經濟部iPAS
「資訊安全工程師能力鑑定」

資訊安全技術概論

Bryan Chen

CISSP, CEH, ISO 2700I LA, Security+, CIW Security Analyst
ITIL Expert SO 2000 LA, ISO 20000 Consultant

講師簡介

- **學歷**
  - 賓州大學 (U. of Pennsylvania) 資訊科學研究所 碩士
- **經歷**
  - **(現) 104 資訊科技　副總 暨 資安長**
  - 中華電信研究院 資安所 研究員
  - 英國標準協會(bsi) 主導稽核員/講師
  - Asiainfra Ltd. 資安服務處協理
  - 鈺松國際 監控中心(SOC)資安工程師
  - 啟碁科技 研發工程師
  - 大同世界科技 軟體工師
- 講師資格
  - (ISC)^2 CISSP CBK Review Seminar 講師
  - Quintica ITIL 講師/ TAOS ITIL 講師
  - 資策會/恆逸 ITIL特約講師
  - BSI 英國標準協會 ISMS/ITSMS 講師
- **資訊安全認證**
  - CISSP – 資訊安全系統專家
  - EC-Council CEH – EC-Council 白帽駭客
  - CompTIA Security+ - CompTIA資訊安全
  - CIW Security Ayalyst – CIW 資訊安全分析專家
- **資訊服務管理 (ITSM)認證**
  - ITIL Expert ITIL - ITIL專家認證
  - ITIL V2 Service Manager – ITIL V2最高認證
  - ITIL V3 SO – ITIL服務維運
  - ITIL V3 RC&V – ITIL服務發行控制與確認
  - ITIL V3 OS&A – ITIL服務提供與支援
  - ITIL V3 SO&A – ITIL服務提供與協定
  - ITIL V2/V3 Foundation – ITIL V2/V3 基礎
  - ISO 20000 Consultant – ISO 20000 顧問
- **稽核**
  - IRCA ISMS LA - 國際註冊資訊安全主導稽核員
  - ISO 20000 LA - ISO 20000 主導稽核員
  - ISO 27001 LA - ISO 27001 主導稽核員
  - ISO 20000 Auditor – ISO 20000 稽核員 (itSMF)

初級資訊安全工程師-考科二

科目	評鑑主題	評鑑內容
科目二： 資訊安全技術概論	網路與通訊安全	網路安全
		通訊安全
	作業系統與應用程式安全	作業系統安全
		作業系統與應用程式(含資料庫與網頁) 攻擊手法
		程式與開發安全
	資安維運技術	惡意程式防護與弱點管理
		資料安全及備份管理
		日誌管理
	新興科技安全	雲端安全概論
		行動裝置安全概論
		物聯網安全概論

先教

重要資安概念

- 邊界與分類 (Boundary and classification)
- 職務區隔 (Segregation of duties, SOD)
- 縱深防禦 (Layered defense, defense in depth)
- 單一脆弱點 (Single point of failure, SPOF)
- 阿奇里斯腱 (Achilles heel)
- 木桶理論 (Bucker principle)
- 僅知原則 (Need to know)

風險管理

評鑑主題七
作業系統與應用程式安全

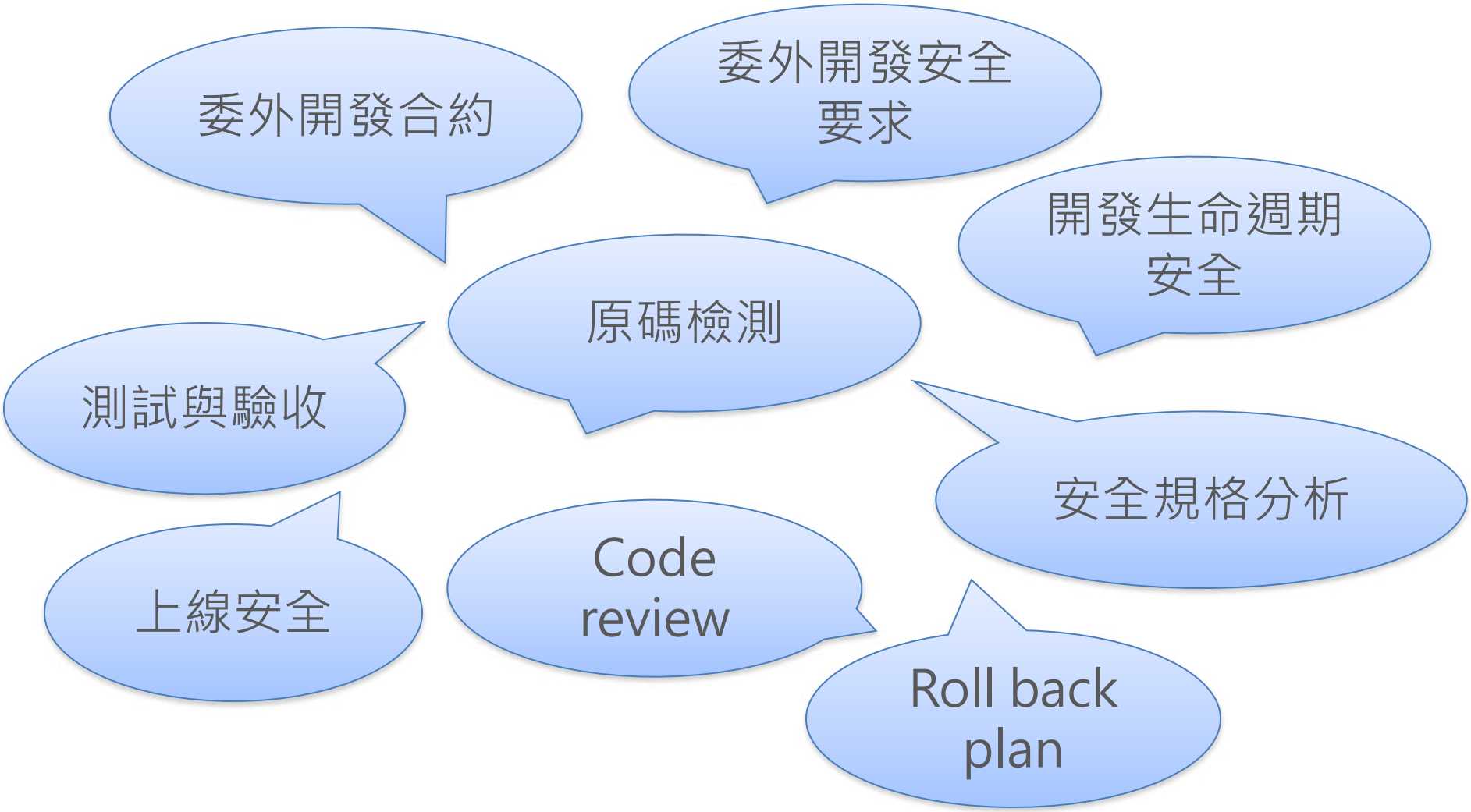
1. 作業系統安全
2. 作業系統與應用程式 (含資料庫與網頁)
   攻擊手法
3. 程式與開發安全

