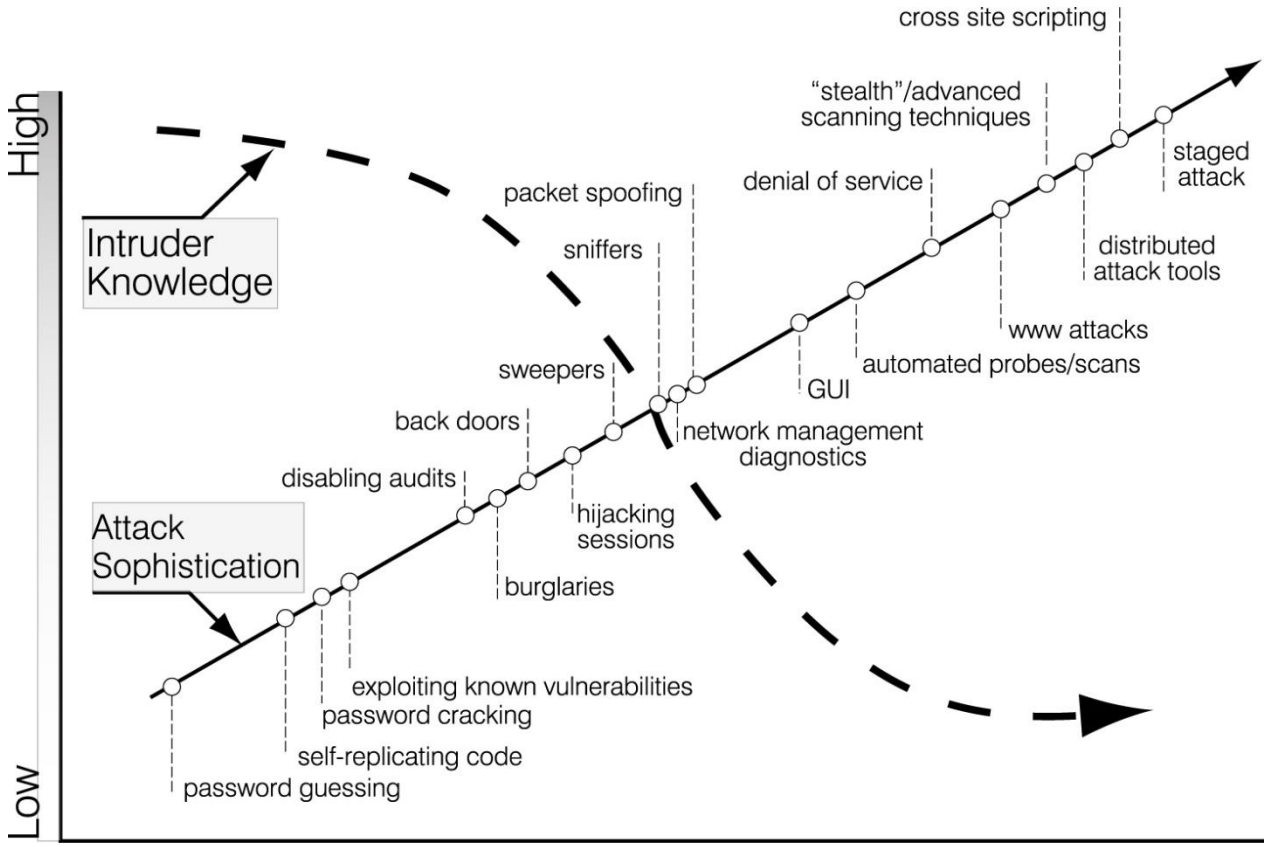
第一章

簡介與名詞介紹

為什麼需要注意資訊安全？

- 有關資訊安全的問題越來越多
- 入侵者所必須具備的專業知識越來越低
- 網路的環境普及

必須具備的專業知識越來越低



造成的問題

- 系統的複雜度
- 電腦環境及網路架構的複雜度
- 系統管理者或網路管理者在管理時的複雜度
- 造成企業直接或間接的損失

名詞解釋

- 威脅（Threat）
- 弱點（Vulnerability)
- 攻擊（Attack）
- 內部攻擊
- 外部攻擊

攻擊者利用的弱點

- 作業系統
- 應用軟體
- 錯誤的設定
- 網路架構太過簡易
- 使用者沒有資訊安全的觀念

安全、功能與便利

名詞解釋

- 黑帽（Black Hats)
- 灰帽（Gray Hats)
- 自殺駭客（Suicide Hackers）
- 白帽（White Hats）
- 道德駭客（Ethical Hacker）

弱點研究

- 依據嚴重等級（Severity level）可將弱點區分為低（low）、中（medium）或高（high）。
- 依據入侵範圍（Exploit range）區分為可被本地（local）入侵的弱點或可被遠端（remote）入侵的弱點。

弱點研究

- 能識別及更正網路的弱點。
- 能保護網路免於被入侵者攻擊。
- 能得到防護安全的資訊。
- 能蒐集關於病毒的資訊。
- 能發現在網路上的弱點，以及在網路被攻擊前，警告網路或系統的管理者。
- 能了解如何從網路的攻擊中復原。

