以 WARGAME 型式建立資訊安全攻防演練平台

丁諭祺　詹偉銘　張光宏　周國森　施君熹
中華電信研究院資通安全研究所
{dingyuchi, james_chan, tonyc, cksp, hsishih}@cht.com.tw

摘要

近年來因為駭客攻擊手法的推陳出新，即使是已知的攻擊手法，只要進行變種或封裝，仍可輕易穿透最新的防護系統。在這種情況下若要做好全面的資安全防護，必須先從認知攻擊手法開始，透過了解攻擊手法的詳細內容，增強資訊安全防護的面向與深度。本研究規劃在實體隔離的網路環境中，以 WARGAME 的型式模擬各種攻防的情境，建立資訊安全的攻防平台；研究人員在平台中將可扮演攻擊者的角色，演練各種攻擊手法；亦可扮演防護者的角色，搭配不同的攻防情境進行監控，透過實際的演練瞭解到各種的攻擊手法與防護方式，建立起資訊安全的攻防技術。

關鍵詞：WARGAME、駭客、資訊安全

壹、前言

隨著通訊科技的發展與網際網路的普及，網路已經成為人類生活中資料交換與資訊分享的主要媒介，近年來以網路為主的服務大幅增加，如電子商務、線上購物等等應用，這使得在網路傳輸的資訊越來越有價值，駭客攻擊事件也因此層出不窮，資訊安全已成為不可不重視的課題。然而目前國內對於資安人員的訓練多注重於防護、檢測與事件鑑識，對於攻擊手法的研究相較之下稍嫌不足，在這種背景之下，如何建立起一套以駭客攻擊技術為基礎的攻防演練系統，協助資安人員面對日新月異的攻擊手法，已經是刻不容緩的議題。

正所謂知己知彼百戰百勝，瞭解駭客的思維，才能做好全面的資訊安全防護。以開放網站軟體安全計畫社群（OWASP）的 Hacking Lab 為例，該計畫以關卡的形式建立了不同類別的資安攻防情境，受訓人員入侵事先建立好的關卡，在闖關的過程中學習相關的攻防技術，從真正的攻防經驗中了解駭客的思維與攻擊方式，這種藉由人員與訓練系統之間闖關形式的互動，在資訊安全的範疇中就稱為 WARGAME。這種形式的系統，在國內外的資訊安全會議上常常可以見到，例如全世界最大的駭客年會 DEFCON，在會議開始前就會舉辦 WARGAME 競賽，成功晉級的隊伍可以免費獲得在拉斯維加斯會議的入場券，並在會議進行的期間進行決賽；又如國內知名的駭客組織 CHROOT，則固定於夏季舉辦駭客年會 HITCON，在會場也有 WARGAME 系統的設置，2014 年也開始舉辦世界性的 CTF 競賽。

本論文將研究如何以 WARGAME 形式建立攻防演練平台，同時分析各種攻防演練模式的優缺點與實際案例說明。在接下來的內容架構中，第二章節將介紹 WARGAME 的背景與由來，第三章以實際案例說明如何建立 WARGAME 系統與系統監控平台，最後第四章為論文的綜合結論。

貳、相關研究

2.1 WARGAME

以 WARGAME 的進行方式來區別，有攻防模式系統(Attack & Defense)與解題模式系統(JeoPardy)。所謂的攻防模式是所有的受訓人員在一個封閉的網路環境中，各自保護好自己管理的主機，這些主機由系統的設計者提供，在預設的安裝之下包含刻意設定好的弱點或漏洞，受訓人員在演練期間進行修補，防止自己的主機被其他人攻擊；另一方面也攻擊其他主機來獲取分數，這種模式主要訓練找出漏洞，利用弱點與修補弱點的能力。「JeoPardy」一詞源自於美國智力競賽電視節目，這種形式的 WARGAME 依照題目的類型分類，各個題目的分數不一定相同，受訓人員在解答這些題目後將獲得一組過關金鑰，將金鑰發送至解題系統取得積分，在限定的時間內取得越多分者將獲得勝利，題型分類主要有為網站型（Web Security）、應用程式分析（Binary/Reversing）、數位鑑識（Forensics）、弱點挖掘（Potent Pwnables）、綜合情境（Trivial/Misc）等等[6]。

2.1.1 網站型

網頁類型的 WARGAME 主要討論網站相關的資安問題，這種類型的關卡中存在刻意設計好的安全漏洞，並且著重於這種類型的漏洞利用。以 SQL Injection 為例，受訓人員必須先找到漏洞所在之處，並利用各種注入技巧如 Blind SQL、Time-based SQL、Error-based SQL 等手法，繞過關卡所設計的 SQL Injection 過濾器，並且在闖關的過程中一步一步的找尋新的闖關線索，才有辦法完成關卡。

