高屏澎 區域網路中心

「臺灣學術網路(TANet)區域網路中心 110 年度基礎維運與資安人員計畫」

民國 109 年 12 月

【 目　　錄 】

壹、 計畫基本項目

計畫期程

民國 110 年 1 月 1 日到 110 年 12 月 31 日

計畫執行單位

高屏澎區網中心
國立中山大學 圖書與資訊處 資訊安全組

貳、 計畫執行內容

一、區域網路中心基本維運現況說明

（一） 臺灣學術網路(TANet)高屏澎區域網路中心(也是台灣高品質學術研究網路的 GigaPOP)，提供區域內大高雄市、屏東縣、澎湖縣教育網路中心及大專院校與社會服務組織連接到學術網路的接取服務。

（二） 中心除提供穩定與安全的網際網路連線外，並積極提供更好的網路服務品質和更佳的網路資源管理。對於大高雄市、屏東、澎湖區域內的各連線單位，可透過高屏澎區網中心首頁(https://web.kpprc.edu.tw)取得各項相關的資訊與公告。除此之外，高屏澎區網中心亦提供異常流量分析及入侵服務偵測系統，有網路問題發生時，得以於最短時間內處理相關問題。

二、配合教育部資訊及科技教育司工作重點

(一)、網路管理

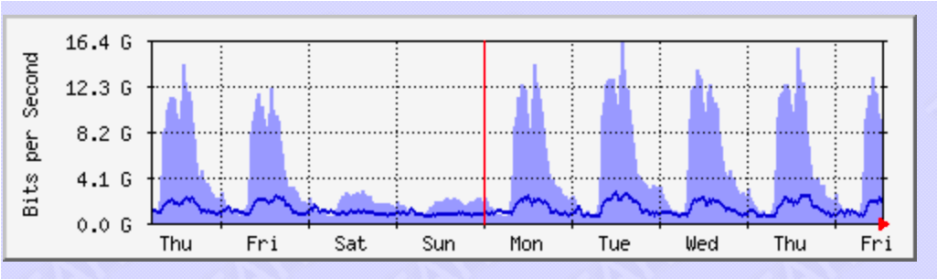
1. 網路使用及流量統計分析

(1) 高屏澎區網中心首頁(https://web.kpprc.edu.tw)：提供本中心各項服務，並已取得 IPv6 Ready Logo。

(2) 高屏澎區網中心 DNS (163.28.129.1 與 163.28.129.2)：提供給本區域內連線單位使用，IPv6 位址為 2001:288:8000::1:1、2001:288:8000::1:2。

(3) 高屏澎區網 MRTG IPv4 流量統計，提供給本區域內連線單位網路流量狀況與資訊。

流量更新時間：2020 年 12 月 4 日星期五 13:51，來源 http://mrtg.tanet.edu.tw/tanet/tanetbb/asr-nsysu-ipv4.html

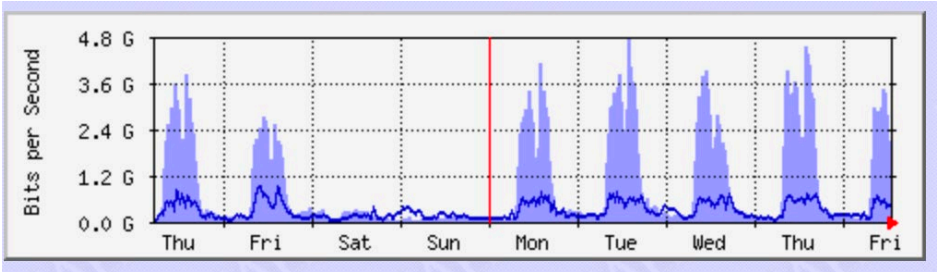


最大 In 16.2 Gb/秒 (40.4%) 4578.7 Mb/秒 (11.4%) 9329.7 Mb/秒 (23.3%)
最大 Out 2700.2 Mb/秒 (6.8%) 1187.6 Mb/秒 (3.0%) 1663.0 Mb/秒 (4.2%)

(4) 高屏澎區網 MRTG IPv6 流量統計

流量更新時間：2020 年 12 月 4 日星期五 13:55，來源

http://mrtg.tanet.edu.tw/tanet/tanetbb/asr-nsysu-ipv6.html

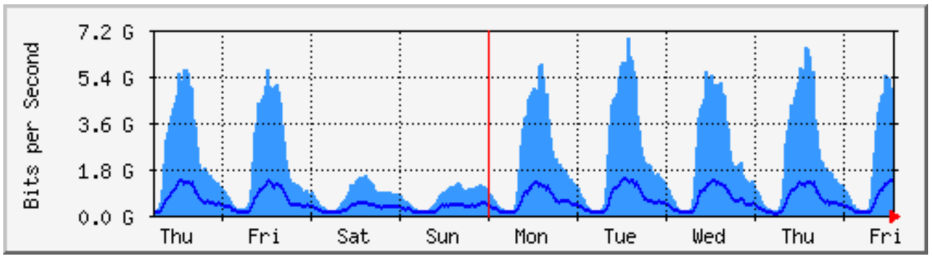


最大 In 4761.4 Mb/秒 (11.9%) 914.5 Mb/秒 (2.3%) 2078.9 Mb/秒 (5.2%)
最大 Out 895.4 Mb/秒 (2.2%) 266.0 Mb/秒 (0.7%) 301.0 Mb/秒 (0.8%)

