臺灣資安大會
CYBERSEC 2019

IT人轉職資安人的起手式

博格企業資安讀書會 創辦人 X1

PRESENTED BY iThome

About Me

社群代號:

資安黑武士/ X1

社群經歷:

博格企業資安讀書會 創辦人

中華民國無店面零售商業同業公會 -資安防護講座講師

TDOH 2017 - 反抗無用，接受進步 (北韓惡意樣本分析)

TDOH 2018 - 企業防禦 DDoS 方式與探討 – 工作坊講師

HITCON Defense 2018 技術總招

聲明

想分享一切所知卻受束縛的資安人，深怕打開潘朵拉盒子，引起殺生之禍 / 查水表 / 歡樂送 / 失業，只能蒙上面具，以黑武士奉獻自己的淺學

本人對外之言行及演講內容均與本人服務公司無關，亦不代表公司立場

議程

- 本議程適用對象&目標
- 資安問題怎麼辦？
- 問題討論(Q&A)

臺灣資安大會
CYBERSEC 2019

議程

PRESENTED BY iThome

臺灣資安大會
CYBERSEC 2019

本議程適用對象&目標

PRESENTED BY iThome

本議程適用對象

IT人轉職資安人

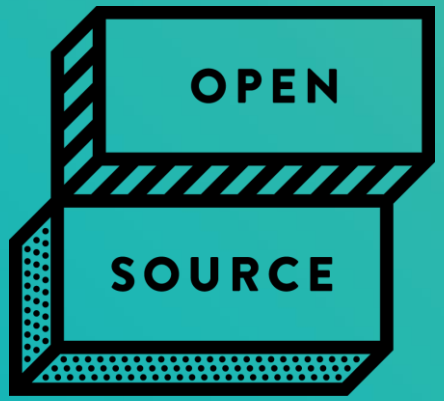
中小企業主

預算有限的朋友

本議程目標

How to start

搜索簡報的關鍵字

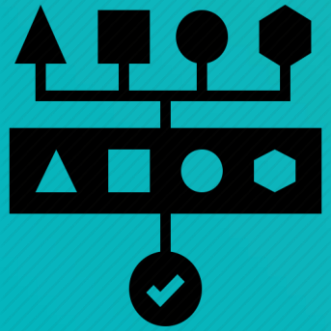


低預算也很安全

特別注意的風險 ！！

Open Source 和 商用付費還是有差異的 !!

壞了要自己修



自己的資料自己分析

花時間研究和部署

更新與相容問題

臺灣資安大會
CYBERSEC 2019

資安問題怎麼辦？

PRESENTED BY iThome

資安問題怎麼辦？

事前
- 所有資產做過資安盤點了嗎？
- Internet出入口/雲端服務 如何整合、管制?
- 到底開了多少對外服務?
- 是否都更新了?
- 我的伺服器在幹嘛？有人登入了？

事中
- 網站DDoS翻了，怎麼辦
- 我的網站是破口嗎？
- 被入侵! 馬上重灌?

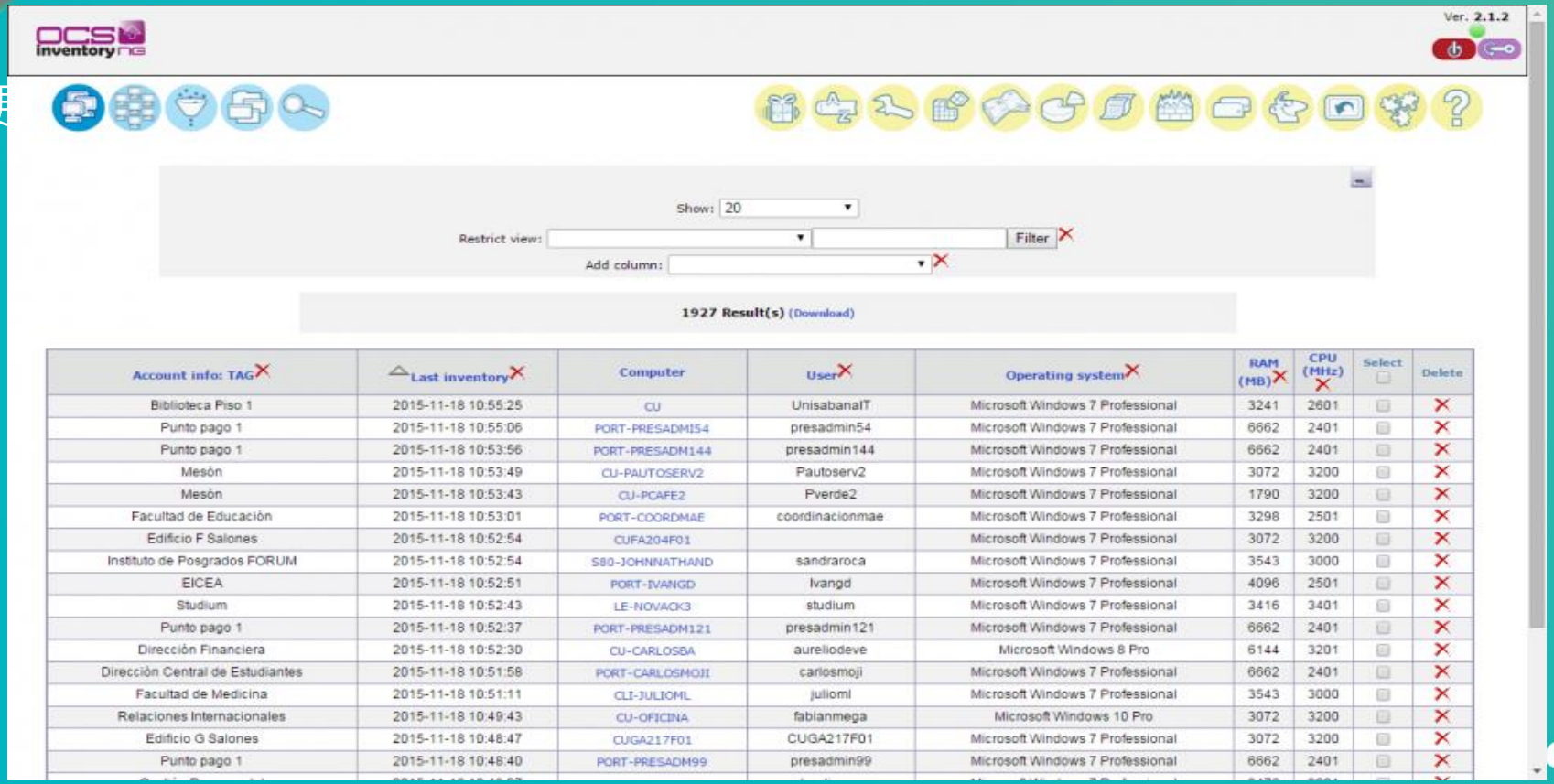
事後
- 資安事件處理、通報，做到位了嗎?
- 防毒軟體防不了駭，怎麼辦?
- 未收集的AP/DB Log如何補救?

