作業系統、軟體及資訊安全

範圍：上冊第 9-10 及 3 章

座號：姓名：

一、作業系統分類

種類	特性	GUI
	一個使用者每次只執行1個程式	
	一個使用者可同時執行1至多個程式	
	一個以上使用者可同時執行多個程式	

二、常見作業系統：

1.MS-DOS、2.UNIX、3.iOS、4.Linux、5.Windows Server、6.Android、7.Chrome OS、8.Windows Phone、9.Windows7、10.Mac OS、11.Red Hat、12.Mac OS Server、Windows10

平台	常見作業系統
微電腦作業系統	
行動作業系統	
網路作業系統	

三、Windows 作業系統特色：

特色	說明
	使用者可同時執行多個程式
	以簡單的圖案代表程式、檔案等物件，方便使用者操作電腦。
	自動辨識並安裝支援硬體的驅動程式
	利用剪貼簿於不同軟體間交換資料
	不同程式所建立的物件能夠相互使用，可省去使用者在各個程式中切換的麻煩，如在Word中，匯入Excel圖表，即可直接在Word中編輯該圖表。
多點觸控(7以上)、動態磚、跨平台(10)	

四、影響資訊安全的因素：

1. _____：包含有意外災害、人為疏失、軟硬體設備故障等。
2. _____：泛指各種電腦犯罪的行為，如散播電腦病毒、駭客入侵等，是最難預防的資訊安全威脅。

五、電腦病毒、惡意軟體與駭客攻擊：

類型	說明	實例
	1. 隱藏在**磁碟啟動磁**區（Boot Sector） 2. 會修改磁片的**檔案配置表**（FAT）或硬碟分割表 3. 若以中毒磁碟開機，病毒程式會比作業系統更早進入記憶體（RAM），取得磁碟控制權，感染其他磁片或硬碟。	米開朗基羅
	1. 隱藏在**可執行檔案中**（附檔名為 com 或 exe），依傳染方式不同，分成非常駐型及常駐型 2 種。 2. 當含有檔案型病毒的程式執行時，非常駐型病毒會嘗試去傳染給一個或多個檔案，而常駐型病毒則會「常駐」在記憶體（RAM）中感染其他可執行檔。	13 號星期五、兩隻老虎
	1. 以 VBA（Visual Basic Application）語言所寫成的巨集程式。 2. 隱藏在 **Word（.doc）、Excel（.xls）**等應用軟體的文件檔案中。	台灣 NO.1’釣魚台
	1. 此類病毒或後門程式常隱藏於網頁、電子郵件中。 2. 常利用網路（E-mail、FTP）為傳染媒介。	梅麗莎、紅色警戒
隨身碟病毒（USB 蠕蟲）	1. 利用系統自動播放 USB 隨身碟的功能來傳播，蠕蟲程式自己設定於 Autorun.inf 檔中，以便隨身碟插上電腦就可以自動被執行。 2. 中毒的特徵如隨身碟點兩下無法開啟、用檔案總管才可開啟、或是隨身碟的根目錄中自動產生 Autorun.inf 檔。	

攻擊模式：

類型	說明
特洛伊木馬（網頁掛馬）	通常會在免費軟體中加入一些特殊指令，使用者下載使用時，啟動這些特殊指令，而執行了一些未經授權的作業，造成重要資料被竊取、串改或開啟後門程式。
	在合法的程式中加上一些特殊的程式，它們被設計成隨時或在某個特定的時刻，執行特定的程式引發破壞的動作。
	某些有心人士對一些網路伺服器發送大量服務請求封包，進而讓伺服器無法有效處理這些請求而當機，使得伺服器無法運作而造成損失。
電腦蟑螂	專門在網路上登記知名企業的名稱做為網址，然後再以高價向企業兜售的人。
義大利臘腸式犯罪	非法入侵更改程式，從大批交易或多人的帳戶中竊取微小的金額到特定的帳戶中，積少成多。

