網路攻防技術-資訊安全滲透測試技術

程凱[1]、鄭錦楸[2]、郭文中[3*]
[1]陸軍軍官學校資訊系、[2]南台科技大學資訊工程系、[3*]國立雲林科技大學資訊工程系
[1]chainkai@mail2000.com.tw、[2]chiou@mail.stust.edu.tw、[3*]simonkuo@yuntech.edu.tw

摘要

資安滲透測試是保護網路安全的技術工具和過程，本課程設計是經由介紹、說明及透過互動，實務操作在資安滲透測試過程中常用的工具與方法，藉以挖掘組織、網路及系統的安全弱點(脆弱處)與風險之行為，進而知道如何實際檢驗與證實受測對象網路安全之強度、現階段系統環境與安全狀態，同時幫助發掘系統中已知與未知的漏洞。

本課程透過資訊安全相關技術議題，以挖掘網路與系統安全性及弱點測試與驗證為核心，規劃「網路攻防技術-資訊安全滲透測試技術」共 22 模組課程，可用以培養及訓練合格的滲透測試人員。

關鍵詞：資安實務、課程發展、網路攻防、滲透測試

Information Security Practice Model Course Development Project - Network Attack and Defense Technology

Kai Chain[1], Jiin-Chiou Cheng[2], Wen-Chung Kuo[3*]
[1]Department of Computer and Information Science, Republic of China Military Academy
[2]Department of Computer Science and Information Engineering, Southern Taiwan University of Science and Technology
[3*]Department of Computer Science and Information Engineering, National Yunlin University of Science and Technology
[1]chainkai@mail2000.com.tw, [2]chiou@mail.stust.edu.tw, [3*]simonkuo@yuntech.edu.tw

Abstract

Information security penetration testing is a technical tool and process to protect network security. The designed course is a tool and method commonly used in the infiltration test process through introduction, description and interaction and practice; learn about the weaknesses (vulnerabilities) and risks of mining organizations, networks, and systems. In turn, we know how to actually check the strength of the network security of the object under test, the current system environment and security status. It also helps to discover known and unknown vulnerabilities in the system.

* 通訊作者 (Corresponding author.)

This course is designed to focus on information security related technical issues, with a focus on mining network and system security and vulnerability testing and verification. Twenty-two module courses are planned to learn and train qualified penetration test personnel for the Demonstration Course: 「Network Attack and Defense Technology-Information Security Penetration Testing Technology」.

Keywords: Security practice, curriculum development, network attack and defense, penetration testing.

壹、課程設計簡介

此次參與教育部補助大學校院辦理新型態資安實務示範課程發展計畫，本團隊為跨校整合方式，由國立雲林科技大學資訊工程系郭文中教授擔任計畫主持人，南台科技大學資訊工程系鄭錦楸副教授及陸軍軍官學校資訊系程凱副教授分別擔任協同主持人，另外聘請國家高速網路與計算中心蔡一郎研究員及安華聯網科技股份公司林敬皇技術總監協助處理相關教材設計事宜，本計畫參與者的資安教學與實務經驗豐富，並抱持著培育資安人才的心情與態度，期望設計出適合的教材資料提供大家使用。

一、課程設計目標

資安滲透測試是保護網路安全的技術工具和過程，本課程經由介紹、說明及透過互動，實務操作在資安滲透測試過程中常用的工具與方法，藉以在挖掘組織、網路及系統的安全弱點(脆弱處)與風險之行為，進而知道如何實際檢驗與證實受測對象網路安全之強度、現階段系統環境與安全狀態，同時幫助發掘系統中已知與未知的漏洞 [2][3]。

整體而言，本課程是實務導向課程，內容實務且皆為特定資安滲透測試技能相關之主題。課程目標希望經由教師及業師專家之經驗分享，並藉由 CDX 平台規畫實際操作場景[1][4]，以培養學生具有道德駭客、資安滲透測試的知識，並且掌握重要之測試與驗證技術，以便未來在撰寫程式或建構系統時，能夠有正確良好的觀念與習慣，並獲取未來在就業市場有關資安檢測相關之職能[5][6][7]。

