軍事演習 - 資安篇

森美力 (Samiux) 編著

二零一七年九月十九日　第一版
二零一八年九月九日　　修訂版
二零一八年十月廿九日　修訂二版

本書是在安卓 (Android) 手機利用 Google Docs 軟件完成。頁面是 B5 大小。

本書是免費版本，可以在我的個人網站 (https://www.infosec-ninjas.com) 下載。歡迎在你的親戚朋友之間轉閱，更歡迎將其翻譯成其他國家語言。

雖然是免費版本，但版權仍然歸於本人。

目錄

前言

軍事演習時，我軍會有分紅隊 (Red Team) 及藍隊 (Blue Team) 。紅隊是作出攻擊隊伍，而藍隊就是防守隊伍。紅隊被要求在特定的時間和規定下，令藍隊的防守崩潰來達致任務成功，而藍隊就要極力阻止紅隊的攻擊成功，目的是同時測試其軍事單位的攻擊及防守能力。

最近幾年，有很多知名美國機構的網站相繼被入侵，而美國法院亦向那些被入侵網站的機構作出巨額罰款，理由為未能妥善保護其網站免受被入侵攻擊而做成大量資料洩露。同時於二零一七年中旬，英國亦正在草擬相關法例利用巨額罰款來懲罰那些未能妥善保護其網站或網絡的機構。相信世界各國相繼亦會步其後塵。

中國國內及國外有很多機構都有其自家的藍隊，有的更擁有紅隊。有的更會聘請第三方對其網絡及網站作出攻擊來測試其系統的安全程度。不論是自家的或聘請第三方的方式，這些演習就是「滲透測試」 (Penetration Test)。

大慨在二零一七年中旬，中國香港才出現資訊科技安全人員的招聘廣告，但只是集中在銀行業和海外的大型企業。雖然香港沒有相關法例來懲罰被入侵者，但是一個安全的網絡系統可以令企業的業務發展蒸蒸日上，相反它可能令你的企業聲譽一敗塗地。

作為機構的掌舵人或部門主管，如果能清楚了解其網絡系統的安全程度，而作出適當的資源投放，可以有助機構的業務發展。

本書將會討論如何做到網絡攻防演習，從認識演習到其好壞處上都會討論到。希望各位閱讀後有所得益和啓發。

雖然，本人力求做到盡善盡美，但其中難免有所錯漏，歡迎讀者指正與交流！

森美力 (Samiux) (網名)
寫於二零一七年九月十八日，中國香港

關於作者

森美力 (Samiux) (網名) 是一名資訊科技安全 (Information Security, InfoSec) 愛好者，他擁有由美國 Offensive Security 發出的 OSCE (Offensive Security Certified Expert)，OSCP (Offensive Security Certified Professional) 及 OSWP (Offensive Security Wireless Professional) 專業認證。他對網絡攻擊有深入認識，了解惡意黑客的行為。他是一名黑客，但並不是惡意黑客，嚴格來說，讀者可以稱他為灰客 (Grey Hat，灰帽子)。他的格言是「未知攻，焉知防」。

他曾在警隊服務，具有多年刑事偵緝經驗，對罪犯行為心態略有研究。

他是 Linux 系統的愛好者，他喜歡使用 Ubuntu Linux。

他擁有多個活躍的資訊科技安全研究項目，例如防禦入侵系統，匿名瀏覽系統，高安全性網頁伺服器設定，「抓我吧，若果你有能力的話」系列，人工智能網頁防火牆等。他也是一名博客 (Blogger)。他閒時會編寫程式及閱讀，他更會在其滲透測試 (Penetration Testing) 實驗室中作實驗時而自得其樂。他有建設同時亦有破壞。

他的其他著作有「武裝自己 - 資安篇」及「知彼知己 - 資安篇」。

讀者可以在這裡接觸他 ：

(1) 其博客 - https://samiux.blogspot.com
(2) 其網站 - https://www.infosec-ninjas.com
(3) IRC freenode - #infosec-ninjas

關於本書

在寫作本書時，我考慮到一般的電腦書籍都因為軟件與硬件的更新，而令書中所描述的題材和內容脫節。所以我想寫一本較為長春的書籍。並且會用較為深入淺出的書寫方式去完成。

本書主要論述的是如何從認識網絡攻防演習來認識自己系統的弱項，而達到有備而戰的境地，從而做到每戰不殆。

本書對象

讀者不需要具有任何資訊科技安全知識。本書是寫給那些機構掌舵人或部門主管及對資訊科技安全領域有興趣的讀者。

致謝

出書是個浩大的工程項目，在本書寫作其間，經常遇到很多困難，經過數天時間的努力才完成。借此機會感謝所有使本書能夠順利出版及提供幫助的專家及朋友。

特別感謝我女友在背後的支持。感謝我的家人和朋友，你們為我付出很多！

在此，我要感謝活躍在網絡上的資訊科技安全專家們，你們的公開文章和技巧讓我學到了很多優秀的技術。

聲明

第一章　漏洞評估

大多數有規模的大型機構都會有自己的審計部門 (Audit)，而有關資訊科技的範疇就交由有關的資訊科技安全審計部門處理。他們會對所有網絡系統設備和軟件作出定期的審計。

