University of Taipei

Computer Science

Homework 1

Student ID: U10916024

Student: Cheng-Hao, Zhang

張呈顥

2023

2.

資訊安全的基本需求可以簡化成三個，稱為 CIA 資安三要素。

I. 機密性 Confidentiality

確保資訊的機密，防止外洩給未經授權（權限）之使用者；且存於系統。可透過加密（Encryption）或相關驗證如雙重驗證（2FA）、一次性密碼（One-Time Password）。

II. 完整性 Integrity

確保系統不被未授權者篡改或偽造；資料進行傳輸時，要確保不受非法篡改，且資訊為正確合法的。數位簽章可以確保資料不被非法更動及其完整性，現在常見的有橢圓曲線數位簽章演算法（ECDSA）。

III. 可用性 Availability

確保資訊系統運作過程的正確性，以防止惡意行為導致資訊系統被毀壞（Destroy）或延遲（Prolong）。常見對此需求的攻擊手段有服務阻斷攻擊（denial-of-service attack DoS）或分散式服務阻斷攻擊（DDoS）。

另外，其他衍生的需求有：

- Authentication

  身份鑒別；資訊來源鑒別（數位簽章、資料加密）。

- Non-Repudiation

  傳送方或接收方，皆不能否認曾進行資料傳輸或接收數位簽章、PKI（Public Key Infrastructure，公開金鑰基礎架構）。

- Access Control

  權限以及人員管控。

- Audit

  由稽核紀錄追蹤非法使用者，一旦發生入侵攻擊事件，可 Recovery(恢復系統)，也可盡快找到發生事件之原因（Audit Log）。

4.

Risk Analysis

- 評估及分析系統風險，對於部分重要資料必須採取更進一步的防護。例如，定期備份及回復處理等，系統發生安全問題時，可以確保重要資料的正確性，以降低問題發生時所帶來的損失。
- 安全漏洞所造成之損失包括有形損失及無形損失。有形損失：包括硬體及軟體設備、人力成本、雜支成本及其他因工作延宕所造成之損失。無形損失：公司形象受到影響，其損失費用無從計算。
- 通常投資在資訊安全之費用，應小於系統發生安全漏洞後所造成之損失，但要大於其損失的十分之一。

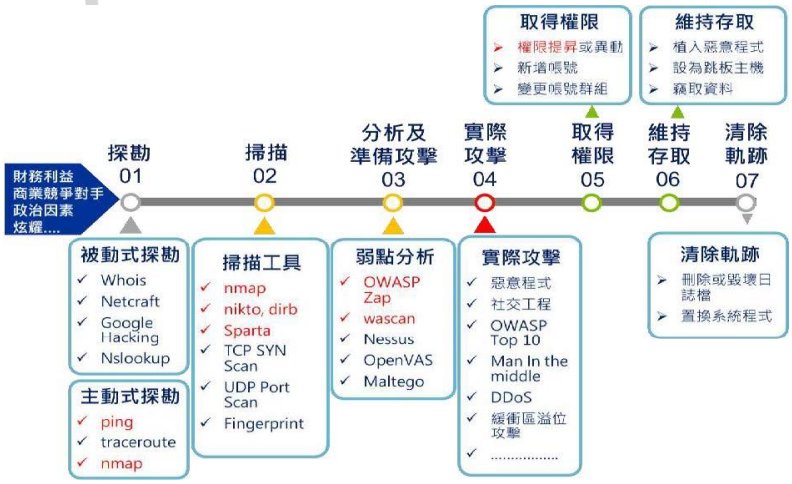
Weakness Analysis

- 對整個系統架構進行瞭解及測試包括系統架設了哪些硬體、使用哪一種作業系統如 Linux、使用哪些通訊協定如 TCP/IP、哪些人會使用本系統及授權了哪些權限給使用者等。
- 管理者瞭解這些資訊後，進而分析系統的弱點在那裡、哪些人有可能會進行攻擊、他們的目的是什麼以及要攻擊哪些地方。

Threats Analysis

- 瞭解系統的弱點之後，進而要分析系統可能遭受的安全威脅及攻擊。常見入侵並危及系統安全的方式，包含利用電子郵件、利用遠端登入、施放電腦病毒、試圖得到具有高存取權限的帳號、刪除或移動檔案等。
- 電腦網路安全相關威脅及事件回報及公告

對策分析



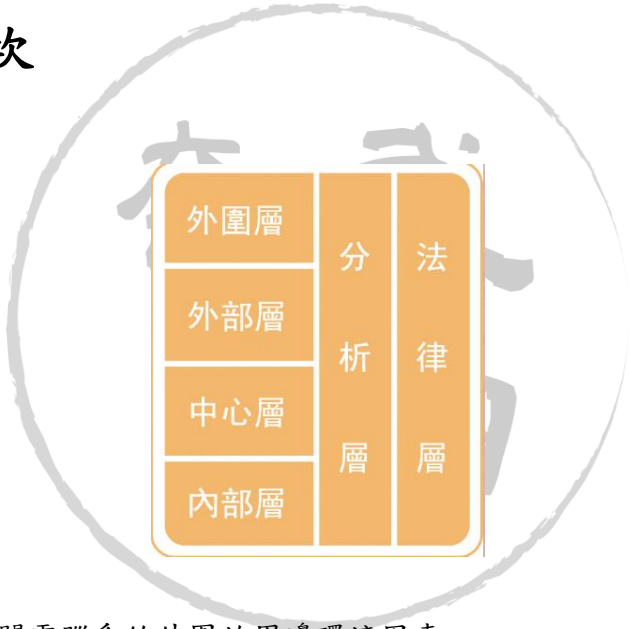
- 針對弱點及所面臨的安全威脅，研擬安全策略及所需的安全機制。例如，存取控制、使用者身分鑑別等。

5.資安的範疇

老實說，資訊安全的範疇十分廣泛，從基礎設施及人員進出管理，到網路、系統、程式安全都算。安全之管理資訊系統，需考慮：資料庫安全、作業系統安全、管理資訊系統安全、網路安全。

根據 PicoCTF[1]上的練習題目類型大致可分為 Web Exploitation, Cryptography, Reverse Engineering, Forensics, Binary Exploitation…。

6.資訊安全層次



- 外圍層牽涉到有關電腦系統外圍的周邊環境因素。
- 外部層是使用者與系統間介面層次，所牽涉到的是個別使用者所能操作的系統。
- 中心層則是內部層與外部層的溝通橋樑。
- 內部層牽涉到資料實際儲存及管理的方式。
- 分析層牽涉到系統的管理及安全威脅的分析。
- 法律層牽涉到有關資訊安全相關的法律條文。如中華民國《資通安全管理法》[2]。

---

[1] 專門給美國國高中生練習的資訊安全解謎式 CTF(Catch The Flag)網站，與實際攻防型競賽為兩種常見 CTF 型態。

[2] https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030297