

檢測工具下載與安裝說明



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



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」



- 進入後，點選**健檢工具下載**

ZYXEL 合勤經銷商專區

最新消息 ▾ 網通知識庫 ▾ 教育訓練 ▾ 影音專區 ▾ 會員專區 ▾ 親愛的會員 CSO 您好! 會員登出

CSO
VIP

健檢紀錄查詢HCR003_SCN1

新增 **健檢工具下載**

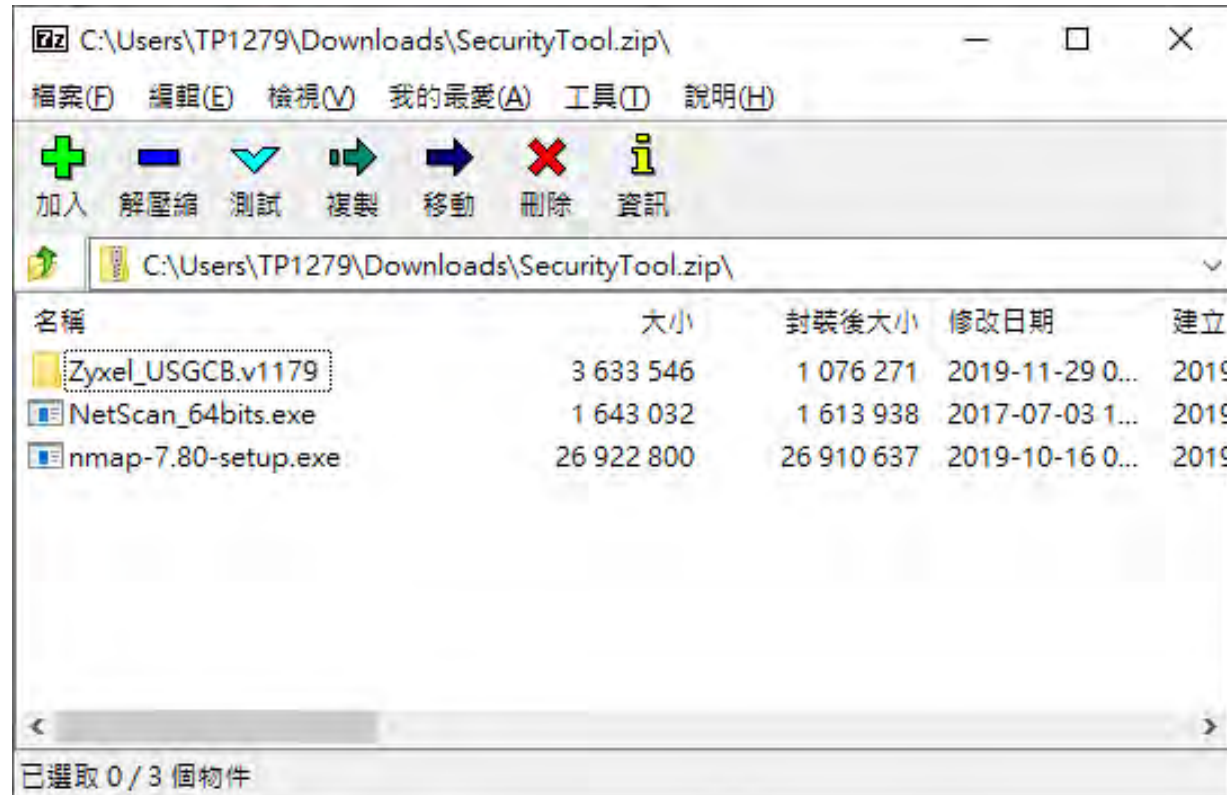
每頁顯示 10 項結果 關鍵字查詢:

受檢測公司	狀態	送出日期	報告日期	操作
11111	暫存			編輯 刪除
1209-FW	報告完成	2019-12-09	2019-12-09	檢視
1209-No-FW	報告完成	2019-12-09	2019-12-09	檢視
1216-1609 上傳記錄_NoFW	報告完成	2019-12-16	2019-12-16	檢視
1216-1614 上傳記錄_FW	待簽收	2019-12-16		檢視
1216_TESTLOG	待簽收	2019-12-16		檢視
1218更新_FW-2VLAN	報告完成	2019-12-18	2019-12-18	檢視
1218更新_NoFW	報告完成	2019-12-18	2019-12-18	檢視

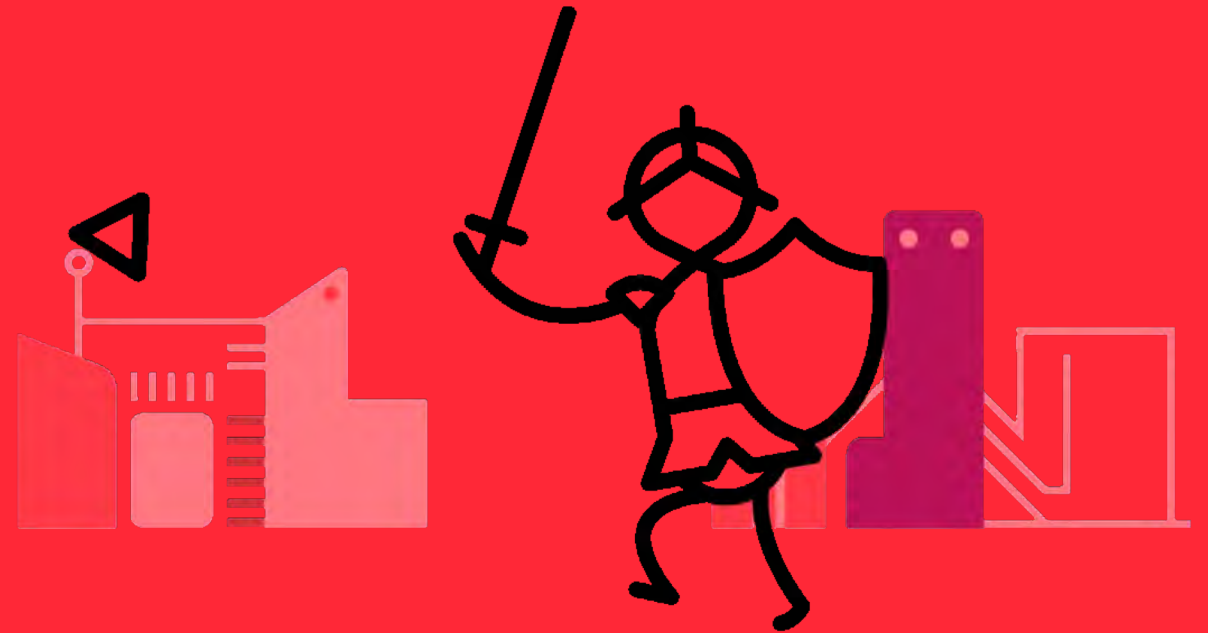
健檢紀錄管理
報名課程
資料修改

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 執行弱點掃描
 - ◆ Nmap-7.8-setup.exe: 需要安裝, 需要再user LAN 執行弱點掃描
 - ◆ Zyxel_USGCB.v1179: 不需要安裝, 放在 USB資料碟進行每一台電腦掃描



健檢工具操作說明



掃描記錄檔命名原則

- 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
- 依掃描功能來命名：
 - ◆ NetScan: Netscan_subnet-n.xml
 - ◆ Nmap: Nmap_subnet-n.xml
 - ◆ GCB: 軟體會自動產生每一台電腦掃描的時間目錄 (不需命名, 確認產出 .json 檔)