當機構完成網絡系統配置、加添或軟件開發，大部份有規模的機構的審計部門都會對其系統或軟件進行漏洞評估測試 (Vulnerability Assessment)。大部份的漏洞評估是利用價格昂貴的漏洞掃描工具來進行評估。當掃描後發現有漏洞警報 (Alert)，他們會將其修復，然後再進行另一次掃描直至沒有漏洞被發現為止。

這樣的話，所有已知的漏洞和比較低檔次的漏洞將會被發現。但較為高檔次的漏洞就不容易被發現了，例如系統的錯誤配置。

但當網絡系統設備的添加或應用程式軟件功能越來越複雜，漏洞掃描工具並不能夠完全確保其被掃描的系統或軟件的真正安全性。

有時漏洞掃描工具有可能誤報 (False Positive) 有漏洞發現，而機構內的員工又沒有足夠能力去証實其所警報的是誤報與否。這樣就會對系統管理員或開發人員做成很多的困惑，或與審計部門做成衝突，形成對立的境地。

通常來說，所有不能夠被利用 (Exploit) 的所謂漏洞並不視為漏洞，它們都被視為誤報。

漏洞評估只用於機構認為自己的網絡系統或軟件不安全時使用的，它的好處是自動化。但有相當高的誤報率，尤其是處理網站的時候。再者，大多數的掃描工具並不能處理受網頁防火牆保護的網站。

第二章　滲透測試

當軍事演習時，我軍會分成兩隊，一隊是藍隊 (Blue Team)，另一隊是紅隊 (Red Team)。藍隊在演習時的主要工作是極力阻止被紅隊攻破，而紅隊的主要工作是想盡辦法去攻陷藍隊。演習目的是要測試攻防能力。

在一些有規模的機構內的資訊科技安全部門會有自己的藍隊，有的更有其紅隊。目的是方便自己進行攻防演習，從而加強網絡系統和網站的安全性。有的更會聘請第三方作出攻擊，這樣的所謂演習就是「滲透測試」(Penetration Test) 了。

滲透測試會在特定的時間和規定內完成，所以其得出的結果有其局限性，不似惡意黑客有無限時間和沒有規則。滲透測試不似漏洞評估主要使用掃描工具作業，它是由滲透測試員去發掘那些潛在的漏洞和入侵點。所以不同的測試員所測試的結果會有可能不盡相同。有豐富經驗的滲透測試員是有能力繞過防火牆、網頁防火牆、防禦入侵系統等。所以有的有足夠資源的機構更會聘請多於一隊的紅隊進行滲透測試。

其實，滲透測試員就是白帽子 (White Hat) 或灰帽子 (Grey Hat)，他們是沒有惡意的黑客。他們會在書面同意下向聘請者的機構網絡系統和網站進行滲透測試，這樣的攻擊和入侵就視為合法了。

滲透測試盡可能在一個極之安全的環境下，在不影響機構的網絡系統和網站運作的大前提下進行，有的範圍、攻擊方式或情況是不能夠作出測試的。所以滲透測試並不能完全反映機構網絡系統和網站的真實安全程度，但它有其一定的代表性。

滲透測試是當機構認為其網絡系統和網站相當安全時才進行的。若果懷疑自己的系統不安全是不適宜進行滲透測試，這只會浪費金錢和時間及人力物力，而是應該進行漏洞評估測試。建議每年最少進行滲透測試一次。

滲透測試的步驟與過程和惡意黑客攻擊大致相同，因為是模擬惡意黑客的攻擊。滲透測試有分黑盒 (Black Box)，灰盒 (Grey Box) 和白盒 (White Box) 測試之分。黑盒測試是在測試前是不知道網絡系統和網站的配置詳細資料，白盒測試是預先知道其配置詳細資料，而灰盒測試就介乎兩者之

間。滲透測試亦有分網外和網內之分。網內是指在機構的網絡內進行，而網外就是在機構網絡以外進行。

所有滲透測試都會經過 ：

(1) 測試目標 (Scope);
(2) 資料搜集 (Reconnaissance) ;
(3) 掃描目標 (Scanning) ;
(4) 漏洞分析 (Vulnerability Analysis) ;
(5) 漏洞利用 (Exploit) ;
(6) 用戶提權 (Privilege Escalation) ;
(7) 後期利用 (Post Exploit) ;
(8) 測試報告 (Reporting)。

