CTF 攻防競賽平台設計

趙正宇、李倫銓
國立交通大學資訊工程研究所、國立台灣大學電機工程研究所
jeffxx@chroot.org、alan@hitcon.org

Capture The Flag (CTF) 是一種資訊安全的競賽，演變至今不僅比拼的是駭客攻防的技術，甚至包含全方位的電腦科學技術，包括系統安全、演算法、密碼學以及程式設計功力，這類競賽能培訓高階資安人才，讓他們有一較高下的舞台，發展自今有兩種較常見的比賽模式 Jeopardy 和 Attack and Defense。Jeopardy 名稱來自于美國 1960 年代的智力問答節目，在有限的題目中，所有隊伍比賽解題的數量與速度，常見的題目類型有：Reverse、 Pwnable、 Crypto、 Forensics、 Misc。

- Reverse 指的是逆向工程，給一個或多個 Binary，過關所需要的 Key 通常加密藏在執行檔裡，要將程式逆向分析出後才能找出。
- Pwnable 會給一個有弱點的程式或 Server 執行檔，主辦方自己會開一台伺服器跑該服務，參賽者要透過靜態分析與動態分析來找出該程式的弱點。例如：Buffer overflow、命令注入等，在遠端伺服器利用漏洞來執行任意指令，進一步取得存在遠端伺服器的金鑰。
- Crypto 給加密過的密文、加密程式，參賽者必須分析加解密演算法甚至需要找出演算法的弱點來破解出真正的明文。
- Forensics 鑑識類型，從封包、log、memory dump、disk image、VM image 找出隱藏在之中的 key
- Misc 沒有較明確的分類，像是給個遊戲要想辦法作弊破到幾百萬分，或是給一個壞掉的 QR code 嘗試修復，或是給一張圖片要找出相關的人事物等。

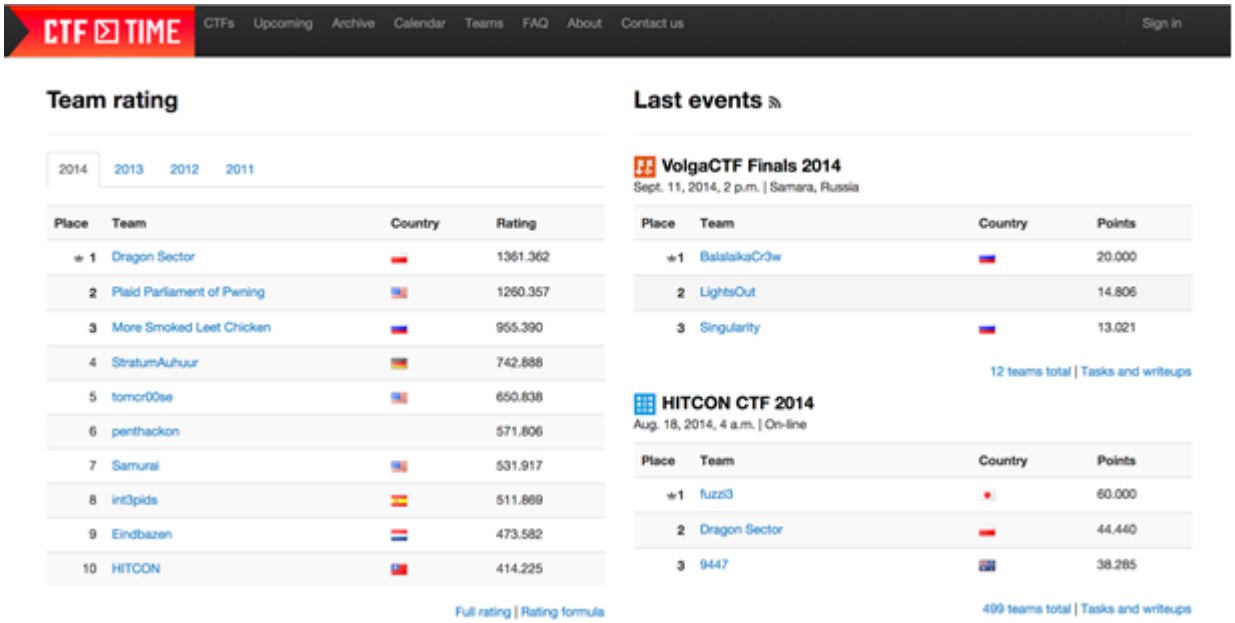
之後還衍生出各種玩法，例如最先解出題目的隊伍可以獲得開題權，或是前三名解出題目可以獲得 bonus 等。國內知名的資安競賽: 金盾獎[1]，HITCON CTF [2]都是屬於這種形態的比賽。

