政府機關滲透測試服務委外服務案
建議書徵求文件
(V4.0)

修訂歷史紀錄

版次	發行修訂生效日期	變更說明
▪ 第 1.0 版	▪ 102 年 12 月 25 日	▪ 新版正式發行
▪ 第 2.0 版	▪ 103 年 11 月 1 日	▪ 強化報告架構與內容要求
▪ 第 3.0 版	▪ 107 年 1 月 16 日	▪ 更新專案工作項目內容說明要求及測試內容項目
▪ 第 4.0 版	▪ 108 年 4 月 23 日	▪ 更新物聯網設備檢測工作項目內容及測試工具項目說明
▪	▪	▪
▪	▪	▪
▪	▪	▪
▪	▪	▪
▪	▪	▪

目　次

壹、專案概述

一、專案名稱

「滲透測試服務」委外服務案（以下簡稱本案）。

二、專案目標

藉由本測試之執行成果，以檢測受測目標在遭遇外部攻擊者攻擊活動時之資安防護能力與執行成效。透過滲透測試報告及改善建議，檢討與精進受測目標之整體資安防護作為。

三、專案範圍

本案的服務範圍設備清單詳見附件 1。

四、專案期間

自簽約日起至 XXX 年 XX 月 XX 日止。

貳、專案工作項目

得標廠商針對機關之伺服器／主機作業系統、應用軟體、網路服務、可直接使用 RJ45 進行連線(配有 IP)之物聯網設備(如：門禁設備、網路印表機、網路攝影機(IPCAM)、無線 AP/無線路由器或環控系統(監控溫度或濕度之機房環控系統的伺服器主機)等安全弱點與漏洞，進行滲透或穿透跳躍主機之入侵測試，設法取得未經授權之存取權限，並測試內部資訊是否有遭受不當揭露、竄改或竊取之可能性。

一、資料蒐集

對受測目標進行資料蒐集與資訊分析(如：嘗試至受測物聯網設備官方網站或透過網路資源取得韌體、使用的通訊方法，以及對應之弱點資訊，若查無公開可下載之韌體或該韌體具保護機制，則蒐集該設備已知弱點資料)，將取得之相關資訊做為執行滲透測試決策。

二、分析報告

根據測試結果，將所發現之弱點與過程詳細記錄，並對結果進行統計分析，提出相關建議與測試報告。

三、風險管理

在滲透測試執行期前，需提出對受測目標進行備份建議，避免發生非預期資料損毀或遺失等情形。

在滲透測試執行期間，執行具侵入性質的檢測作業皆需與機關進行確認，並於雙方議定之適當時間且具備適當應變措施與風險評估後，才進行相關檢測作業。

四、測試內容

(一)測試項目

測試類型	測試類別	測試項目
▪作業系統	▪遠端服務	▪在到場服務的條件下，可執行無線服務弱點測試項目
	▪本機服務	▪在已取得系統控制權限的條件下，可執行至少包含本機服務套件弱點測試等項目
▪網站服務	▪設定管理	▪至少包含應用程式設定測試、檔案類型處理測試、網站檔案爬行測試、後端管理介面測試及 HTTP 協定測試等項目
	▪使用者認證	▪至少包含機敏資料是否透過加密通道進行傳送及使用者帳號列舉測試等項目
	▪連線管理	▪至少包含 Session 管理測試、Cookie 屬性測試、Session 資料更新測試、Session 變數傳遞測試及 CSRF 測試等項目
	▪使用者授權	▪至少包含目錄跨越測試、網站授權機制測試及權限控管機制測試等項目
	▪邏輯漏洞	▪至少包含網站功能測試、網站功能設計缺失測試及附件上傳測試等項目
	▪輸入驗證(1)	▪至少包含 XSS 弱點測試、SQL Injection 測試、LDAP Injection 測試、XML Injection 測試、SSI Injection 測試、XPath Injection 測試及 Code Injection 測試等項目
	▪輸入驗證(2)	▪至少包含 XSS 弱點測試、SQL Injection 測試、OS Commanding 測試及偽造 HTTP 協定測試等項目
	▪Web Service	▪至少包含 WSDL 測試、XML 架構測試、XML

