# Jeffxx Blog

隨手筆記.

- RSS

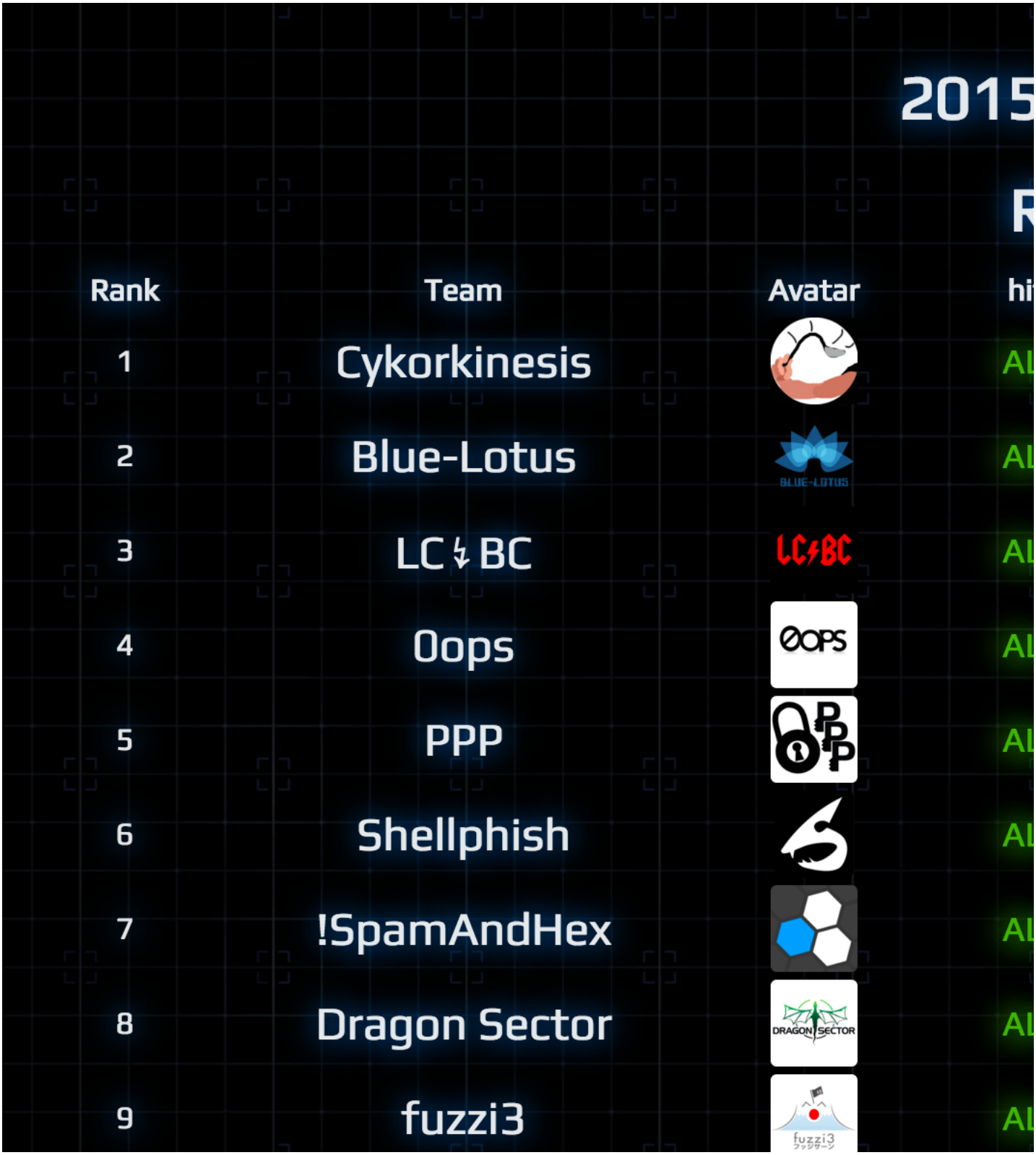
Search

Navigate...

