# 数字政策办公室

## 信息安全

# 渗透测试

# 实务指南

**第 1.3 版**

**2024 年 7 月**

# 版权公告

## 修改记录

| 修改次数 | 修改详情 | 经修改页数 | 版本编号 | 日期 |
|---|---|---|---|---|
| 1 | 简述严格的安全漏洞管理；<br>阐述渗透测试与漏洞扫瞄；和<br>更新开放网上应用系统安全项目(OWASP) 10大漏洞 | 1,6,A-2 | 1.1 | 2021年6月 |
| 2 | 更新参考标准；阐述在攻击前阶段收集资料的方法 | 2,11,A-1 | 1.2 | 2023年12月 |
| 3 | 将「政府资讯科技总监办公室」更改为「数字政策办公室」 | | 1.3 | 2024年7月 |

# 目录

# 1. 简介

按照《信息技术安全指南》，政策局 / 部门需为所有面向互联网的网站及网上应用系统最少每两年一次或在推出前，以及在重大提升或改动前，进行安全漏洞扫瞄及 / 或渗透测试。所有部署在与互联网连接的系统和关键信息系统的服务器和相关装置都应受到严格的安全漏洞管理，例如所有已知的安全漏洞应在安全修补程序发布后一个月内修复，并应每年为该等系统进行安全漏洞扫描或渗透测试。本实务指南旨在协助政策局 / 部门考虑及计划开展渗透测试。政策局 / 部门亦应根据安全风险评估的结果而进行渗透测试。

## 1.1 目的

本文件的目的在于提供渗透测试的一般常识及良好作业模式。本实务指南简述进行渗透测试所需的重要概念，包括渗透测试的定义及限制、界定测试范围及所需要求时的考虑，以及进行测试前、测试中及测试后需注意的主要工作。本文件主要为涉及规划或进行渗透测试的人员而设。

本文件提供渗透测试的概览以及涵盖以下主题：

a) 渗透测试概览；
b) 渗透测试过程；
c) 渗透测试工具；以及
d) 渗透测试员的遴选准则。

## 1.2 参考标准

以下的参考文件为本文件在应用上的参考：

- 香港特别行政区政府《基准信息技术安全政策》（S17）
- 香港特别行政区政府《信息技术安全指南》（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
- 中华人民共和国国家标准《信息安全技术 信息安全风险评估方法》，GB/T 20984-2022
- 中华人民共和国国家标准《信息安全技术 信息安全风险评估实施指南》，GB/T 31509-2015
- 中华人民共和国国家标准《信息安全技术 网络安全漏洞分类分级指南》，GB/T 30279-2020

## 1.3 术语及惯用词

本文件将会采用《基准信息技术安全政策》和《信息技术安全指南》内所使用及以下的术语及惯用词。

| **缩写及术语** | |
|---|---|
| 无 | 无 |

## 1.4 联络方法

本文件由数字政策办公室编制及备存。如对本文件有任何意见或建议，请寄往：

电邮： it_security@digitalpolicy.gov.hk

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

CMMP 电邮： IT Security Team/DPO

# 2. 渗透测试概览

## 2.1 什么是渗透测试

渗透测试是一种安全评估方法。测试会进行漏洞评估，并查证攻击者是否能成功利用系统漏洞进行攻击。它是一个手动程序，而且需要运用专业知识去设计测试用例，以及选择适当的技术或工具，以识别自动化工具不能找出的逻辑漏洞。使用漏洞扫瞄及其他自动化工具通常能帮助渗透测试员减少重复工作。

在渗透测试的过程中，一般会先使用自动化工具来扫瞄网络或系统，以建立已连接工作站及服务器的网络地图，以及识别潜在风险。由于扫瞄过程通常会产生大量测试用例和网络通讯，系统可能因而在渗透测试过程中不能操作。扫描漏洞后，渗透测试员将利用扫描结果作进一步测试。

渗透测试能帮助找出系统的弱点及漏洞，它能模拟出多个攻击方法及让它们同时进行，从而测试攻击会否成功影响系统。渗透测试后，就能知道现行安全控制是否对主动及具丰富经验的攻击者有效。渗透测试结果将有助系统拥有者推行针对安全风险的防护措施。