重要字辭與定義

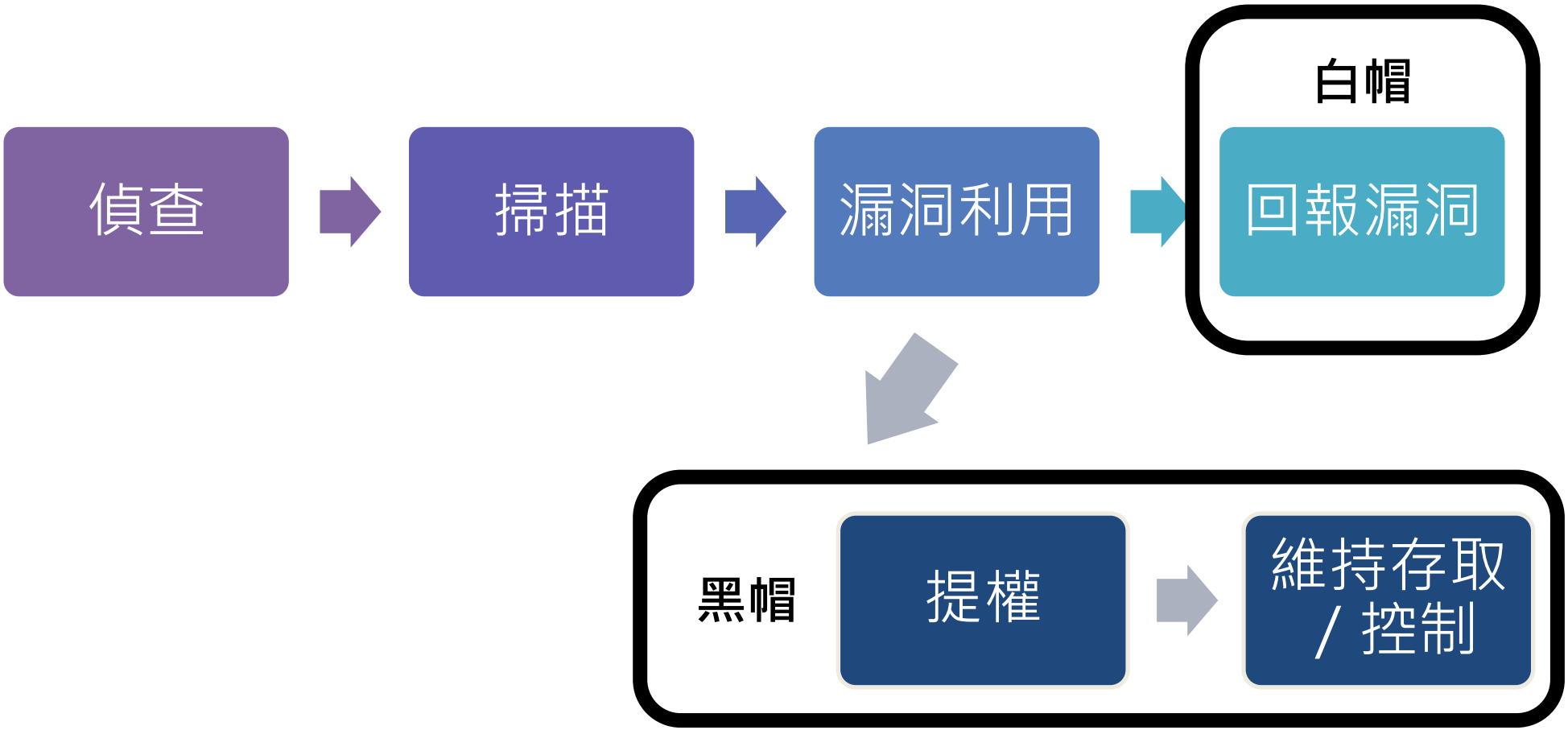
重要字辭與定義


登入安全管控
(錯誤訊息)
特權工具
驗證碼
WSUS/
Antivirus
最低權限
資料庫稽核
勒索軟體 (
對策)
網頁安全/
監控(置換)
網頁攻擊手法
(SQL injection,
XSS...)
WAF
... 各種主機攻擊手
法特性 (Protocol)

重要字辭與定義


委外開發合約
委外開發安全要求
開發生命週期安全
原碼檢測
測試與驗收
安全規格分析
上線安全
Code review
Roll back plan

Black vs. White



作業系統安全

常見議題

- 弱點修補
  - 老舊程式?
- 可移除式媒體
- 安全登入程序
- 通行碼管理系統
- 程式源碼存取

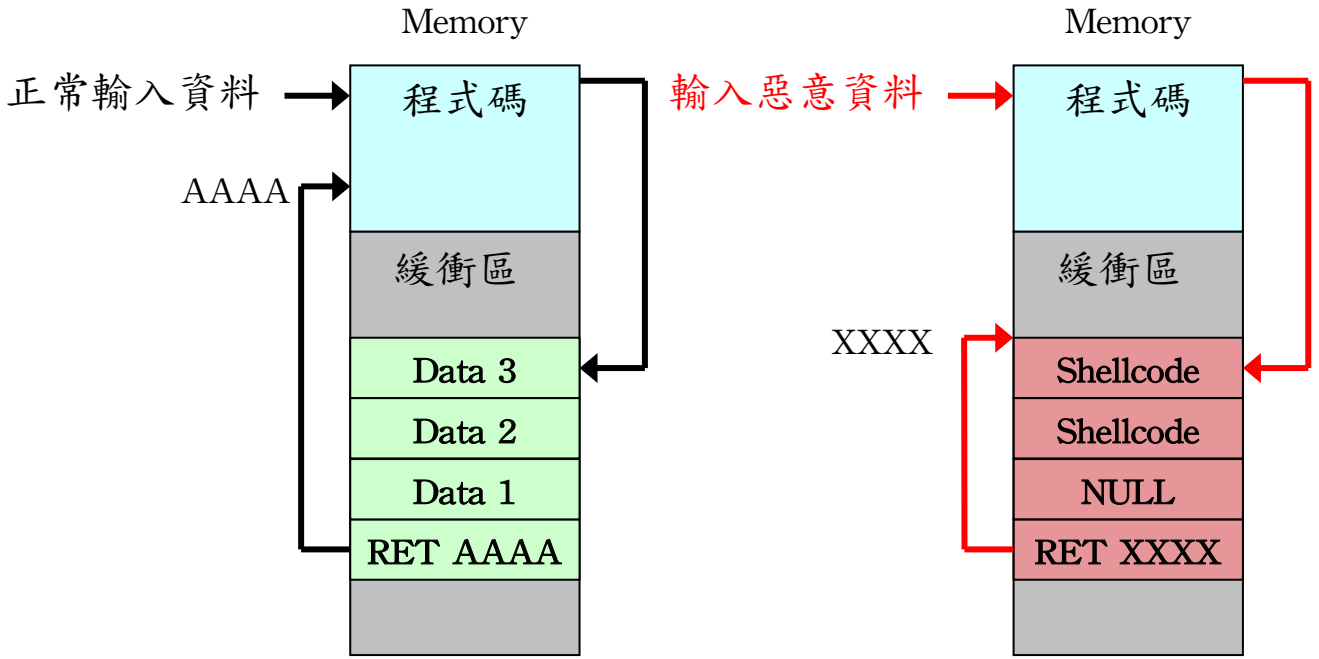
- 通行碼管理系統
- 通行碼安全
- 變更管理
- 容量管理
- 開發測試與線上環境區隔

常見應用程式的威脅

- 緩衝區溢位(Buffer overflow)
- 惡意程式碼(Malware)
- 輸入攻擊
- 後門程式
- 邏輯炸彈
- 行動應用(app)的攻擊
- 社交軟體的攻擊
- 記憶體洩漏 (Memory leaking)

緩衝區溢位(Buffer overflow)

- 緩衝區是程式執行期間在記憶體中用來存放資料的空間
- 當應用程式處理資料時未檢查輸入資料的長度，就有可能讓太長的資料覆蓋到其他記憶體區段，導致惡意程式碼被植入且被執行



惡意程式碼(1/2)

- 惡意程式碼可分為病毒、蠕蟲、後門、木馬及間諜程式
- 這些惡意程式碼可能會附著在應用程式中，也可能獨立存在，導致程式執行效能變差與資料被竊
- 病毒
  - 需被動依賴寄宿的應用程式重製自己或感染其他程式
- 蠕蟲
  - 自己有能力主動進行傳染散播的惡意程式
- 後門
  - 留在系統內不需經一般安全控管程序，就可以被植入者遙控的惡意程式
- 木馬
  - 是一個陷阱程式，等待使用者踩到陷阱程式後，運用使用者權限執行不當的指令

惡意程式碼(2/2)

- 間諜程式
  - 主要以竊取系統的機密資料為主的程式、例如：上網行為與鍵盤側錄等
- 現今的惡意程式不見得只單純扮演一種角色，可結合各種不同的手法與行為感染與散播
  - 例如：USB病毒在USB硬碟時，運用病毒被動感染的方式感染電腦主機，一旦感染電腦主機後可能變成主動感染其他系統的蠕蟲

後門程式

- 留在系統內不需經一般安全控管程序，就可以被植入者遙控的惡意程式
- 維護用後門程式
  - 開發人員私下留存在應用程式內，以方便日後進行維護的程式
  - 應用程式於整合測試階段，應檢查應用程式中是否含有後門程式
- 被惡意植入的後門程式
  - 由於應用程式其他的弱點(如：Command Injection)，導致惡意後門程式被植入應用系統中
  - 應用程式清單應被妥善維護，以區別非授權程式，也可以善用檔案的完整性檢查工具

邏輯炸彈

- 邏輯炸彈是一段被故意插入應用程式的程式片段，在正常情況下並不會被執行。只有當特定條件符合時才會被啟動
  - 例如：程式設計師隱藏了一段刪除薪資資料庫的程式碼，只有當他被解僱的條件符合時才會被執行
- 有些病毒與蠕蟲也會具有邏輯炸彈的程式碼
  - 例如：當4月1日愚人節時將硬碟刪除
- 應用程式於整合測試階段，應檢查應用程式中是否含有邏輯炸彈

常見帳密攻擊比較

暴力破解（Brute Force）	使用所有可能的密碼組合，嘗試登入系統。
字典攻擊 （Dictionary Attack）	收集常見的密碼納入猜測字典，然後用來嘗試登入系統。
密碼潑灑 （Password Spraying）	只使用單一弱密碼，對所有帳號進行測試。
帳號填充 （Credential Stuffing）	利用外洩帳號資料庫的密碼組合嘗試登入系統。

勒索軟體

- Ransomware
- 阻斷存取式攻擊Denial-of-access attack

- 防禦
  - 網路和郵件的內容過濾代理伺服器
  - 限制級別存取
  - 員工警覺性訓練
  - 備份（回復檢查）

已上線網站應用程式安全的防護

- 定期針對作業系統、網站伺服器及資料庫伺服器執行弱點掃描與修補
- 定期執行網站應用程式弱點掃描滲透測試
  - 黑箱：不知軟體結構，直接驗證功能
  - 白箱：取得較多訊息
- 有能力修改程式
  - 修補已發現的應用程式弱點
- 無能力修改程式
  - 建置Web應用程式防火牆進行弱點防禦或其他補償措施
- 新開發的應用程式請參考「安全軟體開發生命週期(SSDLC)」