- Blog
- Archives

## HITCON CTF Final 2015 小記

Dec 7th, 2015




自從 Defcon Final 回來後就在各種死線中徘徊，其中的心路歷程跟掙扎就不提了，記錄一下 HITCON Final 中比較有印象的事件。

這次系統是拿年初台交賽的平台出來重建的，由於這次參賽陣容太過豪華，讓我一直擔心系統撐不住這些隊伍的攻擊能力。*//掛了怎麼對題目組場佈組行政組交代*

結果第一天的回合更新時間真的從一開始的1.5秒完成慢慢成長到5秒才能完成。當天晚上緊急優化一堆東西才撐住第二天最後兩小時的Turbo Mode

如果仔細看戰場的log會發現有時候會有隊伍同時間成功攻擊同一個隊伍多次，這是因為在寫入資料庫時雖然有先檢查本回合有沒有攻擊成功的記錄，但檢查完到真正存進 DB 時沒有 Lock 住，若隊伍送太快就會發生Race Condition。 在預期每秒會有幾百次 submit flag 請求的情況下，我選擇讓 Race Condition 發生，最後回合統計時再將這些重複的記錄刪除。


217 Round 是碰巧的，討論時只有考慮加速的時間要多久比較恰當，最後結束出現 217 時我也嚇一跳，但我都騙人說是算好的XD

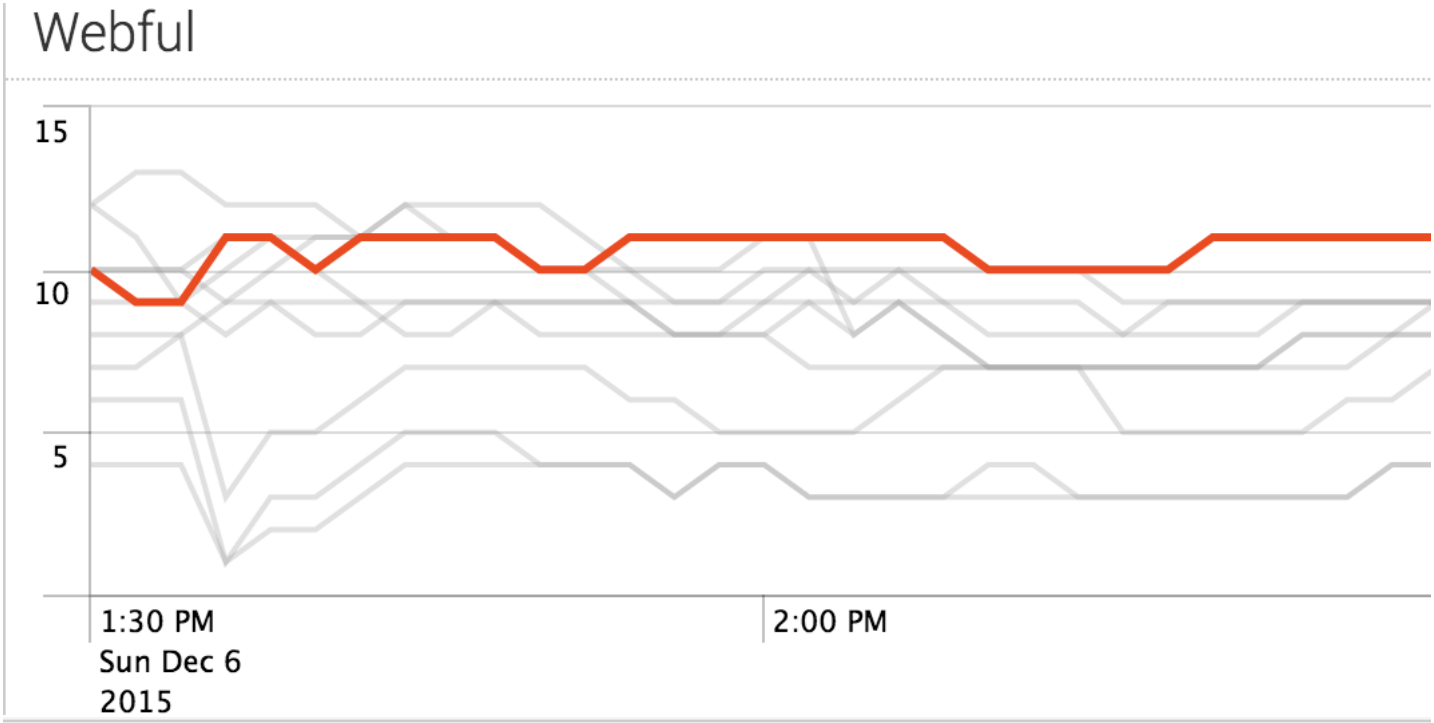
> 美國聖塔芭芭拉大學組成的 Shellphish隊伍是資深的CTF戰隊，曾經在今年八月臺灣駭客年會企業場來臺灣演講的隊長Antonio Bianchi除了肯定HITCON團隊活動舉辦的很好外，他也提出一些建議，可以改善一些小細節讓活動更完美，其中，他最在意的就是計分版的放置位置，他指出，他們會需要從計分版中獲得很多重要的資訊，但可能因為場地限制，他們必須親自走到計分版前觀看，相對不方便。但除此之外，他和團隊成員Amat Cama及Nick D. Stephens都對於HITCON團隊辦活動表現讚譽有加。

