# 基於多面向攻防平台達到全面性資安技能訓練

陳仲寬 謝續平
國立交通大學資訊工程系
ckchen@cs.nctu.edu.tw, ssp@cs.nctu.edu.tw

## 摘要

由於網際網路等資訊技術的重要性日增，資訊安全的重要性也隨之增加。如何維持及培育資安相關人才將是重要的問題。CTF 競賽是在國外相當盛行之資安技能競賽，許多大學或資安團隊皆會透過 CTF 進行資安技術的練習，以增加資安相關實務經驗。本文首先介紹 CTF 的形式與所需具備的技術，接著與實際網路環境所遭受之威脅做比較。說明 CTF 的訓練尚不足以涵蓋部分重要資安議題，並提出多面向攻防平台以延伸 CTF 競賽的涵蓋範圍。透過採用實際網路服務作為競賽題目，並引入一般使用者參與，可以提高競賽的真實性，也能涵蓋更多資安相關議題。最後則將比賽資訊妥善保存，做為數位鑑識的訓練之用。希望能透過多面向攻防平台增加 CTF 訓練的範疇，進行更全面性的資安技能訓練。

**關鍵詞：資訊安全**

## 壹、前言

隨者網路使用之興盛，網路安全的重要程度與日漸增。而網路服務的使用面日益廣泛，亦造成各式各樣與個人隱私、財務資訊相關的資料透過網路傳遞儲存，大幅提高了網路安全的必要性。而許多基礎建設為了管理上的彈性及方便，也會透過網路進行存取操作，無形中也加深了網路安全的影響範圍。由於網際網路逐漸扮演起社會中重要的環節，網路攻擊所造成的危害已由個人損失、商務上的損害提升至國家安全的層級。

為了增進資安實力，人才培育是最為重要之一環。資安人才之培育不僅需要有一定的資訊背景，紮實的技術水平，亦需要有相當的實務經驗。對於一般學生而言，實務經驗的部分尤其困難，資安相關議題或資料時常涉及道德以及法律上的考量而難以提供給一般學生參考，以至於許多資安背景學生缺乏實際的練習經驗。

隨著資安議題逐漸被重視，國內外資安團隊開始參與國際之 CTF 競賽，以競賽之方式鍛鍊資安實務經驗。CTF 競賽也吸引許多對資安有興趣的學生參與。透過舉辦 CTF 競賽以吸引更多學生參與，可以加強最缺乏的實務經驗部分。

本文透過探討 CTF 競賽所涉及之資安技能，並與真實網路攻防環境做比較，提出比賽環境與真實環境隻差異。首先在一般 CTF 競賽中，不常使用真實網路服務作為題目，較難完全反映真實環境。接著，由於缺少與人的互動，許多利用郵件等社交攻擊手段無法使用，而這類攻擊往往是網路攻擊最氾濫的部分。最後，由於比賽環境相對簡單且競

賽時間較短，許多後續的行為無法包含在競賽中，如：植入後門、利用攻陷主機作為中繼站以及後續的數位鑑識等，難以涵蓋在競賽內容中。

因此，本文提出一套多面向攻防平台。在此平台中首先利用主辦方實際運行之網路服務為基礎出題，增加競賽內容的真實性。並引入一般使用者，增加攻防的多樣性，也更貼近一般網路環境。最後，由於競賽的環境貼近真實環境，攻擊成功的後續行為也顯得更為重要，並將過程中的資料保存，作為後續數位鑑識的訓練材料，以延伸 CTF 競賽涵蓋之範疇。

## 貳、CTF 攻防練習簡介

CTF(Capture the Flag)競賽，為一種資訊安全技能競賽的形式。參賽者透過突破出題者設計之資安相關題目，或入侵目標的伺服器，取得一組相對應的旗幟（flag），或稱之為金鑰（key）的字串，並利用該金鑰換取積分的比賽。

利用 CTF 競賽來培養資訊安全人才的方式在國外已行之有年，近年來由於 CTFTIME[1]網站統整世界各項 CTF 競賽資訊，並蒐集參賽者撰寫比賽心得（Writeup）。大幅加速了競賽以及團隊等資訊流通，使得各國參與越來越為熱絡。其中最為重要的競賽為 DEFCON CTF[2]，其餘如 CodeGate[3]、PlaidCTF[4]以及 Ghost in the Shellcode[5]等也是重要競賽，常吸引數百隊隊伍餐賽。這次 HITCON CTF[6]因賽前奪得 DEFCON 亞軍，吸引世界各強關注，共有 1020 各國隊伍參加。