測試類型	測試類別	測試項目
		內容測試及 XML 參數傳遞測試等項目
	▪ Ajax	▪ 至少包含 Ajax 弱點測試等項目，如輸入驗證缺失、權限控管及套件弱點等測試項目
▪ 應用程式	▪ 電子郵件服務套件	▪ 至少包含 SMTP、POP3 及 IMAP 等常見對外郵件服務之弱點測試，如設定缺失、權限控管及套件弱點等測試項目
	▪ 網站服務套件	▪ 包含常見 WEB 套件弱點測試，如設定缺失、權限控管及套件弱點等測試項目
	▪ 檔案傳檔服務套件	▪ 至少包含 FTP、NETBIOS 及 NFS 等常見檔案傳輸服務之弱點測試，如設定缺失、權限控管及套件弱點等測試項目
	▪ 遠端連線服務套件	▪ 至少包含 SSH、TELNET、VNC 及 RDP 等常見遠端連線服務之弱點測試，如設定缺失、權限控管及套件弱點等測試項目
	▪ 網路服務套件	▪ 至少包含 DNS、PROXY 及 SNMP 等常見網路服務之弱點測試，如設定缺失、權限控管及套件弱點等測試項目
	▪ 其它	▪ 包含 Firewall、IDS/IPS、Database、LDAP、SMB、LPD、IPP、Jetdirect 及 RTSP 等常見應用程式或網路套件之弱點檢測項目
▪ 密碼破解	▪ 密碼強度測試	▪ 至少包含 WEB、FTP、SSH、TELNET、SMTP、POP3、IMAP、SNMP、NetBIOS、RDP、VNC 及 Database 等常見對外服務之密碼字典檔測試，在到場服務的條件下，可執行 WiFi 密碼字典檔測試

(二)執行方式

1.得標廠商應組成滲透測試小組，模擬駭客利用各伺服器／主機作業系統、應用軟體、網路服務，以及防火牆、路由器、交換器等網路設備之安全弱點（例如網站設計不當，或防火牆、路由器等安全政策設定錯誤）進行滲透測試，設法取得未經授權之存取權限，並測試內部資訊是否有遭受不當揭露、竄改或竊取之可能。

2.得標廠商應分別針對本機關網際網路及內部網路進行滲透測試。網際網路滲透測試係滲透測試小組直接由遠端進行，內部網路於機關內部（on-site）進行。

3.得標廠商應依排定之日期執行滲透測試，於非公務時段或與機關協調取得適當時間進行測試作業。

4.得標廠商應彙整分析測試結果，提出測試報告，並視需求安排測試結果簡報。

5.得標廠商於檢測後，對於所提建議，應協助本機關進行改善，並針對應修補之弱點進行追蹤管理。

參、管理需求

一、廠商資格

為確保資訊安全及得標廠商所提供的服務水準，得標廠商應符合下列條件，並於服務建議書專章詳述：

(一)凡在政府機關登記合格，無不良紀錄之廠商（檢附設立及登記證明、納稅證明及信用證明）且不得為陸資企業(包括子公司、分公司、獨資或合夥事業及其轉投資事業)。本案服務人員需具有中華民國國籍，不得為外籍勞工或大陸來台人士。

(二)本案服務內容將涉及敏感資訊，得標廠商不得轉包或分包予其他廠商執行。

(三)投標廠商須實施資訊安全管理制度，通過 ISO 27001 或其他類似驗證，並於專案執行期間持續有效，以保護滲透測試服務所取得之資料。

(四)本案團隊人力至少應包含專案負責人/專案經理與滲透測試服務人員。滲透測試服務人員應具備以下所列舉之技能，且各類技能至少有一名成員，以確保服務水準，並於建議書中檢附成員姓名、訓練證書或專業證照等影本以供審核。應具備必要資訊網路、系統技能說明如下:

1. 滲透測試工具使用：接受過 CEH(Certified Ethical Hacker)、EC-Council CertifiedSecurity Analyst (ECSA)或其他類似相關課程訓練。

2. 滲透測試服務：接受過 GPEN (GIAC Certified Penetration Testers)、**GWAPT (GIAC Web Application Penetration Tester)**或其他類似相關課程訓練證明。

二、服務水準協定(SLA)與罰責

(一)服務水準規範

本案各項服務水準協定（Service Level Agreement，SLA），以必須達成該項工作服務項目要求為依據，透過客觀的證據或指標，做為品質管制，以預防各項不符合作業的事項發生，降低委外作業的風險，詳細服務水準規範如下表：

項次	項目	服務水準
1	▪執行時程	▪初測：每次以 2 週為限。 ▪複測：每次以 2 週為限。 ▪檢測報告：初測及複測結束後 2 週內提供。
2	▪設備服務中斷時間	▪因執行滲透測試服務造成軟硬體設備服務中斷時，應協助機關恢復正常運作，服務中斷時間不得超過 8 小時

