107年度執行成效報告

國立中山大學圖書與資訊處副處長

鄺獻榮教授

Agenda

- 網路中心基礎維運
- 網路及資安技術支援
- 創新特色服務
- 連線單位需求分析及滿意度調查
- 未來營運目標

網路中心基礎維運

- 區網網站報名系統
- Nagios HTTPS 服務偵測系統
- IPv6服務推動
- Cacti網管系統及weathermap
- NFSEN異常流量監控系統
- FDNS流量監測系統

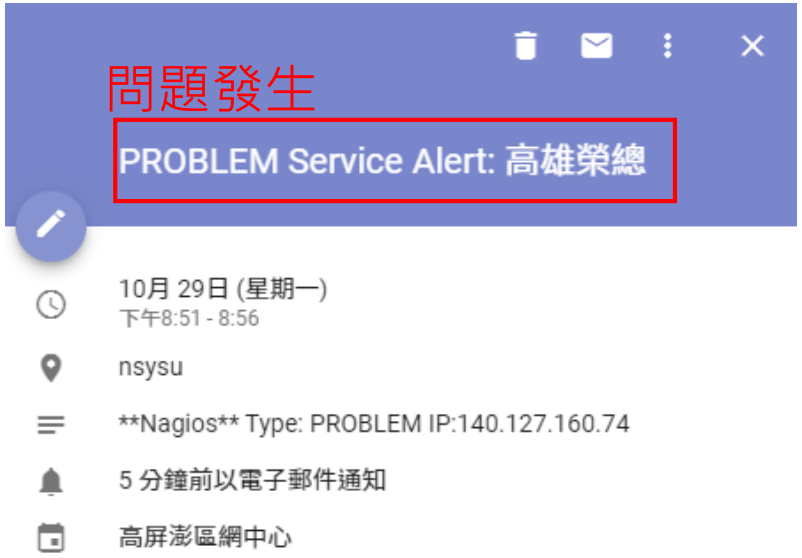
區網網站報名系統開發完成上線

- 網址：https://web.kpprc.edu.tw
- 支援HTTPS連線

支援RWD

Nagios 服務偵測系統

- 即時偵測連線單位連線狀態
- 107年10月29日亞太電信高雄民族陸橋光纖燒毀事件造成連線單位斷線
- 有效即時偵測與排除



Nagios HTTPS服務偵測系統

- 整合Nagios Check_ssl plugin，偵測HTTPS憑證到期日
- 技術推廣至連線單位

Status	Last Check	Duration	Attempt	Status Information
OK	06-04-2018 13:57:36	1d 23h 33m 38s	1/3	OK - Certificate will expire on Jul 15 02:33:33 2018 GMT
OK	06-04-2018 13:54:44	5d 21h 2m 31s	1/3	OK - load average: 0.00, 0.00, 0.00
CRITICAL	06-04-2018 13:53:42	1d 23h 31m 30s	3/3	CRITICAL - Certificate has EXPIRED on (May 27 06:20:04 2018 GMT)! Please replace!

SSL 憑證到期日

SSL 憑證已過期

IPv6網路連線設定

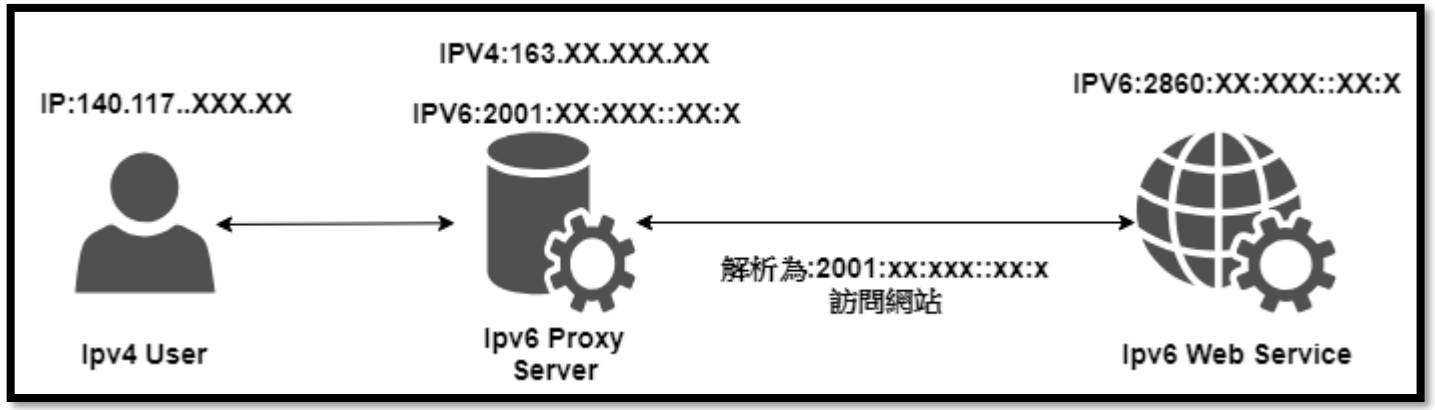
- 官網支援IPv6連線
  - 2001:288:8000::1:67
- OpenVAS弱掃系統支援IPv6連線
  - 2001:288:8000::1:62

```
kpprc@nsmaster:/var/cache/bind/data$ dig  web.kpprc.edu.tw AAAA

; <<>> DiG 9.10.4-P6 <<>> web.kpprc.edu.tw AAAA
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62551
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;web.kpprc.edu.tw.              IN      AAAA

;; ANSWER SECTION:
web.kpprc.edu.tw.       300     IN      AAAA    2001:288:8000::1:67

;; AUTHORITY SECTION:
kpprc.edu.tw.           300     IN      NS      ns1.kpprc.edu.tw.
kpprc.edu.tw.           300     IN      NS      ns2.kpprc.edu.tw.
```

IPv6服務技術推動

- 107年10月19日區網管理會議中技術分享
- IPv6 Proxy Server自動化部署(Jenkins)

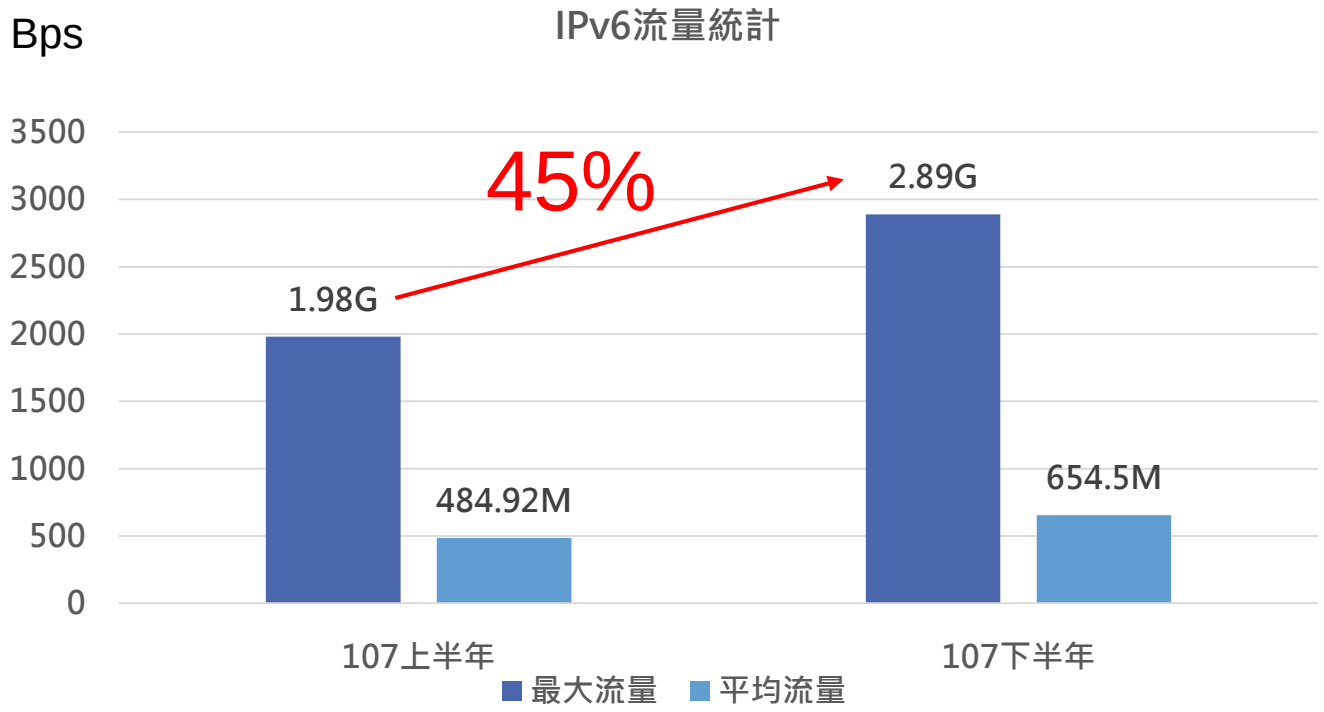
主要功能:讓只有IPv4的使用者，透過IPv6 Proxy Server 連上IPv6網站



