檢測工具下載與安裝說明

開始使用

合勤經銷商專區網址:
https://twzypartner.zyxel.com/

我要登入

尚未成為會員
請先註冊會員後登入

我要註冊

※ 如果有操作上的疑問，歡迎聯絡業務同仁，或是洽詢Line@企業網路資安聯盟

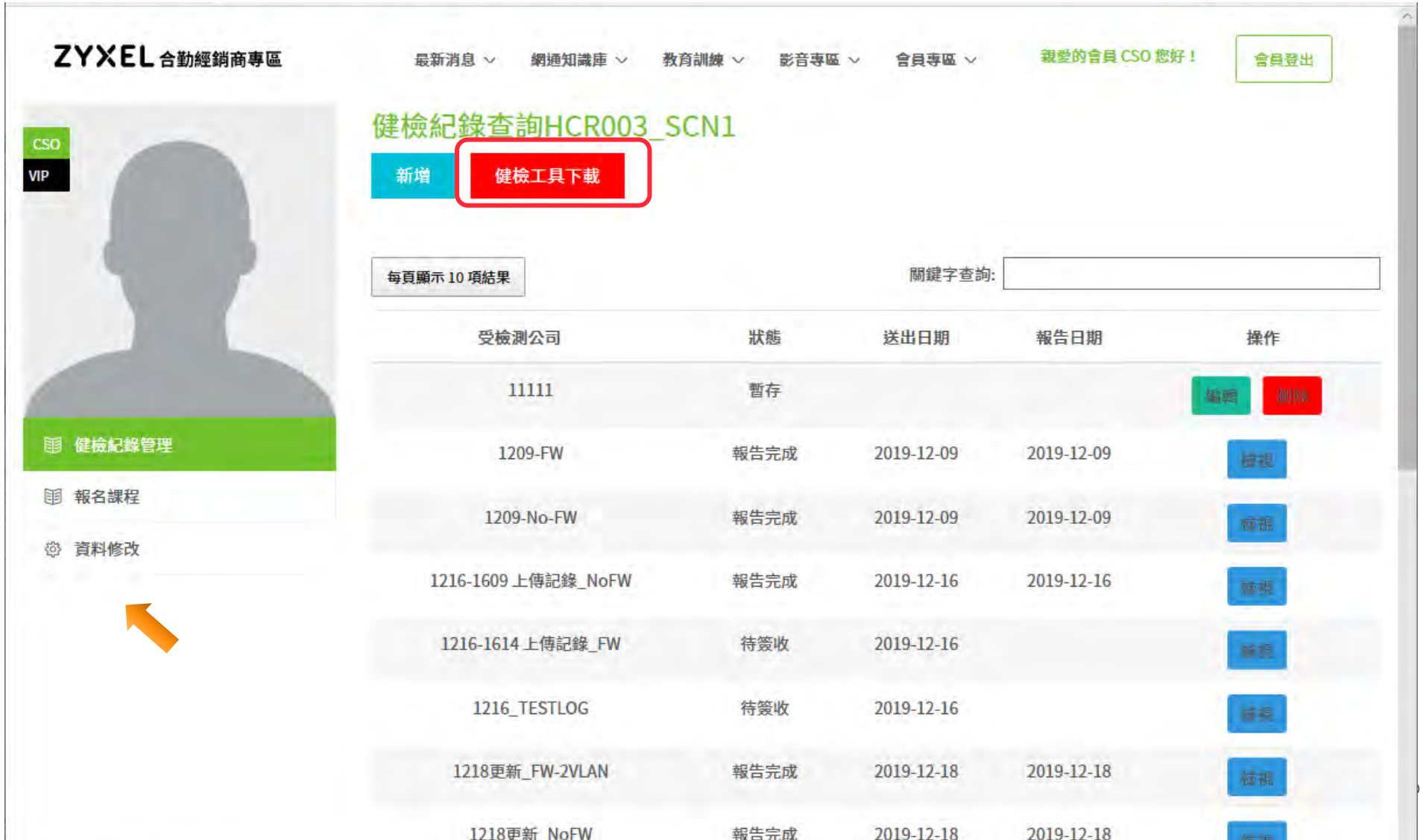
經銷商登入

1. 註冊成為會員之後，於此登入。

2. 回到首頁後，點擊「會員專區」中的「會員維護」

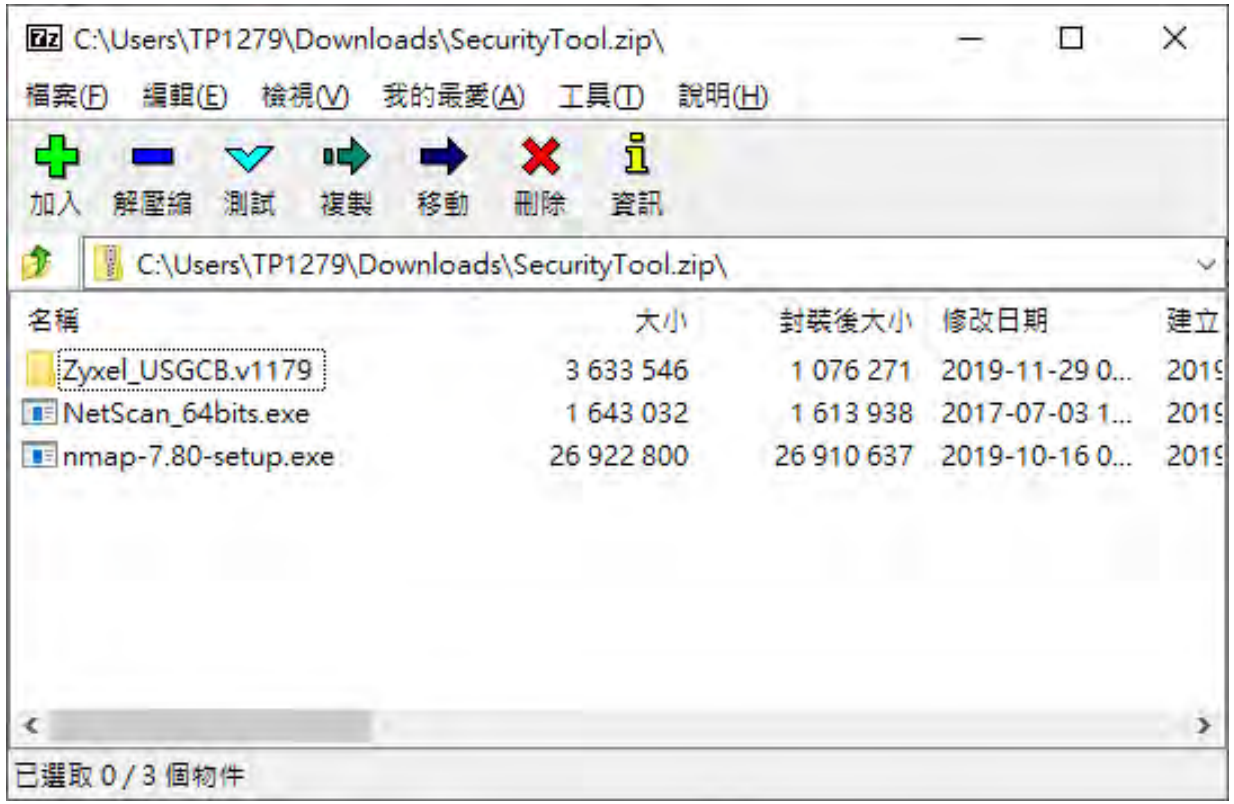
資安檢測工具取得方式

- 進入後，點選健檢工具下載

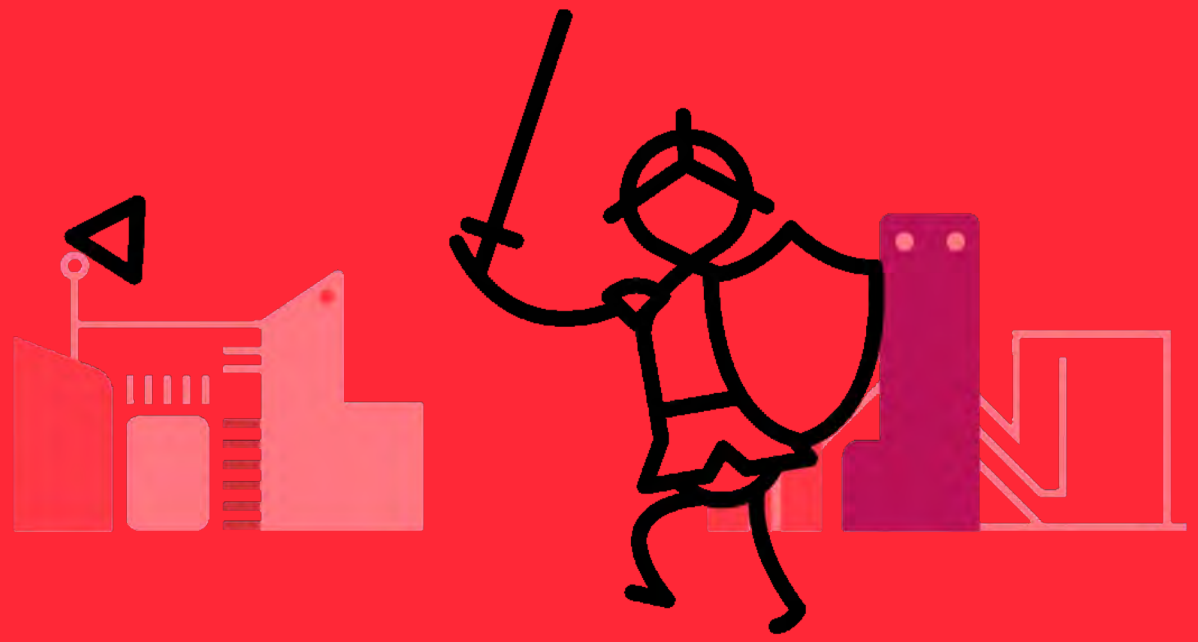


檢測工具下載/安裝

- 下載後進行SecurityTool.ZIP檔案解壓縮，可得以下三個測試工具程式
  - NetScan_64bits.exe: 需要安裝在 user LAN 執行弱點掃瞄
  - Nmap-7.8-setup.exe: 需要安裝, 需要再user LAN 執行弱點掃瞄
  - Zyxel_USGCB.v1179: 不需要安裝, 放在 USB資料碟進行每一台電腦掃瞄



