檢測工具下載與安裝說明







尚未成為會員

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



※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

| | 健檢紀錄查詢HCR003_S | CN1 | | | |
|--------|---------------------|------|------------|------------|-------|
| | 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 | | | |
| 建檢紀錄管理 | 1209-FW | 報告完成 | 2019-12-09 | 2019-12-09 | 按視 |
| 名課程 | 1209-No-FW | 報告完成 | 2019-12-09 | 2019-12-09 | 酸醌 |
| 料修改 | 1216-1609 上傳記錄_NoFW | 報告完成 | 2019-12-16 | 2019-12-16 | 破現 |
| | 1216-1614 上傳記錄_FW | 待箦收 | 2019-12-16 | | 16 AL |
| | 1216_TESTLOG | 待簽收 | 2019-12-16 | | 建築 |
| | 1218更新_FW-2VLAN | 報告完成 | 2019-12-18 | 2019-12-18 | 位視 |
| | 1218更新 NoFW | 報告完成 | 2019-12-18 | 2019-12-18 | |



• 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

| → → → → → → → → → → → → → → → → → | ★ 1 | | | |
|-----------------------------------|---------------------|------------|--------------|-----|
| C:\Users\TP1279\Download | s\SecurityTool.zip\ | | | ~ |
| 名稱 | 大小 | 封裝後大小 | 修改日期 | 建立 |
| Zyxel_USGCB.v1179 | 3 633 546 | 1 076 271 | 2019-11-29 0 | 201 |
| NetScan_64bits.exe | 1 643 032 | 1 613 938 | 2017-07-03 1 | 201 |
| nmap-7.80-setup.exe | 26 922 800 | 26 910 637 | 2019-10-16 0 | 201 |
| < | | | | > |





• 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
 - Mmap: 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



ZYXEL 工具1: SoftPerfect Network Scanner

- 一、執行 NetScan_64bits.exe 程式安装
- 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

| SoftPerfect Network Scann | er | - 🗆 × |
|--|--------------------------|-------------------------|
| 🗋 🗁 🛃 🐮 🐮 👫 🐴 | | 📃 📧 🧟 🔽 🥪 Web-site |
| Pv4 From 172 . 24 . 65 . | 0 To 172 . 24 . 65 . 254 | 🗾 🗹 🕞 Start Scannin 🗸 👍 |
| Any type Specific types | Common Restricted | Printer |
| IP Address | Host Name | MAC Address |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

ZYXEL 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。

| File View Actions Option | s Bookmarks Help | | |
|----------------------------|------------------------------|------------------------|----|
| □ 🗁 🛃 🖺 🔡 🏔 📭 | 0 To 172 - 24 - 65 - 254 • 3 | 🖗 💆 📾 🧟 🔁 🝚 Web-site | 10 |
| Pv4 From 172 . 24 . 78 . | 0 To 172 . 24 . 78 . 254 - 3 | | |
| Any type Specific types | Common Writable | Printer | |
| IP Address | Host Name | MAC Address | Ī |
| 172.24.65.38 | ZYTP 1321-01 | 34-F3-9A-ED-7E-8E | |
| 172.24.65.57 | ZYTP1327-01 | 9C-DA-3E-C6-85-59 | 1 |
| 172.24.65.58 | ZYTP1165-01 | 64-80-99-8C-9A-5B | |
| 172.24.65.56 | ZYTP1147-02 | 74-70-FD-5C-DB-C2 | |
| 172.24.65.103 | ZYTP1001-03 | F4-0F-24-01-38-BC | |
| □ 🚛 172.24.65.122 | ZYTP 1325-01 | D4-25-88-70-83-81 | 1 |
| print\$ | | | |
| 🖻 🜉 172.24.65.115 | ZYTP1310-01 | 9C-4E-36-9A-D2-EC | |
| MSSQLSERVER | | | |
| 172.24.65.145 | ZYTP1291-02 | 4C-ED-FB-00-A9-96 | |
| 172.24.65.158 | ZYTP1331-01 | D4-25-88-70-84-80 | |
| 172.24.65.205 | ZYTP1341-01 | 68-EC-C5-71-37-5C | |
| 172.24.78.6 | ZYXEL_NAS_6 | | |
| 🖃 🌉 172.24.78.8 | zytpdc02.zyxel.com | | |
| SYSVOL | | | |
| METLOGON | | | |
| 172.24.78.9 | NAS9 | | |
| 172.24.78.18 | zytpdc01.zyxel.com | | |
| ⊟ 🜉 172.24.78.30 | zytpwsus.zyxel.com | | |
| WSUSTemp WsusContent | 5 | | |
| UpdateServicesPackag | jes | | |
| 172.24.78.33 | FREENAS | | 1 |

