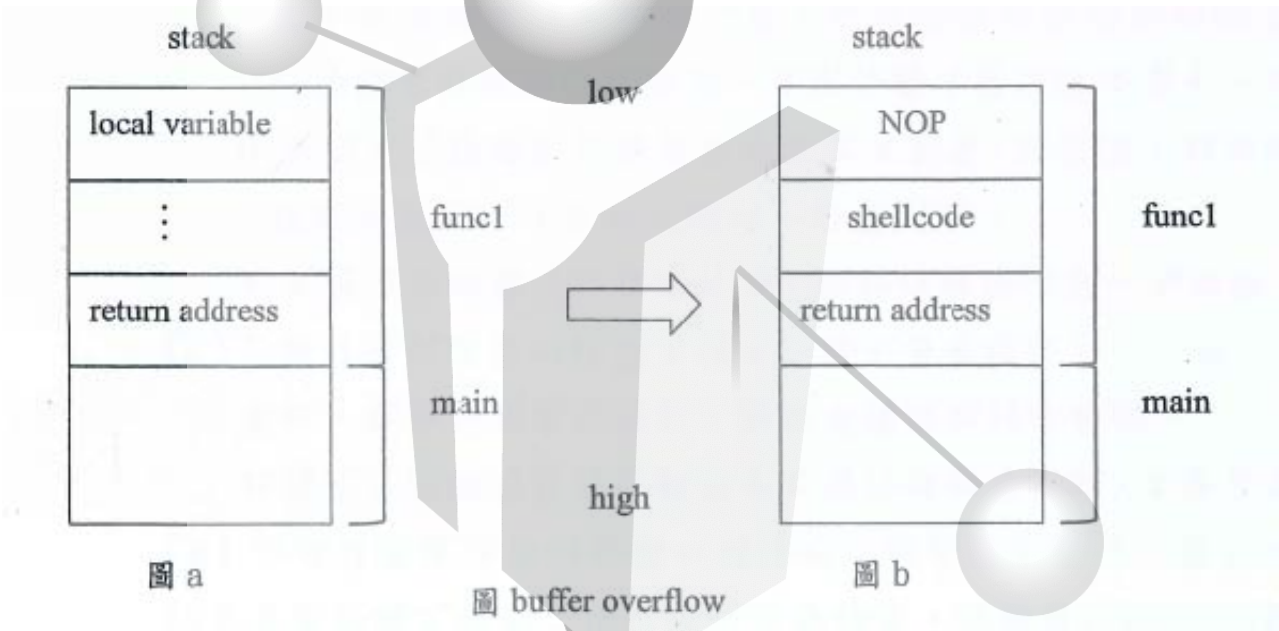
《資通安全》

一、在資訊安全領域，buffer overflow 是駭客常用的攻擊手法之一，這通常需要對系統以及反組譯有深入了解，才能找到程式中 buffer overflow 的漏洞並且加以防患。

(一)請敘述何謂 buffer overflow。(5 分)

(二)buffer overflow 依照位置不同又可以分成 stack overflow 和 heap overflow，請參考下圖來解釋 stack overflow 的運作原理。(5 分)



(三)承上題，圖 b 中的 NOP 指令在組合語言中代表 no operation，代表沒有執行任何動作，請問對攻擊者而言為何要加入 NOP 呢？(5 分)

(四)現在各種作業系統、編譯器(compiler)以及函式庫(library)已經有防禦 buffer overflow 的機制，請以 stack overflow 為例，提出三種程式設計師可以避免及防禦方式。(15 分)

試題評析	爲資訊安全攻擊方法之緩衝區溢位，考題相當靈活，可由講義內容切入。
考點命中	《高點資通安全總複習講義》第一回，張又中編撰，頁 1-22。

【擬答】

(一)針對程式設計缺陷，向程式緩衝區寫入使之溢出的內容(通常是超過緩衝區能保存的最大資料量)，使其出現異常操作，從而破壞程式運作並取得程式至系統控制權。

(二)在 func1 中造成緩衝區溢位，return address 會被修改爲指向 NOP 或是 shellcode 起始 address。

(三)如此一來，return address 不需精確的指向 shellcode 起始 address，僅需指向任一 NOP 指令 address，最後也會執行 shellcode。

(四)防禦方式有：

1.檢查寫入資料長度。

2.利用軟體工具分析程式原始碼，檢查其是否有緩衝區溢位漏洞。

3.Stackguard

爲編譯器工具，因緩衝區溢出攻擊通常會改寫函數返回位址，其產生一個 Canary 值(通常爲 NULL(0x00)、CR(0x0d)、LF(0x0a)、EOF(0xff)或亂數)置於返回位址前，如 Canary 值被改變，即可能遭受緩衝區溢出攻擊。

二、近年來網安事件頻傳，駭客攻擊手法也層出不窮令人防不勝防，資安人員須深入探討與了解駭客常用的攻擊手法，以增加應對防護的能力。

(一)Distributed Denial of Service（DDoS，分散式阻斷服務攻擊）於10年前已有多次攻擊之案例，然目前仍是駭客攻擊時常用的攻擊手法。請描述 DNS Amplification Attack（DNS放大攻擊）如何被使用在DDoS攻擊上。(10分)

(二)Watering Hole Attack（水坑攻擊）及Zero Day Attack（零時差攻擊）為駭客常使用的手法，請描述上列兩項手法的原理。(10分)

