國立聯合大學教育部高等教育深耕計畫

活動成果集錦

活 動 名 稱	基於了解駭客攻擊手法及思路的網路安全防禦方式
活 動 時 間	109 年 10 月 23 日
執 行 單 位	資訊管理學系

活動內容

隨著資通訊科技日益蓬勃發展，如何提供安全、安心、可靠的網際網路使用環境，創新資安服務價值，已成為邁向優質網路社會的關鍵議題。無論是人文社會或經濟環境的發展，都必然受到資通訊技術與應用的影響。因此本活動以『資訊通訊安全與資訊安全』為主軸，辦理產業資源交流工作坊。活動內容涵蓋『資訊通訊安全』與『資訊安全』的理論與方法，希望能夠讓學生深入體會資通訊技術與應用在產業面的實務觀點。

駭客，主要來自英文字「hacker」的翻譯，起初指的是一群熱衷於寫程式的人。這些人認為資訊應該是共享的，因此藉由撰寫一些自由軟體來促進資訊的流通，並將專業分享給他人。因此原先的駭客，指的是一群具有駭客倫理的人。而今日的「駭客」所帶有的負面意涵，主要是來自「cracker」，稱為破網者，或鬼客。主要指的是一群未經許可便透過網路擅入電腦系統並竊取電腦內部資料的人，他們有著超乎一般人的入侵技巧，從事破壞人或機關團體的網路資訊系統的行為。

因此駭客跟鬼客是兩種不同的人，不過在今天一般媒體的使用下，通常以駭客來代表那些從事鬼客工作的人。一般而言，這種入侵他人電腦的行為，不論是否會造成系統的破壞，這種行為的正當性一直都是備受爭議。在法律上，對於這種入侵行為，除非真的觸及法律所規限如隱私權、或智慧財產權的犯罪行為，否則，沒有造成損害的入侵在法律上並未有明確的規範。然而，入侵的行為就如同走在街上亂晃時，挨家挨戶地試著

開啓他人門戶一樣，僅是一種在道德上不見容於社會的行為。

一般而言，鬼客有非常多的攻擊方式是利用網路來攻擊的，如：分散式阻斷服務攻擊（DDOS）、雲端攻擊，甚至也針對網路設備來進行攻擊的中間人攻擊，以及最近針對物聯網設備之漏洞來竊取資料的物聯網攻擊。此外，另一種進階持續性滲透攻擊（APT）是利用各種複雜的工具與手法，相當有耐心的逐步掌握目標的人、事、物，並不動聲色地引誘受害者上當，進而竊取其鎖定的資料。對於這些入侵與攻擊，大多數的防毒軟體或是防火牆皆會阻擋這些惡意軟體和病毒，但這些防火牆並不是 100%都可以偵測到這些入侵與攻擊的，所以電腦、網路設備或是防火牆上面的 Log 就是一個找尋入侵與攻擊很重要的線索，雖然此種偵測的方式沒辦法在第一時間發現並處理情況，但是此種偵測方式可進一步透過 SOC、SIEM 平台去分析防毒軟體或是防火牆所不能阻擋到的威脅和攻擊，以防下次攻擊事件再次發生。

阻斷服務攻擊 (DoS)與分散式阻斷服務攻擊 (DDoS):阻絕服務攻擊(DoS)，主要的目的是由網路遠端的一台攻擊者電腦利用大量的請求封包(Request Packet) 來使目的端主機因無法負荷如此多的請求，而癱瘓其所提供的服務，甚至使其當機，或是利用巨大的傳輸流量來癱瘓目的端主機的網路傳輸，使其無法提供服務。此種攻擊都會搭配 IP Spoofing 使用並且是利用正確的網路封包格式，因此若是攻擊者來自區網外部則很難抓到真正源頭，目前這個部分尚未有效之解決方法，只能根據偵測而來處理，因此在攻擊發生的第一時間，如果能及早發現就能及早處理，否則將造成網路服務中斷；至於若是其來自區網內部，則可透過區域網路設備的控制來定位出攻擊者的位址，加以制止其攻擊的行為。而分散式阻斷服務攻擊(DDoS)則更加恐怖，它聯合多台網路主機一起發動 DoS 攻擊，此種攻擊十分可怕，它可以在瞬間把大型網站的服務頻寬吃掉，如 Yahoo 就曾經遭受攻擊。這類攻擊發動時必須同時號召多部網路主機的完成其攻擊之指令，因此常常會先利用入侵的手法破使網路的主機成為其的魁儡，如:利用殭屍病毒(BotNet)、蠕蟲(Worm)來入侵或者其他電腦病毒如：特洛伊木馬程式等方式來引發群體式的攻擊。

中間人攻擊(MiTM)[11,12]：是一種從中「竊聽」兩端通訊內容的攻擊手法，可能對企業造成重大威脅。由於駭客不僅能從中接收資料，還能從中插入自己的資料，因此企業所傳輸的資料不僅可能外流，更可能遭到竄改。有鑑於企業網路很可能會傳輸一些關鍵的資料，因此 MiTM 攻擊是 IT 人員必須正視的重大真實威脅。