一鍵化安裝，只需設定ACL IP、Domain即可使用

IPv6服務推動成果

- 107年10月份統計，今年IPv6最大流量成長45%



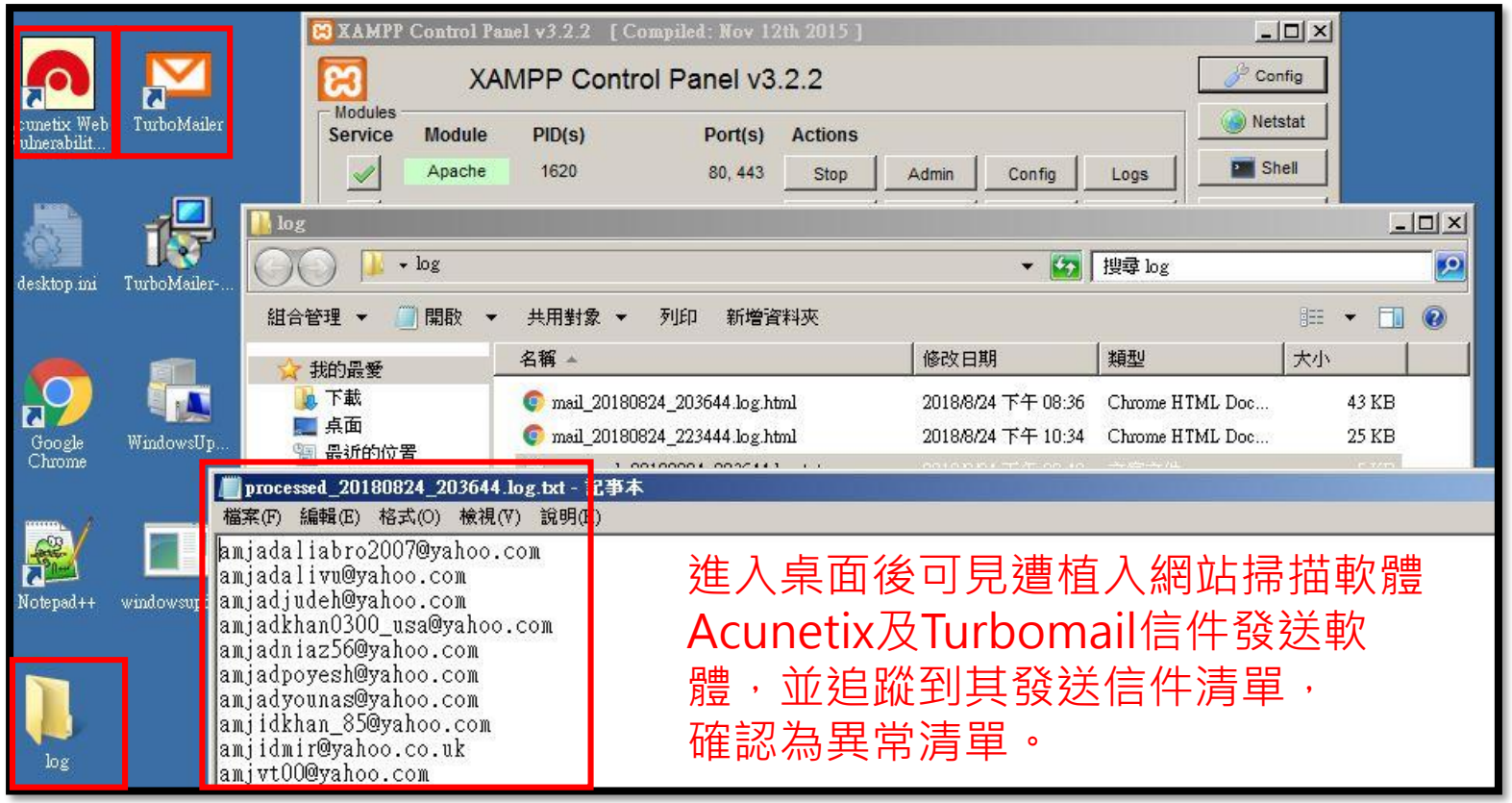
網路及資安技術支援

- 資安事件支援處理
- DNS升級及資安健檢服務
- 資安通報事件處理時效
- 教育訓練辦理情形

連線單位資安技術支援

連線單位資安鑑識支援 (1/3)

- 107年9月27日接獲通報，某校IP透過弱點掃描軟體，企圖掃瞄某機關系統



追蹤到事發主機，先行進行快照備份，並進行斷網

進入桌面後可見遭植入網站掃描軟體Acunetix及Turbomail信件發送軟體，並追蹤到其發送信件清單，確認為異常清單。

連線單位資安鑑識支援 (2/3)

- 進行系統控制台新增移除程式檢查、事件紀錄器、使用者帳號檢查

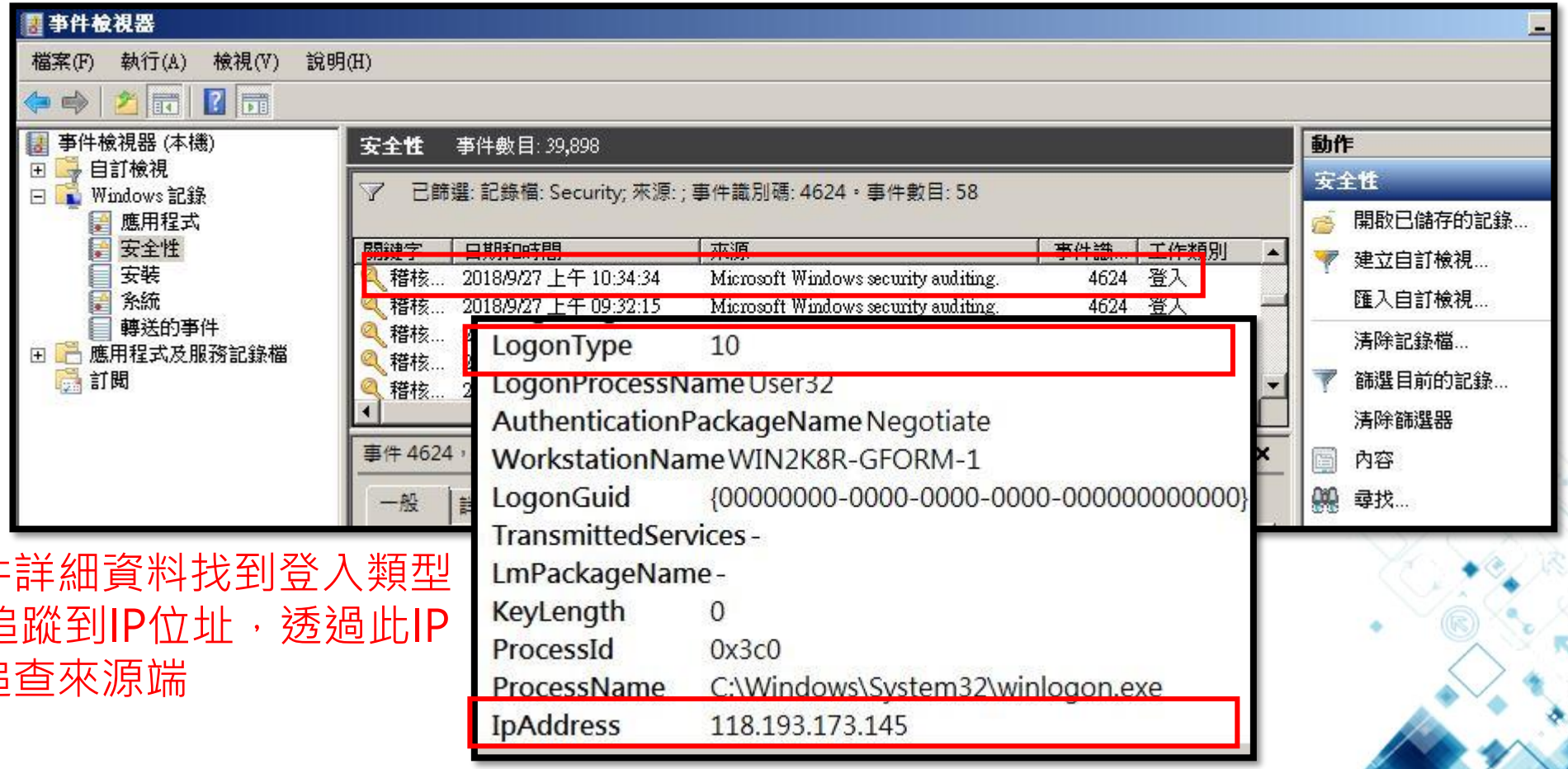
使用者帳戶多出未知帳戶名稱iis_user

安裝日期與發生日期符合

透過事件檢視器篩選4624(遠端登入的安全事件)並找尋發生事件的時間點

連線單位資安鑑識支援 (3/3)