一、主機服務掃描工具



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

- 掃描subnet 位址 .1 ~ .254

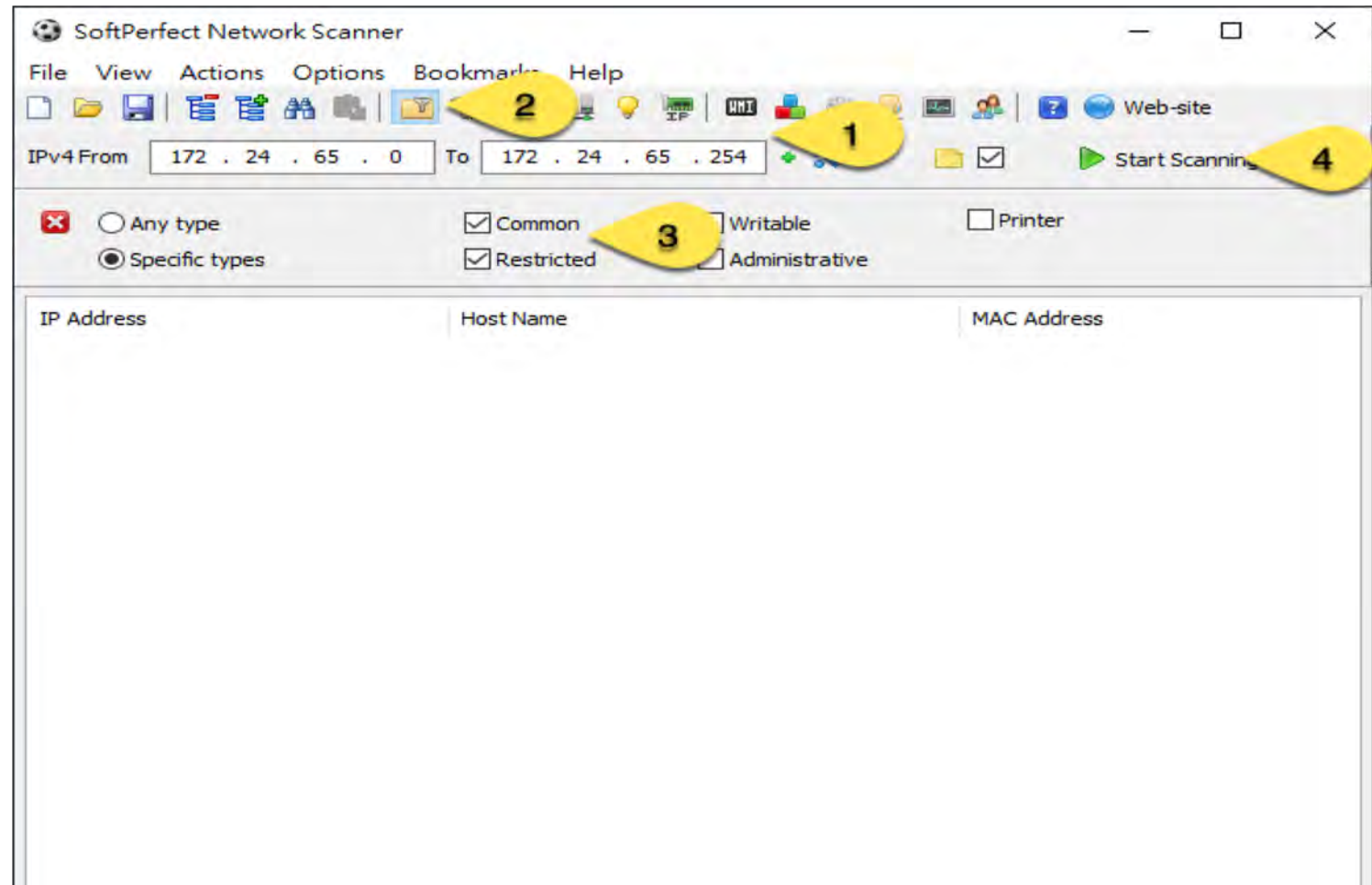
2) 過濾設定

- 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

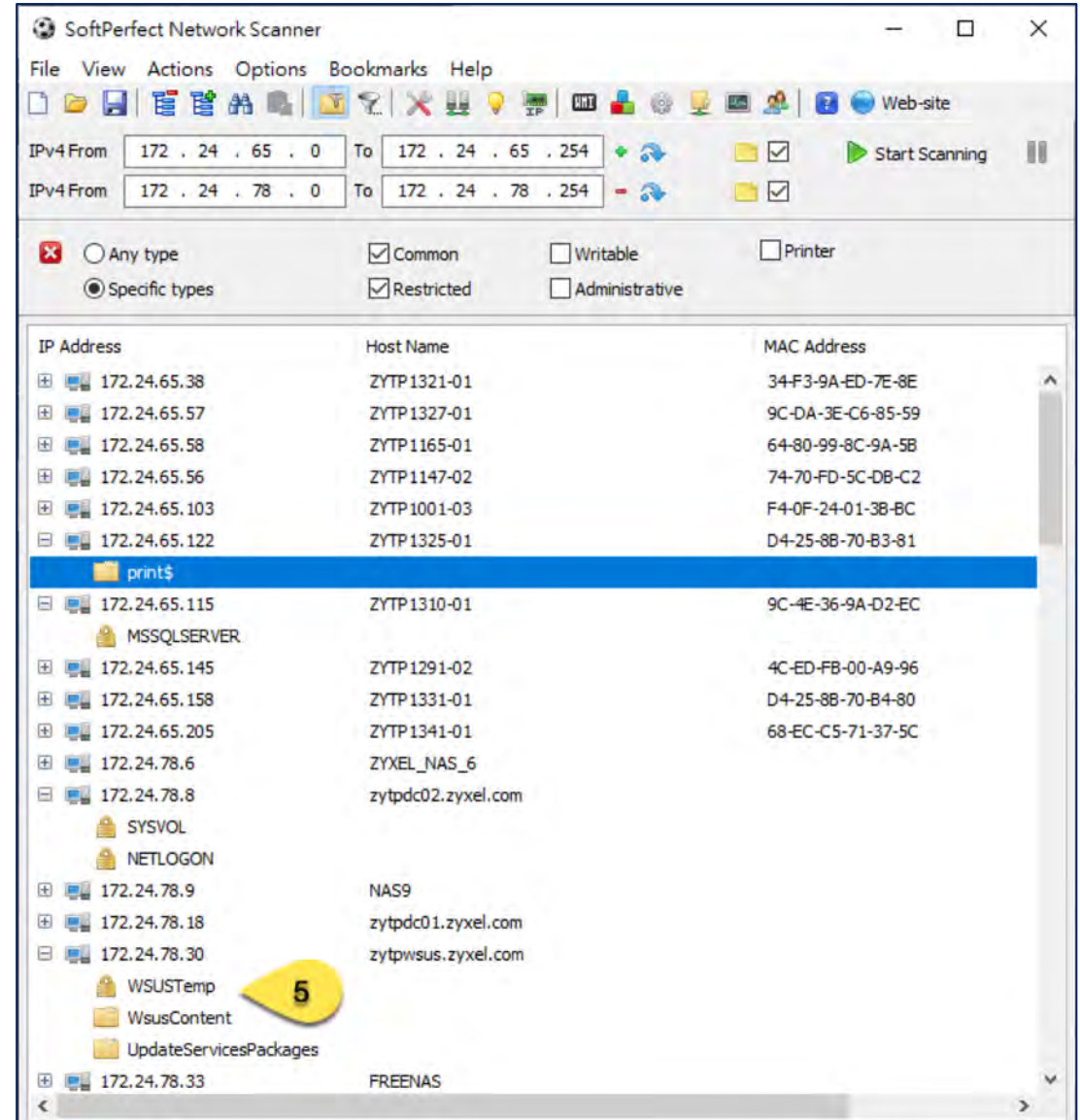
等待約5分鐘掃描完，可以看到視窗中會出現的結果記錄。

灰色字體僅供說明，無需作業

5) 掃描結果:

a. 有鎖頭: 已上鎖

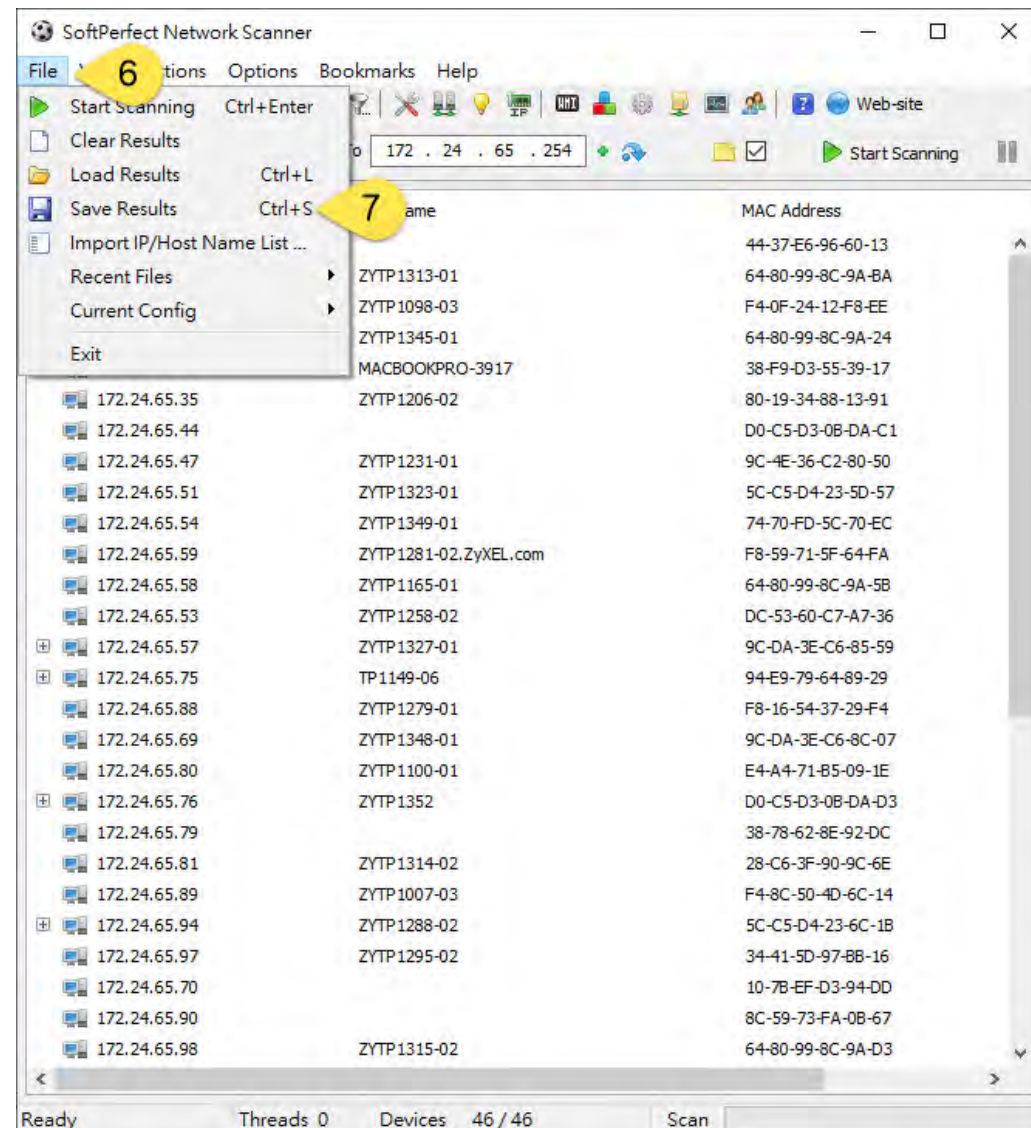
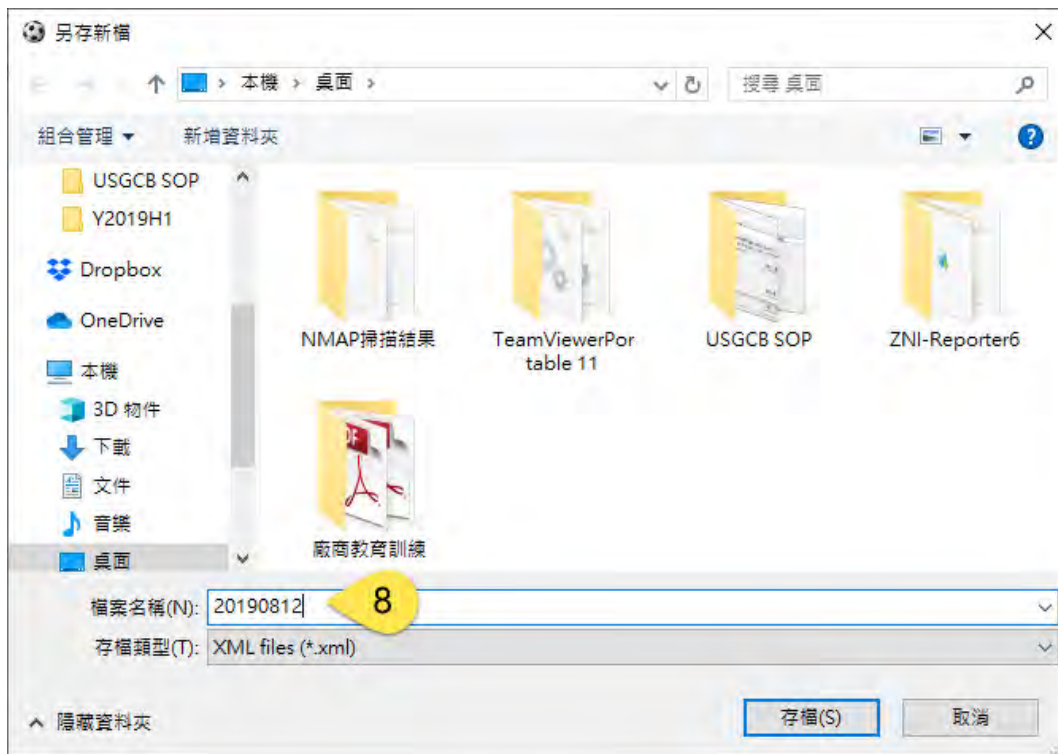
b. 無鎖頭: 未上鎖, 表示不需認證也可以存取該應用服務。



