4MOSAn

掃瞄規範

開始時間：2026/06/29 11:25:55
結束時間：2026/06/29 11:38:25
耗費時間：00:12:30
弱點評估版本： 5.1.5.3
弱點更新日期： 2026-06-23
政策：Default
報表產生：2026/06/29 11:41:27

主機探測摘要

IP 位址	主機名稱	作業系統	MAC / 閘道	稽核
192.168.1.60	www.yantech.com.tw	Ubuntu Linux	192.168.3.254	5
192.168.1.61	itdb.yantech.com.tw	Ubuntu Linux	192.168.3.254	7
192.168.1.62	book.yantech.com.tw	Ubuntu Linux	192.168.3.254	7
192.168.1.200	192.168.1.200	NAS4Free (FreeBSD 10.2-RELEASE) (93%), FreeBSD 7.0-RELEASE (92%), FreeBSD 7.1-PRERELEASE 7.2-STABLE (92%), FreeBSD 9.0-RELEASE - 10.3-RELEASE (91%), FreeBSD 8.0-RELEASE (91%), FreeBSD 8.1-RELEASE (91%), FreeBSD 8.2-RELEASE (90%), VMware ESXi 4.1.0 (89%), FreeBSD 7.1-RELEASE (89%), IBM AIX 7.1 (89%)	192.168.3.254	5
192.168.1.211	dns.yantech.com.tw	(JUST GUESSING): OpenBSD 4.X (85%), Linux 3.X (85%)	192.168.3.254	8
192.168.1.212	yantech.com.tw	Linux 3.X|4.X	0.0.0.0	13
192.168.1.215	192.168.1.215	Windows Server 2016 Standard 14393	192.168.3.254	1
主機統計: 總數=7, 存在=7, 不存在=0				

PCI 符合性報告

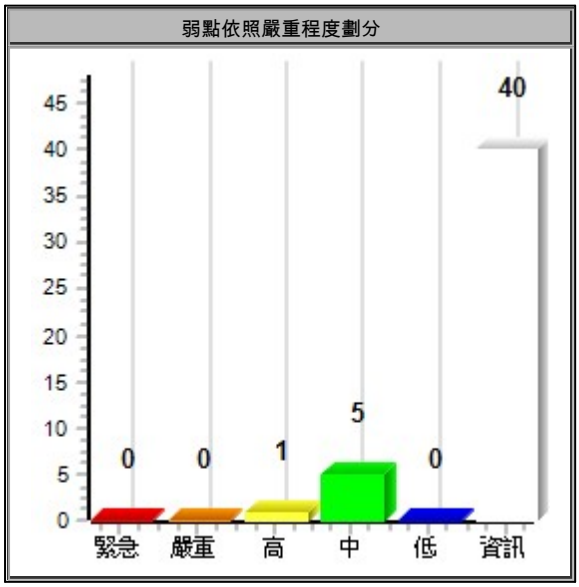
下列表格中標示出整體的法規遵循狀態以及個別系統的法規遵循狀態

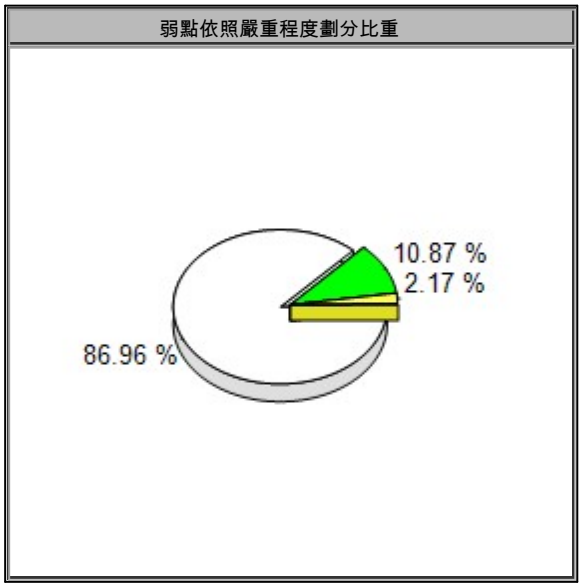
IP 位址	主機名稱	等級 1	等級 2	等級 3	等級 4	等級 5	PCI 法規遵循
192.168.1.60	www.yantech.com.tw	0	0	0	0	0	合格
192.168.1.61	itdb.yantech.com.tw	0	0	0	0	0	合格
192.168.1.62	book.yantech.com.tw	0	2	0	0	0	合格
192.168.1.200	192.168.1.200	0	0	0	0	0	合格
192.168.1.211	dns.yantech.com.tw	0	3	1	0	0	不合格
192.168.1.212	yantech.com.tw	0	0	0	0	0	合格
192.168.1.215	192.168.1.215	0	0	0	0	0	合格
總數		0	5	1	0	0	不合格