渗透测试前应先谨慎考虑及计划。由于进行渗透测试需要非常专业的知识及丰富的经验，因此测试应由合资格的安全专家进行。

### 2.1.1 渗透测试目标

渗透测试是一种安全评估方法。根据测试的目标，它可以用不同方式及不同技术进行。政策局 / 部门应界定自己的渗透测试范围及目标。以下列出部份渗透测试目标的例子：

a) 识别信息资产的风险；
b) 识别难以透过自动化网络或应用系统漏洞扫瞄软件侦测的漏洞，例如防火墙的安全政策设定逻辑、编写在程序内的定时炸弹和后门等；
c) 测试及验证安全防护及控制的效率；
d) 测试防御机制对攻击的侦测及应急能力；
e) 评核防火墙及路由器等网络安全装置的效能；以及
f) 展示系统在抵御真实网上攻击时的表现。

### 2.1.2 渗透测试方式

渗透测试可以按不同的测试目标，以不同方式进行。测试可以在外部网络或内部网络内进行。

a) 外部测试是较常用的方式。测试涉及全面分析机构外部可见的服务器及装置（例如路由器、防火墙、电邮服务器及网页服务器等）。外部测试的目的是辨识网络、系统及应用系统的潜在安全弱点，并示范存在的已知漏洞可被外部攻击者利用。测试亦帮助检查系统是否能够安全防范被入侵、资料损失或外泄。

b) 内部测试于内部网络进行，假设攻击者成功穿越安全防线，或攻击者是机构内部人士。这种测试方式焦点集中在机构内部资源，例如非军事区、内部网络、系统程度的安全、应用系统和服务配置和认证，以及访问控制。内部测试是用来识别个别网络内的计算机系统弱点，以及检查是否有人可以透过滥用用户权限而访问网络内的系统。

无论是外部或内部网络渗透测试，都可以以白盒、灰盒或黑盒方式进行。以下介绍这几种方式：

i) 白盒测试：
对受测系统的内部结构、设计及推行有全面认知的情况下进行测试

ii) 灰盒测试：
对受测系统的内部结构、设计及推行有部分认知的情况下进行测试

iii) 黑盒测试：
对受测系统的内部结构、设计及推行没有任何事前认知的情况下进行测试

若渗透测试的目标是尽量找出安全漏洞，就应采用白盒测试，透过分享程序源码或配置等信息，让测试员可以直接进行分析。另一方面，若测试目标是评核安全部署的效能，则应采用黑盒测试，并保留信息以获取较真实的测试结果。

黑盒测试比白盒测试较消耗时间，及需要更高成本去收集及探索系统资料，更有可能会遗漏测试部分安全范畴。然而，黑盒测试能够模拟一个外来攻击，模拟尝试入侵系统的真实情景。另一方面，白

盒测试可以缩短渗透测试的时间，并因为已向白盒测试员提供全部资料，例如网络布局文件、资产清单，以及应用系统设计资料等，因此测试员能够进行更全面的安全评估。

### 2.1.3 渗透测试技术

渗透测试会使用一系列的技术，以下列出当中最常见的：

a) 被动式研究：
从公众网域来源，例如域名系统记录及域名注册管理机构，收集机构的系统配置资料 ；
b) 操作系统扫描及蒐集网络布局的信息：
辨识整个受测网络的配置；
c) 网络窥窃：
窃取流经网络的通讯数据；
d) 伪冒：
将一台机器伪装成合法机器以窃取信息；
e) 特洛伊木马攻击：
透过如电邮附件等不同方法，于被入侵系统内安装特洛伊木马和恶意软件以访问有用资料；
f) 暴力攻击：
破解密码以获得系统或应用系统的访问。这是一个广为人知的破解密码方法，或是一种用来使系统超出负荷，使系统不能正常回应请求的攻击手法；
g) 漏洞扫瞄：
探索安全系统或应用系统的弱点以作出进一步攻击；
h) 社交工程：
蒐集机构的重要信息。攻击者经常以机构员工作为目标，尝试收集敏感信息；和
i) 翻检垃圾箱：
透过仔细检查垃圾以找寻机构的资料，可以是实体渗透测试的一部分。