- 找尋在事件發生前的時間點檢查是否異常登入IP



點選該事件詳細資料找到登入類型為10，並追蹤到IP位址，透過此IP位址進行追查來源端

網頁置換事件支援處理

- 協助連線單位處理Web defacement 資安事件
- 首頁被強制重新導向

移除首頁惡意Java Script碼後恢復正常

DNS版本升級及資安健檢服務

- DNS Bind版本升級服務(9.10.4以上版本)
- DNS安全性設定服務及健檢
  - ACL設定
  - 限制來源查詢要求
  - Response Rate Limit (RRL)
  - Zone Transfer 限制
- 已協助八間連線單位夥伴完成升級及資安健檢服務
  - 今年協助屏東縣網及高師大完成升級及資安健檢服務

- 服務申請網址：https://goo.gl/6PgWh4

資安通報事件處理時效

- 資安事件緊急通報處理之效率及通報率
  - **所屬之學校及單位1、2級資安事件處理**
    - 通報平均時間：0.42 小時 (106年0.52小時)
    - 應變處理平均時數：0.00 小時。
    - 事件處理平均時數：0.43 小時 (106年0.52小時)
    - 通報完成率：99.86%
    - 事件完成率：100%
  - **所屬之學校及單位3、4級資安事件通報：無任何3、4級事件**
  - **資安事件通報審核平均時數：0.25 小時 (106年0.31小時)。**

17

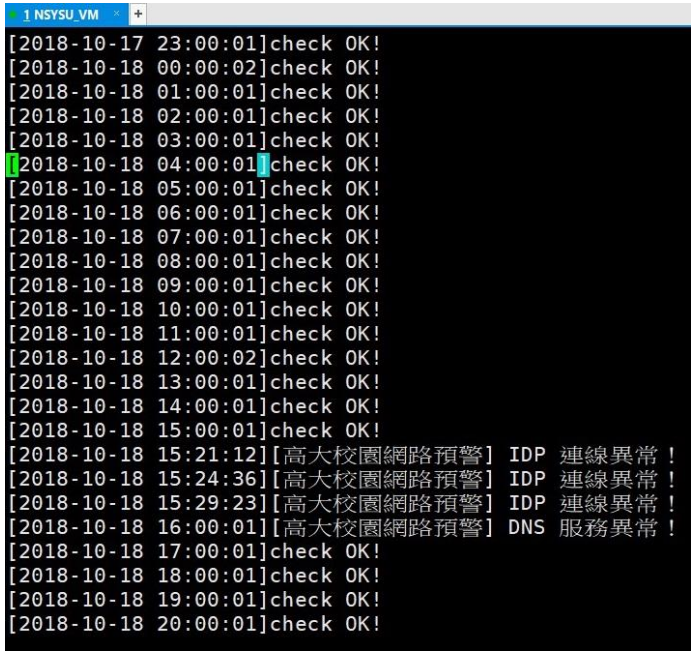
連線單位網路技術支援

雲端虛擬主機服務 (1/2)

- 提供2CPU, 1GB RAM, 40GB硬碟空間
- 已有13所連線單位提出申請(2縣市網路中心、6所科大及5所一般大學)
  - 今年新增高雄大學申請
- DNS Slave虛擬機範本：可直接複製修改使用 (和春技術學院提供)
- 敬請多加利用，申請網址：http://goo.gl/forms/693L2LReZG

雲端虛擬主機服務 (2/2)

- 連線單位申請區網中心VM服務
- 建置連線偵測服務PHP程式
- 偵測異常寄簡訊通知

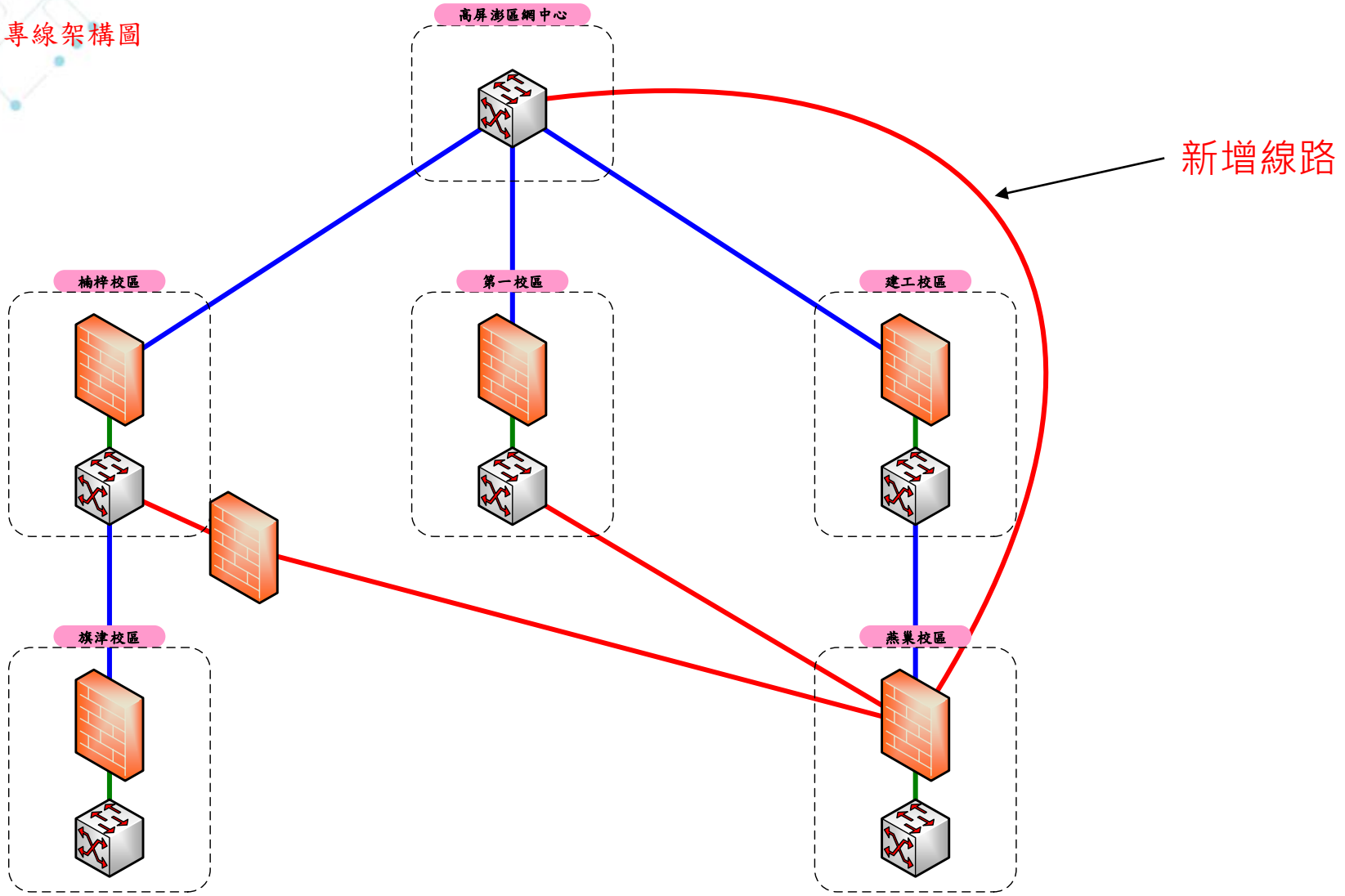


連線單位頻寬升級支援 (1/2)

- 高雄應用科技大學、高雄第一科技大學、高雄海洋科技大學正式合併成「高雄科技大學」
- 合併後資料中心設置於燕巢校區
- 燕巢校區新增一條1G線路至區網中心

連線單位頻寬升級支援(2/2)

整體專線架構圖



教育訓練辦理情形

CEH駭客技術專家認證課程

- 與台北第二區網中心(政治大學)合作主辦Certificated Ethical Hacker(CEH)課程圓滿完成
- 活動日期：7/3~7/5, 7/10~7/12日
- 活動花絮

教育訓練辦理情形 (1/2)

時間	主題
3月7日	區網中心網站弱點掃瞄服務改版說明研討會
3月23日	「個人資料管理制度內部稽核實務」研討會
4月13日	「教育機構個人資料保護」研討會
5月14日	「Suricata Open Source IPS系統」及「中介軟體導向(Middleware-oriented)遠端控制之應用 」
5月28日	網路封包與異常行為分析實務
6月22日	Cuckoo Sandbox惡意程式分實務
7月6日	IPv6 DNS及Web Server建置講習

教育訓練辦理情形 (2/2)