類型	說明
	首先取得攻擊目標的背景資訊，利用社交手腕取得被害人信任，再向受害人要求某一些資訊，利用這些資訊向其他人員欺騙，不斷重複這些步驟，以達到最後目標。（常見的詐騙與攻擊手法相當多元，包括：假冒為同事；假冒新進員工；假冒廠商、客戶或政府單位；假冒具有權威的人；假冒系統廠商，表示欲提供系統修補程式或更新程式；假冒好心人士，告訴對方如果電腦發生問題可以找他，然後製造問題，讓受害人打電話來求援…等。）
	利用偽造電子郵件與網站做為誘餌，並且使用社交工程方式騙取使用者洩漏重要資料，例如：銀行帳號密碼、信用卡號碼等個人機密資料。
網址嫁接	駭客將試用者原本要連接的網站重新導引至一個看似相同的網站，誘騙人們將使用者名稱及密碼輸到偽造網站的資料庫中。
	利用軟體本身的安全漏洞進行攻擊，因為駭客是趕在軟體業者修護漏洞前發動攻擊，所以稱之零時差攻擊。
BotNet 攻擊（殭屍網路）	顧名思義受害電腦一旦被植入可遠端操控該電腦的惡意程式，即會像傀儡一般任人擺佈執行各種惡意行為，當一部電腦成為傀儡網路 Botnet 的一部份時，意味著 Bot 操縱者可將募集到的龐大網路軍團當作機器人來遠端遙控，從事各種非法入侵近年來尤以藉著「網頁掛馬」（入侵合法網頁植入惡意連結）進行資料竊取危害甚遽。瀏覽網頁者在無法察覺的情況下，連線到殭屍網路背景植入間諜軟體等載惡意程式，並從此成為殭屍網路的一員，繼續壯大殭屍網路軍團。 Bot 殭屍網路是網路犯罪者最常使用來從事詐欺與竊盜的主要管道，除此之外，Bot 網路還可用於針對商業網站發動聯合攻擊，讓這些網站無法使用。由於感染殭屍病毒多數沒有徵兆，一般受害者通常並不知道電腦已經遭受遠端控制。
	攻擊者入侵網站伺服器並植入惡意網頁程式，讓使用者瀏覽網頁時受到不同程度的影響
	將攻擊資料庫的指令藏於查詢命令 SQL 中，以便入侵資料庫系統
	駭客入侵他人電腦，將受害者電腦中的所有檔案加密，並威脅受害者於期限內交付贖金才解密，否則所有檔案將無法解密。
	常被設計成一個有用的小程式（如產生密碼的程式），但卻會在暗地裡竊取使用者的個人資料，或是妨礙使用者操作，如彈出廣告視窗。

六、資料加/解密技術

1. 秘密鑰匙密碼術：**對稱性密碼術**，使用相同鑰匙加密及解密（DES）。
2. 公開鑰匙密碼術：**非對稱性密碼術**，具公開鑰匙和私人鑰匙（RSA）。

（1） _____：傳送端以「傳送端私人鑰匙」加密，接收端以「傳送端公開鑰匙」解密，可確定資料由傳送端發出。

（2） _____：非對稱性密碼術，傳送端以「接收端公開鑰匙」加密，接收端以「接收端私

人鑰匙」解密，確保只有接收方才可看到完整資料。

七、睡眠、休眠與關機

種類		
意義	電腦暫時停止運作，資料仍存放在記憶體中，僅保留記憶體電力，關閉螢幕及硬碟電源	將記憶體中的資料儲存至硬碟，再關閉電腦的電源
省電程度		

八、Windows 使用者帳戶的權限：

帳戶類型	設定工作環境	新增/移除硬體	安裝軟體	建立或刪除帳戶	變更帳戶名稱/類型	建立、變更或移除自己帳戶的密碼	存取其他帳戶的資料
系統管理員							
標準使用者							
來賓							

九、管理及維護磁碟的工具：

名稱	說明
	將分散在許多磁區的檔案資料儲存於連續磁區，加快磁碟存取速度
	清除不需長期保存的檔案，如資源回收筒的檔案、Windows 暫存檔、網際網路暫存檔（Temporary Internet File）、不必要的程式檔等
	檢查磁碟中的磁區是否損毀，若找出損毀部分會自動修復
	包含製作備份及系統還原程式，備份程式可備份資料到另一個儲存媒體或區域網路中的其它電腦；系統還原程式可將電腦還原到先前運作正常的狀態

十、Windows、Linux 及 Mac OS 所支援的檔案系統

作業系統	Windows	Linux	Mac OS
檔案系統			