ZYXEL 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



| | Options Poolemarks H | tala | A O | | |
|------------------|----------------------|-----------------------|-------------------|--|--|
| Start Starting | Ctrla Entor | | 🔽 🦳 Web-site | | |
| Class Results | Currenter of 2 | | | | |
| Clear Results | 0 172 . 2 | 24 . 65 . 254 🔹 💦 🛄 🗹 | 👂 Start Scanning | | |
| Load Results | Ctrl+L | | | | |
| Save Results | Ctrl+S ame | MAC A | ddress | | |
| Import IP/Host N | ame List | 44-37 | -E6-96-60-13 | | |
| Recent Files | ZYTP1313-0 | 01 64-80 | -99-8C-9A-BA | | |
| Current Config | ZYTP 1098-0 | 13 F4-0F | -24-12-F8-EE | | |
| Evit | ZYTP1345-0 | 01 64-80 | -99-8C-9A-24 | | |
| LAIL | MACBOOKPI | RO-3917 38-F9 | -D3-55-39-17 | | |
| 172.24.65.35 | ZYTP1206-0 | 12 80-19 | -34-88-13-91 | | |
| 172.24.65.44 | | D0-C5 | -D3-0B-DA-C1 | | |
| 172.24.65.47 | ZYTP1231-0 |)1 9C-4E | -36-C2-80-50 | | |
| 172.24.65.51 | ZYTP1323-0 |)1 5C-C5 | -D4-23-5D-57 | | |
| 172.24.65.54 | ZYTP1349-0 | 11 74-70 | -FD-5C-70-EC | | |
| 172.24.65.59 | ZYTP1281-0 | 2.ZyXEL.com F8-59 | -71-5F-64-FA | | |
| 172.24.65.58 | ZYTP1165-0 | 01 64-80 | -99-8C-9A-5B | | |
| 172.24.65.53 | ZYTP1258-0 | 02 DC-53 | DC-53-60-C7-A7-36 | | |
| 172.24.65.57 | ZYTP1327-0 | 01 9C-DA | -3E-C6-85-59 | | |
| 172.24.65.75 | TP1149-06 | 94-E9 | -79-64-89-29 | | |
| 172.24.65.88 | ZYTP1279-0 |)1 F8-16 | -54-37-29-F4 | | |
| 172.24.65.69 | ZYTP1348-0 |)1 9C-DA | -3E-C6-8C-07 | | |
| 172.24.65.80 | ZYTP1100-0 |)1 E4-A4 | -71-85-09-1E | | |
| 172.24.65.76 | ZYTP1352 | D0-C5 | -D3-0B-DA-D3 | | |
| 172.24.65.79 | | 38-78 | -62-8E-92-DC | | |
| 172.24.65.81 | ZYTP1314-0 | 28-C6 | -3F-90-9C-6E | | |
| 172.24.65.89 | ZYTP 1007-0 |)3 F4-8C | -50-4D-6C-14 | | |
| 172.24.65.94 | ZYTP1288-0 |)2 5C-C5 | -D4-23-6C-1B | | |
| 172.24.65.97 | ZYTP1295-0 |)2 34-41 | -5D-97-BB-16 | | |
| 172.24.65.70 | | 10-7B | -EF-D3-94-DD | | |
| 172.24.65.90 | | 8C-59 | -73-FA-0B-67 | | |
| 172.24.65.98 | ZYTP1315-0 | 02 64-80 | -99-8C-9A-D3 | | |
| < | | | > | | |

二、Zenmap 網路掃瞄工具





- 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)

| ≪ Zenmap 扫描(a) 工具① 配置(Ⅰ) | 2) 帮助(日) | - 🗆 X |
|-----------------------------|--------------------------------|----------|
| 目标: 172.24.65.0/24 | 1 🗸 配置: Quick scan plus < 2 | ~ 扫描 < 3 |
| 命令: nmap -sV -T4 -O | -Fversion-light 172.24.65.0/24 | |
| 主机服务 | Nmap输出 端口/主机 拓扑 主机明细 扫描 | |
| 操作系统 ◀ 主机 ▲ | | - 目明細 |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |