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』

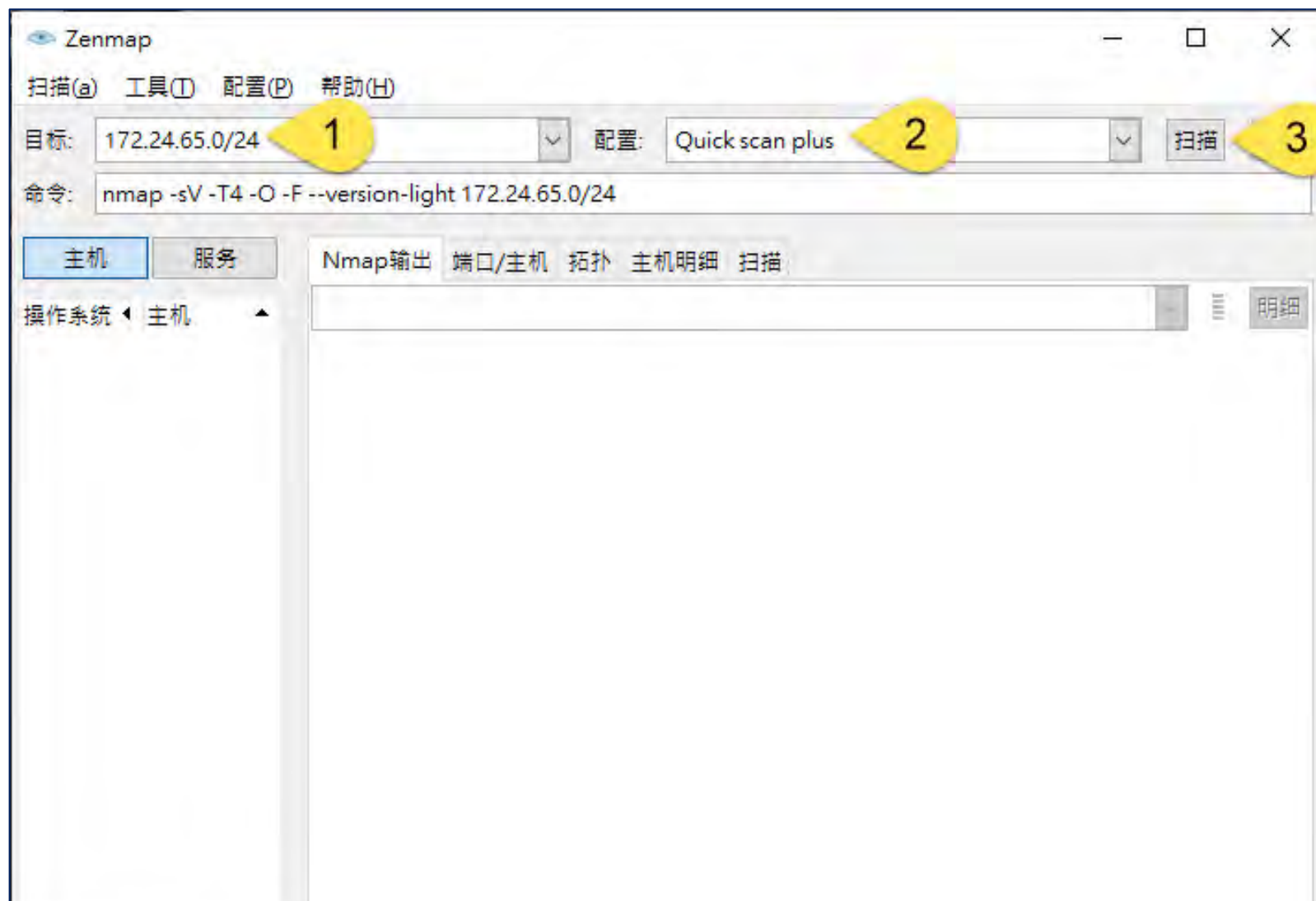
1) 輸入目標網段

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。

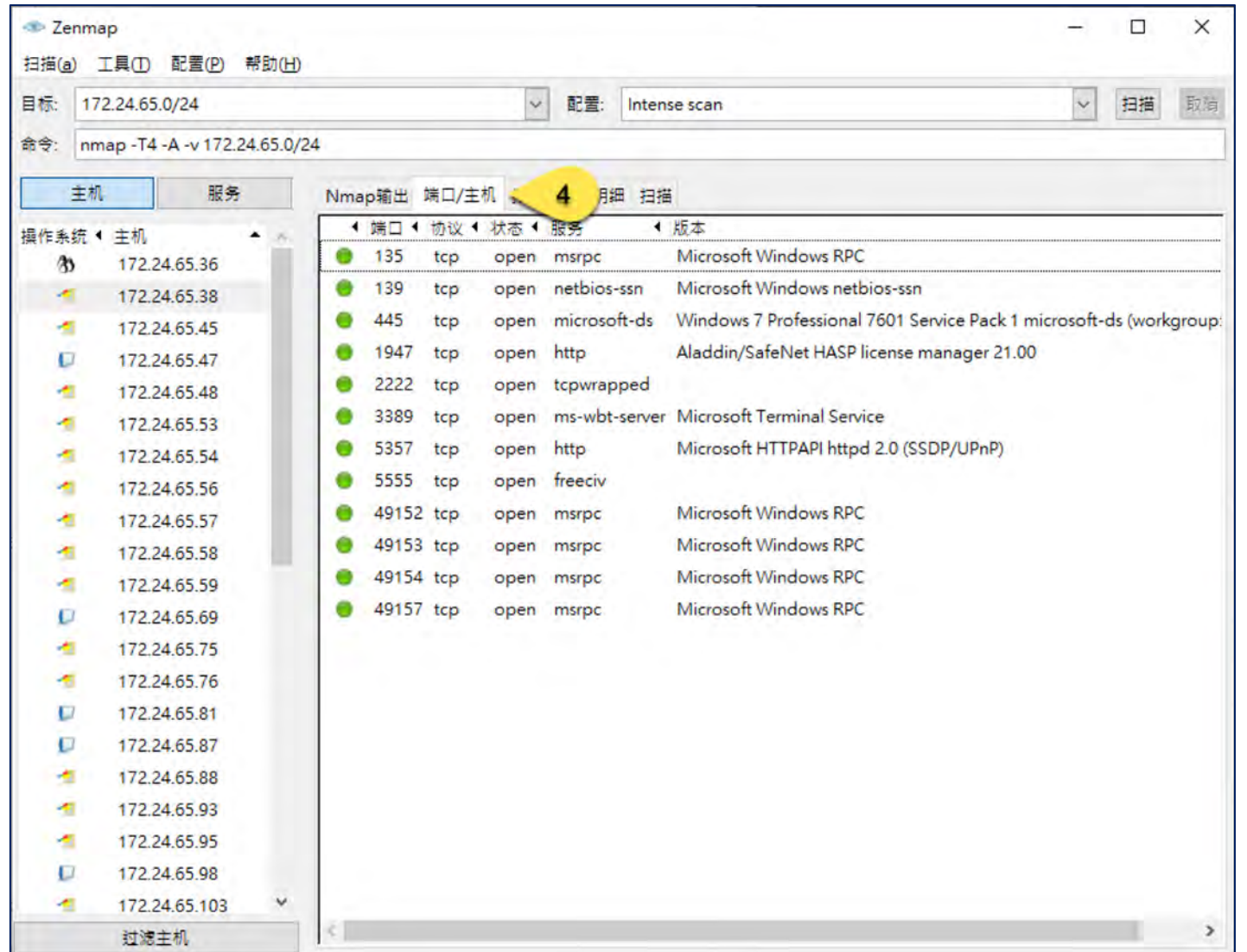
3) 開始掃描(整個過程約5分鐘)