## 2.2 渗透测试对漏洞扫瞄

漏洞扫瞄与渗透测试经常被混淆，而两者亦经常被交换使用，但两者实际上是有分别的。渗透测试通常但并不一定包括漏洞扫描。因此，机构必须在其服务规格中清楚列明这两项要求，以便进行更彻底的测试。

***漏洞扫瞄员对渗透测试员***

漏洞扫瞄利用标准测试用例，能有效找出潜在的已知漏洞，如错误配置、核心缺陷、缓冲区溢满、输入验证不足、及错误的档案和目录权限等。

另一方面，渗透测试员需要利用本身的技能及经验去理解系统流程，并设计出个别测试用例去找出系统的逻辑漏洞。除此之外，渗透测试员亦会尝试利用扫瞄中找出的漏洞，尝试可以取得甚么类型的数据。

***漏洞扫瞄结果的处理***

漏洞扫瞄是用来测试系统是否存在弱点，而扫瞄过程牵涉辨认、排名及汇报漏洞等程序。但测试用例的结果却不能解释为漏洞是否真的为系统带来威胁。因此，漏洞扫瞄结果只被用作系统潜在攻击威胁的基线指标。

相对地，渗透测试员通常利用漏洞扫瞄的结果决定是否需要进行额外测试，以识别自动化工具不能辨认的漏洞。此外，渗透测试会部署更具体的方法来显示如何利用漏洞或如何重复测试结果。简而言之，渗透测试比漏洞扫描产生更全面的结果。

***技能***

漏洞扫瞄利用不同的自动化工具及测试用例去辨认已知的技术漏洞。渗透测试过程涉及大量尝试，而且亦非常倚重测试员的技能。

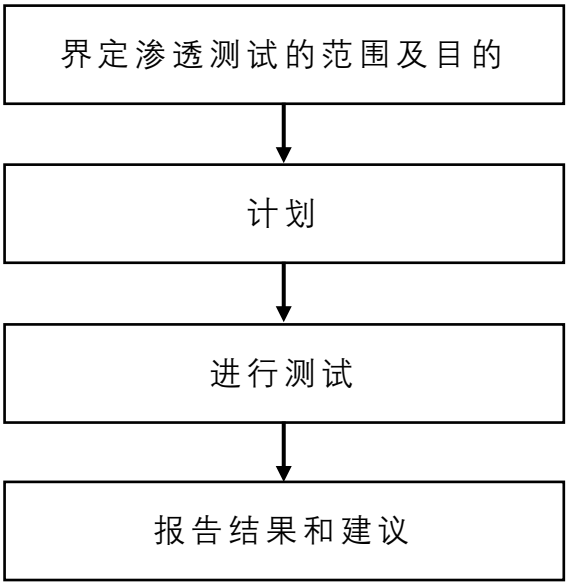
***过程所需时间***

漏洞扫瞄是使用自动化工具，因此扫瞄过程很快在很短的时间内（例如数小时）完成。可是，漏洞扫瞄同时会产生更多假阳性结果，因此需要核实结果。相对地，渗透测试是一个手动程序。通常会根据漏洞扫描结果来进一步识别系统中的漏洞。因此它通常需要比漏洞扫瞄更多的计划和较长时间完成。