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

| 目标: | 172.24.65.0/24 | | | | ~ | 配置: Inten | se scan | ~ | 扫描 | 取猜 |
|-----------|------------------------|-----------|----------|-------|---------|---------------|--|-----------|----------|-------|
| 命令: | nmap -T4 -A -v 172.2 | 4.65.0/24 | | | - Inter | | | | Land I | |
| | 主机 服务 | N | man it W | 推口/主 | 和 _ | A 849 1718 | | | | |
| | | | ▲端□▲ | 前後く | 状态 ◆ | | 版本 | | | _ |
| 操作系 /h | 统 ▲ 王机 172.24.65.26 | ^ | 135 | tcp | open | msrpc | Microsoft Windows RPC | | | |
| 30 | 172.24.03.30 | | 9 139 | tcp | open | netbios-ssn | Microsoft Windows netbios-ssn | | | |
| | 172.24.03.30 | | 445 | tcp | open | microsoft-ds | Windows 7 Professional 7601 Service Pack 1 m | icrosoft- | ds (work | group |
| | 172.24.03.43 | | 9 1947 | tcp | open | http | Aladdin/SafeNet HASP license manager 21.00 | | | |
| - | 172.24.03.47 | | 2222 | tcp | open | tcpwrapped | | | | |
| | 172.24.03.46 | | 3389 | tcp | open | ms-wbt-server | Microsoft Terminal Service | | | |
| | 172.24.03.33 | | 5357 | tcp | open | http | Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) | | | |
| | 172.24.65.56 | | 5555 | tcp | open | freeciv | | | | |
| | 172.24.05.50 | | 49152 | 2 tcp | open | msrpc | Microsoft Windows RPC | | | |
| | 172.24.05.57 | | 49153 | 3 tcp | open | msrpc | Microsoft Windows RPC | | | |
| | 172.24.05.58 | | 49154 | 4 tcp | open | msrpc | Microsoft Windows RPC | | | |
| | 172.24.05.59 | | 49157 | 7 tcp | open | msrpc | Microsoft Windows RPC | | | |
| - | 172.24.03.09 | | e | | | | | | | |
| | 172.24.03.73 | | | | | | | | | |
| | 172.24.03.70 | | | | | | | | | |
| | 172.24.03.01 | | | | | | | | | |
| - | 172 24 65 99 | | | | | | | | | |
| | 172 24 65 02 | | | | | | | | | |
| | 172 24 65 05 | | | | | | | | | |
| | 172 24 65 00 | | | | | | | | | |
| - | 172 24 65 102 | ~ | | | | | | | | |
| | 172.24.03.103 | 1 6 | - | | | | | | 100 | > |



灰色字體僅供說明, 無需作業

- 選擇服務 5)
- 選擇https 6)

服务

主机

afs3-callback

服务

domain

freeciv ftp

> http https microsoft-ds ms-olap4 ms-sal-s ms-wbt-server

msrpc mysql netbios-ssn realserver

ssh

tcpwrapped talaat

8

- 7) 目前有開啟https
- 有開啟ssh服務的 8)

| | | | | - | | × |
|---|-----------------------------------|-----------------------|--------------------------------|--------------------|-----|----|
| 2: Zenmap | 目标: 172.24.65.0/24 | ✓ 配置 | : Intense scan | ~ | 扫描 | 取消 |
| | 命令: nmap -T4 -A -v 172.24.65.0/24 | | | | | |
| 毎雪作業 | 主机 服务 5 | 加出 端口/主机 拓扑 主机明 | 1细 扫描 | | | |
| | 服务 • 1 | 主机名 ▲ 端口 4 协议 4 | 状态 ◀ 版本 | | | • |
| 7/2 | afs3-callback | 172.24.65.75 443 tcp | open | | | |
| 济 | domain 7 | 172.24.65.201 443 tcp | open Allegro-Software-RomPager | | | |
| | freeciv | 172.24.65.254 443 tcp | open | | | |
| ins | http | | | | | |
| 103 | https 6 | | | | | |
| | microsoft-ds | | | | | |
| 用成川川口5日1111次 | ms-olap4 | | | | | |
| | ms-sql-s | | | | | |
| SSh版務的主機 | msrpc | | | | | |
| | mysql | _ | | | | |
| Nman输出 皓口/主机 拓扑 土和服细 扫描 | | | | | | |
| ▲ 主机名 ▲ 端口 ◆ 协议 ◆ 状态 ◆ 版本 | 4 | | | | | |
| 172.24.65.36 22 tcp open OpenSSH 7.9p1 Debian | 10 (protocol 2.0) | | | | | |
| 172.24.65.119 22 tcp open OpenSSH 3.9p1 (protocol) | ol 1.99) | | | | | |
| 172.24.65.193 22 tcp open Dropbear sshd 2014.63 (| protocol 2.0) | | | | | |
| 172.24.65.201 22 tcp open OpenSSH 3.9p1 (protoco 7.2.24.65.201 22 tcp open OpenSSH 3.9p1 (protoco | 51 2.0) | | | | | |
| 172.24.65.254 22 tcp open ZyXEL ZyWALL sshd (prot | tocol 2.0) | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | © 2019 7 ¥¥ | (FL | 15 |
| | | | | | , | |