(5) 高屏澎區網 GGC (Google Global Cache)：提供給連線單位更好的 Google 相關服務，並有效提升頻寬使用效率。

流量更新時間：2020 年 12 月 4 日星期五 13:58，來源

http://mrtg.kpprc.edu.tw/mrtg/192.192.60.117_151.html



最大 In 6853.3 Mb/s (68.6%) 1987.8 Mb/s (19.9%) 4924.1 Mb/s (49.2%)
最大 Out 1436.4 Mb/s (14.4%) 521.3 Mb/s (5.2%) 1167.4 Mb/s (11.7%)

(二)、機房監控與管理

1. 空間狀況：

高屏澎區網中心將 ASR 9010 放置在中山大學機房機櫃中，依照 ISO27001 之實體與環境安全之建置及強化機房實體安全與系統網路管理，讓機房

環境可隨時監測及控制。

2. 電力狀況：

(1) ASR9010 設備的電力平常由台電的市電供給，同時連接到地下二樓電器室 UPS，若有斷電情形則由 UPS 提供電力，且校方發電機值班人員會立即到達，以確定發電機順利啟動，而達到不間斷之電力供應（如圖一所示）。

圖一：電器室 UPS 設備

(2) 為避免 TWAREN 網路設備運作時的電力中斷，本校圖書與資訊處已完成主機房電力雙迴路及雙電力備援之建置，藉此維持網路連線之穩定。

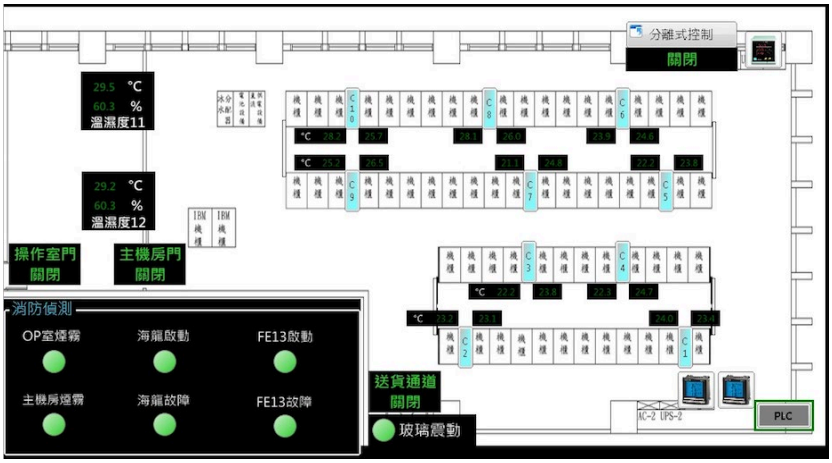
3. 空調現況：

(1) 機房建置機櫃式空調(如圖二所示)，並將區網核心路由器 ASR 9010 放置在機櫃式空調環境中，以提供更穩定的空調環境。

圖二：本機房所使用機櫃式空調

(2) 機房之空調狀況，除了上班時專職維運人員的監控外，非上班時間

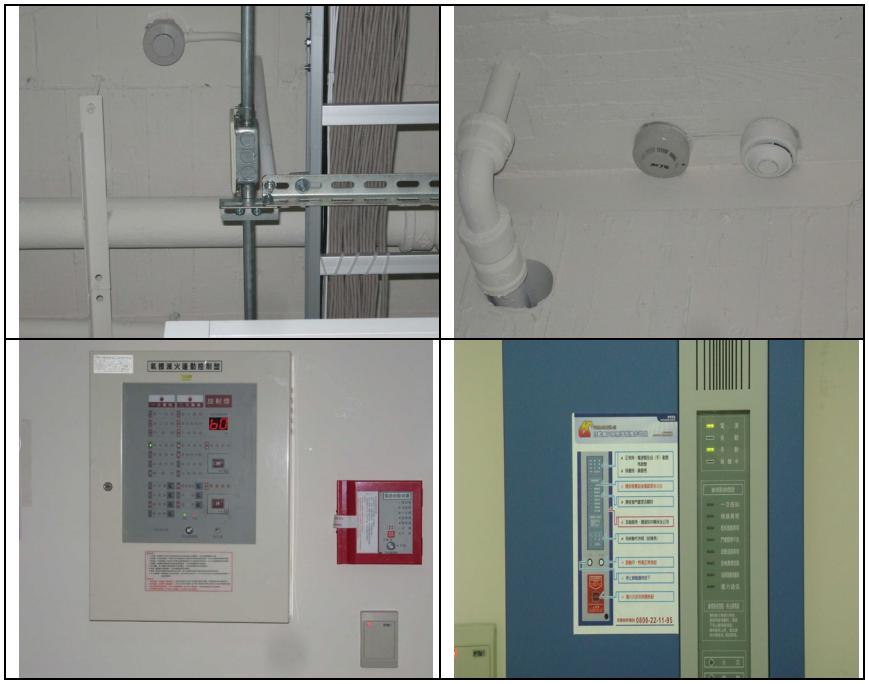
亦可透過環控系統的 WEB 監控頁面，隨時隨地監控機房狀態(如圖三所示)。



圖三：本機房之環控系統

4. 消防與安全管制：

