107年度南投區域網路中心管理委員會

時間：107年02月05日（星期一）中午12點
地點：國立暨南國際大學-圖資大樓1樓會議室
主席：黃育銘主任

主席致詞

區網中心報告

- ✓維運報告
- ✓IPv6 推廣
- ✓弱點掃描平台介紹
- ✓教育訓練課程討論

維運報告

維運報告

影響連外網路事件三件

事件一：亞太A4及A7光纜斷線影響南投區網連外網路	
影響時間	106/12/8日09:19至12:44
影響範圍	透過科技大樓連外之線路
說明	科技大樓目前還是中華電信出口，而目前南投區網連到科技大樓出口是透過其他電路到達並非直達，本次受影響線路雖然是“台灣大學-台北主節點、東華大學-台北主節點”這兩條，但因為台灣大學-台北主節點斷線，導致出口流量滿載，流量僅剩10G，故影響其連外網路。

維運報告

影響連外網路事件三件

事件二：Paloalto CPU 使用率異常	
影響時間	107/01/16日20:07至20:15
影響範圍	南投區網連外線路
說明	網路異常有 loss 狀態 Paloalto CPU 使用率異常，經查後有一筆特別的資料換算此 session 一共持續了34小時傳輸57G的資料。 起 2018/1/15 08:04 迄 2018/1/16 20:09 CPU 過高跟結算此 session 資料有關。

維運報告

影響連外網路事件三件

事件三：網路異常有 loss 狀態	
影響時間	107/01/22日5:15至5:45
影響範圍	南投區網連外線路
說明	Paloalto CPU 使用率正常但是 session 使用狀況有異常，時間內有大量被欄的 session limit 約30分鐘統計有 1,100,000 筆，造成 loss 原因是超過 Paloalto new session 的能力。 備註：目前 Paloalto 每秒有120,000 new session的能力，目前session limit設定每秒2,000筆並drop

維運報告

不影響網路之事件兩件：

107/1/10日 三育中學斷線	光電轉換模組異常，重開光電轉換模組後恢復正常
107/1/12日 1:00 機房冷氣異常	冷氣異常跳脫導致骨幹區溫度過高、重開冷氣後溫度恢復正常

IPv6推廣

106年度年終審查評審建議:區網中心持續推動IPv6連線支援能力，並將IPv6連線概況呈現於區網中心網頁。

- 優點
  - 連線大網站，例如: google、facebook等速度較快
  - IPv6 位址數目大於目前 IPv4 位址的配發量，地址更多
  - 更安全: IPv6 協議下的路由表更小，聚合能力更強，數據轉發所經過的路徑會更短，數據包無需像IPv4那樣經過太過錯綜複雜的中轉
- 缺點
  - Switch/Router 中的 Table 可能會不夠用
  - 如連線網頁 IPv6 設定有誤，會無法連線
    - 常見於公家單位網頁
    - 解決與測試方法，關閉本機 IPv6 以 IPv4 連線就可解決