9) 儲存掃描結果10) 保存掃瞄

| Zenmap | | | | | | | - | | × |
|---|----------------|---------------|------|------|-------|--|---|------------|----------|
| 扫描(4) 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 | 帮助(<u>H</u>) | | | | | | | | |
| ■ 新建窗口(N) | Ctrl+N | | ~ | 配置: | Inter | nse scan | ~ | 扫描 | 取淌 |
| ◎ 打开扫描(O) | Ctrl+O | - | | 1000 | - | | | In comment | 10000000 |
| ✤ 在当前窗口打开扫描(O) | | | | | | | | | _ |
| 🗟 保存扫描(S) 🥄 10 | Ctrl+S | p输出 端口/主相 | 机 拓扑 | 主机明 | 细 扫描 | ä | | | |
| 保存所有扫描到目录(D) | Ctrl+Alt+S | 主机名 🔺 | 端口 < | 协议◀ | 状态◀ | 版本 | | | • |
| 昌 打印 | | 172.24.65.36 | 22 | tcp | open | OpenSSH 7.9p1 Debian 10 (protocol 2.0) | | | |
| | Ctrl+W | 172.24.65.119 | 22 | tcp | open | OpenSSH 3.9p1 (protocol 1.99) | | | |
| · 大内図口 | Ctrl+O | 172.24.65.193 | 22 | tcp | open | Dropbear sshd 2014.63 (protocol 2.0) | | | |
| ftp | CuitQ | 172.24.65.201 | 22 | tcp | open | OpenSSH 3.9p1 (protocol 2.0) | | | |
| http | | 172.24.65.254 | 22 | tcp | open | ZyXEL ZyWALL sshd (protocol 2.0) | | | |
| https | | | | | | | | | |
| microsoft-ds | | | | | | | | | |
| ms-olap4 | | | | | | | | | |
| ms-sql-s | | | | | | | | | |
| ms-wbt-server | | | | | | | | | |
| msrpc | | | | | | | | | |
| mysql | | | | | | | | | |
| netbios-ssn | | | | | | | | | |
| realserver | | | | | | | | | |
| ssh | | | | | | | | | |
| tcpwrapped | | | | | | | | | |
| telnet | | | | | | | | | |
| vmware-auth | | | | | | | | | |
| xmpp | | | | | | | | | |
| | | | | | | | | | |
| 过滤主机 | | | | | | | | | |





| Name: AAA | ml 11 | | |
|-------------------------------|------------------------|-------------|-----------------|
| Save in <u>f</u> older: \ Pro | ogram Files (x86) Nmap | | Create Folde |
| <u>P</u> laces | Name | ▲ Size | Modified |
| Search | 📄 licenses | | 2019/5/28 |
| Recently Used | 📄 nselib | | 2019/5/28 |
| 🛅 TP1281 | py2exe | | 2019/5/28 |
| 🖻 Desktop | 🛅 scripts | | 2019/5/28 |
| Windows (C:) | 🗁 share | | 2019/5/28 |
| | 3rd-party-licenses.txt | 69.5 | KB 2018/3/17 |
| | a-bundle.crt | 252 | 4 KB 2018/3/17 |
| | CHANGELOG | 708 | .8 KB 2018/3/20 |
| | | 27.3 | KB 2018/3/17 |
| | COPYING_HIGWIDGETS | 25.9 | KB 2018/3/17 |
| | 🗋 icon1.ico | 14.7 | KB 2018/3/15 |
| | 🕤 libeay32.dll | 1.2 | MB 2018/3/20 |
| | 🕤 libssh2.dll | 155 | .6 KB 2018/3/20 |
| | 🗋 ncat.exe | 418 | .6 KB 2018/3/20 |
| | 🗋 ndiff.exe | 28.6 | KB 2018/3/20 |
| + | | 1.91 | KB 2018/3/17 |
| | | 选择文本类型: Nma | p XML格式 (.xml) |
| | | Canc | al Cava |