健檢工具操作說明



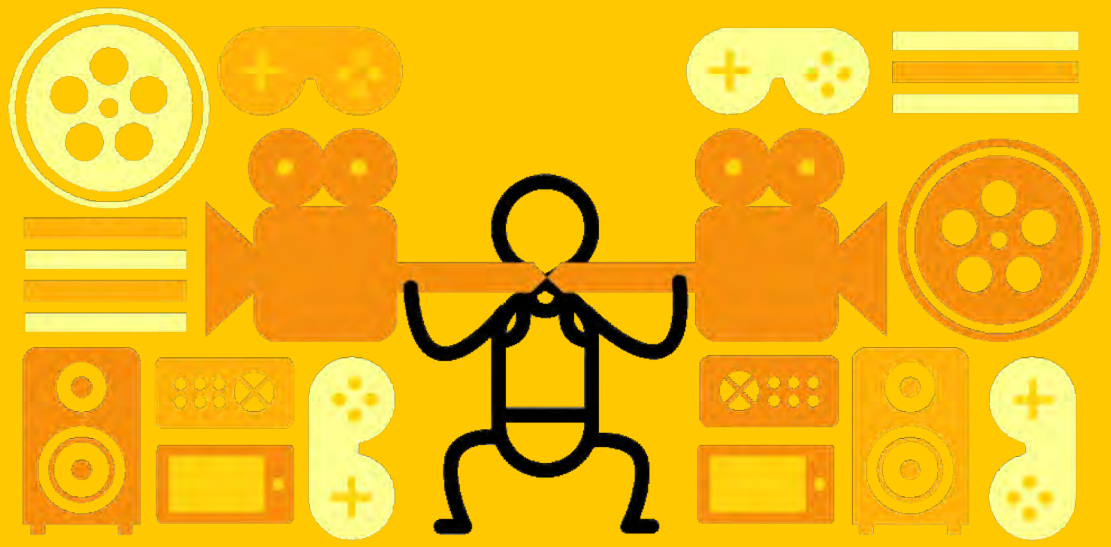
ZYXEL
Your Networking Ally

掃瞄記錄檔命名原則

- 將健檢工具軟體儲存在 USB上，並於客戶的內網與電腦上進行檢測
  - 健檢結束前後請記得 <<使用防毒軟體掃描該USB>> 避免惡意程式進駐

- 同一家公司存放在同一目錄內
- 依掃瞄功能來命名：
  - NetScan: Netscan_subnet-n.xml
  - Nmap: Nmap_subnet-n.xml
  - GCB: 軟體會自動產生每一台電腦掃瞄的時間目錄 (不需命名, 確認產出 .jsn 檔)

一、主機服務掃瞄工具

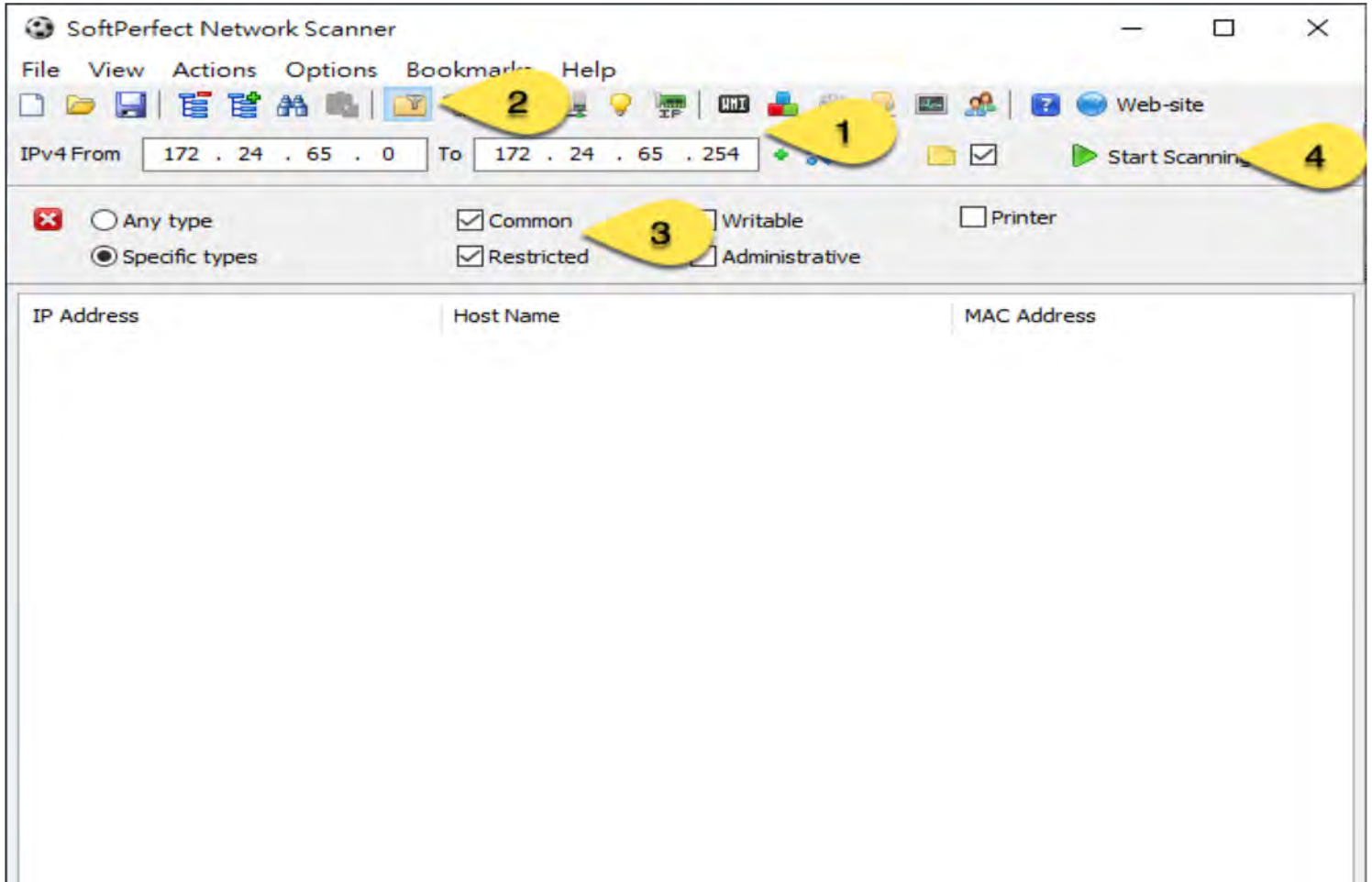


工具1: SoftPerfect Network Scanner

一、執行 NetScan_64bits.exe 程式安裝

二、啟動『SoftPerfect Network Scanner』，如圖所示

1) 掃描網段
   - 掃瞄subnet 位址 .1 ~ .254
2) 過濾設定
   - 使用預設 Any type
3) 特殊格式
   - 使用預設 Any type
4) 開始掃描



工具1: SoftPerfect Network Scanner

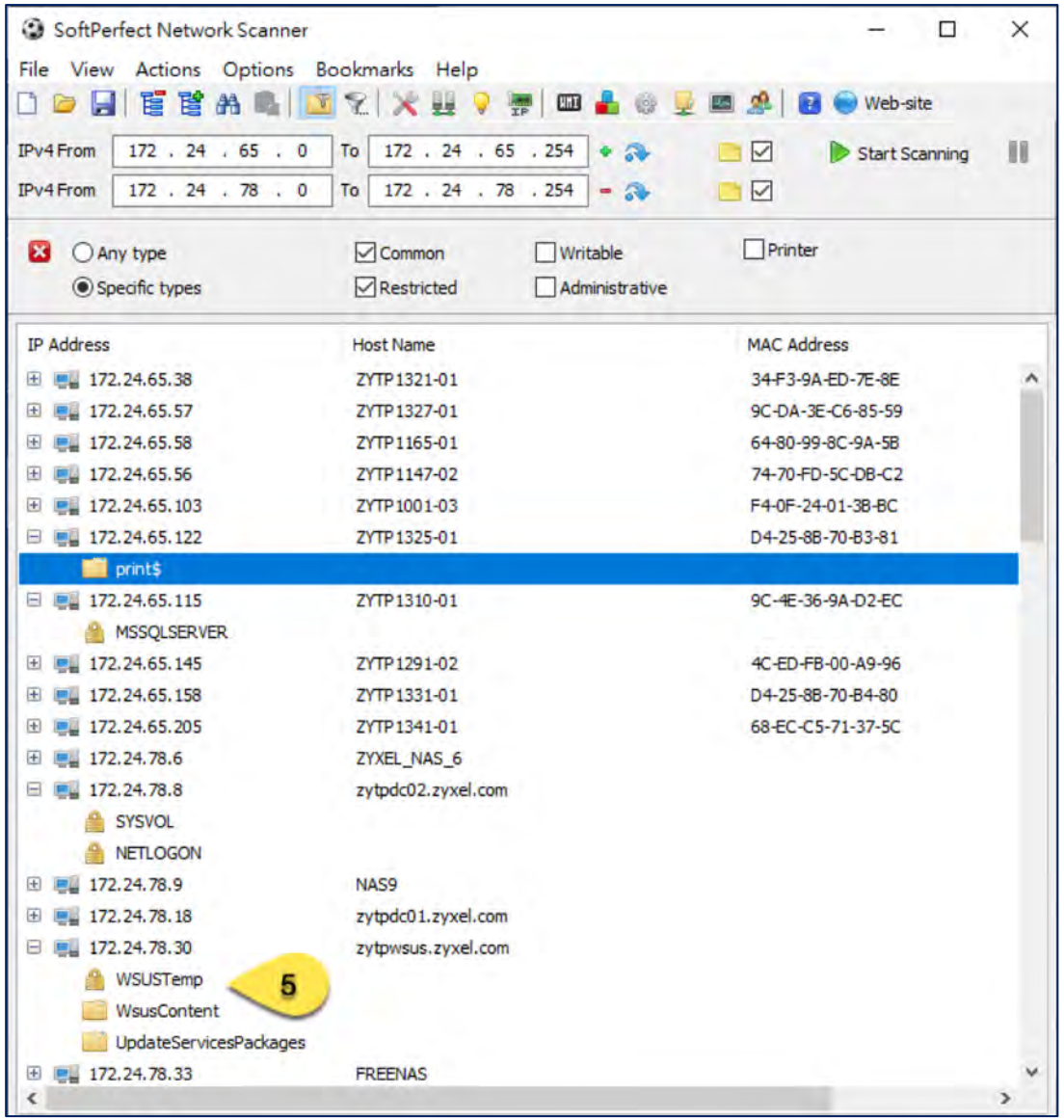
等待約5分鐘掃瞄完，可以
看到視窗中會出現的結果記錄。

灰色字體僅供說明，無需作業

5) 掃瞄結果:

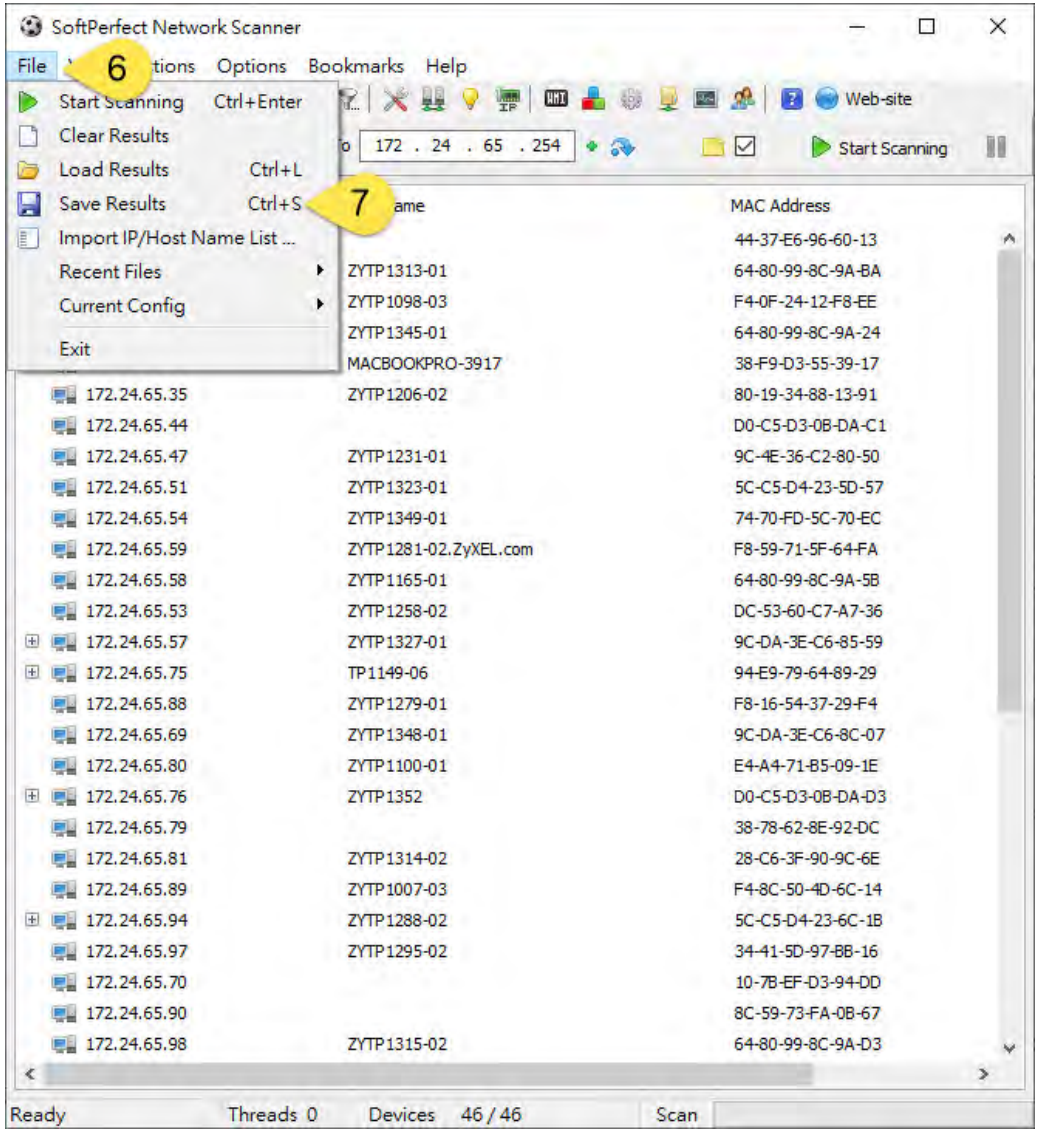
a.有鎖頭: 已上鎖

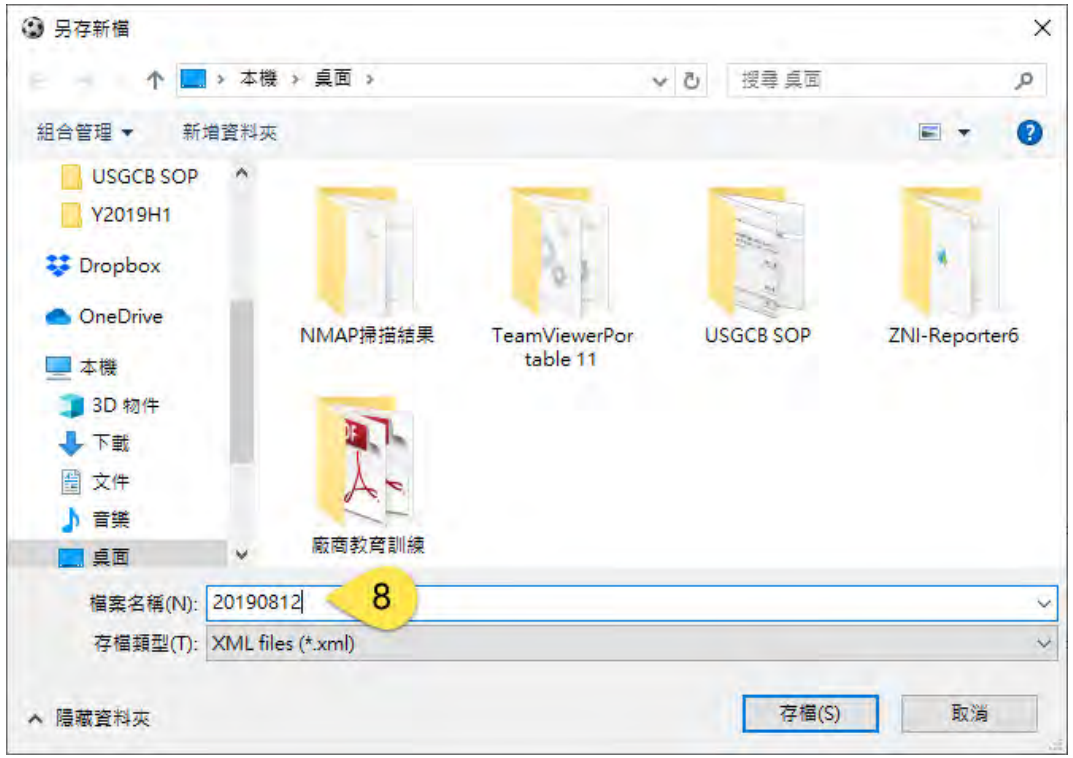
b.無鎖頭: 未上鎖,
表示不需認證也可以
存取該應用服務。



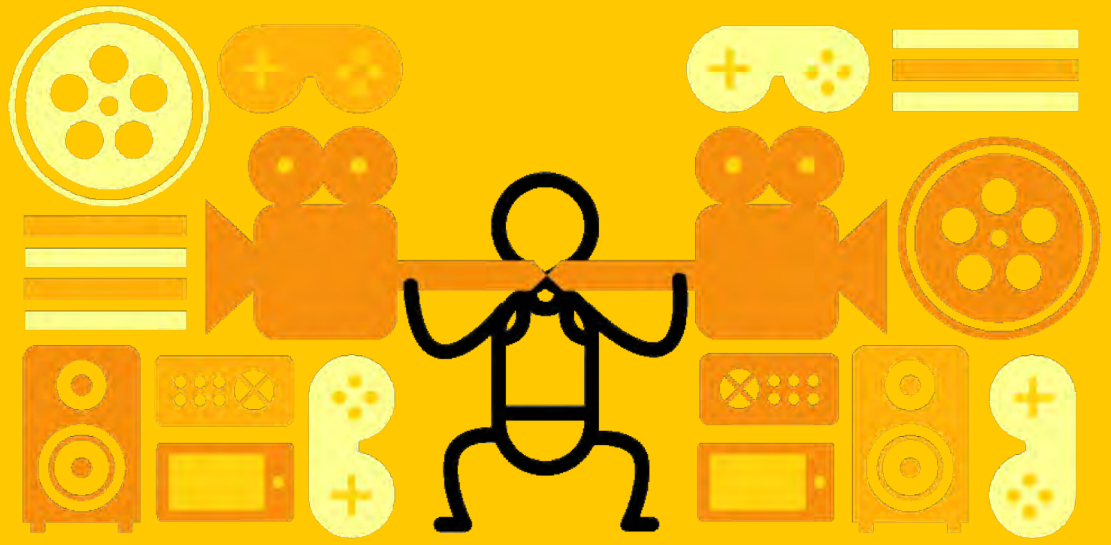
工具1: SoftPerfect Network Scanner

6) 儲存結果
7) 另存新檔
8) 命名檔案名稱
   - 建議命名為 Netscan_subnet-n.xml





二、Zenmap 網路掃瞄工具



工具2: Zenmap

一、執行Nmap-7.8-setup.exe 程式安裝

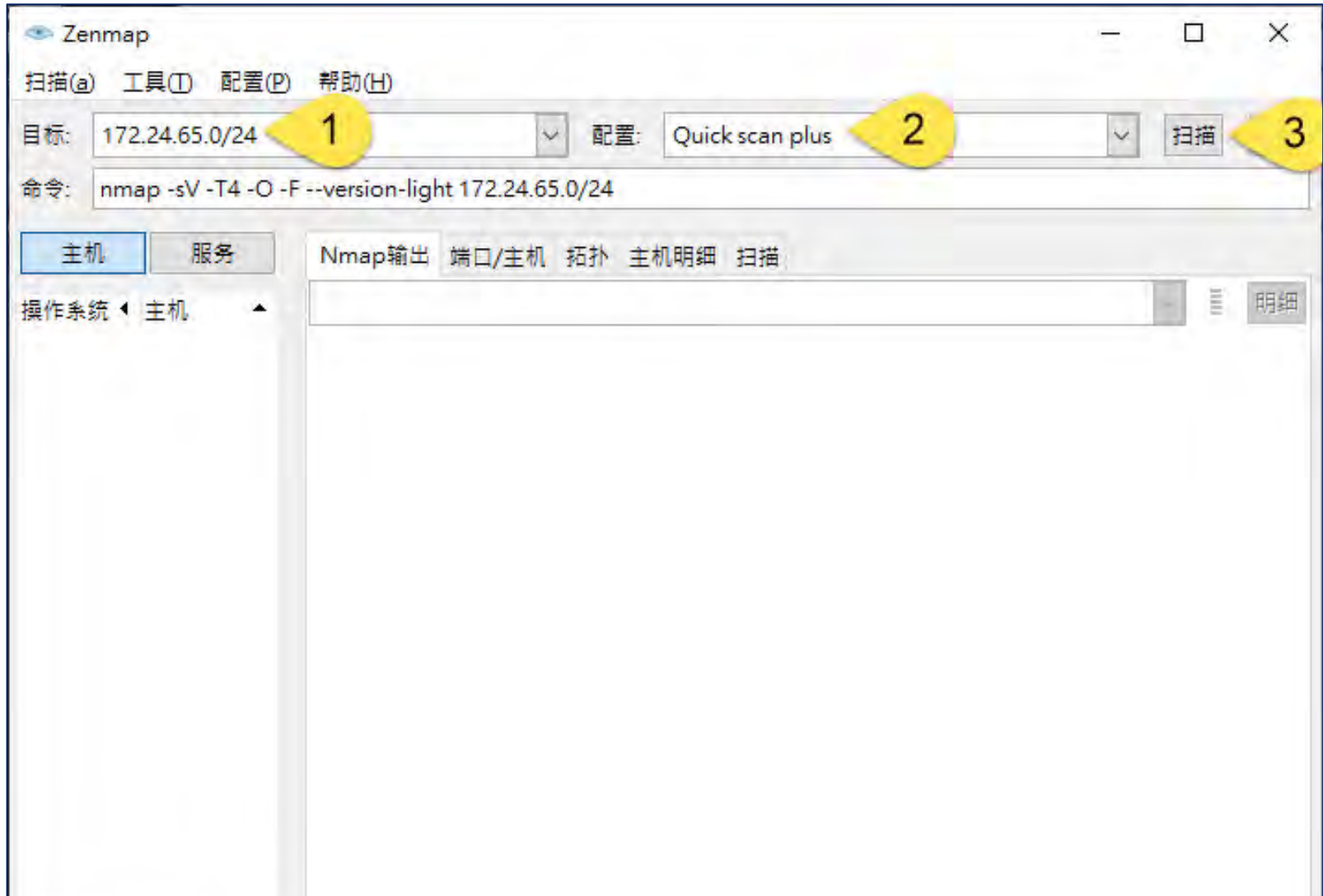
二、啟動『 Zenmap』

1) 輸入目標網段

2) 選擇掃描類型

- 使用Quick scan plus
- * 使用其他類型，可能會時間過長，或是終端機回應問題而卡住。

3) 開始掃描(整個過程約5分鐘)

