109 年公務人員高等考試三級考試試題

類　　科：資訊處理
科　　目：資訊管理與資通安全
考試時間：2 小時

一、電腦設備和網際網路已成為新興的犯罪工具或媒介，因此，面臨訴訟爭議時，常會涉及數位證據的運用：
㈠何謂數位鑑識？（10 分）
㈡何謂證據同一性？（10 分）
㈢當第一線人員取證檔案做證據時，請列出什麼情境，該檔案是有證據能力的；而什麼情境，該檔案是沒有證據能力的？（5 分）

【解題關鍵】
考題難易》：★★
《破題關鍵》資安管理中數位鑑識基本題，掌握數位證據相關概念即可作答。

【擬答】：
㈠數位鑑識乃是鑑識科學的其中一個分支，主要在利用科學驗證的方式調查數位證據，經由數位證據的還原、擷取、分析等過程，還原事件原貌，以利事件調查，並提供法庭訟訴之依據。數位鑑識的調查結果有非常多元的應用，最常見的用途是當作電子偵查的部分程式，在刑事或民事法庭之上，支援或排除犯罪假設。鑑識也能在企業部門應用，例如公司內部調查或侵入調查(intrusion investigation)（專家們探究某次未授權的網路入侵行動的本質以及影響程度）。

㈡證據同一性，指在法院所呈現的證據即原始得用以證明待證事實的證據，亦即呈現於法院的證據必須未經竄改或刪除。換言之，必須是純淨且無污染，確實用以證明待證事實的原始證據，才符合訴訟法對於證據同一性的要求。如果無法通過證據資格檢驗，當然無法成為認事用法的依據。

㈢證據能力，亦可稱為證據資格，係指得成為證明犯罪事實存在與否之證據資格。基本上，是否具備證據資格須由法院證據調查程序加以判斷。對於已提出接受檢驗的事實資料，進行事實關聯性 (證據能力) 及取得正當性 (證據合法取得) 之檢視，具備證據能力並通過合法性審查者，即為具備證據資格。檔案是有證據能力與沒有證據能力的可能情境如下表：

項次	可能情境	取得證據是否具備證據能力？
1	檔案遭修改，第一線人員取證方式又有瑕疵。	很可能被認定為無證據能力
2	第一線人員取證方式無瑕疵，但取得的是被竄改過的證據 (無論取證人員在取證過程中知情與否)。	
3	檔案未遭竄改，但第一線人員取證方式有瑕疵。	
4	檔案未遭竄改，第一線人員取證方式亦無瑕疵。	基本上會被認定具有證據能力

ref: www.fisc.com.tw

二、電腦系統或網路設備，或多或少都有弱點存在，為防止駭客進行惡意入侵，系統應有相對的防禦工具：
㈠何謂網路型入侵偵測系統？（5 分）
㈡說明網路型入侵偵測系統，其部署位置及運作狀況（可以示意圖表示），並陳述其優缺點。（10 分）

㈢當資訊人員遇到攻擊封包或病毒，於企業內迅速擴散時，未更新的主機不斷的散布攻擊封包，資訊人員必須與時間競爭，其處理方法為何？（10 分）

【解題關鍵】
考題難易》：★★
《破題關鍵》
資安技術基本題，了解 NIDS 部署方式即可推論優缺點；第三小題也只要朝資安應變減災來寫就可以答好。

【擬答】：

㈠網路型入侵偵測系統（Network IDS,NIDS）以原始網路封包作為資料來源，它通常運用網路卡於雜亂模式（Promiscuous mode）來偵測及分析所有過往的網路通訊。 當偵測到駭客行為時，NIDS 可採多種反應方式應對，各家產品有不同的應對方式，通常都有提供通知管理者、切斷連線或記錄入侵資料作為事後稽核鑑識的證據等。

㈡*1.* NIDS 作為網路之間或網路組成部分之間的獨立的硬體裝置，部署網路主幹道上，因此所有進入網路主幹道的傳輸都要通過它，可對過往包裹進行深層檢查，然後確定是否放行。

2. 網路型入侵偵測系統的優點

A.成本較低

B.可偵測到主機型入侵偵測系統偵測不到的

C.駭客消除入侵證據較困難

D.可偵測到未成功或惡意的入侵攻擊

E.與作業系統無關

3. 網路型入侵偵測系統的缺點

A.若網路的型態過大，NIDS 往往會遺失掉許多封包，無法完全監控網路上所有流通的封包數。

B.若要擷取大型網路上的流量並分析，需要更有效率的 CPU 處理速度，以及更大的記憶體空間。

C.如果封包是已經加密過的，NIDS 就無法調查其中的內容。

D.NIDS 無法偵測是哪一個使用者正在使用該主機。

㈢此時應該依據事先訂定的資安應變計畫進行減災處理，包括下列措施

1. 攻擊發生第一時間，要能快速減緩並將損害降到最低，因此資管人員應制定應變計劃。緊急應變措施包含立即暫停帳號及其網路存取權限，並檢查該帳號權限可寫入的共享資料夾是否遭感染，接著取出硬碟並備份尚未加密的檔案。全面確認整體環境之防毒軟體更新，檢查是否還有潛伏期內之主機。在第一時間就全部隔離，並將有些遇害的伺服器保存下來，作為鑑識之用。