# 3. 渗透测试过程

## 3.1 渗透测试步骤

渗透测试虽然可以有不同类型，但在测试前后都应进行一些相同步骤。测试一般可以分为以下步骤：




渗透测试步骤

## 3.2 界定渗透测试范围及目标

系统安全由不同范畴组成，并可以应用不同类型的渗透测试。以下列出最常见的范畴：

a) 网络安全：

这会识别全部有可能的网络缺陷，并模拟对已识别的漏洞作出真实攻击；

b) 系统软件安全：

这会识别全部有可能的系统软件缺陷，并模拟对已识别的漏洞作出真实攻击；

c) 客户端应用系统安全：

这会主要集中在客户端功能上，识别全部有可能的应用系统缺陷，并模拟对已识别的漏洞作出真实攻击；

d) 服务器端应用系统安全：

这会主要集中在服务器端功能上，识别全部有可能的应用系统缺陷，并模拟对已识别的漏洞作出真实攻击；

e) 实体安全：

这会获取机构资源的访问（如办工时间前、中，及后的数据中心）。通常会对所有实体安全控制进行测试；

f) 入侵侦测：

这一般会使用软件工具，测试入侵侦测系统的强度；以及

g) 事故应急：

这会测试事故应急程序是否妥善，以及事故或紧急应急小组的准备程度。

政策局／部门应首先根据业务需要、所要达成的目标，以及手上的资源，界定渗透测试的范围及目标，然后可以决定需要进行什么类型的渗透测试。渗透测试范围可以按以下因素而决定：

a) 应用系统、网络装置、服务器的规模及数量。例如：只测试应用系统，或是包括所有服务器，又或是涵盖整个网络架构；
b) 需要进行内部或外部渗透测试，或是两者皆需要进行；以及
c) 需要进行白盒、灰盒或黑盒测试，或是需要进行混合测试。对于灰盒及白盒测试，政策局／部门需要按「有需要知道」原则提供资料，以协助达成渗透测试的目标及目的。

## 3.3 计划

开始渗透测试前，需要先计划测试以作适当准备、监察及控制。渗透测试员应在进行测试前，准备及提交渗透测试计划（就渗透测试计划范本样本，请参阅附件 C）。渗透测试计划应包括，但不限于下列各点：

a) 范围；
b) 目标；
c) 时间表；
d) 持份者的角色及责任；
e) 测试方式及方法；
f) 测试工具；以及
g) 回退及复原程序。

政策局/部门需要与渗透测试员共同制订测试时间表，并就渗透测试环境上（例如生产、生产前或用户验收测试）达成共识。但由于部分渗透测试技术会测试有实际漏洞的应用系统、系统或网络，因而影响系统的可用性，令敏感资料曝光，因此应尽量避免在生产环境内进行测试。另一重要事项是要记录及订立测试程度，而该测试程度应得到双方同意。一旦测试超出某个程度，例如获得个别系统访问时，就停止测试，以免对系统或数据造成伤害。

进行渗透测试前，需遵从下列作业模式：

a) 政策局/部门应向渗透测试员提供系统拥有人及受测系统的信息技术管理员的联络名单，以便尽早报告任何在测试期间内发生的问题；
b) 政策局/部门应取得渗透测试员的联络名单，以便政策局/部门能在需要时迅速终止所有测试；
c) 政策局/部门应考虑是否需要暂停或修改可能影响渗透测试结果的现存安全控制设定（例如入侵防御系统、网上应用系统防火墙等），避免测试受到影响；
d) 政策局/部门应在进行渗透测试前通知及提醒安全监察服务供应商，除非测试目标包括评核安全监察服务供应商的监察效能；
e) 政策局/部门应考虑为渗透测试员提供测试凭证，以有效测试应用层的功能；
f) 政策局/部门应确保存有受测系统的最新完整系统备份，在系统数据完整性受到影响的情况下，可用作复原系统；
g) 政策局/部门应屏蔽所有涉及保密资料及个人资料的测试数据；
h) 政策局/部门应安排于非繁忙工作时间进行渗透测试；以及
i) 政策局/部门应要求渗透测试员签署保密协议书，以保障私隐或系统数据的机密性。

## 3.4 进行测试

一般而言，应用系统、系统或网络的渗透测试牵涉三个阶段：攻击前、攻击中，及攻击后。

### 3.4.1 攻击前

攻击前阶段着重于蒐集针对为目标的应用系统、系统或网络的资料。除非使用白盒方式，否则初步将会使用侦察方法以查找、收集、鉴定及记录受测试的应用系统、系统或网络的资料，其目的是在以不同途径尽量发掘资料，用以制订或辅助攻击。侦察可以分为主动及被动两类型。被动侦察在不主动的情况下收集受测试应用系统、系统或网络的有关资料。这包括从公开来源，例如互联网上的云端平台和开源资料库，收集相关数据。渗透测试员亦可能需要检视系统，以理解其商业逻辑。主动侦察会直接参与受测试应用系统、系统或网络，透过自动化工具，例如漏洞扫瞄工具、网络窥窃工具，以扫瞄端口、扫瞄网络和列举用户帐户等方式试探目标。攻击前阶段所收集的资料可以是：