IPv6推廣

IPv6設定需求表：

需設定項目	使用者本機端	Web服務
Router/防火牆	O	O
DNS	O	O
DHCP	O	X
OS	XP(含)以上	Win2008

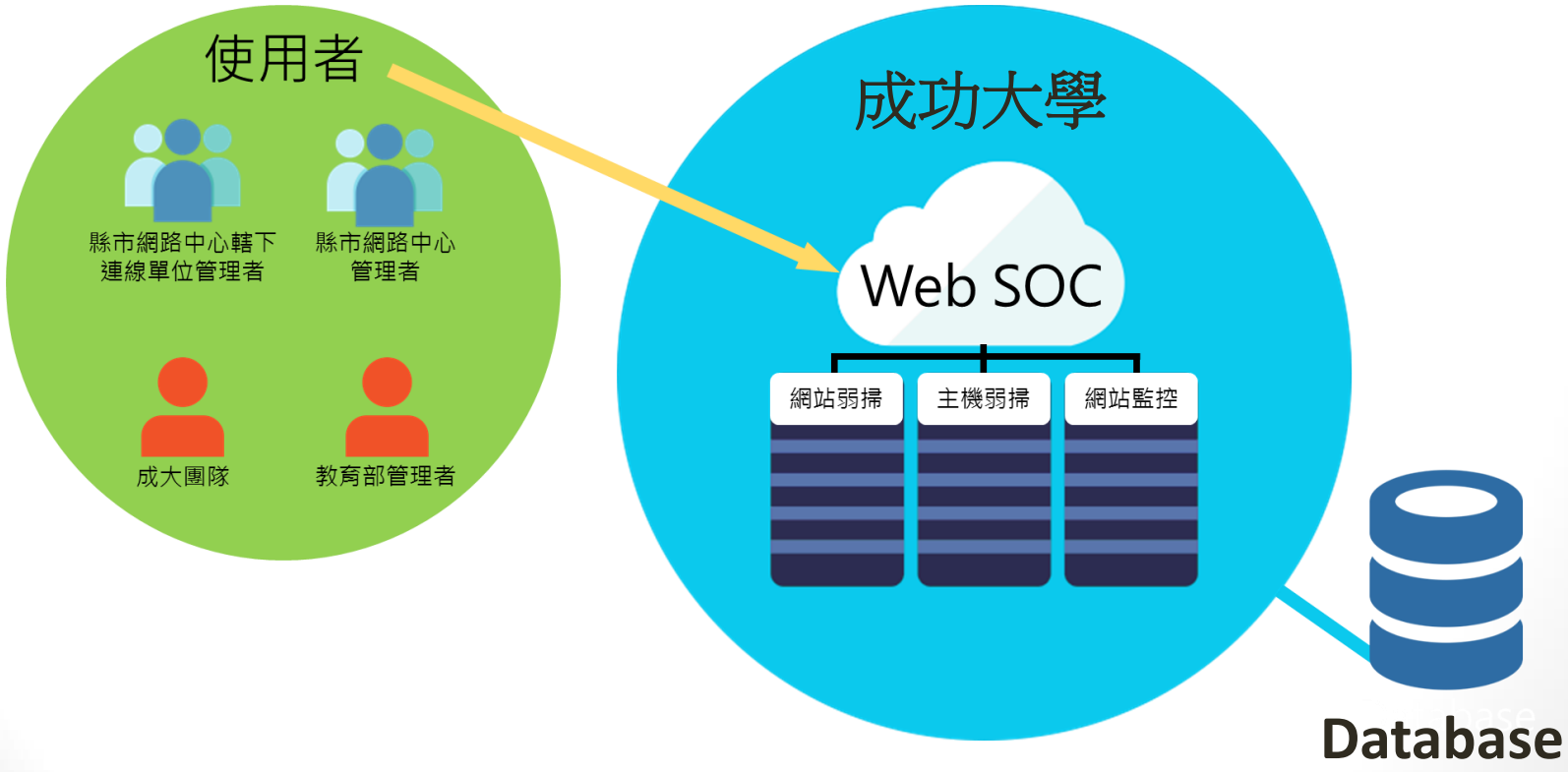
IPv6推廣

- 區網提供服務
  - ✓至各連線單位協助設定 IPv6
  - ✓協助遠端測試 IPv6

弱點掃描平台介紹

弱點掃描平台介紹

- 教育單位網站資安監控中心服務架構



弱點掃描平台介紹

成大團隊建置之教育單位網站資安監控中心，現階段可提供以下服務：

- ✓網站應用程式弱點掃描服務
- ✓網站主機弱點檢測服務
- ✓網站運作與內容監控服務

弱點掃描平台介紹

- 掃描項目-依據 OWASP（The Open Web Application Security Project，開放網站應用程式安全專案）歸納出的十大網路資安風險（OWASP Top 10）

項次	弱點名稱
A1	注入攻擊(SQL Injection)
A2	無效身分認證和Session管理(Broken Authentication and Session Management，BASM)
A3	跨站腳本攻擊(Cross-Site Scripting，XSS)
A4	無效的存取控管(Broken Access Control)
A5	不安全的組態設定(Security Misconfiguration)
A6	敏感資料外洩(Sensitive Data Exposure)
A7	API攻擊防護不足(Insufficient Attack Protection)
A8	跨站請求偽造(Cross-Site Request Forgery，CSRF)
A9	使用已有漏洞的元件(Using Components with Known Vulnerabilities)
A10	API未受防護(Underprotected APIs)