許多大學些成立了技術團隊參與 CTF 的競賽，如：CMU 的 PPP 團隊[7]、南韓科學技術院(KAIST)的 KAIST GoN 團隊[8]以及北京清華大學為主的 Blue-Lotus 團隊[9]。此外，許多隊伍更是由業界資安技術人員組成，如：Google Security Team 的 Dragon Sector[10]。可以說明 CTF 賽事已廣泛受到各國注意，並成為資安人才培育的一環。

一般而言，CTF 分為 JeoPardy 以及 Attack & Defense 兩種形式。於 JeoPardy 競賽形式中，主辦方會設計 15~30 題不等的關卡，參賽者須於競賽期間內解決關卡謎題，取得一組獨特的金鑰即可得分。關卡內容包含網站漏洞，逆向工程，程式漏洞， 鑑識分析等方向。另一方面 Attack & Defense 形式的比賽，主辦方會設計多個具漏洞的網路服務，並提供參賽者包含這些具漏洞服務之伺服器，同時這些伺服器中也設置好金鑰。參賽者需要在競賽期間內保護自己的伺服器正常服務，同時需要攻擊其他參賽者的伺服器已取得目標參賽者的金鑰換取積分。

相較之下，JeoPardy 的競賽模式出題的廣泛度較大，大致上可分為下列幾種題型

- 網站漏洞（Web）：破解出題者設計之具有漏洞的網站以取得金鑰，例如：SQL Injection、Command Injection 等。
- 逆向工程（Reverse Engineering）：參賽者需對出題者提供的可執行檔進行分析，以了解其運作原理。
- 程式漏洞（Pwn）：出題者會建置具有漏洞之程式于遠端伺服器，例如：堆疊溢出（Buffer Overflow）以及格式化字串漏洞（Format String Vulnerability）

等漏洞，參賽者需分析此程式並撰寫攻擊程式碼（shellcode）取得伺服器權限。

- 數位鑑識（Forensic）：參賽者需要對出題者提供的資料進行分析，資料類型相當多樣，從網路封包記錄到硬碟印像檔都有可能，最後需要找出影藏其中的金鑰。
- 密碼學（Crypto）：參賽者需要破解出題者設計的密碼學問題，例如：雜湊碰撞（Hash Collision）等。
- 其他（Misc）：由於資安相關問題廣泛，因此有許多難以歸哪的問題皆屬此類。例如：行動裝置程式分析、程式設計以及資訊搜集（Information Gathering）。