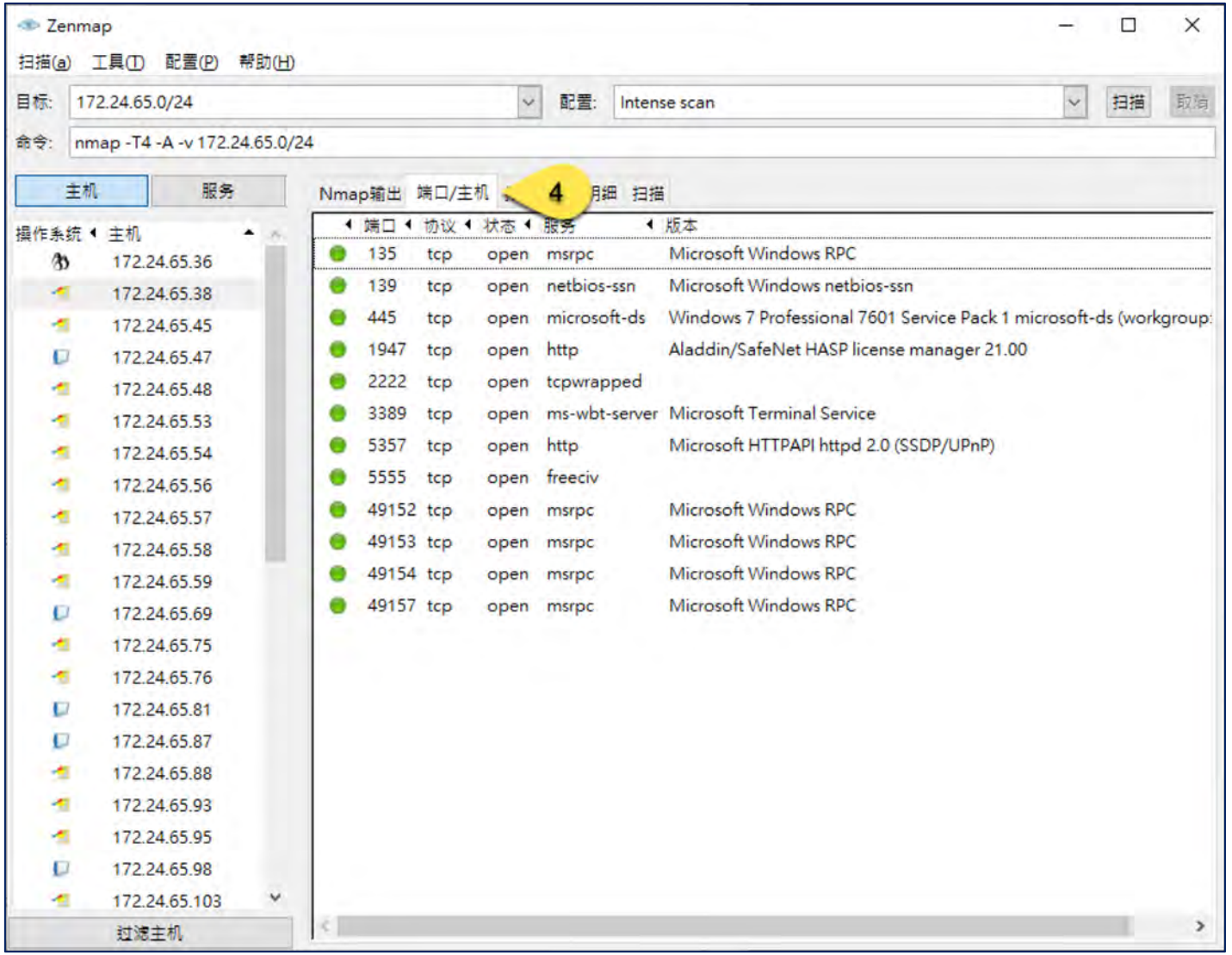


工具2: Zenmap

等待約5分鐘掃瞄完，可以看到視窗中會出現的結果記錄。

灰色字體僅供說明，無需作業

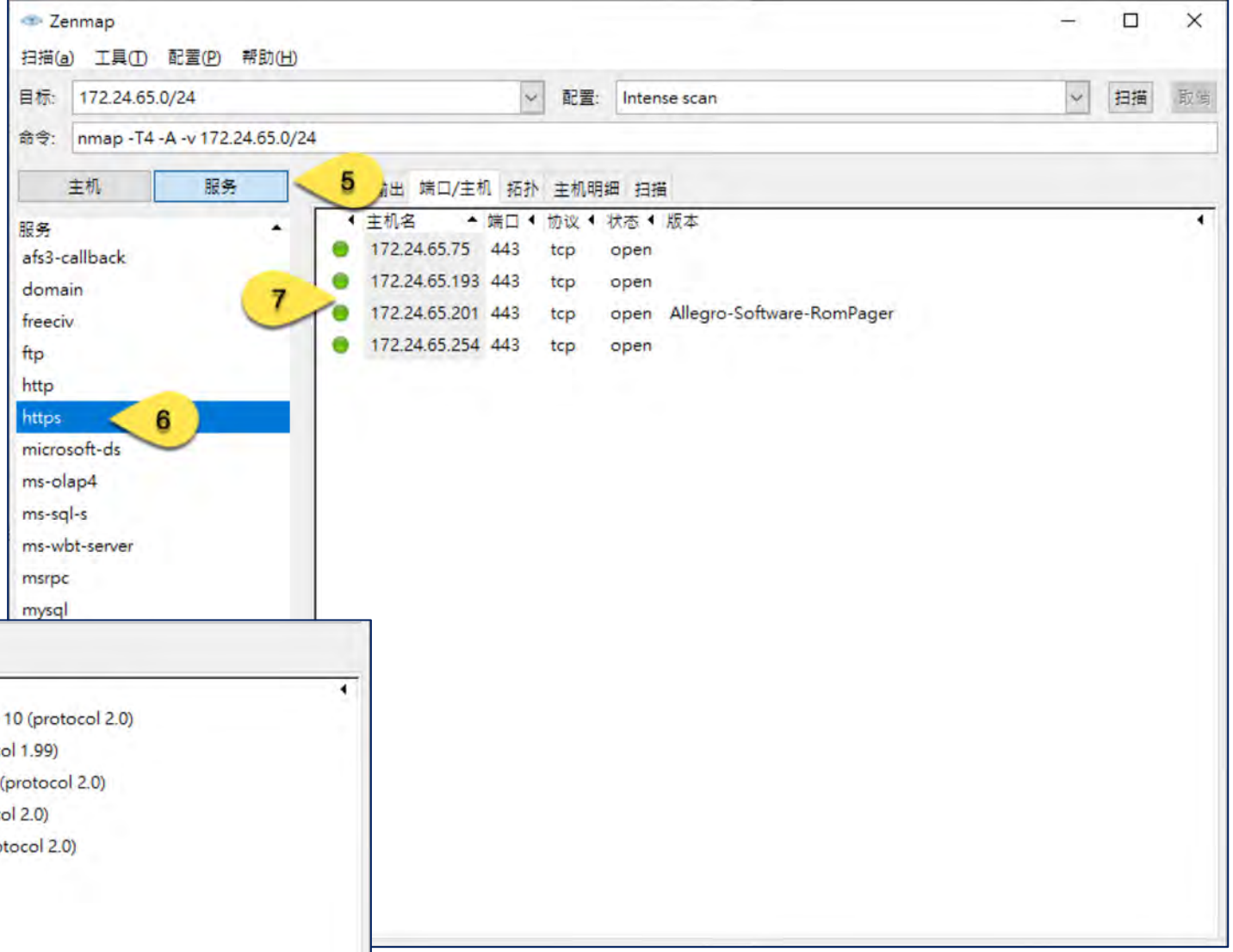
4) 選擇主機,可顯示目前開啟的port

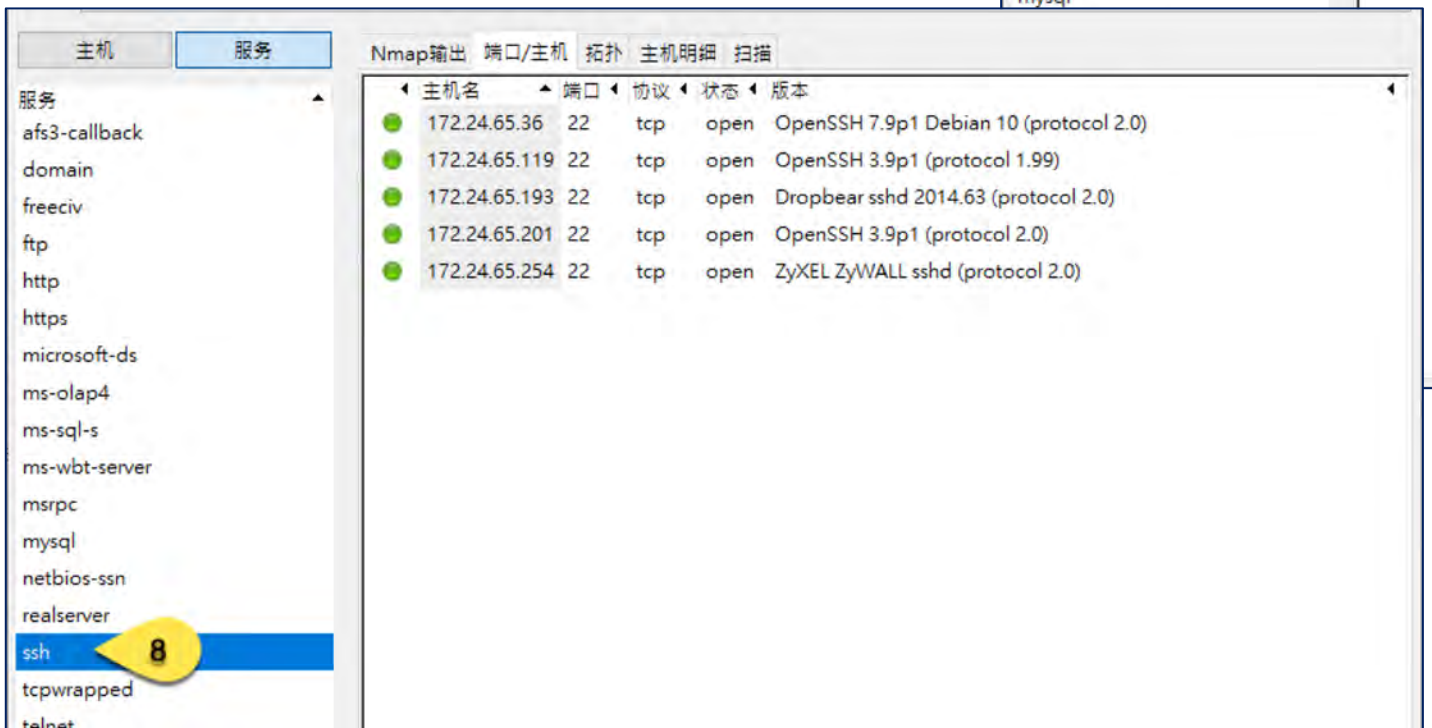


工具2: Zenmap

灰色字體僅供說明，無需作業

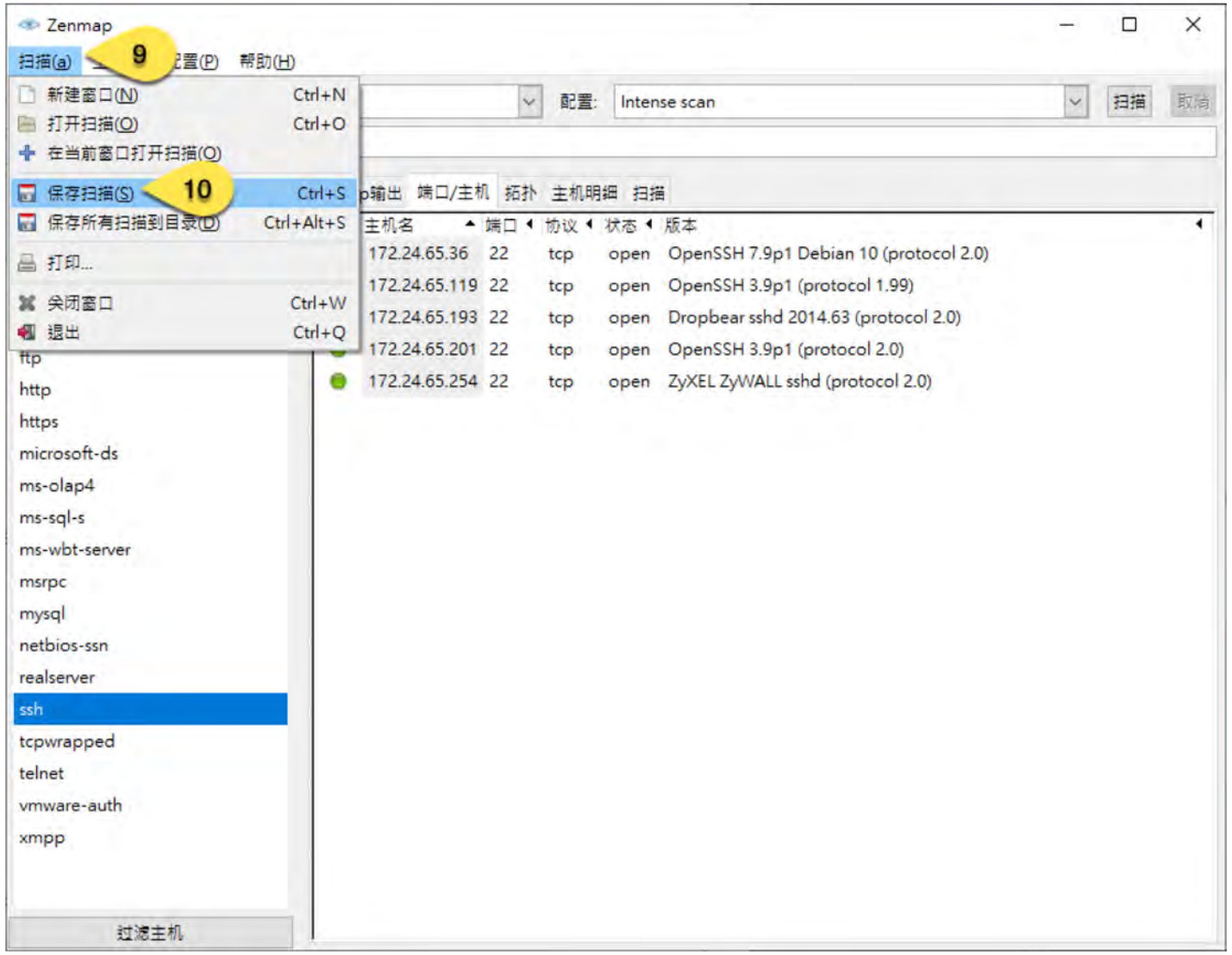
5) 選擇服務
6) 選擇https
7) 目前有開啟https的主機
8) 有開啟ssh服務的主機





