

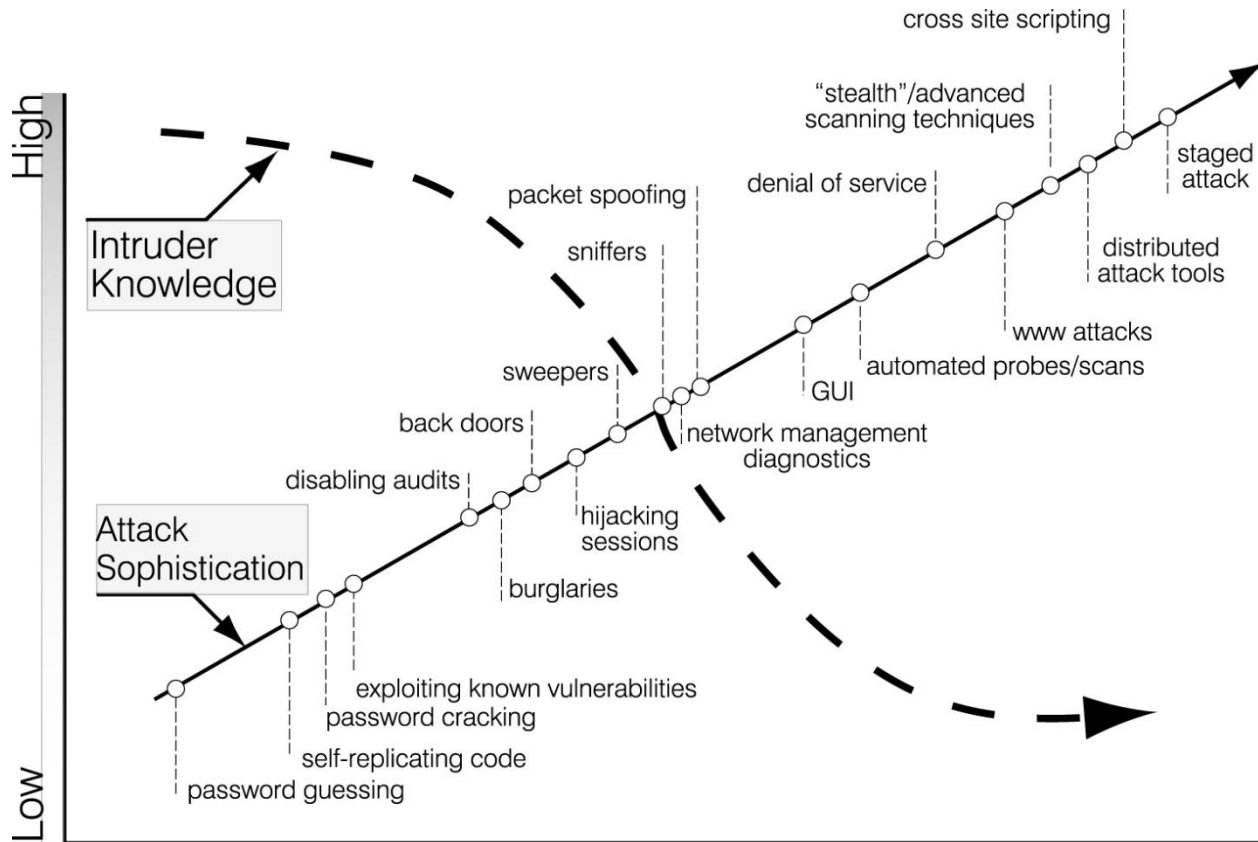
第一章

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

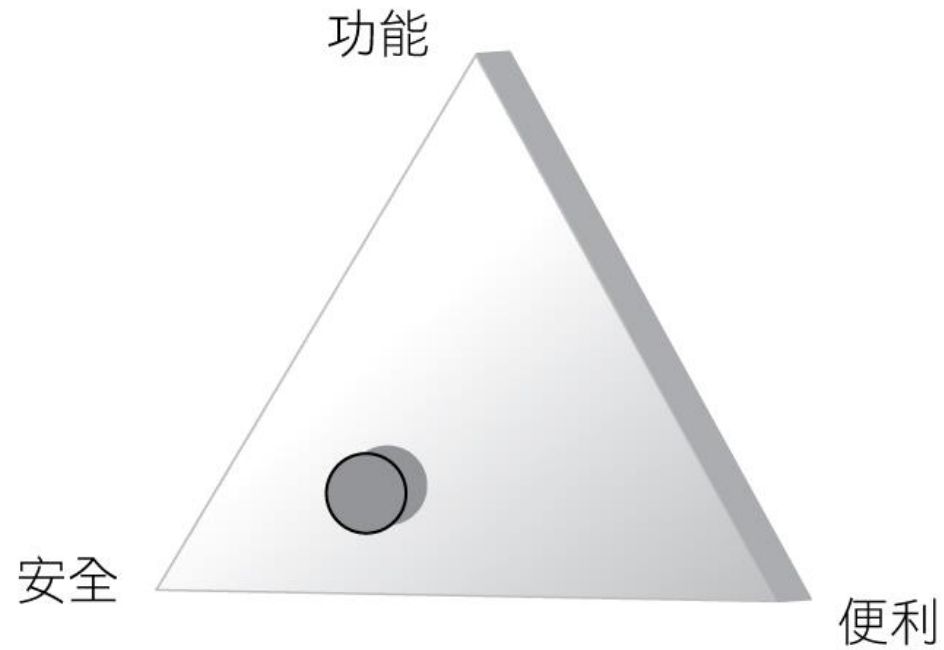
名詞解釋

- 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/>)