而 Attack & Defense 形式的比賽出題形式較為固定，但參賽者需要較為全面的攻防技巧，一般而言，此類型需要之技術有下列幾項：

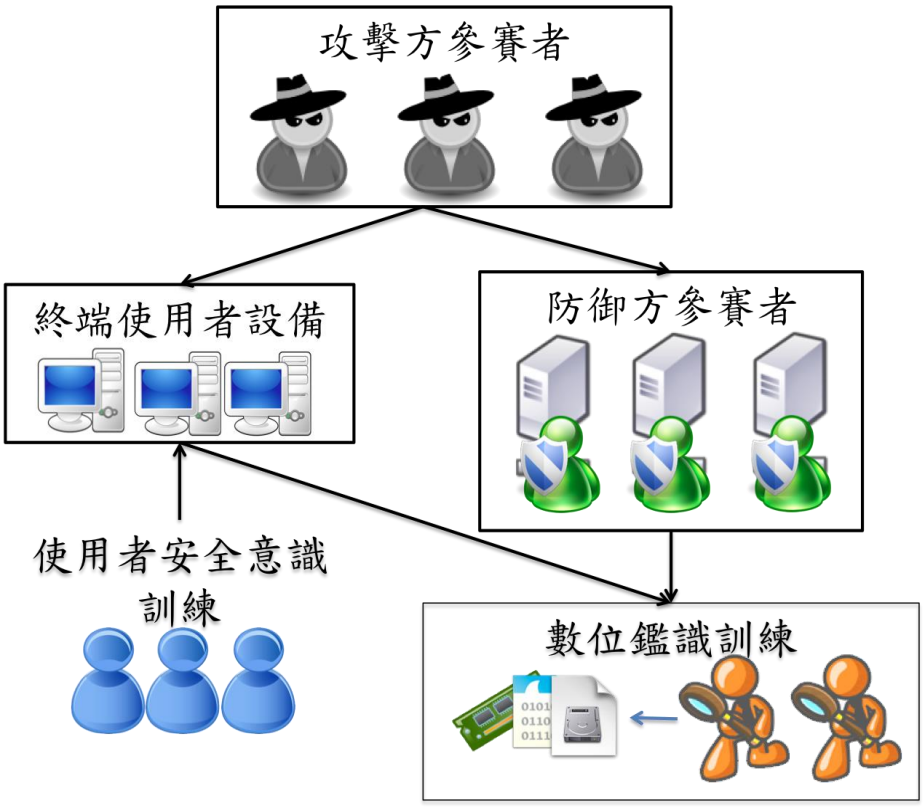
- 程式分析：參賽者必須能對出題者設計之網路服務進行分析，以了解該服務之行為，包含：網頁腳本程式以及網路服務可執行程式。
- 漏洞挖掘：分析完程式行為後，需要進一步尋找程式漏洞，這部分會需要模糊測試（Fuzzing Testing）或逆向分析等技術。
- 程式修補（Patch）：參賽者若是發現程式漏洞，則需進一步對程式進行修補以防止其他參賽者攻擊此漏洞。
- 攻擊程式撰寫：參賽者若是發現程式漏洞，同時亦須撰寫攻擊程式碼入侵其他隊伍之伺服器已奪取其他隊伍之金鑰。
- 封包分析：若是漏洞已經被其他參賽者發現並進行攻擊，這時候則需要觀察網路流量以找出攻擊行為及攻擊所用之技術。

此章節較為簡略地介紹了 CTF 競賽，接著介紹了各項國內外 CTF 競賽以及知名的 CTF 團隊，最後說明了 JeoPardy 模式以及 Attack & Defense 模式的競賽內容及所的資安技能。

## 參、CTF 競賽與資安實務的差異

隨者 CTF 競賽的推廣，許多對資訊安全有興趣的學生可以透過參與比賽的形式進行實戰訓練，提升對實務經驗的不足，並透過同儕間的討論更深入的學習資安技術，可以說提供了相當良好的資安技能訓練。然而礙於比賽環境限制，有許多資安相關之技能無法涵蓋於 CTF 競賽之內。此外，題目皆為出題者所設計，難免與現實網路服務有所差異。若能了解當前 CTF 與實際攻防環境之差異，則可以幫助我們設計新一代的 CTF 攻防環境，以全面性的涵蓋資安相關技能，達到培育學生資安技術的目標。

因此在此章節中，我們提出三點一般 CTF 競賽與真實網路攻防環境的差異，包括了 1) 缺乏真實攻防環境、2) 缺乏實際使用者參與以及 3) 缺乏入侵行為的後續延伸。以下分別探討這三個議題。




圖一：多面向攻防平台

**1. 缺乏真實攻防環境**

就時間方面而言 CTF 競賽大多限制於兩天之內，因此題目難度設計受限，無法規劃過於複雜之漏洞。而于一般網路環境中，網路架構複雜，而網路服務的程式規模也相當龐大複雜，漏洞的難易度根據程式設計師的水準不一，可能會有簡單可以發覺的弱點，也有相當複雜的程式錯誤。另外，像是針對 DNS 伺服器進行的攻擊是相當有效且嚴重的，然而一般難以涵蓋在 CTF 競賽中。進一步的，真實環境中可能會存在許多基本的資安設備，如：防火牆、IPS 以及防毒軟體等設備，更大大提高入侵的複雜度。因此，實際環境與競賽環境還是有相當的不同，若能提升 CTF 競賽對於環境的模擬度，相信可以增加對於資安能力培養的實用性。

**2. 缺乏實際使用者參與**

於實際網路攻擊中，人是最為重要的一環，許多攻擊手法，如：惡意文件攻擊，釣魚信件，Drive-by-Download 等攻擊手法，皆須要借助於使用者的疏忽進行攻擊。尤其近年來興起的 APT（Advance Persistent Attack）攻擊行為，相當重要的一條攻擊途徑即為電子郵件。而隨著使用者的出現，網路伺服器於使用者認證授權的漏洞更容易出現，例如：Session Handling Error，並且 XSS 一類的攻擊行為大多需有使用者介入才能發動。而在一般 CTF 競賽時，大多處於封閉環境內，缺乏實際使用者，因此對於這類需要使用者協助之攻擊難以模擬。