等待約5分鐘掃描完，
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

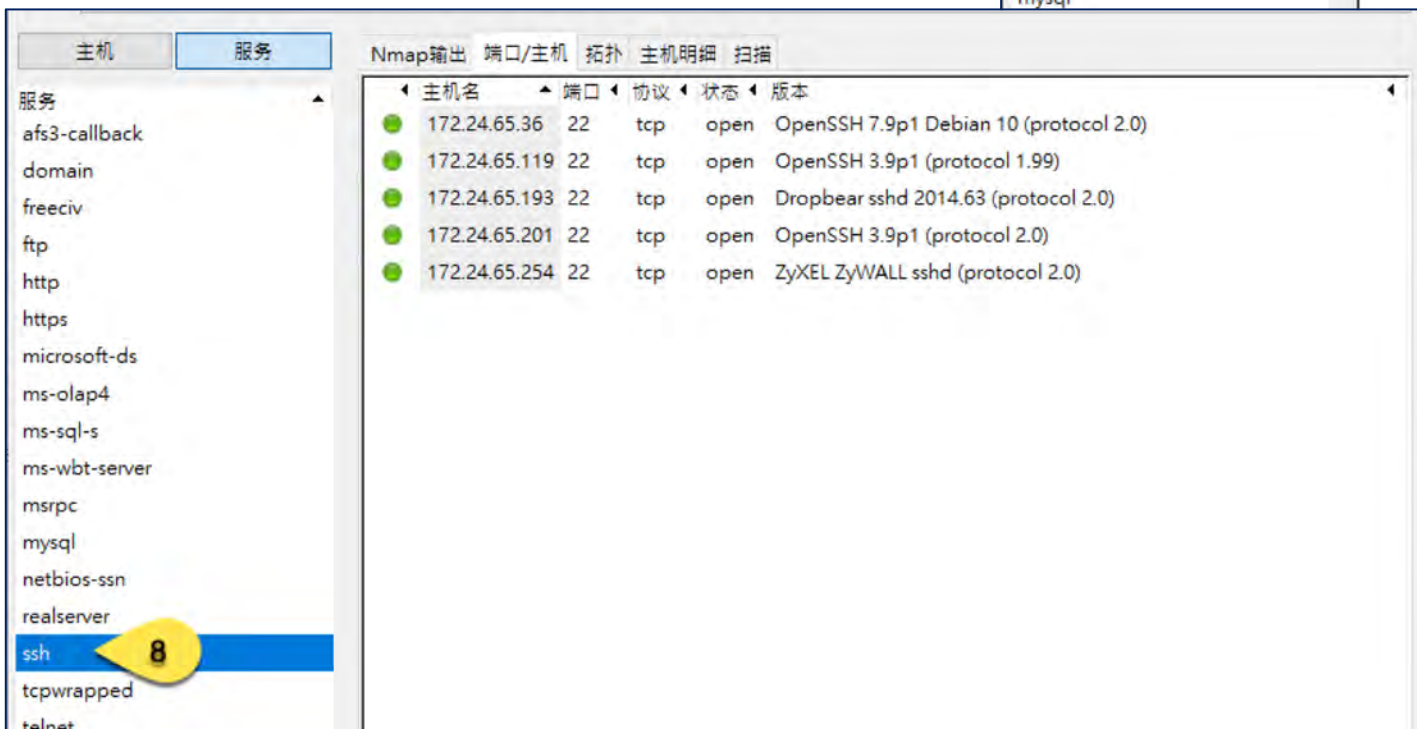
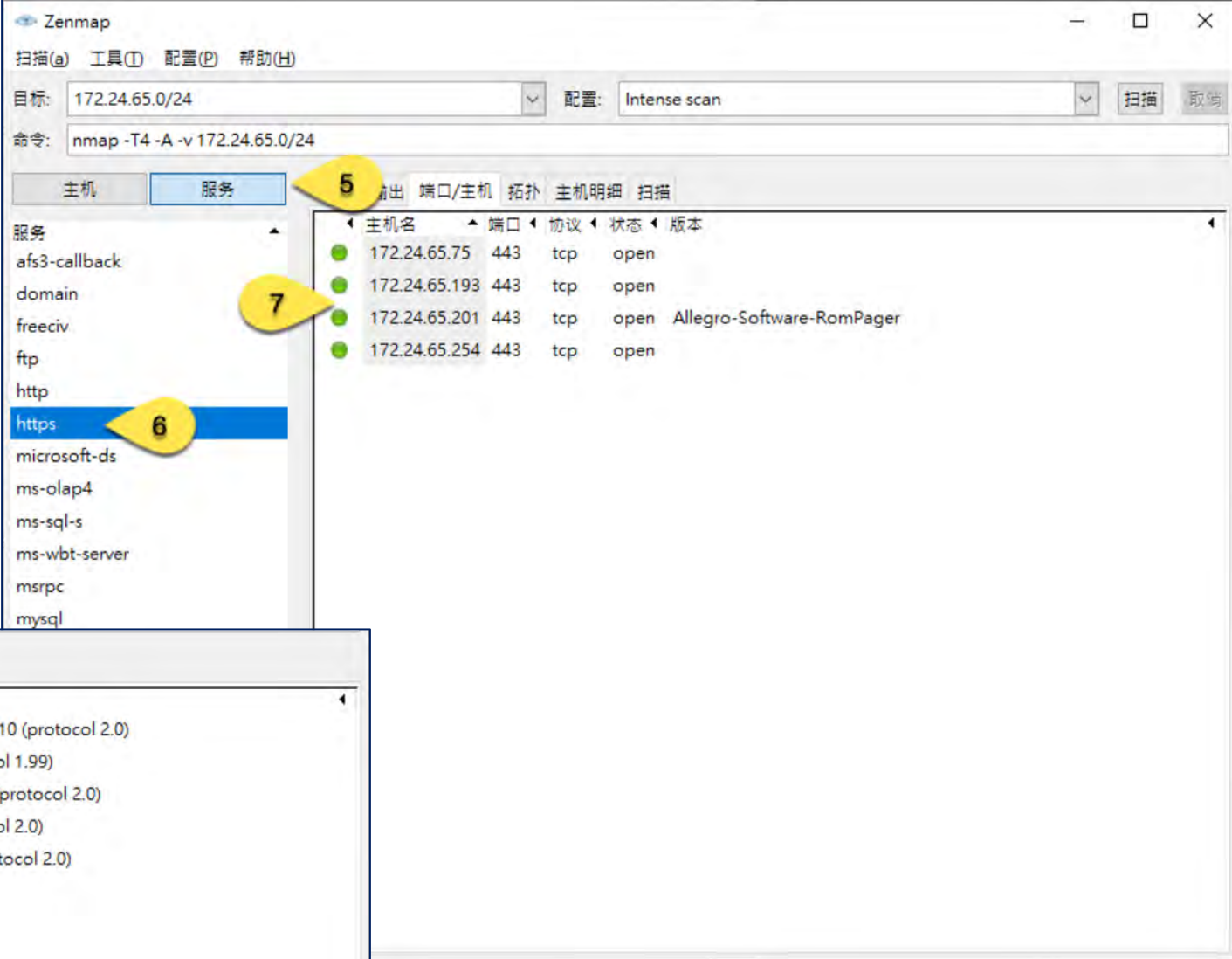