(1) 機房規劃有消防警示系統及自動滅火系統、氣體滅火控制器（含溫度監測之告警系統）（如圖四所示），且當有異常事件發生時，環控系統會自動發送簡訊給管理者。



圖四：本機房的消防警示系統

(2) 機房出入口有門禁及監視系統(如圖五所示)，可 24 小時監控人員與設備的進出。

圖五：本機房之監視器

5. 其他：

   (1) 人員進出機房皆應於「機房進出登記簿」登記。

   (2) 設備進出機房需填寫「設備進出紀錄表」。

   (3) 持續受理高屏澎區網的大專院校介接新世代骨幹網路連線申請 (升速)，於管理會中審查。

6. 本區網中心至 109 年度止，共完成 29 個連線單位的 IPv6 路由設定，其中，包括 3 個縣市網路中心及 26 個連線單位，分項條列如下：

   (1) 縣市網路中心：高雄市網、屏東縣網、澎湖縣網。

   (2) 連線單位：高雄醫學大學、實踐大學高雄校區、屏東大學、海軍官校、中山大學、高雄師範大學、高雄大學、屏東科技大學、義守大學、輔英科技大學、正修科技大學、文藻外語大學、大仁科技大學、陸軍官校、中正預校、高雄榮民總醫院、空軍官校、高雄空大、航空技術學院、慈惠醫專、育英醫專、高雄餐旅大學、高雄科技大學、美和科技大學、高雄科技大學(旗津校區)及高苑科技大學計 26 所。

(三)、資訊服務

1. 教育單位弱點檢測平台 (https://evs.twisc.ncku.edu.tw)：提供給高屏澎區網連線單位申請掃描該單位網站是否有漏洞問題。

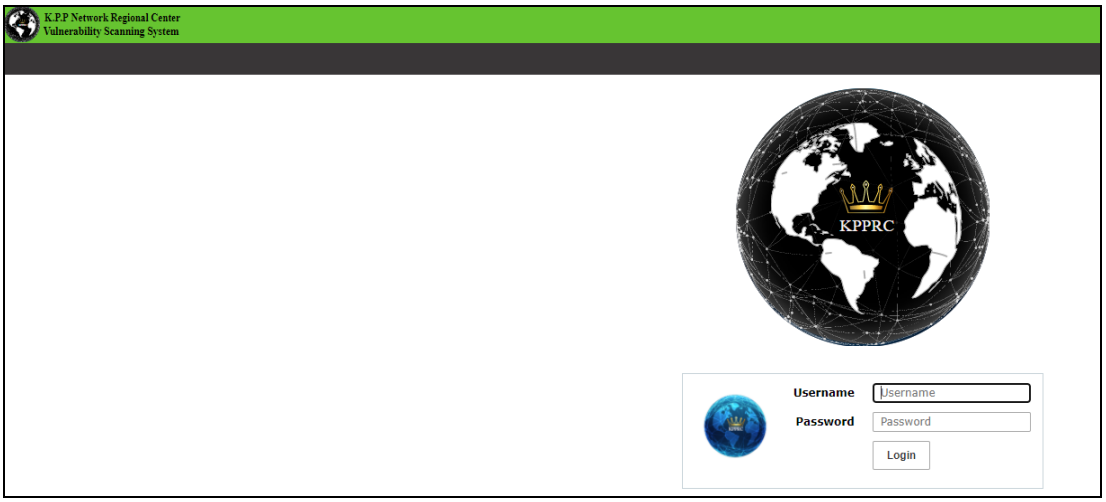
2. 協助連線單位網路與資安等各項問題處理與諮詢服務，如協助連線單位排除 DDoS 攻擊等問題，協同 TACERT、國網中心及臺灣大學 (ASOC)

做流量清洗。

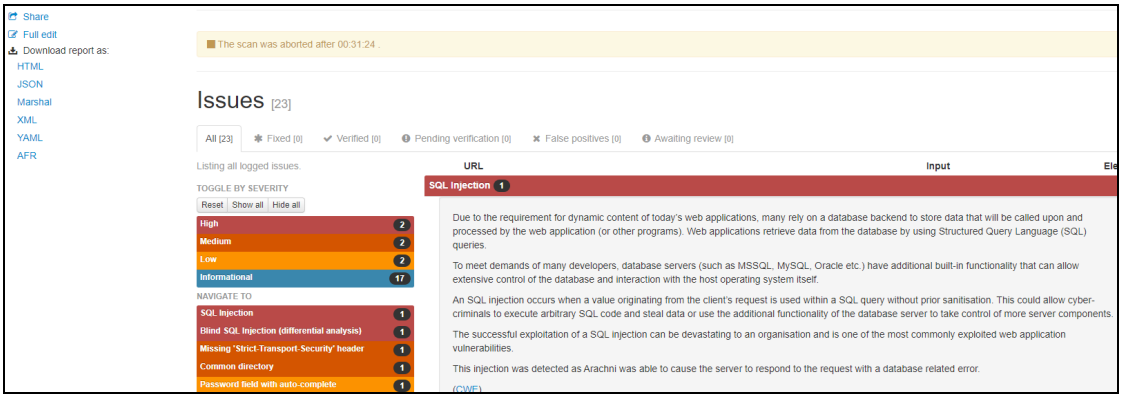
3. 提供 DNS 虛擬機範本服務 (Bind 9.10 以上版本)，並提供範本說明文件，連線單位可依範本修改無痛升級至最新版本，以防止 DNS 相關資安漏洞。