嚴重性層級	風險
5	緊急
4	嚴重
3	高
2	中
1	低

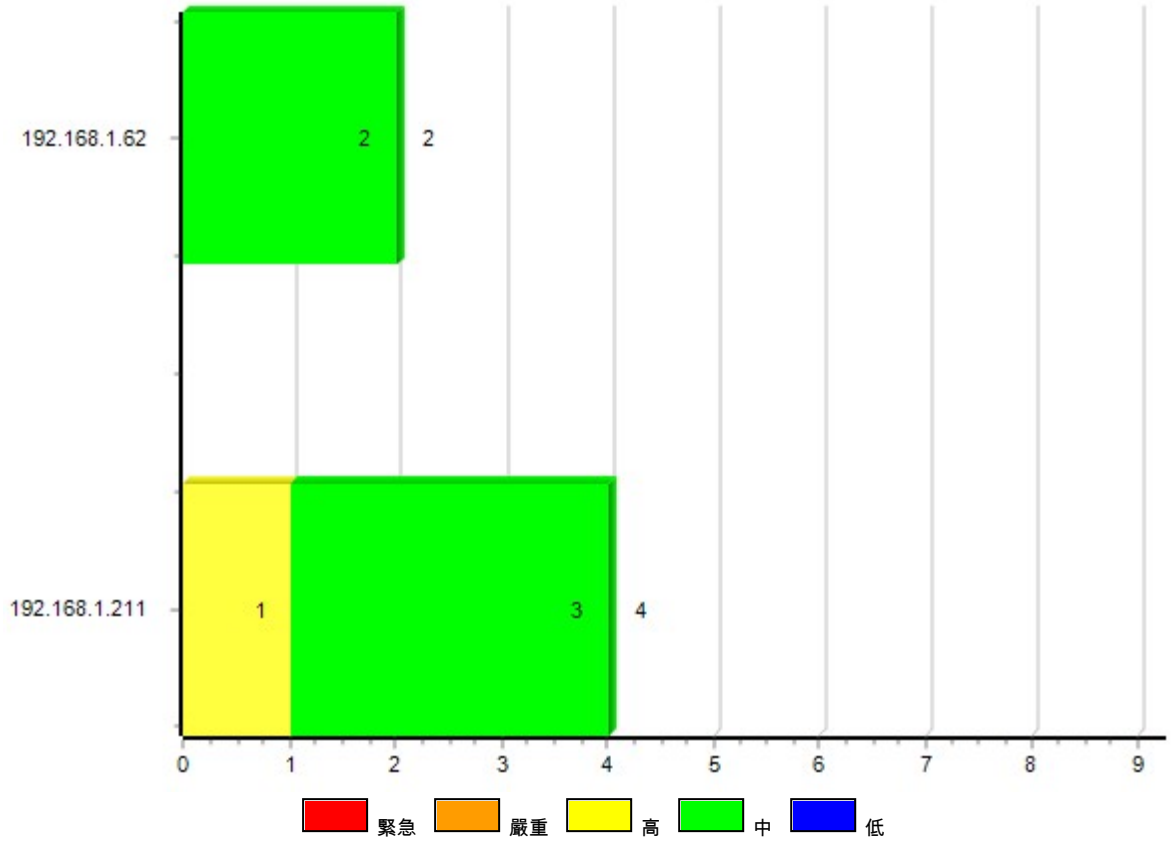
整體的 **PCI** 法規遵循狀態 = 不合格

整體安全風險數量與分佈

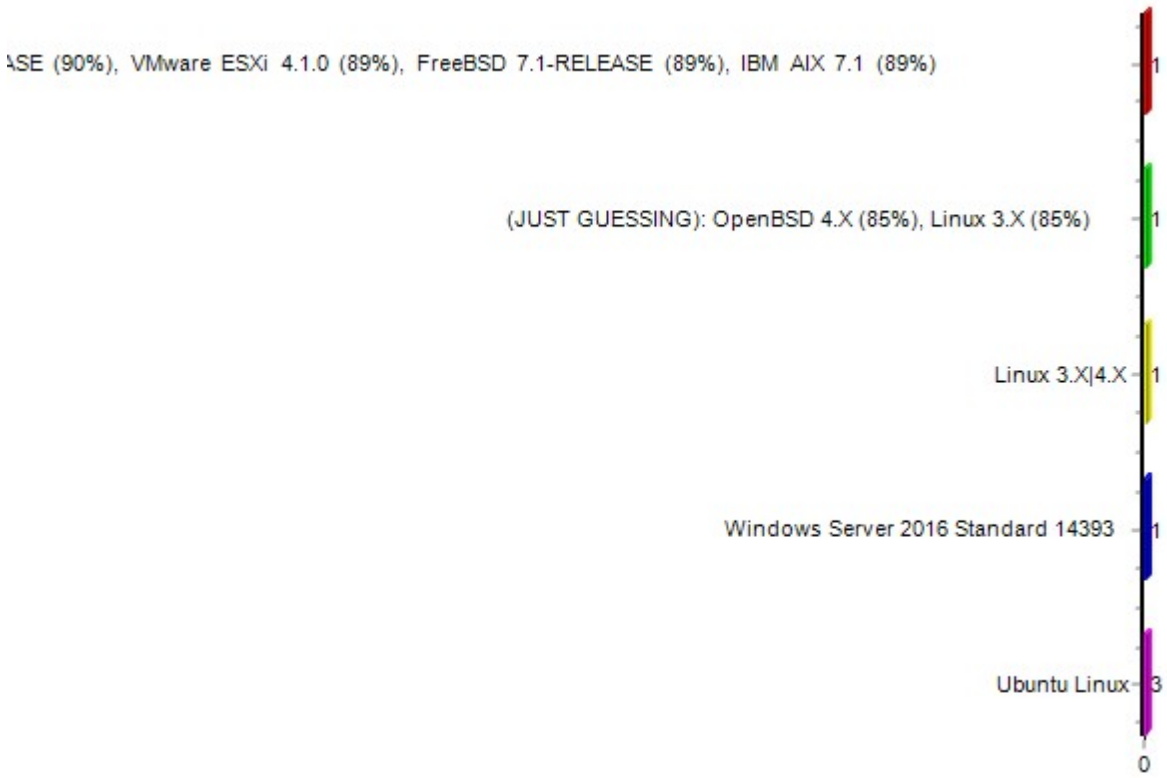




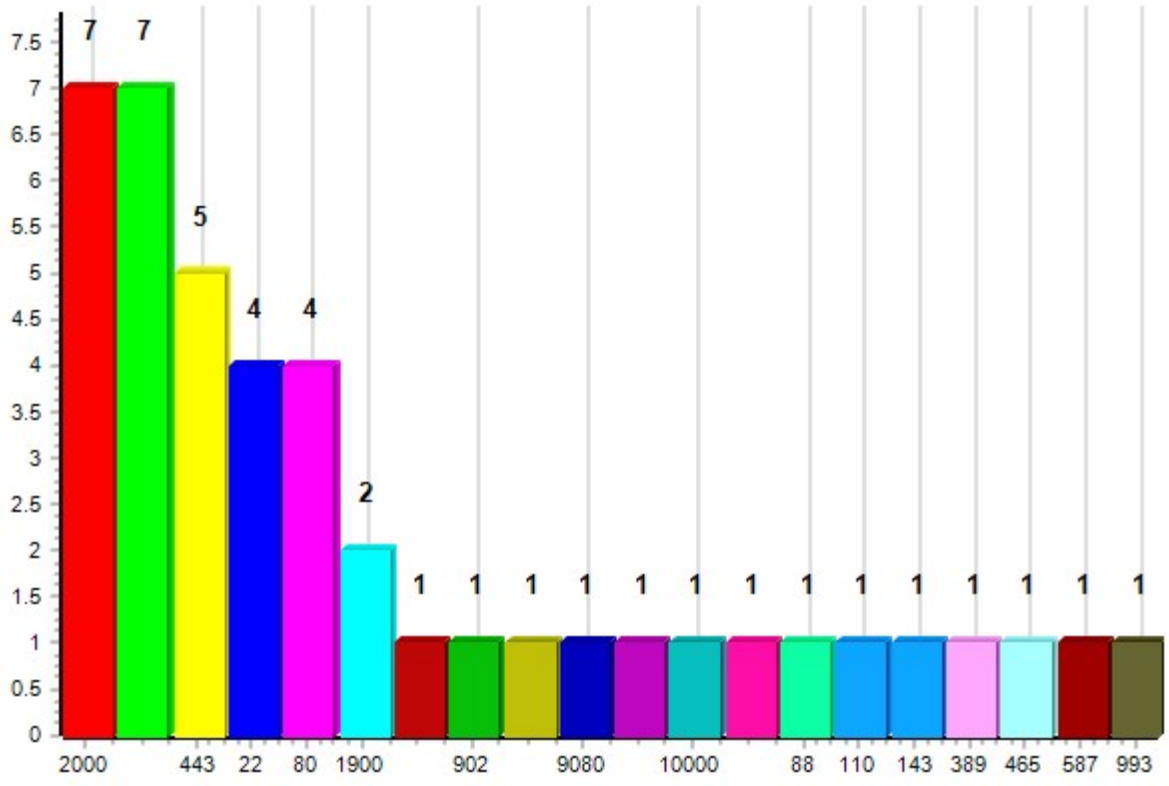
前 20 名高風險主機分佈



作業系統分佈統計圖



前 20 名網路服務統計



前 20 名弱點數量分佈

數量	嚴重性	名稱
1	高	**ISC BIND 9.20.22** 之前版本多個弱點 *192.168.1.211*
1	中	**Apache HTTP Server 2.4.68** 之前版本多個弱點 *192.168.1.62*
1	中	**ISC BIND 9** 遠端快取中毒弱點 *192.168.1.211*
1	中	**DNS** 伺服器 **Recursion** 查詢快取毒害弱點 *192.168.1.211*
1	中	**DNS** 快取刺探弱點 *192.168.1.211*
6	資訊	偵測到 **Web Server HTTP Protocol Version** *192.168.1.60, 192.168.1.61, 192.168.1.62, 192.168.1.200, 192.168.1.211, 192.168.1.212*
5	資訊	偵測到隱藏 **WWW** 伺服器名稱 *192.168.1.60, 192.168.1.61, 192.168.1.62, 192.168.1.211, 192.168.1.212*
5	資訊	偵測到 **SSL Server** 資訊 *192.168.1.60, 192.168.1.61, 192.168.1.62, 192.168.1.212, 192.168.1.215*
4	資訊	偵測到 **Web** 伺服器重新導向 *192.168.1.61, 192.168.1.200, 192.168.1.211, 192.168.1.212*
1	資訊	**VMware Server** 認證程序 *192.168.1.200*
1	資訊	網站目錄偵測 *192.168.1.200*
1	資訊	**DNS** 伺服器版本資訊 *192.168.1.211*
1	資訊	偵測到 **IMAP4** 伺服器 *192.168.1.212*
1	資訊	偵測到 **SMTP** 伺服器 *192.168.1.212*
1	資訊	偵測到 **TLS Version 1.0** 通訊協定 *192.168.1.212*

192.168.1.60 : www.yantech.com.tw

開始時間: 2026/6/29 上午 11:25:55 - 2026/6/29 上午 11:38:25
作業系統: Ubuntu Linux
CPE: cpe:/o:linux
MAC / 閘道: 192.168.3.254
嚴重性層級 : 等級 0 (資訊)

稽核(5)

偵測到 **Web Server HTTP Protocol Version**	等級 **0** (資訊)
內容描述	透過 Web 伺服器從主機獲得 HTTP 通訊協定版本。
修補建議	確認 Web 伺服器符合組織的原則。
系統回應 : HTTP/1.1	