ZYXEL 工具2: Zenmap

Your Networking Ally

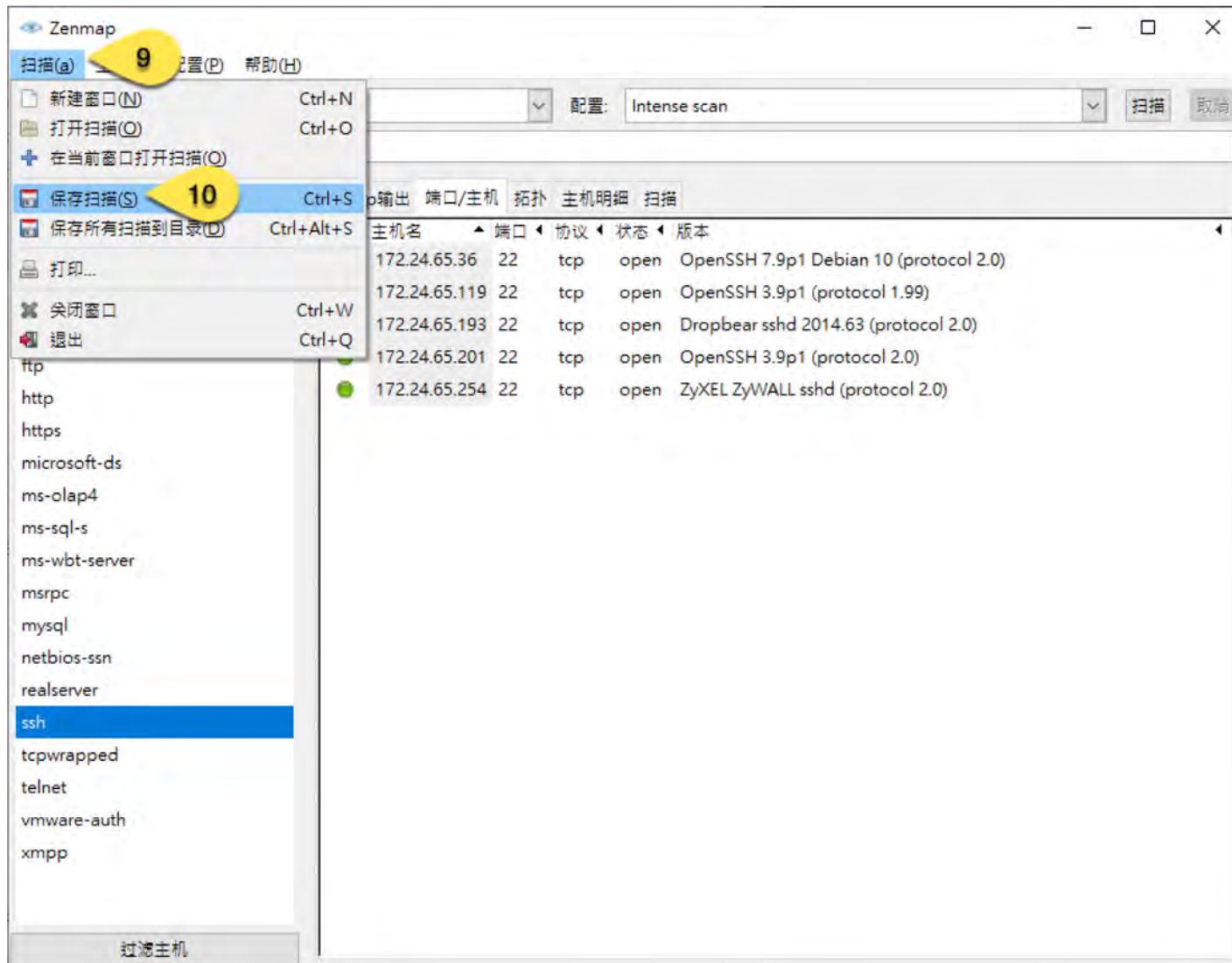
灰色字體僅供說明，無需作業

- 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



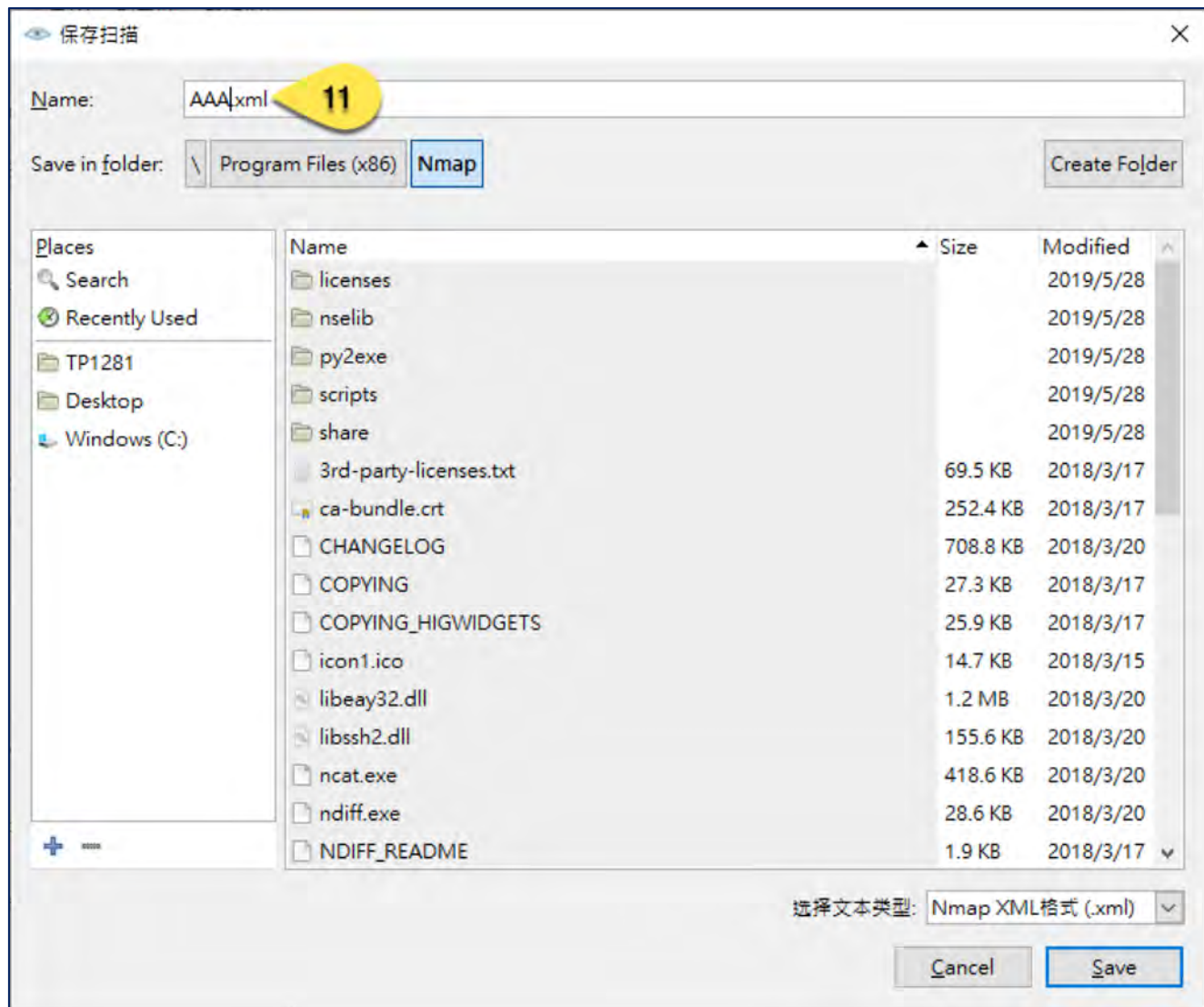
9) 儲存掃描結果

10) 保存掃描

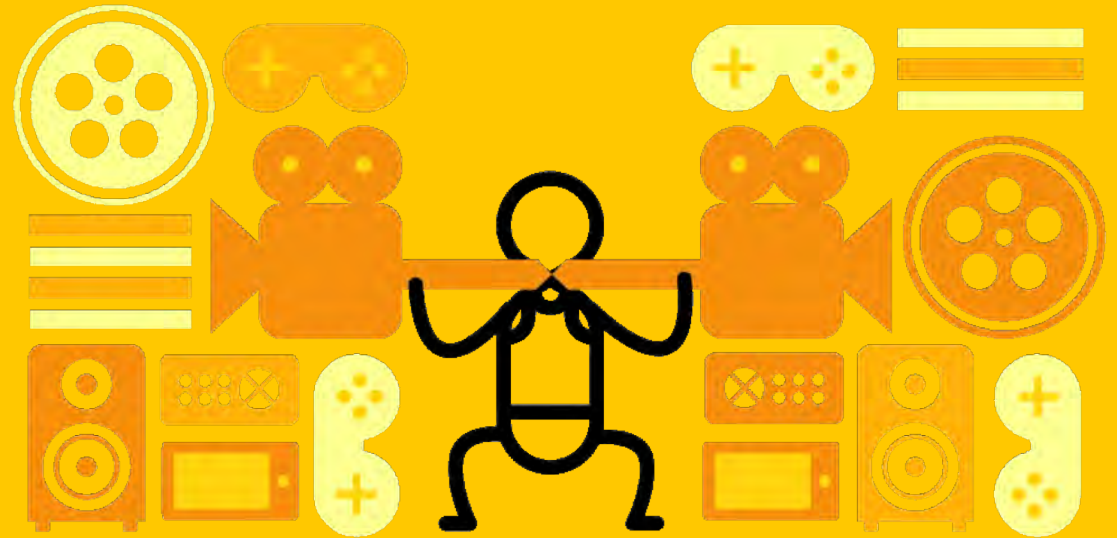


11) 另存新檔 選擇儲存檔名

- 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



1) 選擇執行檔案

- 由目錄

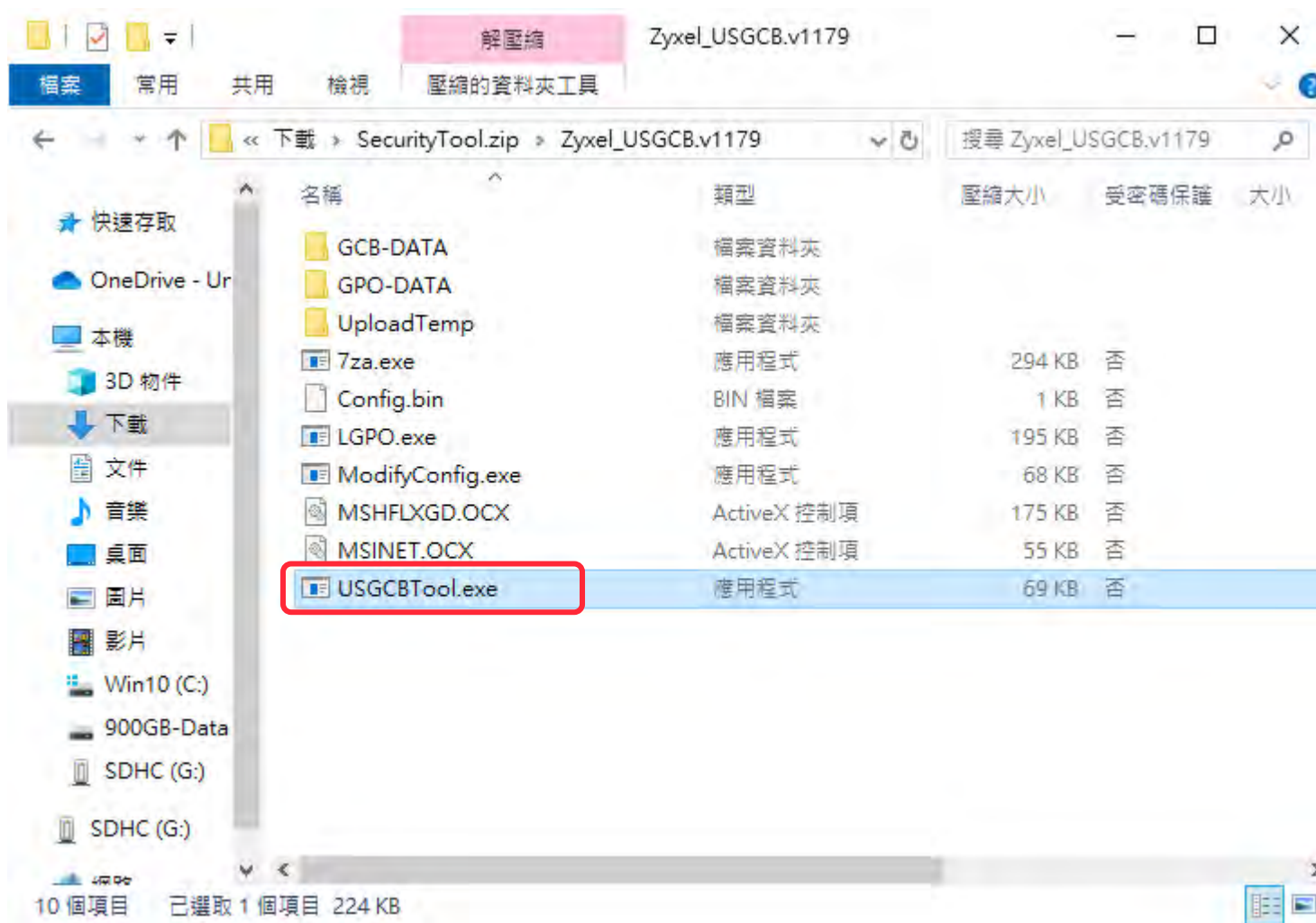
\ZyxeIUSGCB.v1179

執行: USGCBTool.exe

- 在 Windows 的App

執行告警上按“是”鈕，

開始執行檢查工具



2) 新增上傳GPO組態資料

合勤USGCB組態檢測工具

新增上傳GPO組態資料 2

已上傳GPO資料記錄 檢視上傳資料

編號	上傳日期	作業系統資訊	狀態	備註	接收分析結果電郵
----	------	--------	----	----	----------

版本: 1.0.1.413

3) 產生GPO紀錄中

合勤USGCB組態檢測工具

新增上傳GPO組態資料

已上傳GPO資料記錄 檢視上傳資料

編號	上傳日期	作業系統資訊	狀態	備註	接收分析結果電郵
<div style="border: 2px solid red; padding: 10px; display: inline-block;">產生GPO紀錄中</div> 3					

