

## 106 年度臺灣學術網路危機處理中心資安巡迴研討會

### -網路威脅手法暨 DDoS 分析

#### 一、計畫目的

臺灣學術網路危機處理中心(Taiwan Academic Network Computer Emergency Response Team, 簡稱 TACERT)為加強臺灣學術網路(TANet)網站安全防護能力，辦理「106 年度臺灣學術網路危機處理中心資安巡迴研討會-網路威脅手法暨 DDoS 分析」，本次研討會重點在於推廣使用開放原始碼(Open Source)來強化校園的網站安全防護能力。

#### 二、辦理單位

- 指導單位：教育部
- 主辦單位：臺灣學術網路危機處理中心(TACERT)
- 協辦單位：高屏澎區域網路中心-國立中山大學圖書與資訊處  
臺北區域網路中心-國立臺灣大學計資中心  
北區教育學術資訊安全監控中心(N-ASOC)  
南區教育學術資訊安全監控中心(S-ASOC)  
AISAC 暨 miniSOC 計畫團隊(逢甲大學)  
教育單位網站資安防護服務計畫(國立成功大學)

#### 三、參與對象：

臺灣學術網路區域網路中心、各縣市教育網路中心、公私立大專院校、公私立高中職網路管理或資安相關負責人員

#### 四、梯次、日期及地點

地區	日期	地點	人數限制
高雄	8/10(四)	國立中山大學 管理學院 管 CM1037 演講廳	105 人
臺北	8/17(四)	國立臺灣大學 應用力學館 R100 國際會議廳	238 人
高雄	8/24(四)*	國立中山大學 圖書與資訊處 B1 電腦教室 PC03	60 人 (上機課程)

\*8/24 的高雄場次上機課程，重點在教授開放原始碼資安軟體，旨在建立合適的開源碼網管系統。建議參與此課程之學員需對 SQL 資料庫有基礎認識。

## 五、課程大綱及議程

### ■ 8月10日高雄場次及8月17日臺北場次

從網際網路(internet)興起以來，阻斷服務攻擊(denial-of-service attack，縮寫 DoS)即如影隨形的伴隨著 internet 成長。由於其攻擊門檻較低，DoS 攻擊早已成為最常見的資安事件。在本研討會中除了說明最為人所知的洪水(flood)封包攻擊外，另外，也將從程式設計及通訊協定的角度切入，闡述另一種型態的 DoS 攻擊，並提供相關建議措施，來降低 DoS 攻擊危害。另一方面，IoT(物聯網)逐漸的走入我們的生活，此新興應用所衍生的資安問題也日趨嚴重，我們也將在研討會中探討相關議題。

最後，我們也將針對今年的嚴重資安事件，包括 Apache Struts 2 及 WannaCry(勒索蠕蟲)等事件分享相關心得。

時間	議題	講師
9:00~9:30	報到	
9:30~10:30	學術網路安全趨勢分析與資安個案分享	張明達
10:30~10:40	中場休息	
10:40~12:00	網路威脅事件分析	吳惠麟
12:00~13:00	午餐時間	
13:00~14:40	DDoS 手法分析-1	吳惠麟
14:40~15:00	中場休息	
15:00~16:30	DDoS 手法分析-2	吳惠麟

### ■ 8月24日高雄上機課程

在遇到系統異常的情況，相信管理者的第一個念頭通常就是去看看記錄檔中的記錄看看到底發生了什麼事。往往系統記錄檔可以告訴我們許多的線索，甚至從其中可擷取許多有價值的資訊，但一般的記錄檔通常都是儲存在不同的文字檔案中，對於相關資料分析統計的應用總有力有未逮之憾。

因此在本研討會中，將帶領學員如何利用開源碼資源建構一個可將 Apache 網站伺服器所產生的網站記錄(LOG)記錄儲存在資料庫(mysql)，利用資料庫的方法來解讀相關網站記錄(LOG)

時間	議題	講師
9:00~9:30	報到	
9:30~10:40	開源碼主從式網站記錄(LOG) 系統建置-1	吳惠麟
10:40~10:50	中場休息	
10:50~12:00	開源碼主從式網站記錄(LOG) 系統建置-2	吳惠麟
12:00~13:00	午餐時間	
13:00~14:40	網站記錄(LOG)分析-1	吳惠麟
14:40~15:00	中場休息	
15:00~16:30	網站記錄(LOG)分析-2	吳惠麟