常見Port

協定		port
檔案傳輸	File Transfer Protocol, FTP	21
安全遠端登錄	Secure Shell, SSH	22
遠端登錄	Telnet	23
簡單郵件傳輸	Simple Mail Transfer Protocol, SMTP	25
網域名稱服務	Domain Name Service, DNS	53
超文本傳輸	HyperText Transport Protocol, http	80
郵件接收	Post Office Protocol Version 3, POP3	110
網路時間	Network Time Protocol, NTP	123
安全超文本傳輸	Hypertext Transfer Protocol Secure, https	443
網路芳鄰	使用SMB (Simple Message Block)，用NetBIOS來尋找設備 Linux 的Samba即為SMB軟體	UDP137,138 TCP 139, 445

應用程式安全控制

變更控制(1/2)

- 原因
  - 應用程式上線後因需求的變更、新功能要求及發現新瑕疵等因素，需要變更應用系統程式或組態
- 目的
  - 為維持變更後的安全狀態仍可符合安全政策要求
- 方法
  - 組織應實作應用程式變更控制流程
  - 必須確保變更是獲得授權、經過測試且被記錄下來的

變更控制(2/2)

- 變更控制流程必要的步驟
  - 填寫變更需求申請
  - 分析變更需求
  - 發展實作策略、方法或步驟
  - 計算變更所需成本
  - 評估變更與安全的關聯性
  - 記錄變更請求
  - 提交變更申請進行核准
  - 進行應用程式變更的開發工作
  - 記錄變更開發的產出(新增或刪除功能)
  - 將變更的程式碼與變更申請連結(程式碼中的註解)
  - 將變更後的程式碼交付測試與品質認可
  - 變更程式碼版本(上線)
  - 向管理階層報告變更結果

職責區隔

- 作業人員不應有權限存取**線上的程式碼或程式物件**
- 程式設計人員不應存取**線上運作中的軟體**
- 品管部門應測試程式碼品質，且與開發部門採用不同的測試方法
- 一旦軟體被開發測試完成應被保存在程式庫中
- 線上運作的軟體應由程式庫中發行，不應直接由程式設計人員或測試人員進行更新

程式庫維護

- 應用程式應集中存放在程式庫中，並進行存取控管
- 程式庫進行版本控制，並保留所有版本程式碼
  - 主版本：1.0
  - 次版本：1.1
  - 緊急修正版本：1.0.1
- 開發部門凍結版本後應簽入(Check In)到程式庫，也應由程式庫中簽出(Check Out)取得最新版本進行修改
- 測試部門應由程式庫中簽出(Check Out)取得最新版本進行測試
- 上線人員應由程式庫中發行(Release)最新版本應用程式至線上系統

應用程式的品質與安全檢測

- 任何應用程式都有可能有瑕疵或是弱點
  - 安全程式開發(secure programming)是直接嘗試消除程式瑕疵
  - 安全檢測則是嘗試在有瑕疵的程式存在的情況下保護系統資源不受危害
- 使用者、程式設計者與系統管理員對於程式安全的認知是不同的
- 技術上可依病毒的特性對程式進行檢測
- 通常需要工具的輔助

補充:行動應用(app)的安全問題

- 行動應用(app)也是應用程式的一類
- 駭客可以循傳統的技術進行病毒的感染
- 駭客也可以運用反向工程的技術來變造原來的程式，將變造以後的app送上程式商店引誘使用者下載
- 行動應用(app)的資安問題持續攀升
- 開發行動應用(app)時需注意採用的套件的安全
- app開發時，索取過多行動裝置上的敏感資訊，例如：通訊錄、行事曆、座標位置、郵件、簡訊內容等，**易侵犯隱私**

程式與開發安全

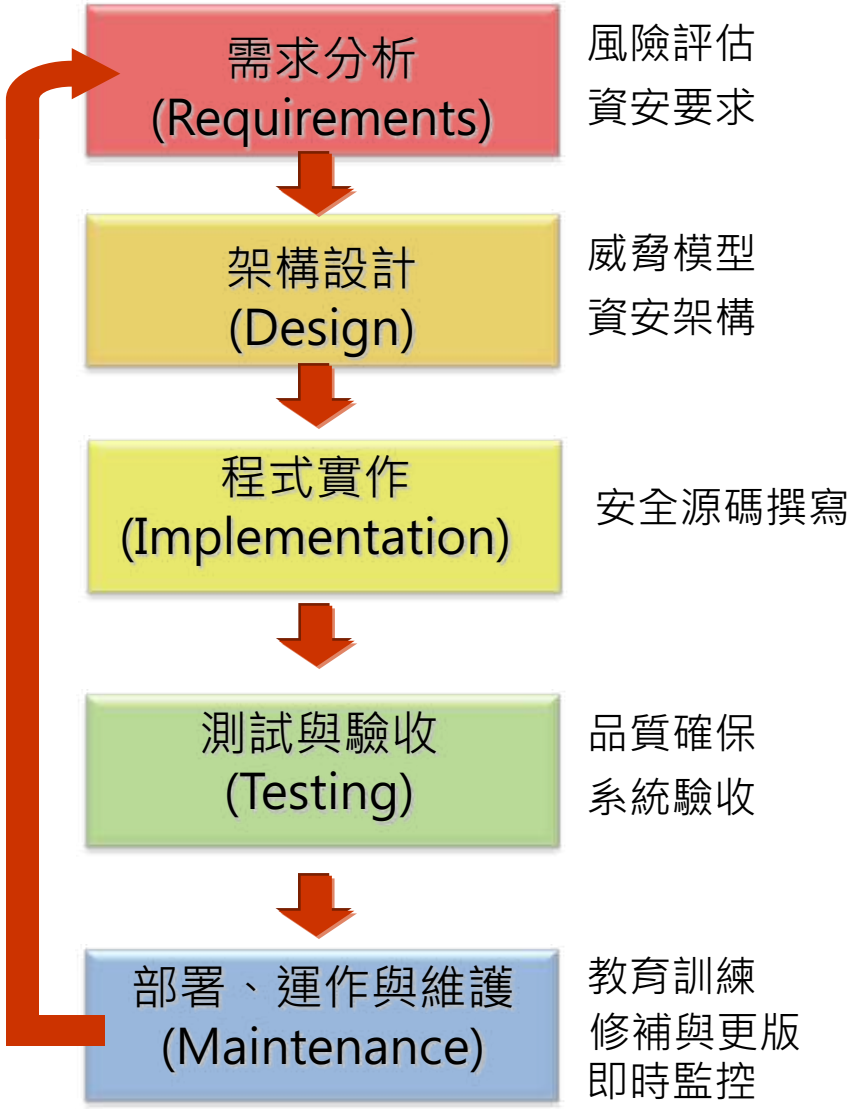
重要議題

- 開發政策
  - 擁抱新技術
  - 技術債
- 系統變更程序
- 平台變更後之技術審查
- 軟體套件變更限制

- 安全開發環境
- 安全測試
- 驗收
- 上線政策
- **測試資料保護**

安全軟體開發生命週期簡介(1/3)

- 安全的軟體開發生命週期(Secure Software Development Life Cycle, SSDLC)意指發展一套安全的軟體之順序，主要可分為：



安全軟體開發生命週期簡介(2/3)

- 需求分析 (Requirements)
  - 著重資安需求定義，以符合使用者需求與法規遵循為目的
- 架構設計 (Design)
  - 根據需求分析結果，進行包含系統任務的目標、功能關聯、邊界範圍及各階層使用者的角色等內外部使用的規劃與搭配適當的資安架構
- 程式實作 (Implementation)
  - 落實既有之規劃，將使用者介面、功能運作及安全性等完整的實現

安全軟體開發生命週期簡介(3/3)

- 測試與驗收 (Testing)
  - 進行運作模擬，檢驗該系統的完成度，確保各項功能與安全性皆可符合既定的需求
- 部署與維運 (Maintenance)
  - 進行軟體之部署，安排教育訓練
  - 落實軟體之穩定運作，應定期修補漏洞(Patch)、按步升級更新版本(Upgrade)及即時監控(Monitor)

委外作業資安要求

委外管理重點

- 委外實體與環境安全
  - 防止組織場所內資訊因委外作業而遭未經授權的實體存取、損害及干擾，關鍵或敏感的資訊處理設施宜置放於安全區域
- 委外之作業管理
  - 委外相關作業應符合組織安全政策與程序之要求
- 委外使用者存取管理
  - 組織宜有正式程序，以控制資訊系統與服務的存取權限配置作業
- 委外資訊安全事故管理
  - 委外組織宜備妥正式的事故通報與提報程序，提供委外作業廠商配合並施予合宜訓練
- 遵循適法性要求
  - 組織於資訊系統設計、運作、使用及管理都應受法律、法令、法規或契約的安全要求所規範，所參照之規範宜明確界定、文件化及維持最新版本

驗收與維護

- 組織執行「驗收階段」程序，係依據契約文件與「履約管理」階段執行成果辦理
- 以「專案工作計畫書」內容確認委外專案之進行方式、專案組織、相關時程及資訊安全要求事項是否符合
- 而委外廠商也須將定期召開工作進度報告會議之內容，如應完成重要工作項目、已完成工作的項目、預計工作項目、問題與建議等，提供驗收單位佐證
- 定期審查廠商效