二、課程特色

本課程旨在培養資安滲透測試人員所需基本知識及技能，除課堂上講義說明及進行作業練習外，部分課程將以討論方式進行教學，將學員分組組成滲透測試服務常見的 Red Team/Tiger Team，並以國網中心 CDX 攻防平台，建構實際滲透測試場景進行實務操作。課程結束前，利用國網中心 CDX 攻防平台，進行校際攻防演練，以驗收學生學生學習網路攻防技術之成效，讓學生從課程中學習到資安滲透測試技巧與方式等技能。本課程

因應不斷演進與更新的資安威脅，因此特別著重在以下六個部分：

(1) 滲透測試方法論：在實務上執行滲透測試時，滲透測試的方法論是受測單位驗證滲透測試服務品質的重要基礎，也是資安滲透測試服務的基石，因此，本課程規劃滲透測試相關知識內容將以滲透測試方法論作為切入點，並在後續的技術課程中，依方法論為骨幹，加入各項實作及實習內容。

(2) 資訊蒐集技巧：資訊蒐集技巧是了解資安現況及資安滲透測試的基礎，此一部分呼應許多資訊科系基本學科的基礎應用，如網路、作業系統的運作等。課程設計以實作方式，帶領學生實際操作與練習相關技巧，並學習如何整理及關連所蒐集之相關資訊，以轉化為弱點分析與風險評估之基礎。

(3) 資訊安全弱點評估：弱點評估是滲透測試產出重要的內容之一，用以說明測試標的可能遭遇的風險與安全現況、強度等。本課程由資訊安全的弱點與風險作為課程切入點，學習及評估如何進行自動化弱點掃瞄技術、通行碼破解與可逆及不可逆密碼破解等技巧，協助學生能夠具備分析、評估資訊系統、網路環境及設備安全之能力。

(4) 弱點測試與驗證：弱點利用從早期的單一攻擊程式到模組化的弱點利用平台，使弱點利用愈來愈容易，但滲透測試的人員，除了知道如何進行弱點利用外，為何利用結果的成功、失敗及評估弱點利用的容易程度，亦是本課程規劃的學習重點之一。另外，經由業界專家經驗的分享與引導，從系統、網路、設備到網頁應用程式(Web Application)及資料庫的各項弱點的利用技巧，皆有助於學生建立資安滲透測試人員的基本技能與職能。

(5) 社交工程與實體滲透：技術面的社交工程與實體安全的搭配，在滲透測試服務實務上是重要的技巧。本課程中規劃社交工程、網路設備滲透、無線網路滲透與實體入侵與滲透等，探討實體安全與系統相關人員的安全性議題，協助學生學習完整的資訊安全測試技巧與方法論。

(6) 阻斷服務攻擊：實務上在特定的行業別中，會需求阻斷服務或對服務的壓力測試，故本課程也規劃相關技術議題，讓學生了解如何進行阻斷服務及壓力測試的工作。

本課程特色包括以下四部分：

(1) 以網路攻防技術及滲透測試服務相關技能培養，作為主要課程內容基礎，透過與業師協力設計的大量實作場景與影音教學內容，以提供學生養成滲透測試服務基本職能。

(2) 依據課程規畫，除了由有經驗授課教師作觀念介紹外，大量邀請業師針對現有技術與現況分享經驗與介紹，除了對於課程內容的認知外，也可以強化學生了解原有基礎知識的重要性。

(3) 課程開始先配合授課內容，規劃實作練習，讓學生養成知識與操作相呼應習慣，之後，再以作業報告讓學生自由發揮，此時，學生可以依照個人心得與興趣自由發揮，並容易與實務相結合。

(4) 設計國網中心 CDX 攻防平台或校際實作練習場景，讓學生藉由競爭，以提升實力。

貳、課程設計執行說明

2.1 教學教案設計

本課程為滲透測試課程，主要著重在(1)滲透測試方法論；(2) 資訊蒐集技巧；(3) 資訊安全弱點評估；(4)弱點測試與驗證；(5) 社交工程與實體滲透；(6) 阻斷服務攻擊等六部分，說明如下。

1. 滲透測試方法論：主要是介紹滲透測試概論、商業滲透測試、滲透測試方法論、滲透測試小組(Red Team)及滲透測試報告撰寫等內容。
2. 資訊蒐集技巧：主要是分成資訊蒐集技巧及網路資訊蒐集方法等來探討。
3. 資訊安全弱點評估：資訊安全弱點基本概念，分成資訊安全弱點與弱點風險評估、自動化弱點發現技術、系統通行碼破解，以及破密學等方面來探討。
4. 弱點測試與驗證：利用不同作業系統的弱點及其弱點檢測技術來探討。
5. 社交工程與實體滲透：主要是介紹實體社交工程及設備滲透方面。
6. 阻斷服務攻擊:介紹 DoS/DDoS 類型、頻寬阻斷及資源耗用等。

