數字政策辦公室

資訊保安

滲透測試

實務指引

第 1.3 版

2024 年 7 月

©中華人民共和國
香港特別行政區政府

中華人民共和國香港特別行政區政府保留本文件內容的所有權，未經中華人民共和國香港特別行政區政府明確批准，不得翻印文件的全部或部分內容。

版權公告

© 2024 中華人民共和國香港特別行政區政府
除非另有註明，本出版物所載資料的版權屬中華人民共和國香港特別行政區政府所有。在符合下列條件的情況下，這些資料一般可以任何格式或媒介複製及分發：

(a) 有關資料沒有特別註明屬不可複製及分發之列，因此沒有被禁止複製及分發；
(b) 複製並非為製造備份作售賣用途；
(c) 必須準確地複製資料，而且不得在可能誤導他人的情況下使用資料；以及
(d) 複製版本必須附上「經中華人民共和國香港特別行政區政府批准複製／分發。中華人民共和國香港特別行政區政府保留一切權利」的字眼。

如須複製資料作上述核准用途以外的用途，請聯絡數字政策辦公室尋求准許。

修改記錄

修改次數	修改詳情	經修改頁數	版本編號	日期
1	簡述嚴格的保安漏洞管理； 闡述滲透測試與漏洞掃瞄； 更新開放網上應用系統保安項目 (OWASP) 10大漏洞	1,6,A-2	1.1	2021 年 6 月
2	更新參考標準；闡述在攻擊前階段收集資料的方法	2,11,A-1	1.2	2023 年 12 月
3	將「政府資訊科技總監辦公室」更改為「數字政策辦公室」		1.3	2024 年 7 月

目錄

1. 簡介 1

1.1 目的 1
1.2 參考標準 1
1.3 術語及慣用詞 2
1.4 聯絡方法 3

2. 滲透測試概覽 4

2.1 甚麼是滲透測試 4
2.2 滲透測試對漏洞掃瞄 8

3. 滲透測試過程 10

3.1 滲透測試步驟 10
3.2 界定滲透測試範圍及目標 10
3.3 計劃 11
3.4 進行測試 13
3.5 報告結果及建議 15
3.6 跟進行動 16

4. 滲透測試工具 17

5. 滲透測試員的遴選準則 19

附件 A 網上應用系統的滲透測試 A-1

附件 B 資訊科技基礎設施的滲透測試 B-1

附件 C 滲透測試計劃範本樣本 C-1

1. 簡介

按照《資訊科技保安指引》，政策局／部門需為所有面向互聯網的網站及網上應用系統最少每兩年一次或在推出前，以及在重大提升或改動前，進行保安漏洞掃瞄及／或滲透測試。所有部署在與互聯網連接的系統和關鍵資訊系統的伺服器和相關裝置都應受到嚴格的保安漏洞管理，例如所有已知的保安漏洞應在保安修補程式發布後一個月內修復，並應每年為該等系統進行保安漏洞掃描或滲透測試。本實務指引旨在協助政策局／部門考慮及計劃開展滲透測試。政策局／部門亦應根據保安風險評估的結果而進行滲透測試。

1.1 目的

本文件的目的在於提供滲透測試的一般常識及良好作業模式。本實務指引簡述進行滲透測試所需的重要概念，包括滲透測試的定義及限制、界定測試範圍及所需要求時的考慮，以及進行測試前、測試中及測試後需注意的主要工作。本文件主要為涉及規劃或進行滲透測試的人員而設。

本文件提供滲透測試的概覽以及涵蓋以下主題：

a) 滲透測試概覽；
b) 滲透測試過程；
c) 滲透測試工具；以及
d) 滲透測試員的遴選準則。

1.2 參考標準

以下的參考文件為本文件在應用上的參考：

- 香港特別行政區政府《基準資訊科技保安政策》（S17）
- 香港特別行政區政府《資訊科技保安指引》（G3）
- Information technology – Security techniques – Information security management systems – Requirements, ISO/IEC 27001:2013
- Information technology – Security techniques – Code of practice for information security controls, ISO/IEC 27002:2013

- Information technology – Security techniques – Information security risk management, ISO/IEC 27005:2018
- PCI Security Standards Council, "Information Supplement: Penetration Testing Guidance", September 2017

  (https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf?agreement=true&time=1620631951140)
- Open Web Application Security Project, "OWASP Testing Guide v4.2"

  (https://github.com/OWASP/wstg/releases/download/v4.2/wstg-v4.2.pdf)
- The Association of Banks in Singapore, 2015, "Penetration Testing Guidelines for the Financial Industry in Singapore"

