2019-06-11　108年北區區網管理委員會第**1**次會議

一、區網中心報告

1.圖書館網頁無法連線？

使用telnet、ping、　80 or 81　or 3389 觀察TTL值

2.DDOS攻擊

外對內：DNS反射攻擊20190124考場公佈

20190303-0305 max 25-130Gbps

觀察與解決方式:

使用區網中心mrtg圖（流圖、封包）

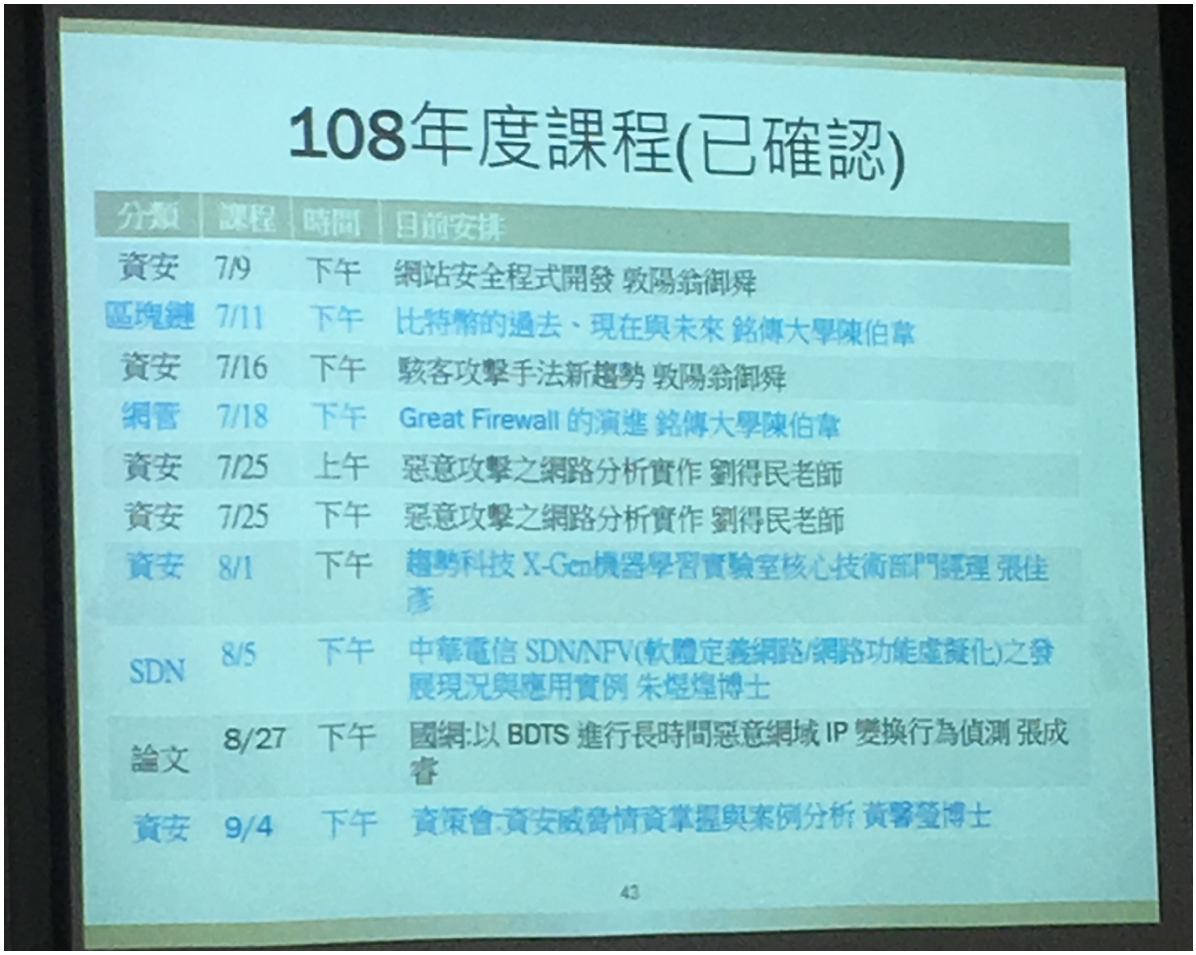
或使用設備阻檔：如大同使用：A10 3030s(Inline)

ASOC-清洗DDOS流量(概念：Home Non-Home)