**3. 缺乏入侵行為的後續延伸**

對於攻擊者而言，有效地入侵目標的系統只是攻擊的第一步，更重要的是保持對於目標的後續控制權，以利後續的攻擊並在目標網路系統內進行橫向擴散。另一方面，對防守方而言，除了分析弱點修補漏洞之外，使後的鑑識分析也是相當重要的一環。以了解攻擊之來源，並釐清入侵攻擊帶來的損失，以及清查系統內之惡意程式。而在 CTF 比賽中，雖有植入後門之策略，但一般而言較無對於目標系統進一步攻擊的練習，攻擊行為一般停止于取得目標系統權限為止。

## 肆、多面向攻防平台

由上述章節，我們歸納了當前 CTF 比賽尚未涵蓋的範圍，包含了 1) 缺乏真實攻防環境，2) 缺乏實際使用者參與 以及 3) 缺乏入侵行為的後續延伸。因此本文提出多面向攻防平台的架構，以期能將 CTF 的實用面增廣，應用於滲透測試，使用者安全意識訓練以及數位鑑識訓練等方面。提供更全面的資安訓練。

**1. 整體架構**

本平台包含五個部分，如圖一：，攻擊方參賽者、防御方參賽者、終端使用者設備、使用者安全訓練以及數位鑑識訓練。主辦方需要設定終端使用者設備以及防御方參賽者之環境，攻擊方參賽者則負責對防御方參賽者以及終端使用者設備進行攻擊。防御方參賽者則需對負責的服務進行維護，避免被攻擊者入侵。使用者安全意識訓練部分則透過終端使用者設備解決主辦方設計的任務，於此同時，避免被攻擊方利用釣魚信件等社交工程手段欺騙。最後，於 CTF 比賽結束後，競賽期間的資料可以用於數位鑑識之訓練。以下章節則詳細說明各部分的細節。

**2. 防御方參賽者**

承襲 CTF 比賽，主辦方需要建構數台伺服器以運行各種網路服務，包含常見之網頁伺服器，如：LAMP 伺服器，或任意語言撰寫之網路服務，如：python， c 實作之網路服務。防御方參賽者則負責維護網路服務正常運行，監控攻擊方發動之攻擊行為並進行應變。

為增加對環境真實性的模擬，此部分包含有模擬實際運行之服務環境。透過 P2V（Physical-to-Virtual）等相關技術，主辦方可將待測環境轉換為虛擬機器進行佈建，並加上額外設計之漏洞。例如：學校單位可將校園網站之伺服器轉換為虛擬機器，於競賽環境內重建虛擬之校園網站，並額外加入部分漏洞，以供參賽者競賽。

此外，近年來 Bug Bounty Program 逐漸廣泛被企業採用，但一般企業或學校組鑑於成本及知名度，難以吸引駭客們對其系統進行弱點掃描。而大多數滲透測試團隊亦難以基於駭客攻擊的思維對資訊系統進行測試。透過舉辦 CTF 的方式，可以讓網管人員了解駭客可能的攻擊手段，並可能透過此種方式找出系統弱點。

**3. 攻擊方參賽者**

攻擊方則需對防御方的伺服器進行攻擊，攻擊者可過虛擬私有網路（VPN）的方式連入比賽網路進行攻擊行為，並避免影響比賽網路以外的系統。亦可以讓參賽者使用自己習慣的攻擊環境，降低對參賽者的限制並提高攻擊方式的質量及多樣性。

不同於一般 CTF 模式，本平台嘗試引入一般使用者，以增加攻擊手段的多樣性。除了一般針對網路服務弱點進行遠端攻擊之外，攻擊者亦可透過電子郵件等手法做為媒介，進行惡意文件或惡意連結的方式進行本地端漏洞攻擊。

同樣源於引進一般使用者，攻擊方對於已攻陷機器的後續控制權變得更加重要。攻擊方可以透過植入後門以長期監控使用者並竊取後續的資料。或利用以攻陷機器進行後續的滲透攻擊。增加攻擊方對於攻擊技術的利用更加深入。

**4. 使用者安全意識測試**

與一般 CTF 競賽模式不同，此平台包含一般使用者存在以進一步模擬真實環境，提高攻防環境多樣性。一般使用者可以由主辦方組織的非技術成員擔任，或邀請一般民眾或學生參與，體驗駭客攻擊手法。