2.2 實務課程教學環境設計

1. 實務課程的教法

實務課程除業師分享相關實務經驗外，授課過程中亦規畫實作練習場景的操作展示，並在授課場地中(電腦教室)，實際指導學生進行練習與實作。另外，部分課程內容以個案解說方式，使學生能夠融入實務情境中學習與理解各相關議題。

2. 教學環境設計

教學環境(授課場地)將安排於電腦教室中，除可組成區域網路的教學環境外，透過授課環境的交換器與實體設備，可讓各分組網路進行 VLAN 或實體分隔，作為部分議題實作練習的場景。再者，透過國網中心 CDX 攻防平台的實作練習場境之設計與規劃，學生可透過 VPN 連入後，開啟個人實作練習，或組團進行測試場景之實作練習。透過競爭或團隊刺激學生學習意願，有助於學生於實際環境中進行實作與學習相關知識內容。

3. 課程操作

課程規畫安排業師大量的參與課程設計及授課分享實務經驗，透過實作練習的進行實務操作練習，營造實際場景與環境，使學生能夠在課程中沉浸學習實務的滲透測試服務活動。最後透過校際(校對校)學生團隊競賽，以協同合作、團隊競爭等方式驗收學習成果，讓學生了解所學不足之處，持續學習相關議題，以培養學生未來資安產業就業能

力。

2.3 教學評量機制

1. 在單元課程進行中：

針對每一單元課程，建置隨堂測驗機制，作為學生每單元學習的成效參考指標。所謂隨堂測驗是一完整測驗，亦是在當天隨堂考試，測驗內容較為廣泛。因此可透過此機制，即時清楚了解學生的學習情形，並在教學現場做適當的回應，包括了解學生的學習困難處、以及立即調整教學的方法等。

2. 在單元課程結束後：

本課程教學之學習成效評量機制，採取實機操作演練考評。每周講授單元主題結束，當天實施的該主題的實機考試，以求貫徹即學即用的教學精神。另外，期中考試及期末考試則模擬 WAR GAME 形式，實施線上搶分考試，試題內容來自授課的主題。

3. 在課程結束後：

(1) 進行三校跨校之 CTF 競賽，以檢視三校學生的學習成效。

(2) 鼓勵三校學生積極參加金盾獎競賽，以檢視三校學生的學習成效：
金盾獎競賽目前是國內較有名之駭客競賽，舉辦的歷史也較久，歷年有大量的學生參與競賽，初賽分北、中、南三區進行筆試競賽，經評審錄取優秀團隊進入闖關複賽。本計畫課程目的，就是要培養具實戰能力之道德駭客，金盾獎競賽是檢視學生學習成效的最佳舞台，將請業師授課時，逐步挖掘具駭客天分之優秀學生，並在授課期間及課程結束後，持續對他們進行培訓工作，務求在金盾獎競賽中嶄露頭角。

(3) 鼓勵三校學生積極參加 CEH 駭客證照檢定，以檢視三校學生的學習成效：
舉辦「資安證照輔導」班，以考取 CEH 證照為目標，期盼為修課同學資安學養，提供更多學習的管道，並為其未來的就業提供更多的利基。

(4) 鼓勵三校學生各自在校園內成立「道德駭客社團」，長期從事駭客技術之研究推廣，並適時為各校資安事件提供諮詢工作。

(5) 鼓勵三校「道德駭客社團」，每年定期參與國內或國外的駭客年會，展現三校學習的成效，以展現資安學習人口之提升。

參、教學資源建置情形

本課程目前已完成 22 個課程模組，其中包括 22 份教學設計手冊、17 份實務課程操作手冊、17 份教學環境設計手冊、14 份教學影片及 6 份作業設計手冊。表二所呈現的是課程完成之教案手冊、課程教學設計與操作手冊、實作課程教學環境設計手冊、多媒體教學資源等。