資安問題怎麼辦？

硬體：OCS Inventory – 記錄所有用戶以利資安盤點

資安問題怎麼辦？

硬



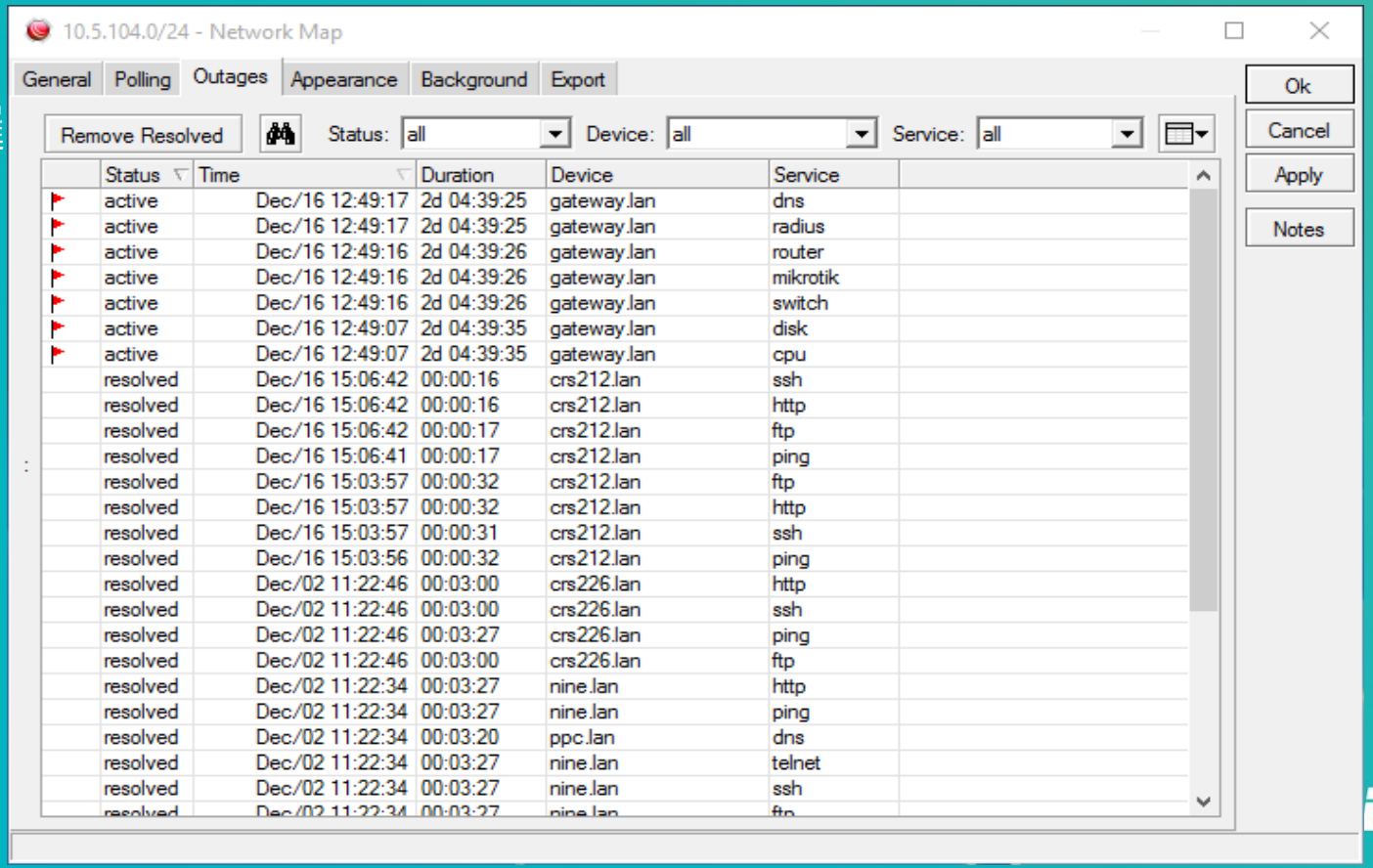
Account info: TAG	Last inventory	Computer	User	Operating system	RAM (MB)	CPU (MHz)	Select	Delete
Biblioteca Piso 1	2015-11-18 10:55:25	CU	UnisabanalT	Microsoft Windows 7 Professional	3241	2601		
Punto pago 1	2015-11-18 10:55:06	PORT-PRESADMI54	presadmin54	Microsoft Windows 7 Professional	6662	2401		
Punto pago 1	2015-11-18 10:53:56	PORT-PRESADM144	presadmin144	Microsoft Windows 7 Professional	6662	2401		
Mesón	2015-11-18 10:53:49	CU-PAUTOSERV2	Pautoserv2	Microsoft Windows 7 Professional	3072	3200		
Mesón	2015-11-18 10:53:43	CU-PCAFE2	Pverde2	Microsoft Windows 7 Professional	1790	3200		
Facultad de Educación	2015-11-18 10:53:01	PORT-COORDMAE	coordinacionmae	Microsoft Windows 7 Professional	3298	2501		
Edificio F Salones	2015-11-18 10:52:54	CUFA204F01		Microsoft Windows 7 Professional	3072	3200		
Instituto de Posgrados FORUM	2015-11-18 10:52:54	S80-JOHNNATHAND	sandraroca	Microsoft Windows 7 Professional	3543	3000		
EICEA	2015-11-18 10:52:51	PORT-IVANGD	Ivangd	Microsoft Windows 7 Professional	4096	2501		
Studium	2015-11-18 10:52:43	LE-NOVACK3	studium	Microsoft Windows 7 Professional	3416	3401		
Punto pago 1	2015-11-18 10:52:37	PORT-PRESADM121	presadmin121	Microsoft Windows 7 Professional	6662	2401		
Dirección Financiera	2015-11-18 10:52:30	CU-CARLOSBA	aureliodeve	Microsoft Windows 8 Pro	6144	3201		
Dirección Central de Estudiantes	2015-11-18 10:51:58	PORT-CARLOSMOJI	carlosmoji	Microsoft Windows 7 Professional	6662	2401		
Facultad de Medicina	2015-11-18 10:51:11	CLI-JULIOML	julioml	Microsoft Windows 7 Professional	3543	3000		
Relaciones Internacionales	2015-11-18 10:49:43	CU-OFICINA	fabianmega	Microsoft Windows 10 Pro	3072	3200		
Edificio G Salones	2015-11-18 10:48:47	CUGA217F01	CUGA217F01	Microsoft Windows 7 Professional	3072	3200		
Punto pago 1	2015-11-18 10:48:40	PORT-PRESADM99	presadmin99	Microsoft Windows 7 Professional	6662	2401		