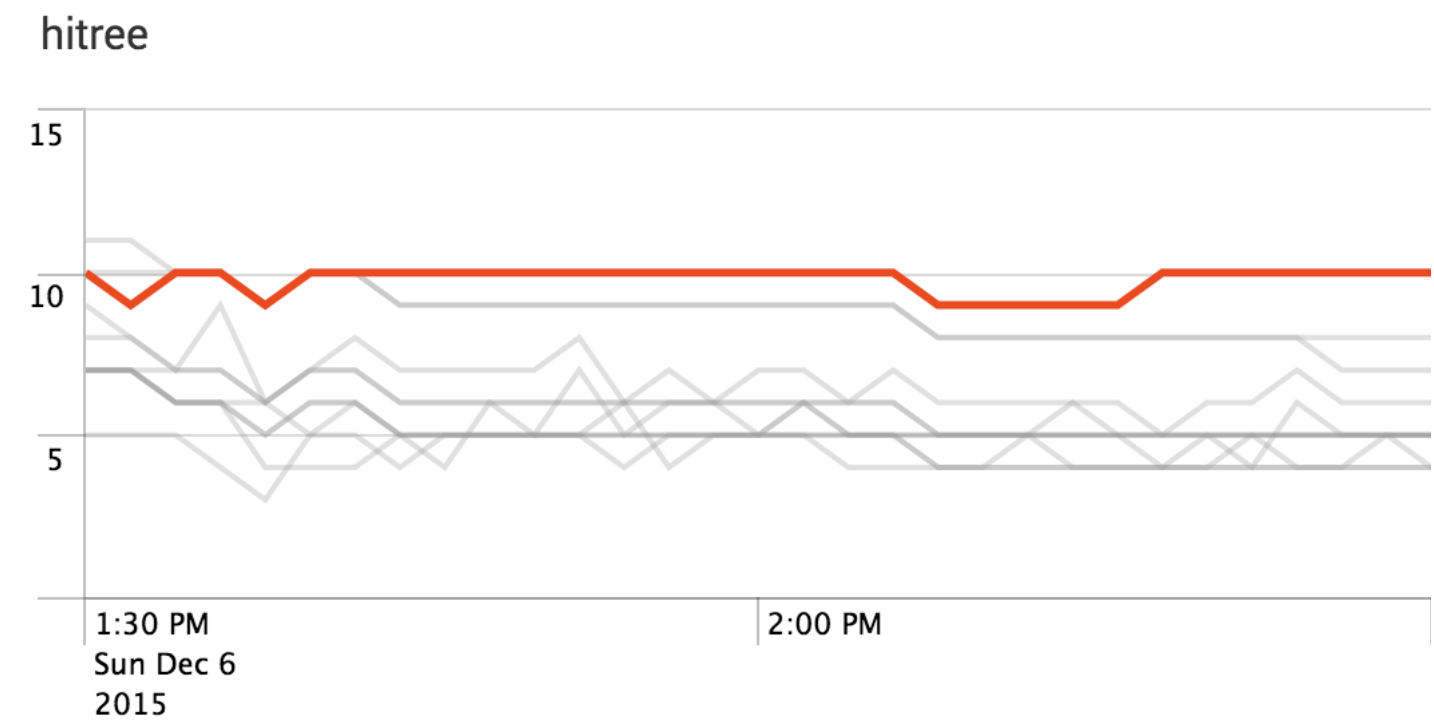
我也是看報紙才知道原來有隊伍抱怨計分板。

最一開始規劃是要將戰場也開放給參賽者的，但是一直到週六凌晨四點還是修不掉 Rails-websocket 所有人都可以廣播訊息的問題，不得不忍痛放棄開放給參賽者。 原本做了許多跟參賽者互動的功能最後也只能在大螢幕上秀給大家看了。

這次場地已經算非常不錯了*除了喇叭有點悲劇*，投影幕 + 電視足足有七個。 