  (https://abs.org.sg/docs/library/abs-pen-test-guidelines.pdf)
- NIST Special Publication 800-115, "Technical Guide to Information Security Testing and Assessment"

  (http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf)
- Patrick Engebreston, Syngress, "The Basics of Hacking and Penetration Testing", 2nd Edition 2013
- 中華人民共和國國家標準《信息安全技術 信息安全風險評估方法》，GB/T 20984-2022
- 中華人民共和國國家標準《信息安全技術 信息安全風險評估實施指南》，GB/T 31509-2015
- 中華人民共和國國家標準《信息安全技術 網絡安全漏洞分類分級指南》，GB/T 30279-2020

1.3 術語及慣用詞

本文件將會採用《基準資訊科技保安政策》和《資訊科技保安指引》內所使用及以下的術語及慣用詞。

縮寫及術語	
無	無

1.4 聯絡方法

本文件由數字政策辦公室編製及備存。如對本文件有任何意見或建議，請寄往：

電郵： it_security@digitalpolicy.gov.hk

Lotus Notes 電郵： IT Security Team/DPO/HKSARG@DPO

CMMP 電郵： IT Security Team/DPO

2. 滲透測試概覽

2.1 甚麼是滲透測試

滲透測試是一種保安評估方法。測試會進行漏洞評估，並查證攻擊者是否能成功利用系統漏洞進行攻擊。它是一個手動程序，而且需要運用專業知識去設計測試用例，以及選擇適當的技術或工具，以識別自動化工具不能找出的邏輯漏洞。使用漏洞掃瞄及其他自動化工具通常能幫助滲透測試員減少重覆工作。

在滲透測試的過程中，一般會先使用自動化工具來掃瞄網絡或系統，以建立已連接工作站及伺服器的網絡地圖，以及識別潛在風險。由於掃瞄過程通常會產生大量測試用例和網絡通訊，系統可能因而在滲透測試過程中不能操作。掃瞄漏洞後，滲透測試員將利用掃瞄結果作進一步測試。

滲透測試能幫助找出系統的弱點及漏洞，它能模擬出多個攻擊方法及讓它們同時進行，從而測試攻擊會否成功影響系統。滲透測試後，就能知道現行保安控制是否對主動及具豐富經驗的攻擊者有效。滲透測試結果將有助系統擁有者推行針對保安風險的防護措施。

滲透測試前應先謹慎考慮及計劃。由於進行滲透測試需要非常專業的知識及豐富的經驗，因此測試應由合資格的保安專家進行。

2.1.1 滲透測試目標

滲透測試是一種保安評估方法。根據測試的目標，它可以用不同方式及不同技術進行。政策局／部門應界定自己的滲透測試範圍及目標。以下列出部分滲透測試目標的例子：

a) 識別資訊資產的風險；
b) 識別難以透過自動化網絡或應用系統漏洞掃瞄軟件偵測的漏洞，例如防火牆的保安政策設定邏輯、編寫在程式內的計時炸彈和後門等；
c) 測試及驗證保安防護及控制的效率；
d) 測試防禦機制對攻擊的偵測及應變能力；
e) 評核防火牆及路由器等網絡保安裝置的效能；以及
f) 展示系統在抵禦真實網上攻擊時的表現。

2.1.2 滲透測試方式

滲透測試可以按不同的測試目標，以不同方式進行。測試可以在外部網絡或內部網絡內進行。

a) 外部測試是較常用的方式。測試涉及全面分析機構外部可見的伺服器及裝置（例如路由器、防火牆、電郵伺服器及網頁伺服器等）。外部測試的目的是辨識網絡、系統及應用系統的潛在保安弱點，並示範存在的已知漏洞可被外部攻擊者利用。測試亦幫助檢查系統是否能夠安全防範被入侵、資料損失或外泄。

b) 內部測試於內部網絡進行，假設攻擊者成功穿越保安防線，或攻擊者是機構內部人士。這種測試方式焦點集中在機構內部資源，例如非軍事區、內部網絡、系統程度的保安、應用系統和服務配置和認證，以及接達控制。內部測試是用來識別個別網絡內的電腦系統弱點，以及檢查是否有人可以透過濫用用戶權限而接達網絡內的系統。

無論是外部或內部網絡滲透測試，都可以以白盒、灰盒或黑盒方式進行。以下介紹這幾種方式：

i) 白盒測試：

對受測系統的內部結構、設計及推行有全面認知的情況下進行測試

ii) 灰盒測試：

對受測系統的內部結構、設計及推行有部分認知的情況下進行測試

iii) 黑盒測試：

對受測系統的內部結構、設計及推行沒有任何事前認知的情況下進行測試

若滲透測試的目標是盡量找出保安漏洞，就應採用白盒測試，透過分享程式源碼或配置等資訊，讓測試員可以直接進行分析。另一方面，若測試目標是評核保安部署的效能，則應採用黑盒測試，並保留資訊以獲取較真實的測試結果。