(二)相關說明：

1.承作廠商無法達成相關工作項目要求或交付文件，其罰款(違約金)計算方式為每延遲 1 日(以日曆天計，星期日、國定假日及其他休息日均應計入，不滿 1 日以 1 日計算)，本機關得按契約總價之千分之一計算懲罰性違約金，款項可自契約總價或履約保證金項中扣抵。

2.違約金上限依採購法之採購契約要項第四十五點規定，違約金以契約總價之 20%為上限。如違約金逾 20%時，本機關得以書面通知得標廠商終止契約或解除契約之部分或全部，且不補償得標廠商所生之損失。

3.得標廠商應於議價後所提成本分析中，詳列各項工作項目成本，如於驗收時，經審查發現有不合格之工作項目，得標廠商應依期

限予以改正。如未改正，本機關有權扣除該項工作之款項。

4.得標廠商指派之專案負責人及工作成員，未經本機關同意，不得更換，如有未經本機關同意自行更換時，每更換乙次得依契約總價之千分之一計算懲罰性違約金。

5.得標廠商應將文件品質保證納入專案品質保證項目，嚴謹製作本專案各項文件，包含版面及內容皆須嚴格要求一致性及正確性。交付本機關之文件經本機關審閱時，所發現錯漏處達 N 處以上，或業經本機關要求修訂仍未修訂者，本機關得按每字新台幣 XXX 元計算懲罰性違約金，並自付款項中扣抵；其有不足者，得通知廠商繳納或自履約保證金扣抵。

三、品質需求與驗收標準

(一)品質需求

1.為確保專案如期如質完成，廠商應針對本專案之需求，妥慎成立專案小組，執行本專案所需之各項作業，並指派專案經理負責督導工作項目。

2.得標廠商訂定品質管理流程，本機關得以稽核。

3.得標廠商於專案期間應辦理啟始會議與結束會議，並視情況召開專案管理會議以掌控品質，會議討論內容與結果需作成紀錄與追蹤辦理，送本機關備考。

(二)驗收標準

得標廠商應依貳、專案工作項目之服務需求，以及符合服務水準協定(SLA)中所列事項，完成專案工作，並依本說明文件所訂之交付時程，完成相關文件與紀錄之交付。

(三)驗收方式

本機關將於各項工作項目交付完成後進行審查作業，得標廠商需依本機關審查意見修正交付項目，並再送至本機關複驗。

四、業務保密安全責任

(一)廠商基於本案需要，所取得各種形式之資訊，包含文書、圖片、紀錄、照片、錄影（音）及電腦處理資料等，可供聽、讀、閱覽或藉助科技得以閱讀或理解之文書或物品，應負資訊保密及確保資訊安全責任，並簽定保密協議書。

(二)廠商對特別以文字標示或口頭明示為機密資料者，非經本機關書面同意，不得洩漏資料予第三者，致使造成之法律責任或賠償，廠商應負完全責任。

(三)廠商對於可能接觸與本案相關資料或文件之人員，須提供保密管理機制，相關人員均須簽署保密切結書(切結書形式由廠商自訂)。

(四)契約終止時，廠商應將有關本案過程中處理之任何形式資訊，整理歸檔後退還本機關或經本機關同意後銷毀。

(五)履約期間造成保密及安全事件，得歸咎於廠商之責任時，廠商應負所有法律及賠償責任。

(六)本機關對廠商保留實地稽核權，以確保廠商於委外服務期間與合約終止時之資料安全、設備管理及其他安全維護事項已採取必要措施。

五、專案經費預算金額

(一)本案 XXX 年度預算金額為新台幣 XXX 萬元整。

(二)本案所須之人力由得標廠商自由運用調配，並於建議書中詳述計費標準與成本分析。

肆、交付項目

一、交付項目與時程

(一)工作計畫書：決標日起 2 週(日曆天)內交付。

(二)滲透測試服務報告：依工作計畫書載明之交付時程。

二、交付文件格式

(一)各項文件應提供紙本 N 份，電子檔 N 份（以光碟或本機關同意之儲存媒體及提交方式）。

(二)必要時本機關得要求派員親臨說明。

三、交付項目說明

交付項目	內容說明
1. 工作計畫書	▪工作計畫書應以廠商投標時之「建議書」為基礎，並依採購評選意見修改 ▪內容除包括對本專案之執行敘述，含專案管理、組織、人力、分工、職掌、工作項目、執行測試方式、時程說明、工作進度稽核點及品質管理流程
2. 滲透測試服務報告	▪文件內容應包括：摘要說明(受測目標風險等級與數量列表/受測目標風險漏洞名稱列表/風險漏洞分布列表)、專案執行計畫(執行期間/執行項目/執行範圍/專案成員)、執行結果(受測目標/漏洞名稱/問題 URL 或 IP/問題參數/測試語法/測試截圖等)、改善與建議、結論