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
 - \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

| 📕 i 🖸 🛄 🖛 i | | 解壓縮 | Zyxel_USGCB.v1179 | | - 0 | × |
|---------------------------------------|-----------|-----------------------|-------------------|------------|------------|-----|
| 檔案 常用 共用 | 檢視 | 壓縮的資料夾工具 | | | | ~ (|
| ← · · ↑ | 下載 > Secu | rityTool.zip » Zyxel_ | USGCB.v1179 ∽ Ö | 搜尋 Zyxel_U | SGCB.v1179 | ,o |
| ^ | 名稱 | ^ | 類型 | 壓縮大小 | 受密碼保護 | 大小 |
| ★ 快速存取 | GCB-D | ATA | 福塞曾料本 | | | |
| 📥 OneDrive - Ur | GPO-E | ATA | 檔案資料夾 | | | |
| □ ★攤 | Uploa | dTemp | 檔案資料夾 | | | |
| ····································· | Tza.ex | e | 應用程式 | 294 KB | 否 | |
| | Config | .bin | BIN 檔案 | 1 KB | 杏 | |
| | IGPO. | exe | 應用程式 | 195 KB | Ka Ka | |
| 圓 文件 | Modif | yConfig.exe | 應用程式 | 68 KB | | |
| ♪ 音樂 | MSHFI | LXGD.OCX | ActiveX 控制項 | 175 KB | 否 | |
| 三 桌面 | MSINE | T.OCX | ActiveX 控制項 | 55 KB | 否 | |
| ■ 圖片 | USGCE | 3Tool.exe | 應用程式 | 69 KB | 否 | |
| 影片 | | | | | | |
| 🏪 Win10 (C:) | | | | | | |
| 🕳 900GB-Data | | | | | | |
| 📋 SDHC (G:) | | | | | | |
| DHC (G:) | | | | | | |
| | | | | | | F |



2) 新增上傳GPO組態資料

| ち 合勤USGCB組想 | 態檢測工具 | | | | × |
|----------------|-------------|--------|----|----|---------------|
| 新增上傳GPO組態 | 資料 2 | | | | |
| 已上傳GPO資 | 圣料記錄 | | | | 檢視上傳資料 |
| 編號 | 上傳日期 | 作業系統資訊 | 狀態 | 備註 | 接收收分析結果電郵 |
| × | | | | | * |
| | | | | | 版本: 1.0.1.413 |



3) 產生GPO紀錄中

| 合勤USGCB組 | 且態檢測工具 | | | | × |
|---|--------------------|--------|----------|-----|---------------|
| 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日 | <u>態資料</u> 容料記録 | | | | 檢視上傳資料 |
| 編號 | 上傳日期 | 作業系統資訊 | 狀態 備 | ilt | 接收收分析結果電郵 |
| | | - | | _ | |
| | | | 產生GPO紀錄中 | 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

| 5. 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* | | 1 |
| *必填欄位 | | 確定 取消 |

5) 勾選 "我同意"後・請按<確定>進行掃瞄

| and a second | 5. 联络资訊 | | Σ | 3 |
|------------------|---|----------------------------------|--|----------------|
| ZYXEL合動理網商專區 | 檢測公司資訊: | | 重填 | 1 |
| 合勤USGCB組態檢測程式 | 公司全名* | 公司電話 | 主要聯絡人 | 22 |
| 5 進行GCB掃瞄GPO組態資料 | ZYXEL 公司地址 | | | |
| 已進行GCB掃瞄GPO | 資料 日 確認上傳本機組態資訊 | | | 後視GCB掃瞄資料 |
| MA | ✓ <u>我同意</u> 合勤USGCB組 料,並將之傳述 檢視GPO組 | 態分析工具收集本機的(到組態分析中心做進一 態資料 | GPO(Group Policy Object)組態資 步分析。 確定 取消 | |
| ets | 存檔資料夾名稱* | - | | 版本: 1.2.0.1179 |
| .機IP | *必填欄位 | | 確定 取消 | Ĩ |
| ASIP | - | | (以行動) | |