2.1.2 應用程式分析

這類型的關卡著重於對應用程式的分析，受訓人員必須對逆向工程有一定程度的了解，就如同分析惡意程式一般，先把加密過的殼解密後，再使用靜態分析（Static Analysis）與動態分析(Dynamic Analysis)的技巧，追蹤程式執行的流程並推測程式的下一個動作，在這個過程中尋找過關的蛛絲馬跡。

2.1.3 數位鑑識

數位鑑識關卡包含了各種類型的資料鑑識，訓練受訓人員如何在龐大且雜亂的資料中尋找有用的資訊，例如網路封包的鑑識、磁碟檔案系統的鑑識、刪除資料的還原、圖片資訊隱藏技巧等等，抑或混合各種類型的資料。受訓人員在闖關的過程中將學習到各種資訊隱藏的技巧，透過這種方式瞭解駭客的行為。

2.1.4 弱點挖掘

不論在軟體開發的過程之中進行了多少測試，在軟體發佈之後往往還是會出現臭蟲（Bug），一般的情況之下使用者會將這些資訊回報給廠商進行改善，但也有可能被駭客所利用，弱點挖掘可以說是應用程式分析更進階一步的關卡，這類型的 WARGAME 除了要瞭解程式執行的流程，還必須尋找應用程式漏洞並且撰寫程式進行利用。

2.1.5 綜合情境

在真實的情況下，資安人員隨時在面對各種類型攻擊的挑戰，此類型的 WARGAME 並沒有一定的主題，必須綜合了不同類型的攻擊技巧，或許還需要碰碰運氣才有辦法闖關，這種訓練就像駭客實際在入侵系統一般。

2.2 網路攻防演練系統

過去研究[1][2][3]指出，有別於傳統資訊安全教育訓練，建構一套有效的網路攻防演練系統，可讓受訓人員在實際攻防演練操作過程中更容易掌握入侵者的攻擊技術，並從不同的情境演練中培養出較全面的資安防禦及應變能力。

網路攻防演練開始應用資安教育可追溯至 2001 年西點美國軍事學院發起的 CDX(Cyber Defense Exercise)。CDX 由美國大專院校組隊參加，競賽模式主要測驗各隊伍是否能有效偵測防禦全職攻擊者的入侵破壞，並維持系統網路服務正常運作。CDX 的概念成為往後全球各種受歡迎的資訊安全技能競賽效仿的模型，例如 DEFCON 的 CTF(Capture the Flag)，參賽隊伍必須在規定時間內利用弱點攻破對手的主機拿到 Token，同時間偵測對手攻擊並迅速修補己方的弱點漏洞保護主機避免失分。

在國內，網路攻防演練在實務上亦成為提升機關組織資安意識與整體資安防禦能力的重要方法途徑。《2010 資通安全政策白皮書》中將實施跨領域資安演練列為國家資安發展的重要施行策略，並規劃建置資安虛擬攻防平台，以強化國內研發成果的可應用性與競爭優勢[7]；《國家資通安全發展方案(102 年至 105 年)》明訂資通安全辦公室需辦理政府機關資安演練作業，並規劃資安情境演練與實兵演練[8]。

參考美國國土安全部緊急事務管理總署(FEMA, DHS)的定義，將過去國內資安攻防演練依據訓練類型進行歸納[5]，初步可區分為簡報引導型(Orientation Session)、技術演練(Drills)、桌上演練(Tabletop)、功能性兵棋推演(Functional)以及實兵驗證演習(Full-Scale)，如**表一**。其中簡報引導型和技術演練型是一般最常見的訓練類型，但通常只局限於單一資安技術講習操作，面對處理實際攻擊狀況成效有限。

為培養各機關在面對網路攻擊時的處理能力，102 行政院開始針對所屬 33 個二級機關進行網路攻防演練，其中演練進行的方式可分為桌上演練(Tabletop)和實兵演練(Full-Scale)兩種，前者以書面及視訊應答方式，模擬機關遭受目前常見之網路攻擊時(如 DDoS、網頁入侵、AD 入侵等情境)，機關對事件處理標準程序、通報應變程序的熟悉程度；後者則由國安局、國防部、法務部調查局、內政部警政署刑事警察局、技服中心組成攻擊組，參考 OWASP TOP 10 常見攻擊手法，針對行政院所屬二級部會的上線主機網路進行弱點掃描、滲透測試、社交工程信件的實際攻擊演練。桌上模擬活動主要聚焦在