伍、建議書製作規定

一、服務建議書格式

(一)紙張：宜用 A4 規格。

(二)繕打及裝訂方式：由左至右橫式繕打，加註頁碼，加裝封面及目錄，封面上註明廠商名稱、廠商地址、本案名稱及日期，裝訂線在左側。

(三)目次：應標示各章節之出處頁碼。

(四)廠商投標建議書之份數為 1 式 N 份。

二、服務建議書內容

(一)專案概述

1.專案名稱

2.專案目標

3.專案時程

(二)廠商說明

1.廠商簡介

2.公司營運狀況，包含參與人員名單、能力證明及廠商經驗說明

(三)專案計畫

1.專案服務內容項目

2.組織與人力配置

3.專案時程、品質、風險管理與交付項目計畫，包含工作項目、時程規劃及查核點

4.本案帶來之預期效益

5.本案 SLA 之承諾

(四)其它

陸、建議書評選事宜

一、評選辦法

(一)依據「政府採購法」第 22 條第 1 項第 9 款之規定辦理，透過書面審查及簡報答詢的方式，以合於招標文件，標價合理且在預算金額內，經評選委員評選為合格的廠商，依序議價。

(二)由本機關邀集專家學者組成評選委員會,除對廠商之建議書進行書面審查外，並由本機關召開評選會議，由廠商提出 15 分鐘對建議書之簡報,其後並接受評選委員之詢問,答詢時間以不超過 10 分鐘為限，惟因評審委員詢問題目過多時，主席得酌以延長答詢時間。評選會議時間及地點，將於資格審查時當場宣布或另備文通知，而廠商之簡報順序，亦於資格審查時抽籤決定。

(三)簡報及答詢結束後,各評選委員根據本徵求建議書說明文件第柒之二「評審項目」所列項目及配分評定各廠商名次及其是否為合格廠商（以總得分 XX 分(含)以上為合格）。

(四)各評選委員評定結果不得有同名次或從缺情形。

(五)過半數(含)評選委員評定為合格之廠商方列入排名與序分計算；另半數以上（含）評選委員評定不合格之廠商，視為不合格，若所有廠商均不合格時，主席應宣布廢標，重新辦理本案。

(六)本案評選採序位法辦理，就各評審項目分別評定並換算為序位，再加總計算廠商序位，最低者為第 1 優先序位，次低者為第 2 序位，餘依此類推。

(七)經評選委員會評定優勝廠商，依優勝序位，自最優勝者起，依序以議價方式辦理，但有二家以上廠商為同一優勝序位者，以建議書的標價低者優先議價，若仍相同者，則擇獲得評選委員評定序位第一較多者決標；仍相同者，抽籤決定之。

(八)評選結果簽請首長或授權人員核定後,由本機關另定時間通知廠商依序辦理議價。

二、評選標準

本案由評選委員就廠商所提出建議書之內容，針對其經驗、能力與服務水準，依下列各項目及配分，予以評分，總分 100 分，得分總計達 XX 分(含)以上者為合格。

評審項目	評審項目內容	配分
廠商業績及履約能力	1.廠商人力規模、商譽 2.資安實績與相關技術經驗	20
專案管理	1.對本案工作內容之瞭解 2.進度時程控管、資料管制與品質保證 3.本案之團隊規模與專案負責人之經驗 4.本案團隊成員之專業證照符合程度	20
專案規劃完整性	1.本案要求之各項服務項目的執行專業性 2.本案要求之各項交付項目之完整性	30
成本合理性	本案規劃、執行、專案管理及報告撰寫等各項費用估算之合理性	20
簡報及答詢	廠商簡報與答詢內容是否清楚、完整	10
總分		100
是否合格		□合格 □不合格
名次序位		

三、其他評選注意事項

(一)本機關得因故終止評選事宜，通知投標廠商領回建議書。

(二)本文件未盡事宜，依據「政府採購法」相關規定辦理。

柒、附件

附件 1 滲透測試服務範圍設備清單

附件1　滲透測試服務範圍設備清單

例如：

項目	設備類別	數量	備註
1	個人電腦 Windows Base (或 Linux Base)		
2	網站伺服器 Windows Base (或 Linux Base)		
3	資料庫伺服器 Windows Base (或 Linux Base)		
4	代理伺服器 Windows Base (或 Linux Base)		
	…		