103年公務人員特種考試司法人員、法務部調查局調查人員、國家安全局國家安全情報人員、海岸巡防人員及移民行政人員考試試題

代號：10960　全一張（正面）

考 試 別：司法人員
等　　別：三等考試
類 科 組：檢察事務官電子資訊組
科　　目：資通安全
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、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。

㈠請敘述何謂 buffer overflow。（5 分）

㈡ 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）

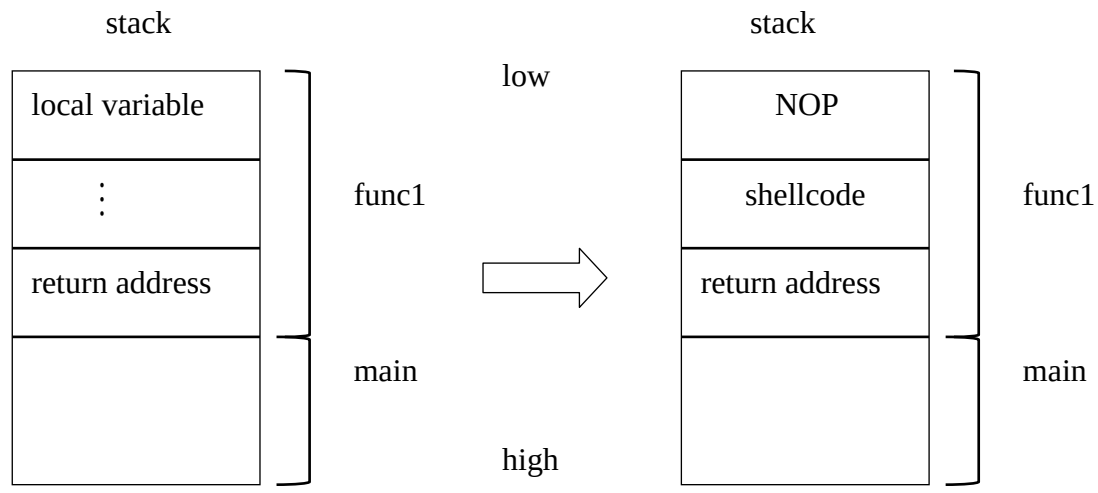

圖 a　　圖 b

圖 buffer overflow

㈢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）

㈣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）

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。

㈠ 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）

㈡ 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）

㈢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）

（請接背面）

103年公務人員特種考試司法人員、法務部調查局調查人員、國家安全局國家安全情報人員、海岸巡防人員及移民行政人員考試試題

代號：10960 全一張（背面）

考 試 別：司法人員
等　　別：三等考試
類 科 組：檢察事務官電子資訊組
科　　目：資通安全

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：
㈠在進行密碼的破解時，常會使用⑴Brute Force、⑵Dictionary、⑶Rainbow Table 及⑷Social Engineering（社交工程）進行破解，請分別描述這四種破解的方法。（20 分）
㈡ 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）

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。
㈠何謂個人資料？（4 分）
㈡企業為何要建立個人資料保護機制？（4 分）
㈢企業如何建立個人資料管理保護機制？（4 分）
㈣企業如何建立個人資料安全保護機制？（4 分）
㈤企業如何建立個人資料事件鑑識調查機制？（4 分）