2. 資安事件發生的 1 小時內通報主管機關，評估事件影響等級，以便依據影響等級發布警訊公告，避免災情擴大。

三、何謂儲存型跨站攻擊（Stored Cross-Site Scripting（XSS））/反射型跨站攻擊（Reflected Cross-Site Scripting （XSS）） ?依攻擊者（Attacker）、目標網站（Website）、受害者（User）分別說明出其關係（可以示意圖表示），並描述其攻擊步驟。（25 分）

【解題關鍵】
考題難易》：★★★
《破題關鍵》資訊安全技術進階題，需要了解 XSS 機制與分類才能解出。

【擬答】：

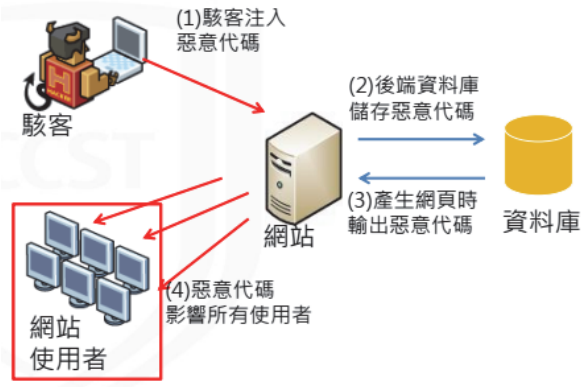
跨網站指令碼（Cross-site scripting， XSS）是一種網站應用程式的安全漏洞攻擊，是代碼注入的一種。它允許惡意使用者將程式碼注入到網頁上，其他使用者在觀看網頁時就會受到影

響。

㈠儲存式(Stored XSS)

藉由伺服器與使用者的互動，攻擊者寫了一段 JavaScript 代碼存入伺服器的後端資料庫，且伺服器沒有正確進行過濾輸出，就會造成瀏覽這個頁面的用戶執行這段 JavaScript 代碼。如下圖所示為其攻擊步驟：

1. 駭客藉由顧客互動過程注入惡意代碼。
2. 後端資料庫沒有正確進行過濾輸出，儲存此惡意代碼。
3. 後端資料庫產生網頁時輸出惡意代碼。
4. 網站使用者接收惡意代碼受到影響。

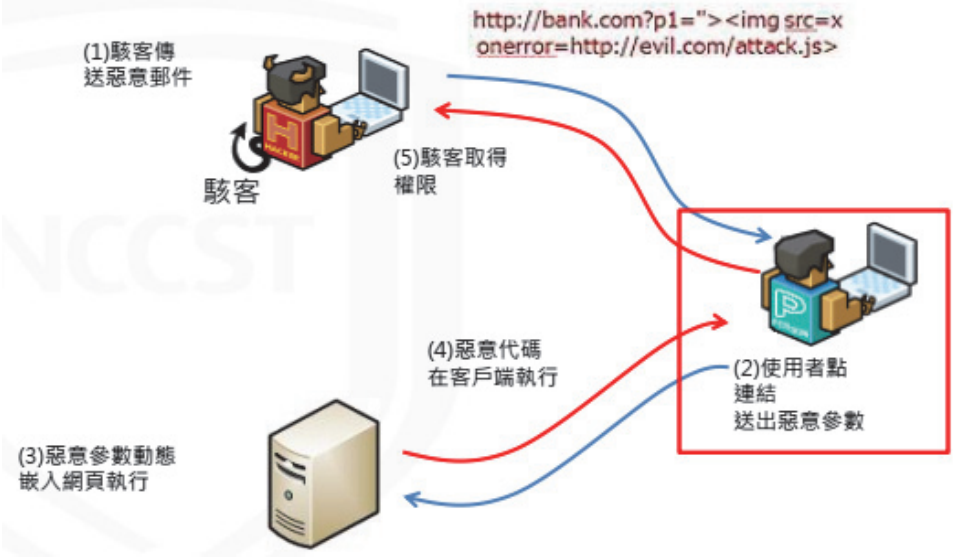


ref:技服中心107 安全資訊系統開發訓練研討會教材

㈡反射式(Reflected XSS)