工具2: Zenmap

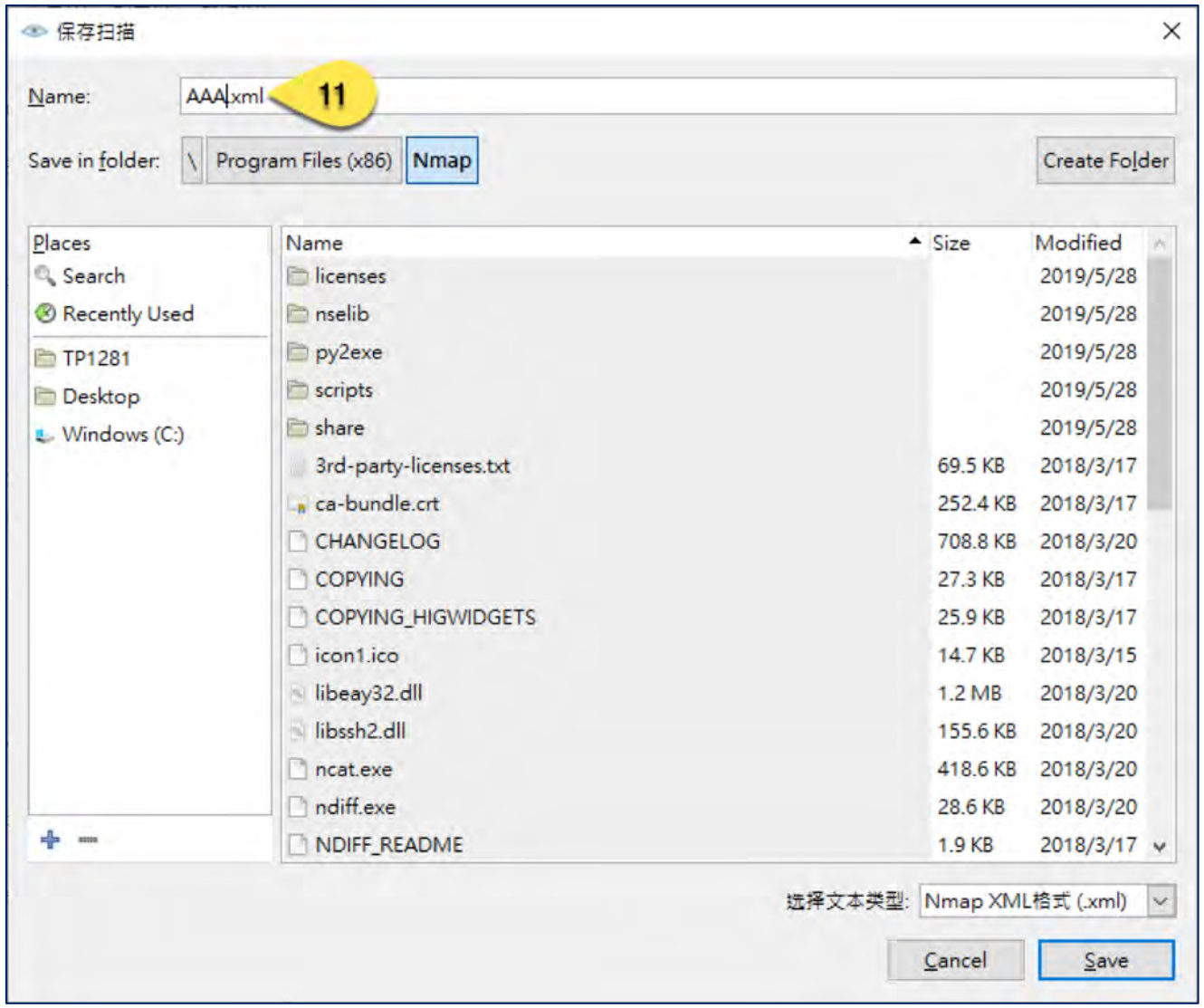
9) 儲存掃描結果
10) 保存掃瞄



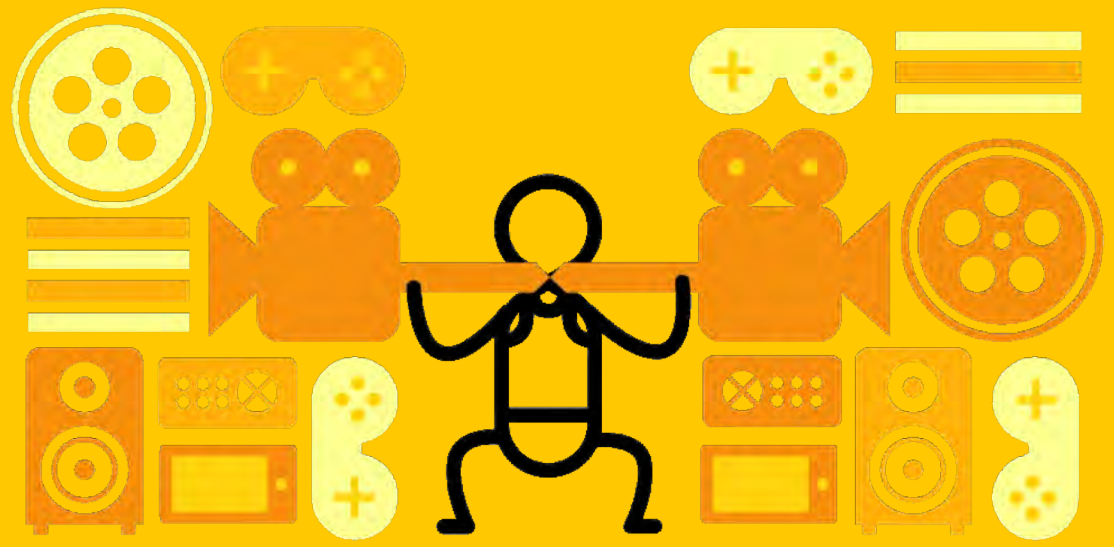
工具2: Zenmap

11) 另存新檔
選擇儲存檔名

- 建議命名為:
  NMap_subnet-n.xml



三、GCB政府電腦安全組態設定基準檢查



工具3: GCB政府電腦安全組態設定基準檢查

1) 選擇執行檔案

- 由目錄

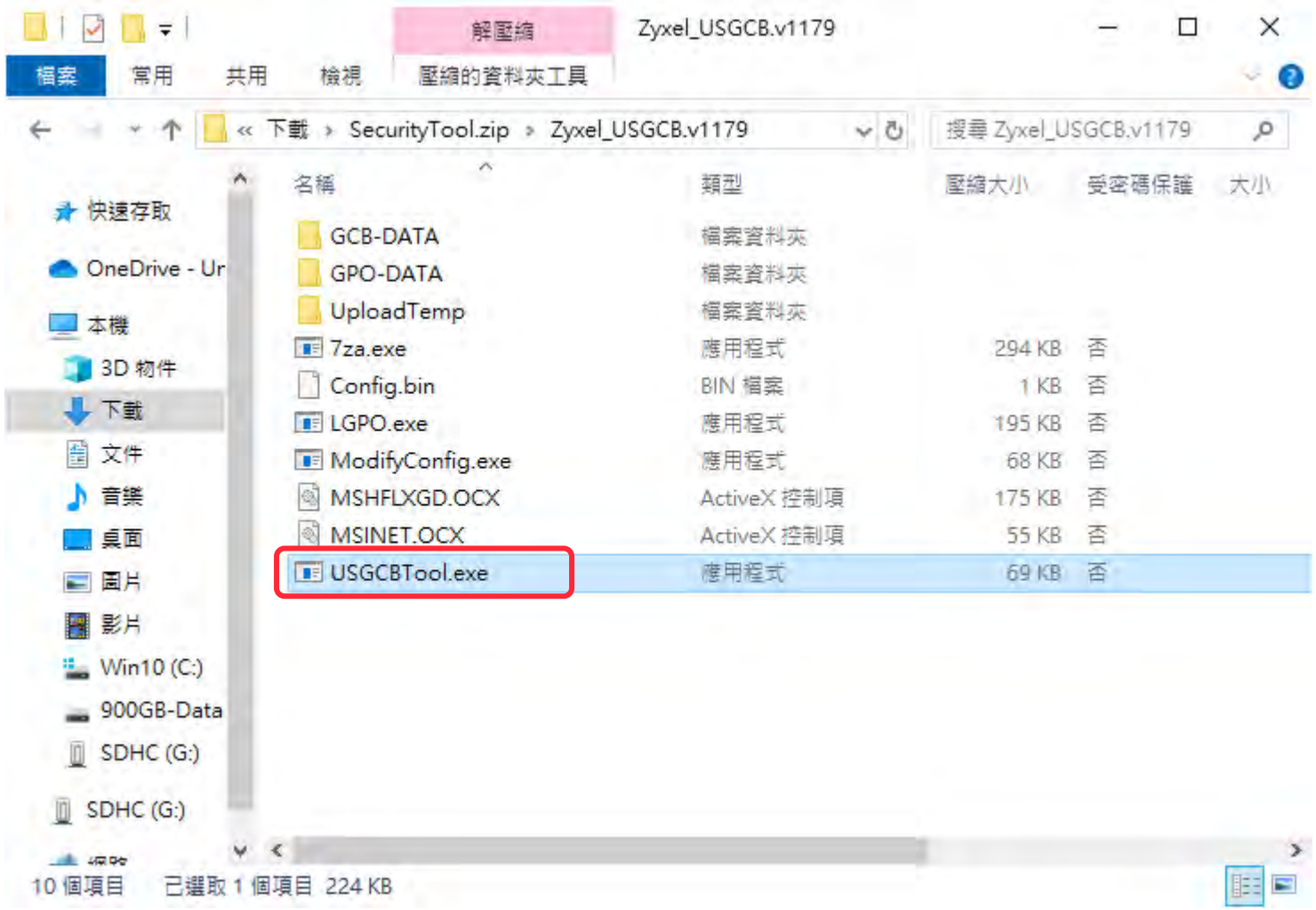
  \ZyxelUSGCB.v1179

  執行: USGCBTool.exe

- 在 Windows 的App

  執行告警上按 “是” 鈕，

  開始執行檢查工具



工具3: GCB政府電腦安全組態設定基準檢查

2) 新增上傳GPO組態資料

工具3: GCB政府電腦安全組態設定基準檢查

3) 產生GPO紀錄中

工具3: GCB政府電腦安全組態設定基準檢查

4) 填寫受測資料(皆必填)

