104年公務人員特種考試警察人員、一般警察人員考試及104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　代號：50860　全一頁

等　　別：三等警察人員考試
類 科 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。

一、請說明下列名詞意涵及使用於何情境：（每小題 5 分，共 25 分）
㈠ SQL Injection
㈡ APT（Advanced Persistent Threat）
㈢滲透測試
㈣弱點掃描（並說明與滲透測試之差別）
㈤分散式阻斷服務攻擊法（Distributed Denial of Service Attack）

二、數位證據之蒐集、處理應掌握那些原則與特性，以強化其證據力，避免辯方律師質疑數位證據已經變造或證明力不足？（25 分）

三、數位證據保全之意義為何？主要的程序為何？其與數位鑑識有何差別？請參考國際標準 ISO27037 加以說明。（25 分）

四、甲機關通報內政部警政署刑事警察局偵查第九大隊（以下簡稱偵九隊），說明發現該機關有部分個人電腦會不定時向特定不明中繼站報到，並發現有重要檔案被傳送出去，懷疑遭到駭客入侵並竊取機關案件資料，主動請偵九隊協助。你受指派擔任此一事件對於該機關進行數位證據蒐集擷取等工作，以便進行後續之鑑識，請問：本案所涉法律為何？你事前（出發前）會做何準備？到現場發現電腦是開機狀態，採證之重點資料項目為何？如何採證以確保所蒐集保存之資料具備數位證據能力？（25 分）