

## CEH 駭客剋星課程與認證介紹

隨著網路的普及化，很多企業除運用電腦網路作資料、文件等傳輸及處理外，電子商務 (e-Commerce) 更推行得如火如荼，讓現行的商業行為打破了時間及地域的限制。但在帶給我們方便的同時，卻隱藏一些危機。一直以來，企業及個人所使用的電腦一直受病毒威脅所困擾，而這些病毒的傳染途徑，除了 email 以外，還可能透過網頁和其他的方式傳送，令人防不勝防。除此之外，駭客的入侵也日益嚴重，面對巨大威脅，但台灣目前各企業所投資於資訊安全不少的資源，依然嚴重不足。

### ■ 駭客人數急速增加

所謂駭客攻擊是一種針對資訊系統的防禦和保護，所採取的有系統之智慧型攻擊行為，值得注意的是這種智慧型行為是經過深思熟慮的，而攻擊廣泛而言可以分為積極/破壞型(active)與消極/非破壞型(passive)，兩者主要的差異在前者會破壞系統或是系統內的資料。而後者只是竊聽系統或竊取系統內資料的內容，並不會更動系統及其內容。不少駭客入侵別人的電腦網路可能只是「好玩」，但是有些駭客則以盜取商業和個人的機密資訊以獲得利益。

以往我們以為，駭客人數不多，因為需要很深奧高超的技術才能擔任駭客，但隨著駭客工具及軟體的日益增加，駭客不再需要高深的技術就可以具有一定的功力，能夠入侵網站及系統，而這些工具都可以在駭客家族的網站找到，這些駭客會彼此交換工具、經驗及展示自己的成果。

### ■ 瞭解駭客手法堵塞漏洞

談及駭客攻擊的手法，以下簡單地介紹一個範例。駭客規劃攻擊的流程很簡單，先從網頁、或資料庫入侵系統，而後埋入後門或從事遠端遙控。

駭客首先針對目標機，使用工具找出漏洞，並決定是否對該漏洞立即從事攻擊行為。攻擊成功後，取得低階的權限。在低階權限下，即可取得資料、複製資料、或埋入後門、遠端遙控。但駭客並不會就此滿足。欲取得更高的使用權限，以利從事更多的動作。此時駭客可能利用某些特定工具的缺陷，攻擊目標機之後，將低階權限轉換成最高權限。成功進入後，駭客得在目標機電腦上加入一個新的使用者，並將該使用者設定在擁有最高權限的群組，即系統管理員。如此一來，該

台電腦便擁有兩名最高權限的使用者，一是原來的 Administrator，另一是駭客設定的使用者。擁有最高權限後，駭客可以埋入更多更好的後門，使駭客能更容易利用這台電腦。

駭客成功入侵電腦之後，下一個目標可能是想辦法取得密碼檔。一般密碼檔無法取得，但藉由同時利用三種工具，可以找到密碼檔。經過編碼的密碼檔，亦可藉由不同的工具，一一破解。此時就需要注意，如果密碼設得太簡單，很快就會被破解。例如 Administrator 密碼設為 admin、或使用者名稱與密碼相同，僅需要 0 秒，即可破解密碼。如果密碼較為複雜，但位數不多，仍然可以被解出來。例如密碼 123456，約需 15 分鐘；而六位數以下的密碼，不論字母或數字，皆可在 1 小時內破解。因此建議在 window 底下，密碼至少要選擇八位數以上。只要擁有帳號與密碼，駭客就可以從事遠端遙控的動作。目前遠端遙控的軟體很多，功能亦很強。例如有的軟體，可以將所有鍵盤輸入的內容做紀錄，或可以用螢幕側錄的方式，紀錄電腦的一舉一動。

## ■ 駭客剋星(Ethical hacking) 的誕生

究竟怎樣才可以對付「駭客」？所謂「知己知彼，百戰百勝」，要保護網絡安全，免受駭客入侵，你需要進入他們的思想世界：先成為他們一份子，了解其犯罪途徑和技巧，明白他們的入侵過程，設法尋找及堵塞網絡的漏洞，作出相應的防禦措施，並改善企業的網絡安全問題。有見及此，Informatics 與美國 EC Council 特設的 Certified Ethical Hacker (CEH) 課程，教授駭客所應用的知識和技術，從而防止駭客的入侵。

要防護上面所舉例之駭客攻擊情況發生，可以藉由觀察電腦的埠來發現。了解竟經常掃瞄自己電腦常用的埠號(port)，若出現陌生的埠號在使用，即可能已被建立後門。或利用程式命令，了解各埠號是由誰開啟的，若出現陌生人開啟的埠號，亦得是發現駭客入侵的警訊。

## ■ 國際電子商務協會 (EC-COUNCIL)

國際電子商務協會 (EC-COUNCIL) 是一個世界性的專業組織，總會設在美國紐約，擁有許多會員以及遍佈全世界的聯會。在九十三年七月九日正式登陸台灣與國人見面。對於台灣人民而言，國際電子商務協會 (EC-COUNCIL) 是個新的名詞，但對全世界其他國家資訊安全好手及電子商務領域專家而言，這是一個代表專業與榮譽的名詞。