- 填寫檢測資訊，

  以供報告載明相關內容

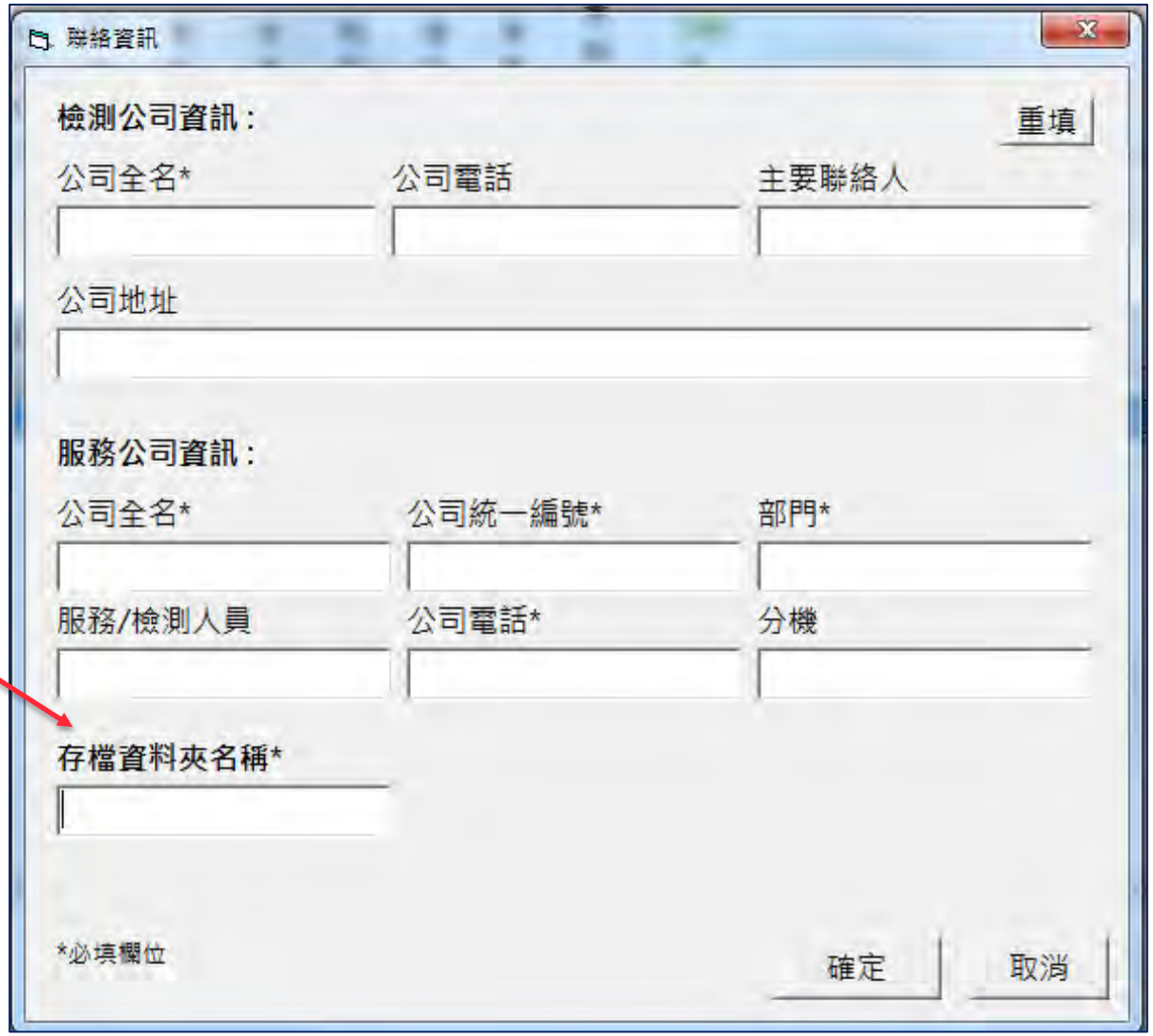
存檔資料夾名稱可自行命名避免受測PC混雜。

- 每家公司可以自定

  一個目錄名稱

- 目錄名稱避免使用

  中文與空白

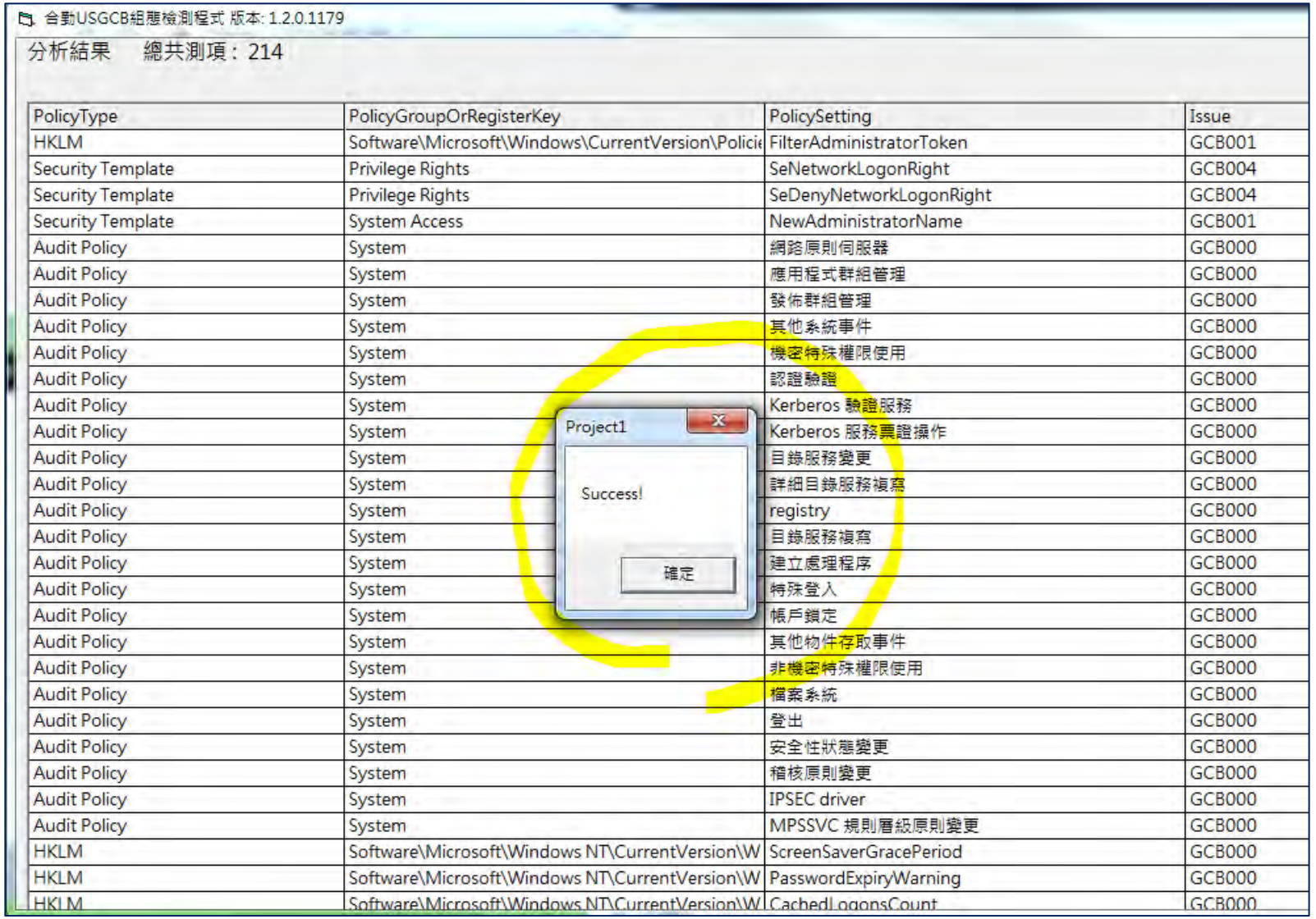


工具3: GCB政府電腦安全組態設定基準檢查

5) 勾選“我同意”後，請按<確定>進行掃瞄

工具3: GCB政府電腦安全組態設定基準檢查

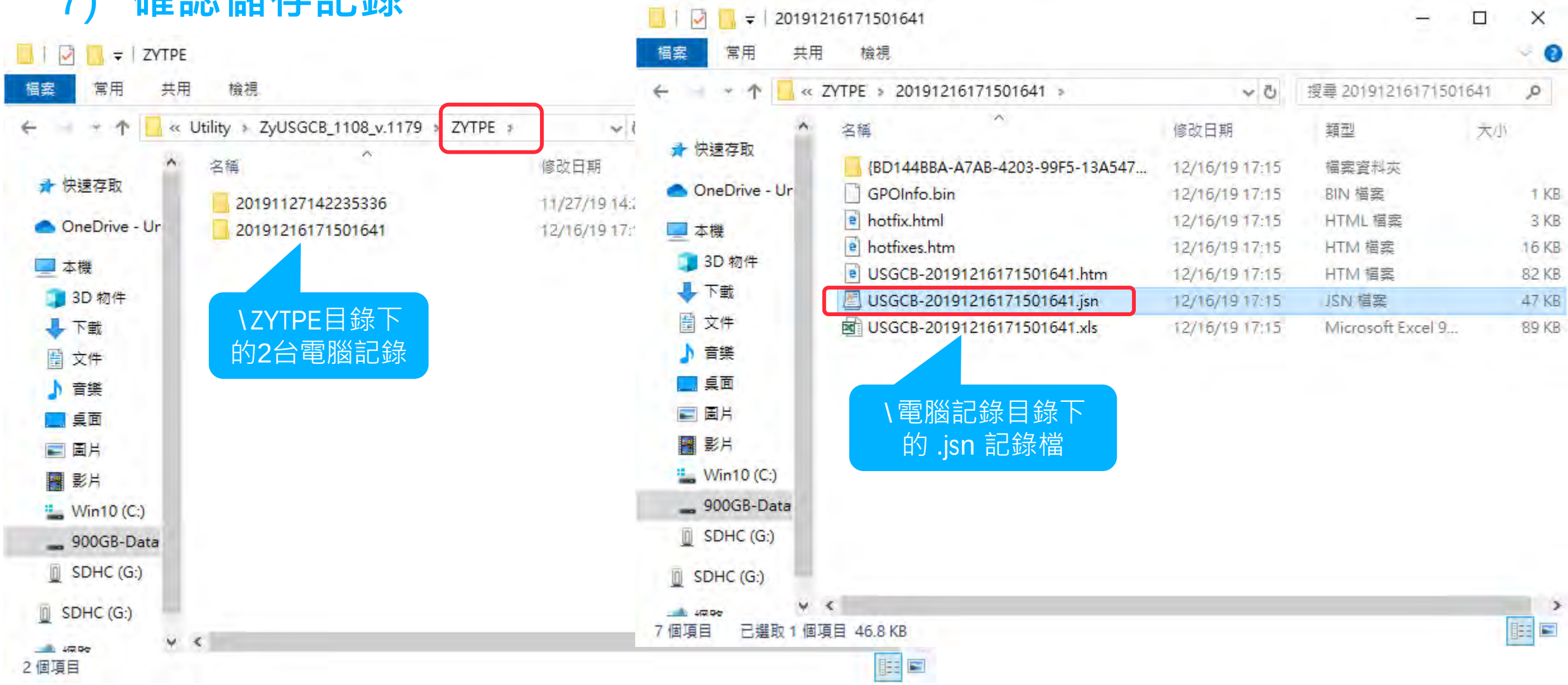
6) 完成單台
電腦掃瞄作業



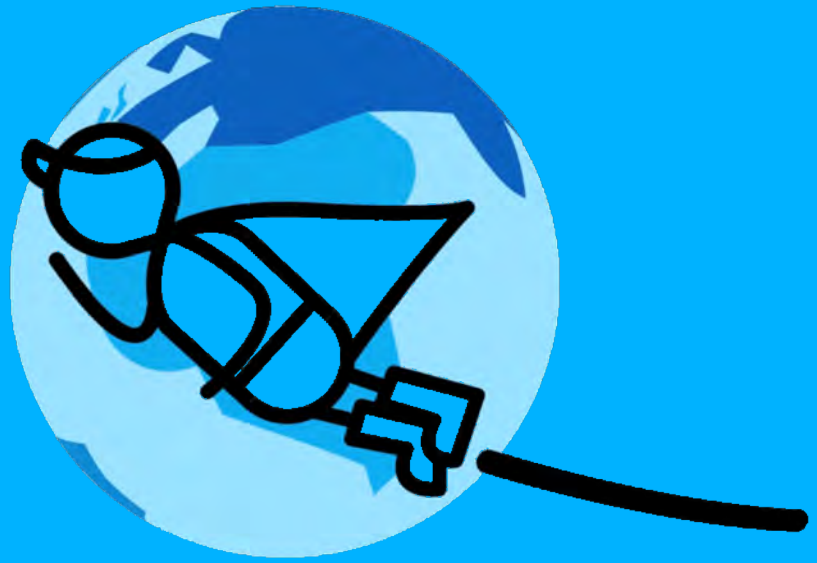
PolicyType	PolicyGroupOrRegisterKey	PolicySetting	Issue
HKLM	Software\Microsoft\Windows\CurrentVersion\Policie	FilterAdministratorToken	GCB001
Security Template	Privilege Rights	SeNetworkLogonRight	GCB004
Security Template	Privilege Rights	SeDenyNetworkLogonRight	GCB004
Security Template	System Access	NewAdministratorName	GCB001
Audit Policy	System	網路原則伺服器	GCB000
Audit Policy	System	應用程式群組管理	GCB000
Audit Policy	System	發佈群組管理	GCB000
Audit Policy	System	其他系統事件	GCB000
Audit Policy	System	機密特殊權限使用	GCB000