黑盒測試比白盒測試較消耗時間，及需要更高成本去收集及探索系統資料，更有可能會遺漏測試部分保安範疇。然而，黑盒測試能夠模擬一個外來攻擊，模擬嘗試入侵系統的真實情景。另一方面，白盒測試可以縮短滲透測試的時間，並因為已向白盒測試員提供全部資料，例如網絡布局文件、資產清單，以及應用系統設計資料等，因此測試員能夠進行更全面的保安評估。

2.1.3 滲透測試技術

滲透測試會使用一系列的技術，以下列出當中最常見的：

a) 被動式研究：從公眾網域來源，例如域名系統記錄及域名註冊管理機構，收集機構的系統配置資料 ；
b) 操作系統掃描及蒐集網絡布局的資訊：辨識整個受測網絡的配置；
c) 網絡窺竊：竊取流經網絡的通訊數據；
d) 偽冒：將一台機器偽裝成合法機器以竊取資訊；
e) 特洛伊木馬攻擊：透過如電郵附件等不同方法，於被入侵系統內安裝特洛伊木馬和惡意軟件以接達有用資料；
f) 暴力攻擊：破解密碼以獲得系統或應用系統的接達。這是一個廣為人知的破解密碼方法，或是一種用來使系統超出負荷，使系統不能正常回應請求的攻擊手法；
g) 漏洞掃瞄：探索保安系統或應用系統的弱點以作出進一步攻擊；
h) 社交工程：蒐集機構的重要資訊。攻擊者經常以機構員工作為目標，嘗試收集敏感資訊；和
i) 翻檢垃圾箱：透過仔細檢查垃圾以找尋機構的資料，可以是實體滲透測試的一部分。

2.2 滲透測試對漏洞掃瞄

漏洞掃瞄與滲透測試經常被混淆，而兩者亦經常被交換使用，但兩者實際上是有分別的。滲透測試通常但並不一定包括漏洞掃描。因此，機構必須在其服務規格中清楚列明這兩項要求，以便進行更徹底的測試。

漏洞掃瞄員對滲透測試員

漏洞掃瞄利用標準測試用例，能有效找出潛在的已知漏洞，如錯誤配置、核心缺陷、緩衝區溢滿、輸入驗證不足、及錯誤的檔案和目錄權限等。

另一方面，滲透測試員需要利用本身的技能及經驗去理解系統流程，並設計出個別測試用例去找出系統的邏輯漏洞。除此之外，滲透測試員亦會嘗試利用掃瞄中找出的漏洞，嘗試可以取得甚麼類型的資料。

漏洞掃瞄結果的處理

漏洞掃瞄是用來測試系統是否存在弱點，而掃瞄過程牽涉辨認、排名及滙報漏洞等程序。但測試用例的結果卻不能解釋為漏洞是否真的為系統帶來威脅。因此，漏洞掃瞄結果只被用作系統潛在攻擊威脅的基線指標。

相對地，滲透測試員通常利用漏洞掃瞄的結果決定是否需要進行額外測試，以識別自動化工具不能辨認的漏洞。此外，滲透測試會部署更具體的方法來顯示如何利用漏洞或如何重複測試結果。簡而言之，滲透測試比漏洞掃描產生更全面的結果。

技能

漏洞掃瞄利用不同的自動化工具及測試用例去辨認已知的技術漏洞。滲透測試過程涉及大量嘗試，而且亦非常倚重測試員的技能。

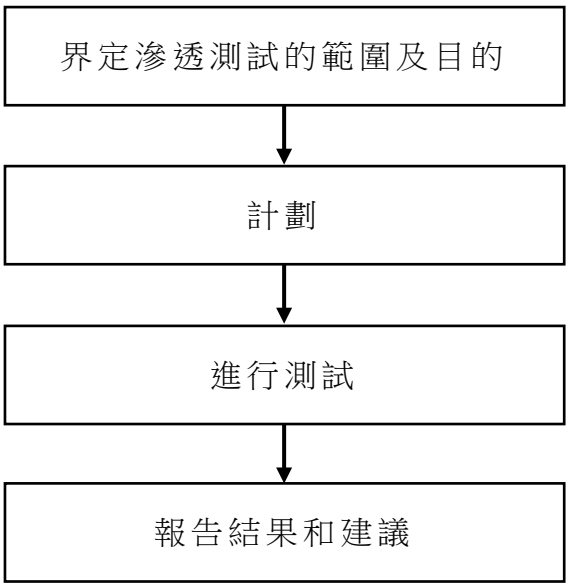
過程所需時間

漏洞掃瞄是使用自動化工具，因此掃瞄過程很快在很短的時間內（例如數小時）完成。可是，漏洞掃瞄同時會產生假陽性結果，因此需要核實結果。相對地，滲透測試是一個手動程序，通常會根據漏洞掃描結果來進一步識別系統中的漏洞。因此它通常需要比漏洞掃瞄更多的計劃和較長時間完成。