測試政府機關針對不同警戒層級使用對應之標準作業程序(SOP)，受訓者僅限於單位主管或重要指揮人員，並非第一線事件處理人員，因此實際處理的誤差現象。實兵演練方式，但需要動員模的人力，此外缺乏彈性，無法針對單一較弱的環節重複演練，此外由於是採實兵演練，攻擊的對象是已經上線運的主機系統，因為如果在沒有受控制的環境下可能會造成服務無法正常運作。

表一：國內資安攻防演練訓練類型歸納表

演練類型	內容說明	優點	缺點	資安實例
簡報引導型（Orientation Session）	由專家或規畫者，透過簡報方式，將訓練課程目標、內容、注意事項等重要關鍵點一一向參與人員說明。	單一人員負責準備即可	●受訓者只是被動的被告知資訊。 ●參與人員沒有實際操作，效果有限。 ●無法衡量演練成效。	大專院校資安學程或坊間的資安教育訓練課程講習。
技術演練（Drills）	對於單一技術課目或單一狀況進行操作演練，具有一定的方法或步驟。通常用於驗證某種專業操作能力。	補足了簡報引導型實作執行面上的不足	●局限於工具或產品操作，面對複雜的狀況效果有限。	●實作資安認證課程(如CEH、CHFI、SCNA、SCNP) ●資安產品實作訓練
桌上演練（Tabletop）	訓練對象是單位主管，針對攻防情境進行抽象的邏輯推算訓練。以小組討論形式進行，目標是誘發具有建設性的討論，找出既有計畫需改善之處。	●可了解現有緊急應變處理計畫做法是否合理洽當。 ●不需啟動應變中心，可不涉時間壓力下進行	●訓練對象非第一線處理人員。 ●容易淪為紙上談兵，與實際發生狀況有落差。	102 年網路攻防演練桌上情境模擬演練，以書面及視訊應答方式，對行政院所屬 33 個二級部會，模擬受到攻擊時機關事件處理標準程序、通報應變程序及聯防機制的熟悉程度。
功能性兵棋推演(Functional)	類似戰爭遊戲(WARGAME)形式模擬實際危機發生，強調受控制小區域	●在受控制的環境下進行演練。 ●具備彈性，可以擴充不同演	攻防模擬平台設計者需要有豐富資安技術能力與經驗。	WARGAME 攻防實驗系統

	環境下的應變能力演練	練情境。 ●從攻擊面向學習防禦方法，更加有效。 ●較低成本。 ●可以針對較弱的環節或情境，重複演練。		
實兵驗證演習（Full-Scale）	以最接近實際狀況之方式模擬危機發生時之應變作業。	可比照真實情況下，驗證高度壓力環境下，緊急應變系統如何執行任務並發揮其危機管理能力。	●耗費高額人力和資源成本。 ●缺乏彈性，無法針對單一較弱的環節重複演練。 ●演練過程中發生的錯誤，可能會影響其他系統正常運作。	102 年網路攻防演練的實兵演練(live action exercise on operation Network)，針對行政院所屬 33 個二級部會，以遠端弱點掃描、滲透測試、社交工程郵件信件等方式，實際攻擊機關之系統與網路。