爭議處理

- 組織與廠商因履約管理產生爭議未能達成協議者，得以下列方式之一處理：
  - 向採購申訴審議委員會申請調解
  - 向仲裁機構提付仲裁
- 然若雙方於問題標準界定上有所爭議時
  - 可蒐集發生的事證與相關資訊
  - 尋求具公信力之第三者、學者專家、法院或調解委員會(如行政院公共工程委員會)等
  - 進行問題的釐清與相關問題的調解

範例考題

當某一作業系統中的兩個程式因互相搶用資源而造成兩個程式均無法完成既定工作之結果，請問此現象稱為？

- (A)碰撞（Collision）
- (B)死結（Deadlock）
- (C)佇列（Queue）
- (D)欺騙（Spoof）

關於資安組織OWASP（開放Web軟體安全計畫—Open Web Application Security Project），下列敘述何者不正確？

- (A)是一個開放社群、營利性組織
- (B) 主要目標是研議協助解決 Web 軟體安全之標準、工具與技術文件
- (C) 長期協助政府或企業瞭解並改善網頁應用程式與網頁服務的安全性
- (D)美國聯邦貿易委員會（FTC）強烈建議所有企業需遵循 OWASP 所發佈的十大 Web 弱點防護守則

請問針對作業系統訂定的資訊安全策略中，下列何種安全模式中「檔案持有者」可授權決定「其他使用者」存取該檔案的權限？

- (A) 自由存取控制（Discretionary Access Control，DAC）
- (B) 強制性存取控制（Mandatory Access Control，MAC）
- (C) 角色存取控制（Role-based Access Control，RBAC）
- (D) 屬性存取控制（Attribute-based Access Control，ABAC）

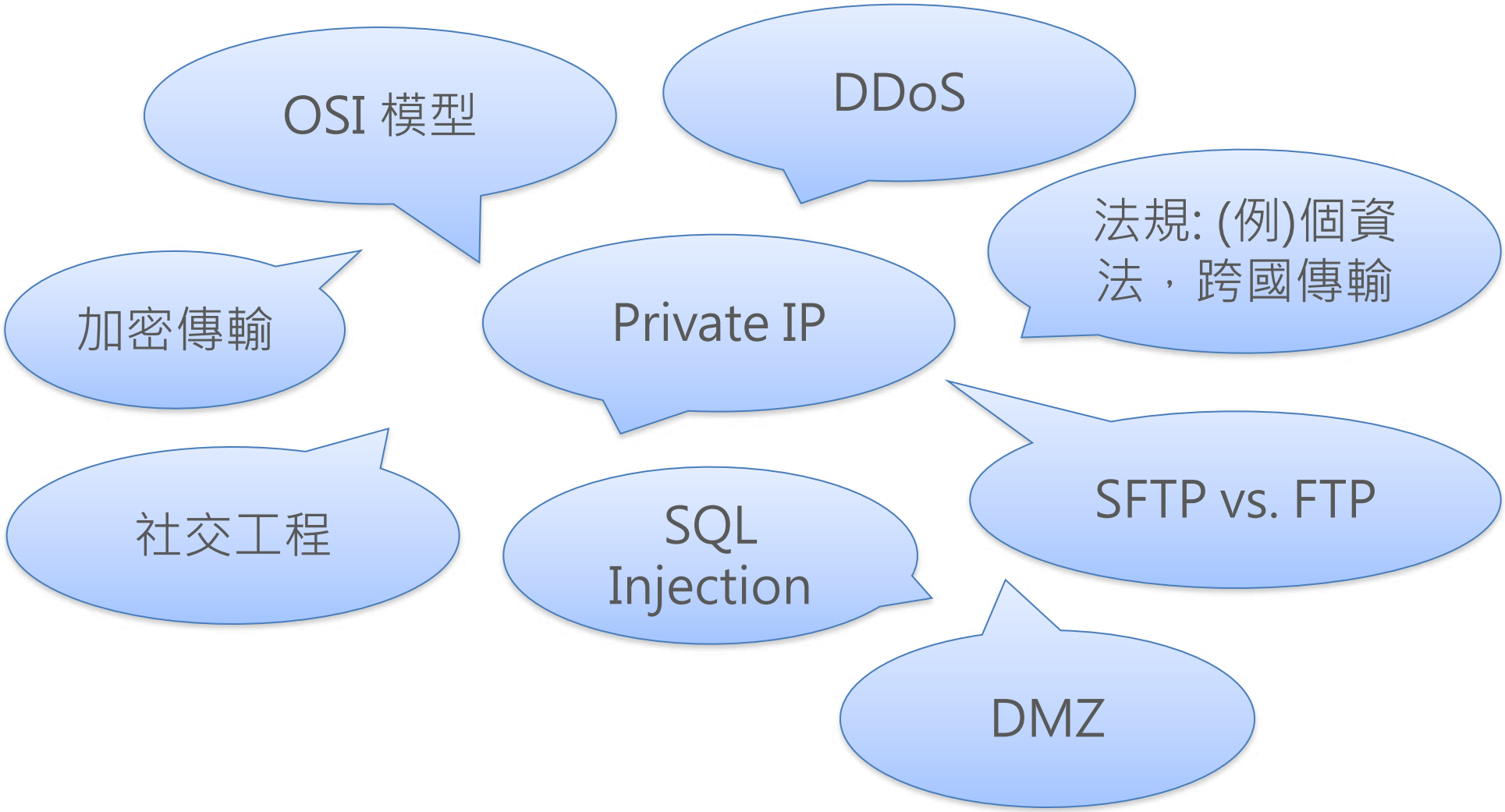
用在入侵和攻擊他人的電腦系統上，取得系統管理員的權限，具有隱藏和遠端操控的能力；電腦病毒、間諜軟體等也常使用來隱藏蹤跡。該工具軟體為？

- (A)Cookie
- (B) Rootkit
- (C) Backdoor
- (D)Phishing

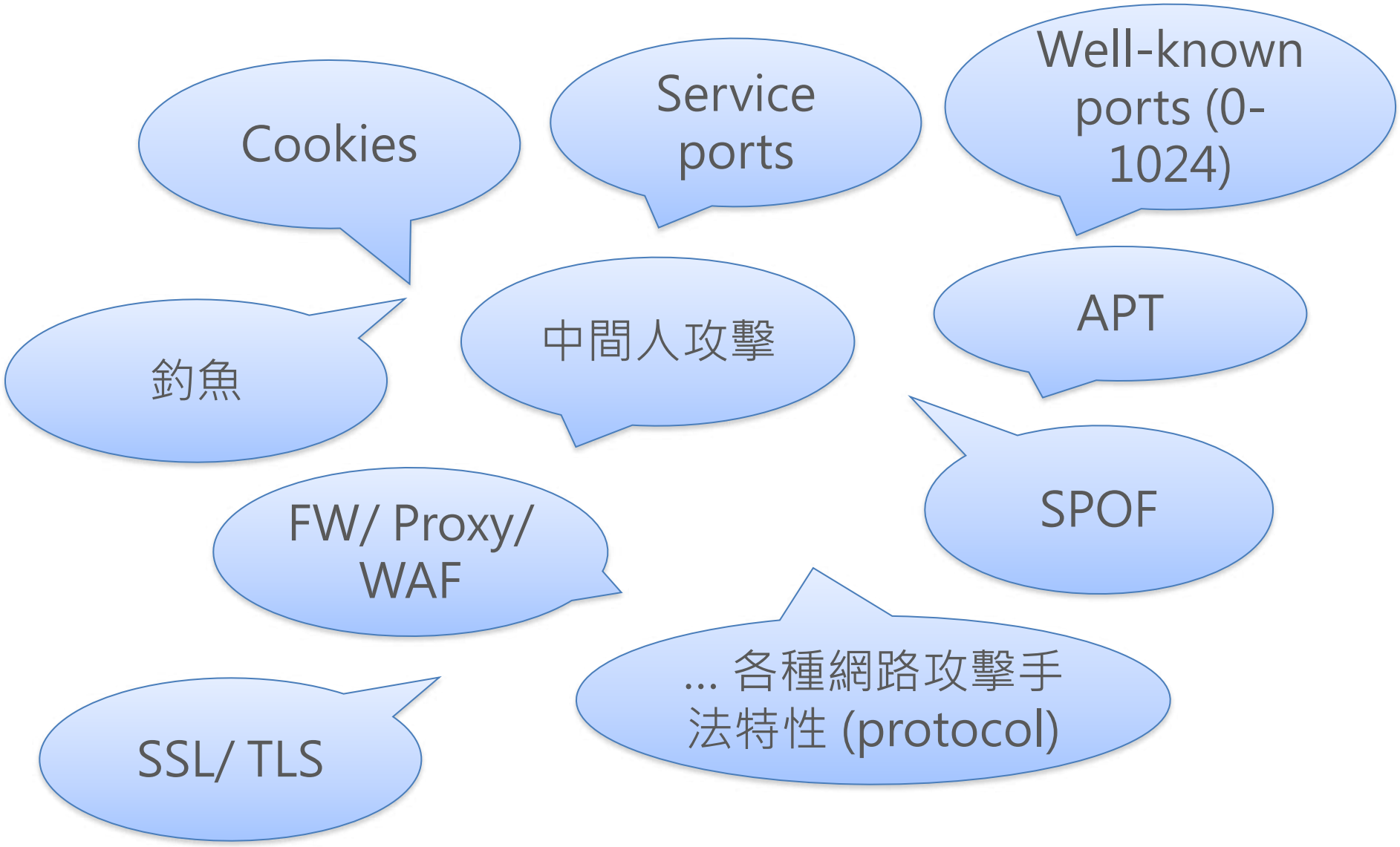
評鑑主題六
網路與通訊安全

1. 網路安全
2. 通訊安全

重要字辭與定義


OSI 模型
DDoS
法規: (例)個資法，跨國傳輸
加密傳輸
Private IP
SFTP vs. FTP
社交工程
SQL Injection
DMZ

重要字辭與定義


Cookies
Service ports
Well-known ports (0-1024)
釣魚
中間人攻擊
APT
SPOF
FW/ Proxy/ WAF
SSL/ TLS
... 各種網路攻擊手法特性 (protocol)