我們只投影 計分板 跟 戰場 並確保每一隊一抬頭就可以看到計分板跟戰場，除了正對著大螢幕的 cykor 外，其他隊伍要看到戰場 detail log 都要走到螢幕前。* Cykor從頭到尾屌打全場，他們應該不care到底要不要走過去看的問題 *

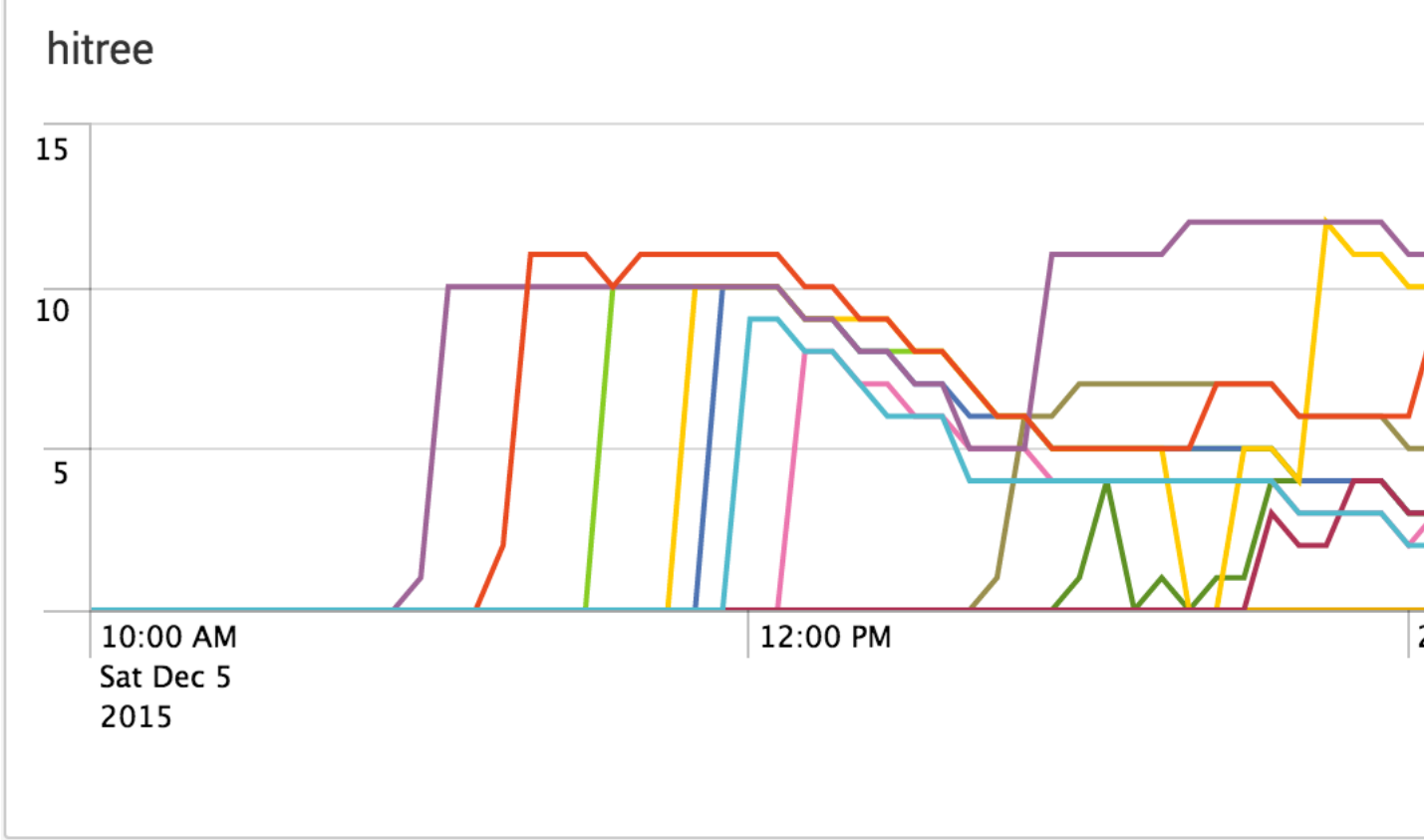
不過外國人真的很NICE，我們的英文實在太爛了，常常外國人跑來問問題，被問的人一個抓一個求救，每一個的反應都是:蛤？，同一個問題重複三四次也不會生氣。*Sean表示:只有你們英文這麼爛*