偵測到 **Web Server HTTP Protocol Version : 443**	等級 **0** (資訊)
系統回應 : HTTP/1.1	

偵測到隱藏 **WWW** 伺服器名稱	等級 **0** (資訊)
內容描述	偵測到隱藏 WWW 伺服器名稱。
修補建議	確認 Web 伺服器符合組織的原則。WWW 伺服器為電腦應用程式，可透過 HTTP 提供 web 型內容。偵測到隱藏 WWW 伺服器名稱。為了安全考量，可隱藏 Web 伺服器名稱。
系統回應 : Apache	

偵測到隱藏 **WWW** 伺服器名稱 **: 443**	等級 **0** (資訊)
系統回應 : Apache	

偵測到 **SSL Server** 資訊 **: 443**	等級 **0** (資訊)
內容描述	在主機上偵測到 SSL 伺服器資訊。
修補建議	確認 SSL 伺服器的協定以及加密方法符合公司原則。
Protocol: TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3	
Cipher: TLS_1_2_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 : Recommended TLS_1_2_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 : Recommended TLS_1_2_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 : Recommended TLS_1_3_AES_128_GCM_SHA256 : Recommended TLS_1_3_AES_256_GCM_SHA384 : Recommended TLS_1_3_CHACHA20_POLY1305_SHA256 : Recommended	

通訊埠(5)

通訊埠	內容描述	類型	稽核	風險
22	The Secure Shell (SSH) Protocol	TCP	0	資訊
SSH-2.0-OpenSSH_10.0p2 Debian-7+deb13u4				
80	World Wide Web HTTP	TCP	2	資訊
HTTP/1.1 200 OK Date: Mon, 29 Jun 2026 03:27:56 GMT Server: Apache X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN Content-Security-Policy: frame-ancestors 'self' Set-Cookie: PHPSESSID=6cd08ae23faa775aa63078d7300d0459; expires=Tue, 30 Jun 2026 03:27:56 GMT; Max-Age=86400; path=/; secure; HttpOnly Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Vary: Accept-Encoding Connection: close Content-Type: text/html; charset=UTF-8Server: Apache				
443	http protocol over TLS/SSL	TCP	3	資訊
HTTP/1.1 200 OK Date: Mon, 29 Jun 2026 03:33:46 GMT Server: Apache X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN Content-Security-Policy: frame-ancestors 'self' Set-Cookie: PHPSESSID=72773b0a60110e1d298ad77696e9a875; expires=Tue, 30 Jun 2026 03:33:46 GMT; Max-Age=86400; path=/; secure; HttpOnly Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Vary: Accept-Encoding Connection: close Content-Type: text/html; charset=UTF-8Server: Apache				
2000	Cisco SCCP	TCP	0	資訊
5060	SIP	TCP	0	資訊

192.168.1.61 : itdb.yantech.com.tw

開始時間: 2026/6/29 上午 11:25:56 - 2026/6/29 上午 11:38:25
作業系統: Ubuntu Linux
CPE: cpe:/o:linux
MAC / 閘道: 192.168.3.254
嚴重性層級 : 等級 0 (資訊)

稽核(7)

偵測到 **Web Server HTTP Protocol Version**	等級 **0** (資訊)
內容描述	透過 Web 伺服器從主機獲得 HTTP 通訊協定版本。
修補建議	確認 Web 伺服器符合組織的原則。
系統回應 : HTTP/1.1	

偵測到 **Web Server HTTP Protocol Version : 443**	等級 **0** (資訊)
系統回應 : HTTP/1.1	

偵測到隱藏 **WWW** 伺服器名稱	等級 **0** (資訊)
內容描述	偵測到隱藏 WWW 伺服器名稱。
修補建議	確認 Web 伺服器符合組織的原則。WWW 伺服器為電腦應用程式，可透過 HTTP 提供 web 型內容。偵測到隱藏 WWW 伺服器名稱。為了安全考量，可隱藏 Web 伺服器名稱。
系統回應 : Apache	

偵測到隱藏 **WWW** 伺服器名稱 **: 443**	等級 **0** (資訊)
系統回應 : Apache	

偵測到 **Web** 伺服器重新導向	等級 **0** (資訊)
內容描述	在主機上偵測到 Web 伺服器重新導向狀態。
修補建議	確認 Web 伺服器符合組織的原則。Web 伺服器可廣泛在用戶端瀏覽器上提供動態和靜態內容。在主機上偵測到 Web 伺服器重新導向狀態。
系統回應 : 302	

偵測到 **Web** 伺服器重新導向 **: 443**	等級 **0** (資訊)
系統回應 : 302	

偵測到 **SSL Server** 資訊 **: 443**	等級 **0** (資訊)
內容描述	在主機上偵測到 SSL 伺服器資訊。
修補建議	確認 SSL 伺服器的協定以及加密方法符合公司原則。
Protocol: TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3	
Cipher: TLS_1_2_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 : Recommended TLS_1_2_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 : Recommended TLS_1_2_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 : Recommended TLS_1_3_AES_128_GCM_SHA256 : Recommended TLS_1_3_AES_256_GCM_SHA384 : Recommended TLS_1_3_CHACHA20_POLY1305_SHA256 : Recommended	

通訊埠(5)

通訊埠	內容描述	類型	稽核	風險
22	The Secure Shell (SSH) Protocol	TCP	0	資訊
SSH-2.0-OpenSSH_10.0p2 Debian-7+deb13u4				
80	World Wide Web HTTP	TCP	3	資訊
HTTP/1.1 302 Found Date: Mon, 29 Jun 2026 03:27:56 GMT Server: Apache X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block location: /changtax/ Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8Server: Apache				
443	http protocol over TLS/SSL	TCP	4	資訊
HTTP/1.1 302 Found Date: Mon, 29 Jun 2026 03:33:46 GMT Server: Apache X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block location: /changtax/ Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8Server: Apache				
2000	Cisco SCCP	TCP	0	資訊
5060	SIP	TCP	0	資訊

192.168.1.62 : book.yantech.com.tw

開始時間: 2026/6/29 上午 11:25:56 - 2026/6/29 上午 11:37:30

作業系統: Ubuntu Linux

CPE: cpe:/o:linux

MAC / 閘道: 192.168.3.254

嚴重性層級 : 等級 2 (中)

稽核(7)

Apache HTTP Server 2.4.68 之前版本多個弱點		等級 **2** (中)
內容描述	Apache HTTP Server 在 v2.4.68 之前的版本存在多個安全問題.	
修補建議	升級到 2.4.68 最新版本的 Apache. http://httpd.apache.org/download.cgi	
影響	**(C)**機密性: 無, **(I)**完整性: 部分, **(A)**可用性: 無	
CVSS v2	4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)	**CVE 編號: CVE-2026-49975**
相關連結	. CONFIRM: Apache HTTP Server 2.4.67 Released http://httpd.apache.org/security/vulnerabilities_24.html	
系統回應 : Apache/2.4.66 (Ubuntu)		

Apache HTTP Server 2.4.68 之前版本多個弱點 **: 443**	等級 **2** (中)
系統回應 : Apache/2.4.66 (Ubuntu)	

偵測到 **Web Server HTTP Protocol Version**		等級 **0** (資訊)
內容描述	透過 Web 伺服器從主機獲得 HTTP 通訊協定版本。	
修補建議	確認 Web 伺服器符合組織的原則。	
系統回應 : HTTP/1.1		

偵測到 **Web Server HTTP Protocol Version : 443**	等級 **0** (資訊)
系統回應 : HTTP/1.1	

偵測到隱藏 **WWW** 伺服器名稱		等級 **0** (資訊)
內容描述	偵測到隱藏 WWW 伺服器名稱。	
修補建議	確認 Web 伺服器符合組織的原則。WWW 伺服器為電腦應用程式，可透過 HTTP 提供 web 型內容。偵測到隱藏 WWW 伺服器名稱。為了安全考量，可隱藏 Web 伺服器名稱。	
系統回應 : Apache/2.4.66 (Ubuntu)		

偵測到隱藏 **WWW** 伺服器名稱 **: 443**	等級 **0** (資訊)
系統回應 : Apache/2.4.66 (Ubuntu)	