3. 滲透測試過程

3.1 滲透測試步驟

滲透測試雖然可以有不同類型，但在測試前後都應進行一些相同步驟。測試一般可以分為以下步驟：



滲透測試步驟

3.2 界定滲透測試範圍及目標

系統保安由不同範疇組成，並可以應用不同類型的滲透測試。以下列出最常見的範疇：

a) 網絡保安：

這會識別全部有可能的網絡缺陷，並模擬對已識別的漏洞作出真實攻擊；

b) 系統軟件保安：

這會識別全部有可能的系統軟件缺陷，並模擬對已識別的漏洞作出真實攻擊；

c) 客戶端應用系統保安：

這會主要集中在客戶端功能上，識別全部有可能的應用系統缺陷，並模擬對已識別的漏洞作出真實攻擊；

d) 伺服器端應用系統保安：

這會主要集中在伺服器端功能上，識別全部有可能的應用系統缺陷，並模擬對已識別的漏洞作出真實攻擊；

e) 實體保安：

這會獲取機構資源的接達（如辦工時間前、中，及後的數據中心）。通常會對所有實體保安控制進行測試；

f) 入侵偵測：

這一般會使用軟件工具，測試入侵偵測系統的強度；以及

g) 事故應變：

這會測試事故應變程序是否妥善，以及事故或緊急應變小組的準備程度。

政策局／部門應首先根據業務需要、所要達成的目標，以及手上的資源，界定滲透測試的範圍及目標，然後可以決定需要進行甚麼類型的滲透測試。滲透測試範圍可以按以下因素而決定：

a) 應用系統、網絡裝置、伺服器的規模及數量。例如：只測試應用系統，或是包括所有伺服器，又或是涵蓋整個網絡架構；
b) 需要進行內部或外部滲透測試，或是兩者皆需要進行；以及
c) 需要進行白盒、灰盒或黑盒測試，或是需要進行混合測試。對於灰盒及白盒測試，政策局／部門需要按「有需要知道」原則提供資料，以協助達成滲透測試的目標及目的。

3.3 計劃

開始滲透測試前，需要先計劃測試以作適當準備、監察及控制。滲透測試員應在進行測試前，準備及提交滲透測試計劃（就滲透測試計劃範本樣本，請參閱附件 C）。滲透測試計劃應包括，但不限於下列各點：

a) 範圍；
b) 目標；
c) 時間表；
d) 持份者的角色及責任；
e) 測試方式及方法；
f) 測試工具；以及
g) 回退及復原程序。

政策局／部門需要與滲透測試員共同制訂測試時間表，並就滲透測試環境上（例如生產、生產前或用戶驗收測試）達成共識。但由於部分滲透測試技術會測試有實際漏洞的應用系統、系統或網絡，因而影響系統的可用性，令敏感資料曝光，因此應盡量避免在生產環境內進行測試。另一重要事項是要記錄及訂立測試程度，而該測試程度應得到雙方同意。一旦測試超出某個程度，例如獲得個別系統接達時，就停止測試，以免對系統或數據造成傷害。

進行滲透測試前，需遵從下列作業模式：

a) 政策局／部門應向滲透測試員提供系統擁有人及受測系統的資訊科技管理員的聯絡名單，以便盡早報告任何在測試期間內發生的問題；
b) 政策局／部門應取得滲透測試員的聯絡名單，以便政策局／部門能在需要時迅速終止所有測試；
c) 政策局／部門應考慮是否需要暫停或修改可能影響滲透測試結果的現存保安措施設定（例如入侵防禦系統、網上應用系統防火牆等），避免測試受到影響；
d) 政策局／部門應在進行滲透測試前通知及提醒保安監察服務供應商，除非測試目標包括評核保安監察服務供應商的監察效能；
e) 政策局／部門應考慮為滲透測試員提供測試憑證，以有效測試應用層的功能；
f) 政策局／部門應確保存有受測系統的最新完整系統備份，在系統數據完整性受到影響的情況下，可用作復原系統；
g) 政策局／部門應遮蔽所有涉及保密資料及個人資料的測試數據；
h) 政策局／部門應安排於非繁忙工作時間進行滲透測試；以及
i) 政策局／部門應要求滲透測試員簽署保密協議書，以保障私隱或系統數據的機密性。