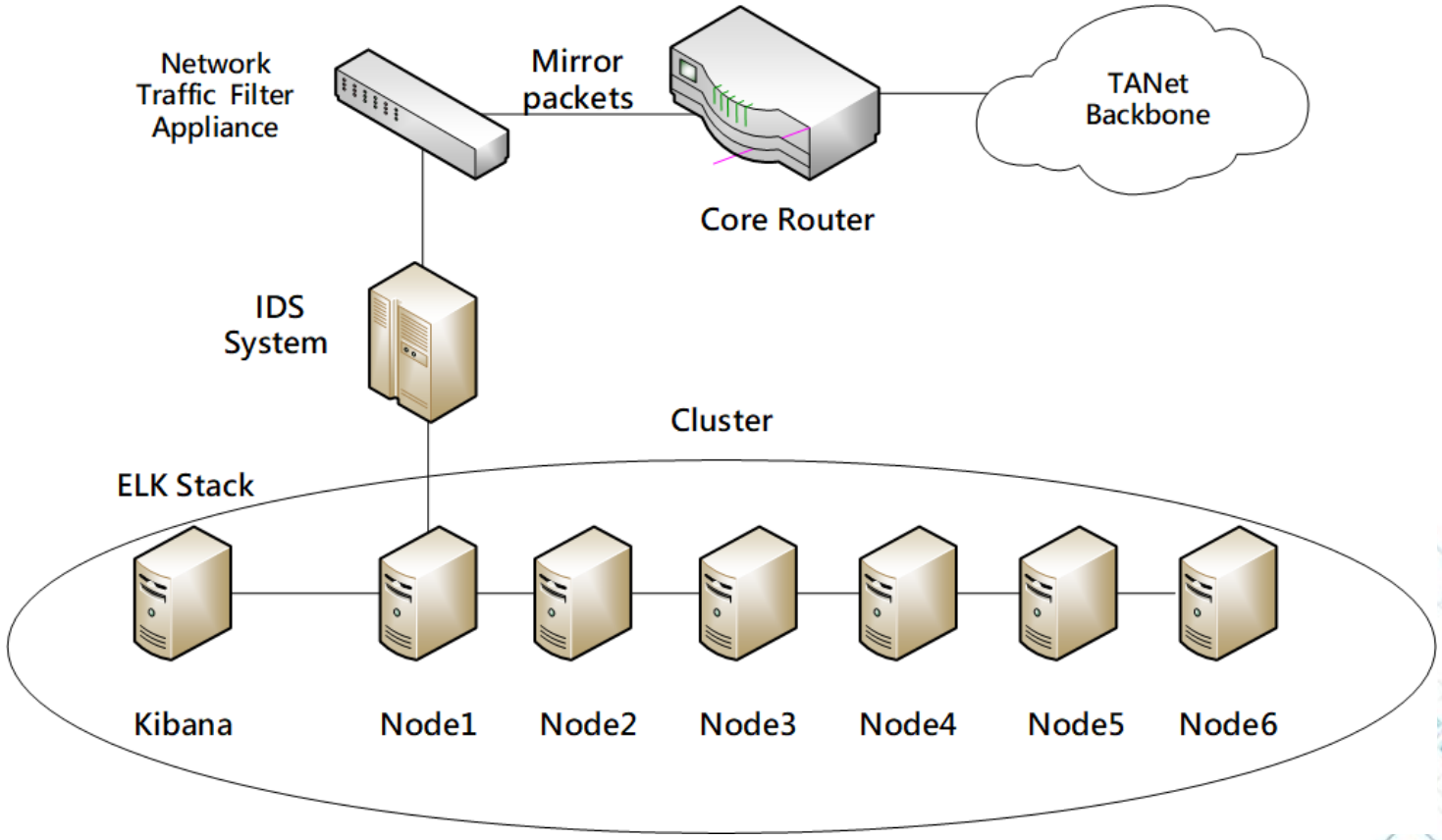
時間	主題
7月3日~5日	CEH道德駭客認證課程(一)(與台北第二區網中心聯合舉辦)
7月10日~12日	CEH道德駭客認證課程(二)(與台北第二區網中心聯合舉辦)
7月16日	「雲端應用服務安全與檢測實務(一)」研討會
7月17日	「雲端應用服務安全與檢測實務(二)」研討會
9月18日	「個資管理新挑戰-GDPR」研討會
10月19日	區網中心網路技術分享及交流研討會議
10月26日	新型破壞式攻擊分析與防禦方案

創新特色服務

- 區網中心IDS服務 → TANET 2018 論文發表
- 資安系統自動化部署 → TANET 2018 論文發表
- OpenVAS弱點掃瞄系統
- 誘補系統(Honeypot)
- 偏鄉服務

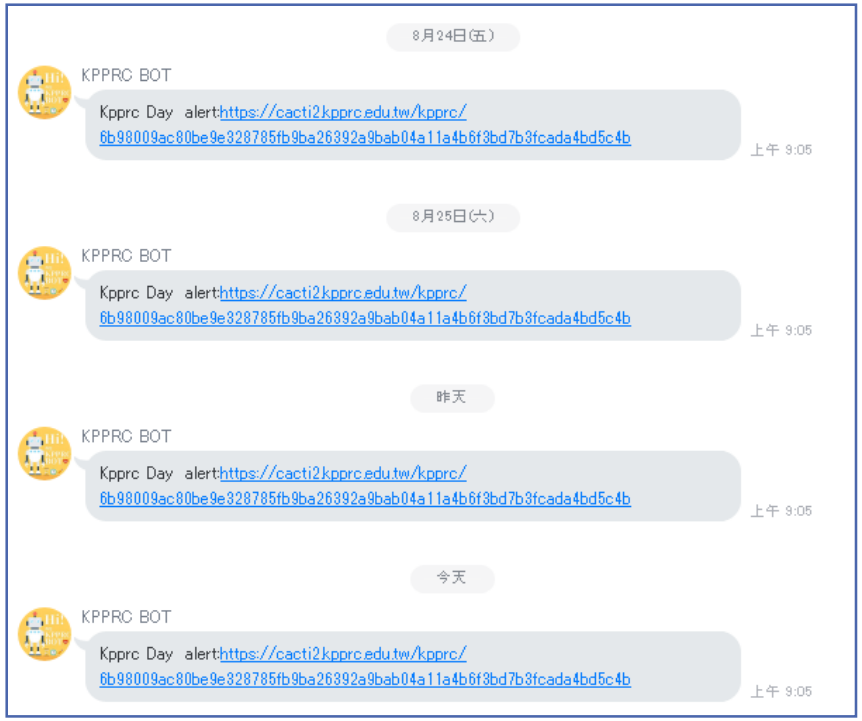
區網中心IDS服務升級及更新

- 偵測流量: 1G -> 10G
- 伺服器數量:3->7
- Suricata 版本更新: 4.0.4
- ELK 版本更新至：6.4.0



區網中心IDS Line Bot

- KPPRC BOT IDS Alert主動訊息通知
- Python程式語言開發

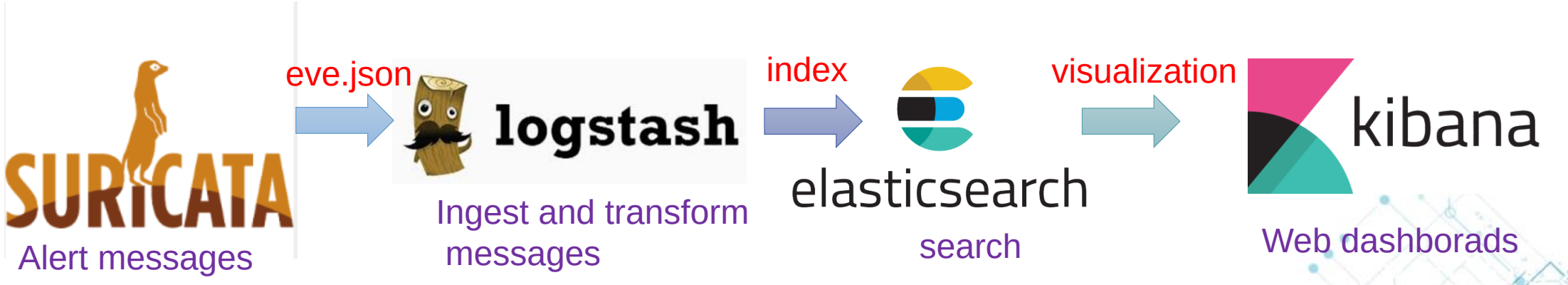


KPPRC Daily Alert

#	time	連線單位	Alert Signature	Source IP and Port	Dest IP and Port
1	2018-08-22 10:59:50.857000+00:00	澎湖縣	ET P2P BitTorrent DHT ping request	192.168.0.102:21352	140.127.X.X:6881
2	2018-08-22 11:03:33.093000+00:00	高雄縣	ET POLICY possible Xiaomi phone data leakage DNS	140.127.11.X:19028	14.215.5.X:53
3	2018-08-22 11:11:58.340000+00:00	屏東縣	ET EXPLOIT ETERNALBLUE Exploit M2 MS17-010	163.24.X.X:52291	103.80.X.X:445
4	2018-08-22 11:13:33.581000+00:00	屏東縣	ET POLICY possible Xiaomi phone data leakage DNS	163.24.20.X:59709	8.8.8.8:53
5	2018-08-22 11:17:12.784000+00:00	屏東縣	ET EXPLOIT ETERNALBLUE Exploit M2 MS17-010	163.24.155.X:53914	103.80.239.77:445