4. 提供「DNS 升級及資安健檢服務」，本中心主動連絡連線單位夥伴，協助升級老舊 DNS 版本，採線上服務表單，方便申請。迄今年共協助八所連線單位夥伴成功升級及設定：包含中正國防幹部預備學校、輔英科技大學、育英護理專科學校、國立屏東大學、美和科技大學、國立澎湖科大、屏東縣網及高雄師範大學。

5. 今年因應資安稽核建議「弱點掃瞄監測系統」，導入容器化部署並將版本提升為 10，提供連線單位自行建置，並開立相關教學課程。協助連線單位檢視管控之伺服器目前開啟服務是否有弱點，以利網管人員針對弱點進行修正，防止駭客利用該弱點進行攻擊。



6. 本中心推出 Open Source 網站應用程式弱點掃瞄平台，採用 Ruby On Rails 架構提供跨平台執行，發佈 Windows 及 Linux 兩種版本，使用者可直接在本機直接執行，使程式開發者可以即時掃描修正弱點，提升網站安全。



7. 於 98 年 7 月 20 日通過教育體系資訊安全管理規範 (ISMS) 之驗證，並

取得證書，今年於 8 月 13 日、14 日，通過教育體系資安認證 (ISMS) 重新驗證，確保區網中心業務持續營運，可以提供更安全及更穩定的區網網路服務。

8. 提供異常流量偵測系統 NFSEN，提供連線單位查詢即時與過去 TCP、UDP、ICMP，封包、流量及總量大小等服務。

9. 與桃園區網中心合作導入 FDNS 異常流量系統，可偵測 UDP flooding 及 Port scanning 等異常流量及查詢 TopN 流量，並以研討會方式推廣至連線單位夥伴。

10. 將區網中心相關服務如官方首頁、服務偵測系統導入 HTTPS 服務，以提升 WEB 服務安全性。

(四)、網管及連線管理

1. **服務偵測系統**：採用 NAGIOS 系統為基礎，進行主機連線偵測，當所設定偵測的服務無法偵測時，將會把訊息回傳到個人 Google 行事曆。可設定偵測不同服務及 PORT，當該服務無法偵測時則發送告警，並將 Nagios 系統導入 HTTPS 服務，並整合 Nagios Check_ssl plugin，偵測 HTTPS 憑證到期日

   系統網址：https://mgmt.kpprc.edu.tw/nagios/

2. **WhatsUp 簡訊系統監控連線單位界面**：使用此系統定期監控每個界面是否正常運作，若發生斷線，將立即以簡訊方式通知區網網路管理人員。系統網址：http://netmgm.nsysu.edu.tw/

3. **Arcsight Logger 系統（syslog 訊息監控）**：將區網核心路由器 log message 導到此 log 管理系統，區網管理人員每日定期檢視是否有異常 log 出現並能立即處理。

   系統網址：https://logger.kpprc.edu.tw/platform-ui/

4. **Mrtg 流量監控連線單位界面流量狀態**:提供連線單位夥伴查詢即時流量。

   系統網址：https://web.kpprc.edu.tw（網路流量 MRTG 查詢）

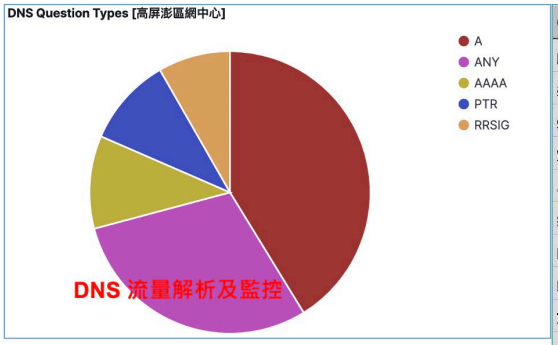
5. **Cacti 流量監控連線單位界面流量狀態**:提供連線單位夥伴查詢即時流量。

   系統網址：https://web.kpprc.edu.tw（網路流量 CACTI 查詢）

6. **Cacti plugin weathermap**：將網路流量以圖形化表現，不同顏色代表不同 Traffic Load，監控連線單位流量是否異常及過載。

   系統網址：https://web.kpprc.edu.tw（網路流量 weathermap 查詢）

7. **DNS 異常流量偵測系統**：分析連線單位 DNS 流量，以找出潛在 DNS Open Resolver 主機，並通知連線單位修正，以防止 DNS 放大攻擊。