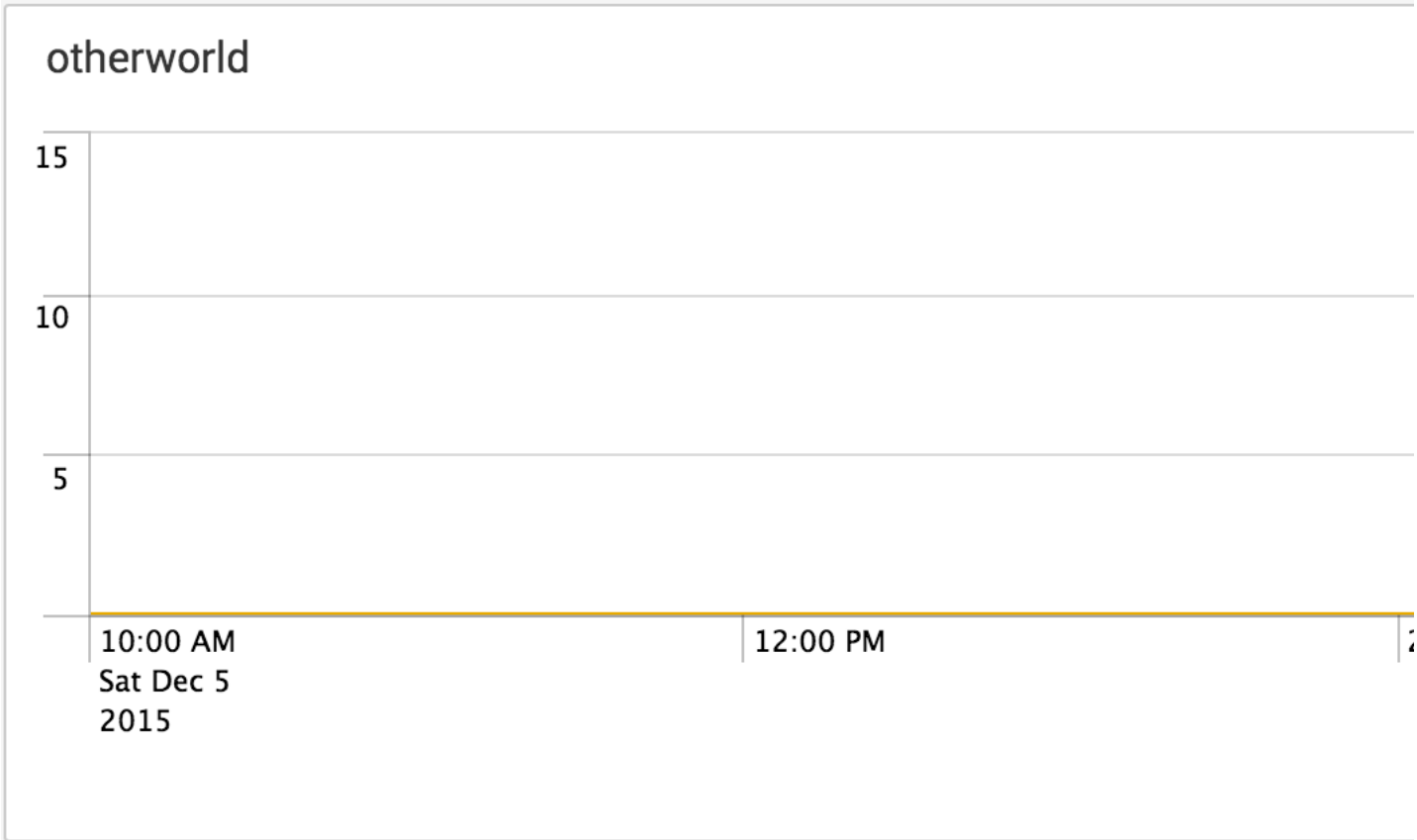



最後兩小時Turbo Mode Webful & hitree Flag Submit 狀態

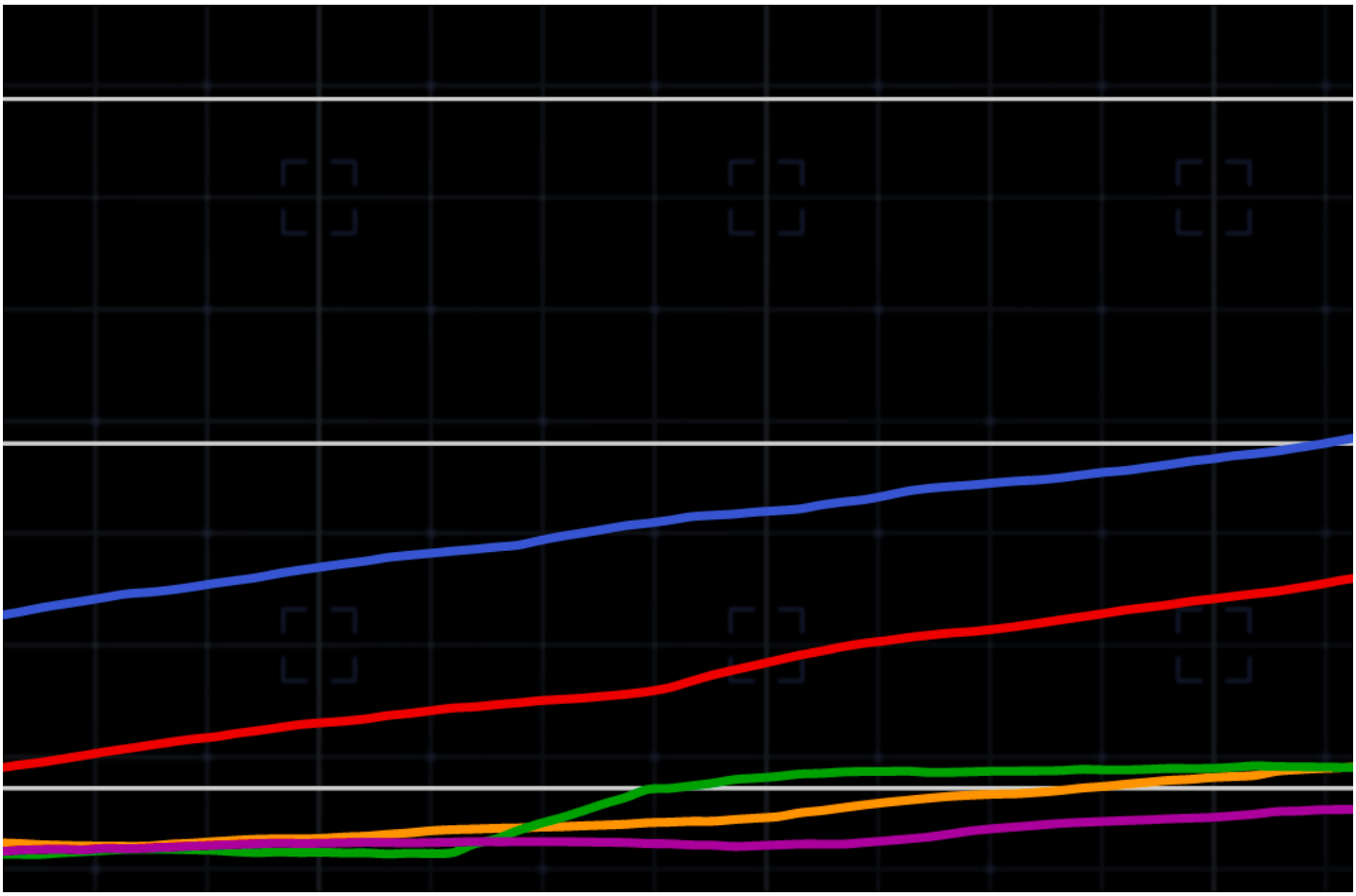
Cykorkinesis 有如 bug 般的 Binary 能力碾壓整場比賽，每道題目的獲得的flag數量在大多數時間都是前三名。當各隊伍陸續Patch後，他們可以放出更進階的攻擊再次搶到 Flag 。 如果只是Binary開外掛就算了，Web題到最後掌握度也是數一數二，韓國的 BoB 計畫不知道到底培養出多少技術這麼好的資安人才。