一般來說這種類型的 XSS，需要攻擊者提前構造一個含有惡意腳本之連結，來誘使客戶點擊，如下圖所示為其攻擊步驟：

1. 駭客傳送含有惡意腳本連結之惡意郵件。
2. 使用者點選後送出惡意參數。
3. 惡意參數動態嵌入網頁執行。
4. 受害者電腦執行惡意代碼。
5. 駭客取得受害者電腦控制權限。



ref:技服中心107 安全資訊系統開發訓練研討會教材

四、專家系統（Expert System）是一種在特定領域內，具有專家水平解決問題能力的程式系統：

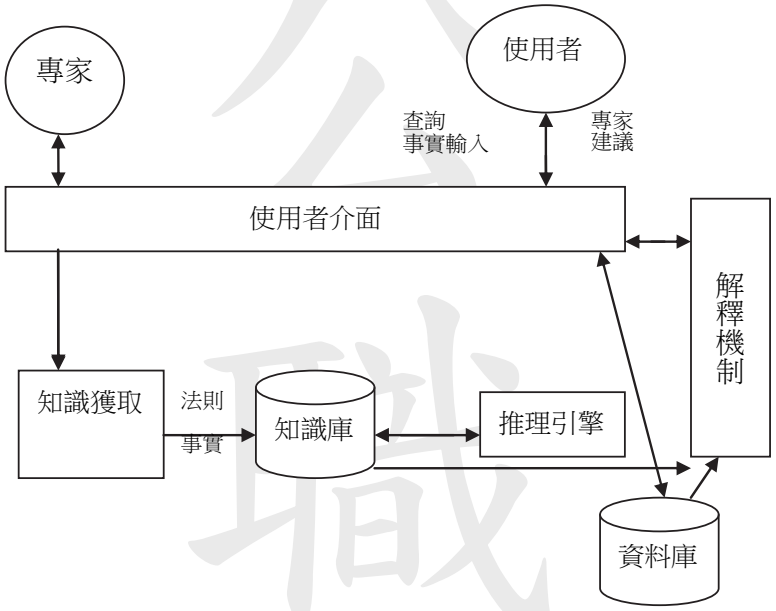
㈠專家系統主要由 6 個部分構成，請說明該 6 個部分之關係（可以示意圖表示），並描述各部分之功能。（20 分）

㈡說明專家系統和人工智慧的關係。（5 分）

【解題關鍵】
考題難易》：★★
《破題關鍵》專家系統古老題，但其結構參考較為古老的寫法，可從林東清專家系統架構調整推出。

【擬答】：

㈠專家系統的基本結構如圖所示，其中箭頭方向為資料流動的方向。專家系統通常由使用者介面、知識庫、推理引擎、解釋機制、資料庫、知識獲取等 6 個部分構成。



1. 知識庫用來存放專家提供的知識。專家系統的問題求解過程是通過知識庫中的知識來模擬專家的思維方式的，因此，知識庫是專家系統質量是否優越的關鍵所在，即知識庫中知識的質量和數量決定著專家系統的質量水平。一般來說，專家系統中的知識庫與專家系統程式是相互獨立的，用戶可以通過改變、完善知識庫中的知識內容來提高專家系統的性能。人工智慧中的知識表示形式有產生式、框架、語義網路等，而在專家系統中運用得較為普遍的知識是產生式規則。產生式規則以 IF…THEN…的形式出現，就像 BASIC 等編程語言里的條件語句一樣，IF 後面跟的是條件（前件），THEN 後面的是結論（後件），條件與結論均可以通過邏輯運算 AND、OR、NOT 進行複合。在這裡，產生式規則的理解非常簡單：如果前提條件得到滿足，就產生相應的動作或結論。
2. 推理引擎針對當前問題的條件或已知信息，反覆匹配知識庫中的規則，獲得新的結論，以得到問題求解結果。在這裡，推理方式可以有正向和反向推理兩種。正向推理是從前件匹配到結論，反向推理則先假設一個結論成立，看它的條件有沒有得到滿足。由此可見，推理機就如同專家解決問題的思維方式，知識庫就是通過推理機來實現其價值的。
3. 使用者介面是系統與用戶進行交流時的界面。通過該界面，用戶輸入基本信息、回答系統提出的相關問題，並輸出推理結果及相關的解釋等。
4. 資料庫專門用於存儲推理過程中所需的原始數據、中間結果和最終結論，往往是作為暫時的存儲區。解釋器能夠根據用戶的提問，對結論、求解過程做出說明，因而使專家系統更具有人情味。
5. 知識獲取是專家系統知識庫是否優越的關鍵，也是專家系統設計的“瓶頸”問題，通過知識

獲取，可以擴充和修改知識庫中的內容，也可以實現自動學習功能。

6.解釋機制用於解釋推理過程與推理結果間的因果關係。

㈡專家系統是早期人工智慧的一個重要分支，它可以看作是一類具有專門知識和經驗的計算機智能程序系統，一般採用人工智慧中的知識表示和知識推理技術來模擬通常由領域專家才能解決的複雜問題。