3.4 進行測試

一般而言，應用系統、系統或網絡的滲透測試牽涉三個階段：攻擊前、攻擊中及攻擊後。

3.4.1 攻擊前

攻擊前階段著重於蒐集針對為目標的應用系統、系統或網絡的資料。除非使用白盒方式，否則初步將會使用偵察方法以查找、收集、鑒定及記錄受測試的應用系統、系統或網絡的資料，其目的是在以不同途徑盡量發掘資料，用以制訂或輔助攻擊。偵察可以分為主動及被動兩類型。被動偵察在不主動的情況下收集受測試應用系統、系統或網絡的有關資料。這包括從公開來源，例如互聯網上的雲端平台和開源資料庫，收集相關數據。滲透測試員亦可能需要檢視系統，以理解其商業邏輯。主動偵察會直接參與受測試應用系統、系統或網絡，透過自動化工具，例如漏洞掃瞄工具、網絡窺竊工具，以掃瞄埠、掃瞄網絡和列舉用戶帳戶等方式試探目標。攻擊前階段所收集的資料可以是：

a) 網絡註冊資料，例如域名、註冊人姓名及電郵地址；
b) 域名系統及電郵伺服器資料，例如域名系統名稱及電郵伺服器名稱；
c) 操作系統資料：例如操作系統類型及版本；
d) 認證及憑證資料：例如目標系統的用戶登入名稱及密碼；
e) 聯絡資料：例如機構聯絡人及電話號碼；
f) 網站資料：例如網站劃一資源定位址、互聯網規約地址及程序源代碼；以及
g) 其他可以幫助測試目標應用系統、系統及網絡的資料。

蒐集有關資料後，漏洞掃瞄工具會自動開始進行漏洞分析，將從應用系統、操作系統及網絡所收集的資料與漏洞數據庫比較，或根據滲透測試員對漏洞的知識進行漏洞分析。手動程序能夠辨認假陽性掃瞄結果和自動化掃瞄工具可能遺留的新漏洞，但需要較多工夫和時間。

3.4.2 攻擊中

根據滲透測試的範圍和目標，測試員應決定最適合的方式、工具或技術，在攻擊階段進行滲透測試。這是一個手動過程，需要技巧和

經驗去決定特定的測試用例及選擇適當技術或工具去識別系統缺陷。可使用漏洞掃瞄工具或其他自動化工具輔助，為滲透測試員提供系統潛在攻擊漏洞的基線。

此攻擊階段通常需要透過嘗試利用攻擊前階段所找到的漏洞，對應用系統、系統及網絡作出實際破解。這階段一般牽涉三個主要活動：獲得接達、提升權限，以及安裝額外工具。

測試員會首先嘗試取得受測試系統的接達，成功後會接達系統或應用系統以進行漏洞攻擊，例如結構化查詢語言插入、系統數據修改等。此外，測試員亦會嘗試將用戶權限提升，以接達更多敏感資料，亦會在可行的情況下，於目標系統安裝額外軟件或工具，以作出進一步的攻擊或利用更多漏洞。

在攻擊階段中，滲透測試員應設計針對系統的測試用例，並記錄測試方法（即是如何可以重新製造相同的成功破解）及收集證據，以準備滲透測試報告。若發現會影響現行系統的嚴重漏洞，滲透測試員應詳細記錄如何導致該嚴重漏洞，並立刻通知負責人士。

3.4.3 攻擊後

攻擊後階段包括清理測試環境、將系統回復至測試前的狀態，以及獲取成功攻擊的日誌記錄作證明。以下列出一般於攻擊後階段進行的活動：

a) 取得相關日誌記錄作為測試證明；
b) 清理所有曾上載至測試系統的檔案；
c) 移除所有在測試過程中產生的檔案；
d) 刪除測試過程中新增的任何用戶帳戶；
e) 解除所有已安裝於測試系統內進行測試的工具；
f) 回遡所有用戶權限及設定的改動；以及
g) 回復系統或應用系統的配置或設定。