攻擊方式：

IP 欺騙：指帶有假的源 IP 位址，目的是冒充另一個計算系統身份。使發送方可以保持匿名的一種技術是使用代理伺服器。

DNS 欺騙：攻擊者利用提供錯誤的 IP 位址，使得伺服器將 DNS 導向至惡意的網頁。

ARP 欺騙：攻擊者不斷傳送竄改過 MAC 位址的封包給受害電腦，並讓該電腦持續將錯誤的紀錄寫入 ARP 表，此後受害者欲連接至其他電腦時，便會把封包傳至遭竄改後的 MAC 位址，攻擊者則能在此位址截取封包。

Email 挾持：就是所謂的釣魚郵件，攻擊者利用帳密外流的信箱冒充受害者所信任的對象，將人引導至惡意網頁或是誘騙人去下載惡意程式。

SSL 剝離：攻擊者攔截受害者的 HTTPS 請求，再將其轉送到受害者欲連線之伺服器，隨後攻擊者便能收到伺服器的回應並能將其從 HTTPS 降級成 HTTP 再轉傳至受害者，在這之後受害者將會變成在 HTTP 的連線下進行操作。

WiFi 竊聽：公共場所的 WiFi 很多都是未加密的，未加密的連線若是遭人竊聽後，其內容將會以明文的方式洩漏給對方。

攻擊目的：透過冒充身分，使受害者誤認為自己是在與他們所信任的對象進行聯繫，進而偷取對攻擊者有用之帳號及密碼(例如：網路銀行、信用卡卡號等)，將其盜用身分及金錢等。

進階持續性攻擊(APT)[4,8,10]：是一種最近常見的網路攻擊型態，攻擊特色在於低調且緩慢，利用各種複雜的工具與手法，相當有耐心的逐步掌握目標的人、事、物，不動聲色地引誘受害者上當，進而竊取其鎖定的資料。而與社交工程密不可分的原因在於，

通常駭客利用特製的釣魚網站、社交程式或電子郵件當作攻擊的進入點，攻擊的手法除了以電腦入侵方式外，也會透過其他的傳統的手法達到竊取資料的目的(如電話竊聽等)。

攻擊方式：

盜版網站：吸引被害者點進去客製化崁入有惡意程式的盜版網站，標題通常是聳動吸引人的，或者是偽裝成與正牌網站相同的樣式。

惡意社交電子郵件：是 APT 攻擊型態中最常見的手法，駭客會分析被害者的背景和社交取向，訂做看起來就是要寄給您的郵件及附檔，但檔案中暗藏惡意程式。

水坑式攻擊：駭客避開網路環境防禦機制，直接埋伏惡意程式在您常去的網站等待您執行進而受控制。

攻擊目的：盜取被害者之個人資料進行變賣與偽造，另亦可利用被害者帳號盜取更多帳號及資料。

因此，基於上述這麼多的攻擊與入侵的手法，講者說明了要了解駭客攻擊的思路，才能比較了解他所應用的攻擊手法，透過所了解的攻擊方法，才能夠制定安全的網路保護模式，以進行網路安全的防禦。因此，講師從駭客入門開始講起，駭客是如何成為駭客，他們怎們練習當駭客，使用什麼工具如何去練功等等，讓學生了解當駭客也是一件非常辛苦的工作，因此講師認為駭客這個工作，如果要找到等值(辛苦的程度)對等的工作那就是線上遊戲 online game 的工作者，需要 24 小時全天無休，因此非常辛苦。因此既然花了那麼多時間，學習了那麼多技能，那為什麼要當駭客呢？因此講師建議同學們，既然有這樣的技能為什麼不把這些技能用在對的事情上呢? 因此講師建議同學若有興趣學習了駭客的技能，應該將它用於網路保護者的工作，這樣才是更正確的選擇。以下幾點是講師的建議：

1.請當道德駭客-白帽駭客

2.發現弱點需通報

3.不可竊取資料

4.不要攻擊未授權的政府網站

過程中，同學們又發現要當駭客還需要再學習英文、寫程式，而且要有不怕失敗，有耐心的心裡素質，這些都是同學們之前都沒有想過的駭客所需要具備的技能，因此整個過程當同學們都非常專注聽講學習中，毫無冷場，相信這場演講的工作坊同學們必定是收穫滿滿。

喬治·法蘭西斯·霍茲（英語：George Francis Hotz，1989年10月2日－），別號 Geohot，美國知名駭客。2007年8月解鎖蘋果（Apple）iPhone手機，使得iPhone手機不僅僅局限於AT&T網路，也支援其他GSM網路。

目錄 [隱藏]

1 個人介紹
2 解鎖iPhone
3 解鎖PlayStation 3
4 注釋
5 外部連結

喬治·霍茲

個人介紹 [編輯]