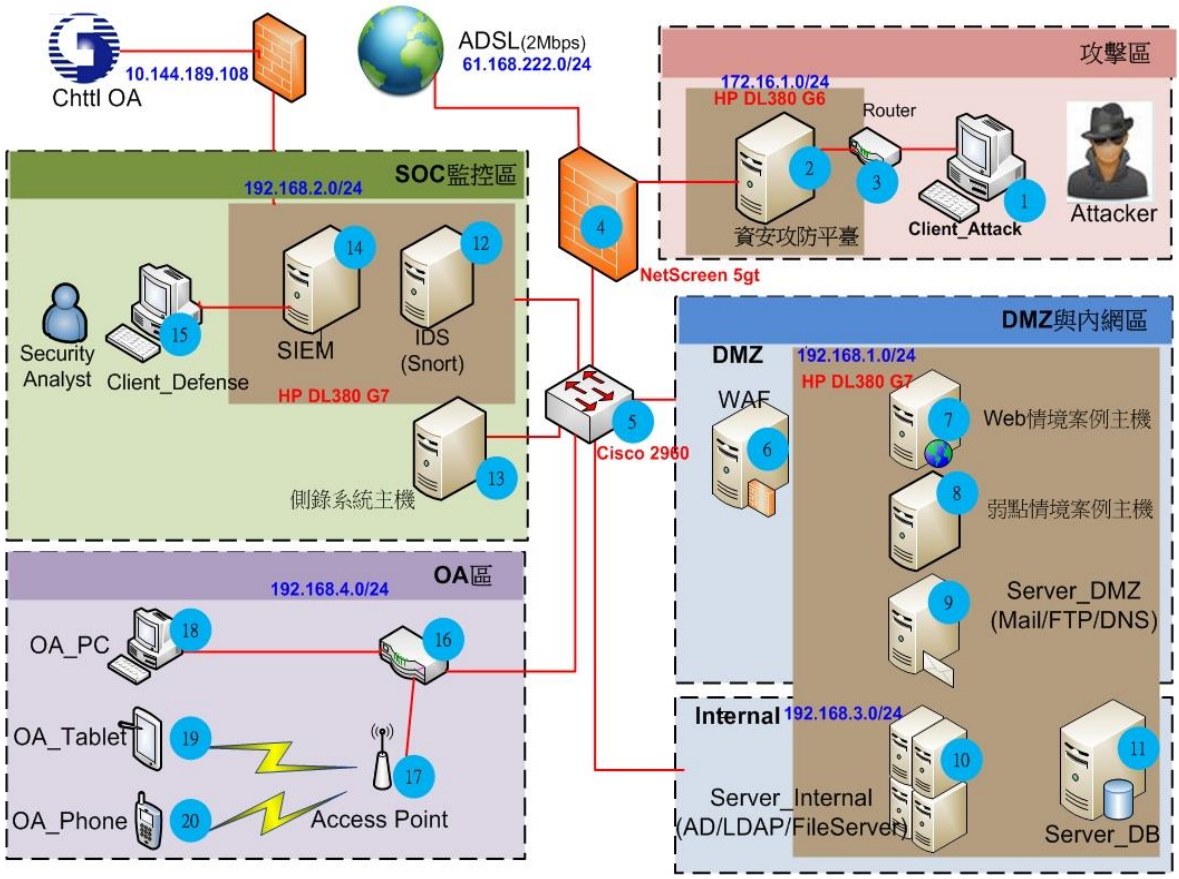
參、WARGAME 的設計與建置

在這個章節中，我們將說明如何以 WARGAME 的方式，建置一套完整的攻防演練系統；另外也將目前的駭客攻擊手法分成十個類別，並以這些分類為基礎，做為 WARGAME 的資安攻防情境。

3.1 WARGAME 攻防系統網路架構

圖一為攻防系統的整體網架構劃，主要可以分為攻擊區、SOC 監控區、DMZ 與內網區、OA 區等四個子網路區域。實驗人員可在攻擊區扮演駭客的角色，登入 WARGAME 資安攻防平臺，針對 DMZ /Internal 和 OA 區預先設計好的各種關卡情境進行演練；實驗人員亦可在監控區扮演防守者的角色，分析攻擊者在進行攻擊過程中遺留下來的各種日誌紀錄證據，偵測各種情境的攻擊，並操作各種資安設備(如 IDP、WAF、FW)進行防禦。

在整個網路架構的規劃中可滿足二個重要的原則。首先，本實驗環境需 利用防火牆隔離出一獨立演練環境，以確保演練的過程中不會對公司內部網路或外部網際網路造成影響；再者本實驗系統利用 ESXi 實現主機系統虛擬化，未來可依照演練情境進行彈性擴充調整，亦可以針對某些演練情境快速還原主機到原始未受破壞的狀態。



圖一：WARGAME 攻防系統網路架構圖

表二：WARGAME 攻防系統各網段功能整理表

網路區段	主要功能說明	配置設備
攻擊區	執行 WARGAME 系統各種攻擊情境演練	資安攻防平台、駭客整合工具系統
監控區	監控各種演練情境攻擊	入侵偵測系統、封包側錄系統、資安事件分析管理平台
DMZ 與內網區	放置各種模擬情境及重要的後端主機伺服器	後端演練情境關卡系統、Active Directory 主機、郵件伺服器系統、後端資料庫系統等
OA 區	模擬行動裝置、社交工程、內網入侵等情境	個人 PC、Android 手機、Android 平板、無線接取器