弱點掃描平台介紹

- 弱掃平台網址 https://evs.twisc.ncku.edu.tw/
- 掃描網域僅限於**edu.tw**
- 首先需向成功大學申請帳號密碼

  聯絡資訊：evs_service@mail.moe.gov.tw

  電話：06-2761204

弱點掃描平台介紹

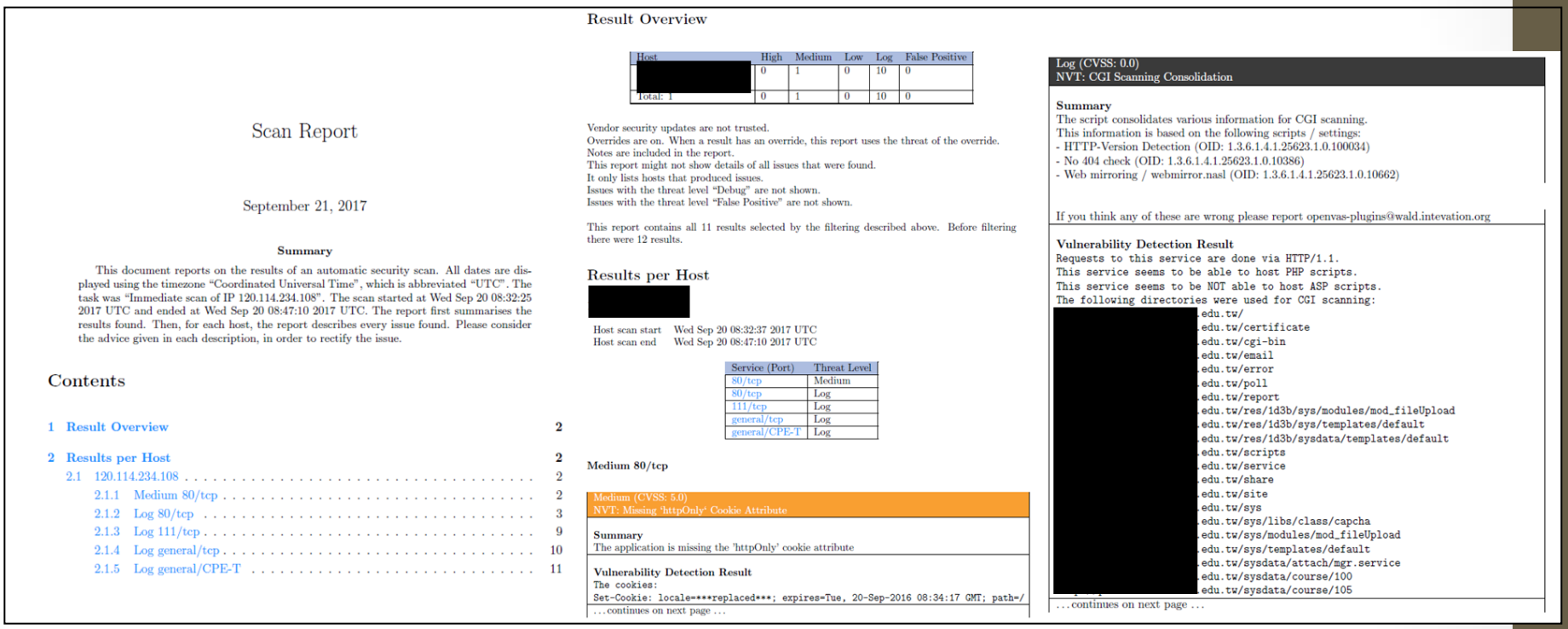
- 新增掃描網站
  - 使用網域:
    - 中心單位：依初登入所填網域來新增網站
    - 轄下單位：依轄下單位初登入所填網域；若轄下單位未填網域(如:尚未完成初登入帳號)則依管理者網域驗證
  - 使用IP:僅限區網中心及縣市網中心
    - 若轄下單位欲使用IP需由區網中心協助以「匯入」方式處理
  - 匯入格式請由系統下載範本填寫後上傳（系統可下載）
    - 欄位：單位代碼、主機網域、用途
    - 工作表名稱：檢測目標

弱點掃描平台介紹

- 因弱掃主機資源有限，需限制檢測數量(未來視情況調整)
  - 區網中心、縣市網中心：5個
  - 轄下單位：2個
- 排程日期
  - 可供排程的時段:
    - 每日開放3天後～30天內的日期
    - 週一～五，每日有2種時段：
      - 晚間時段(17 ～ 24點) ：3個檢測上限
      - 凌晨時段(0 ～ 8點)：5個檢測上限
  - 申請：
    - 單網站：可選擇排程日期
    - 多網站：由系統自動排程
  - 排程日期僅為排程參考依據，實際掃描時間需視掃描狀況而定

弱點掃描平台介紹

- 產出掃描結果報告



Scan Report

September 21, 2017

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Immediate scan of IP 120.114.234.108". The scan started at Wed Sep 20 08:32:25 2017 UTC and ended at Wed Sep 20 08:47:10 2017 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

Result Overview

Host	High	Medium	Low	Log	False Positive
[redacted]	0	1	0	10	0
Total: 1	0	1	0	10	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.