The screenshot displays a Microsoft Internet Explorer browser window with the address bar showing <http://www.us-cert.gov/vuln/878044>. The page header features the US-CERT logo and the text "US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM". The main content area is titled "Vulnerability Note VU#878044" and "SNMPv3 improper HMAC validation allows authentication bypass". The page includes a navigation menu on the left with links for "Vulnerability Notes Database", "Search Vulnerability Notes", "Vulnerability Notes Help Information", "View Notes By", "Home", "ID Number", "CVE Name", "Date Public", "Date Published", "Date Updated", and "Security Metric". The main text under "Overview" states: "A vulnerability in the way implementations of SNMPv3 handle specially crafted packets may allow authentication bypass." Under "I. Description", it explains that authentication for SNMPv3 is done using keys and Hash Message Authentication Code (HMAC), and that implementations may allow a shortened HMAC code to authenticate. Under "II. Impact", it states that attackers can read and modify any SNMP object. Under "III. Solution", it lists affected versions: Net-SNMP 5.4.1.1, 5.3.2.1, 5.2.4.1, 5.1.4.1, 5.0.11.1 and UCD-SNMP 4.2.7.1. The footer of the page includes the text "US-CERT Vulnerability Notes - Home" and "Internet Explorer".

http://twcert.org.tw

The screenshot shows a Microsoft Internet Explorer browser window displaying the TWCERT website. The browser's address bar shows the URL: <http://www.twcert.org.tw/forums/showthread.php?p=1561&TW-CA-2008-005&PHPSESSID=44f103ed888d96970ee1418044306>. The website header includes the TWCERT logo and the text "台灣電腦網路危機處理暨協調中心" (Taiwan Computer Emergency Response Team / Coordination Center). A navigation menu contains links for "最新消息", "服務項目", "文件下載", "會員專區", "網路資源", "關於我們", and "English".

The main content area is titled "Download 文件下載" and "安全彙報" (Security Report). It features a sidebar with a tree view containing "安全彙報", "中心資訊", "技術專欄", "TWCERT公告", and "語言頁". The main content displays a security advisory for TW-CA-2008-005 (TA08-150A), titled "Apple Updates for Multiple Vulnerabilities/Precedence: list".

TWCERT發布日期:	2008-06-11
建議清除日期:	2008-06-29
分類:	Dos Den Gain Privilege Info Leak
來源參考:	TA08-150A
適用安全弱點編號:	

簡述
Apple 已公佈安全更新 2008-003 和 OS X 10.5.3 以修正多個影響 Apple Mac OS X 和 Mac OS X Server 的安全弱點。攻擊者可能利用這些弱點執行任意程式、存取敏感資訊、或造成系統當機攻擊。

說明
Apple 安全更新 2008-003 和 OS X 10.5.3 修正多個影響 Apple Mac OS X 和 Mac OS X Server 10.4.11 和 10.5.2 (含)以前版本的安全弱點。更詳細的資訊可以在 [OS-CERT Vulnerability Notes Database](#) 中取得。此更新也解決其他與關於 Apple OS X 或 OS X Server 相關產品的弱點。

影響平台

- * Mac OS X v10.5.3 (含)以前的版本
- * Mac OS X Server v10.4.11 (含)以前的版本

修正方式

--更新:
安裝 Apple Security Update 2008-003 或 Apple Mac OS X 10.5.3。這些更新可經由 Software Update 或 Apple Downloads 取得。

--參考資料:

<https://moda.gov.tw/ACS/> 數位發展部安全署

數位發展部資通安全署
Administration for Cyber Security, moda

關於資安署 ▾ 資安法規專區 ▾ 業務專區 ▾ 行政院國家資通安全會報 ▾ 訊息公告 ▾ 相關連結 ▾

業務專區

- 資安政策與法規**
推動國家資通安全發展方案，並落實資通安全管理法，以打造堅韌安全之智慧國家
- 關鍵基礎設施資安防護**
指定關鍵基礎設施提供者，推動落實相關法遵事項及防護基準，並連結八大領域之主管部會，擴大國家資安聯防運作機制
- 資安事件通報應變**
推動各政府機關落實事前安全防護、事中緊急應變、事後復原作業，配合定期辦理各項演練作業，建立迅速通報及緊急應變處置機制
- 資安演練與稽核**
辦理資安稽核協助機關落實資通安全管理法遵事項，並透過網路攻防演練協助機關提升資安防護意識及能量
- 資安教育訓練**
強化政府資安專職人員知能，建立完善之資安人才培訓體系，定期培訓各機關資安(訊)人員，以孕育優質資安人才

資安法專區 NICST 資安月報 政府資訊公開

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？（**偵測及掃描階段**）
- 在哪些系統上曾經發現有駭客嘗試入侵的行為？（**偵測及掃描階段**）
- 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

- 進行弱點掃描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。