Question	Count
peacecorps.gov	64,715
aids.gov	24,485
dns.msftncsi.com	16,534
www.google.com	6,364
.	6,209
swscan.apple.com	5,845
ns1.kpprc.edu.tw	4,799
ns2.kpprc.edu.tw	4,672
test.52dumpling.com	4,012
www.viewcan.net	3,190

DNS Top 10 Questions [高屏澎區網中心]

Question	Count
www.viewcan.net	48,348
www.google.it	8,537
www.google.com.tw	7,320
www.google.com	23,118
topsrv.us.to.shute.edu.kh.tw	60,600
topsrv.us.to	53,441
teredo.ipv6.microsoft.com	10,430
swscan.apple.com	14,760
sl	22,342
RuckusController	6,952

DNS Response Codes [Packetbeat] ECS

Response Code	Count
NOERROR	3,129,422
NXDOMAIN	161,378
SERVFAIL	108,908
REFUSED	79,868
FORMERR	30,281

Export: Raw Formatted

至目前為止，已監控到 10 臺 DNS Server 存在 Open DNS resolver 問題，並通知對方做 DNS server 設定修正，IP 及連線單位如下

- 140.127.114.21 -國立高雄科技大學(建工/燕巢校區)
- 140.133.78.58 - 國立高雄科技大學(建工/燕巢校區)
- 210.71.32.4 - 高雄市政府教育局資訊教育中心
- 140.127.242.254 - 澎湖縣教育網路中心
- 163.24.157.1 - 屏東縣教育網路中心
- 163.24.79.8 - 屏東縣教育網路中心
- 210.60.80.1 - 高苑科技大學
- 210.60.80.2 - 高苑科技大學
- 140.117.11.165 - 中山大學
- 163.15.183.33 -高雄市立空中大學

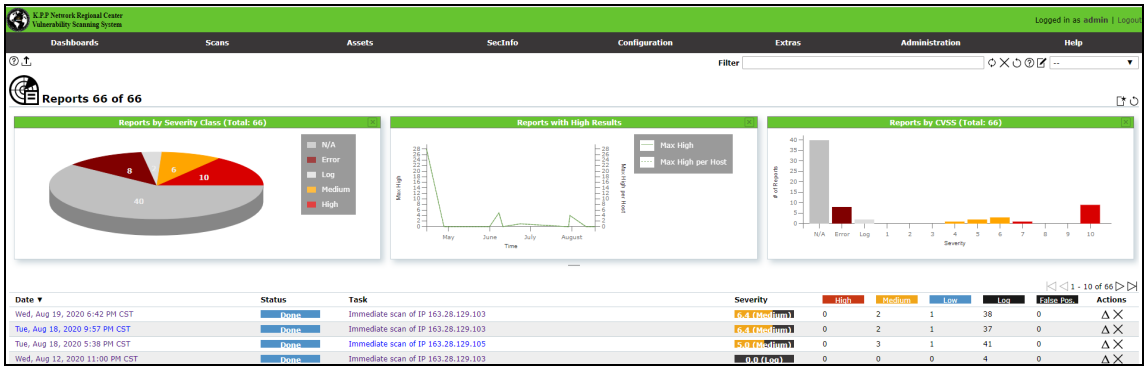
(五)、弱點掃瞄監測系統(推出容器化版本)與網站應用程式弱掃系統

1. 說明：提供最新弱點定義庫與新版掃描引擎，呈現拓撲軌跡、風險弱點統計，協助連線單位掃描管控之伺服器目前開啟服務是否有弱點，以利連線單位網管人員針對弱點進行修正，防止駭客利用該弱點進行攻擊。

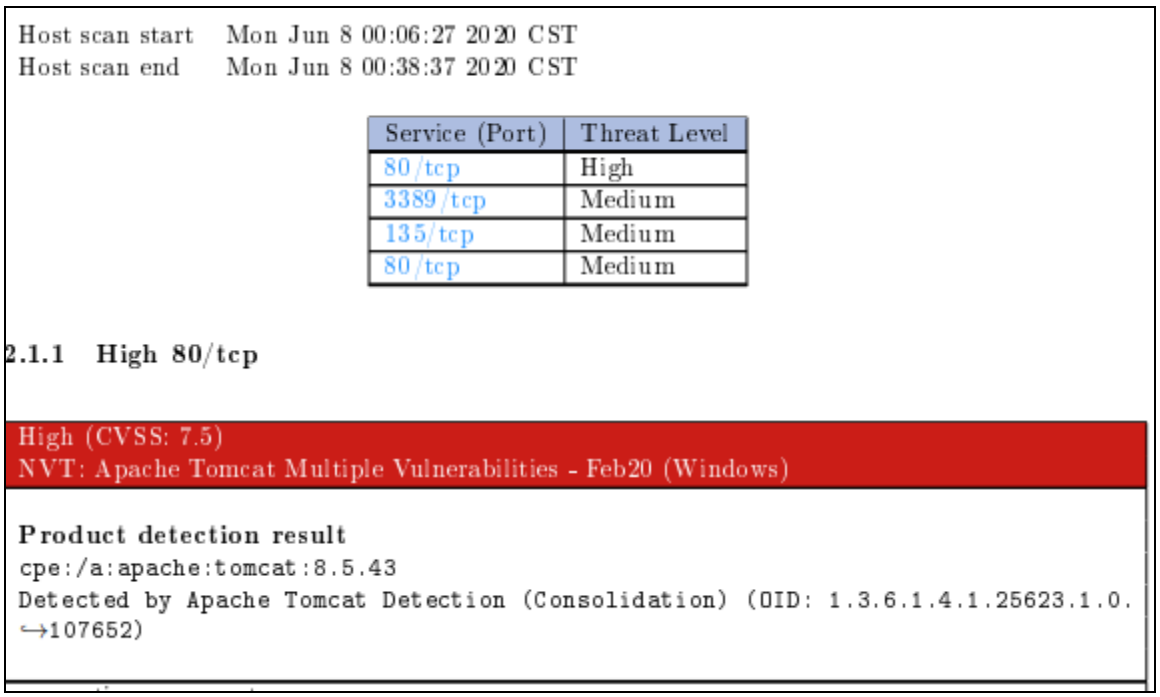
2. 功能簡介： 系統提供弱點掃瞄後 LOG 檔匯出 PDF、XML 檔，排程掃描、批次掃描及自定義掃描。