#### 六、報名方式

- (一)、報名網址 <http://tacert.mis.nsysu.edu.tw>，本研討會為免費參加，中午提供便當，採網路報名方式自行選擇參加梯次，並依報名先後順序額滿為止。
- (二)、8月24日高雄上機場次報名時間自7月25日9:00起至8月11日17:00止，名額限60名(額滿提前結束)。
- (三)、本研討會提供公務員終身學習時數認證或教師研習時數6小時。
- (四)、本研討會無法支付來賓停車費，敬請與會人員多搭乘大眾運輸工具。
- (五)、響應環保節能，本研討會不提供紙本講義，敬請與會人員自行於報名網站下載研討會講義電子檔(講義電子檔將於106年8月1日公佈於報名網站)。
- (六)、聯絡人：陳小姐。電話：(07)525-2000 轉 4771；E-mail：[kate0814@cert.tanet.edu.tw](mailto:kate0814@cert.tanet.edu.tw)。

■ 106年8月10日(四)國立中山大學管理學院 1樓管 CM1037 演講廳

地址：高雄市鼓山區蓮海路70號

交通方式：<http://www.nsysu.edu.tw/files/11-1000-4132.php>



- (1).高雄場次開車前往的來賓，請將車子停於來賓收費停車場，否則會遭本校車管會拖吊，汽車拖吊處理費壹仟參佰元，機車拖吊處理費伍佰元，敬請合作。
- (2).來賓收費停車場汽車一天收費 60 元，機車不需費用，停車費用請與會人員自行吸收。
- (3).若搭乘高鐵者，可直接搭乘西城快線直達本校。西城快線班次表：  
<http://www.stbus.com.tw/cityrouteE05.htm>
- (4).若搭乘高雄捷運者，可由西子灣站 2 號出口(鼓山一路)出站，再轉搭橋 1 接駁車(每 30 分一班車)至中山大學行政大樓下車。(橋 1 時刻表：  
<http://southeastbus.com/index/kcg/O1A.html>)

■ 106年8月17日(四)國立臺灣大學 應用力學館 R100 國際會議廳

地址：台北市大安區羅斯福路四段1號

交通資訊：<http://www.iam.ntu.edu.tw/conference-room>

應用力學館位於楓香道與桃花心木道口



- (1).臺北捷運新站線：公館站(羅斯福路大門進入)
- (2).臺北捷運文湖線：科技大樓站（沿復興南路往南走約 250 公尺由辛亥路校門進入）
- (3).停車資訊(停車費率若有調整，依各停車場公告為準)：於研討會櫃台蓋章享優惠價。
  - 校園停車格 30 元/30 分鐘，優惠價 15 元/30 分鐘
  - 辛亥地下停車場(入口：進辛亥路校門約 40 公尺右側，出口：辛亥路 2 段)
    - 汽車：20 元/30 分鐘，優惠價 10 元/30 分鐘
    - 機車：20 元/次，優惠價 10 元/次

■ 106年8月24日(四)國立中山大學 圖書與資訊處 B1 電腦教室 PC03

地址：高雄市鼓山區蓮海路70號

交通方式：<http://www.nsysu.edu.tw/files/11-1000-4132.php>



- (1).高雄場次開車前往的來賓，請將車子停於來賓收費停車場，否則會遭本校車管會拖吊，汽車拖吊處理費壹仟參佰元，機車拖吊處理費伍佰元，敬請合作。
- (2).來賓收費停車場汽車一天收費 60 元，機車不需費用，停車費用請與會人員自行吸收。
- (3).若搭乘高鐵者，可直接搭乘西城快線直達本校。西城快線班次表：  
<http://www.stbus.com.tw/cityrouteE05.htm>
- (4).若搭乘高雄捷運者，可由西子灣站 2 號出口(鼓山一路)出站，再轉搭橋 1 接駁車(每 30 分一班車)至中山大學行政大樓下車。(橋 1 時刻表：  
<http://southeastbus.com/index/kcg/O1A.html>)