(三)韓國於2013年5月遭受到進階持續性滲透攻擊（Advanced Persistent Threat, APT)，造成多家銀行、電視台無法提供正常服務。請解釋何為進階持續性滲透攻擊，並請解釋 APT攻擊和一般攻擊的不同。(5分)

試題評析	爲資訊安全攻擊方法典型考題，可由講義內容切入。
考點命中	1.《高點資訊管理與資通安全講義》第三回，張又中編撰，頁3-29~31。 2.《高點資通安全總複習講義》第一回，張又中編撰，頁1-22。

【擬答】

(一)亦稱DNS反射攻擊(DNS Reflection Attack)，攻擊者僞裝受害者IP向開放的DNS伺服器發出DNS查詢請求，讓DNS回應之流量送往受害者主機。以32 Bytes的DNS查詢封包爲例，可產生3296 Bytes的DNS回應封包。

(二)1.水坑攻擊爲攻擊者入侵合法網站，插入一偷渡式(Drive-by)惡意程式，等待被害者造訪該網站時趁機感染、發動攻擊，部分水坑攻擊會結合零時差攻擊。

2.零時差攻擊爲攻擊者利用尚未被公開、修補的弱點來攻擊受害者，弱點標的可能是各類型的作業系統、應用程式、信件軟體與網頁瀏覽器等。

(三)進階持續性滲透攻擊之Advanced指精心策畫的進階攻擊手法，Persistent則是長期、持續性的潛伏。APT攻擊重點在於低調且緩慢，利用各種複雜的工具與手法，逐步掌握目標的人、事、物，不動聲色地竊取其鎖定的資料。根據營運創新資安委員會所提出的策略白皮書，說明APT特色有：

1.資金充裕。
2.高度針對性。
3.擁有資料情報分析能力。
4.具有潛伏並保持低調的技術能力。
5.擁有多樣工具的重面向攻擊方式。

三、一個良好的密碼系統除了進行身分的驗證外更可以增加被破解的困難度，降低密碼遭到解密之風險，請針對密碼系統回答下列之問題：

(一)在進行密碼的破解時，常會使用(1)Brute Force、(2)Dictionary、(3)Rainbow Table及(4)Social Engineering（社交工程）進行破解，請分別描述這四種破解的方法。(20分)

(二)Windows XP所使用的密碼系統為Lan Man Hash（LM Hash)，請說明輸入密碼長度可達14位元的LM Hash為何其密碼強度僅等同於7位元。(5分)

試題評析	爲資訊安全攻擊方法典型考題，可由講義內容切入。
考點命中	《高點資訊管理與資通安全講義》第三回，張又中編撰，頁3-29~31。

【擬答】

(一)1.暴力攻擊法(Brute Force)：藉由合法字元組合不斷的嘗試，直到猜測出正確的密碼爲止。

2.字典攻擊法(Dictionary)：由於一般人在取密碼時，爲記憶所需常會取有意義的單字。因此藉由常用的字彙，不斷地改變組合，一直到破解密碼爲止。

3.彩虹表(Rainbow Table)：建立一個預先計算好的明文與雜湊值對照表，當獲得雜湊值後經過比較、查詢與

運算，可快速破解各類雜湊密碼。

4 社交工程(Social Engineering)：利用人性弱點、人際交往或者互動特性所發展出來的一種攻擊方法。早期社交工程是使用電話或者其他非網路的方式來詢問個人資料，而目前社交工程大都是利用電子郵件、網頁或簡訊來進行攻擊。

(二)Windows 所使用的 LM Hash，由於其將 14 位元的密碼以兩組 7 位元的方式儲存，故其密碼強度僅等同於 7 位元。

四、個人資料保護法已於民國 99 年完成修訂，並於 101 年 10 月 1 日正式上路。其法條無緩衝寬限期，且其適用對象不再侷限於八大民生相關產業，因此個人資料保護法之實施將對各種規模之企業皆造成不小衝擊，企業未遵循個人資料保護法將可能產生商譽、法律、訴訟、財務及停業之風險，甚至將會面臨高達 2 億元之損害賠償，宜加以正視。

(一)何謂個人資料？（4 分）

(二)企業為何要建立個人資料保護機制？（4 分）

(三)企業如何建立個人資料管理保護機制？（4 分）

(四)企業如何建立個人資料安全保護機制？（4 分）

(五)企業如何建立個人資料事件鑑識調查機制？（4 分）

試題評析	可由個人資料保護法、個人資料保護法施行細則思考。
考點命中	《高點資訊管理與資通安全講義》第三回，張又中編撰，頁 3-46 及補充講義。

【擬答】

(一)根據個人資料保護法第 1 條，個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

(二)根據個人資料保護法第 27 條，非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

此外，根據個人資料保護法第 29 條，非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。

(三)根據個人資料保護法施行細則第 12 條，企業應：

1.配置管理之人員及相當資源。

2.界定個人資料之範圍。

3.個人資料之風險評估及管理機制。

4.事故之預防、通報及應變機制。

5.個人資料蒐集、處理及利用之內部管理程序。

(四)根據個人資料保護法施行細則第 12 條，企業應實施：

1.資料安全管理及人員管理。

2.認知宣導及教育訓練。

3.設備安全管理。

(五)根據個人資料保護法施行細則第 12 條，企業應實施：

1.資料安全稽核機制。

2.使用紀錄、軌跡資料及證據保存。

3.個人資料安全維護之整體持續改善。