Audit Policy	System	認證驗證	GCB000
Audit Policy	System	Kerberos 驗證服務	GCB000
Audit Policy	System	Kerberos 服務票證操作	GCB000
Audit Policy	System	目錄服務變更	GCB000
Audit Policy	System	詳細目錄服務複寫	GCB000
Audit Policy	System	registry	GCB000
Audit Policy	System	目錄服務複寫	GCB000
Audit Policy	System	建立處理程序	GCB000
Audit Policy	System	特殊登入	GCB000
Audit Policy	System	帳戶鎖定	GCB000
Audit Policy	System	其他物件存取事件	GCB000
Audit Policy	System	非機密特殊權限使用	GCB000
Audit Policy	System	檔案系統	GCB000
Audit Policy	System	登出	GCB000
Audit Policy	System	安全性狀態變更	GCB000
Audit Policy	System	稽核原則變更	GCB000
Audit Policy	System	IPSEC driver	GCB000
Audit Policy	System	MPSSVC 規則層級原則變更	GCB000
HKLM	Software\Microsoft\Windows NT\CurrentVersion\W	ScreenSaverGracePeriod	GCB000
HKLM	Software\Microsoft\Windows NT\CurrentVersion\W	PasswordExpiryWarning	GCB000
HKLM	Software\Microsoft\Windows NT\CurrentVersion\W	CachedLogonsCount	GCB000