偵測到 **SSL Server** 資訊 **: 443**		等級 **0** (資訊)
內容描述	在主機上偵測到 SSL 伺服器資訊。	
修補建議	確認 SSL 伺服器的協定以及加密方法符合公司原則。	
Protocol: TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3		
Cipher: TLS_1_2_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 : Recommended TLS_1_2_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 : Recommended TLS_1_2_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 : Recommended TLS_1_3_AES_128_GCM_SHA256 : Recommended TLS_1_3_AES_256_GCM_SHA384 : Recommended TLS_1_3_CHACHA20_POLY1305_SHA256 : Recommended		

通訊埠(6)

通訊埠	內容描述	類型	稽核	風險
22	The Secure Shell (SSH) Protocol	TCP	0	資訊
SSH-2.0-OpenSSH_10.2p1 Ubuntu-2ubuntu3.2				
80	World Wide Web HTTP	TCP	3	中
HTTP/1.1 200 OK Date: Mon, 29 Jun 2026 03:26:48 GMT Server: Apache/2.4.66 (Ubuntu) Cache-Control: no-cache, no-store, private pragma: no-cache Expires: Sun, 12 Jul 2015 19:01:00 GMT Content-Security-Policy: frame-ancestors 'self'; frame-src 'self' https://*.draw.io https://*.youtube.com https://*.youtube-nocookie.com https://*.vimeo.com https://embed.diagrams.net; script-src http: https: 'nonce-SymCXJopYA7YgYztaWJTNcge' 'strict-dynamic'; style-src 'self' 'unsafe-inline' http: https:; img-src 'self' data: blob: http: https:; object-src 'self'; base-uri 'self' Set-Cookie: XSRF-TOKEN=eyJpdiI6ImhXT0VOWWIrZGx3Sk5XVTNmejBQYUE9PSIsInZhbHVlIjoiN1BiTHU3TzJRbWhBdElKTFQ4R0hhY3lVdFUvMFR0aFBmZ0ZhTnlxcVMvRXpRSlF4WmxYTCtmTGZEUm1aWlNIV0VHbDlyRDgrK0g5bHJWbUVmK0xCSmFGQnR0djJkYXYybjNJK3dja1luME1BV3J6Z3JsOU5rRUxOWGV4TE5sbTkiLCJtYWMiOiIyNjNlNGExMDY2MGU2ZjcyNDM5N2IzZGQzNmYyMjNhZmIzMDZlYmE2ZTUwNzk2YzU4NjhjZDY4ZjNjMWU5NjJlIiwidGFnIjoiIn0%3D; expires=Mon, 29 Jun 2026 05:26:48 GMT; Max-Age=7200; path=/; secure; samesite=lax Set-Cookie: bookstack_session=eyJpdiI6ImhBQ1BDdWoyczFLUXhYMUZwdWVwSnc9PSIsInZhbHVlIjoia0VpMnBDWmhhSG4xaVR0b2JpTnoxbmdrMEFUL0tXcmJqcE9nV2JCYUdGaER6d0hlUWE1MUFVSzlKczk2VWhyazl2aElQTHozREZLeGwzNEFOYk5neVYrMHRzZGJ0WnpUUjU2YTNFQ2ZmZm1OZ1FDRjBvWUExSlRvdmFUdG4zMFgiLCJtYWMiOiIxYzVjMGI0NDNlMmRkOGRjZmFiOWI0M2ZiNjllYTkwMDY1YTlmYmU4N2U1ZmJlNDE1NDQ5MDk1MzNmMTlmOTc2IiwidGFnIjoiIn0%3D; expires=Mon, 29 Jun 2026 05:26:48 GMT; Max-Age=7200; path=/; secure; httponly; samesite=lax Vary: Accept-Encoding Connection: close Content-Type: text/html; charset=utf-8Server: Apache/2.4.66 (Ubuntu) Allow: GET,HEAD				
443	http protocol over TLS/SSL	TCP	4	中
HTTP/1.1 200 OK Date: Mon, 29 Jun 2026 03:32:46 GMT Server: Apache/2.4.66 (Ubuntu) Cache-Control: no-cache, no-store, private pragma: no-cache Expires: Sun, 12 Jul 2015 19:01:00 GMT Content-Security-Policy: frame-ancestors 'self'; frame-src 'self' https://*.draw.io https://*.youtube.com https://*.youtube-nocookie.com https://*.vimeo.com https://embed.diagrams.net; script-src http: https: 'nonce-7ljnrBKfpD4Gpg9vhtKeqGVG' 'strict-dynamic'; style-src 'self' 'unsafe-inline' http: https:; img-src 'self' data: blob: http: https:; object-src 'self'; base-uri 'self' Set-Cookie: XSRF-TOKEN=eyJpdiI6InlleE9uYkptOGpqTm9Ba0xrc3pBaWc9PSIsInZhbHVlIjoiT2JLWGtZOGRFV25DdUhjUklSYnJBbUt5SWlxdFBkeVE2dHQvUllzMnZkMjczVTJwMmdlaGJPRFp4WlJIcGtTRkFENHI1ZUFZR0Q2ekVkM243NGtMZ2pzUDdBeXgzenlpdEp1azllSEJHcDFiYjRBZERjM3BVSTBoRXBVeDdSdWQiLCJtYWMiOiIwYTg1Y2QyZDBiZDAwNTRlZDdhYjQyNmRmNzFiZmFjMTExM2FiNjVlYTY3MWJjZmI5NWJjNzk5MjcyN2M1M2FiIiwidGFnIjoiIn0%3D; expires=Mon, 29 Jun 2026 05:32:46 GMT; Max-Age=7200; path=/; secure; samesite=lax Set-Cookie: bookstack_session=eyJpdiI6IjM3SWEyWk84YjFCcDRXdi9GWmtaYnc9PSIsInZhbHVlIjoiMC83emc5c0xzNUx2Y1g2K2YwaDIzOGhxZHFaVkxQQ2ovVzdNb2FNaEVueGtBT2lEU25pRHZzdElkMVVRa3FBRzI1N1hMNWU2SEs2SVhaeTVBenNsYXNPYjk1N3BRZHhSWjg5eU9KQUFsS2ZrVFhPYi9FbklBUkZ0eWtsZEFKMEliLCJtYWMiOiIyNThhNjM5YTE3YjhiNTc2NzcxYjY0YWEyZGE4NzE3MTllNDBkOGVjOGNmN2YzNTMyYzM5MTkxMWU3YWM5ZTJjIiwidGFnIjoiIn0%3D; expires=Mon, 29 Jun 2026 05:32:46 GMT; Max-Age=7200; path=/; secure; httponly; samesite=lax Vary: Accept-Encoding Connection: close Content-Type: text/html; charset=utf-8Server: Apache/2.4.66 (Ubuntu) Allow: GET,HEAD				
1900	SSDP	UDP	0	資訊
2000	Cisco SCCP	TCP	0	資訊
5060	SIP	TCP	0	資訊

192.168.1.200 : 192.168.1.200

開始時間: 2026/6/29 上午 11:25:56 - 2026/6/29 上午 11:37:44

作業系統: NAS4Free (FreeBSD 10.2-RELEASE) (93%), FreeBSD 7.0-RELEASE (92%), FreeBSD 7.1-PRERELEASE 7.2-STABLE (92%), FreeBSD 9.0-RELEASE - 10.3-RELEASE (91%), FreeBSD 8.0-RELEASE (91%), FreeBSD 8.1-RELEASE (91%), FreeBSD 8.2-RELEASE (90%), VMware ESXi 4.1.0 (89%), FreeBSD 7.1-RELEASE (89%), IBM AIX 7.1 (89%)

CPE: cpe:/o:freebsd

MAC / 閘道: 192.168.3.254

嚴重性層級 : 等級 0 (資訊)

稽核(5)

VMware Server 認證程序	等級 **0** (資訊)
內容描述	偵測到 VMware Server 認證程序.
修補建議	如果使用VMware Server是不符合你的系統政策，考慮解除安裝 VMware服務器。
相關連結	. VMWare Homepage http://www.vmware.com/

網站目錄偵測 : 443	等級 **0** (資訊)
內容描述	網站目錄偵測
修補建議	確認目錄內不包含敏感資訊.
相關連結	. OWASP OTG-CRYPST-007 https://www.owasp.org/index.php/Testing_for_Sensitive_information_sent_via_unencrypted_channels_%28OTG-CRYPST-007%29
Directory 1: http://192.168.1.200:443/ui/	