表二:教材資源表

課程大綱 主題名稱	教材課程	實作Lab編撰	作業課程	影音課程
主題一: 滲透測試方法論				
1. 資訊安全滲透測簡介	01 資訊安全滲透測簡介		01 資訊安全滲透測簡介(滲透作業)	01 資訊安全滲透測簡介(Google Hacking)
主題二: 資訊蒐及技巧				
2. 資訊蒐集技巧	02 資訊蒐集技巧			02 資訊蒐集技巧
3. 網路資訊蒐集方法	03 網路資訊蒐集	01 實作 Lab 編撰(NMAP 與 Hping 工具練習)		03 網路資訊蒐集
主題三: 資訊安全弱點評估				
4. 資訊安全弱點基本概念	04 資訊安全弱點基本概念	02 實作 Lab 編撰(掃描工具練習)		04 資訊安全弱點基本概念
5. 自動化弱點發現技術	05 自動化弱點發現技術	03 實作 Lab 編撰(Nessus 弱點掃描工具實作)		05 自動化弱點發現技術
6. 系統通行碼破解	06 系統通行碼破解	04 實作 Lab 編撰(通行碼破解 CTF)	02 系統通行碼破解	06 系統通行碼破解
7. 密碼學與密碼分析	07 密碼學與密碼分析			07 PDF 密碼破解
主題四: 弱點測試與驗證				
8. 弱點利用平台	08 弱點利用平台(弱點利用平台)	05 實作 Lab 編撰(Metasploit framework 弱點利用平台實作)		08 弱點利用平台
9. Windows-based 弱點利用	09Windows-based 弱點利用	06_實作 Lab 編撰(權限提升弱點利用)		09Windows-based 弱點利用
10. Windows Network 弱點利用	10Windows Network 弱點利用	07_實作 Lab 編撰(內網滲透技巧實作)		10Windows Network 弱點利用

課程大綱 主題名稱	教材課程	實作Lab編撰	作業課程	影音課程
11. Linux-like-based 弱點利用	11Linux-like-based 弱點利用	08 實作 Lab 編撰(Linux-based 權限提升弱點利用實作)		11Linux-like-based 弱點利用
12. HTTP Server 弱點利用	12HTTP Server 弱點利用	09 實作 Lab 編撰(SSL 安全弱點分析)	03HTTP Server 弱點利用(IIS)	12HTTP Server 弱點利用
13. Web Application;常見安全弱點檢測	13Web Application 常見安全弱點檢測			
14. Web Application 安全弱點測試技術	14Web Application 安全弱點測試技術	10 實作 Lab 編撰(Web Application 滲透實作)		13Web Application 安全弱點測試技術
15. 資料庫安全測試	15 資料庫安全測試			
16. VPN 安全測試	16VPN 安全測試	11 實作 Lab 編撰(VPN 弱點分析)		
17. 通訊掩護	17 通訊掩護	12 實作 Lab 編撰(Hide IP 實作)	04 通訊掩護	
主題五：社交工程與實體滲透				
18.社交工程	18 社交工程	13 實作 Lab 編撰(MiTM attack 實作)		14 社交工程
19.網路設備滲透	19 通網路設備滲透	14 實作 Lab 編撰(IPbased 設備滲透實作)	05 通網路設備滲透	
20.無線網路滲透	20 無線網路滲透	15 實作 Lab 編撰(WiFi 破解分析與實作)		
21.實體滲透	21 實體滲透	16 實作 Lab 編撰(Bad	06 實體滲透	

課程大綱 主題名稱	教材課程	實作Lab編撰	作業課程	影音課程
		USB 實作)		
主題六: 阻斷服務攻擊				
22.阻斷服務與壓力測試	22 阻斷服務與壓力測試(阻斷服務與壓力測試)	17 實作 Lab 編撰(DDoS 實作)		

肆、示範課程推動工作規劃

4.1 課程推動說明

有關課程推動相關工作項目說明如下：

(1) 在課程開課方面：本工作團隊已在 106 學年度第二學期開始分別在雲科大、南台科大及陸軍官校等三所學校開設資安或網路攻防課程，並且規劃每學年都會開設相關課程。

(2) 滾動式方式來修訂課程內容：本工作團隊成員在上課或備課過程中，除適當地將本課程融入上課內容之外，同時也會依據在課程進行中的問卷調查或學生實務操作之隨堂測驗資料，進行滾動式修訂示範課程內容。