第一天 Binary Flag Submit 狀態

Bluelotus 展現了令人敬畏的封包分析能力，可以從第一天如屎一般的封包中迅速找出攻擊流量並實現重放攻擊/*楊坤表示: 我以為你們是故意讓我們的工具無法使用*/，三道 Binary 題目都是第二個成功重放的隊伍，而且重放還可以比原版多打一隊真的不知道怎麼回事。



PPP, 0ops LC↯BC 拉鋸了非常久，許多人驚訝 PPP First Blood了兩題，竟然最後還是被超過去。其實題目都有簡單的洞跟困難的洞， PPP 有作出較難的exploit，但不知為何有超過半數的隊伍直到比賽結束都沒有Patch最簡單的漏洞，導致他們開發更進階的exploit獲得的效益很有限。*/只要成功搶到flag就會平分分數，不管用困難或是簡單的漏洞/*

最後講講 LC↯BC 神奇的逆轉，Orange第一天一直在說沒有人發現他在 webful 埋了一個 DoS 的漏洞。沒想到第二天最後兩小時，我們把回合加速、及時分數顯示關掉後 LC↯BC 立刻發動了 webful 的 DoS 攻擊，將所有隊伍的 Service 打掛，獨得所有Webful Service Down 的分數 (隊伍服務不正常時會扣 26 分, 平均分配給服務正常的隊伍)，在其他隊伍都在專心檢查有沒有被攻擊時，利用戰場 Service Down 效果較不起眼的優勢 默默的以每回合成長兩三百分的速度追過了 PPP 與 0ops。

而台灣隊伍 Bamboofox-DSNS 反應非常迅速，在沒辦法短時間內找出洞補上的情況下，選擇使用人力手動重啟服務，硬是通過了幾次服務檢查，從 LC↯BC 手中分了不少分數，追過 WesternTokyo 和 Samurai，在等同於Defcon決賽隊伍名單的比賽中獲得第十名的好成績。

最後的最後，感謝所有的人，這次最大的收獲就是認識了很多國內外的新朋友，也謝謝大家在過程中忍受我的爛脾氣/ *尤其是Alan Orz* / 。

Posted by cychao Dec 7th, 2015

Tweet

« Defcon 22 Final HITCON 參賽心得 (下)

## Recent Posts

- HITCON CTF Final 2015 小記
- Defcon 22 Final HITCON 參賽心得 (下)
- CSAW CTF 2014 Forensics 300 Fluffy No More Write-up
- Defcon 22 Final HITCON 參賽心得 (上)
- Defcon 22 Qual Sick Writeup