3. 109 年開放申請以來共計 14 所單位申請，包含 13 所大專院校、1 所高中職。

4. 風險報告及轉出：



風險報告轉出



Host scan start Mon Jun 8 00:06:27 2020 CST
Host scan end Mon Jun 8 00:38:37 2020 CST

Service (Port)	Threat Level
80/tcp	High
3389/tcp	Medium
135/tcp	Medium
80/tcp	Medium

2.1.1 High 80/tcp

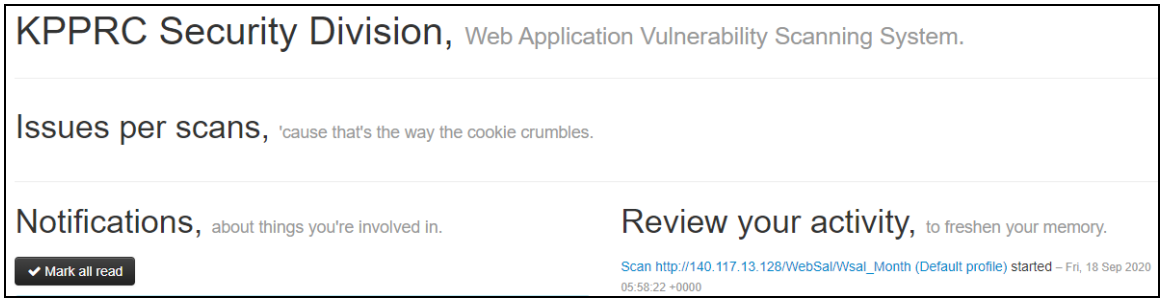
High (CVSS: 7.5)
NVT: Apache Tomcat Multiple Vulnerabilities - Feb20 (Windows)

Product detection result
cpe:/a:apache:tomcat:8.5.43
Detected by Apache Tomcat Detection (Consolidation) (OID: 1.3.6.1.4.1.25623.1.0.
↪107652)

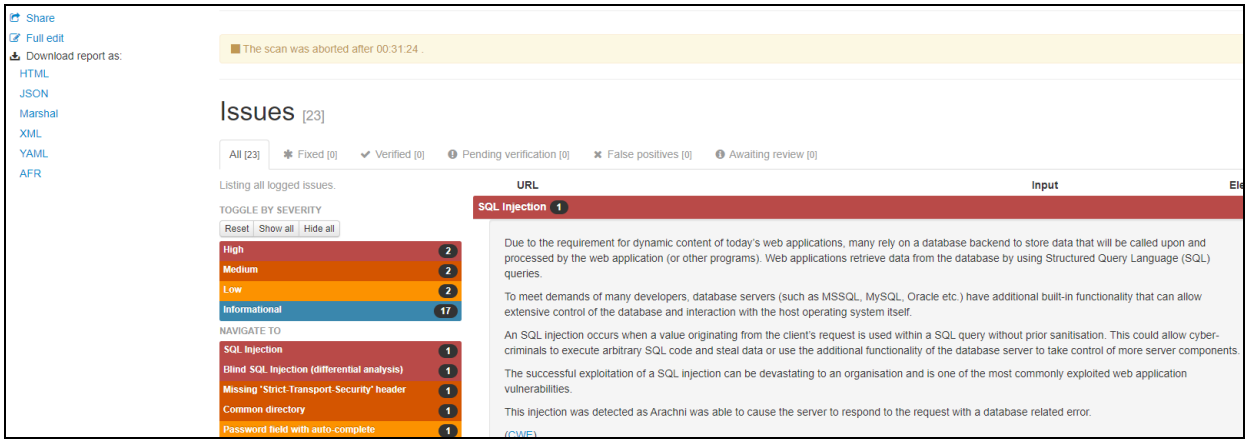
網站應用程式弱點掃瞄系統

1. 說明：本中心推出 Open Source 網站應用程式弱點掃瞄平台，採用 Ruby On Rails 架構提供跨平台執行，發佈 Windows 及 Linux 兩種版本，使用者可直接在本機直接執行，使程式開發者可以即時掃描修正弱點，提升網站安全。