圖一：Jeopardy 計分板 Defcon 2012 Qual

Attack and Defense 相較於 Jeopardy 就殘酷許多，主辦單位會為所有參加的隊伍準備需要守護的伺服器，這檯伺服器上會有網頁，遊戲或其他特殊用途的服務。每個服務都有數個漏洞，漏洞可能只是簡單的資訊泄露，阻斷服務；也可能是一個嚴重的漏洞讓客戶端可以在伺服器上執行任意指令。

參賽的隊伍需要做的事情就是守護好自己的伺服器然後打進對手的伺服器偷取 Token。守護好自己的伺服器必須要能正常提供服務。若服務沒有正常運作，每一回合都會扣分，扣的分數平均分配給服務正常的隊伍。而正常運作的服務若沒有將漏洞補上，就會被其他隊伍利用來偷取伺服器上的檔案－token。只要被搶走 token，該回合一樣被扣分，由搶到該 token 的隊伍平分。

每種服務都會獨立計算，所以如果同時數個服務都被打穿，一回合掉的分數是極為驚人的。通常這種形態的比賽都是現場賽，持續兩到三天。長時間的比賽除了比拼技術實力外，還要拼體力與意志力。



圖二：CTFTime 世界隊伍排名及比賽列表，截稿時台灣 HITCON 戰隊排行世界前十

CTF 於近幾年蓬勃發展，2011 年俄國強隊 More Smoked Leet Chicken 架設了一個提供 CTF 資訊的網站-CTFTime[3]，讓許多不得其門而入的人有獲取比賽資訊的管道，去年度世界上大大小小的 CTF 共計超過 50 個。此外 CTF Time 設計了評分制度，不同比賽的規模，名氣，題目難度，參加人數，舉辦方實力，是否提供獎金等等，都會影響該比賽的權重。以世界公認大賽 Defcon[4]為例，奪得 Defcon 初賽冠軍的隊伍獲得 160 分，而奪得其他較小型或首次舉辦的 CTF 冠軍只能獲得 20 分，此機制使各國戰隊的戰力能有相對客觀的比較，不再只是靠 Defcon Final 競賽的名次來評估實力，各地隊伍也更加積極參與比賽。

其中 Defcon CTF Qual （初賽）是一年中競爭最激烈的比賽。全世界一千多個隊伍在三天三夜的比賽中爭奪 12 個決賽名額，許多團隊在這場比賽通常會選擇跟其他隊伍合併，嘗試用較強的戰力取得決賽資格。最後搶到門票的 12 隊加上 8 個種子賽冠軍隊伍(Defcon final、RuCTFe、Ghost in the shellcode、Olympic CTF、Boston Key party、Codegate Final、PHDays、Secuinside) 會在每年於拉斯維加斯舉辦的 DEFCON 會議進行更刺激的 Attack & Defense 形式的 Defcon CTF Final。

Attack and Defense 形態的比賽，參賽門檻高，參加隊員需要有獨立漏洞挖掘的能力，並且要能在短時間內實作成自動攻擊程式，幫執行檔打補丁，熟稔 Unix 系統防禦其他隊的攻擊等，導致一般的隊伍很難自行舉辦練習賽來累積比賽經驗。且除了較大規模的 CTF 會在決賽時採用 Attack and Defense 形式外，大部份的比賽都是 Jeoparady 形式。這也導致就算有新隊伍打進決賽也很容易因為參賽經驗不足而很難取得好成績。