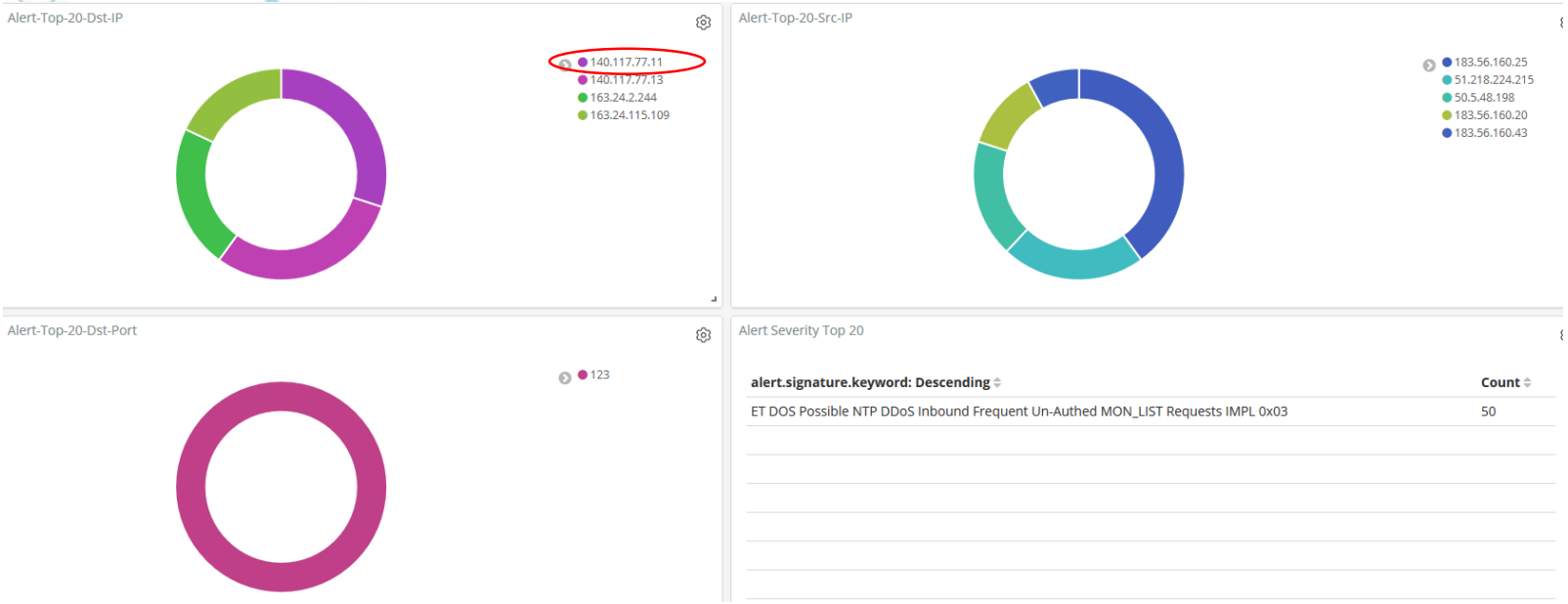
成果及論文發表

- 主題：Intrusion Detection System with ELK Stack and Line Bot Notification
- 中央大學TANet 2018發表



IDS成功偵測NTP攻擊

IDS成功偵測畫面



TACERT資安事件單

2018/8/20 (週一) 上午 08:17
service <service@cert.tanet.edu.tw>
(事件單編號:AISAC-148629)(告知通報)入侵事件警訊
收件者 service@cert.tanet.edu.tw

教育機構資安通報平台

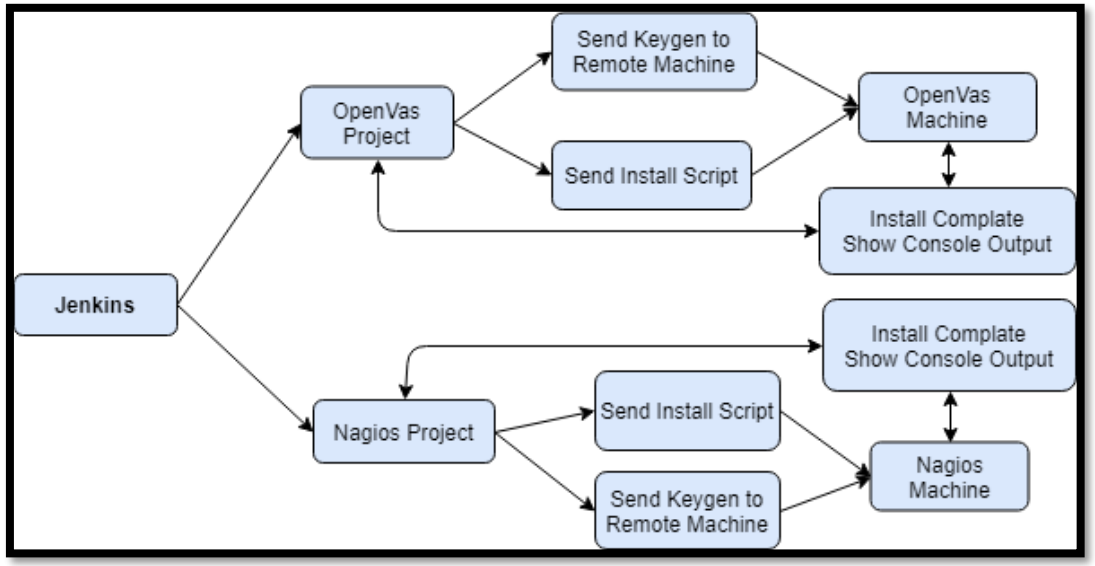
事件類型:入侵事件警訊

事件單編號:AISAC-148629

原發布編號	ASOC-INT-201808-0835	原發布時間	2018-08-20 08:17:22
事件類型	對外攻擊	原發現時間	2018-08-19 19:08:18
事件主旨	通報:[國立中山大學]140.117.77.11 NTP.Monlist.Command.DoS		
事件描述	ASOC發現貴單位(國立中山大學)所屬 140.117.77.11 疑似對外進行 NTP.Monlist.Command.DoS 攻擊		
手法研判	網路時間協定(Network Time Protocol，NTP)，NTP主要在提供網路上可以進行網路校時的功能。在NTP v4.2.7p26之前的版本存有多個安全漏洞，貴單位疑似對外進行非法的入侵攻擊，Monlist是NTP的舊版本，透過一個未經身份驗證系統發送請求，連接到該伺服器最後600主機列表的遠程命令，遠端攻擊者透過發出請求，並偽造封包返回地址，進而達成阻斷式服務(DoS) 攻擊。 影響版本： NTP before 4.2.7p26		
建議措施	惠請貴單位： 1.檢查防火牆紀錄：查看內部是否有開啟異常的連接埠。 2.利用工具程式(如:TCPview、procexp)於來源主機觀察，找出實際執行連線的程式，確認該程式是否為惡意程式。 3.若連線並非預期行為，則來源主機可能已遭植入惡意程式，建議利用木馬或後門清除程式掃瞄該主機，並手動檢測是否有惡意程式執行。 4.檢視及執行各系統之安全修補，並升級NTP至4.2.7版本。 5.透過指令NOQUERY在NTP conf文件啟用啟動NTP守護進程，這將禁止訪問模式6和7查詢packetts（包括monlist）。6.請參閱-FortiGuard-http://www.fortinet.com/ids/VID38074 CVE - Common Vulnerabilities and Exposures (CVE) http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5211 Hackers Spend Christmas Break Launching Large Scale NTP-Reflection Attacks http://www.symantec.com/connect/blogs/hackers-spend-christmas-break-launching-large-scale-ntp-reflection-attacks		
參考資料	無		
此事件需要進行通報，請 貴單位資安聯絡人登入資安通報應變平台進行通報應變作業			
如果您對此通告的內容有疑問或有關於此事件的建議，歡迎與我們連絡。			

資安系統自動化部署 (1/2)

- 自動化部署OpenVAS(弱掃系統)、Nagios(服務偵測系統)
- 透過Jenkins持續整合軟體，同時進行部署，並訂制OpenVAS、Nagios標準化部署流程
- 於區網第一次管理會技術會議中分享



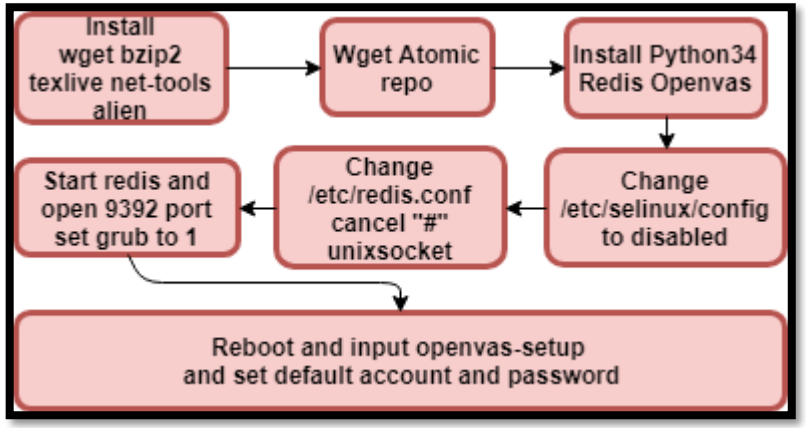
資安系統自動化部署 (2/2)