偵測到 **Web Server HTTP Protocol Version**	等級 **0** (資訊)
內容描述	透過 Web 伺服器從主機獲得 HTTP 通訊協定版本。
修補建議	確認 Web 伺服器符合組織的原則。
系統回應 : HTTP/1.1	

偵測到 **Web Server HTTP Protocol Version : 443**	等級 **0** (資訊)
系統回應 : HTTP/1.1	

偵測到 **Web** 伺服器重新導向	等級 **0** (資訊)
內容描述	在主機上偵測到 Web 伺服器重新導向狀態。
修補建議	確認 Web 伺服器符合組織的原則。Web 伺服器可廣泛在用戶端瀏覽器上提供動態和靜態內容。在主機上偵測到 Web 伺服器重新導向狀態。
系統回應 : 301	

通訊埠(8)

通訊埠	內容描述	類型	稽核	風險
80	World Wide Web HTTP	TCP	2	資訊
HTTP/1.1 301 Moved Permanently Date: Mon, 29 Jun 2026 03:23:35 GMT Location: https://192.168.1.200/ Connection: close Content-Type: text/html Content-Length: 56				
427	Server Location	TCP	0	資訊
443	http protocol over TLS/SSL	TCP	2	資訊
HTTP/1.1 200 OK Date: Mon, 29 Jun 2026 03:28:21 GMT Connection: close Content-Security-Policy: block-all-mixed-content Content-Type: text/html Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff X-Frame-Options: DENY X-XSS-Protection: 1 Content-Length: 258				
902	VMware Authentication Daemon	TCP	1	資訊
220 VMware Authentication Daemon Version 1.10: SSL Required, ServerDaemonProtocol:SOAP, MKSDisplayProtocol:VNC , VMXARGS supported, NFCSSL supported/t				
2000	Cisco SCCP	TCP	0	資訊
5060	SIP	TCP	0	資訊
8000	iRDMI	TCP	0	資訊
9080	Groove GLRPC	TCP	0	資訊

192.168.1.211 : dns.yantech.com.tw

開始時間: 2026/6/29 上午 11:25:56 - 2026/6/29 上午 11:27:22

作業系統: (JUST GUESSING): OpenBSD 4.X (85%), Linux 3.X (85%)

CPE: cpe:/o:openbsd:openbsd:4.0 cpe:/o:linux:linux_kernel:3.18

MAC / 閘道: 192.168.3.254

嚴重性層級 : 等級 3 (高)

稽核(8)

ISC BIND 9.20.22 之前版本多個弱點		等級 **3** (高)
內容描述	ISC BIND 9.20.0 - 9.20.20 版本存在多個安全弱點.	
修補建議	參考 ISC BIND，升級到最新版本。 http://www.isc.org/downloads/all	
影響	**(C)**機密性**:** 無, **(I)**完整性**:** 無, **(A)**可用性**:** 完全	
CVSS v2	7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)	**CVE** 編號**:** **CVE-2026-3104**
相關連結	. CVE-2026-3104: Memory leak in code preparing DNSSEC proofs of non-existence https://kb.isc.org/docs/cve-2026-3104	
系統回應 : 9.20.18-1ubuntu2.1-Ubuntu		

ISC BIND 9 遠端快取中毒弱點		等級 **2** (中)
內容描述	ISC BIND 9 一直到 9.5.0a5 的版本使用脆弱的隨機數字產生器，當查詢時發送傳出訊息產生可預測的 DNS 查詢識別碼，如 NOTIFY 回答問題時作為解析器，它允許遠端攻擊者通過 DNS 快取毒害。	
修補建議	參考 ISC BIND9，升級到最新版本。	
影響	**(C)**機密性**:** 無, **(I)**完整性**:** 部分, **(A)**可用性**:** 無	
CVSS v2	4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)	**CVE** 編號**:** **CVE-2007-2926**
相關連結	. CERT: TA07-319A http://www.us-cert.gov/cas/techalerts/TA07-319A.html . CERT-VN: VU#252735 http://www.kb.cert.org/vuls/id/252735 . VUPEN: ADV-2007-2627 http://www.frsirt.com/english/advisories/2007/2627 . CONFIRM: http://www.isc.org/index.pl/sw/bind/bind-security.php http://www.isc.org/index.pl/sw/bind/bind-security.php . SECUNIA: 26152 http://secunia.com/advisories/26152 . HP: SSRT071449 http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jspobjectID=c01123426	
系統回應 : 9.20.18-1ubuntu2.1-Ubuntu		

DNS 伺服器 Recursion 查詢快取毒害弱點		等級 2 (中)
內容描述	在目標主機上偵測到 DNS, 並已啟用 Recursion 選項. 這可以允許查詢第三方的主機名稱. 如果這是內部網路或是只提供授信任的網路查詢的名稱伺服器, 應該限制存取. 避免攻擊者送出大量 UDP 封包造成阻斷服務, 或者成為攻擊者的跳板. (如果是允許公開查詢的 DNS 則可排除此弱點)	
修補建議	此弱點為組態設定問題, 不需要修補程式. 應該限制只有 LAN 內部網路或信任的網路才可以查詢此名稱伺服器. 如果是 bind 8, 可以在 named.conf 設定 'allow-recursion'. 如果是 bind 9, 可以使用 'acl' 命令設定內部網路的位址. 如果是 Windows Server, 可以使用 "系統管理工具" - "DNS" - 按右鍵點選 "內容", 勾選 "停用遞迴", 按 "確定"	
影響	(C)機密性: 無, (I)完整性: 部分, (A)可用性: 無	
CVSS v2	5 (AV:N/AC:L/Au:N/C:N/I:P/A:N)	CVE 編號: CVE-1999-0024
相關連結	. InfoSec Handlers Diary Blog - DNS queries for https://isc.sans.edu/diary/DNS+queries+for+/5713 . BIND 9 Administrator Reference Manual https://www.isc.org/bind-9-11-arm/	
系統回應 : \x07\xDE\xAD\x81\x80\x00\x01\x00\x02\x00\x00\x00\x00\x03\x77\x77 \x77\x09\x77\x69\x6B\x69\x70\x65\x64\x69\x61\x03\x6F\x72\x67\x00 \x00\x01\x00\x01\xC0\x0C\x00\x05\x00\x01\x00\x01\x21\x58\x00\x11 \x04\x64\x79\x6E\x61\x09\x77\x69\x6B\x69\x6D\x65\x64\x69\x61\xC0 \x1A\xC0\x2F\x00\x01\x00\x01\x00\x00\x00\x18\x00\x04\x67\x66\xA6		

DNS 快取刺探弱點		等級 2 (中)
內容描述	在目標主機上偵測到 DNS, 並已啟用 Cache 選項. 攻擊者可以進行快取刺探弱點. (如果組態已經正確設定, 而且檢測來源 IP 是來自內部網路或信任的網路, 則可排除此弱點)	
修補建議	此弱點為組態設定問題, 不需要修補程式. 應該限制只有 LAN 內部網路或信任的網路才可以允許快取. (或取消快取) 如果是 bind 8, 可以在 named.conf 設定 'allow-query-cache'. 如果是 bind 9, 可以使用 'acl' 命令設定內部網路的位址. 如果是 Windows Server, 可以使用 "系統管理工具" - "DNS" - 按右鍵點選 "內容", 勾選 "保護快取以防侵害", 按 "確定"	
影響	(C)機密性: 無, (I)完整性: 部分, (A)可用性: 無	
CVSS v2	5 (AV:N/AC:L/Au:N/C:N/I:P/A:N)	CVE 編號:
相關連結	. What is DNS Cache snooping https://kb.isc.org/article/AA-00509/0/What-is-DNS-Cache-snooping.html . Microsoft DNS Server vulnerability to DNS Server Cache snooping attacks https://support.microsoft.com/zh-tw/kb/2678371 . Paper http://cs.unc.edu/~fabian/course_papers/cache_snooping.pdf	
recursive: \x07\x00\x4A\x81\x80\x00\x01\x00\x02\x00\x00\x00\x00\x03\x77\x77 \x77\x09\x77\x69\x6B\x69\x70\x65\x64\x69\x61\x03\x6F\x72\x67\x00 \x00\x01\x00\x01\xC0\x0C\x00\x05\x00\x01\x00\x01\x21\x58\x00\x11 \x04\x64\x79\x6E\x61\x09\x77\x69\x6B\x69\x6D\x65\x64\x69\x61\xC0 \x1A\xC0\x2F\x00\x01\x00\x01\x00\x00\x00\x18\x00\x04\x67\x66\xA6		
non-recursive: \x07\xFA\xB5\x80\x80\x00\x01\x00\x02\x00\x00\x00\x00\x03\x77\x77 \x77\x09\x77\x69\x6B\x69\x70\x65\x64\x69\x61\x03\x6F\x72\x67\x00 \x00\x01\x00\x01\xC0\x0C\x00\x05\x00\x01\x00\x01\x21\x58\x00\x11 \x04\x64\x79\x6E\x61\x09\x77\x69\x6B\x69\x6D\x65\x64\x69\x61\xC0 \x1A\xC0\x2F\x00\x01\x00\x01\x00\x00\x00\x18\x00\x04\x67\x66\xA6		