This report contains all 11 results selected by the filtering described above. Before filtering there were 12 results.

Results per Host

[redacted]

Host scan start Wed Sep 20 08:32:37 2017 UTC
Host scan end Wed Sep 20 08:47:10 2017 UTC

Service (Port)	Threat Level
80/tcp	Medium
80/tcp	Log
111/tcp	Log
general/tcp	Log
general/CPE-T	Log

Medium 80/tcp

Medium (CVSS: 5.0)
NVT: Missing 'httpOnly' Cookie Attribute

Summary
The application is missing the 'httpOnly' cookie attribute

Vulnerability Detection Result
The cookies:
Set-Cookie: locale=***replaced***; expires=Tue, 20-Sep-2016 08:34:17 GMT; path=/

...continues on next page ...

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)

If you think any of these are wrong please report openvas-plugins@wald.intevation.org

Vulnerability Detection Result
Requests to this service are done via HTTP/1.1.
This service seems to be able to host PHP scripts.
This service seems to be NOT able to host ASP scripts.
The following directories were used for CGI scanning:
[redacted]
edu.tw/
edu.tw/certificate
edu.tw/cgi-bin
edu.tw/email
edu.tw/error
edu.tw/poll
edu.tw/report
edu.tw/res/1d3b/sys/modules/mod_fileUpload
edu.tw/res/1d3b/sys/templates/default
edu.tw/res/1d3b/sysdata/templates/default
edu.tw/scripts
edu.tw/service
edu.tw/share
edu.tw/site
edu.tw/sys
edu.tw/sys/libs/class/capcha
edu.tw/sys/modules/mod_fileUpload
edu.tw/sys/templates/default
edu.tw/sysdata/attach/mgr.service
edu.tw/sysdata/course/100
edu.tw/sysdata/course/105

...continues on next page ...

弱點掃描平台介紹

- 漏洞危險層級說明

危險層級	資安項目
High **高風險**	OWASP TOP10資安議題、已知著名資料庫系統嚴重漏洞
Medium **中風險**	更舊版資料庫系統漏洞 (與High之差別為版本太過老舊，較無人使用) 較無立即資安危機但仍需注意
Low **低風險**	敏感資料未加密、網頁暫存Cookie安全、 網站原始碼洩漏檔案路徑、未使用之服務未關閉等
Informational **訊息提示**	錯誤顯示、網站連結失效、可能洩漏之帳號密碼、 洩漏網站、資料庫環境版本等

弱點掃描平台介紹

- 弱點報告及處理建議

檢測資訊

檢測時間	檢測狀態	網站資訊	檢測速度	風險程度/數量
開始: 2018-01-22 00:02 共434分鐘	執行失敗 aborting	• OS: Unix • Server: Apache 2.x • Technologies: PHP • 響應式網頁	• 請求數量:431566 • 網址數量:99981 • 平均回應毫秒:501	中風險:3 低風險:2 信 息:8

弱點資訊

	弱點	影響及建議	受影響項目
1	**Slow HTTP Denial of Service Attack** Your web server is vulnerable to Slow HTTP DoS (Denial of Service) attacks. Slowloris and Slow HTTP POST DoS attacks rely on the fact that the HTTP protocol, by design, requires requests to be completely received by the server before they are processed. If an HTTP request is not complete, or if the transfer rate is very low, the server keeps its resources busy waiting for the rest of the data. If the server keeps too many resources busy, this creates a denial of service.	**影響** A single machine can take down another machine's web server with minimal bandwidth and side effects on unrelated services and ports. **建議** Consult Web references for information about protecting your web server against this type of attack. **參考** Slowloris DOS Mitigation Guide http://www.funtoo.org/wiki/Slowloris_DOS_Mitigation_Guide Protect Apache Against Slowloris Attack http://blog.secaserver.com/2011/08/protect-apache-slowloris-attack/	中風險項目明細 1. /