亞洲國家在這方面的發展落後于歐美，過去幾屆的世界冠軍都在歐美的隊伍中產生，韓國日本大陸已意識到這個問題，韓國於 2012 年開啟了 Best of Best 的計劃：從高中與大學生中，選出 60 名有電腦專才的學生，培訓至今已淘汰 40 人。但從今年 Defcon Final 的參賽隊伍組成可以看到韓國的 BOB 計劃有顯著的成果-20 隊裡面有 1/4 是韓國的隊伍。大陸自去年 Blue-lotus 戰隊首次進入 Defcon Final 之後，也興起了 CTF 的風潮，一年內舉辦超過五個 CTF 競賽，Blue-lotus 戰隊憑藉參賽經驗舉辦了兩岸第一次的 Attack & Defense 形式 CTF -百度杯[5]，提供高額獎金引發媒體關注。

而台灣 HITCON 戰隊，若沒有百度杯的 Attack and Defense 參賽經驗，今年在初賽最後一刻才僥倖進入 Defcon 決賽的 HITCON 戰隊未必能取得如此好的成績。台灣迫切需要一個自己的 Attack & Defense 系統，培養新一代的電腦科學人才。

圖三：理想的 Attack & Defense 戰場呈現

HITCON 戰隊目前正在開發一個理想中的 Attack & Defense 系統：容易部署、系統架構簡單、擴充性高及最重要的-戰況的呈現。前面三點較容易達成，將報名、計分版、送交 Token、訊息發佈等功能整合到同一檯伺服器上；撰寫自動部署程式，啟動符合隊伍數量的虛擬機器，植入該次比賽所會用到的服務程式；再用自動化腳本程式更新每回合的 Token，檢查服務存活狀態，更新資料庫；參賽者僅需透過 VPN 連線至虛擬的網路進行比賽。在這樣的規劃下，只需要一部效能不錯的伺服器就能舉辦規模在 20 隊左右的 Attack & Defense 比賽。

戰況的呈現很難做好，在過去 Attack & Defense 比賽中做的最好的是百度杯，做了一個戰場圖，將隊伍送 Token 的動作用攻擊的動畫呈現在戰場上，讓非相關背景的觀眾也能感受比賽刺激程度。而我們希望能在這方面做得更好，戰場不應該只呈現攻擊的事件，隊伍自己做的防守動作，攻擊失敗等這些訊息應該都要能呈現在戰場動畫上。最終

呈現出來的效果應是隊伍被攻擊，戰場上的基地會被破壞；隊伍若更新了服務的程式，據點會恢復成未破壞的狀態；發出了無效攻擊的話則會被基地的防護罩擋下。有了好的戰況呈現，就能增加比賽的可看性，吸引更多的觀眾，普及全民的資訊安全意識。

今年在 8 月舉辦的 HITCON CTF 競賽，第一次改成線上，並開放給國際參賽，由 HITCON 戰隊負責出題，而形式仍保持 Jeopardy，因為今年 HITCON 戰隊才獲得 DEF CON CTF 第二名的緣故，吸引了許多國際知名隊伍參賽，總參賽隊伍數達 1020 隊，在 CTFtime 排名前 30 名隊伍有 14 隊參賽、前 100 名隊伍有 45 隊參賽。另外共 500 隊得分大於零，此數據已超過 DEF CON 初賽，所有題目也都至少有一隊解出，顯示題目設計的正確性，賽後題目水準也獲得國際高手的讚揚。本次競賽也運用了國內 hicloud 雲端服務來做為比賽平台，在效能上和穩定度都有不錯的表現。未來此類 Jeopardy 形式的 CTF 競賽日益成熟，而雲端服務隨租即用的特性，頗適合擔任此一平台角色。

參考文獻

[1] 資安技能金盾獎，https://security.cisanet.org.tw/
[2] 台灣駭客年會 HITCON CTF，http://ctf2014.hitcon.org/
[3] CTFtime，https://ctftime.org/
[4] Defcon 官方網站，https://www.defcon.org/
[5] 百度杯官方網站，http://bctf.cn/