常見議題

- 網段區隔
- 帳號安全
- 權限審查
- 脆弱性管
- 傳輸安全
- 金鑰管理
- 白名單 vs 黑名單
- 不明policy
- 無線網路密碼管理
- 無人區域無線網路

OSI 七層

Layer 1 實體層 Physical Layer, PHY	定義了最基礎的網路硬體標準，包括各種網路線、各種無線連線方式，各種設備規範、以及各種接頭的規則，還有傳輸訊號的電壓等等。 Repeater (1轉 1), Hub (1轉多)
Layer 2 資料連接層 Data-Link Layer	在這一層當中就制訂了 frame 的格式以及通過網路的方式。 包括訊框的資料格式、錯誤控制、流量控制、檢查資料傳輸錯誤的方法等等，常聽到的 MAC (media access control) 即在此層。 Physical address Bridge, Switch

OSI 七層 (續)

Layer 3 網路層 Network Layer	IP (Internet Protocol) 就是在這一層定義的， 同時也定義出電腦之間的連線建立、終止與維持等，資料封包 (packet) 的傳輸路徑選擇等等， 因此這個層級當中最重要的除了 IP 之外，就是封包能否到達目的地的路由 (route) 概念 Router
Layer 4 傳送層 Transport Layer	定義了發送端與接收端的連線技術，與封包格式，常見有： Transmission Control Protocol, TCP 技術，三向交握，具可靠性。 User Datagram Protocol, UDP 則為非可靠性。

OSI 七層 (續)

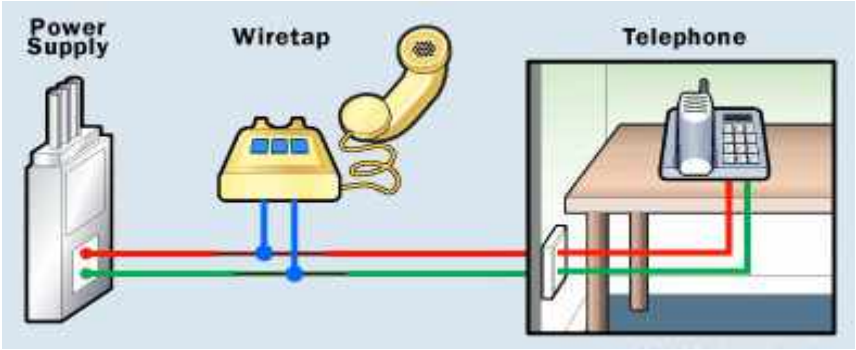
Layer 5 會談層 Session Layer	定義了兩個位址之間的連線通道之連接與掛斷，負責在資料傳輸中設定和維護電腦網路中兩台電腦之間的通訊連接。
Layer 6 表現層 Presentation Layer	將來自本地端應用程式的資料格式轉換(或者是重新編碼)成為網路的標準格式。在這個層級上面主要定義的是網路服務(或程式)之間的資料格式的轉換， 包括資料的加解密也是在這個分層上面處理。
Layer 7 應用層 Application Layer	與程式有關，提供為應用軟體而設的埠，以設定與另一應用軟體之間的通訊。例如: HTTP，HTTPS，FTP，TELNET，SSH，SMTP，POP3等

針對網路各層的攻擊手法

- 實體層
  - 線路搭接與線路私接
- 資料連結層
  - 封包監聽與ARP Spoofing
- 網路層
  - Source Route、Smurf 、Ping of Death
- 連線層
  - SYN Flood、DDoS及Session Hijacking
- 應用層
  - DNS Poisoning、Brute force Login、SQL Injection及Cross-Site Scripting

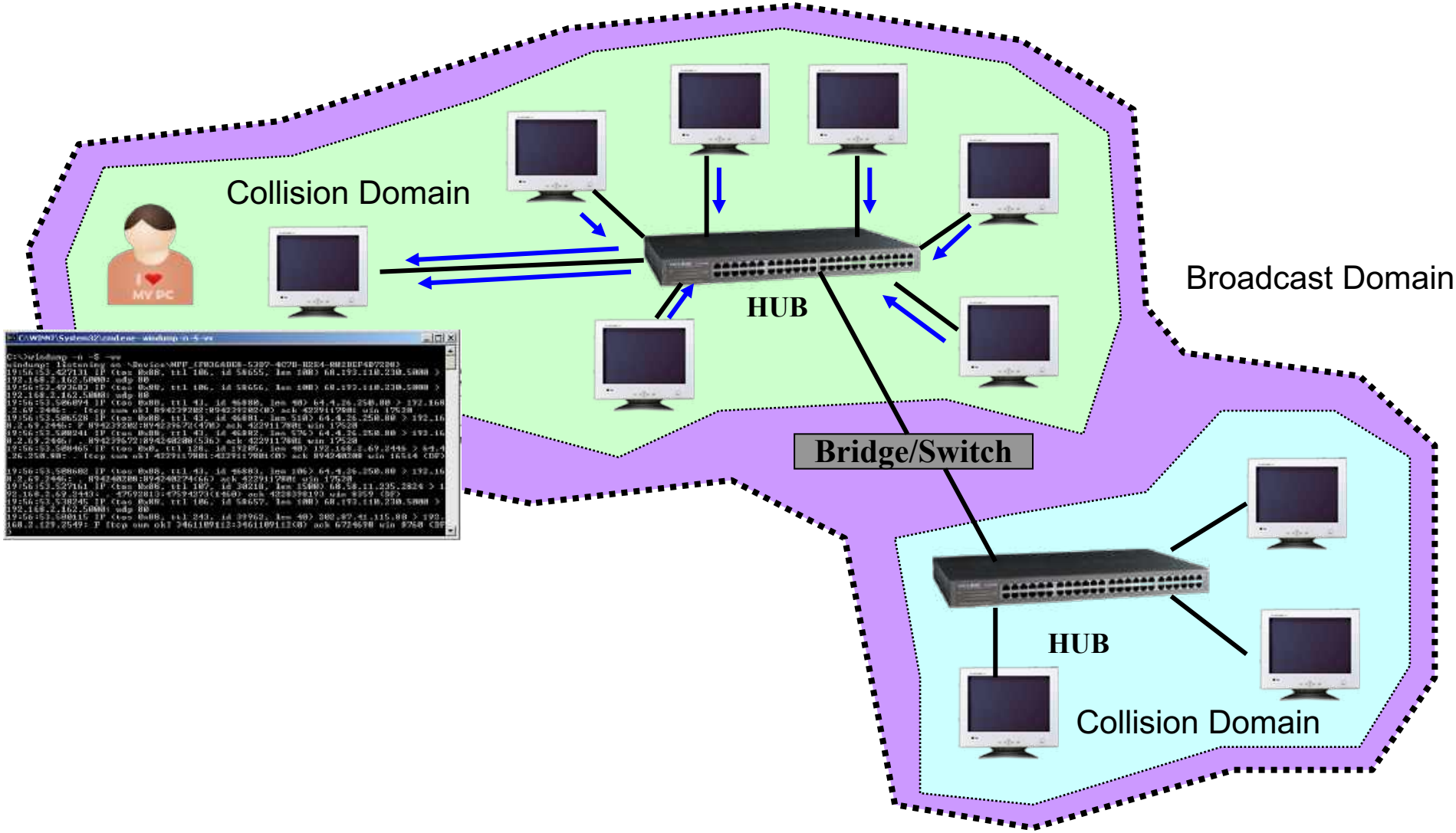
實體層

- 攻擊方式
  - 搭接線路(網路與電話)進行訊號竊聽
  - 私接線路變成隱匿通道(非控管中的線路)
- 防護建議
  - 機房、機櫃、線路室及管道間進行存取控管
  - 採用不同顏色區隔不同網段(安全區域)
  - 定期的線路盤查