滲透測試員需要記錄及向負責人士披露在測試過程中對相關環境所作出的任何改動。測試員或負責人士需要將目標環境復原至測試前的狀態。

附件 A 及 B 分別附上對網上應用系統及資訊科技基礎設施進行滲透測試的例子，示範如何將上述三個階段應用在滲透測試上。

3.5 報告結果及建議

滲透測試後須提交滲透測試報告。（於大部分情況下，會有一個滲透測試簡報會，解釋報告細節。）滲透測試報告應詳細記錄已進行的測試活動、發現及相關建議，報告內容應包括，但不限於下列各點：

a) 執行摘要：

   滲透測試範圍、目標及發現的高層次摘要；

b) 項目範圍：

   詳細描述受測試應用系統、系統或網絡範圍；

c) 測試方法：

   詳細描述用來完成測試的方式及方法；

d) 曾使用的工具；

e) 限制及約束：

   詳細描述推行在測試上的所有限制，例如規定測試時間，及對舊有系統的特殊測試要求等；

f) 測試活動：

   詳細描述已進行的攻擊活動；

g) 發現及相關建議：

   詳細描述所發現的漏洞、漏洞風險排名、針對每個漏洞進行過的攻擊、攻擊結果、能支持所發現的證據，以及減低風險的建議；以及

h) 滲透測試後的環境清理：

   詳細描述及指示如何進行清理，以及如何核實保安控制已獲回復。

驗收滲透測試項目前，政策局／部門應核查：

a) 已簽妥及遞交保密協議書；
b) 服務供應商或滲透測試員已完成所有必須的攻擊後工作；
c) 已推行所有在工作簡介中指明的項目要求；以及
d) 提供足夠及正確的細節於已提交的報告中（如滲透測試報告及滲透測試計劃）。

3.6 跟進行動

接收滲透測試報告後，重要的是政策局／部門應在測試後於合理時間內跟進修補方案內的項目。

滲透測試結果未必都能全面識別每個漏洞情況，例如在程式內發現一個跨網站指令碼，未必表示同一漏洞不會在其他範圍內出現。政策局／部門應小心調查這些存在的漏洞，以確保所有漏洞都被修補方案處理。

進行修補後，政策局／部門應安排重新測試，證明新實行的措施能減低原有風險。

4. 滲透測試工具

滲透測試工具能夠協助滲透測試員和改善滲透測試效率。由於有不同的滲透測試範圍，例如網絡、應用系統及入侵偵測系統等，因此亦有不同種類的滲透測試工具為進行特定測試而設。滲透測試工具通常滿足兩個主要目的：

a) 收集目標系統／應用系統的資料；以及
b) 按特定漏洞進行攻擊。

部分滲透測試工具可以用來辨認現存於應用系統、網絡，或個別主機（主機為本）的漏洞，以及發動攻擊。而另一部分則是設計來進行漏洞掃瞄，但不能進行攻擊。

具蒐集網絡布局功能、窺竊網絡及掃瞄漏洞的工具經常會被利用於網絡滲透測試中，去探索以下資料：

a) 網絡布局；
b) 活躍伺服器及網絡裝置；以及
c) 操作系統類型、在活躍伺服器和網絡裝置上運行的應用系統和服務。

當發現與資訊科技基礎設施有關的漏洞後，就能以手動方式或利用具攻擊能力的自動化滲透測試工具發動附件 B － 資訊科技基礎設施的滲透測試內所提及的攻擊。

網上應用系統的滲透測試會通常使用具下列功能的工具收集資料及識別漏洞：

a) 截取代理：

   檢查及修改瀏覽器和目標應用系統間的超文本傳輸協定通訊；

b) 網上應用系統蜘蛛：

   抓取網上應用系統的內容和功能，以發現被遺漏或隱藏的網頁內容，從而提供應用系統內容的全面描述；以及

c) 網頁漏洞掃瞄：

   發掘應用系統漏洞。例如結構化查詢語言插入、跨網址程式編程及目錄遊歷等。

在收集資料及識別應用系統相關的漏洞後，滲透測試員可以利用其結果判斷是否需要進行額外測試。進一步的攻擊可以以手動方式或利用自動化滲透測試工具發動，以測試附件 A － 網上應用系統的滲透測試內提及的常見的嚴重網上應用系統漏洞。

滲透測試工具應根據下列選擇：

a) 滲透測試類型。例如網絡滲透測試或應用系統滲透測試；以及
b) 滲透測試員的取向或專業判斷。

滲透測試可使用市場上的工具及滲透測試員自己開發的工具來進行。

5. 滲透測試員的遴選準則

合資格的滲透測試員應擁有相關證書及工作經驗以進行滲透測試。

準候選滲透測試員所持的認證可能顯示技能級別及能力。以下是部分常見滲透測試認證：

a) 注冊網絡安全滲透評估專業人員 (NSATP-A)；
b) 道德駭客認證 (CEH)；
c) 注冊信息安全專業人員滲透測試工程師 (CISP-PTE)；
d) 注冊信息安全專業人員滲透測試專家 (CISP-PTS)；
e) CREST 滲透測試證書；
f) 全球資訊保證認證 (GIAC) 證書；以及
g) 攻擊型安全師專業認證 (OSCP) 證書。