喬治·霍茲出生於美國新澤西州（New Jersey）Glen Rock市，2007年畢業於Bergen County Academies，並進入羅徹斯特理工學院（Rochester Institute of Technology，RIT）生物工程專業，學習生物資訊。[1]

2007年，霍茲參加了國際科學與工程大獎賽（Intel International Science and Engineering Fair，簡稱ISEF），他的課題「I want a Holodeck」為他贏得了很多獎項，並獲得2萬美元的獎金。

2011年6月至2012年1月，喬治·霍茲在Facebook公司任職。

圖一、 網路上非常知名的駭客

圖二、駭客常用的遠端入侵的手法

事實上，產業人才的培訓在於養成兼具領域技術專業能力與掌握產業技術趨勢務實人才。透過本活動的舉辦，相信參與的學生們能夠透過理論理解與專案演練，深化在『資

訊通訊安全』與『資訊安全』的產業能力與實務技能。

參考文獻及附錄

[1] Digicertl，病毒、蠕蟲與特洛伊木馬程式的不同，取自 https://reurl.cc/yZ7ry8

[2] iThome，中國出現新的勒索軟體 WannaRen 大規模攻擊，臺灣用戶要小心加以防範，取自 https://reurl.cc/Nj0Y9Q

[3] iThome，Let's Encrypt 因臭蟲而撤銷 300 萬個 TLS 憑證，取自 https://reurl.cc/arVeA7

[4] 陳淑萍，淺談社交工程與 APT 攻擊，取自 http://www.cc.ntu.edu.tw/chinese/epaper/0035/20151220_3504.html

[5] SOC 之介紹，取自 http://blog.tsc-tech.com/?page_id=55

[6] FortiGate Log 資訊，取自 https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-logging-reporting-54/logs.htm

[7] SIEM 相關介紹資訊，取自 https://ithelp.ithome.com.tw/articles/10195623

[8] iThome_從政府、企業到個人 都是駭客鎖定發動 APT 攻擊的對象，取自 https://www.ithome.com.tw/news/91262

[9] iThome_網路防禦新架構—應用層防火牆，取自 https://www.ithome.com.tw/node/34843

[10] iThome_攻擊行為－進階持續性滲透攻擊 APT，取自 https://ithelp.ithome.com.tw/articles/10188821

[11] 維基百科_中間人攻擊、應用層防火牆、公開金鑰基礎建設、IP 位址欺騙，取自 https://zh.wikipedia.org/wiki/Wikipedia

[12] 三甲科技_何謂中間人攻擊，取自 https://cms.aaasec.com.tw/index.php/2019/12/03/s-11/

[13] 資安人_企業網路的終極門神—應用層防火牆，取自 https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=557

[14] IPRO_防火牆(Firewall), 入侵偵測(IDS), 入侵防護(IPS)，取自 https://www.ipro.tw/hr/302-it-professional-services/enterprise-security-solutions/1047-firewall-ids-ips.html

[15] 每日頭條_「網絡安全」安全設備篇（4）——防火牆、IDS、IPS 的區別，取自 https://kknews.cc/zh-tw/news/gmzmomm.html

[16] 張思楊，”以網路流量偵測 ARP 欺騙攻擊之研究”，2009

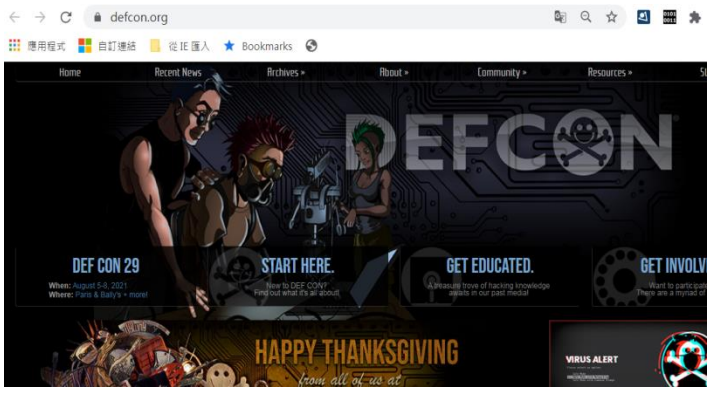
活動海報及照片

『了解駭客攻擊手法及思路的網路安全防禦方式』

學員認真聽講

『了解駭客攻擊手法及思路的網路安全防禦方式-被駭客攻擊的案例』

『了解駭客攻擊手法及思路的網路安全防禦方式-駭客攻防篇』

	
『了解駭客攻擊手法及思路的網路安全防禦方式-駭客基礎知識技能篇』	『產業實作觀點的系統性思考與組織學習實務-駭客的攻擊方式種類』
	
活動現場，每一位學員都很認真聽講	學員問答
	
網路上的 10 大漏洞 https://owasp.org/www-project-top-ten/	DEFCON ： 全球最大的電腦安全會議之一