此部分可透過遠端連線等方式，讓使用者連上終端使用者設備進行操作，對每位使用者需付予一個虛擬身份及職務，主辦方則不定時利用郵件發送任務與使用者，如：上網查詢常見使用者密碼等等。而同時攻擊者亦可假造郵件誘使使用者開啓。因此參與使用者安全測試的成員，需要回答主辦方賦予的任務並同時避免落入攻擊者的圈套。此外，此部分亦可包含額外的資安測試練習，如：釣魚網站的分辨等資安相關議題，增加互動性。

**5. 數位鑑識訓練**

最後，此平台包含了數位鑑識訓練的部分，於 CTF 舉行期間，主辦方需要對網路流量進行監控與錄製。同樣的，防御方的虛擬機器映像檔以及記憶體狀況亦需要妥善保存。於 CTF 結束後，則可進行數位鑑識的訓練。此部分之參與者需要分析競賽期間的資料，嘗試找出攻擊之來源，以及攻擊所採用之手法。

總結以上架構，本平台透過延伸 CTF 競賽的機制，已涵蓋更多的資安範疇，以下總結本平台的應用範圍：

- 資安技能練習
- 滲透測試
- 使用者安全意識訓練
- 數位鑑識訓練
- 系統維護與維運訓練

於此章節最後，我們回顧於“CTF 競賽與資安實務的差異”一節中提出之不足點，並說明本平台如何解決這些問題，以延伸 CTF 競賽的能涉及的範圍，進行更全面性的資安技能訓練。

為解決缺乏真實攻防環境之問題，本系統提出利用真實運行之網路服務輔以額外加入之漏洞作為 CTF 之題目。透過實際網路服務的練習，攻擊者可以學習到更加實際的攻擊手法。而防御方亦可了解其系統潛在之威脅。

本平台接著透過引入一般使用者來解決缺乏實際使用者參與的問題，透過真實使用者之介入，攻擊手法可以變得更加多樣化，而一般網路攻擊行為中相當重要的攻擊手法，如：社交工程、惡意郵件等技術也可以引入至競賽中，增加比賽的涵蓋範圍級趣味性。另一方面，使用者方面則可以進行使用者安全意識之訓練，親身體驗駭客攻擊手法，增進對資安議題的了解。

藉由以上兩點，網路環境的多元化以及使用者的介入，攻擊成功後的延續行為重要性亦會增加。最後透過引入後續的數位鑑識分析訓練，來加強 CTF 競賽缺乏入侵行為的後續延伸的不足，來達到全面性的資安技能培訓。

## 伍、結論

為因應未來對資安人才的需求，更全面的資安培訓視為必要的。本文首先透過介紹 CTF 競賽，說明競賽之方式以及所能訓練的相關資安技能。接著說明目前 CTF 競賽 CTF 競賽與真實網路攻防環境的差異，包括了 1) 缺乏真實攻防環境、2) 缺乏實際使用者參與以及 3) 缺乏入侵行為的後續延伸。基於以上三點，本文接著提出一套“多面向攻防平台“。本平台首先透過引入一般網路服務作為競賽題目的基礎，來模擬真實的環境，不儘可以增加攻防環境的真實度，也可以讓防守芳了解攻擊者入侵的技術。接著透過加入一般使用者，一方面可以增加攻擊方的攻擊範圍與入侵手法，一方面可以提供資安意識訓練。最後則將比賽過程中的資料保存，提供後續的數位鑑識訓練。透過延伸 CTF 競賽所能涵蓋的主題，希望能踢公更全面性的資訊安全技能訓練。以應對未來對資安人才的需求。

## 參考文獻

[1] CTF TIME，https://ctftime.org/
[2] DEFCON， https://www.defcon.org/
[3] CodeGate CTF， http:// codegate.org/
[4] PlaidCTF， http://www.plaidctf.com/
[5] Ghost in the Shellcode， http://ghostintheshellcode.com/
[6] HITCON CTF， http://hitcon.org/2014/CTF/
[7] Plaid Parliament of Pwning， http://ppp.cylab.cmu.edu/wordpress/
[8] KAIST GoN， http://gon.kaist.ac.kr/
[9] Blue-lotus CTF Team， http://www.blue-lotus.net/
[10] Dragon Sector， http://blog.dragonsector.pl/