資安問題怎麼辦？

網路邏輯 : The Dude 盤點自己的網路

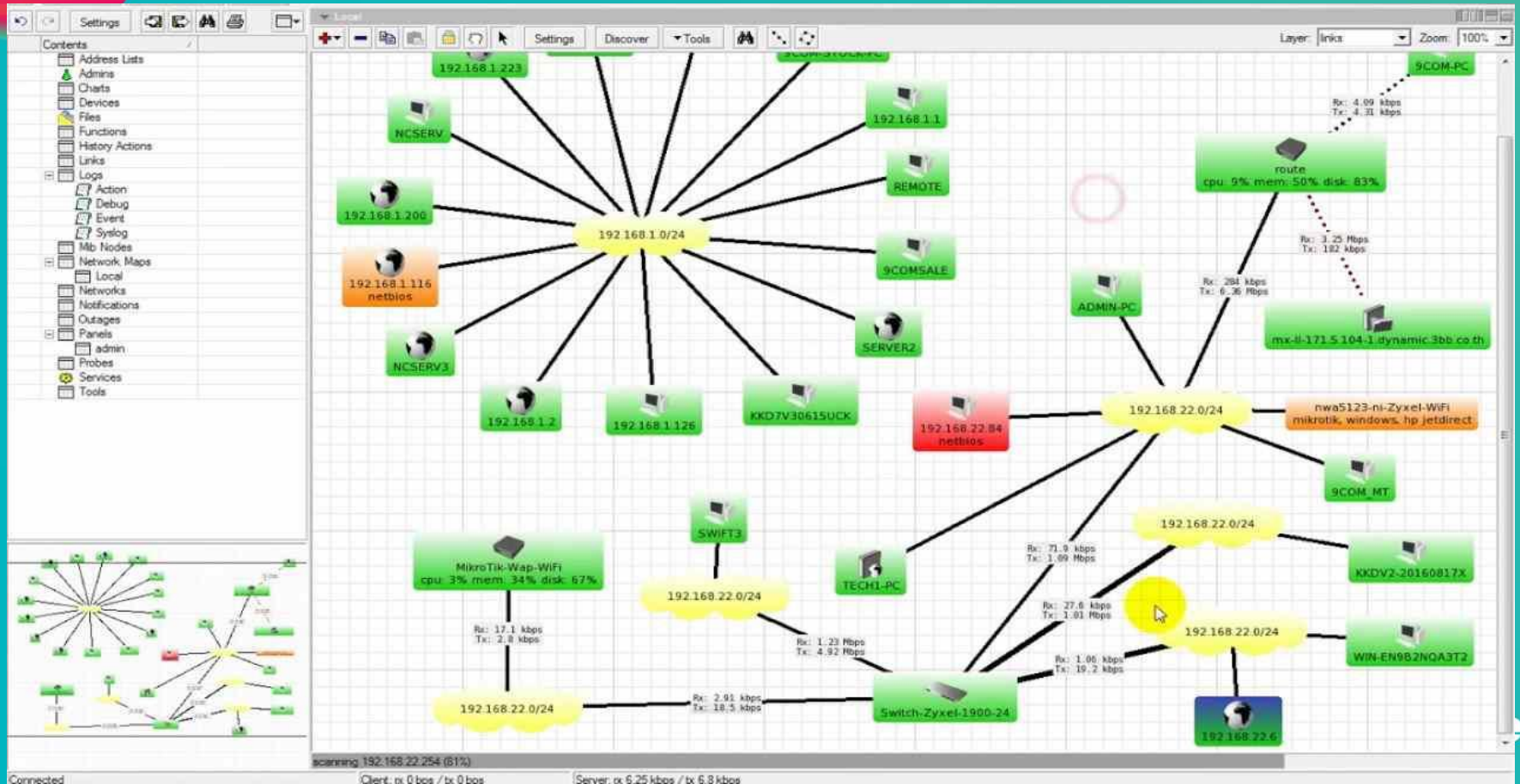
資安問題怎麼辦？

網路邏


10.5.104.0/24 - Network Map
General
Polling
Outages
Appearance
Background
Export
Ok
Cancel
Apply
Notes
Remove Resolved
Status: all
Device: all
Service: all
Status Time Duration Device Service
active Dec/16 12:49:17 2d 04:39:25 gateway.lan dns
active Dec/16 12:49:17 2d 04:39:25 gateway.lan radius
active Dec/16 12:49:16 2d 04:39:26 gateway.lan router
active Dec/16 12:49:16 2d 04:39:26 gateway.lan mikrotik
active Dec/16 12:49:16 2d 04:39:26 gateway.lan switch
active Dec/16 12:49:07 2d 04:39:35 gateway.lan disk
active Dec/16 12:49:07 2d 04:39:35 gateway.lan cpu
resolved Dec/16 15:06:42 00:00:16 crs212.lan ssh
resolved Dec/16 15:06:42 00:00:16 crs212.lan http
resolved Dec/16 15:06:42 00:00:17 crs212.lan ftp
resolved Dec/16 15:06:41 00:00:17 crs212.lan ping
resolved Dec/16 15:03:57 00:00:32 crs212.lan ftp
resolved Dec/16 15:03:57 00:00:32 crs212.lan http
resolved Dec/16 15:03:57 00:00:31 crs212.lan ssh
resolved Dec/16 15:03:56 00:00:32 crs212.lan ping
resolved Dec/02 11:22:46 00:03:00 crs226.lan http
resolved Dec/02 11:22:46 00:03:00 crs226.lan ssh
resolved Dec/02 11:22:46 00:03:27 crs226.lan ping
resolved Dec/02 11:22:46 00:03:00 crs226.lan ftp
resolved Dec/02 11:22:34 00:03:27 nine.lan http
resolved Dec/02 11:22:34 00:03:27 nine.lan ping
resolved Dec/02 11:22:34 00:03:20 ppc.lan dns
resolved Dec/02 11:22:34 00:03:27 nine.lan telnet
resolved Dec/02 11:22:34 00:03:27 nine.lan ssh