版本: 1.0.1.413

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

聯絡資訊

檢測公司資訊：重填

公司全名* 公司電話 主要聯絡人

公司地址

服務公司資訊：

公司全名* 公司統一編號* 部門*

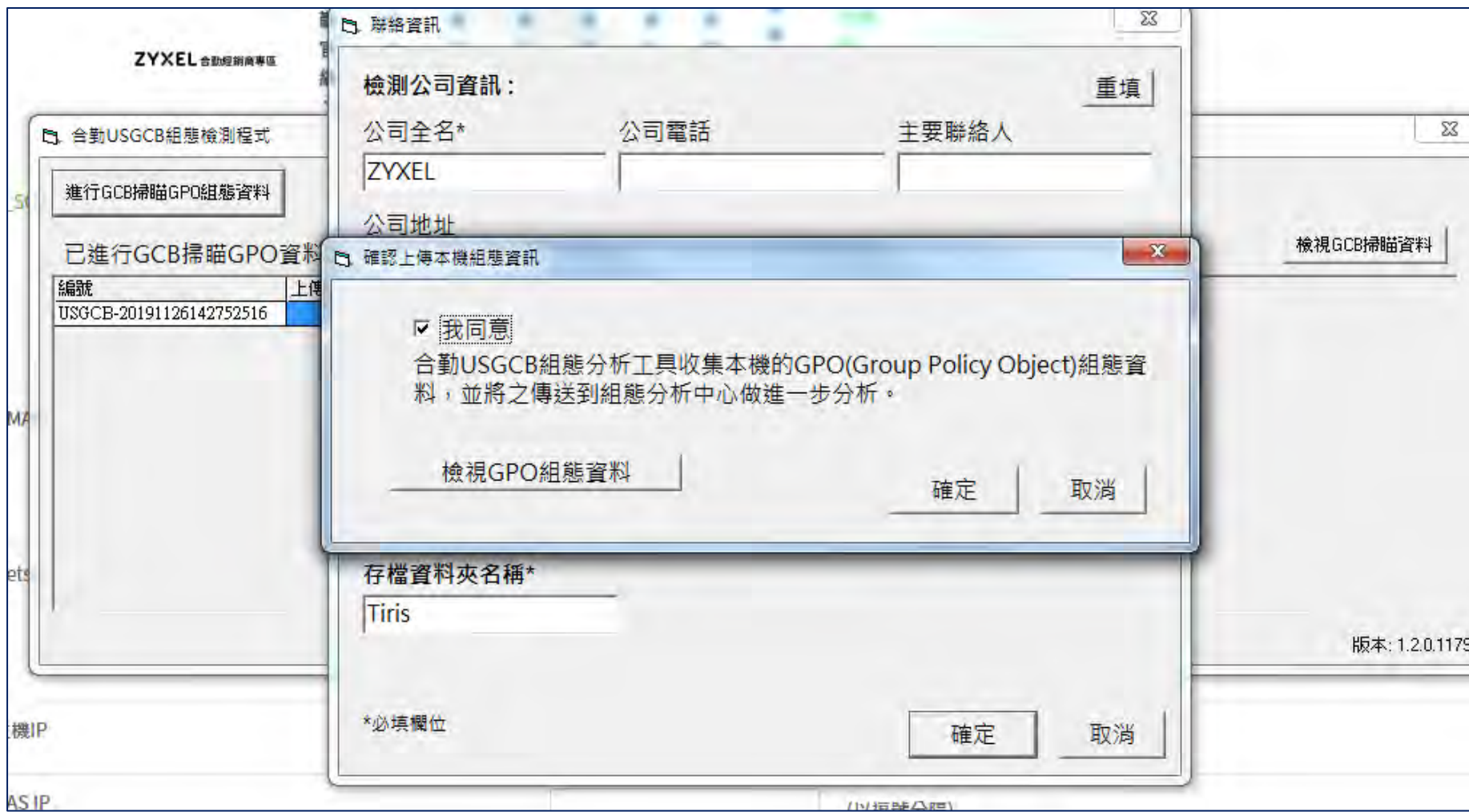
服務/檢測人員 公司電話* 分機

存檔資料夾名稱*

*必填欄位

確定 取消

5) 勾選“我同意”後，請按<確定>進行掃描



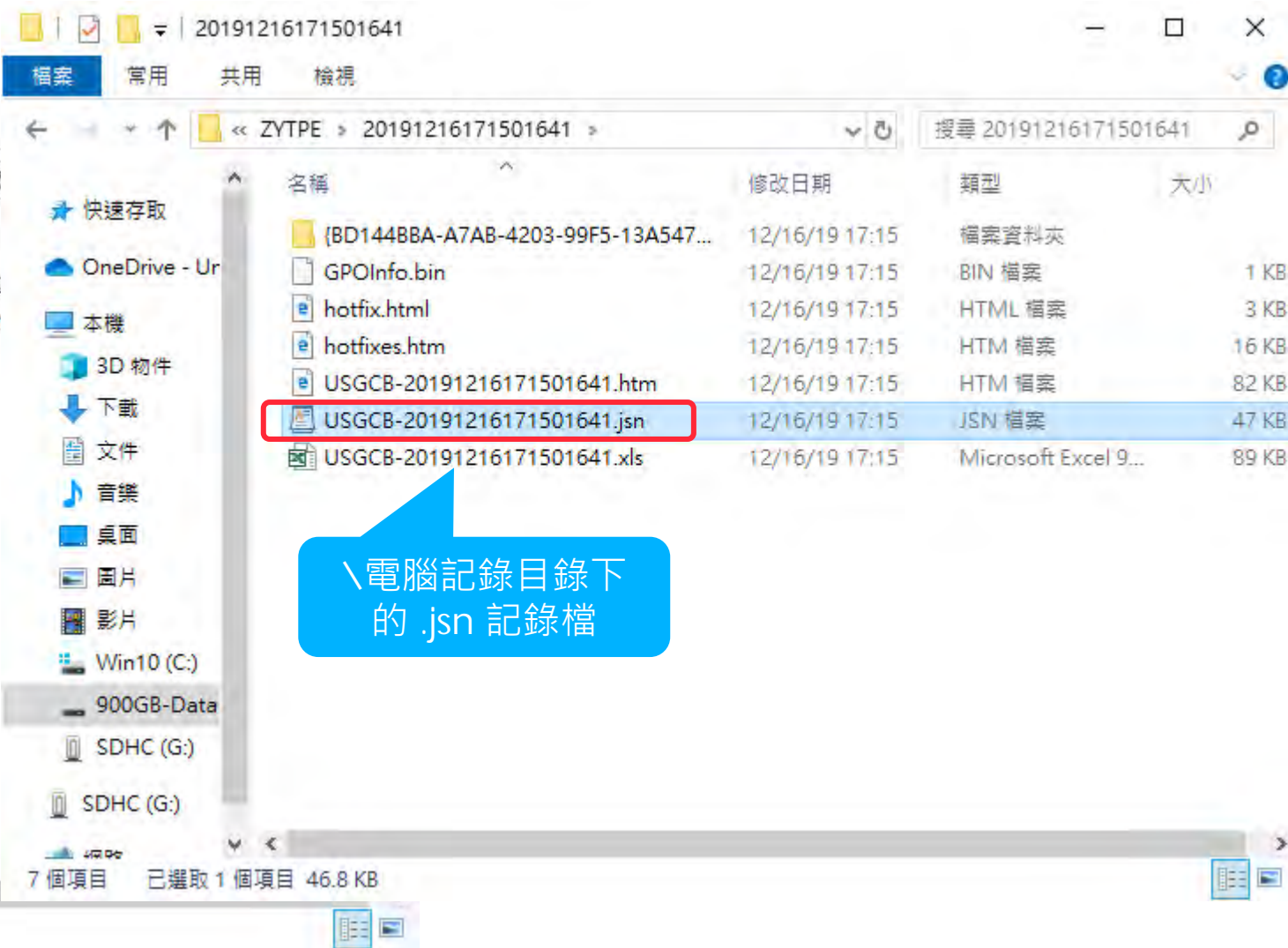
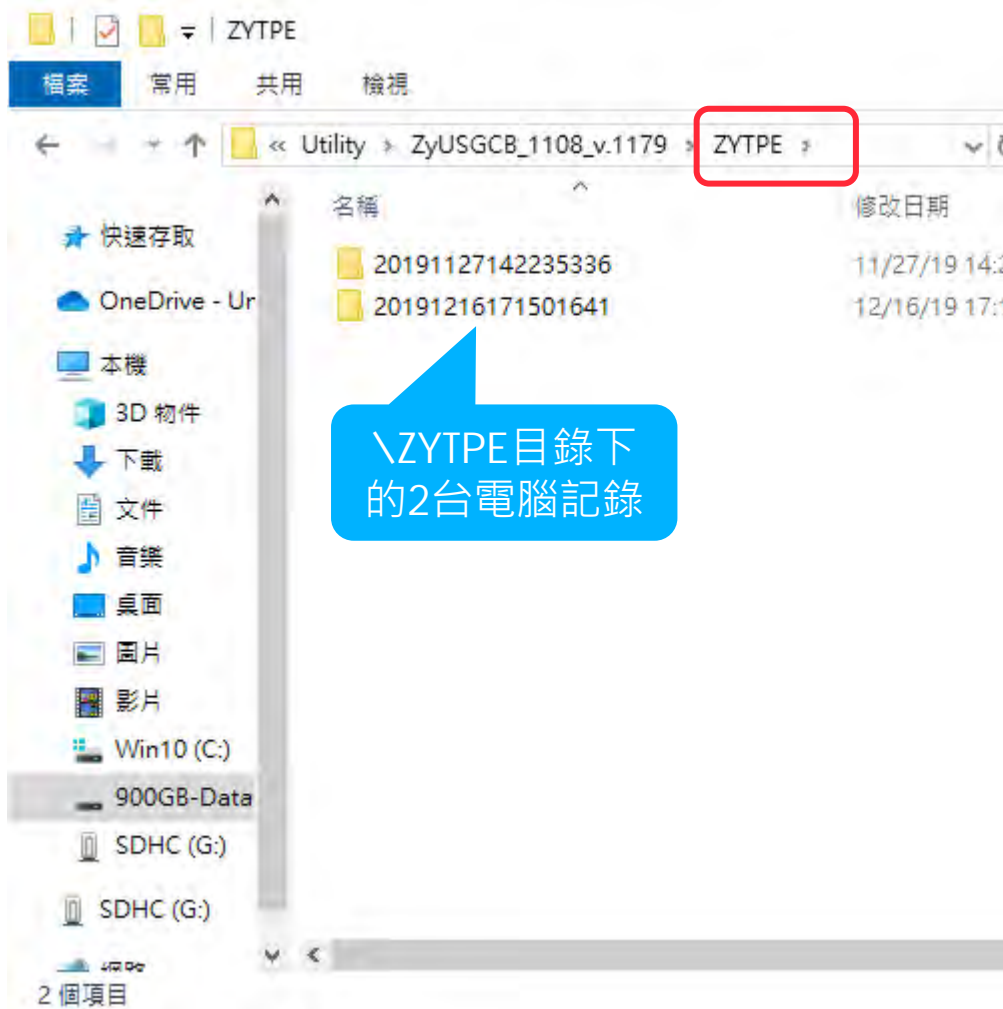
6) 完成單台電腦掃描作業

台動USGCB組態檢測程式 版本: 1.2.0.1179

分析結果 總共測項: 214

PolicyType	PolicyGroupOrRegisterKey	PolicySetting	Issue
HKLM	Software\Microsoft\Windows\CurrentVersion\Policy	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

