代號：50830
頁次：1－1

112年公務人員特種考試警察人員、一般警察人員、國家安全局國家安全情報人員考試及112年特種考試交通事業鐵路人員、退除役軍人轉任公務人員考試試題

考 試 別：警察人員考試
等　　別：三等考試
類科組別：警察資訊管理人員
科　　目：警政資訊管理與應用
考試時間：2 小時　　座號：_____

※注意：㈠禁止使用電子計算器。
㈡不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。
㈢本科目除專門名詞或數理公式外，應使用本國文字作答。

一、傳統上，在開發大型資訊系統的時候，經常會使用系統開發生命週期（SDLC）或瀑布法進行。如果你的機關希望利用類似微軟Azure ChatGPT的服務為底層，透過API介接，開發一個專屬機關的服務，請評估SDLC的適用性。開發這樣的系統，是否有其他的替代方案作為基礎的方法論？請評估其間的取捨。（20 分）

二、你被賦予建立一個利用 NFC 進行警察巡邏、員警報到查核的系統。請提出三個可能的方法來取得和建置該系統。請分析三者的利弊得失。（20 分）請挑選一個方案，提出你怎麼著手規劃推動該計畫。（10 分）

三、根據某新聞網（2020 年 5 月 31 日）政治中心／綜合報導：近日國外網站揭露，有專家在暗網（dark web）發現一個數據庫，其中包含超過 2,000 萬筆臺灣公民戶政的詳細資訊，並稱這是我國內政部戶政資料外流。對此，行政院資安處表示並非事實，經分析後發現，該項資料並非從單一來源取得，也不是戶政系統之內容。資安處指出，據上述國外資安網站揭露之資料，經比對內容，應係流傳於暗網多年，最近一次出現是在 2017 年底於暗網拍賣，當時即已協請戶政單位確認，不是戶政單位資料……。請分析這種個資外洩的資安事件可能的原因。（10分）你需要蒐集什麼資訊來協助你進行判斷？（10分）

四、假設你在一個大型的軟體公司任職。主管交辦一件任務，是去規劃投標一個大型案子。你初步瞭解了使用者需求。這是某個物流公司提出的，希望開發一個動態的人力調派系統。需要能在一個控制室中，隨時在大螢幕上看到管轄地區的地圖、當前交通狀況（類似 Google Map）、各物流車的位置等。點選其中一輛物流車，就可以知道其業務細節（例如：正在從 A 地點開往 B 地點等）。在接受到一個臨時送貨任務時，系統需要能很快地分析出，那一輛物流車是最適合被調派出任務的（依據預計抵達時間等等）。你認為這項系統是屬於以下那一類：OLTP, DSS, EIS, Data Analytics, GIS？為什麼？（10 分）請提出一套解決方案，包括可能的初步需求、所需要的技術項目、進行步驟和進行方式等。（20 分）

代號：50860
頁次：1－1

112年公務人員特種考試警察人員、一般警察人員、國家安全局國家安全情報人員考試及112年特種考試交通事業鐵路人員、退除役軍人轉任公務人員考試試題

考 試 別：警察人員考試
等　　別：三等考試
類科組別：警察資訊管理人員
科　　目：電腦犯罪偵查
考試時間：2 小時　　座號：＿＿＿＿＿＿

※注意：㈠禁止使用電子計算器。
㈡不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。
㈢本科目除專門名詞或數理公式外，應使用本國文字作答。

一、請解釋何謂 MITRE ATT&CK 資安框架，並且說明此框架對偵辦電腦犯罪之幫助。（25 分）

二、請說明駭客發起分散式阻斷服務攻擊（DDoS）之流程；（10 分）DNS 放大攻擊為 DDoS 攻擊手法之一，請說明其攻擊特點以及原理。（15 分）

三、虛擬貨幣為目前常被犯罪者使用之貨幣之一，請舉例說明三種虛擬貨幣犯罪態樣並且說明虛擬貨幣查扣之流程。（25 分）

四、調查惡意程式相關案件時，可能會使用靜態分析以及動態分析的技術，請說明何謂靜態分析及動態分析？並說明這兩種分析方式的優缺點。（25 分）

代號：50870
頁次：1－1

112年公務人員特種考試警察人員、一般警察人員、國家安全局國家安全情報人員考試及112年特種考試交通事業鐵路人員、退除役軍人轉任公務人員考試試題

考 試 別：警察人員考試
等　　別：三等考試
類科組別：警察資訊管理人員
科　　目：數位鑑識執法
考試時間：2 小時　　座號：_____

※注意：㈠禁止使用電子計算器。
㈡不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。
㈢本科目除專門名詞或數理公式外，應使用本國文字作答。

一、請以國內學者所提出數位證據鑑識標準程序（Digital Evidence Forensics Standard Operating Procedure, DEFSOP）四大階段（原理概念階段、準備階段、操作階段、報告階段）為基礎及參考國際資安鑑識相關標準（如 ISO/IEC 27037/27041/27042/27043 等），如何建立一套完整行動鑑識標準作業程序（DEFSOP for Mobile Forensics, DEFSOP-MF）？並請舉例及繪圖表說明之。（25 分）

二、請說明電腦鑑識（Computer Forensics）、軟體鑑識（Software Forensics）、資料鑑識（Data Forensics）、網路鑑識（Network Forensics）、行動鑑識（Mobile Forensics）、雲端鑑識（Cloud Forensics）及資安鑑識（Cyber Forensics）的異同處（含定義、原理、功能及應用等）。並請舉例及繪圖表說明之。（25 分）

三、近年來全球發生勒索病毒（Ransomware）攻擊事件層出不窮，對各行各業的政府部門及企業組織（營運持續性）攻擊犯罪問題帶來了重大威脅。請問透過資安鑑識及系統性的資安風險管理，並結合 NIST Cybersecurity Framework（如 ISO 27110：2021）的 IPDRR 五大功能應用（識別（Identify）、保護（Protect）、偵測（Detect）、應變（Respond）、復原（Recover）），如何有效地降低勒索病毒及其他資安事件對企業營運的影響，並有能力偵辦該網路犯罪事件，進行事前相關的風險評估、防護措施建立、事中應變策略制定，以及事後的修復與檢討，以提高其營運的持續性與恢復力？並請舉例及繪圖表說明之。（25 分）

四、臺灣近年爆發多起重大個資外洩事件，且是從公部門到民間企業私部門，甚至在海外遭販賣；另根據內政部警政署統計，2022-2023 年（網路）詐欺案，也創下 10 年新高紀錄，專家學者指出，很大一部分是來自於個資外洩事故。請從資安鑑識角色（含事前預警系統+事中反應系統+事後復原系統等），說明如何有效偵查及防制上述個資外洩犯罪事故，並提高其數位證據能力及符合資安鑑識基本原則（CIAC Principles）？請用相關國際資安鑑識標準（如 DEFSOP/ISO 27042/27050 等），並請舉例及繪圖表說明之。（25 分）（CIAC Principle 是指 Consistent, Integrity, Accuracy and Compliance）（ISO/IEC 27050:2018-2021 — Information Technology — Security Techniques — Electronic Discovery）