》第一回，張又中編撰，頁 1-50~53。 第三題：《高點資訊管理與資通安全講義》第三回，張又中編撰，頁 3-5。 第四題：高點張又中 FB 補充資料，6/21PO 文：勒索病毒。 第五題：《高點資訊管理與資通安全講義》第三回，張又中編撰，頁 3-29、45~46。

一、企業為了解本身之網路設施安全程度，往往會進行滲透測試（Penetration Test）。何謂滲透測試？並詳述其測試程序內容。（20 分）

【擬答】

滲透測試(Penetration Testing)為委託受信任的第三方—通常為資訊安全顧問，針對受測標的模擬駭客的手法進行攻擊測試。目的是發掘受測標的之弱點，並提出改善建議，以提升其資訊安全防護能力。

根據美國 NIST(National Institute of Standards and Technology)定義滲透測試程序內容如下：

(一)規劃(Planning)

決定受測的目標與範圍，訂定滲透測試計畫與簽署雙方同意協定(Rules of Engagement, ROE)，為成功的滲透測試背景作業。

(二)探索(Discovery)

蒐集與掃描受測標的以獲得資訊，包含辨識其網路的通訊埠與服務等。亦包含弱點分析(Vulnerability Analysis)，其為針對受測標的之服務、應用程式與作業系統，比較弱點資料庫與測試者的弱點知識。

(三)攻擊(Attack)

為滲透測試的核心，利用實際的攻擊行為，針對先前辨識出的潛在風險進行攻擊嘗試。如果攻擊成功即可找出弱點。

(四)回報(Reporting)

針對已完成的滲透測試活動進行整理，描述所發現的弱點，評比風險，並給予改善建議。

二、何謂數位鑑識？為能有效保全及使用數位證據，說明其方法與基本原則為何？（20 分）

【擬答】

(一)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。

(二)數位鑑識方法與基本原則如下：

1.在不改變或破壞證物的情況下取得原始證物。

2.證明所抽取的證物來自於扣押的證物。

3.在不改變證物的情況下進行分析。

三、所謂身分認證是要系統能辨認出使用者的真正身分，採用的認證資訊必須要有唯一性，不會與其他人重複。目前有那三種身分認證方式可達到此種要求？並舉例說明利用前述身分認證方式達到雙重因子認證（two-factor authentication）的目的。（20 分）

【擬答】

(一)身分認證的三個因子為：

1.所知之事(Something You Know)

例如：密碼、PIN、個人資料。

2.所有之物(Something You Have)

例如：提款卡、智慧型手機、USB Token。

3.與生俱來(Something You Are)
例如：指紋、視網膜、DNA。

(二)雙重因子認證，即是結合上述的兩個因子進行身分認證。例如，至 ATM 提款時，需先插入提款卡(所有之物)，之後輸入提款卡密碼(所知之事)，相較於單一因子認證，較為安全。

四、日前報章雜誌報導企業或公司行號遭受勒索病毒（Ransomware）的攻擊。何謂勒索病毒？並說明其可能感染途徑及防禦措施。（20 分）

【擬答】

(一)分為鎖定被害者電腦的非加密型，以及系統性加密被害者檔案的加密型。其要求被害者繳納贖金，以取回電腦的控制權或是加密金鑰。通常透過特洛伊木馬，將自身掩蓋為看似無害的檔案。

(二)1.勒索病毒可能感染途徑有：
(1)網路釣魚
(2)網頁木馬
(3)後門程式
(4)社交工程
(5)軟體漏洞

2.勒索病毒防禦措施如下：
(1)使用防毒軟體
(2)備份重要檔案
(3)定期更新軟體
(4)關閉郵件預覽功能
(5)避免點選不明連結

五、若資安事故生命週期是以事前預防、事中監看與事後處理等三個階段做區分：
（一）說明資訊安全監控中心（Security Operation Center, SOC）大致可分為那五項主要功能以滿足資安事故生命週期之需求。（10 分）
（二）國內各級政府機關在國家資通安全會報的要求下，均已完成或正在進行資訊安全管理制度（Information Security Management System, ISMS）的導入，說明 SOC 與 ISMS 之間的關係。（10 分）

【擬答】

(一)SOC 主要功能有：

1.資安警訊管理
每日蒐集最新的資安警訊，判斷其是否會對系統造成風險，並對新發現的弱點進行修補。

2.資安弱點管理
常見的稽核方式為弱點掃描及滲透測試，必須定期執行，並對發現的弱點進行修補。

3.資安設備管理
如定期更新防毒軟體病毒碼、定期審定防火牆規則、定期檢視 IDS 與 IPS 的 Log。

4.資安事件監看
7x24 監看系統，由 SOC 平台進行初步的資料過濾，再由專業的資安技術人員分析，於資安事件發生時立即處理。

5.資安事故處理
進行資安事故的後續處理與改善，事故處理的方式端視系統重要性與關鍵性，如重要性較低的主機可以逕行重新安裝作業系統的方式解決。

(二)於 ISMS 標準 ISO 27001:2013，其將資訊安全事件管理(Information Security Incident Management)獨立成一個領域(A.16)，可見資安事件管理於 ISMS 的重要性。SOC 的功能涵蓋資訊安全事件管理的控制措施，透過 SOC 的運作，可對資安事件進行有效的安全管控。因此，導入 ISMS 與 SOC 這兩項政策，在實務上是資安管理相輔相成的兩種工具。