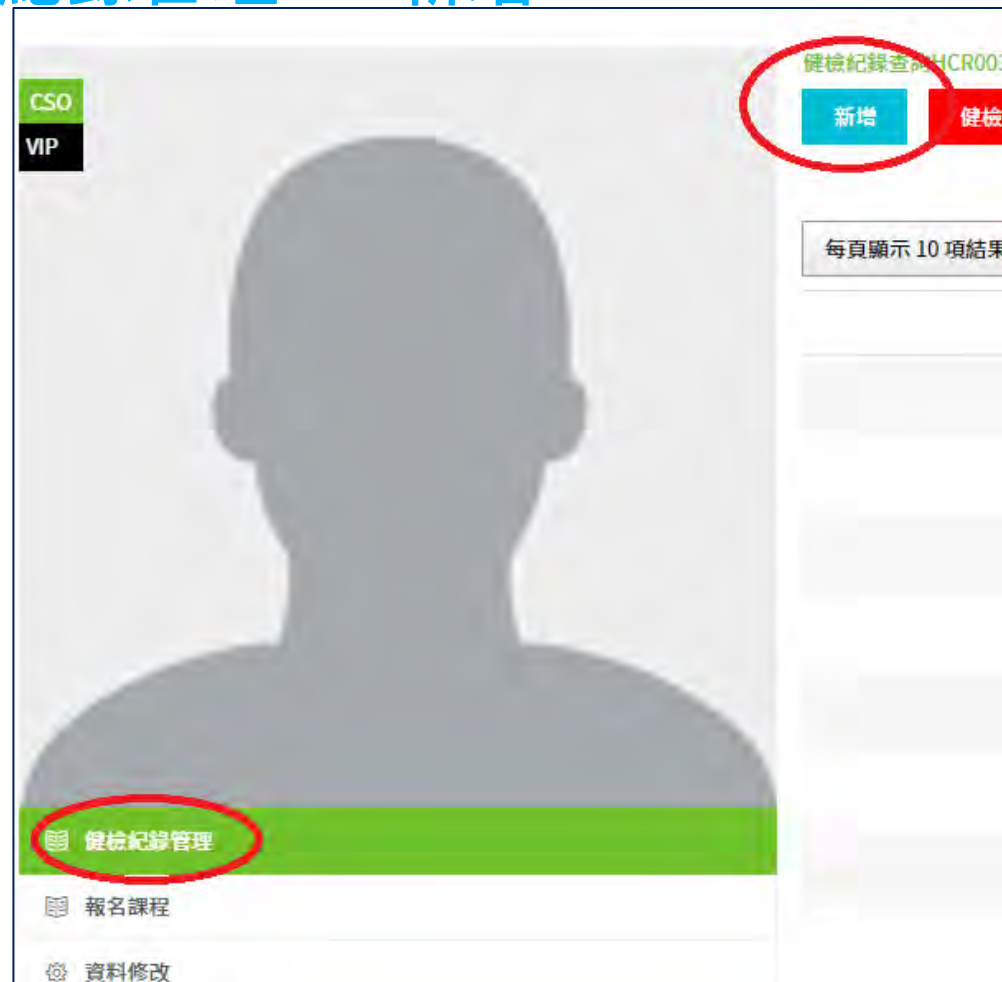
7) 確認儲存記錄



上傳資安掃描記錄檔 進行資安健檢分析



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



● 填寫基本資訊

- ◆ 填寫的檢測資訊，將列印在檢測報告的封面

健康紀錄查詢HCR003_SCN2

基本資訊 問卷填寫

受測公司資訊

*公司名稱：

主要聯絡人： 公司電話：

公司地址：

服務公司資訊

*公司名稱：

*統一編號： *部門：

服務/檢測人員： *公司電話： #

暫存 下一步

CSO
VIP

健康紀錄管理
報名課程
資料修改

● 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	<input type="radio"/> 是(續填1.1) <input type="radio"/> 否(跳至第2題)
1.1	系統網段是否可以直接連結 Internet ?	<input type="radio"/> 是 <input type="radio"/> 否
2	貴公司是否有對外的服務 (例如:網頁服務)	<input type="radio"/> 是(續填2.1) <input type="radio"/> 否(跳至第3題)
2.1	對外伺服器直接使用公有IP	<input type="radio"/> 是 <input type="radio"/> 否
2.2	對外伺服器使用 防火牆NAT轉址提供服務	<input type="radio"/> 是 <input type="radio"/> 否
2.3	如有網頁服務,公司是否有架設網站應用防火牆	<input type="radio"/> 是 <input type="radio"/> 否
3	貴公司是否有使用企業防火牆 (非家用 Router)	<input type="radio"/> 是(續填3.1) <input type="radio"/> 否(跳至第4題)
3.1	是否啟用內網/外網/DMZ安全防禦設定	<input type="radio"/> 是 <input type="radio"/> 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	<input type="radio"/> 是 <input type="radio"/> 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)	<input type="radio"/> 一個月以內 <input type="radio"/> 一~三個月 <input type="radio"/> 半年以上
4.1	員工進入公司網路是否認證	<input type="radio"/> 是 <input type="radio"/> 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)	<input type="radio"/> 是 <input type="radio"/> 否
5.1	公司無線網路 加密等級是否到達 WPA2	<input type="radio"/> 是 <input type="radio"/> 否
5.2	公司無線網路是否區分用途的 SSID	<input type="radio"/> 是 <input type="radio"/> 否
5.3	公司無線網路是否有分群(員工、訪客)?	<input type="radio"/> 是 <input type="radio"/> 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)	<input type="radio"/> 是 <input type="radio"/> 否
6	員工是否有從外部連入內網需求	<input type="radio"/> 是(續填6.1) <input type="radio"/> 否(跳至第7題)
6.1	使用 VPN 遠端連入公司	<input type="radio"/> 是 <input type="radio"/> 否
6.2	是否可透過其他遠端軟體連入公司	<input type="radio"/> 是 <input type="radio"/> 否
7.1	是否有使用RAID5等級以上 NAS 或 File Server 進行檔案備份	<input type="radio"/> 是 <input type="radio"/> 否
7.2	是否有準備系統還原檔 (System Image) 以供系統救援使用	<input type="radio"/> 是 <input type="radio"/> 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)	<input type="radio"/> 全部安裝 <input type="radio"/> 部分未安裝 <input type="radio"/> 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)	<input type="radio"/> 一個月以內 <input type="radio"/> 一~三個月 <input type="radio"/> 半年以上

上一步
暫存
下一步

- 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。

紀錄上傳HCR003_SCN4

基本資訊 問卷填寫 上傳掃描紀錄

第一組網段

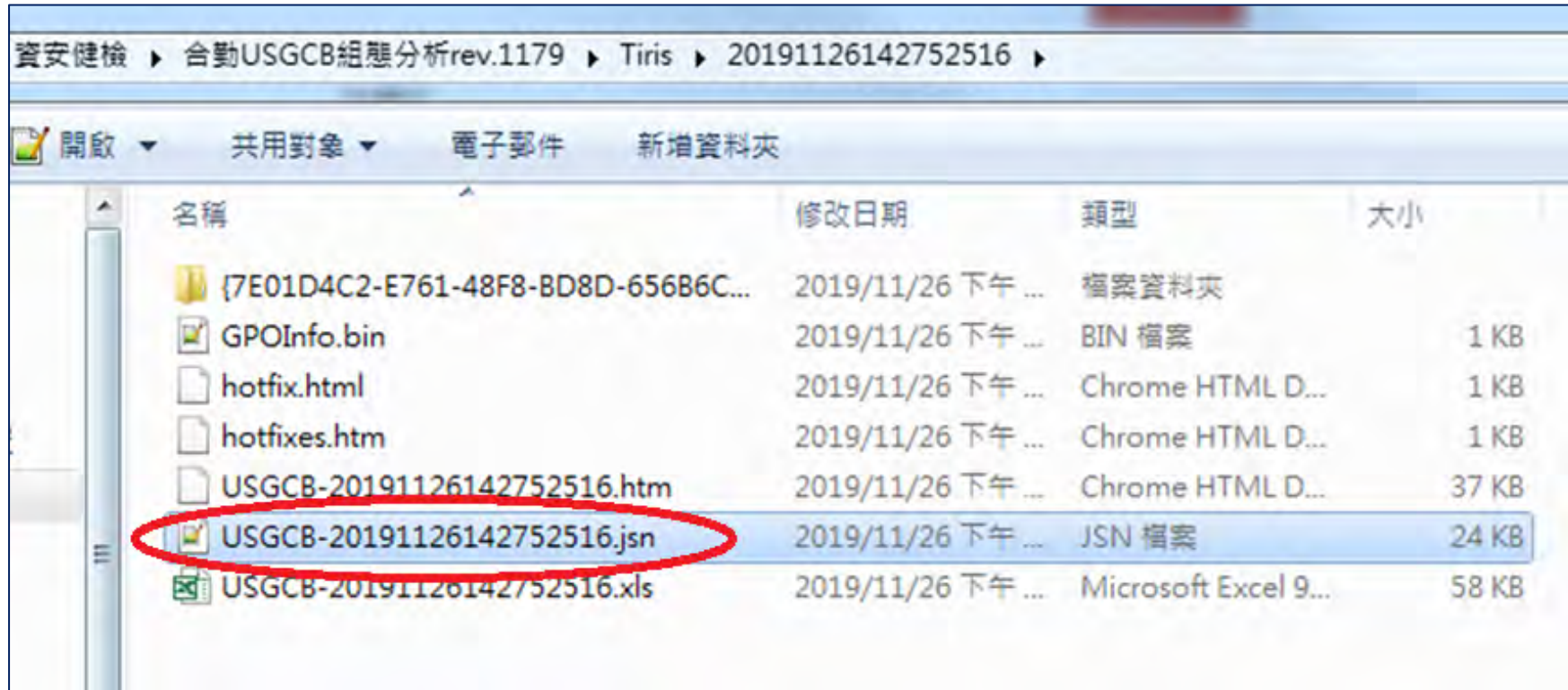
1	NMAP 掃描紀錄	<input type="button" value="選擇檔案"/> 未選擇任何檔案	僅可上傳xml檔案
		<input type="button" value="刪除"/>	
2	Netscan 掃描紀錄	<input type="button" value="選擇檔案"/> 未選擇任何檔案	僅可上傳xml檔案
		<input type="button" value="刪除"/>	
	主機IP	<input type="text"/>	(以逗號分隔)
	NAS IP	<input type="text"/>	(以逗號分隔)

第二組網段

1	NMAP 掃描紀錄	<input type="button" value="選擇檔案"/> 未選擇任何檔案	僅可上傳xml檔案
		<input type="button" value="刪除"/>	

上傳步驟

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



● 上傳網路拓樸圖



網路拓樸圖

選擇檔案 未選擇任何檔案

註：僅可上傳jpg, doc, docx, pdf檔案

刪除

上一步 暫存 下一步

The screenshot shows a web interface for uploading a network topology diagram. At the top, the title '網路拓樸圖' (Network Topology Diagram) is displayed. Below it, there is a file selection area with a button labeled '選擇檔案' (Select File) and the text '未選擇任何檔案' (No file selected). A red note below states '註：僅可上傳jpg, doc, docx, pdf檔案' (Note: Only jpg, doc, docx, pdf files can be uploaded). To the left of the note is a red '刪除' (Delete) button. At the bottom of the interface, there are three navigation buttons: '上一步' (Previous Step) in orange, '暫存' (Save) in red, and '下一步' (Next Step) in green.

- 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。

紀錄檔

第1組 NMAP:

NetScan:

第2組 NMAP:

NetScan:

第3組 NMAP:

NetScan:

GCB

網路拓模圖

上一步 確認送出

ZYXEL
Your Networking Ally