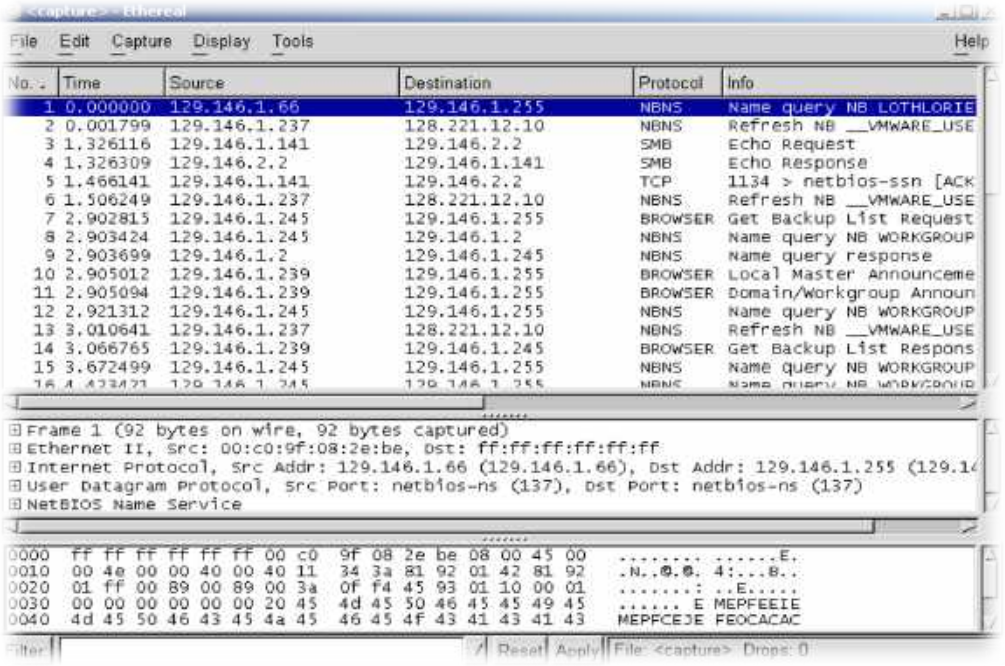
資料連結層 – 封包監聽(1/2)

- 透過工具或軟體被動蒐集網路封包



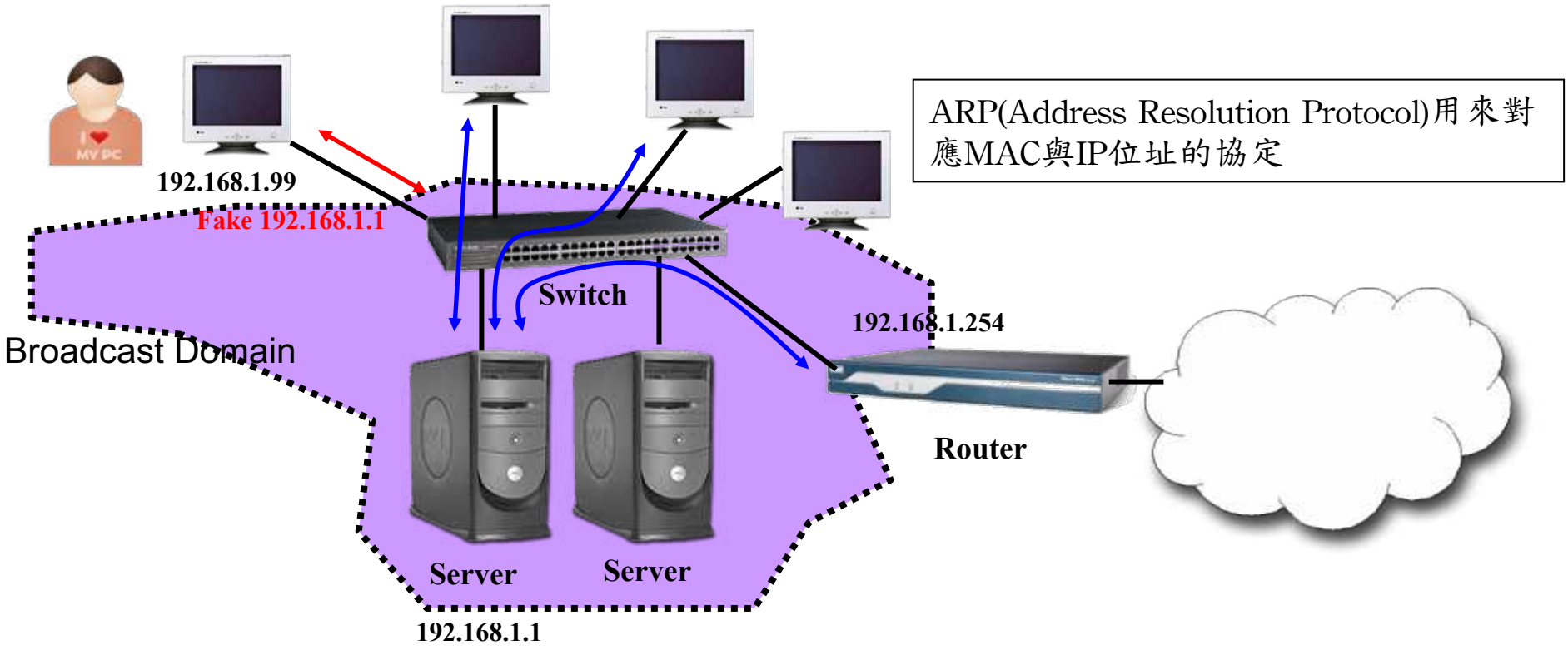
資料連結層 – 封包監聽(2/2)

- 監聽工具
  - Sniffer, MailSnarf
  - URLSnarf, WebSpy
  - Tcpdump ,Windump
  - Wireshark(Ethereal)
  - Ettercap
  - NetIntercept
- 防護建議
  - 採用加密連線(最佳方法)
  - 改用Switch (別用Hub, 全都聽)
  - 網路線路的實體存取控制，避免搭接或私接問題



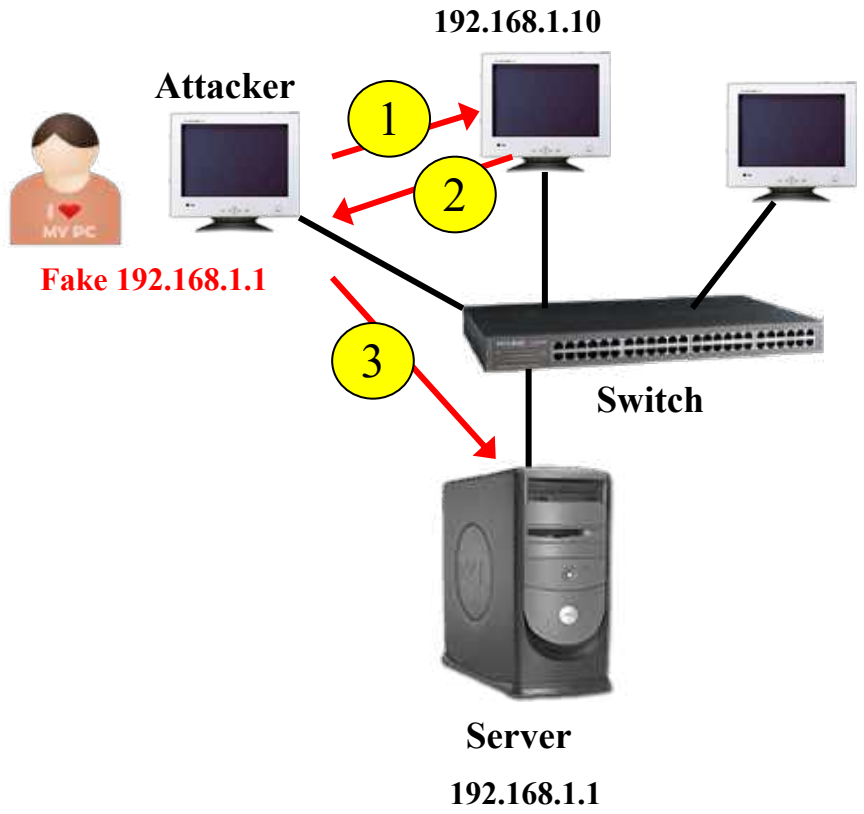
資料連結層 – ARP Spoofing(1/2)

- 又稱為ARP flooding、ARP poisoning或ARP Poison Routing
- 在Broadcast Domain下無法被動監聽其他電腦間連線封包
- ARP Spoofing攻擊強迫偽冒其他IP，讓攻擊者有機會監測到其他電腦間的通訊



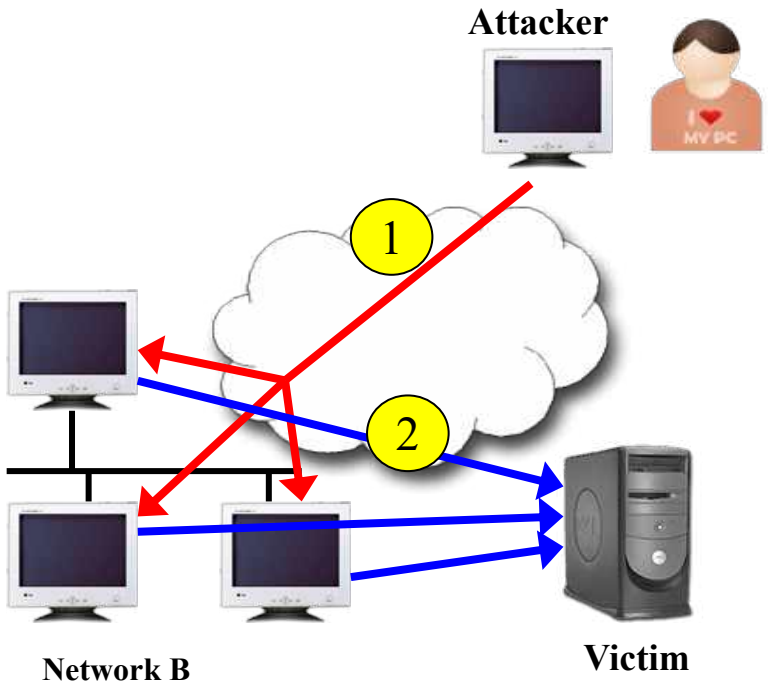
資料連結層 – ARP Spoofing(2/2)