(3) 本團隊會架設一個雲端教學網站，除收集並管理各老師的示範教學相關資源及同學的學習成效之外，同時也建立一常見問題集錦，以解決同學發問問題，另外從收看的影片資料的次數，可了解修課同學對於那些單元較有興趣或者有其難度，這些資料可當作修訂課程內容方向的參考資料。

(4) 在課程結束之際，舉辦小型的 CTF 競賽活動，以測試各校學生的學習成效如何。

(5) 本團隊也邀請國網中心人員來講解 CDX 平台的功能及其相關測驗機制。

(6) 宣導示範課程實驗皆可在 CDX 平台完成，不需要多餘的設備，除讓有意參與本教材教學的老師更能深入了解本課程的內容及教學設計理念之外，同時也藉由競賽活動讓學生了解其所學不足，然後鼓勵他們跨校選修本示範課程。

4.2 課程推廣與擴散規劃

一、示範課程推廣:

(1) 為讓同學多了解資安示範課程內容及其相關性，本團隊成員會利用機會到相關科系做課程宣導活動，主要用意除讓同學知悉事件發生前的稽核、發生時之攻防演練及

事後證據收集之外，也讓同學了解滲透測試功用為何?要修此課程前，應具備哪些資安知識。

(2) 為俾利教案推廣至他校，舉辦各項種子師資培訓研討會或到他校進行推廣，讓有意參與本教材教學推廣的老師們對本課程的教學設計理念有深入了解及認識，進而願意採用本課程教材開設相關資安課程。

(3) 參與中心舉辦的課程分享會，或 CDX 環境使用推廣活動，以擴大課程宣傳的面向。

二、擴散方案規劃:

(1) 本團隊已在 106.09.22 示範教材推廣課程研討會，先將規劃中的課程資料雛型納入研習課程內容，再聽取參與老師的建議，作為課程規劃的草案。

(2) 107.05 配合離島資訊科技與應用研討會的舉行，順便到澎湖地區進行本課程宣傳活動。

(3) 未來在計畫結束前，會持續選擇適當學校進行校際課程推廣活動。

4.3 所遭遇之問題

所設計的課程教材模組，需搭配國網中心提供之 CDX 平台環境來實施操作，初期在設計教材時，CDX 平台上的操作介面仍有一些技術上的問題需克服，幸經由國網中心技術團隊的協助下，現在均已獲得解決。

另外，為了因應實作課程的教學，也花費一番心力將模組實作的部分錄製成影片，提供教師及學生能更清楚了解如何進行實作。

伍、結論

本課程已進入推廣階段，在計畫主持人、協同主持人與相關業師的合作之下，22 個模組教學教材皆已完成，目前已接洽多所學校教師，願意將本教材納入教學課程中，且持續提供相關資訊來修正及豐富課程內容，期望本計畫所設計之教材能提供教師與學生更充足的滲透測試知識與技能。

[誌謝]

感謝教育部新型態資安實務示範課程推廣補助計畫，以及教育部資訊安全人才培育計畫推動辦公室的協助，另感謝國家高速網路與計算中心蔡一郎研究員，以及安華聯網科技股份公司林敬皇技術總監，對於本課程設計上之持續相關指導。

參考文獻

[1] Cyber Defense Exercise, https://cdx.nchc.org.tw/

[2] C. S. Laih, J. S. Li, M. J. Lin, S. H. Chang, L. D. Chen, S. H. Tseng and M. Chang, "Development and Operation of Testbed@TWISC," *The 3rd Joint Workshop on Information Security(JWIS 2008)*, PP. 532-546, Jul. 2008.

[3] A.K. Sood and R.J Enbody, "Targeted Cyberattacks: A Superset of Advanced Persistent Threats," *IEEE Security & Privacy*, IEEE, vol. 11, no. 1, pp. 54-61, 2013.

[4] Testbed@TWISC - Network Security Testbed web-site, http://testbed.ncku.edu.tw/

[5] 丁諭祺、詹偉銘、張光宏、周國森、施君熹，"以 WARGAME 型式建立資訊安全攻防演練平台"，*Communications of the CCISA*，vol. 20， no. 4，pp. 72-83，2014。

[6] 林敬皇、盧建同、李忠憲、楊竹星，"網路攻擊與防禦平台之研究與實作"， *CISC 2012*, Taichung, Taiwan, May.

[7] 郭振忠、盧建同、林敬皇、李忠憲、楊竹星，"基於測試平台之網路攻防演練活動設計與實作"，*NCS 2013*，Taiwan。