除了滲透測試員所持的認證外，亦應根據以下滲透測試員的工作經驗細節，以決定滲透測試員是否合資格參與滲透測試項目：

a) 滲透測試員在滲透測試的工作年資（注意：所需年資沒有特定的限制。為確保滲透測試員擁有足夠經驗進行測試，建議選擇較高年資的）；
b) 對目標環境的認識和相關的工作經驗（即是包括操作系統、硬件、網上應用系統、網絡服務及規約等）；以及
c) 曾經進行類似的滲透測試範圍項目的次數。

附件 A:網上應用系統的滲透測試

網上應用系統滲透過程

要進行網上應用系統滲透測試，就涉及以下三個階段。

攻擊前階段

網上應用系統滲透測試在攻擊前階段會進行：

a) 收集資料，例如網站地圖或應用系統的劃一資源定位址；
b) 分析其功能、核心保安機制例如應用系統的對話管理和接達控制；以及
c) 識別網上應用系統所採用的技術。

目的是要找出應用系統所曝露的攻擊面，以及設計辨識應用系統漏洞的方法。

在過程中通常會使用自動化網上應用系統掃瞄工具。由於大部分網上應用系統漏洞都有個別識別特徵，自動化的網頁掃瞄工具能夠在操作系統層面上偵測已知的漏洞，例如已過時的軟件版本、遺漏的安裝修補程式、緩衝區溢滿，及錯誤配置等。掃瞄工具亦能夠偵測部分應用層的漏洞，例如小型文字檔案（cookies）問題、跨網址程式編程、目錄遍歷及結構化查詢語言插入等。一般而言，自動化網上應用系統掃瞄工具為滲透測試員提供潛在漏洞和攻擊方法的基線。滲透測試員可以利用掃瞄結果決定是否需要額外的測試：

a) 收集應用系統的基本資料，例如操作系統類型、應用系統伺服器版本、網頁伺服器版本等。亦會瀏覽所有網頁、目錄，並為所有構成網上應用系統的檔案建立索引；以及
b) 識別應用層面的漏洞，例如小型文字檔案問題、目錄遍歷及結構化查詢語言插入等。

可是，以下部分常見漏洞並沒有標準識別特徵，因而不能被自動化工具偵測：

a) 弱接達控制，例如某用戶可以接達其他用戶的資料，或低權限的用戶能夠接達管理功能；
b) 應用系統功能設計上的缺陷，例如弱密碼規則，或在登入失敗訊息中列出用戶名稱；

c) 敏感資料外泄，例如網上應用系統回應被用作漏洞分析及檢查，或敏感資料（如程序源代碼或配置文件）被上載至向公眾開放的代碼存管平台；

d) 修改對應用系統有特殊意義的參數，例如，漏洞掃瞄工具並不能知道隱藏欄的意義；以及

e) 對話管理的缺陷。

攻擊階段

經研究漏洞掃瞄所得出的結果後，滲透測試員應檢視受測試的網上應用系統及測試其功能，然後設計特定的測試用例及根據自己的專業判斷和經驗尋找可能的漏洞。

滲透測試員可以利用截取代理修改瀏覽器和應用系統之間的超文本傳輸協定通訊以進行測試。自動化工具或手動技術都可以用來發動攻擊，例如結構化查詢語言插入、修改系統數據、提升用戶權限，或如可行的話，安裝額外軟件或工具，以發動進一步的攻擊或利用更多漏洞。

攻擊後階段

一如其他類型的滲透測試，網上應用系統滲透測試在攻擊後階段包括清理測試環境、復原系統或配置至測試前的狀態、獲取成功攻擊的日誌記錄作證明，以及解除安裝任何曾作測試用途安裝的軟件。

開放網上應用系統保安項目 (OWASP) 10 大漏洞

開放網上應用系統保安項目是一個網上社群。它曾發表一系列最嚴重的網上應用系統缺陷。這些缺陷經常在網上應用系統上發生，亦很容易被找到及被利用。政策局／部門應確定滲透測試範圍包括所有已知最嚴重的漏洞。以下列出 2013 年度 OWASP 10 大漏洞：

a) 代碼插入；
b) 有缺陷的認證；
c) 敏感資料曝光；
d) XML 外部實體(XXE) ；
e) 無效的接達控制；
f) 錯誤保安配置；
g) 跨網址程式編程(XSS)；
h) 危險的反序列化；
i) 使用已知有漏洞的組件；以及

j) 不足的記錄和監察。

附件 B: 資訊科技基礎設施的滲透測試

資訊科技基礎設施滲透過程

這裡的資訊科技基礎設施滲透測試局限於利用網絡保安裝置和伺服器，如防火牆、路由器、網頁伺服器、應用系統伺服器及數據庫伺服器等的現存漏洞。要進行資訊科技基礎設施滲透測試就需要經過三個階段：攻擊前、攻擊中和攻擊後。