- 攻擊手法
  - 攻擊者使用ARP Broadcast封包告訴其他電腦，192.168.1.1的MAC是Attacker的MAC
  - 其他電腦要傳送給192.168.1.1的封包會被送到Attacker
  - Attacker將封包錄下後轉送到真正的192.168.1.1
- 防護建議
  - 強制使用靜態ARP Table(小型網路)
  - 採用VLAN縮小Broadcast Domain的範圍
  - 啟用Switch中的Port、MAC及IP的對應控管



網路層 – Smurf Attack

- 藉由Ping封包塞爆受害者網路頻寬的阻斷服務攻擊
- 攻擊手法
  - 攻擊者(Attacker)偽冒受害者IP(Victim)發送大量Echo Request給B網段的Broadcast IP位址(B.255或B.0)
  - B網段所有電腦收到Echo Request封包，都回覆Echo Reply封包給Victim
  - 導致Victim端頻寬被大量的Echo Reply封包所占用
- 防護建議
  - 在防火牆或路由器上阻擋Network/Broadcast IP的傳送

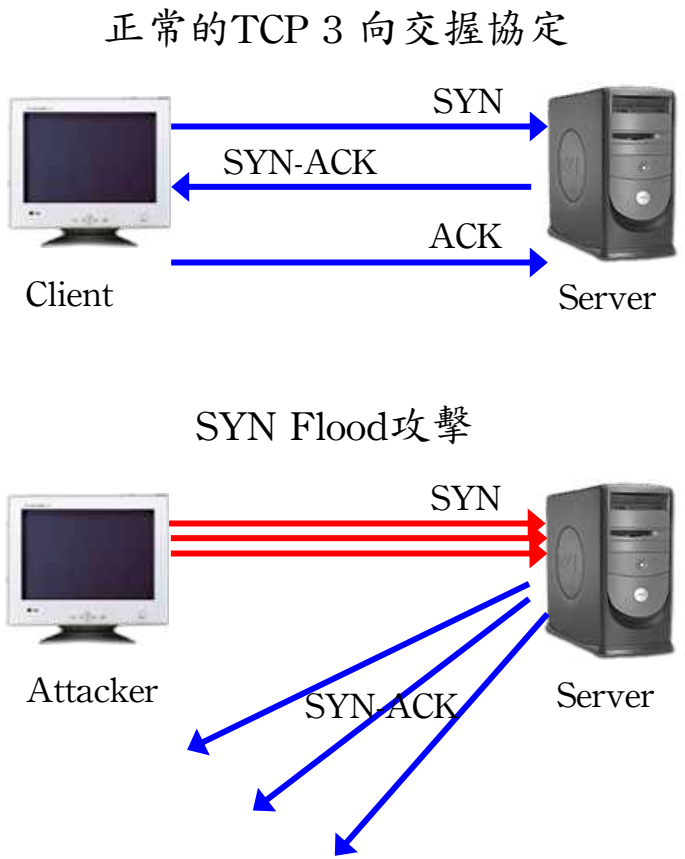


網路層 – Ping of Death

- 屬於一種阻斷服務攻擊，只要一個Ping封包就讓作業系統當機
- 攻擊手法
  - 一般正常的Ping封包大小為56位元(含IP標頭為84位元)
  - 攻擊者故意傳送一個大小超過65536位元的Ping封包給受害者(IP協定允許封包大於65536)
  - 受害作業系統無法處理大於65536位元的Ping封包，導致系統當機或重新開機
  - 攻擊者的來源IP經常是偽冒的IP位址
- 防護建議
  - 修補作業系統弱點(目前大部份作業系統都已修補這個弱點)

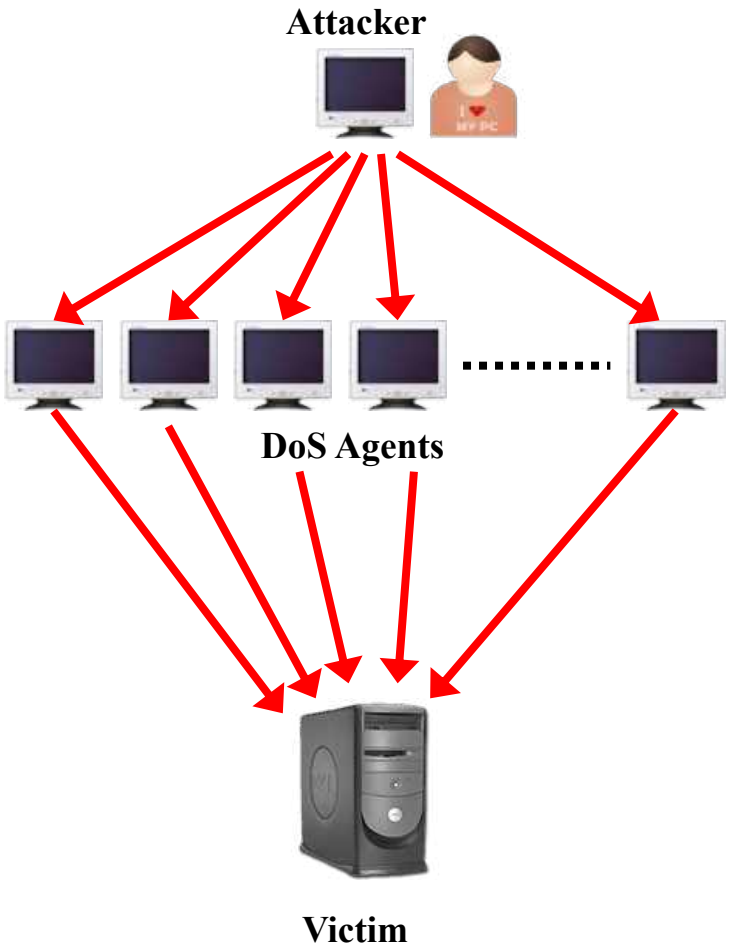
連線層 – SYN Flood

- 攻擊手法
  - 攻擊者傳送大量的TCP SYN請求封包到受害伺服器
  - 受害伺服器為每一個連線請求分配系統記憶體資源，導致系統連線資源被耗用殆盡，正常的連線無法建立
  - 大量惡意的TCP SYN封包，其來源IP通常也都是偽冒的，因此無法以封鎖來源IP阻擋攻擊
- 防護建議
  - 防火牆限制同來源IP的連線數量
  - 請求ISP協助



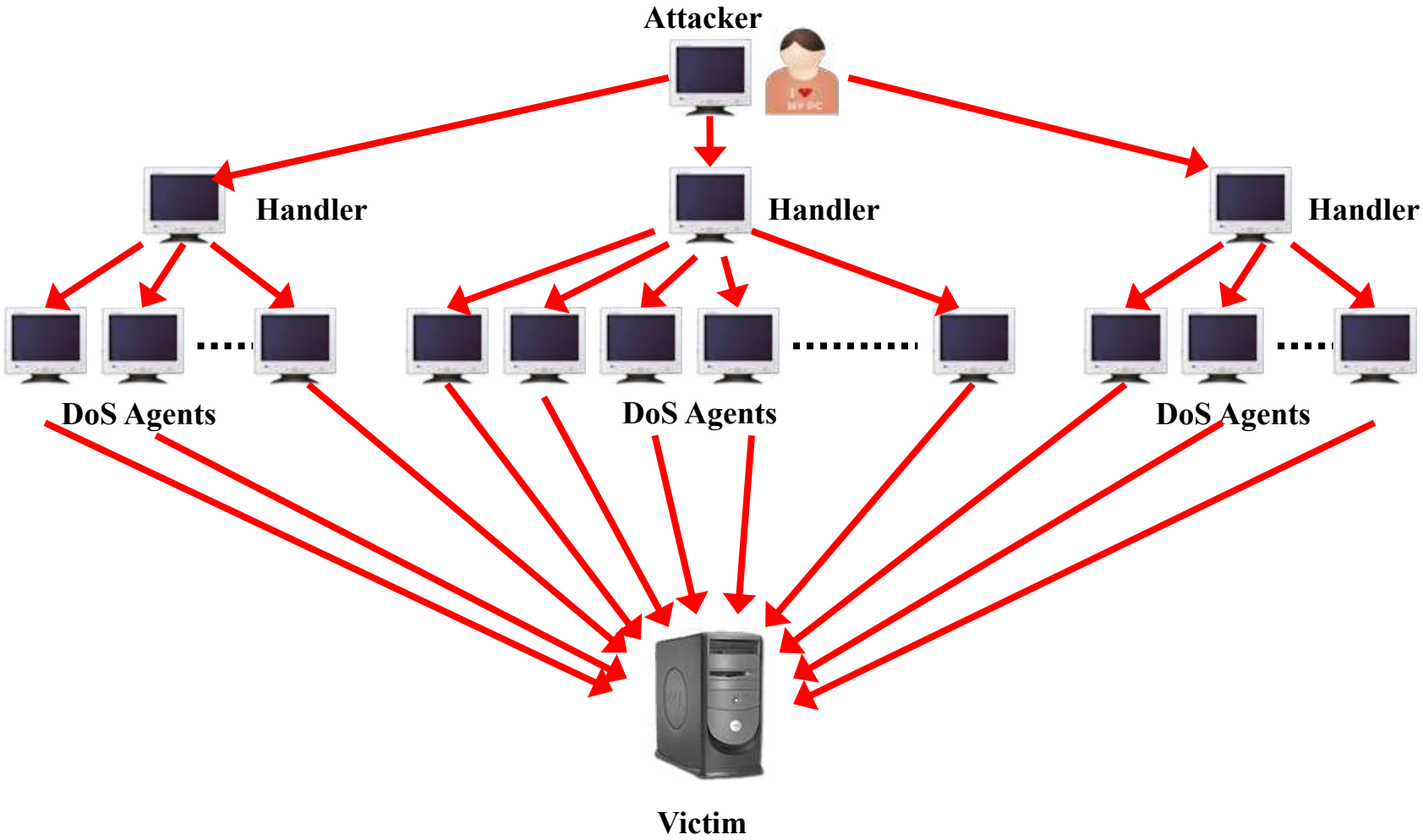
連線層 – 分散式阻斷服務攻擊(1/3)