臺灣資安大會
CYBERSEC 2019

資安問題怎麼辦？



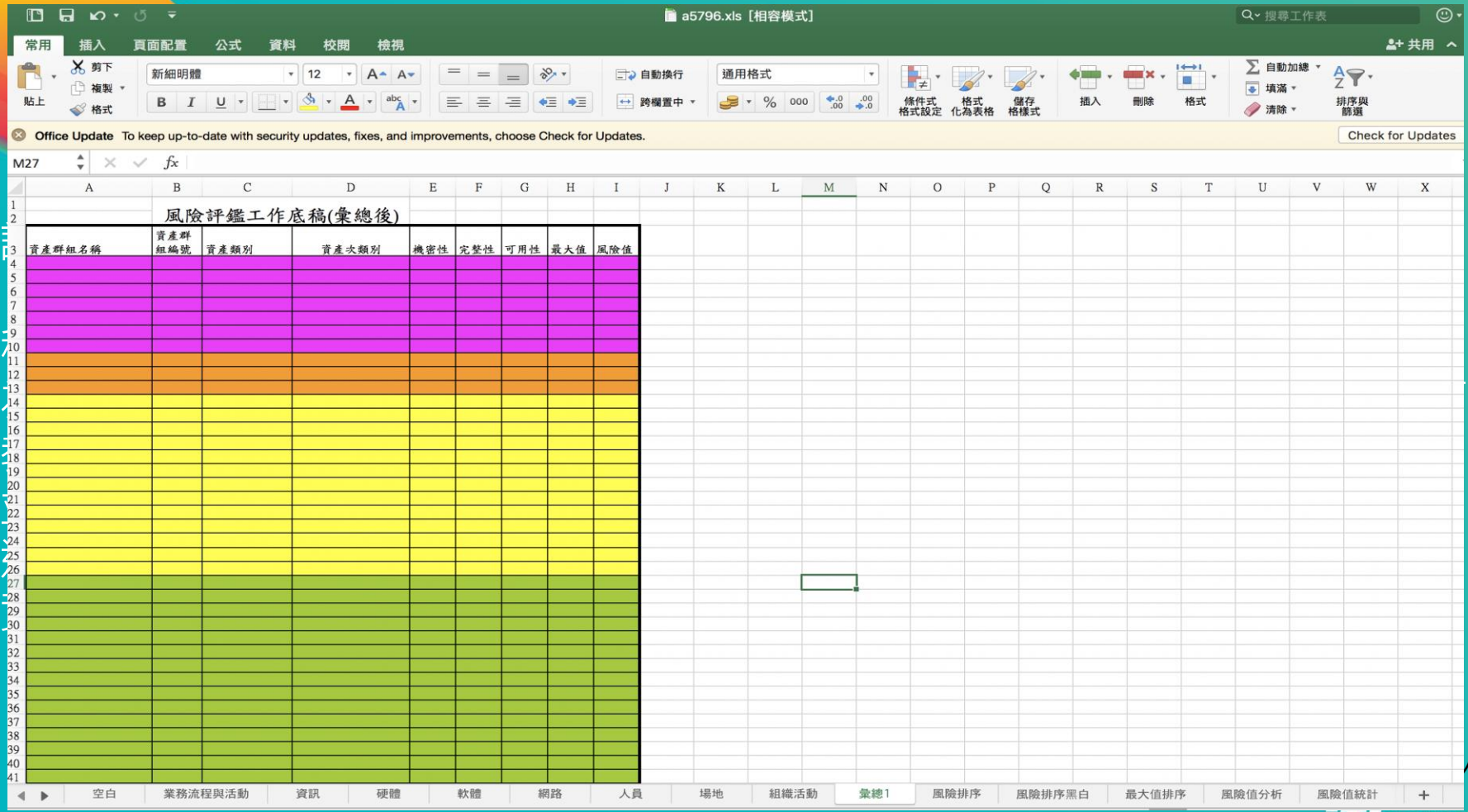
資安問題怎麼辦？

評估資安風險 – 範例表單 （新竹市稅務局）：

稅務資料處理過程中必須符合機密性、完整性及可用性，
為了達到這個目標及降低資訊作業風險，於2009年以專案方式聘請專業講師，
教導竹市稅務員工自行建置資訊安全管理系統，
並將攸關納稅人權益之退稅業務為核心業務納入驗證，
進而推動資安治理、制定各項文件等，其中，
資訊資產盤點表就是建置ISMS時不可或缺的文件。

