《資通安全》

一、請試述下列名詞之意涵：（每小題 5分，共 25 分）

(一)Electromagnetic Recording

(二)Integrity

(三) Zero-Knowledge Penetration Test

(四)Hash Value

(五)Access Control List

【擬答】

(一)根據我國刑法第 10 條第 6 項：「稱電磁紀錄者，謂以電子、磁性、光學或其他相類之方式所製成，而供電腦處理之紀錄。」

(二)完整性係指避免未經授權的使用者或處理程序竄改資料，所使用的文件經傳送或儲存過程中必須證明其內容未遭竄改或偽造。

(三)滲透者處於對系統一無所知的狀態下，進行滲透測試。滲透者最初的資訊源自於 Web、DNS、Email 及各種公開對外的伺服器。

(四)將不定長度的位元資料輸入雜湊函數(Hash Function)後，以函數運算轉換為固定長度的雜湊值(Hash Value)輸出。可防止資料被竄改，驗證其資料完整性。

(五)存取控制清單為限制資源存取的處理方式與程序之清單，以保護系統資源不會被未經授權者存取或授權者本身的不當存取。

二、有關入侵偵測與防禦系統（IDS/IDPS），請回答下列問題：

(一)IDS/IDPS 偵測資安事件有四種方法：Signature-based Detection、Anomaly-based Detection、Stateful Protocol Analysis Detection 及 HybridDetection。請說明這四種方法的運作方式。（15 分）

(二)以網路為基礎的 IDPS 會記錄它所偵測到的資安事件相關訊息，以提供驗證、告警、事件調查或其他相關資安紀錄的比對等用途，請寫出 IDPS 紀錄內容包括那些？（10 分）

【擬答】

(一)特徵基礎偵測(Signature-based Detection)亦稱誤用偵測(Misuse Detection)，為最常用於 IDS 的偵測方式。系統先建立一個入侵特徵資料庫，只要偵測到的行為與資料庫內的特徵相符，系統就會將其視為入侵。

異常基礎偵測(Anomaly-based Detection)先建立一個正常的使用者行為或網路流量之統計模型，再對通過的封包進行比對，如超過正常行為門檻值即視為異常。

狀態協定分析偵測(Stateful Protocol Analysis Detection)辨別協定狀態的偏差，與異常基礎法類似，然本方法使用廠商或是業界領導者預先設定的啟始活動之可接受定義。

混合偵測(Hybrid Detection)則是綜合使用上述方法稱之。

(二)1.時間

2.IP 位址

3.通訊埠(Port)

4.通訊協定(Protocol)

5.封包內容

三、美國國家標準暨技術局(NIST)的 SP800-30 文件「資訊技術體系風險管理指南」(Risk Management Guide for Information Technology Systems)對風險(Risk)定義如下：

particular potential vulnerability, and the resulting impact of that adverse event on the organization.

(一)請針對上述風險(Risk)英文定義以中文表示。(5 分)

(二)定義「Vulnerability」和「Impact」。(10 分)

(三)請寫出我國《資通安全管理法》(公布日期：民國 107 年 06 月 06 日)第 3 條第 3 款「資通安全」和第 7 款「關鍵基礎設施」之用詞定義。(10 分)

【擬答】

(一)風險為給定威脅來源使用潛在弱點的可能性之函數，其會對組織負面事件造成影響。

(二)根據 NIST SP800-30 Rev. 1 定義 Vulnerability 如下：

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

根據 NIST SP800-53 Rev. 4 定義 Impact 如下：

The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system.

(三)資通安全：指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。

關鍵基礎設施：指實體或虛擬資產、系統或網路，其功能一旦停止運作或效能降低，對國家安全、社會公共利益、國民生活或經濟活動有重大影響之虞，經主管機關定期檢視並公告之領域。

四、根據《中華民國刑法》第三十六章妨害電腦使用罪有關第 358 條至第 363 條之規定，以及資料(或資訊)隱藏，回答下列問題：

(一)何謂資料(或資訊)隱藏？(5 分)

(二)寫出三種資料(或資訊)隱藏技術。(6 分)

(三)寫出二種「反資料(或資訊)隱藏」的技巧或做法。(4 分)

(四)如果嫌疑犯利用資料(或資訊)隱藏技術致生被害人無法正常使用電磁紀錄時，則該嫌疑犯可能觸犯那條條文，請寫出適用條文內容，並加以說明。(10 分)

【擬答】

(一)指不讓預期的接收者之外的任何人，知曉資料/資訊的內容或是傳遞事件。

(二)語言隱碼術(Linguistic Steganography)為利用語言或是文字的知識，將資訊隱藏於其中而不被接收者之外的人士覺察的技術。例如：文字的大小、間距、字體，或是其他可用來修改以包含隱藏的資訊之特性。只有接收者知道所使用的隱藏技術，才能夠恢復所乘載的原始資訊。

科技隱碼術(Technical Steganography)為利用數位影像或是數位訊號，隱藏資訊於其中而不被接收者之外的人士覺察的技術。例如：可將資訊嵌入至數位圖片中，然該圖片與原始圖片乍看之下幾無差異，待接收者收到後再將圖片經由演算法運算後得到所乘載的原始資訊。

數位浮水印(Digital Watermarking)是將代表合法擁有者的資訊加入至被保護的媒體中，一旦此媒體被懷疑有被剽竊或盜用的嫌疑時，即可透過一公開演算法來取出數位浮水印，以做為此媒體的智慧財產權認證。

(三)文字內容分析為解析文字出現的頻率、字首、位移量、語言學之意義，以及文字之意涵，以求得所隱含的原始資訊。

檔案內容分析則是利用軟體工具，試圖驗證檔案是否有經過資料串接、資料替換，以及資料延伸以隱藏資訊，再依據不同的面向進一步求得所隱含的原始資訊。

(四)

中華民國刑法	條文內容
第 358 條	無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
第 359 條	無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。
第 360 條	無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
第 361 條	對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。
第 362 條	製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。