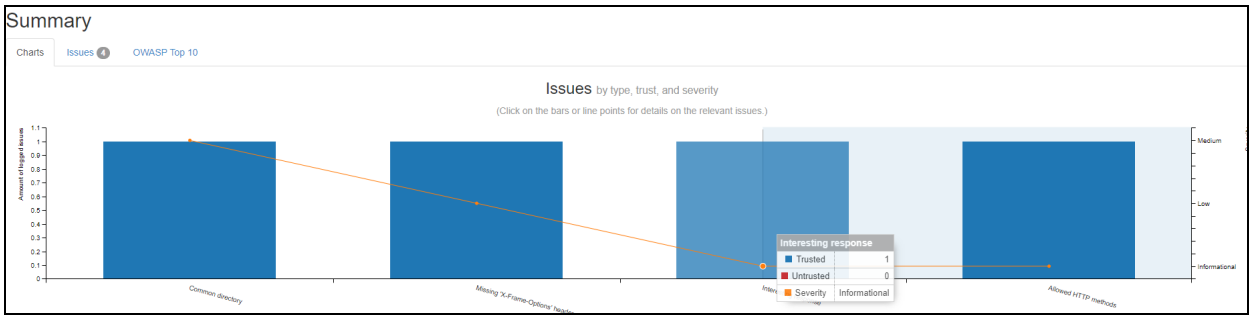
2.系統畫面：



3.弱點分析



4.報表轉出

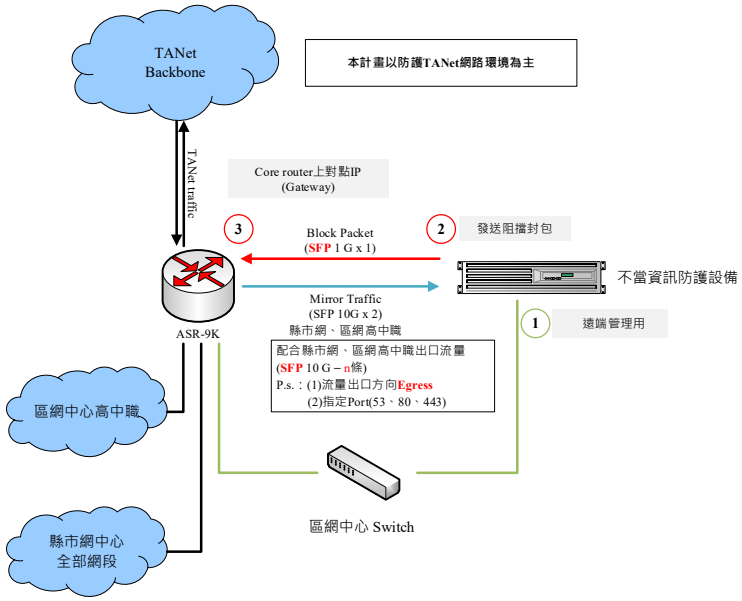


(六)、開發、建置並導入 TANet 不當資訊防護系統

1. 說明：今年度高屏澎區網中心自行研發不當資訊防護系統技術，以防護 TANet 之高中職、國中小學及縣市網連線單位連線不當資訊網站(如暴力、色情、賭博等網站)，此系統主要特色如下：
   - **同時運用 DNS 防護技術、Layer7 防護技術及 IP 阻擋技術**，將流量進行過濾，採用三重防護方式，提高防護效能。
   - **建置虛擬化伺服器（VM Server）**，進行系統環境測試，當系統遇突發狀況，透過 VM 即時測試與修正，避免因測試系統負荷量超載，造成設備故障問題產生。
   - **即時報表系統數據統計**，提供系統過濾之每日瀏覽次數、每日阻擋次數及阻擋之不當網域及 IP 位置等統計資訊，另外依使用者 IP 的防護次數和不當網站的防護次數進行每月排名。
   - **模擬瀏覽測試程式**開發，偵測需阻擋黑名單是否正確實阻擋，並檢視是否有誤擋情形發生，確保系統阻擋的正確性。
   - **資料庫管理**，建立完整資料庫名單，完整囊括各大防護機制白名單及黑名單資料，並不定期去除無效網域位址名單。
   - **建置監控及資料派送系統**，透過監控系統，監測各區網主機運作情況，並將資料庫黑白名單透過派送系統傳輸至各區網中心及縣市網中心，區網及縣市網之黑白名單資料庫亦可回傳至主系統中，進行資料更新。
   - **申訴檢舉平台建置**，提供學術網路使用者於連線時，發現可建議系統阻擋的網站或使用者回饋已被阻擋意見之完整管道，由團隊進行問題排除並即時回報。
2. 高屏澎區網中心實際運作情形(目前已導入所屬全部國中小學及高中職連線單位)：
   - 縣市網：高雄市網、屏東縣網及澎湖縣網 (含所有國中小學)
   - 高中職：左營高中、瑞祥高中及中正預校
3. 各區網導入狀況：
   - 108 年度計畫已導入之區網中心：台北第一區網(臺灣大學)、台北第二區網(政治大學)、桃園區網(中央大學)、台南區網(成功大學)。
   - 109 年度計畫預計建置(含已建置):竹苗區網(交通大學)、台中區網(中興大學)、雲嘉區網(中正大學)、花蓮區網(東華大學)。