a) 网络注册资料，例如域名、注册人姓名及电邮地址；
b) 域名系统及电邮服务器资料，例如域名系统名称及电邮服务器名称；
c) 操作系统资料：例如操作系统类型及版本；
d) 认证及凭证资料：例如目标系统的用户登入名称及密码；
e) 联络资料：例如机构联络人及电话号码；
f) 网站资料：例如网站划一资源定位器、互联网协议地址及程序源代码；以及
g) 其他可以帮助测试目标应用系统、系统及网络的资料。

蒐集有关资料后，漏洞扫瞄工具会自动开始进行漏洞分析，将从应用系统、操作系统及网络所收集的资料与漏洞数据库比较，或根据渗透测试员对漏洞的知识进行漏洞分析。手动程序能够辨认假阳性扫瞄结果和自动化扫瞄工具可能遗留的新漏洞，但需要较多工夫和时间。

### 3.4.2 攻击中

根据渗透测试的范围和目标，测试员应决定最适合的方式、工具或技术，在攻击阶段进行渗透测试。这是一个手动过程，需要技巧和

经验去决定特定的测试用例及选择适当技术或工具去识别系统缺陷。可使用漏洞扫瞄工具或其他自动化工具辅助，为渗透测试员提供系统潜在攻击漏洞的基线。

此攻击阶段通常需要透过尝试利用攻击前阶段所找到的漏洞，对应用系统、系统及网络作出实际破解。这阶段一般牵涉三个主要活动：获得访问、提升权限，以及安装额外工具。

测试员会首先尝试取得受测试系统的访问，成功后会访问系统或应用系统以进行漏洞攻击，例如结构化查询语言插入、系统数据修改等。此外，测试员亦会尝试将用户权限提升，以访问更多敏感资料，亦会在可行的情况下，于目标系统安装额外软件或工具，以作出进一步的攻击或利用更多漏洞。

在攻击阶段中，渗透测试员应设计针对系统的测试用例，并记录测试方法（即是如何可以重新制造相同的成功破解）及收集证据，以准备渗透测试报告。若发现会影响现行系统的严重漏洞，渗透测试员应详细记录如何导致该严重漏洞，并立刻通知负责人士。

### 3.4.3 攻击后

攻击后阶段包括清理测试环境、将系统回复至测试前的状态，以及获取成功攻击的日志记录作证明。以下列出一般于攻击后阶段进行的活动：

a) 取得相关日志记录作为测试证明；
b) 清理所有曾上传至测试系统的档案；
c) 移除所有在测试过程中产生的档案；
d) 删除测试过程中新增的任何用户帐户；
e) 解除所有已安装于测试系统内进行测试的工具；
f) 回溯所有用户权限及设定的改动；以及
g) 会复系统或应用系统的配置或设定。

渗透测试员需要记录及向负责人士披露在测试过程中对相关环境所作出的任何改动。测试员或负责人士需要将目标环境复原至测试前的状态。

附件 A 及 B 分别附上对网上应用系统及信息技术基础设施进行渗透测试的例子，示范如何将上述三个阶段应用在渗透测试上。

## 3.5 报告结果及建议

渗透测试后须提交渗透测试报告。（于大部份情况下，会有一个渗透测试简报会，解释报告细节。）渗透测试报告应详细记录已进行的测试活动、发现及相关建议，报告内容应包括，但不限于下列各点：

a) 执行摘要：
渗透测试范围、目标及发现的高层次摘要；

b) 项目范围：

详细描述受测试应用系统、系统或网络范围；

c) 测试方法：

详细描述用来完成测试的方式及方法；

d) 曾使用的工具；

e) 限制及约束：

详细描述推行在测试上的所有限制，例如规定测试时间，及对旧有系统的特殊测试要求等；

f) 测试活动：

详细描述已进行的攻击活动；

g) 发现及相关建议：

详细描述所发现的漏洞、漏洞风险排名、针对每个漏洞进行过的攻击、攻击结果、能支持所发现的证据，以及减低风险的建议；以及

h) 渗透测试后的环境清理：

详细描述及指示如何进行清理，以及如何核实安全控制已获回复。

验收渗透测试项目前，政策局 / 部门应核查：

a) 已签妥及递交保密协议书；
b) 服务供应商或渗透测试员已完成所有必须的攻击后工作；
c) 已推行所有在工作简介中指明的项目要求；以及
d) 提供足够及正确的细节于已提交的报告（如渗透测试报告及渗透测试计划）。