攻擊前階段

在攻擊前階段，資訊科技基礎設施滲透測試一般會進行以下工作：

a) 網絡探索：

可以使用被動式或主動式的技術去探索活躍的和有回應的網絡裝置及伺服器，藉此了解網絡布局。被動式的技術以網絡窺竊工具監察網絡通訊，並識別使用中的互聯網規約地址和埠，以及活躍的網絡裝置和伺服器的操作系統。主動式的技術透過自動化工具傳送不同類型的網絡封包，例如網際網路控制訊息規約，向網絡裝置及伺服器要求回應；

b) 網絡埠及服務識別：

基於在網絡探索過程中找到的互聯網規約地址，便可使用掃瞄工具找出活躍的網絡裝置及活躍的伺服器的網絡埠、服務、應用系統及執行中的服務。透過稱為操作系統指紋套取、服務識別，及標誌獲取的過程，埠掃瞄能相應地分別辨識操作系統種類、在網絡裝置及活躍的伺服器上執行的應用系統以及應用系統版本；以及

c) 漏洞掃瞄：

埠掃瞄工具可以識別活躍的裝置、操作系統、埠、服務及應用系統，但不能辨認漏洞。自動化漏洞掃瞄工具會嘗試基於網絡埠及服務識別過程中收集的資料識別漏洞。掃瞄工具可以將已收集的資料和掃瞄工具內漏洞數據庫的已知漏洞資料作比較，來辨認已過時的軟件版本、遺漏安裝的修復程式及錯誤配置。

這些的目的是要識別伺服器、網絡裝置和網絡環境所曝露的漏洞，並設計利用這些漏洞的方法。

攻擊階段

漏洞被識別後，就會開始獲取目標網絡裝置或活躍的伺服器的接達、嘗試利用自動化工具、自己開發的程式或手動方式去提升權限，以及安裝額外工具和軟件，作進一步的攻擊。

攻擊後階段

就如其他類型的滲透測試，資訊科技基礎設施滲透測試的攻擊後階段，包括清理測試環境、復原系統或配置至測試前的狀態、獲取成功攻擊的日誌記錄作證明、刪除任何測試帳戶和作測試用途的檔案，以及解除安裝任何曾作測試用途的軟件。

資訊科技基礎設施漏洞利用類別

以下列出最常在資訊科技基礎設施滲透測試中被利用的漏洞：

a) 錯誤配置：

錯誤配置裝置的保安設定，例如不安全的預設設定；

b) 核心缺陷：

核心編碼是操作系統最重要的核心，它是系統的整體保安模型的約束。任何在核心的保安缺陷會成為被利用的漏洞；

c) 不正確的檔案和目錄權限：

檔案和目錄權限控制分配給賦予用戶及程序對檔案接達權。不當的權限會造成許多類型的攻擊，例如讀取或修改密碼檔案；

d) 遺漏安裝保安修補程式：

遺漏安裝保安修補程式會成為用作惡意攻擊的漏洞；以及

e) 權限提升：

透過利用系統漏洞盡可能獲取最高管理權限，進一步接達整個網絡及敏感資料。

附件 C: 滲透測試計劃樣本

a) 範圍

這節列明項目的範圍、已測試的互聯網規約地址資料、所進行的滲透測試類型（如應用系統或網絡），以及其他會影響項目所需的時間及預算的資料。

b) 目標

這節提供一些目標，當政府部門在得知滲透目標的互聯網地址 / 系統或應用系統相關的風險及在實行滲透測試的建議，並減低這些風險後將會帶來的好處。

c) 時間表

這節提供滲透測試的開始及結束日期，為目標受眾提供以下資料：

- 測試期限
- 只在這測試期限內，從滲透測試觀點的已測試互聯網規約地址的風險
- 若在這測試期限後，因目標系統有所變動而帶來部分風險，滲透測試員無需為此負上任何責任

d) 持份者角色及責任

這節列出持份者在滲透測試內的工作。

e) 測試方式及方法

這節提供有關滲透測試進行的方式、收集和分析資料所應跟從的步驟、計算每個漏洞個案風險排名的方法等。

f) 使用工具

這節提供滲透測試員在每個滲透測試階段中使用過的工具資料。

g) 回退及復原程序

這節提供持份者在滲透測試期間應該採取的回退及復原程序。