磨課師平台介紹

- 成功大學提供弱點掃描服務外，並將相關課程資訊放置磨課師平台 http://portal2.k12moocs.edu.tw/。

磨課師平台介紹

1. 弱點掃描簡介

- 1.1 【課程影片】弱點掃描簡介 04:51
- 1.2 【課程影片】弱點掃描標準(CVE、OWASP)與結果分析
- 1.3 微軟修補程式(準備中)
- 1.4 報告與風險評估(準備中)

2. OWASP TOP 10 介紹與實作

- 2.1 【課程影片】2017 OWASP Top 10 簡介 02:58
- 2.2 A1-注入(Injection)
- 2.3 A2-失效的身分認證和會話管理(準備中)
- 2.4 A3-跨站腳本攻擊(Cross-Site Scripting (XSS))
- 2.5 A4-A10(準備中)

3. 物聯網安全

- 3.1 網路印表機
- 3.2 網路攝影機

4. 弱掃工具介紹

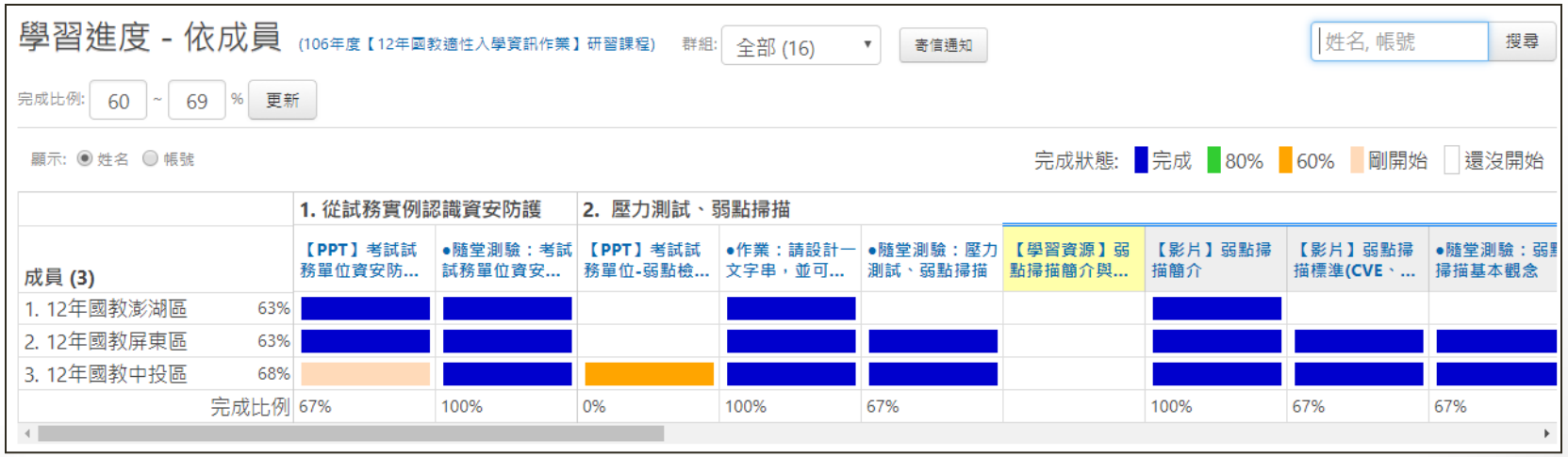
- 4.1 NMAP
- 4.2 SQLMap
- 4.3 SuperScan
- 4.4 GetIf
- 4.5 OpenVAS
- 4.6 W3AF

5. 平台使用介紹(準備中)

- 5.1 個人與學校資料維護
- 5.2 弱掃登錄與排程
- 5.3 報表與查詢

磨課師平台介紹

- 平台內提供弱點掃描及資安素養課程，範本還可以讓老師直接開課及提供查看學習進度、批改作業、計算成績、測驗等功能，請老師踴躍利用。
- 如要用平台辦理研習課程請於一週前填寫「研習學生帳號申請表」並將申請表 Email 至：service@k12moocs.edu.tw



本年度教育訓練
課程討論

本年度教育訓練課程討論

- 建置 Cacti 監控軟體，提供可回溯的流量紀錄與查詢
- IPv6 設定與教育訓練
- Micro:bit
- 弱點掃描平台教育訓練