偵測到 Web Server HTTP Protocol Version : 10000		等級 0 (資訊)
內容描述	透過 Web 伺服器從主機獲得 HTTP 通訊協定版本。	
修補建議	確認 Web 伺服器符合組織的原則。	
系統回應 : HTTP/1.0		

偵測到隱藏 WWW 伺服器名稱 : 10000		等級 0 (資訊)
內容描述	偵測到隱藏 WWW 伺服器名稱。	
修補建議	確認 Web 伺服器符合組織的原則。WWW 伺服器為電腦應用程式，可透過 HTTP 提供 web 型內容。偵測到隱藏 WWW 伺服器名稱。為了安全考量，可隱藏 Web 伺服器名稱。	
系統回應 : MiniServ		

偵測到 **Web** 伺服器重新導向：**10000**	等級 **0**  **(資訊)**
內容描述	在主機上偵測到 Web 伺服器重新導向狀態。
修補建議	確認 Web 伺服器符合組織的原則。Web 伺服器可廣泛在用戶端瀏覽器上提供動態和靜態內容。在主機上偵測到 Web 伺服器重新導向狀態。
系統回應 ：302	

DNS 伺服器版本資訊	等級 **0**  **(資訊)**
內容描述	在目標主機上偵測到 DNS，並已取得其版本資訊。
修補建議	確認 DNS 設定符合貴公司的原則。
系統回應 ：9.20.18-1ubuntu2.1-Ubuntu	

通訊埠(6)

通訊埠	內容描述	類型	稽核	風險
22	The Secure Shell (SSH) Protocol	TCP	0	資訊
SSH-2.0-OpenSSH_10.2p1 Ubuntu-2ubuntu3.2				
53	Domain Name Server	TCP	5	高
version.bind: 9.20.18-1ubuntu2.1-Ubuntu				
1900	SSDP	UDP	0	資訊
2000	Cisco SCCP	TCP	0	資訊
5060	SIP	TCP	0	資訊
10000	Network Data Management Protocol	TCP	3	資訊
HTTP/1.0 302 Moved Temporarily Date: Mon, 29 Jun 2026 03:27:01 GMT Server: MiniServ Location: https://192.168.1.211 Connection: closeServer: MiniServ				

192.168.1.212 : yantech.com.tw

開始時間: 2026/6/29 上午 11:25:56 - 2026/6/29 上午 11:38:12
作業系統: Linux 3.X|4.X
資訊: Linux 3.11 - 4.1
CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
MAC / 閘道: 0.0.0.0
嚴重性層級 : 等級 0 (資訊)

稽核(13)

偵測到 **Web Server HTTP Protocol Version**	等級 **0** (資訊)
內容描述	透過 Web 伺服器從主機獲得 HTTP 通訊協定版本。
修補建議	確認 Web 伺服器符合組織的原則。
系統回應 : HTTP/1.1	

偵測到 **Web Server HTTP Protocol Version : 443**	等級 **0** (資訊)
系統回應 : HTTP/1.1	

偵測到 **Web Server HTTP Protocol Version**	等級 **0** (資訊)
系統回應 : HTTP/1.1	

偵測到隱藏 **WWW** 伺服器名稱	等級 **0** (資訊)
內容描述	偵測到隱藏 WWW 伺服器名稱。
修補建議	確認 Web 伺服器符合組織的原則。WWW 伺服器為電腦應用程式，可透過 HTTP 提供 web 型內容。偵測到隱藏 WWW 伺服器名稱。為了安全考量，可隱藏 Web 伺服器名稱。
系統回應 : Apache	

偵測到隱藏 **WWW** 伺服器名稱	等級 **0** (資訊)
系統回應 : Server	

偵測到 **Web** 伺服器重新導向 **: 443**	等級 **0** (資訊)
內容描述	在主機上偵測到 Web 伺服器重新導向狀態。
修補建議	確認 Web 伺服器符合組織的原則。Web 伺服器可廣泛在用戶端瀏覽器上提供動態和靜態內容。在主機上偵測到 Web 伺服器重新導向狀態。
系統回應 : 302	

偵測到 **SSL Server** 資訊	等級 **0** (資訊)
內容描述	在主機上偵測到 SSL 伺服器資訊。
修補建議	確認 SSL 伺服器的協定以及加密方法符合公司原則。
Protocol: TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3	
Cipher: TLS1_RSA_WITH_IDEA_CBC_SHA : Weak TLS1_RSA_WITH_AES_128_CBC_SHA : Weak TLS1_DHE_RSA_WITH_AES_128_CBC_SHA : Weak TLS1_DH_anon_WITH_AES_128_CBC_SHA : Insecure TLS1_RSA_WITH_AES_256_CBC_SHA : Weak TLS1_DHE_RSA_WITH_AES_256_CBC_SHA : Weak TLS1_DH_anon_WITH_AES_256_CBC_SHA : Insecure TLS1_RSA_WITH_CAMELLIA_128_CBC_SHA : Weak TLS1_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA : Weak TLS1_DH_anon_WITH_CAMELLIA_128_CBC_SHA : Insecure TLS1_RSA_WITH_CAMELLIA_256_CBC_SHA : Weak TLS1_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA : Weak TLS1_DH_anon_WITH_CAMELLIA_256_CBC_SHA : Insecure TLS1_RSA_WITH_SEED_CBC_SHA : Weak	