## 3.6 后续行动

接收渗透测试报告后，重要的是政策局 / 部门应在测试后于合理时间内跟进修补方案内的项目。

渗透测试结果未必都能全面识别每个漏洞情况，例如在程序内发现一个跨网址指令码，未必表示同一漏洞不会在其他范围内出现。政策局 / 部门应小心调查这些存在的漏洞，以确保所有漏洞都被修补方案处理。

进行修补后，政策局 / 部门应安排重新测试，证明新实行的措施能减低原有风险。

# 4. 渗透测试工具

渗透测试工具能够协助渗透测试员和改善渗透测试效率。由于有不同的渗透测试范围，例如网络、应用系统及入侵侦测系统等，因此亦有不同种类的渗透测试工具为进行特定测试而设。渗透测试工具通常满足两个主要目的：

a) 收集目标系统 / 应用系统的资料；以及
b) 按特定漏洞进行攻击。

部分渗透测试工具可以用来辨认现存于应用系统、网络，或个别主机（主机为本）的漏洞，以及发动攻击。而另一部分则是设计来进行漏洞扫瞄，但不能进行攻击。

具蒐集网络布局功能、窥窃网络及扫瞄漏洞的工具经常会被利用于网络渗透测试中，去探索以下资料：

a) 网络布局；
b) 活跃服务器及网络装置；以及
c) 操作系统类型、在活跃服务器和网络装置上运行的应用系统和服务。

当发现与信息技术基础设施有关的漏洞后，就能以手动方式或利用具攻击能力的自动化渗透测试工具发动附件 B － 信息技术基础设施的渗透测试内所提及的攻击。

网上应用系统的渗透测试会通常使用具下列功能的工具收集资料及识别漏洞：

a) 截取代理：

   检查及修改浏览器和目标应用系统间的超文本传输协定通讯；

b) 网上应用系统蜘蛛：

   抓取网上应用系统的内容和功能，以发现被遗漏或隐藏的网页内容，从而提供应用系统内容的全面描述；以及

c) 网页漏洞扫瞄：

   发掘应用系统漏洞。例如结构化查询语言插入、跨网址程序编程及目录游历等。

在收集资料及识别应用系统相关的漏洞后，渗透测试员可以利用其结果判断是否需要进行额外测试。进一步的攻击可以以手动方式或利用自动化渗透测试工具发动，以测试附件 A － 网上应用系统的渗透测试内提及的常见的严重网上应用系统漏洞。

渗透测试工具应根据下列选择：

a) 渗透测试类型。例如网络渗透测试或应用系统渗透测试；以及
b) 渗透测试员的取向或专业判断。

渗透测试可使用市场上的工具及渗透测试员自己开发的工具来进行。

# 5. 渗透测试员的遴选准则

合资格的渗透测试员应拥有相关证书及工作经验以进行渗透测试。

准候选渗透测试员所持的认证可能显示技能级别及能力。以下是部分常见渗透测试认证：

a) 注册网络安全渗透评估专业人员（NSATP-A）；
b) 道德骇客认证（CEH）；
c) 注册信息安全专业人员渗透测试工程师（CISP-PTE）；
d) 注册信息安全专业人员渗透测试专家（CISP-PTS）；
e) CREST 渗透测试证书；
f) 全球信息保证认证（GIAC）证书；以及
g) 攻击型安全师专业认证（OSCP）证书。

除了渗透测试员所持的认证外，亦应根据以下渗透测试员的工作经验细节，以决定渗透测试员是否合资格参与渗透测试项目：

a) 渗透测试员在渗透测试的工作年资（注意：所需年资没有特定的限制。为确保渗透测试员拥有足够经验进行测试，建议选择较高年资的）；
b) 对目标环境的认识和相关的工作经验（即是包括操作系统、硬件、网上应用系统、网络服务及协议等）；以及
c) 曾经进行类似的渗透测试范围项目的次数。