3.2 情境分類

我們將情境分為十大類，如下表所示

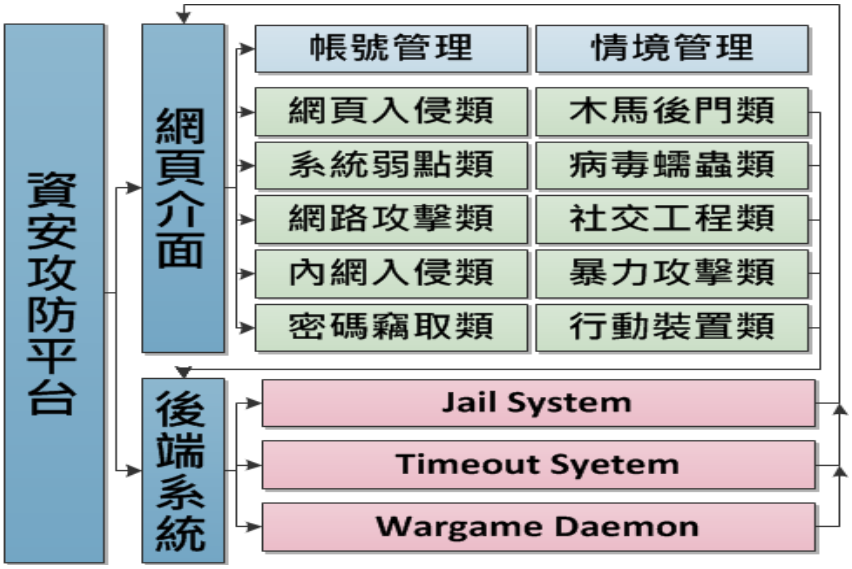
表三：WARGAME 情境分類表

情境分類	說明	情境範例
網頁入侵	基礎入侵技巧與進階入侵手法	● XSS ● SQL Injection ● Command Injection ● Code Injection ● LDAP Injection ● XML Injection ● Directory Traversal ● File Include ● Advanced SQL Injection ● NoSQL Injection
木馬後門	瞭解後門程式如何隱藏在系統當中	● 一句話木馬 ● 圖片木馬 ● 後門程式
系統弱點	各種 OS 與 Service 已知的弱點編號	● 弱點情境演練 ● 系統程式安全
病毒蠕蟲	如何分析病毒程式	● Sandbox 運用 ● Crackme(動靜態程式分析)
網路攻擊	常見的網路攻擊手法情境	● Deny of Service ● Network Sniffer、Man-in-the-middle
社交工程	釣魚(Phishing)手法分析	● 網頁式釣魚 ● Email 方式釣魚
內網入侵	入侵成功後的進一步滲透	● 機敏系統設定檔 ● 內網拓樸分析
暴力攻擊	常見的密碼破解程式	● 使用 CPU 與 GPU 破解密碼 ● 常用的 Service 暴力攻擊
密碼竊取	常見的加解密與 Hash 演算法	● 編碼(Base64, URL Encode 等) ● Hash 演算法(SHA1, MD5, NTLM 等) ● 加密方式
行動裝置	OWASP Mobile Risk Top 10	● M1 - Insecure Data Storage ● M2 - Weak Server Side Controls ● M3 - Insufficient Transport Layer Protection

		● M4 - Client Side Injection ● M5 - Poor Authorization and Authentication ● M6 - Improper Session Handling ● M7 - Security Decisions Via Untrusted Inputs ● M8 - Side Channel Data Leakage ● M9 - Broken Cryptography ● M10 - Sensitive Information Disclosure

