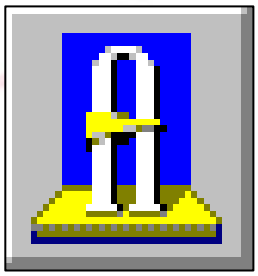
題組十　參考答案

又到了報稅的日子，隨著電腦科技的進步，報稅的方式也從傳統的表格到網路申請認證申報，尤其今年國稅局更在各媒體上宣導網路申報的好處，製作報稅軟體光碟免費贈送、網路報稅抽獎、配合 HiNet 贈送使用時數等各種方式，就是要吸引民眾使用此管道來完成報稅手續。直至 3 月 31 日止，完成網路報稅的民眾也已突破萬人次，對國稅局而言，此小小的成績算令人欣慰，不過在辦理認證的過程中，程序繁複，造成許多有心配合政府政策的民眾不小的困擾，如：若非 HiNet 的使用者申請認證，得跑中華電信窗口好幾次，既然要跑，乾脆填寫傳統表格算了。還有贈送的光碟中，內附的二維條碼程式所列印出的稅單申報報表，只能在北區國稅局使用，中區及南區不接受此報表格式，真可謂「一局兩制」！筆者雖是個每天活在網路上的人，但也受不了此一擾民程序，決定還是填寫傳統表格報稅，輕鬆完成此一年度大事。

話說在 3 月初報稅的時期，接到網路通訊編輯傳來的一篇傳真，希望筆者能提供些意見，該篇文章是另一名作者所寫有關此次網路報稅安全漏洞的探討，該作者提出一個很有趣的題目，假設有駭客以假 IP 冒用使用者，取得其安全憑證資料，那駭客真的是有如取得銀行金庫鑰匙，可以為所欲為。當然使用此一方式，需要天時、地利、人和的配合，再加上駭客高超的技術，缺一不可，但並非人人皆有此能力可以截取到資料，因此筆者親自上網申請認證，在申請憑證的過程中，原想使用假 IP 攻擊法來試試，但此行為卻會觸犯法律範圍（別因小小的好奇而讓您深陷囹圄，畢竟 Hacker 與 Cracker 只有一線之隔），所以只能以正常程序申請，填寫各項資料，同時監控資料封包，這時發現了一個從以前就存在的有趣議題，只是許多人會忽略了它，所以在此提出與各位共同來討論。



民眾使用網路報稅的上網環境不外乎，在家中使用電話撥接至 ISP，然後連至 GCA 認證中心的網址，此外就是使用公司或公眾區域網路，上線申請。現在我們假設一位守法納稅的民眾（我們就稱他為小張），在公司透過區域網路連上 Internet，到 GCA 認證中心的網頁填寫資料，看看其取得憑證鑰匙的過程中會有什麼狀況。

讓我們回到現實世界，Sniffer 原本是協助網管人員或程式設計師，分析封包資料，解決網路 Traffic 問題的軟體，但用在駭客手中，卻成為最佳入侵工具。如 Dan Farmer 與 Wietse Venema 所設計之 SATAN 軟體，可以掃瞄電腦系統與網路的安全漏洞，發現可能遭人入侵的途徑，網管人員可以防堵此一安全弱點，不過對駭客而言，它是個能搜集偵查目標系統資料，用準備計畫來進行入侵的理想軟

體。如果今天您有 Sniffer 類的軟體，只要您鎖定特定的 IP 位址及所要 Listen 的封包格式，然後像漁夫般的撒網出去，等待鎖定的目標完成整個填表註冊動作後，您就可以收網截取到這頁表格的資料。

檔案名稱	組成	組織	說明
學員基本資料檔	學號+姓名+班別+學業成績+群育成績+德育成績	按學號遞增順序排序	（無）
別名			備註
學籍檔			

此外驗證身分過程還可透過 HiNet 來進行，也就是說若您是 HiNet 的使用者，那麼在填了帳號與密碼，GCA 中心就會和 HiNet 連線，進行您的身分確認，在一個工作天後，便會以 E-Mail 通知您是否通過身分檢查，如此您就不用跑到中華電信窗口辦理身分驗證。雖然這是便民的措施，但好玩的漏洞就在這兒，您也可以看到 HiNet 的撥接識別碼變數 isp_name 為 abcdefg，密碼 isp_passwd 為 yesismee，電子郵件位址 E-Mail 為 abcdefg@ms9.hinet.net，而這些封包資料，透過網路傳送給 GCA 認證中心的過程，很有可能會被有心人士從中截取，然後駭客就很高興的用您的 HiNet 帳號與密碼，準備下次的入侵行動，哪天您突然發現您 HiNet 的帳單費用高的離譜，這可不是 HiNet 記錯帳喔！或者調查局要求您到案說明，為何您的網路帳號侵入某家銀行系統，造成嚴重破壞，這時您才發現，原來您的網路鑰匙已被人複製一份了。

那若是在家中使用撥接的用戶上線申請，是否也會遭到竊聽？理論上若您使用 Modem 撥接到 ISP 的 Terminal Server，那別擔心會受其他也是撥接用戶的監視，因為 Terminal Server 會過濾不該傳出的封包，但從 ISP 到 GCA 認證中心這段的線路，可就不一定囉！假若有人是從 ISP 或 GCA 認證中心的網路下手，突破安全系統，潛伏在這兩段網路節點中攔截，資料同樣的也會落到他人口袋，因此，還是「小心能駛萬年船」。