# 附件 A：网上应用系统的渗透测试

网上应用系统渗透过程

要进行网上应用系统渗透测试，就涉及以下三个阶段。

攻击前阶段

网上应用系统渗透测试在攻击前阶段会进行：

a) 收集资料，例如网站地图或应用系统的划一资源定位器；
b) 分析其功能、核心安全机制例如应用系统的会话管理和访问控制；以及
c) 识别网上应用系统所采用的技术。

目的是要找出应用系统所曝露的攻击面，以及设计辨识应用系统漏洞的方法。

在过程中通常会使用自动化网上应用系统扫瞄工具。由于大部分网上应用系统漏洞都有个别识别特征，自动化的网页扫瞄工具能够在操作系统层面上侦测已知的漏洞，例如已过时的软件版本、遗漏的安装修补程序、缓冲区溢满，及错误配置等。扫瞄工具亦能够侦测部份应用层的漏洞，例如小型文本文件（cookies）问题、跨网址程序编程、目录遍历及结构化查询语言插入等。一般而言，自动化网上应用系统扫瞄工具为渗透测试员提供潜在漏洞和攻击方法的基线。渗透测试员可以利用扫瞄结果决定是否需要额外的测试：

a) 收集应用系统的基本资料，例如操作系统类型、应用系统服务器版本、网页服务器版本等。亦会浏览所有网页、目录，并为所有构成网上应用系统的档案建立索引；以及
b) 识别应用层面的漏洞，例如小型文字档案问题、目录遍历及结构化查询语言插入等。

可是，以下部分常见漏洞并没有标准识别特征，因而不能被自动化工具侦测：

a) 弱访问控制，例如某用户可以访问其他用户的资料，或低权限的用户能够访问管理功能；
b) 应用系统功能设计上的缺陷，例如弱密码规则，或在登入失败讯息中列出用户名称；
c) 敏感资料外泄，例如网上应用系统回应被用作漏洞分析及检查，或敏感资料（如程序源代码或配置文件）被上载至向公众开放的代码存管平台；

d) 修改对应用系统有特殊意义的参数，例如，漏洞扫瞄工具并不能知道隐藏栏的意义；以及
e) 会话管理的缺陷。

攻击阶段

经研究漏洞扫瞄所得出的结果后，渗透测试员应检视受测试的网上应用系统及测试其功能，然后设计特定的测试用例及根据自己的专业判断和经验寻找可能的漏洞。

渗透测试员可以利用截取代理修改浏览器和应用系统之间的超文本传输协定通讯以进行测试。自动化工具或手动技术都可以用来发动攻击，例如结构化查询语言插入、修改系统数据、提升用户权限，或如可行的话，安装额外软件或工具，以发动进一步的攻击或利用更多漏洞。

攻击后阶段

一如其他类型的渗透测试，网上应用系统渗透测试在攻击后阶段包括清理测试环境、复原系统或配置至测试前的状态、获取成功攻击的日志记录作证明，以及解除安装任何曾作测试用途安装的软件。

开放网上应用系统安全项目 （OWASP）10 大漏洞

开放网上应用系统安全项目是一个网上社群。它曾发表一系列最严重的网上应用系统缺陷。这些缺陷经常在网上应用系统上发生，亦很容易被找到及被利用。政策局 / 部门应确定渗透测试范围包括所有已知最严重的漏洞。以下列出 2013 年度 OWASP 10 大漏洞：

a) 代码插入；
b) 有缺陷的认证；
c) 敏感资料曝光；
d) XML 外部实体 (XXE)；
e) 无效的访问控制；
f) 错误安全配置；
g) 跨网址程序编程(XSS)；
h) 危险的反串行化；
i) 使用已知有漏洞的组件；以及
j) 不足的记录和监察。

# 附件 B：信息技术基础设施的渗透测试

信息技术基础设施渗透过程

这里的信息技术基础设施渗透测试局限于利用网络安全装置和服务器，如防火墙、路由器、网页服务器、应用系统服务器及数据库服务器等的现存漏洞。要进行信息技术基础设施渗透测试就需要经过三个阶段：攻击前、攻击中，及攻击后。