3.3 WARGAME 攻防平台介面

資安攻防平台系統分為兩個部分，一個是網頁介面的攻防情境管理平台，另一個則是後端的關卡系統。

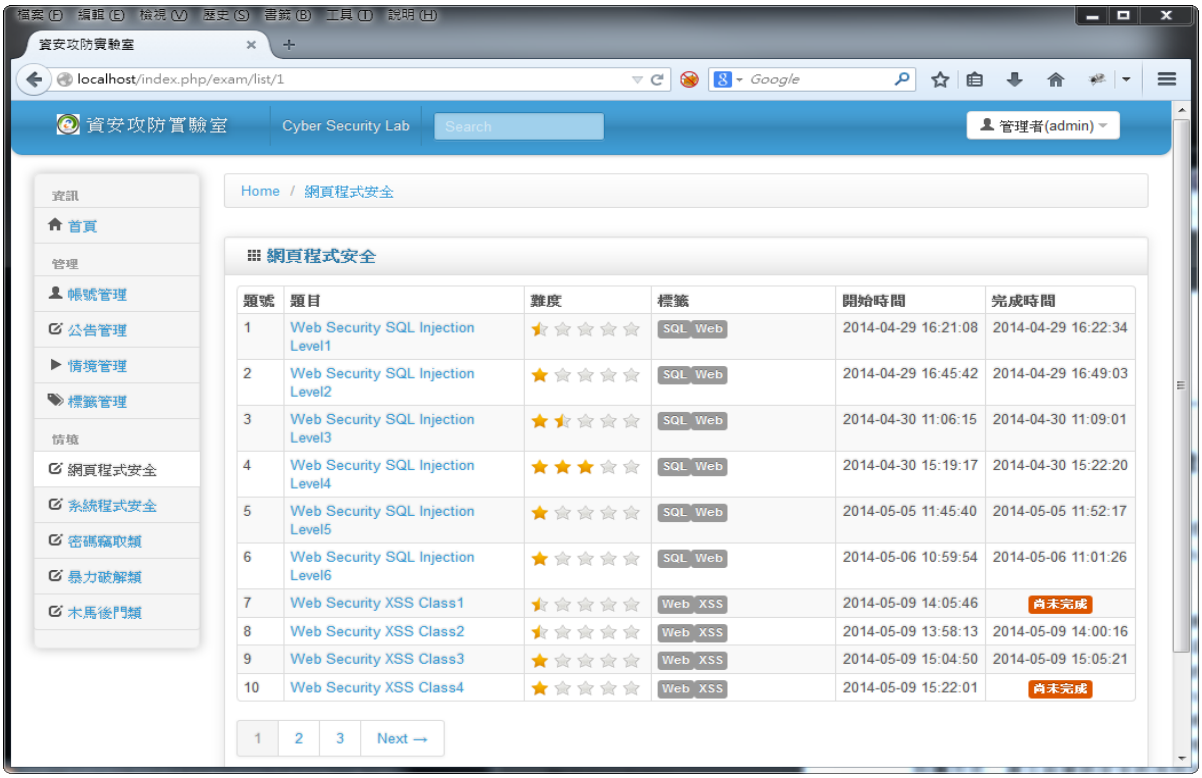


圖二：資安攻防平台系統架構圖

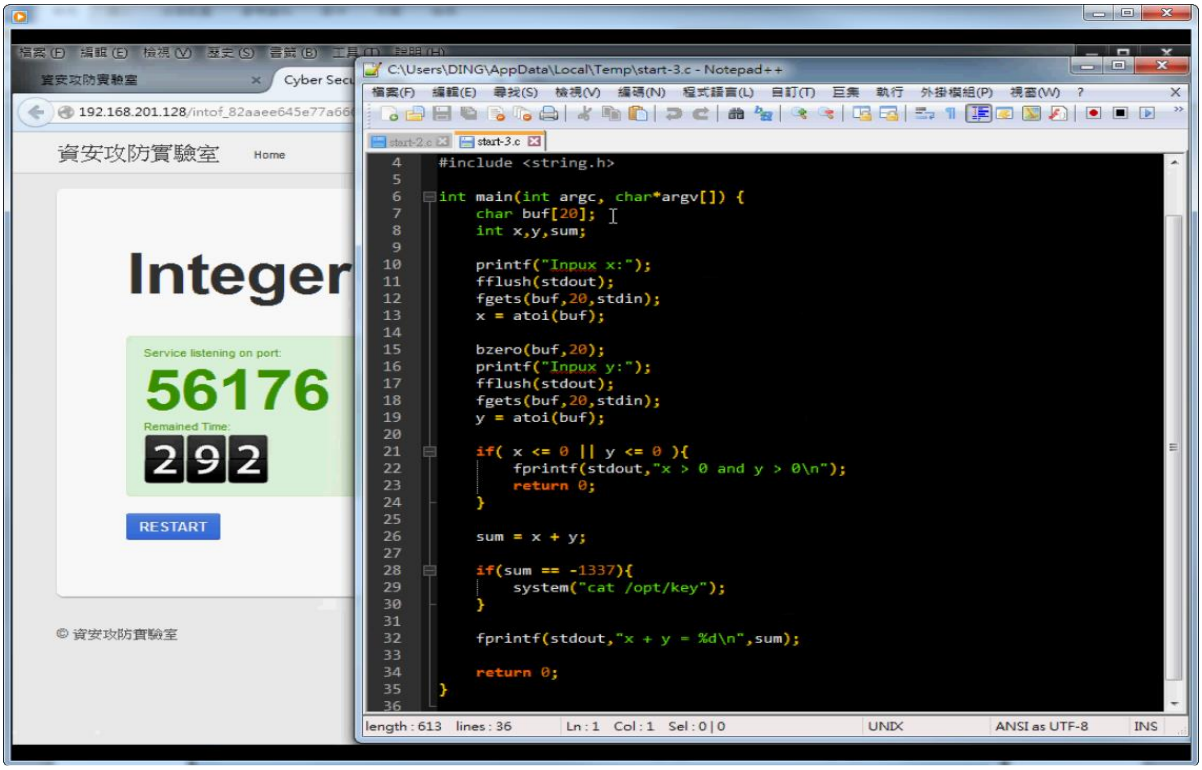
3.3.1 前端網頁介面

攻防情境管理平台中包含帳號管理模組與情境管理模組與十個類型的關卡分類，在帳號管理模組中可以新增修改刪除受訓人員的帳號，受訓人員可利用此帳號登入網頁平台；在情境管理模組中可新增修改刪除 WARGAME 系統的關卡，當中包含關卡的說明、難度、關卡分類、搜尋標籤與過關的金鑰；在關卡說明中將設計 WARGAME 關卡的資訊，例如關卡的 IP 位置以及提示等等，難度分類採用十個等級的設置，最低難度是半顆星，最高難度則是五顆星，此難度由關卡的設計者決定，另外各個關卡的類別可透過關卡分類與搜尋標籤設置。

受訓者登入網頁平台後，可以選擇演練的分類，以網頁類型的分類為例，進入分類中選擇一個情境進行演練，在情境中扮演駭客的角色攻擊情境主機尋找過關金鑰，最後再將金鑰輸入至網頁平台驗證是否過關，如圖三、圖四。