- 應用持續整合(DevOps)的概念將部署流程自動化
- 比較自動化部署與人工部署OpenVAS及Nagios資安系統所耗費之時間，發現使用自動化部署，可節省大量部署時間，減少在建置基礎環境及日常維運所耗費的時間

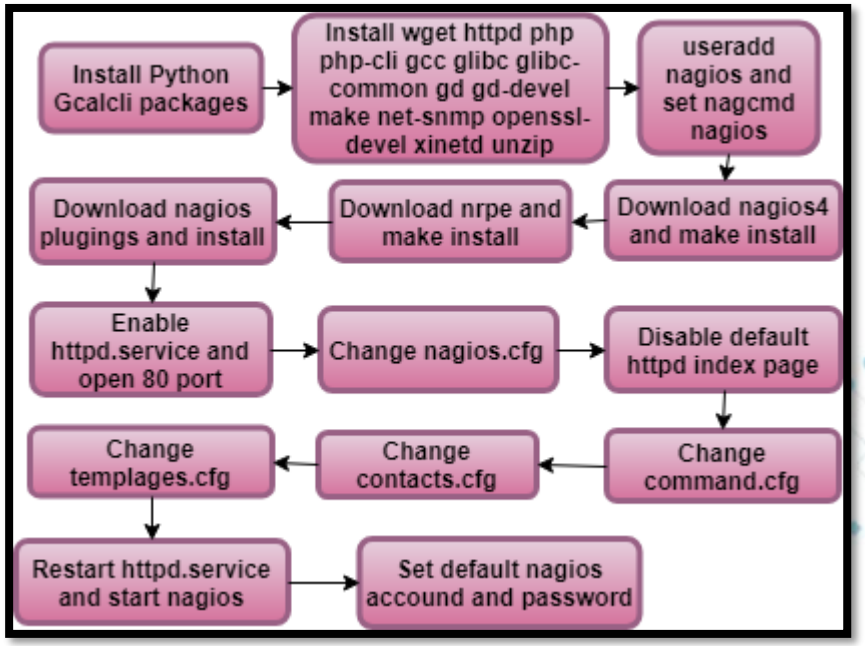
ITEM	Our Approach	Manual Deployment
OpenVAS	23m14s	35m23s
Nagios	14m	18m54s
Total Time	23m14s (At the same time)	53m17s

成果及論文發表

- 主題：資安系統之自動化持續部署與驗證-以OpenVAS及Nagios為例
- 中央大學TANet 2018發表



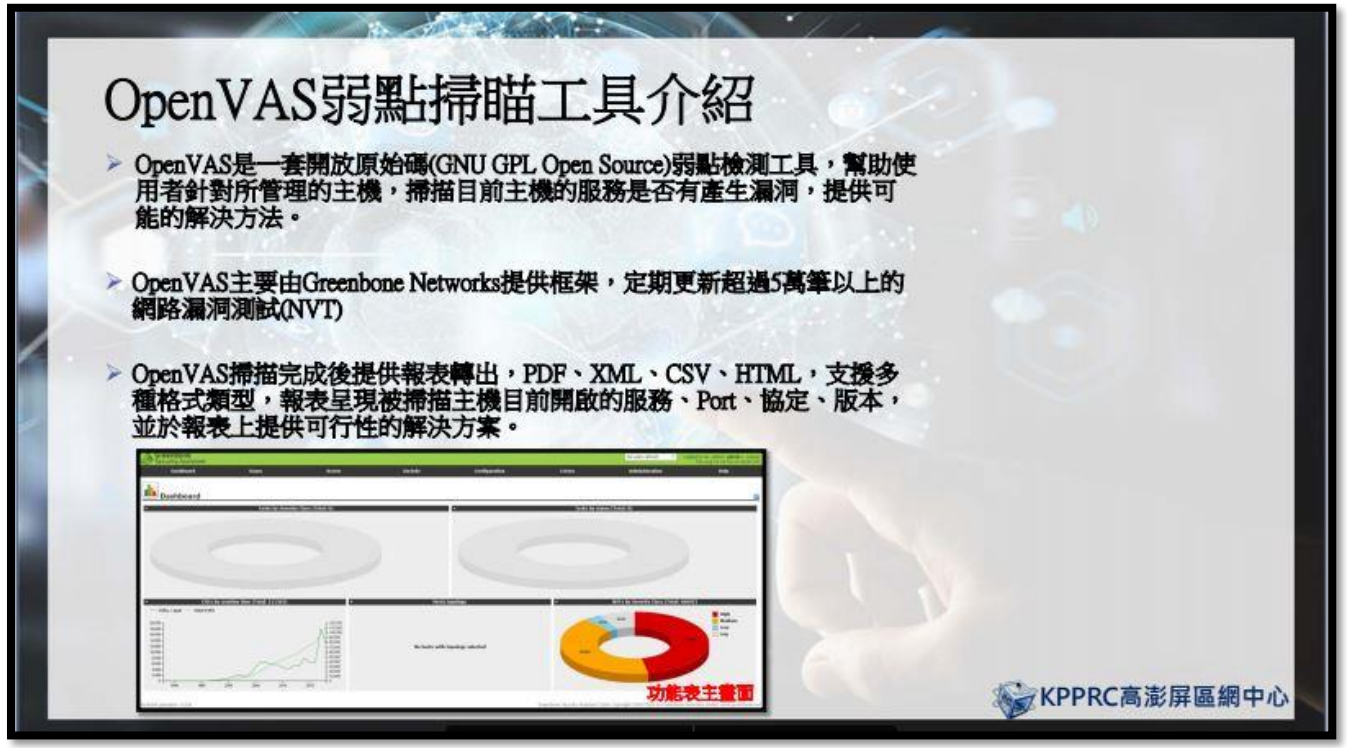
OpenVAS-部署流程圖



Nagios-部署流程圖

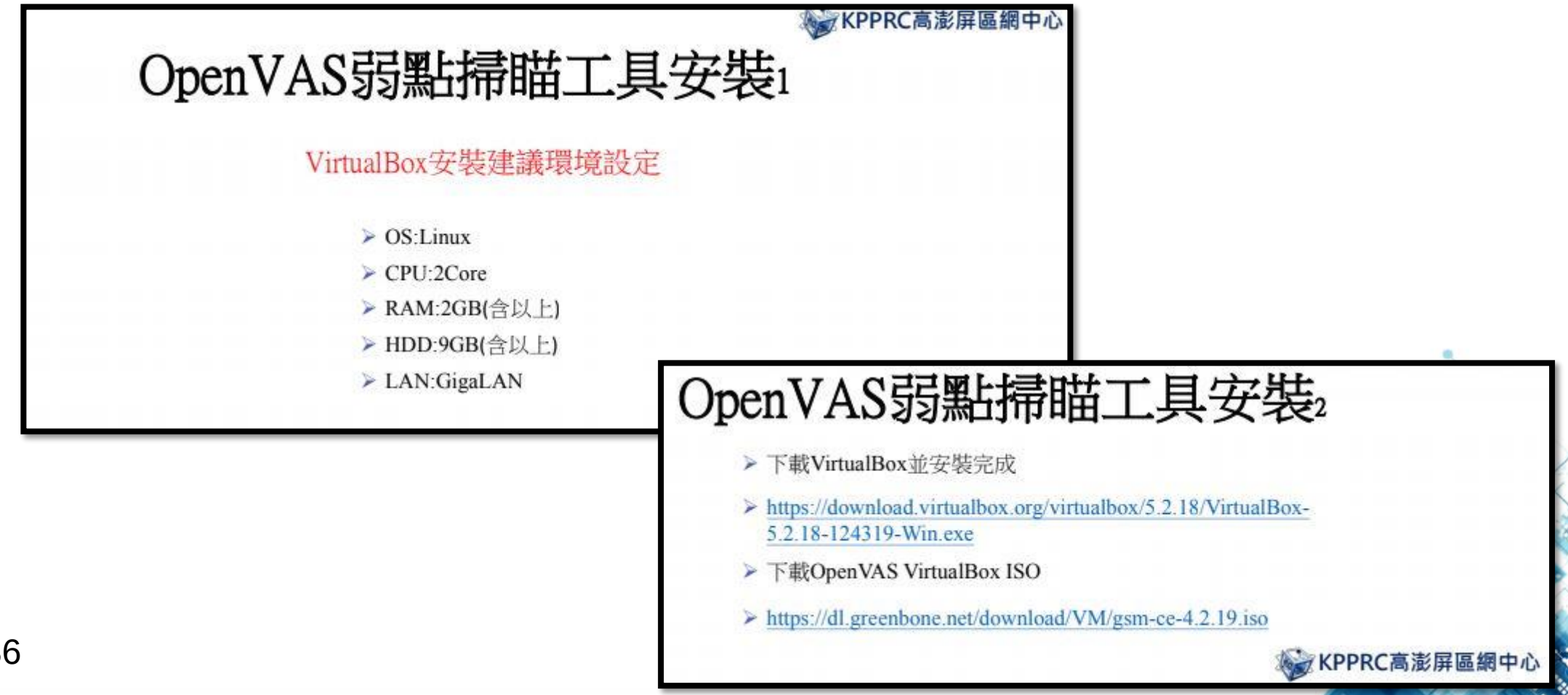
弱點掃描工具實作教材 (1/3)