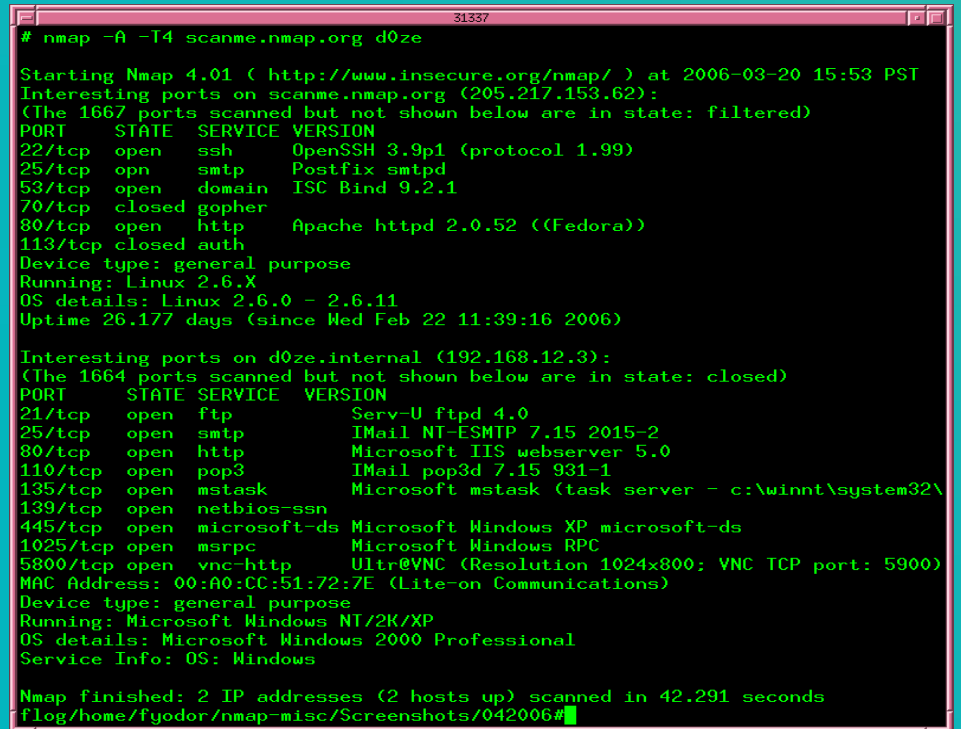
引用來源: 資安人

www.informationsecurity.com.tw/article/article_print.aspx?aid=5796



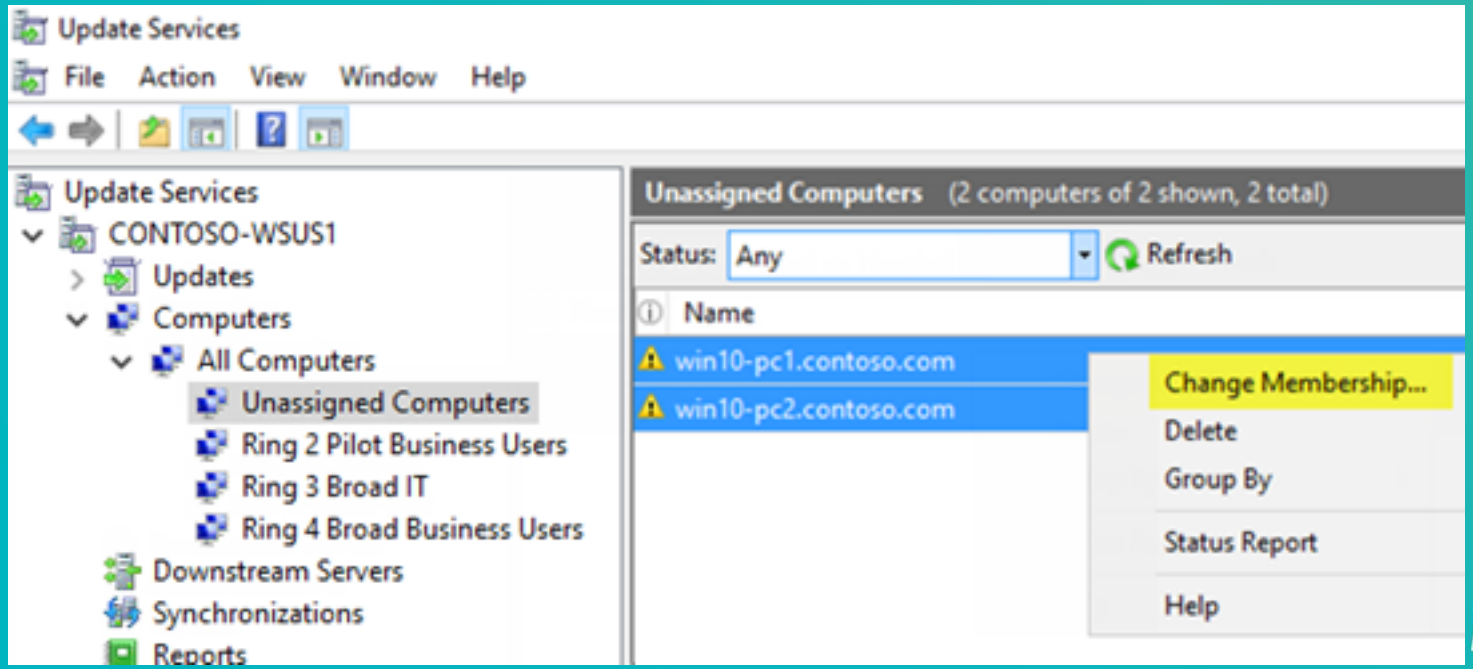
資安問題怎麼辦？

到底開了多少對外服務 – nmap 定期盤點您是否有不知道服務對外？



資安問題怎麼辦？

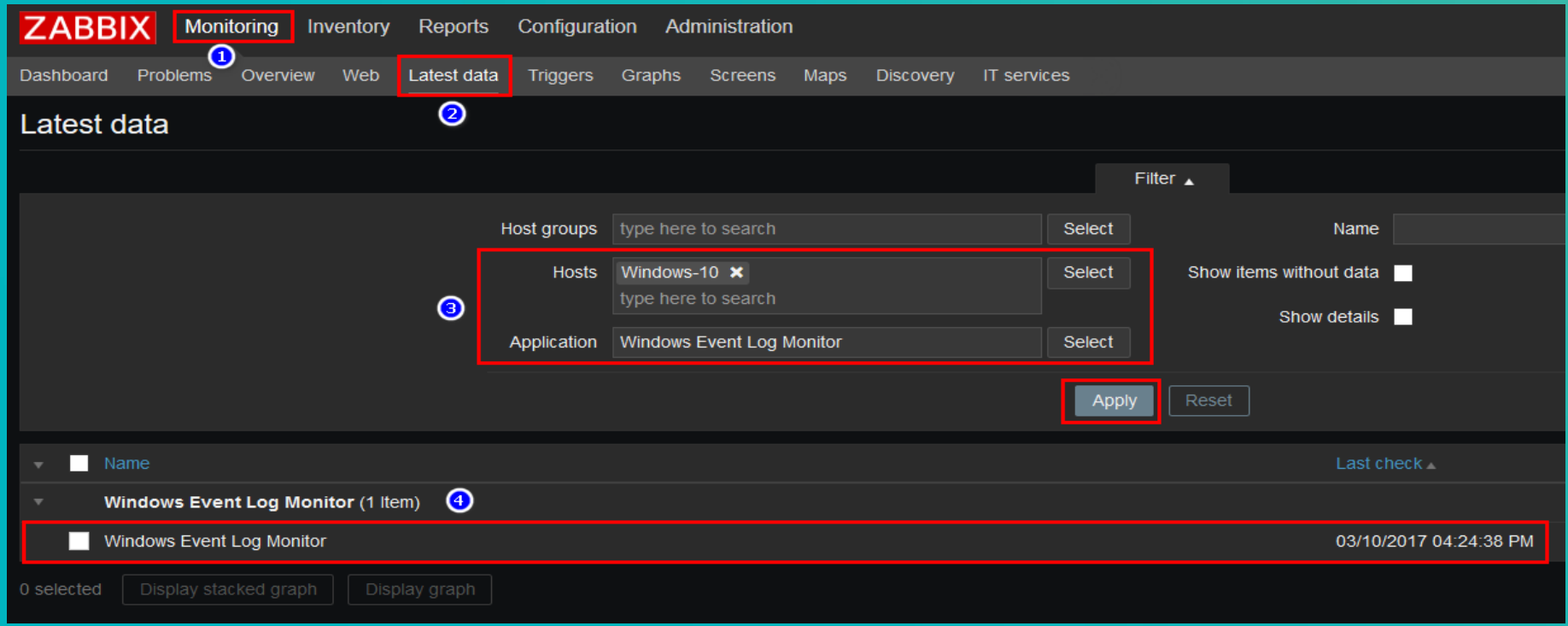