圖三：資安攻防演練平台



圖四：資安攻防演練平台

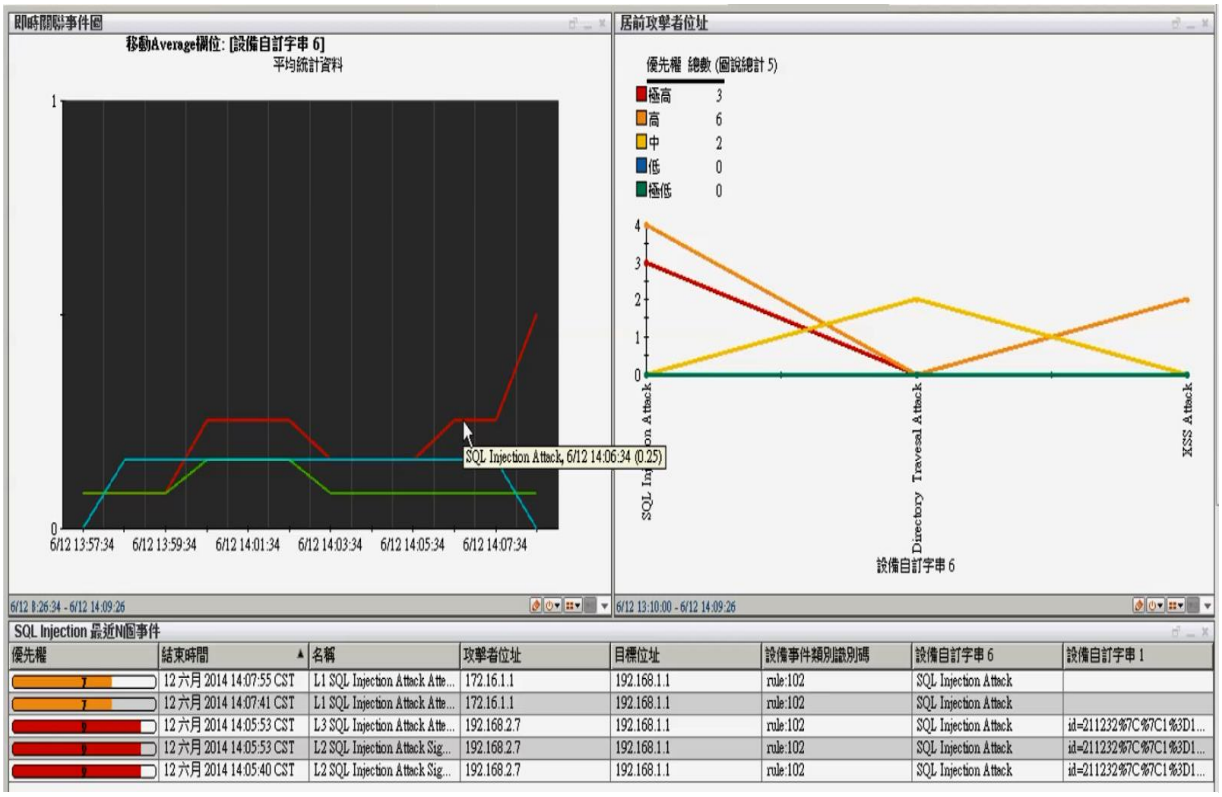
3.3.2 後端系統

後端的關卡系統分網頁與系統程式兩大部分，網頁關卡使用 Debian 作業系統，架構 Web Server、PHP、MySQL 作為網頁關卡的平台，並使用 Apache mod_ruid2 限制關卡的對系統的存取權限，防止受訓者在演練的過程中跳脫關卡限制，破壞關卡系統主機。在系統程式部分採用 Debian 為作業系統，並使用 schroot 作為沙盒（Sandbox）限制關卡對於本機的存取權限，另外使用 NETCAT 工具將關卡綁定至隨機的 TCP Port，在搭配 Timeout 指令控制關卡的執行時間。

3.4 監控防禦

攻擊端和防禦端獨立進行，事前防禦端並不知道攻擊端將採取何種攻擊手法進行演練，防禦端的監控人員收集防火牆、網路型入侵偵測系統、網頁型防火牆、網站伺服器、作業系統稽核日誌、資料庫稽核日誌等，並針對演練區的網路封包進行側錄，分析日誌紀錄撰寫偵測關聯規則，並對攻入侵攻擊行為發出告警。演練過程可以提高資安人員的敏感度，訓練從大量的訊息中找到入侵者從網路端到端點設備所留下的各種數位證據的關聯性，以掌握攻擊者的最新動態，如**圖五、圖六**。

圖五：即時攻擊事件圖



圖六：即時關聯規則告警監控圖

肆、結論

本研究以 WARGAME 的形式，建立一套資訊安全的攻防平台，透過實際演練駭客攻擊的方式，讓受訓人員站在駭客的角度，瞭解駭客的目的，並深入研究攻擊的手法技術與背景，期許在面對日新月異的攻擊手法時，增加資安防護的面向與深度。本平台不僅僅可用於資安人員的訓練，在未來可以融入校園的資安課程中，培養資安人才。

參考文獻

[1] M. S. Aboutabl, “The CyberDefense Laboratory: A Framework for Information Security Education, ” *Information Assurance Workshop, 2006 IEEE* , pp.55,60, 21-23 June 2006.

[2] A. Conklin, “The use of a collegiate cyber defense competition in information security education. Proceedings of the 2nd annual conference on Information security curriculum development”. *Kennesaw, Georgia,* ACM: 16-18., 2005.