- 運用OpenVAS弱掃工具程式，提升下轄單位，資安弱點防護能力
- 定期自行健診、系統更新，減低資安事件產生。
- 教材分享:區網網站>區網系統服務專區>弱點掃描工具安裝實作



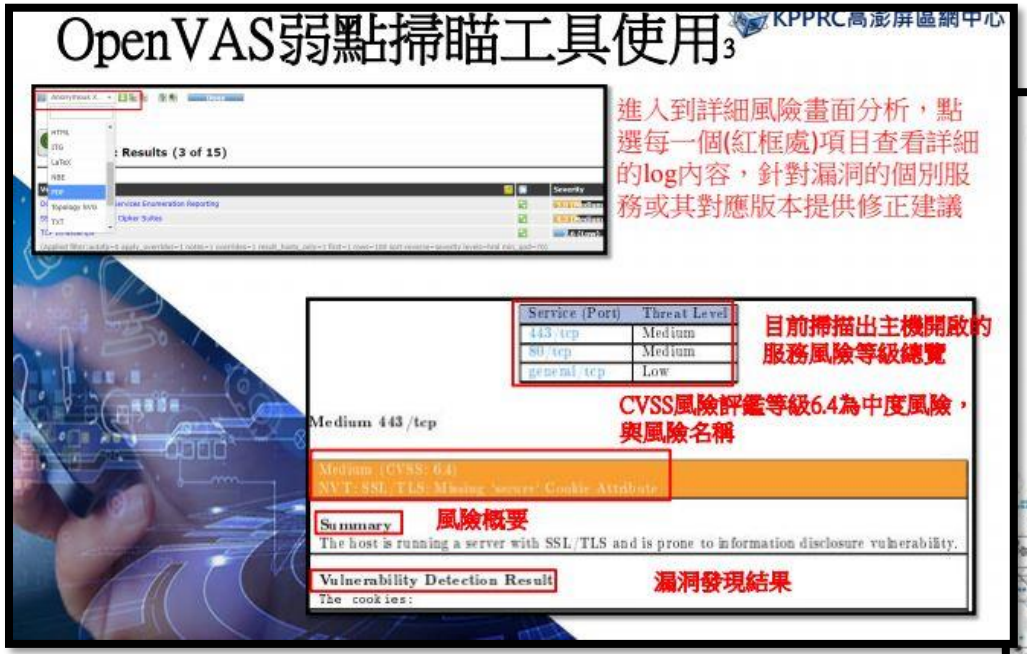
弱點掃描工具實作教材 (2/3)

- 系統需求說明、檔案載點



弱點掃描工具實作教材 (3/3)

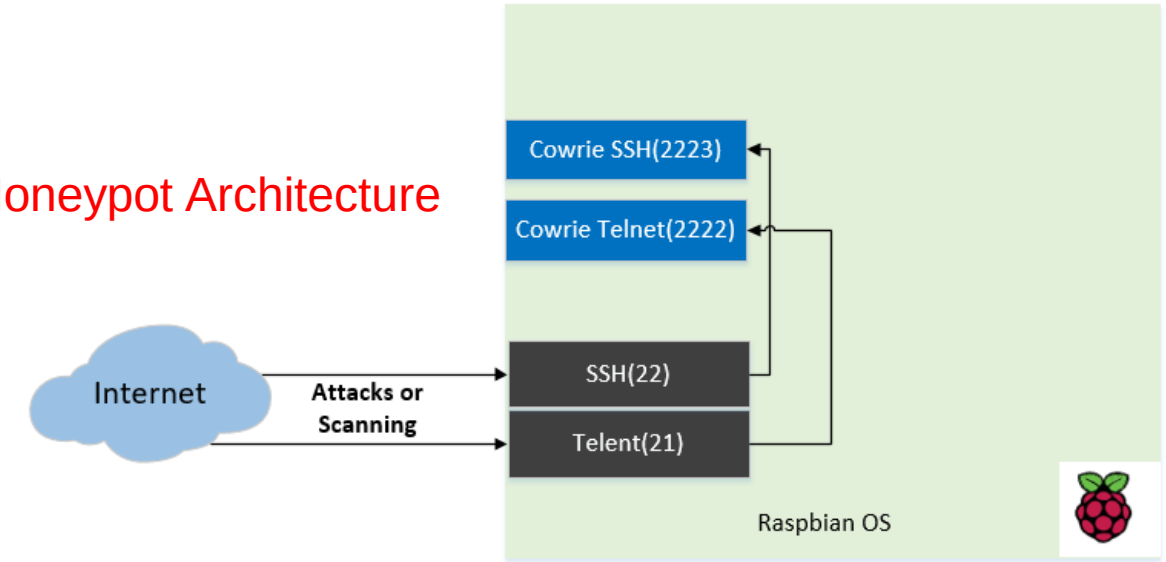
- 工具使用、結果判讀



區網誘補系統(Honeypot)

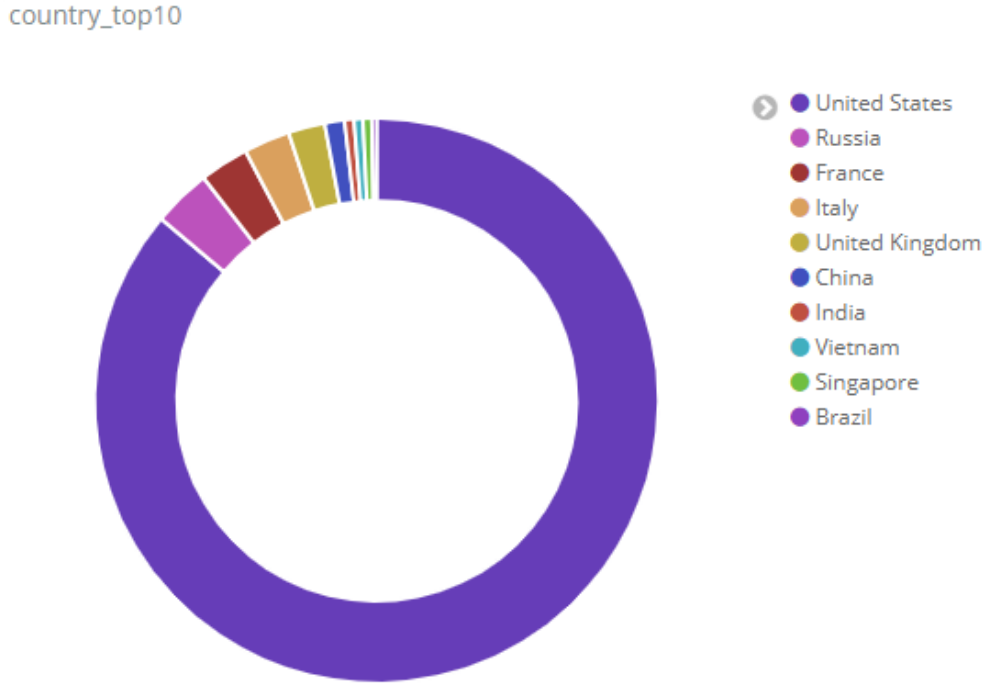
- Hardware: Raspberry Pi 3
- Operating System: Raspbian
- Honeypot Software : Cowrie (SSH & TELNET)

Honeypot Architecture



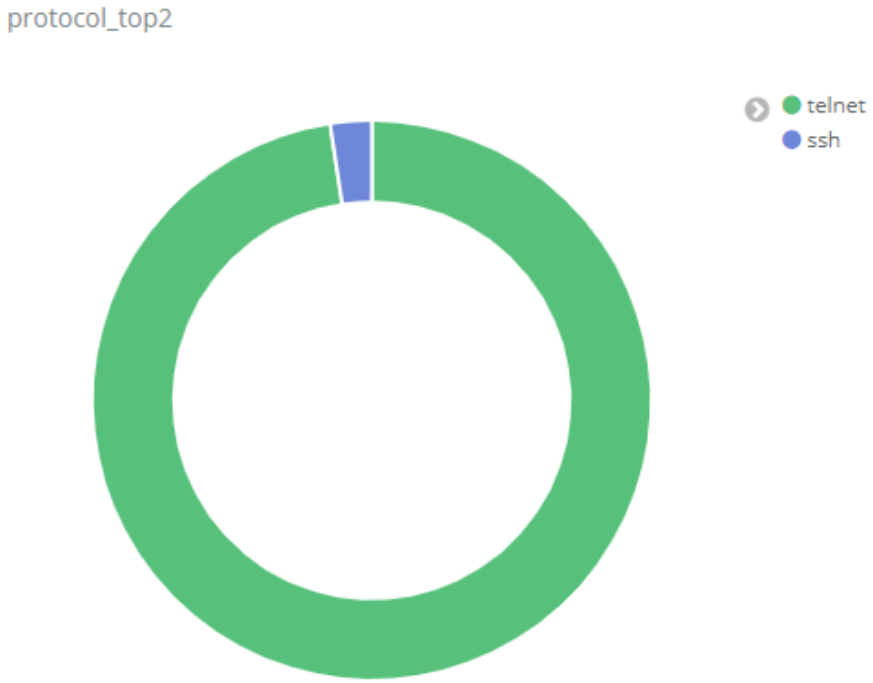
誘補系統佈署結果(1/2)