測試目標

在進行滲透測試前，受僱的紅隊和機構應該訂立守則，規定受測試的範圍、時間、攻擊方式，那些攻擊手法不可使用等。訂立在測試時出現不能預測的後果時如何應對和處理等。最後便是要書面列明以上的要求，同時要簽署不洩露資料同意書等，以作相方的保障。大多數情況下，藍隊 (或者網絡管理員等) 是不應該知道紅隊在那時作出行動的，目的是要反映比較真實的環境。

資料搜集

如果紅隊對其目標未有足夠的認識和資料，他們會進行資料搜集。資料搜集分為主動式 (Active) 和被動式 (Passive)。主動式資料搜集會在目標處作出搜索，務求得到有價值的訊息。但此等搜索方法會在目標留下大量的足跡，目標 (藍隊) 有可能察覺得到而作出防範而打草驚蛇。

至於被動式，紅隊會在周邊環境作出資料搜集。例如招聘廣告、接觸員工、從互聯網上的搜尋器所得等等。這樣的話，他們幾乎不會留下任何足跡在目標處。有時兩種搜集方式都會同時使用，以求得到最多有價值的訊息，但搜集訊息的時間不會太長。

掃描目標

當紅隊完成了資料搜集後，他們會對目標進行掃描。目的是要找出目標是正在運行那些服務 (Service) 或軟件。掃描亦有分主動式和被動式，主動式是直接向目標進行掃描，而被動式就是經過第三方作出掃描動作。

漏洞分析

當掃描完成後，紅隊會根據掃描所得的資料對目標進行漏洞分析。大多數的時間是分析現有已被發現的漏洞 (Vulnerability)，但有時紅隊會不惜公本去發掘那些零日漏洞 (0day)，目的只求達到入侵目標。

漏洞發掘和開發是需要較高的技術，所以並不是所有紅隊成員都能夠做到。除了漏洞分析外，此階段紅隊有可能發動社會工程 (Social Engineering) 來對付其目標，如果在書面合約上有列明准許的話。

漏洞利用

一但發現目標正在運行或使用有漏洞的服務或軟件，紅隊就會進行漏洞利用 (Exploit)，作出入侵行動。如果目標沒有在防禦措施的保護下，如防毒軟件、防火牆等等，紅隊就會如入無人之境，輕鬆自在地進行入侵。

若果遇有防禦措施，紅隊會想盡辦法去繞過其保護，又或直接關掉其保護機制來作進一步的入侵。

用戶提權

入侵後，若果有漏洞的服務或軟件不是以管理員身份運行的話，紅隊就會利用系統錯誤的設置，又或是利用系統的漏洞進行提升權限，令其得到系統的最高權限。有時並不需要權限提升也可以完成任務。又或者利用社會工程來得到所需權限 (若果容許的話)。

後期利用

當完成入侵行動後，紅隊有可能留下後門 (Backdoor)，以便下次再來時不必大費周章。他們更會在系統內清除所有足跡，以防洩露行蹤。他們會盡力去獲取所有賬戶密碼或其他東西來証明他們成功進入該系統。並且同時入侵網內其他的系統，直至所有系統被入侵和取得有關証明為止。

測試報告

當滲透測試完成後就會寫測試報告，測試報告大致分為三個部份，第一部份是給掌舵人 (Chief Executive Officer, CEO) 或其他高級行政人員，第二部份是給部門主管或資訊科技安全部門主管，而第三部份是給開發人員或資訊科技安全人員的。

第一部份是十分簡潔，一針見血，多以圖表列出受測試系統的安全程度。方便掌舵人作出決定和資源分配。

第二部份是較為詳盡，大慨包含安全程度和風險，更會提出補救方法等。而第三部份就是詳細的入侵報告和証明，有時會加入避免方法等。

更有時如有需要，紅隊會展示如何入侵受測試的系統。

附件一　基本概念

甚麼是惡意軟件?
惡意軟件 (Malware) 具有不良企圖的軟件。例如，病毒 (Virus)，木馬 (Trojan)，蠕蟲 (Worm)，勒索軟件 (Ransomware) 等。其出現形態包括執行檔或腳本 (Script)，如 JavaScript。

病毒有自我複製及感染其他檔案的能力。木馬就是所謂的後門 (Backdoor)。蠕蟲具有滲透能力，即會攻擊下一個目標。勒索軟件可能會具備以上所有特徵及加上將受害者的檔案加密，並要求贖金來解密。