是否都更新了？ - WSUS



臺灣資安大會
CYBERSEC 2019

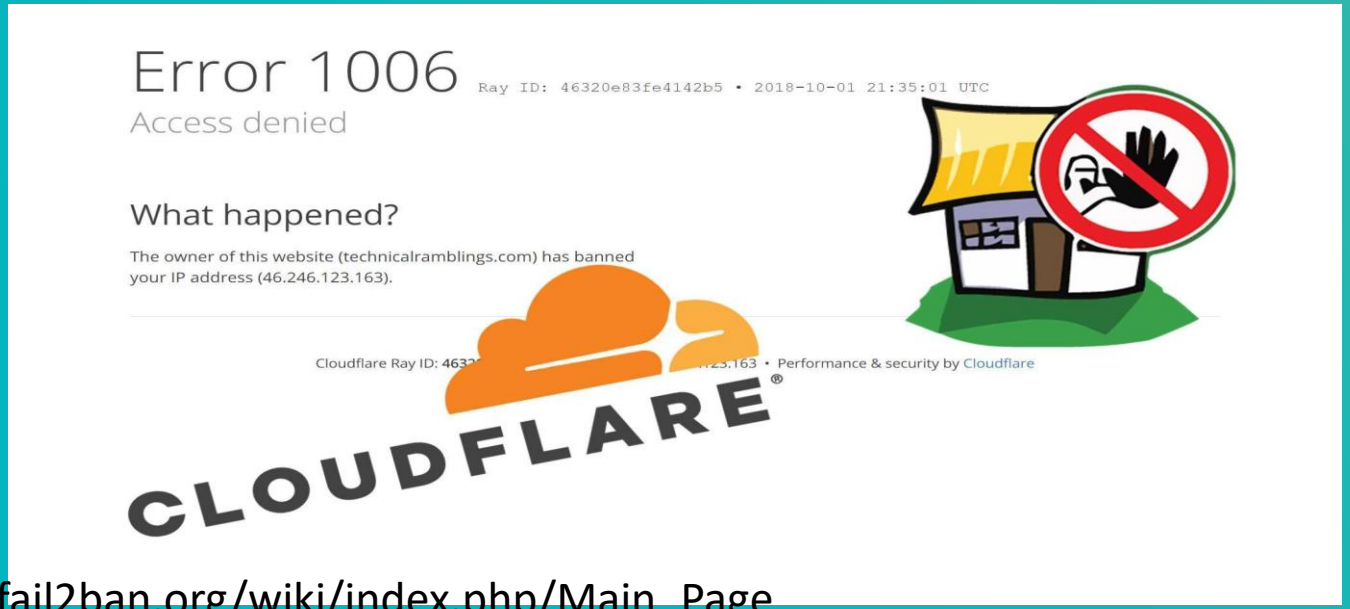
資安問題怎麼辦？

我的伺服器在幹嘛？有人登入了？



資安問題怎麼辦？

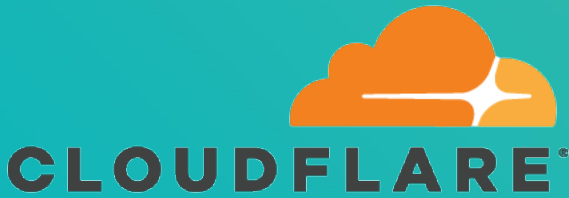
自動化封鎖 - fail2ban/wail2ban



https://www.fail2ban.org/wiki/index.php/Main_Page
https://github.com/glasnt/wail2ban