- Country Top 10



- US: 86.16%
- Russia: 3.33%
- France: 2.81%
- Italy: 2.65%

- Protocol Top 2



- Telnet: 97.62%
- SSH: 2.38%

誘補系統佈署結果(2/2)

- Username Top 10

username_top20_datatable

username.keyword: Descending	Count
root	166,084
enable	10,556
shell	10,120
admin	4,722
default	2,141
guest	1,260
user	650
support	541
sh	506
adm	288

- Password Top 10

password_top20_datatable

password.keyword: Descending	Count
123456	17,695
admin	17,497
vizxv	15,599
888888	13,274
xc3511	13,267
system	10,290
sh	9,833
xmhdipc	9,076
root	8,913
00000000	8,618

- Input Command Top 10

top20_input

input.keyword: Descending	Count
shell	304,620
enable	152,743
sh	152,170
cat /proc/mounts	133,553
ps	133,497
echo -e \x6b\x61\x6d\x69	133,429
/bin/busybox echo -e '\x6b\x61\x6d\x69' > /.nippon; /bin/busybox cat /.nippon; /bin/busybox rm /.nippon	133,425
/bin/busybox ECCHI	125,778
/bin/busybox ps; /bin/busybox ECCHI	125,752

偏鄉服務及遠距教學

107年度偏鄉服務場次表

日期區間	地點	教學類型	教學內容
107/01/25	屏東潮東國小	資訊營	資安概念講習電腦硬體組裝
107/01/29~30	澎湖中興國小 澎湖隘門國小	種子教師營 資訊營	資安攻防實作 Scratch教學
107/02/02	屏東興華國小	資訊營	資安概念講習電腦硬體組裝

澎湖中興、隘門國小種子教師、資訊營

屏東潮東國小資訊營

圖書資訊偏遠地區服務列車

圖書資訊偏遠地區服務列車
主辦單位:國立中山大學(National Sun Yat-sen University)、高屏澎區網中心

圖書資訊偏遠地區服務列車

連線單位需求分析及滿意度調查

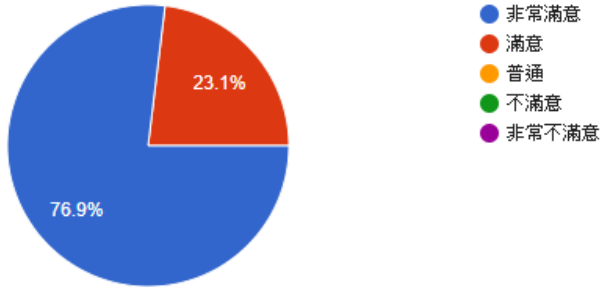
- 區網服務滿意度問卷調查
- 連線單位需求分析

服務滿意度問卷調查結果 (1/2)

- 今年75%以上連線單位達到非常滿意 (106年70%)

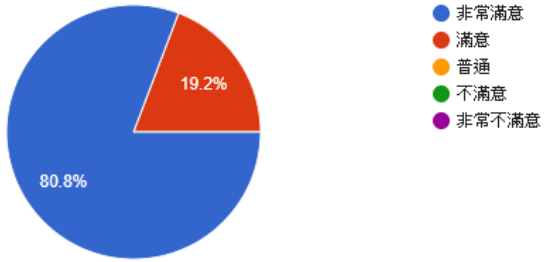
2 . 本年度區網中心對　貴校(單位)之網路連線服務，您認為是否滿意？

26 則回應



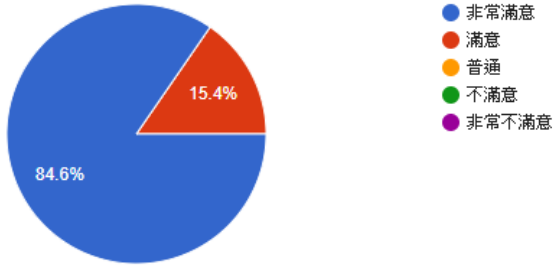
3. 本年度貴校(單位)如有網路管理或連線的技術諮詢時，區網中心的協助是否符合您的需求？

26 則回應



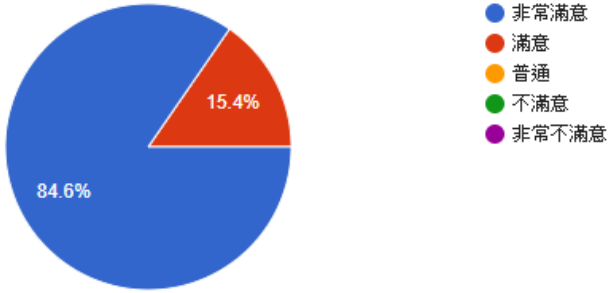
4. 召開區域網路中心之管理會，提供連線服務學校(單位)意見交流的機會：

26 則回應



5. 資通安全事件的通報應變的協助處理：

26 則回應

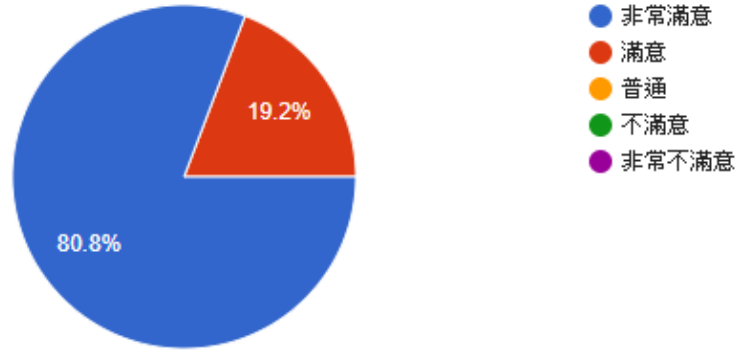


服務滿意度問卷調查結果 (2/2)

➢今年服務人員熱忱及親和力非常滿意達96.2% (106年80%)

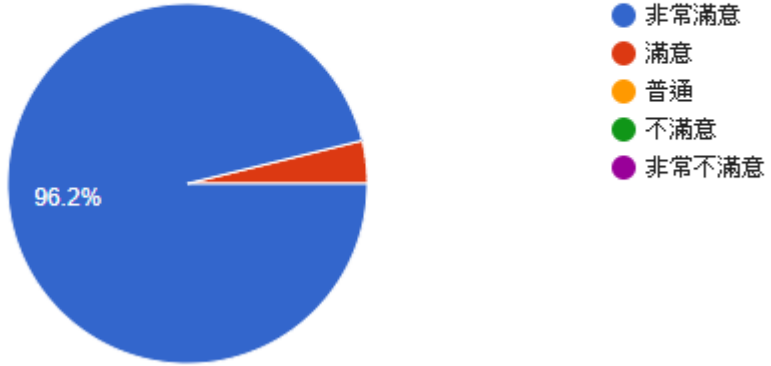
7. 聯繫協調與溝通管道上：

26 則回應



10. 貴校(單位)對於區網中心服務人員之熱忱及親和力的滿意度？?

26 則回應



連線單位需求分析(問卷調查)

- 區網中心待辦事項
  - 建置TANET整體防禦網絡，阻絕惡意IP(網站)連線。
  - 分享校內實際發生案例及處理建議
  - 希望可以更快落實各校申裝10G需求
- 向鈞部建議事項
  - 人力、經費不足

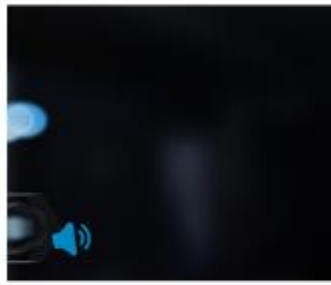
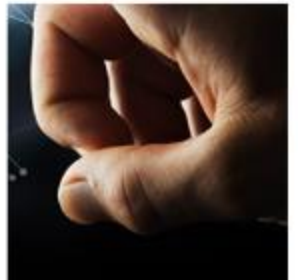
未來營運目標

108年度預計推動之重點工作(1/2)

- 虛擬容器導入持續整合自動化部署弱掃系統
- 誘補系統(Honeypot)持續精進
- IDS系統服務持續維運及改進
- 推動持續整合開發實作應用教學
- DNS升級及資安健檢服務持續推動

108年度預計推動之重點工作(2/2)

- 資安弱點及威脅情資整合
- 持續推動區網網站服務導入IPV6
- 協助連線單位有關TANet連線及資安相關問題排除
- 持續推動區網中心與連線單位夥伴技術分享
- 持續加強網路連線管理機制

敬請　委員指教

謝謝!!