外對內-可以清洗

內對外-比較難以清洗

3.108年度台大課程

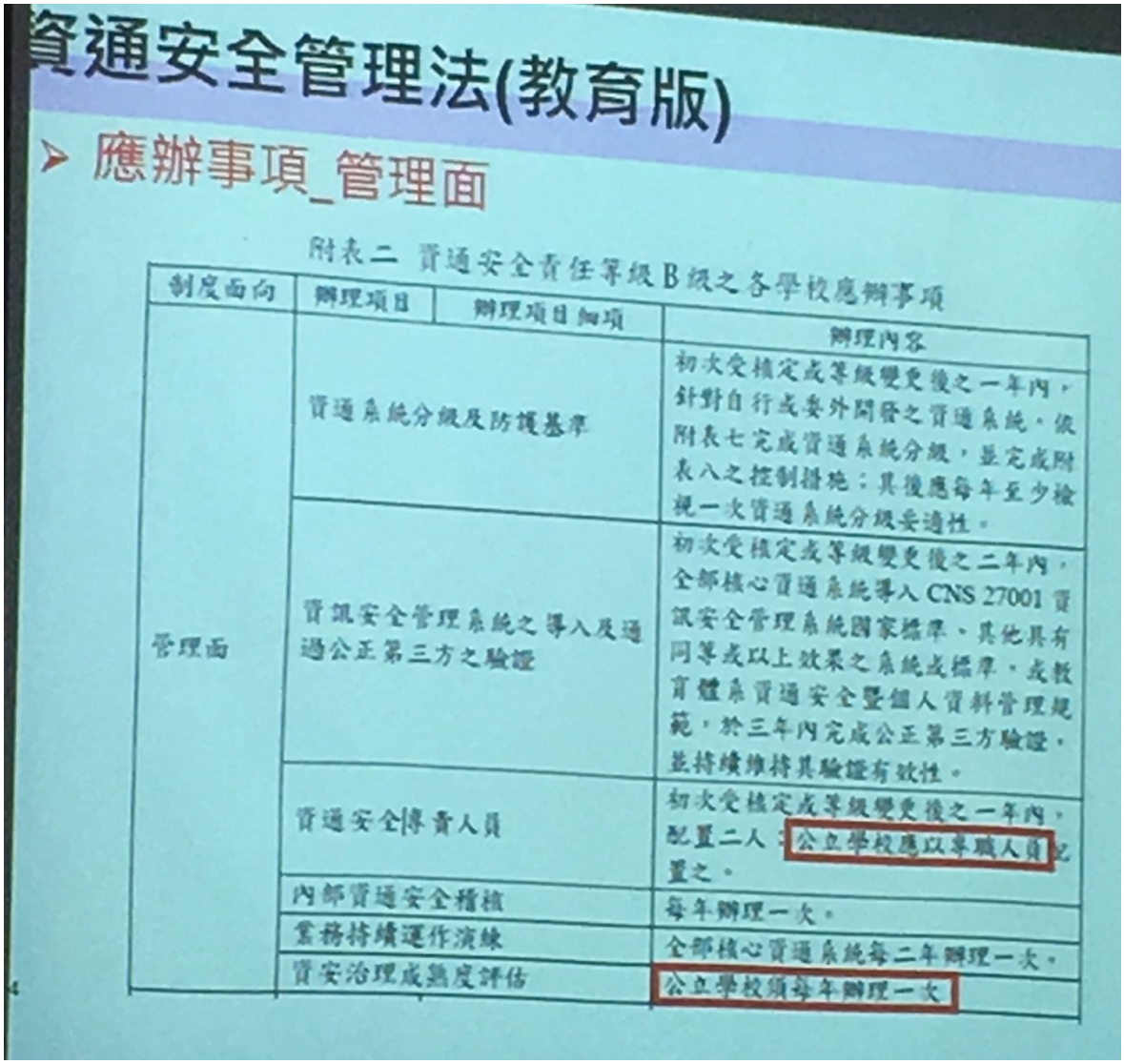


108年度課程(已確認)

分類	課程	時間	目前安排
資安	7/9	下午	網站安全程式開發 敦陽翁御舜
區塊鏈	7/11	下午	比特幣的過去、現在與未來 銘傳大學陳伯韋
資安	7/16	下午	駭客攻擊手法新趨勢 敦陽翁御舜
網管	7/18	下午	Great Firewall 的演進 銘傳大學陳伯韋
資安	7/25	上午	惡意攻擊之網路分析實作 劉得民老師
資安	7/25	下午	惡意攻擊之網路分析實作 劉得民老師
資安	8/1	下午	趨勢科技 X-Gen機器學習實驗室核心技術部門經理 張佳彥
SDN	8/5	下午	中華電信 SDN/NFV(軟體定義網路/網路功能虛擬化)之發展現況與應用實例 朱煜煌博士
論文	8/27	下午	國網:以 BDTS 進行長時間惡意網域 IP 變換行為偵測 張成睿
資安	9/4	下午	資策會:資安威脅情資掌握與案例分析 黃馨瑩博士

二、資安分享

1.資通安全管理法：



專職人員：某次行政院會議說明專職人員指公務人員，教育體系部分會在說明

（台大李oo轉述）

2.各軟體漏洞，請更新

WinRAR-unacev2.dll upgrade to 5.7.0
ShadowHammer Asus ->asus
Windows RDP CVE-2019-0708 MS_T120
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0708#ID0EWIAC

三、弱掃平台相關說明

1.網頁弱掃：請多加利用

2.未來上線：主機弱掃功能

3.資安通報，請注意1小時內通報完成。

四、**BGP Hijacks**

case:2018/11/19中華電信網路大當機

類型：

BGP OUTTAGES
BGP Hijacking
  partial
  complete
BGP Leaks

可搭配確認：https://bgpstream.com 、https://bgp.he.net/cc

五、**shodan & OpenVAS**

1.shodan 搜尋引擎(網路攝影機等)

需註冊

2.OpenVAS—>Greenbone Community Edition(70%商業版功能）

https://secinfo.greenbone.net/login/login.html (UI demo)

Nessus為開發，約有7萬筆弱點掃描提供

參考資訊：vulners.com

可搭配 shodan 搜尋+Greenbone api(json,…etc)組合弱掃工具。