[3] K. E. Kercher, and D. C. Rowe. “Risks, rewards and raising awareness: training a cyber workforce using student red teams.” *Proceedings of the 13th annual conference on Information technology education,* ACM, pp. 75-80, 2012

[4] D. P. Coppola, “Introduction to international disaster management,” *Butterworth-Heinemann*, 2006.

[5] A. Conklin, "Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course", *System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on*, vol. 9, pp. 220b-220b, 2006.
[6] CHROOT.ORG , "The WARGAME：駭客訓練基地 – 決戰台灣版"，2008 年 10 月。
[7] 行政院科技顧問組"2010 資通安全政策白皮書"，2010 年 11 月。
[8] 行政院國家資通安全會報(2013) "國家資通訊安全發展方案(102 年至 105 年)"，2013 年 12 月 25 日。

[作者簡介]

丁諭祺
國立政治大學資訊科學研究所碩士，現任中華電信研究院資通安全研究所副研究員，專長於網站應用程式安全、滲透測試，具備多年駭客技術研究經驗；曾執行政府機敏資訊系統滲透測試，發表過知名 SIEM 平臺弱點獲得 CVE 編號。

詹偉銘
國立台灣大學資訊管理研究所碩士，現任中華電信研究院資通安全研究所副研究員，專長於資安偵測監控技術、封包日誌紀錄分析、資安通報與事件應變處理等防護機制，曾經協助國內外政府及大型企業規劃導入資安監控中心(SOC) 。

張光宏
美國南加州大學(USC)電腦科學碩士，現任中華電信研究院資通安全研究所研究員，主要負責行動裝置安全技術研發、網路安全鑑識、資安事件調查與應變及大型資安監控中心(SOC)建置。

周國森
國立中央大學資訊工程研究所博士,現任中華電信研究院資通安全研究所主任級研究員。

施君熹
逢甲大學自動控制研究所碩士，現任中華電信研究院資通安全研究所主任級研究員。