攻击前阶段

在攻击前阶段，信息技术基础设施渗透测试一般会进行以下工作：

a) 网络探索：
   可以使用被动式或主动式的技术去探索活跃的和有回应的网络装置及服务器，借此了解网络布局。被动式的技术以网络窥窃工具监察网络通讯，并识别使用中的互联网协议地址和端口，以及活跃的网络装置和服务器的操作系统。主动式的技术透过自动化工具传送不同类型的网络小包，例如互联网控制讯息协议，向网络装置及服务器要求回应；
b) 网络端口及服务识别：
   基于在网络探索过程中找到的互联网协议地址，便可使用扫瞄工具找出活跃的网络装置及活跃的服务器的网络端口、服务、应用系统及执行中的服务。透过称为操作系统指纹套取、服务识别，及标志获取的过程，端口扫瞄能相应地分别辨识操作系统种类、在网络装置及活跃的服务器上执行的应用系统以及应用系统版本；以及
c) 漏洞扫瞄：
   端口扫瞄工具可以识别活跃的装置、操作系统、端口、服务及应用系统，但不能辨认漏洞。自动化漏洞扫瞄工具会尝试基于网络端口及服务识别过程中收集的资料识别漏洞。扫瞄工具可以将已收集的资料和扫瞄工具内漏洞数据库的已知漏洞资料作比较，来辨认已过时的软件版本、遗漏安装的修复程序及错误配置。

这些的目的是要识别服务器、网络装置和网络环境所曝露的漏洞，并设计利用这些漏洞的方法。

攻击阶段

漏洞被识别后，就会开始获取目标网络装置或活跃的服务器的访问、尝试利用自动化工具、自己开发的程序或手动方式去提升权限，以及安装额外工具和软件，作进一步的攻击。

攻击后阶段

就如其他类型的渗透测试，信息技术基础设施渗透测试的攻击后阶段，包括清理测试环境、复原系统或配置至测试前的状态、获取成功攻击的日志记录作证明、删除任何测试帐户和作测试用途的档案，以及解除安装任何曾作测试用途的软件。

信息技术基础设施漏洞利用类别

以下列出最常在信息技术基础设施渗透测试中被利用的漏洞：

a) 错误配置：

错误配置装置的安全设定，例如不安全的默认设定；

b) 核心缺陷：

核心编码是操作系统最重要的核心，它是系统的整体安全模型的约束。任何在核心的安全缺陷会成为被利用的漏洞；

c) 不正确的档案和目录权限：

档案和目录权限控制分配给赋予用户及程序对档案访问权。不当的权限会造成许多类型的攻击，例如读取或修改密码档案；

d) 遗漏安装安全修补程序：

遗漏安装安全修补程序会成为用作恶意攻击的漏洞；以及

e) 权限提升：

透过利用系统漏洞尽可能获取最高管理权限，进一步访问整个网络及敏感资料。

# 附件 C：渗透测试计划样本

a) 范围

这节列明项目的范围、已测试的互联网协议地址资料、所进行的渗透测试类型（如应用系统或网络），以及其他会影响项目所需的时间及预算的资料。

b) 目标

这节提供一些目标，当政府部门在得知渗透目标的互联网地址 / 系统或应用系统相关的风险及在实行渗透测试的建议，并减低这些风险后将会带来的好处。

c) 时间表

这节提供渗透测试的开始及结束日期，为目标受众提供以下资料：

- 测试期限
- 只在这测试期限内，从渗透测试观点的已测试互联网协议地址的风险
- 若在这测试期限后，因目标系统有所变动而带来部分风险，渗透测试员无需为此负上任何责任

d) 持份者角色及责任

这节列出持份者在渗透测试内的工作。

e) 测试方式及方法

这节提供有关渗透测试进行的方式、收集和分析资料所应跟从的步骤、计算每个漏洞个案风险排名的方法等。

f) 使用工具

这节提供渗透测试员在每个渗透测试阶段中使用过的工具资料。

g) 回退及复原程序

这节提供持份者在渗透测试期间应该采取的回退及复原程序。