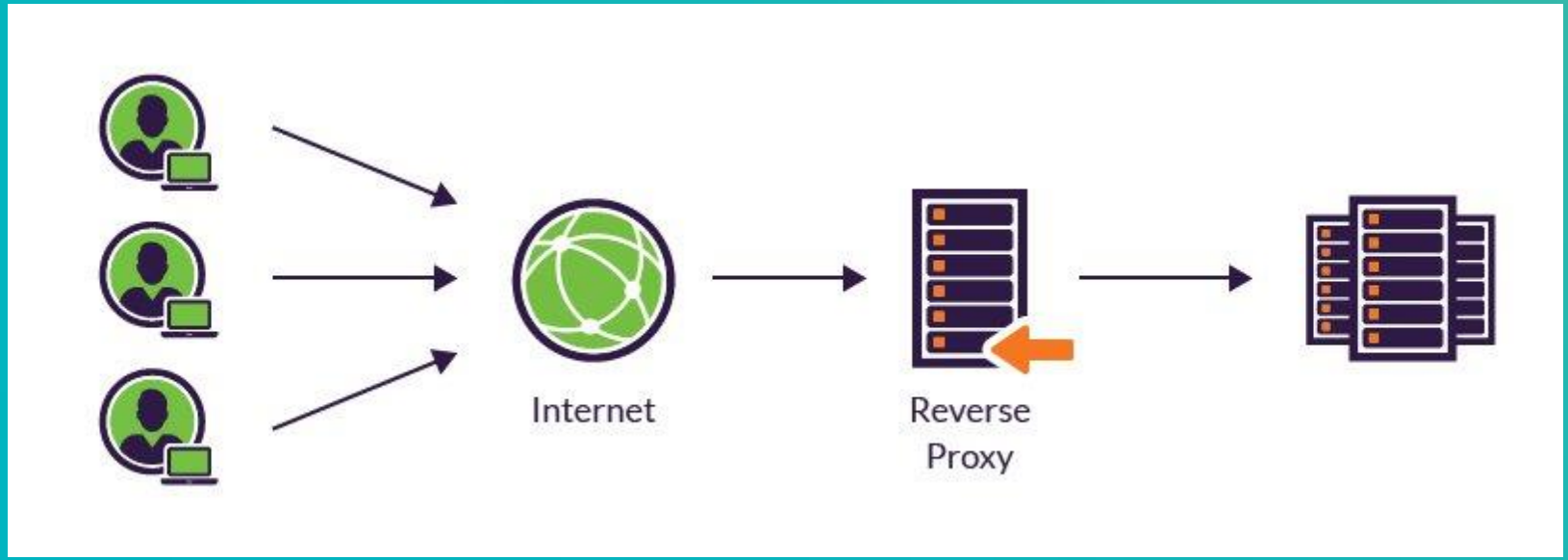
資安問題怎麼辦？

網站DDoS翻了，怎麼辦 ？



資安問題怎麼辦？

我的網站是破口嗎？ - WAF



WAF – NGINX

https://www.nginx.com/blog/nginx-plus-r10-released/

https://github.com/unixhot/waf

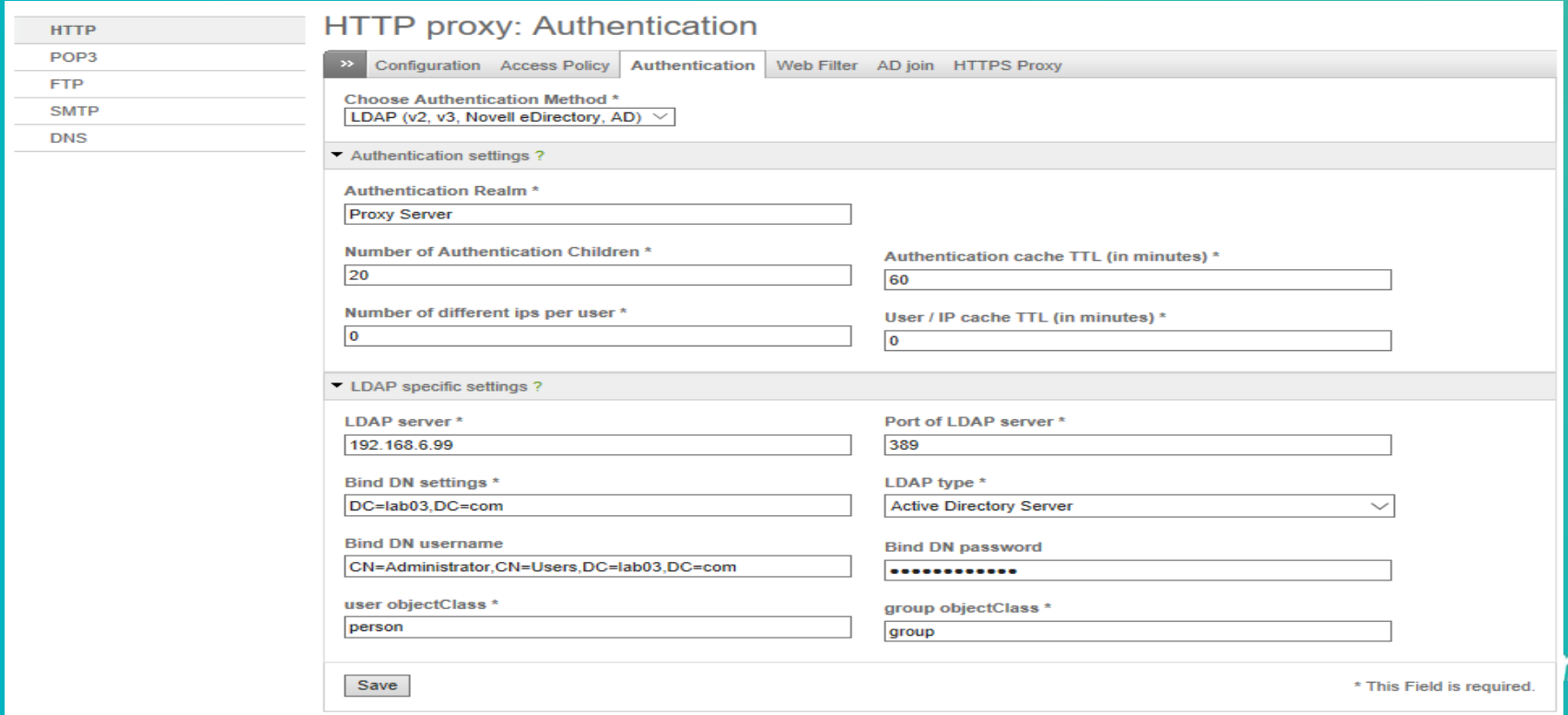
https://github.com/starjun/openstar

資安問題怎麼辦？

資安問題怎麼辦？

資安問題怎麼辦？

Endian UTM



資安問題怎麼辦？

被入侵! 馬上重灌? - 錯 ！ 數位鑑識包 - Helix

臺灣資安大會
CYBERSEC 2019

Q&A

PRESENTED BY iThome

臺灣資安大會
CYBERSEC 2019

Q&A ?

https://t.me/BorgEnt

PRESENTED BY iThome

社群夥伴

TDOHACKER

UCCU

BORG
企業資安讀書會

臺灣資安大會

CYBERSEC 2019

PRESENTED BY iThome