當下幾乎所有網站都有使用 JavaScript 來製作互動網頁。JavaScript 是在瀏覽者的電腦上運行。若果網站被騎劫或者該網站由惡意黑客所建立，在其網頁植入惡意的 JavaScript 的話，受害者多數在不知情的情況下受到感染而被入侵。

甚麼是社會工程？
社會工程 (Social Engineering) 是一種欺騙的手段和技巧。出現的形態可以千變萬化，可以是經電話、電郵、連結、網站及下載等。我們經常聽到的「釣魚」 (Phishing)，就是其中一種。誘使受害者作出或不作出某種行為，而達到目的。

甚麼是中間人攻擊？
中間人攻擊 (Man-In-The-Middle Attack) 是受害者的通訊被脅持，其通訊被脅持者篡改或監聽 (Sniffing)。有時已加密的通訊亦可以被脅持者篡改或監聽。

有時可以在受害者下載或上載檔案時，植入惡意軟件。這的確是防不勝防。

甚麼是漏洞？
漏洞 (Vulnerability) 是指程式設計時在邏輯上或編程上出錯。這可以看作是一個「臭蟲」(Bug)。不是所有臭蟲都是漏洞，不是所有的漏洞都可以被利用 (Exploit)。可被利用的漏洞是可以入侵受害者的系統。

通常漏洞可以經更新而修復。但是在某些情況下，有些系統在有更新的情況下，也不能作出更新，例如若果更新了，系統就會崩潰。

甚麼是密碼強度？
從前的密碼長度建議是八個位，但是因為現今的硬件運算能力非常強大，八個位長度的密碼可以在少於十五分鐘內被破解。

所以我現時建議至少十六個位的長度，其組合包括大細楷英文字母，數目字及標點符號。而且其組合不能有意思或可以被推算得到。

因為這麼長的密碼是非常難記憶的，所以讀者應該要有密碼策略 (Password Policy)。再者，盡可能不要重用密碼。因為只要密碼被洩漏，你的所有賬號就會全軍覆沒。

甚麼是保安設備？
常見的保安設備有防毒軟件及防火牆。但尚有統一威脅管理系統 (Unified Threat Management System, UTM) 及防禦入侵系統 (Intrusion Detection and Prevention System, IDPS) 等。

現在的統一威脅管理系統和防禦入侵系統十分相似。所以在選購時要清楚了解產品的特性和自己的需求。現在更流行一種叫做下世代防火牆 (Next-Generation Firewall)，其實它與統一威脅管理系統和防禦入侵系統相當近似。

甚麼是備份？
備份 (Backup) 是將你的有價值的檔案做一個複製品，並安置於一個安全地方。備份有分日、月、年。而當中亦有雙單日，雙單月，雙單年之分。以防數據流失，最好有超過一個複製品。

甚麼是黑客？
黑客 (Hacker) 一般是指技術精湛的人，能令設備做出一些不在設計情況之下運作。

在資訊科技安全領域下，黑客是指一個具有精湛電腦技術的人，能使電腦或其程式於不在其設計的情況下運作。在我等來說，黑客有分黑帽子 (Black Hat)，白帽子 (White Hat)，灰帽子 (Grey Hat) 及腳本小子 (Script Kiddies)。

黑帽子是指所謂駭客，他們是作奸犯科之流。

白帽子是指資訊科技安全專家或研究員，他們測試系統漏洞，並公報結果給有關開發人員或機構。

灰帽子也是資訊科技安全專家或研究員，他們也測試系統漏洞，但他們大多數不會向有關開發人員或機構公報其發現，他們會直接披露 (Full Disclosure)。他們多數走在法律邊緣，但並沒有惡意。

至於腳本小子，他們並不是資訊科技界中人。他們會利用黑客工具作樂或者作惡。

附件二　牛角包

牛角包 (Croissants) 是一個設計十分獨特的防禦入侵系統。她是一個開源項目，由我獨自開發，她是完全免費使用的。她獨特之處在於她能夠識別惡意黑客的企圖，進而作出攔截反應。

雖然設計簡單，沒有華麗的使用介面，但是她的效能非常高，能處理 1000 Mbps 或以上流量。她的低延遲特性，對綫上遊戲的影響減至最少。適合用於個人，家庭，小型企業等。

她近似於統一威脅管理系統和下世代防火牆。她具有抵擋病毒，偵測掃描，堵塞漏洞等等功能。

硬件基本要求 ：

(1) 多核心 x86 處理器
(2) 具有 AVX2 功能的核心
(3) 8 GB 記憶體
(4) 128 GB 硬碟
(5) 3 個 1000 MB 網絡界面

詳情請瀏覽我的個人網站 (https://www.infosec-ninjas.com)，是英文版本的。

全書完