6) 完成單台電腦掃瞄作業

| | 14 | | |
|-------------------|---|-----------------------------|--------|
| PolicyType | PolicyGroupOrRegisterKey | PolicySetting | Issue |
| HKLM | Software\Microsoft\Windows\CurrentVersion\Polic | ie FilterAdministratorToken | GCB001 |
| Security Template | Privilege Rights | SeNetworkLogonRight | GCB004 |
| Security Template | Privilege Rights | SeDenvNetworkLogonRight | 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 Project1 | 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 REAL | 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 | V ScreenSaverGracePeriod | GCB000 |
| HKLM | Software\Microsoft\Windows NT\CurrentVersion\W | V PasswordExpiryWarning | GCB000 |
| HKIM | Software\Microsoft\Windows NT\CurrentVersion\M | V Cachedl ogonsCount | GCB000 |



上傳資安掃瞄記錄檔 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

| ③ Aug 08, 20: 最新課程介紹 9月【合勤客戶 巡迴列車啟動 ◎ 11 / □ 4 | | | A REAL | | ① A 最詳 8月 巡迴 ② 2: | ug 07,2 新課程介 【合勤客 列車啟動 3 / 명 | 019 何服務 別 | | | |
|--|----|---|--------------|---|-------------------------------|--|-----------------|--------|----------------|----|
| | ~ | ~ | 庫 ~ | - | ~ | | ~ | > (III | 版 好! 員維護 |) |
| ムイズヒレ 合動短期商専區 | 網 | 息 | 識 | 頁 | 練 | V | | 專區 | CSO | 會員 |
| | 韌官 | 新 | 知 | 首 | 周訓 | 速訊 | 音專 | 員 | 町曹 | |
| | 合 | 最 | 網 | 影 | 教 | 最 | 影 | 會 | 親愛 | |



27



● 填寫基本資訊

◆ 填寫的檢測資訊·將列印在檢測報告的封面

| so | 健檢紀錄查詢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: | | | |
| | 012 70F (1) == 240 + 70 | | | |
| | *公司名稱: | | | |
| 〕 健檢記錄管理 | *統一編號: | *部門: | | |
| 國 報名課程 | 服務/檢測人員: | *公司電話: | | # |
| ② 資料修改 | | | | 暫存 下一步 |





| 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 | 是一百 |
| 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) 以供系統教援使用 | 是一百 |
| 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。

| 器上傳HC | R003_SCN4 | | |
|-------|--------------|--------------|-----------|
| | 基本資訊 | 問卷填寫 | 上傳掃描紀錄 |
| 一組網段 | | | |
| L | NMAP 掃瞄紀錄 | 選擇檔案 未選擇任何檔案 | 僅可上傳xml檔案 |
| | | 刪除 | |
| | Netscan 掃瞄紀錄 | 選擇檔案 未選擇任何檔案 | 僅可上傳xml檔案 |
| | | 刪除 | |
| | 主機IP | (以道 | 回號分隔) |
| | NASIP | (以超 | 国號分隔) |
| 二組網段 | | | |
| | NMAP 掃瞄紀錄 | 選擇檔案 未選擇任何檔案 | 僅可上傳xml檔案 |
| | | 删除 | |



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。

| in the second | |
|---|--|
| GCB掃描紀錄 | |
| 選擇檔案 未選擇任何檔案 | |
| 註1:僅可上傳Jsn檔案 | |
| 註2:可上傳多個檔案 | |

| 開啟 | ▼ 共用對象 ▼ 電子郵件 新増資料夾 | | | |
|----|---------------------------------|---------------|-------------------|-------|
| ^ | 名稱 | 修改日期 | 類型 | 大小 |
| | {7E01D4C2-E761-48F8-BD8D-656B6C | 2019/11/26下午 | 檔案資料夾 | |
| | GPOInfo.bin | 2019/11/26下午 | BIN 檔案 | 1 KB |
| | hotfix.html | 2019/11/26 下午 | Chrome HTML D | 1 KB |
| | hotfixes.htm | 2019/11/26 下午 | Chrome HTML D | 1 KB |
| | USGCB-20191126142752516.htm | 2019/11/26下午 | Chrome HTML D | 37 KB |
| - | USGCB-20191126142752516.jsn | 2019/11/26下午 | JSN 檔案 | 24 KB |
| - | SGCB-20191120142752516.xls | 2019/11/26下午 | Microsoft Excel 9 | 58 KB |



● 上傳網路拓樸圖





- 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 | |
| 網路拓枝 | 楼圖 |
| | |



ZYXEL Your Networking Ally