弱點研究的工具網站 (https://www.us-cert.gov/)

http://twcert.org.tw

https://moda.gov.tw/ACS/
數位發展部安全署

黑客世界大戰圖

http://map.norsecorp.com/

https://threatmap.bitdefender.com/

https://www.spamhaus.com/threat-map/

https://threatbutt.com/map/

http://www.digitalattackmap.com

https://threatmap.checkpoint.com/ThreatPortal/livemap.html

https://threatmap.fortiguard.com/

https://securitycenter.sonicwall.com/m/page/worldwide-attacks

道德駭客

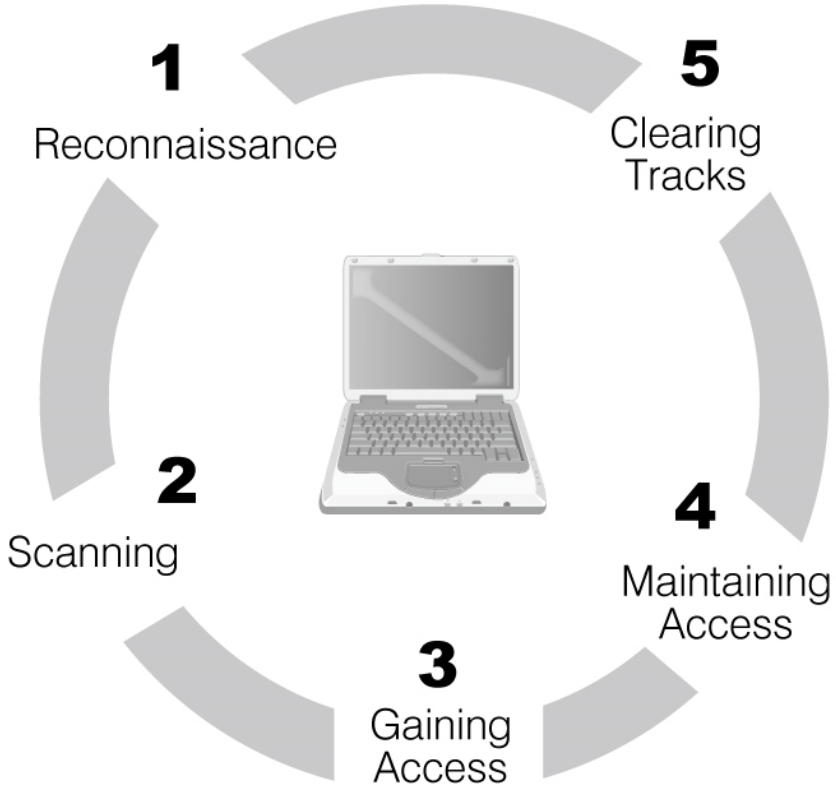
- 精通寫程式與電腦網路技能。
- 熟悉弱點研究。
- 能掌握不同的入侵技術。
- 遵守嚴格的行為規範。

駭客偵測系統時的五個步驟

- 偵查
- 掃瞄
- 獲得存取權限
- 維護存取
- 清除軌跡

駭客偵測系統時的五個步驟

- Reconnaissance
  - Active/passive
- Scanning
- Gaining access
  - Operating system level/application level
  - Network level
  - Denial of service
- Maintaining access
  - Uploading/altering/ downloading programs or data
- Clearing tracks



偵查（Reconnaissance）

- 真實的駭客入侵 99.9%不會這麼簡單就成功。
- 駭客通常會先蒐集很多關於目標的資訊，以進行評估及攻擊。

偵查（Reconnaissance）

- 被動式偵查（Passive reconnaissance）
- 主動式偵查（Active reconnaissance)

掃描（Scan)

- 電話撥號（dialers）
- Port掃描器
- network對應圖
- 弱點掃描器

獲得存取權限（Gaining Access）

- 此階段屬於滲透階段，是駭客真正在入侵系統的時期。
- 入侵的行為可以透過區域網路，網際網路或欺騙。手法包括了「緩衝區溢位」、「阻斷服務」、「攔截」及「密碼破解」...等，這些手法將在後續章節中介紹。
- 駭客可以獲取作業系統等級（operating system level）、應用程式等級（ application level）或網路等級（network level）的權限。

維護存取（Maintaining access）

- 在此階段，駭客已經取得系統的權限，並且使用此系統的資源。
- 駭客可以在這個系統上進行下列的任一項行為：
  - 上傳（Uploading）
  - 變更（altering）
  - 下載（downloading)

清除軌跡（Clearing tracks）

- 許多主機對於連線的行為都會進行記錄，因此駭客會設法覆蓋或刪除入侵的軌跡，以隱藏活動的訊息，避免被發現。

- 方法包括：偽裝（Steganography）、建立通道（tunneling）及改變log檔。

資訊人員要注意的事

- 入侵者會看上什麼系統？（***偵測及掃瞄階段***）
- 在哪些系統上曾經發現有駭客嘗試入侵的行為？（***偵測及掃瞄階段***）
- 入侵者獲得這些資訊可以用來做什麼？（***獲得存取權限及維護存取權限階段***）
- 是否曾發現系統有被入侵的可能，但是找不到任何資訊？（***清除軌跡階段***）

入侵測試

- 黑箱（Black box）：從外部來看，對於目標網路設施沒有完整訊息的情況下，所進行的測試。
- 白箱（White box）：從外部來看，對於目標網路設施擁有完整訊息的情況下，所進行的測試。.
- 灰箱（Gray box）：就是內部測試（Internal Testing）。

測試報告與文件

- 進行弱點掃瞄與滲透測試的過程與結果，必須以報告（Report）的方式呈現。
- 測試入侵的活動細節，並要記載其相對應的工作時間表。
- 詳細的弱點列表及對策方案建議。

測試報告與文件

- 基於安全的理由，若要傳送報告，通常以電腦的輸出文件（hard copy）來傳送，避免直接在網路上傳送。
- 入侵測試若是以小組的形式來進行時，要考量及評估團隊成員的誠信及資訊內容的敏感度。