工具3: GCB政府電腦安全組態設定基準檢查

7) 確認儲存記錄

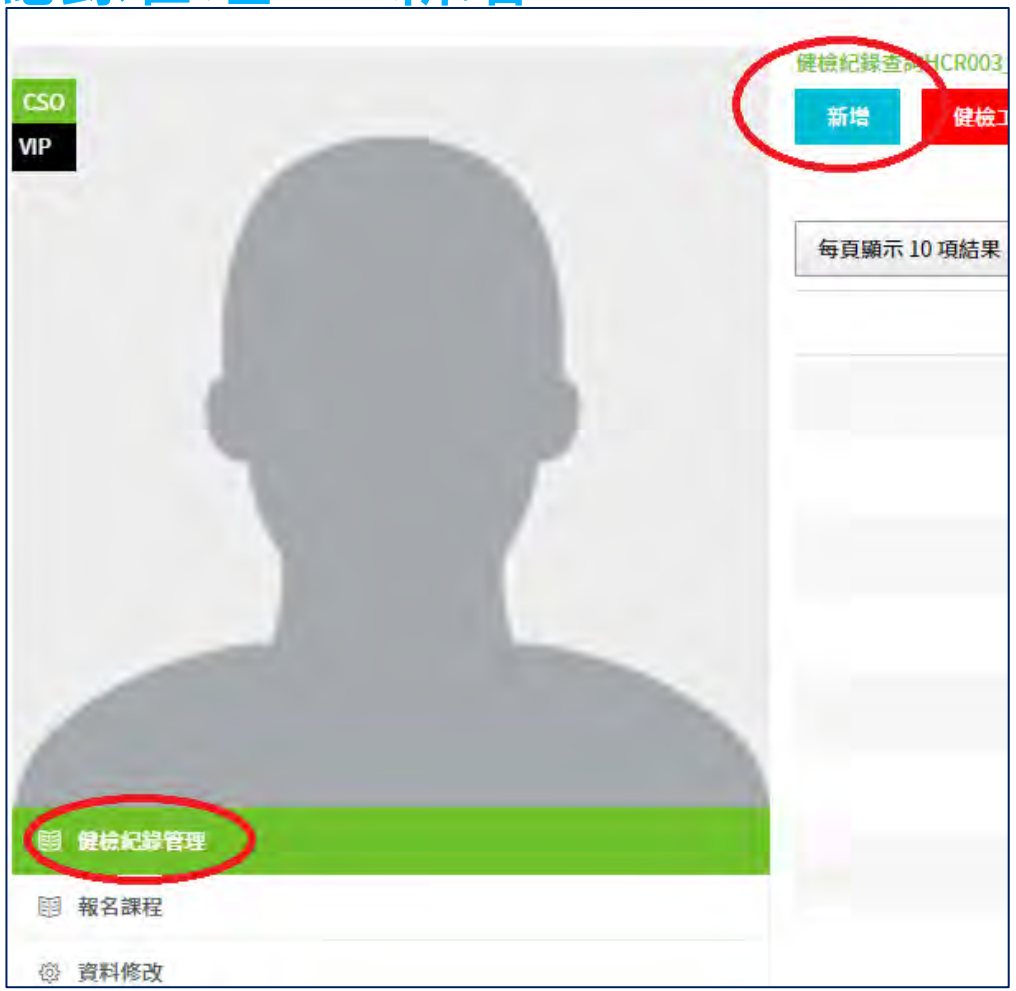


上傳資安掃瞄記錄檔
進行資安健檢分析



上傳步驟

- https://twzypartner.zyxel.com/
- 登入經銷商專區 → 會員維護 → 健檢紀錄管理 → 新增



上傳步驟

- 填寫基本資訊
  - 填寫的檢測資訊，將列印在檢測報告的封面

上傳步驟

- 填寫問卷

客戶網路相關資訊

編號	說明	答案
1	貴公司是否有區分主機, 個人電腦的VLAN 與 子網段 subnet	是(續填1.1) 否(跳至第2題)
1.1	系統網段是否可以直接連結 Internet ?	是 否
2	貴公司是否有對外的服務 (例如:網頁服務)	是(續填2.1) 否(跳至第3題)
2.1	對外伺服器直接使用公有IP	是 否
2.2	對外伺服器使用 防火牆NAT轉址提供服務	是 否
2.3	如有網頁服務,公司是否有架設網站應用防火牆	是 否
3	貴公司是否有使用企業防火牆 (非家用 Router)	是(續填3.1) 否(跳至第4題)
3.1	是否啟用內網/外網/DMZ安全防禦設定	是 否
3.2	是否有使用 UTM 防火牆, 並啟用 IDP/IPS/防毒/應用程式控管等功能	是 否
3.3	防火牆UTM特徵碼最後更新的日期 (1~3: 1個月以內, 3個月, 半年以上)	一個月以內 一~三個月 半年以上
4.1	員工進入公司網路是否認證	是 否
4.2	內部網路是否進行設備認證管控 (例如:MAC管控 或 NAC, 802.1x)	是 否
5.1	公司無線網路 加密等級是否到達 WPA2	是 否
5.2	公司無線網路是否區分用途的 SSID	是 否
5.3	公司無線網路是否有分群(員工、訪客)?	是 否
5.4	訪客上網是否有隔離? (訪客進入公司IP取得為何? 區分內部IP網段或訪客IP網段)	是 否
6	員工是否有從外部連入內網需求	是(續填6.1) 否(跳至第7題)
6.1	使用 VPN 遠端連入公司	是 否
6.2	是否可透過其他遠端軟體連入公司	是 否
7.1	是否有使用RAID5等級以上 NAS 或 FIle Server 進行檔案備份	是 否
7.2	是否有準備系統還原檔 (System Image) 以供系統救援使用	是 否
8.1	電腦是否全部安裝防毒軟體 (1~3: 全部, 部分未安裝, 一半以上未安裝)	全部安裝 部分未安裝 一半以上未安裝
8.2	防毒軟體特徵碼最後更新的日期 (1~3: 1個月以內, 3個月, 半年以上)	一個月內 一~三個月 半年以上

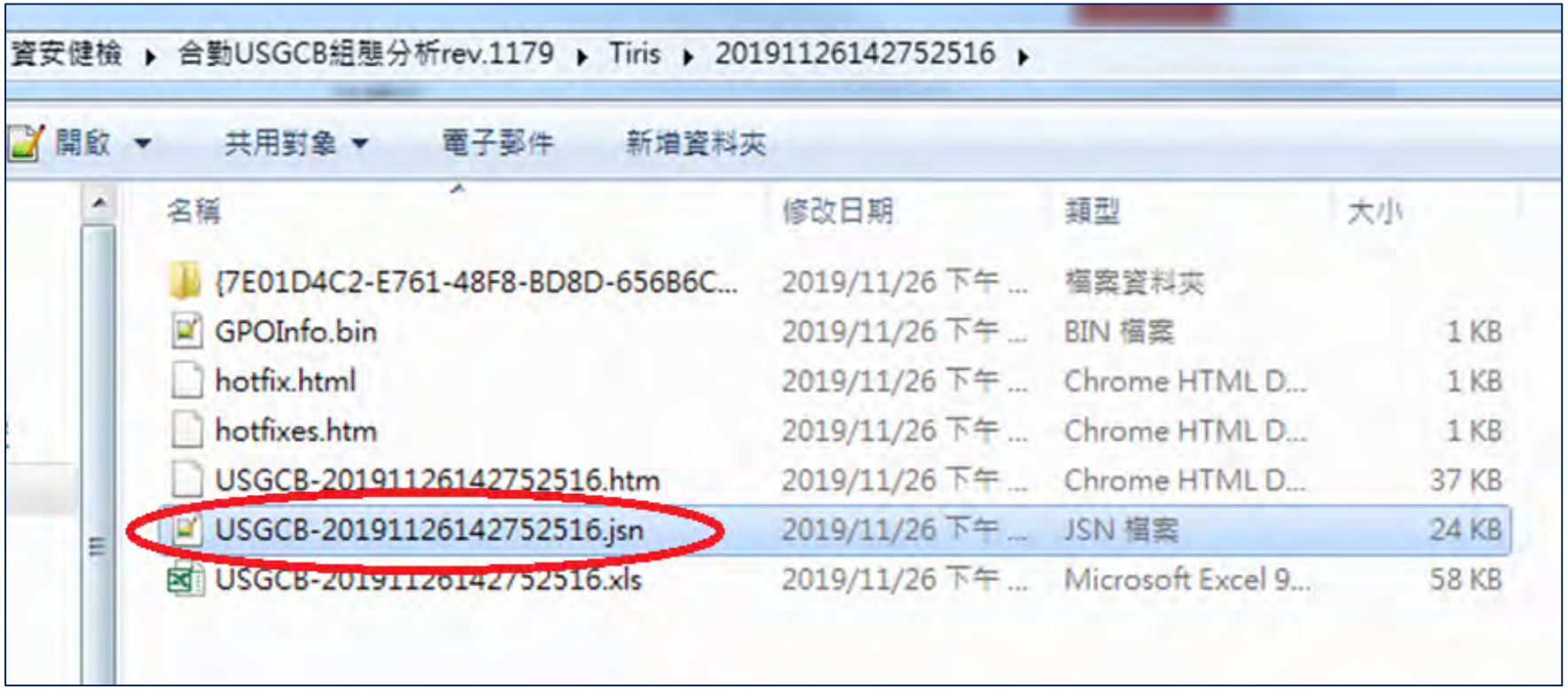
上一步 暫存 下一步

上傳步驟

- 上傳NMAP以及NetScan檔案。(僅可上傳Xml檔案)
- 主機IP請填寫掃描網段中的IP。
- NAS IP請填寫有開啟網路資料夾共享的設備。

上傳步驟

- 上傳GCB掃瞄記錄檔案。
  (僅可上傳 jsn檔案)
- 最多一次可上傳20個檔案。



上傳步驟

- 上傳網路拓樸圖

上傳步驟

- 確認問卷以及檔案名稱皆無誤後點選確認送出。
- 再請您主動在Line@上留言給小編：
  經銷商的寶號、
  上傳了那個客戶的資料。
- 預計2個工作天會完成資安健檢分析報告。
- 報告完成後，小編會請業務窗口與您聯繫。


ZYXEL
Your Networking Ally