- 110 年度計畫將建置：南投區網(暨南大學)、宜蘭區網(宜蘭大學)、台東區網(台東大學)
- 短期建置於縣市網中心(將於區網中心建置完畢後向上集中防護管理)：台中市網、彰化縣網、南投縣網、宜蘭縣網、台東縣網。

4. 系統佈署架構圖如下：



三、110 年度區網中心工作重點及特色服務

110 年度工作重點將致力於提升區網中心**資訊安全防護**，包含以下事項：

- 高屏澎區網網路流量分析系統建置，110 年將加入監測如 LDAP、NTP 等網路流量，以防止被利用作為放大攻擊。
- 將本中心開發之容器化弱點掃描系統導入鄰近區網中心，以強化區網中心弱點防護能力。
- 持續精進容器化弱點掃描系統引擎版本及弱點定義庫，使下轄連線單位快速操作及使用，降低原先集中於區網中心掃描之資安風險。
- 運用容器化整合資安檢測及網路檢測工具，簡化其設定流程，預期達到更新便利，安裝快速簡便，輕鬆簡易的維護與操作，提升下轄單位整體資安防護之能力。
- 持續協助連線單位夥伴升級 DNS 系統版本(Bind 9.10.5 以上)，及加強 IPv6 系統支援，提升 IPv6 使用率。
- 容器化弱點掃瞄系統掃描引擎精進與服務推廣。
- 容器化流量監控系統佈署服務推廣。

(一)、應用特色服務

項 目	KPI 指 標
網路流量分析系統	1. 偵測連線單位如 NTP、DNS、LDAP 封包流量，並進一步分析是否有異常行為發生可能性，以防止相關漏洞被利用做為放大攻擊。 2. 今年已提供 DNS 流量分析服務，預計再加入 NTP 流量分所服務
不當資訊防護系統導入	3. 110 年上半年導入台中區網及南投區網。 4. 進行台南、雲嘉、桃園、台北第一區網進行網路架構調整，完善防護系統(備援機制)
容器化弱點掃瞄系統	1.110 年進行掃描引擎更新，容器化重建。 2.110 年 6 月前進行改版，提供給下轄單位使用。

DSN 版本升級及健檢服務	1. 提供連線單位 DNS Bind 版本升級服務及設定檔資安健檢服務。 2. 110 年至少協助 3 所連線單位以上實施資安健檢及升級服務。
容器化系統精進整合	110 年將綜整下轄單位建議，發布容器化流量監控系統(如 Cacti 網管系統)。
資安威脅情資整合	今年已與空軍航空技術學院進行威脅情資整合，預計明年再跟另一所連線單位進行整合。

(二)、雲端及偏鄉服務

項 目	KPI 指 標
雲端服務	持續提供連線單位更佳之雲端虛擬主機服務，包含更便利使用的虛擬機範本。
偏鄉服務	偏鄉服務：高雄、屏東及澎湖地區偏鄉服務，以遠距教學方式進行，預計 1 年將對 2 所學校進行 2 學期的 scratch 程式設計教學，提升偏鄉學生對於程式邏輯概念與認知。

(三)、協助連線單位工作及應用服務推廣重點

項 目	KPI 指 標
區網管理會及技術交流成果推廣會議	預計上半年及下半年各舉辦 1 場，共計 2 場。
應用服務推廣	1. 推廣 DNS 及資安健診服務。 2. 推廣主機弱點掃描 Container 服務。 3. 推廣 Web 弱點掃描服務。

項 目	KPI 指 標
	4. VoIP 應用服務推廣 5. 容器化流量監控系統服務推廣

(四)、辦理研討會及技術交流成果推廣會議

項 目	KPI 指 標
辦理研討會	研討會：主題包括資訊安全、個人資料保護及網路技術相關等主題研討會，預計舉辦 4 場研討會以上。

參、 經費需求

經費項目包括人事費、業務費、設備費，總計預算經費 **1,855,000** 元，其預算內容如附件一。

一、人事費

（一） 網管人數 1 位，依據科技部補助專題研究計畫專任助理人員工作酬金參考表及參考工作年資編列（所具曾任年資經審定合於採計提敘者，得於本職高薪範圍內酌予提晉薪級，惟每滿一年最多提敘一級）。

（二） 資安人數 1 位，依據科技部補助專題研究計畫專任助理人員工作酬金參考表及參考工作年資編列（所具曾任年資經審定合於採計提敘者，得於本職高薪範圍內酌予提晉薪級，惟每滿一年最多提敘一級）。

（三） 網管人員、資安人員之勞健保費、離職儲金、補充保費。

（四） 預算經費 **1,172,629** 元

二、業務費

包括講座鐘點費、膳費、差旅費、雜支、電信費、設備維護費、工讀費、週邊零件費、教育訓練費及工作費，預算經費 **532,371** 元。

三、設備費

包括網路設備、研究開發設備費，預算經費 **150,000 元**。