TLS1_DHE_RSA_WITH_SEED_CBC_SHA : Weak
TLS1_DH_anon_WITH_SEED_CBC_SHA : Insecure
TLS1_ECDHE_RSA_WITH_AES_128_CBC_SHA : Weak
TLS1_ECDHE_RSA_WITH_AES_256_CBC_SHA : Weak
TLS1_ECDH_anon_WITH_AES_128_CBC_SHA : Insecure
TLS1_ECDH_anon_WITH_AES_256_CBC_SHA : Insecure
TLS1_RSA_WITH_IDEA_CBC_SHA : Weak
TLS1_RSA_WITH_AES_128_CBC_SHA : Weak
TLS1_DHE_RSA_WITH_AES_128_CBC_SHA : Weak
TLS1_DH_anon_WITH_AES_128_CBC_SHA : Insecure
TLS1_RSA_WITH_AES_256_CBC_SHA : Weak
TLS1_DHE_RSA_WITH_AES_256_CBC_SHA : Weak
TLS1_DH_anon_WITH_AES_256_CBC_SHA : Insecure
TLS1_RSA_WITH_CAMELLIA_128_CBC_SHA : Weak
TLS1_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA : Weak
TLS1_DH_anon_WITH_CAMELLIA_128_CBC_SHA : Insecure
TLS1_RSA_WITH_CAMELLIA_256_CBC_SHA : Weak
TLS1_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA : Weak
TLS1_DH_anon_WITH_CAMELLIA_256_CBC_SHA : Insecure
TLS1_RSA_WITH_SEED_CBC_SHA : Weak
TLS1_DHE_RSA_WITH_SEED_CBC_SHA : Weak
TLS1_DH_anon_WITH_SEED_CBC_SHA : Insecure
TLS1_ECDHE_RSA_WITH_AES_128_CBC_SHA : Weak
TLS1_ECDHE_RSA_WITH_AES_256_CBC_SHA : Weak
TLS1_ECDH_anon_WITH_AES_128_CBC_SHA : Insecure
TLS1_ECDH_anon_WITH_AES_256_CBC_SHA : Insecure
TLS_1_2_RSA_WITH_AES_128_CBC_SHA : Weak
TLS_1_2_RSA_WITH_AES_256_CBC_SHA : Weak
TLS_1_2_RSA_WITH_AES_128_CBC_SHA256 : Weak
TLS_1_2_RSA_WITH_AES_256_CBC_SHA256 : Weak
TLS_1_2_DHE_RSA_WITH_AES_128_CBC_SHA256 : Weak
TLS_1_2_DHE_RSA_WITH_AES_128_CBC_SHA : Weak
TLS_1_2_DHE_RSA_WITH_AES_256_CBC_SHA : Weak
TLS_1_2_DHE_RSA_WITH_AES_256_CBC_SHA256 : Weak
TLS_1_2_DHE_RSA_WITH_AES_128_GCM_SHA256 : Weak
TLS_1_2_DHE_RSA_WITH_AES_256_GCM_SHA384 : Weak
TLS_1_2_RSA_WITH_AES_128_GCM_SHA256 : Weak
TLS_1_2_RSA_WITH_AES_256_GCM_SHA384 : Weak
TLS_1_2_DH_anon_WITH_AES_128_CBC_SHA256 : Insecure
TLS_1_2_DH_anon_WITH_AES_256_CBC_SHA256 : Insecure
TLS_1_2_DH_anon_WITH_AES_128_GCM_SHA256 : Insecure
TLS_1_2_DH_anon_WITH_AES_256_GCM_SHA384 : Insecure
TLS_1_2_ECDHE_RSA_WITH_AES_128_CBC_SHA256 : Weak
TLS_1_2_ECDHE_RSA_WITH_AES_256_CBC_SHA384 : Weak
TLS_1_2_ECDHE_RSA_WITH_AES_128_GCM_SHA256 : Secure
TLS_1_2_ECDHE_RSA_WITH_AES_256_GCM_SHA384 : Secure
TLS_1_2_RSA_WITH_ARIA_128_GCM_SHA256 : Weak
TLS_1_2_RSA_WITH_ARIA_256_GCM_SHA384 : Weak
TLS_1_2_DHE_RSA_WITH_ARIA_128_GCM_SHA256 : Weak
TLS_1_2_DHE_RSA_WITH_ARIA_256_GCM_SHA384 : Weak
TLS_1_2_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256 : Secure
TLS_1_2_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384 : Secure
TLS_1_2_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 : Weak
TLS_1_2_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 : Weak
TLS_1_2_RSA_WITH_AES_128_CCM : Weak
TLS_1_2_RSA_WITH_AES_256_CCM : Weak
TLS_1_2_DHE_RSA_WITH_AES_128_CCM : Weak
TLS_1_2_DHE_RSA_WITH_AES_256_CCM : Weak
TLS_1_2_RSA_WITH_AES_128_CCM_8 : Weak
TLS_1_2_RSA_WITH_AES_256_CCM_8 : Weak
TLS_1_2_DHE_RSA_WITH_AES_128_CCM_8 : Weak
TLS_1_2_DHE_RSA_WITH_AES_256_CCM_8 : Weak
TLS_1_2_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256: Secure
TLS_1_2_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 : Weak
TLS_1_3_AES_128_GCM_SHA256 : Recommended
TLS_1_3_AES_256_GCM_SHA384 : Recommended
TLS_1_3_CHACHA20_POLY1305_SHA256 : Recommended

偵測到 **SSL Server** 資訊	等級 **0** (資訊)

Protocol: TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3

Cipher: TLS_1_2_RSA_WITH_AES_128_CBC_SHA : Weak
TLS_1_2_RSA_WITH_AES_256_CBC_SHA : Weak
TLS_1_2_RSA_WITH_AES_128_CBC_SHA256 : Weak
TLS_1_2_RSA_WITH_AES_256_CBC_SHA256 : Weak
TLS_1_2_DHE_RSA_WITH_AES_128_CBC_SHA256 : Weak
TLS_1_2_DHE_RSA_WITH_AES_128_CBC_SHA : Weak
TLS_1_2_DHE_RSA_WITH_AES_256_CBC_SHA : Weak
TLS_1_2_DHE_RSA_WITH_AES_256_CBC_SHA256 : Weak
TLS_1_2_DHE_RSA_WITH_AES_128_GCM_SHA256 : Weak
TLS_1_2_DHE_RSA_WITH_AES_256_GCM_SHA384 : Weak
TLS_1_2_RSA_WITH_AES_128_GCM_SHA256 : Weak
TLS_1_2_RSA_WITH_AES_256_GCM_SHA384 : Weak
TLS_1_2_ECDHE_RSA_WITH_AES_128_CBC_SHA256 : Weak
TLS_1_2_ECDHE_RSA_WITH_AES_256_CBC_SHA384 : Weak
TLS_1_2_ECDHE_RSA_WITH_AES_128_GCM_SHA256 : Secure
TLS_1_2_ECDHE_RSA_WITH_AES_256_GCM_SHA384 : Secure
TLS_1_2_RSA_WITH_ARIA_128_GCM_SHA256 : Weak
TLS_1_2_RSA_WITH_ARIA_256_GCM_SHA384 : Weak
TLS_1_2_DHE_RSA_WITH_ARIA_128_GCM_SHA256 : Weak
TLS_1_2_DHE_RSA_WITH_ARIA_256_GCM_SHA384 : Weak
TLS_1_2_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256 : Secure
TLS_1_2_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384 : Secure
TLS_1_2_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 : Weak
TLS_1_2_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 : Weak
TLS_1_2_RSA_WITH_AES_128_CCM : Weak
TLS_1_2_RSA_WITH_AES_256_CCM : Weak
TLS_1_2_DHE_RSA_WITH_AES_128_CCM : Weak
TLS_1_2_DHE_RSA_WITH_AES_256_CCM : Weak
TLS_1_2_RSA_WITH_AES_128_CCM_8 : Weak
TLS_1_2_RSA_WITH_AES_256_CCM_8 : Weak
TLS_1_2_DHE_RSA_WITH_AES_128_CCM_8 : Weak
TLS_1_2_DHE_RSA_WITH_AES_256_CCM_8 : Weak
TLS_1_2_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256: Secure
TLS_1_2_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 : Weak
TLS_1_3_AES_128_GCM_SHA256 : Recommended
TLS_1_3_AES_256_GCM_SHA384 : Recommended
TLS_1_3_CHACHA20_POLY1305_SHA256 : Recommended

偵測到 **SSL Server** 資訊	等級 **0** (資訊)

Protocol: TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3

Cipher: TLS_1_2_RSA_WITH_AES_128_CBC_SHA : Weak
TLS_1_2_RSA_WITH_AES_256_CBC_SHA : Weak
TLS_1_2_RSA_WITH_AES_128_CBC_SHA256 : Weak
TLS_1_2_RSA_WITH_AES_256_CBC_SHA256 : Weak
TLS_1_2_DHE_RSA_WITH_AES_128_CBC_SHA256 : Weak
TLS_1_2_DHE_RSA_WITH_AES_128_CBC_SHA : Weak
TLS_1_2_DHE_RSA_WITH_AES_256_CBC_SHA : Weak
TLS_1_2_DHE_RSA_WITH_AES_256_CBC_SHA256 : Weak
TLS_1_2_DHE_RSA_WITH_AES_128_GCM_SHA256 : Weak
TLS_1_2_DHE_RSA_WITH_AES_256_GCM_SHA384 : Weak
TLS_1_2_RSA_WITH_AES_128_GCM_SHA256 : Weak
TLS_1_2_RSA_WITH_AES_256_GCM_SHA384 : Weak
TLS_1_2_ECDHE_RSA_WITH_AES_128_CBC_SHA256 : Weak
TLS_1_2_ECDHE_RSA_WITH_AES_256_CBC_SHA384 : Weak
TLS_1_2_ECDHE_RSA_WITH_AES_128_GCM_SHA256 : Secure
TLS_1_2_ECDHE_RSA_WITH_AES_256_GCM_SHA384 : Secure
TLS_1_2_RSA_WITH_ARIA_128_GCM_SHA256 : Weak
TLS_1_2_RSA_WITH_ARIA_256_GCM_SHA384 : Weak
TLS_1_2_DHE_RSA_WITH_ARIA_128_GCM_SHA256 : Weak
TLS_1_2_DHE_RSA_WITH_ARIA_256_GCM_SHA384 : Weak
TLS_1_2_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256 : Secure
TLS_1_2_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384 : Secure
TLS_1_2_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 : Weak
TLS_1_2_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 : Weak
TLS_1_2_RSA_WITH_AES_128_CCM : Weak
TLS_1_2_RSA_WITH_AES_256_CCM : Weak
TLS_1_2_DHE_RSA_WITH_AES_128_CCM : Weak
TLS_1_2_DHE_RSA_WITH_AES_256_CCM : Weak
TLS_1_2_RSA_WITH_AES_128_CCM_8 : Weak
TLS_1_2_RSA_WITH_AES_256_CCM_8 : Weak
TLS_1_2_DHE_RSA_WITH_AES_128_CCM_8 : Weak
TLS_1_2_DHE_RSA_WITH_AES_256_CCM_8 : Weak
TLS_1_2_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256: Secure
TLS_1_2_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 : Weak