EC-Council 全稱為 International Council of E-Commerce Consultants，是一家以會員制為基礎的專業機構，會員主要來自哈佛大學、紐約市立大學、加利福尼亞大學、澳洲昆士蘭中央大學等大學教授及講師，以及從事電子商務的企業界人士，如來自 Microsoft, IBM, SONY, Cisco 等國際著名機構的代表所組成。EC-Council 成立的宗旨及目的，是支援和加強在設計、建立、管理、推廣電子商務事業上發展的個人及組織機構的機能，並提供電子商務專業認證，教育，技術等，在互信互利的原則上提供自由討論、交流信息的平台。

EC-Council 的課程及證照已經獲得全世界許多著名公司及團體的認同、諸如 Canon(佳能)、HP(惠普)、SONY(新力)、Kodak(柯達)、US Air Force Reserve(美國空軍)、US Military(美國軍方)、FBI (國家聯邦調查局)、CIA(美國國家情報局)、US Army(美國陸軍)等等，有些已經成為其人員訓練課程的一部份。

目前 EC-Council 提供的認證種類有 CEA、CEP、CEC、CEH、CHFI 等級，其中 CEA、CEP、CEC 三類認證為電子商務資訊管理類的認證，而 CEH 與 CHFI 為駭客防護領域的認證。CEA 認證與教育課程包含電子商務安全、無線網路安全、網路安全設計、Linux 安全、顧客關係管理(CRM)、供應鏈管理(SCM)……等共十一科目，EC-Council 所提供課程與其他公司產品不同之處在於 EC-Council 的課程很完整的從觀念引導、規劃、建置到風險評估有系列的整理陳述，不偏重於特定公司之特定產品，完全技術整合與中立，可說是目前電子商務領域最完整的教材。

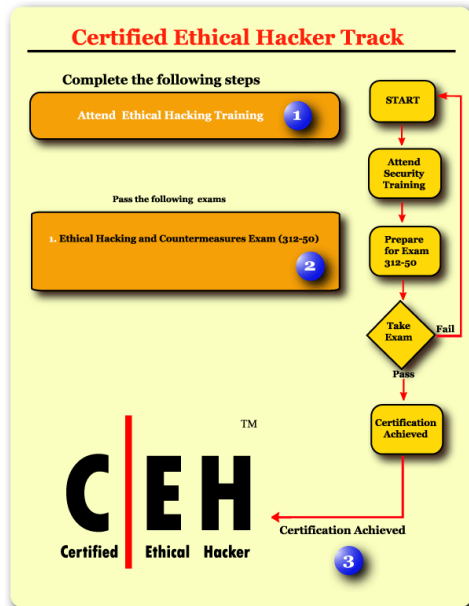
CEH 與 CHFI 目前為美國 FBI 機構訓練人才的認證與教育課程，在台灣已做為軍方單位、金融票券業、資訊網路公司等重視資訊安全公司的人員訓練課程，目前全世界已經超過 3000 人取得 CEH 證照，而台灣已經超過 30 位駭客高手取得 CEH 證照，CEH 證照同時也是近年來在資訊安全領域中成長最快的資訊安全證照。

## ■ CEH 課程內容

CEH 課程內容從特洛伊木馬及開後門(Trojans and Backdoors)、資訊攔截(Session Hijacking)，到目前最嚴重的病毒及資料庫入侵(SQL Injection)，共包括 20 個模組，都有完整的介紹，且原廠教材中所附光碟中還提供所收集的三百多個駭客工具。課程內容除了有關資訊安全等的理論和概念外，更有大量的實例和示範，透過 CEH 專業講師，都是多年資安相關工作經驗的高手，來教導及介紹這些駭客常用的工具、方法，藉以實際了解駭客行為，進而知道如何保護網路、

系統免受攻擊。透過互動、實務操作中教導學生如何掃描及測試自己系統的安全漏洞藉以保護系統安全，並將加強實際的上機操作以針對系統安全有更深一層的了解，藉由上課所模擬的網路環境中了解駭客如何掃描並攻擊網路系統，學生也將學到如何制定策略、權限以防堵不法駭客的入侵。

這樣有趣的課程，究竟適合甚麼人來進修呢？個人認為除了政府機關或企業組織中的系統網路管理員、資安技術員、稽核員、資安專業人員外，任何對網路安全有興趣的人士均適合研讀。



學員需修畢所有學科，並通過 Prometric 所舉辦的線上考試，一共 125 題，70% 通過才能取得 CEH 證書，資歷亦獲美國 The International of Electronic Commerce Consultant 承認。

## ■ 總結

許多企業及組織，都以為買了防火牆和防毒軟體就萬無一失了，但事實上，SoftEther 以及 NC、Hopster、HttpTunnel 等軟體工具都可以穿越現有防火牆。這些軟體皆可利用 Tunnel 或 Proxy 的方式穿越防火牆，突破防火牆的限制。此外像是資料庫入侵(SQL Injection)的問題，也不是防火牆可以擋掉的，唯有深入瞭解系統的弱點，才能防護系統，而這點就從 CEH 駭客防護課程開始吧。