TLS_1_3_AES_128_GCM_SHA256 : Recommended
TLS_1_3_AES_256_GCM_SHA384 : Recommended
TLS_1_3_CHACHA20_POLY1305_SHA256 : Recommended

偵測到 **SMTP** 伺服器	等級 **0** (資訊)
內容描述	在主機上偵測到 SMTP 伺服器。
修補建議	確認 SMTP 伺服器符合公司原則。
系統回應 ：220 ESMTP MAIL Server	

偵測到 **SMTP** 伺服器	等級 **0** (資訊)
系統回應 ：220 ESMTP MAIL Server	

偵測到 **IMAP4** 伺服器	等級 **0** (資訊)
內容描述	在主機上偵測到 IMAP4 伺服器。
修補建議	確認 IMAP4 伺服器符合公司原則。
相關連結	. Internet Message Access Protocol http://en.wikipedia.org/wiki/Internet_Message_Access_Protocol

偵測到 **TLS Version 1.0** 通訊協定	等級 **0** (資訊)
內容描述	TLS Version 1.0 has a number of cryptographic design flaws.
修補建議	確認 TLS Version 1.0 通訊協定以及加密方法符合公司原則, 或禁用 TLS Version 1.0。
Protocol: TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3	
Cipher: TLS1_RSA_WITH_IDEA_CBC_SHA : Weak TLS1_RSA_WITH_AES_128_CBC_SHA : Weak TLS1_DHE_RSA_WITH_AES_128_CBC_SHA : Weak TLS1_DH_anon_WITH_AES_128_CBC_SHA : Insecure TLS1_RSA_WITH_AES_256_CBC_SHA : Weak TLS1_DHE_RSA_WITH_AES_256_CBC_SHA : Weak TLS1_DH_anon_WITH_AES_256_CBC_SHA : Insecure TLS1_RSA_WITH_CAMELLIA_128_CBC_SHA : Weak TLS1_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA : Weak TLS1_DH_anon_WITH_CAMELLIA_128_CBC_SHA : Insecure TLS1_RSA_WITH_CAMELLIA_256_CBC_SHA : Weak TLS1_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA : Weak TLS1_DH_anon_WITH_CAMELLIA_256_CBC_SHA : Insecure TLS1_RSA_WITH_SEED_CBC_SHA : Weak TLS1_DHE_RSA_WITH_SEED_CBC_SHA : Weak TLS1_DH_anon_WITH_SEED_CBC_SHA : Insecure TLS1_ECDHE_RSA_WITH_AES_128_CBC_SHA : Weak TLS1_ECDHE_RSA_WITH_AES_256_CBC_SHA : Weak TLS1_ECDH_anon_WITH_AES_128_CBC_SHA : Insecure TLS1_ECDH_anon_WITH_AES_256_CBC_SHA : Insecure	

通訊埠(14)

通訊埠	內容描述	類型	稽核	風險
25	Simple Mail Transfer	TCP	1	資訊
220 ESMTP MAIL Server				
88	Kerberos	TCP	2	資訊
HTTP/1.1 400 Bad Request Date: Mon, 29 Jun 2026 03:28:47 GMT Server: Apache X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1;mode=block X-Content-Type-Options: nosniff Content-Security-Policy: default-src 'self'; style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self' https: data:; frame-ancestors 'self'; X-Content-Security-Policy: default-src 'self'; style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self' https: data:; frame-ancestors 'self'; X-WebKit-CSP: default-src 'self'; style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self' https: data:; frame-ancestors 'self'; Strict-Transport-Security: max-age=31536000; includeSubdomains Content-Length: 483 Connection: close Content-Type: text/html; charset=iso-8859-1Server: Apache				
110	Post Office Protocol - Version 3	TCP	0	資訊
+OK MS OK				
143	IMAP4 (Internet Message Access Protocol 4)	TCP	1	資訊
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS AUTH=PLAIN AUTH=LOGIN] MS OK				
389	Lightweight Directory Access Protocol	TCP	0	資訊
443	http protocol over TLS/SSL	TCP	2	資訊
HTTP/1.1 302 Found Date: Mon, 29 Jun 2026 03:29:32 GMT X-FRAME-OPTIONS: SAMEORIGIN X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Content-Security-Policy: default-src 'self'; style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self' http: https: data:; frame-ancestors 'self'; X-Content-Security-Policy: default-src 'self'; style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self' http: https: data:; frame-ancestors 'self'; X-WebKit-CSP: default-src 'self'; style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self' http: https: data:; frame-ancestors 'self'; Strict-Transport-Security: max-age=31536000; Location: https://192.168.1.212/webmail Content-Length: 0 Connection: keep-alive				
465	URL Rendesvous Directory for SSM	TCP	2	資訊
587	Submission	TCP	1	資訊
220 ESMTP MAIL Server				
993	imap4 protocol over TLS/SSL	TCP	1	資訊
995	pop3 protocol over TLS/SSL (was spop3)	TCP	1	資訊
1024	Reserved	TCP	0	資訊
Reply Banner:				
2000	Cisco SCCP	TCP	0	資訊
5060	SIP	TCP	0	資訊
8888	NewsEDGE server TCP (TCP 1)	TCP	2	資訊
HTTP/1.1 200 OK Set-Cookie: JSESSIONID=862B35C9AABD8E9C98C16A38E9B5F7EA; Path=/; HttpOnly Content-Type: text/html Content-Length: 1073 Date: Mon, 29 Jun 2026 03:37:50 GMT Connection: keep-alive Server: ServerServer: Server				

192.168.1.215 : 192.168.1.215

開始時間: 2026/6/29 上午 11:25:56 - 2026/6/29 上午 11:28:05
作業系統: Windows Server 2016 Standard 14393
資訊: Windows Server 2016 Standard 14393
MAC / 閘道: 192.168.3.254
嚴重性層級 : 等級 0 (資訊)

稽核(1)

偵測到 **SSL Server** 資訊		等級 **0** (資訊)
內容描述	在主機上偵測到 SSL 伺服器資訊。	
修補建議	確認 SSL 伺服器的協定以及加密方法符合公司原則。	
Protocol: TLS 1.0, TLS 1.1, TLS 1.2		

通訊埠(9)

通訊埠	內容描述	類型	稽核	風險
111	SUN Remote Procedure Call	TCP	0	資訊
135	Microsoft Remote Procedure Call (RPC) service	TCP	0	資訊
139	NETBIOS Session Service	TCP	0	資訊
445	Microsoft-DS	TCP	0	資訊
Native OS: Windows Server 2016 Standard 14393 Native LAN Manager: Windows Server 2016 Standard 6.3				
2000	Cisco SCCP	TCP	0	資訊
2049	Network File System - Sun Microsystems	TCP	0	資訊
Probe Hex: \x80\x00\x00\x18\x72\xFE\x1D\x13\x00\x00\x00\x01\x00\x00\x00\x00 \x00\x00\x00\x03\x00\x00\x00\x00\x00\x00\x00\x00 Probe Text: ....r..... Detect: rpcbind				
3389	Microsoft Terminal Services	TCP	1	資訊
5060	SIP	TCP	0	資訊
9401	Samsung Twain for Network Client	TCP	0	資訊