- 分散式阻斷服務攻擊(Distributed Denial-of-Service，簡稱DDoS)
- 攻擊手法
  - 攻擊者控制多部阻斷服務攻擊主機(DoS Agent)，對受害者發動大規模的阻斷服務攻擊
  - 被攻擊的受害者為主要受害者，被控制的阻斷服務攻擊主機本身也是次要的受害者
  - 其攻擊來源IP太多(數百至數千個)，通常很難透過防火牆封鎖來源IP



連線層 – 分散式阻斷服務攻擊(2/3)

- 多層次的控制架構

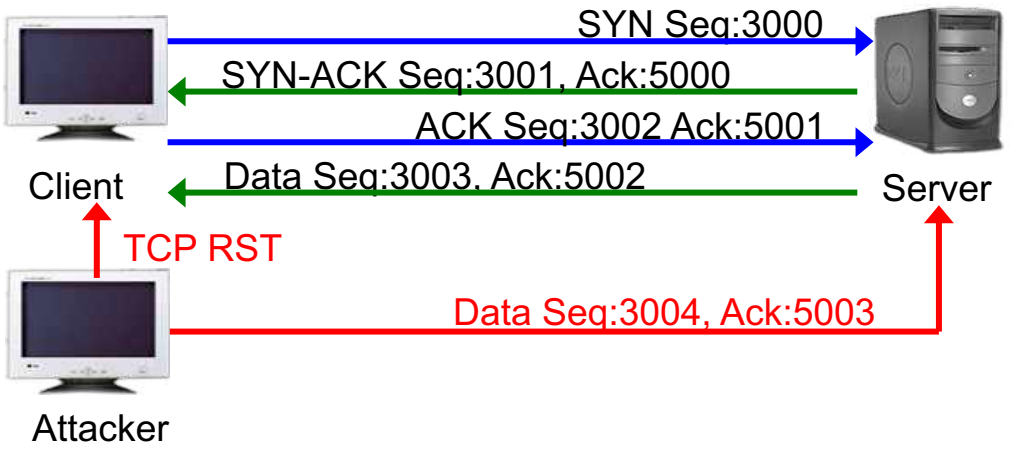


連線層 – 分散式阻斷服務攻擊(3/3)

- 防護建議
  - 防火牆限制同一來源IP的連線數量
  - 請求ISP協助
- 案例：巴哈姆特遭大陸駭客DDoS攻擊

連線層 – Session Hijacking

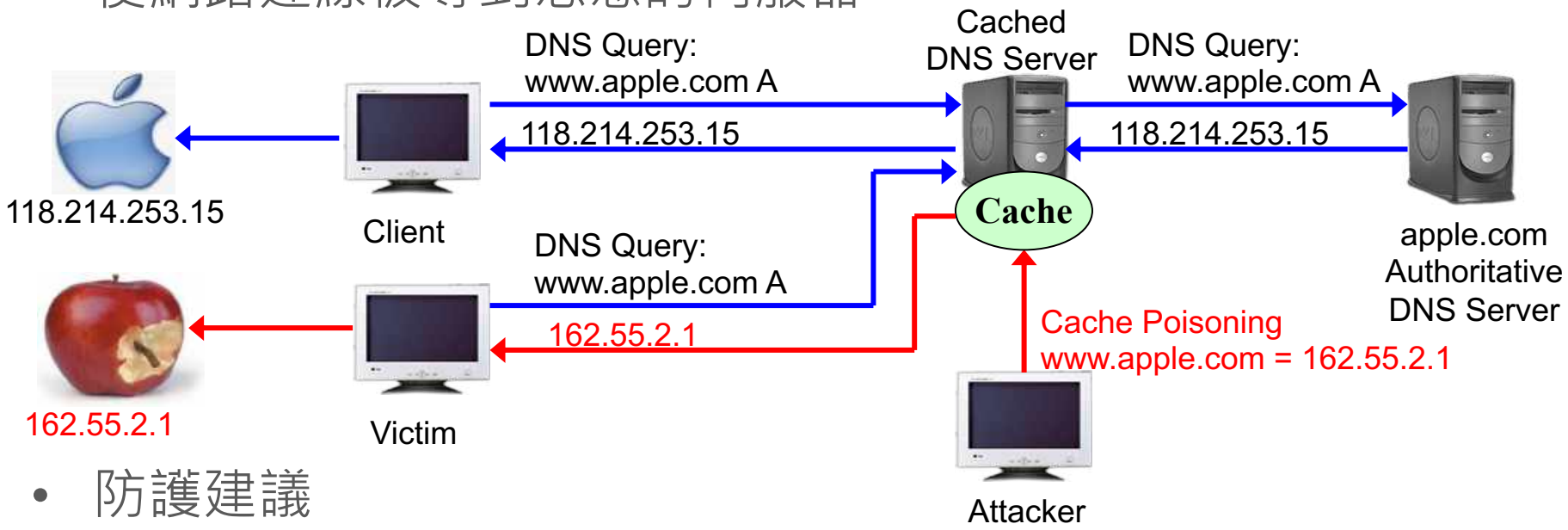
- 當合法使用者建立連線後，攻擊者從中攔截或取代該連線
- 可分為兩種類型
  - 主動型：攻擊者取代已建立之有效的連線
  - 被動型：攻擊者攔截連線後只監聽連線內容
- 攻擊的步驟
  - 追蹤連線過程
  - 連線去同步化
  - 注入攻擊者的封包
- 防護建議
  - 採用IPSec或SSL雙向認證的加密連線



當攻擊者可以預測到Client下一個封包的序號時，就可以偽冒Client的IP送出封包給Server，達到攔截連線的攻擊

應用層 – DNS Poisoning

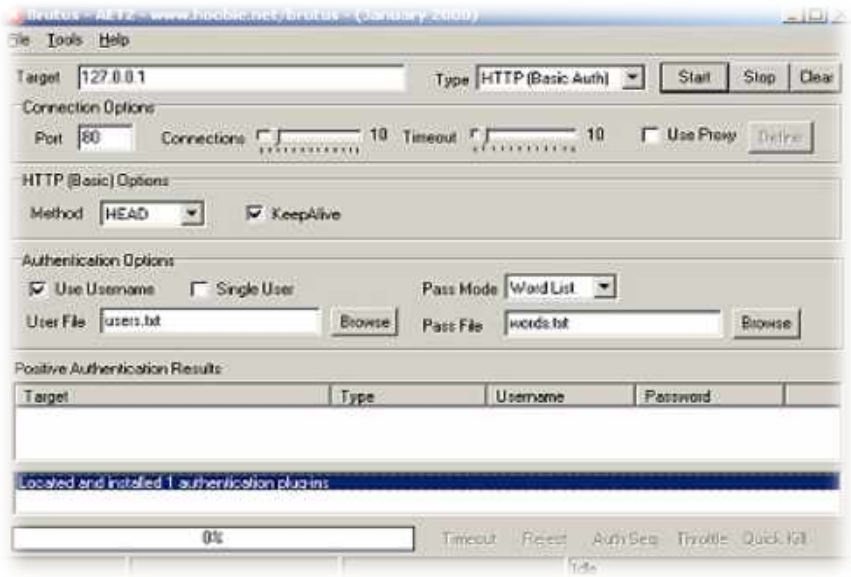
- 攻擊者藉由DNS伺服器的弱點，將錯誤的名稱解析植入DNS伺服器的快取區(Cache)中，導致DNS用戶端解析到錯誤的IP，使網路連線被導到惡意的伺服器

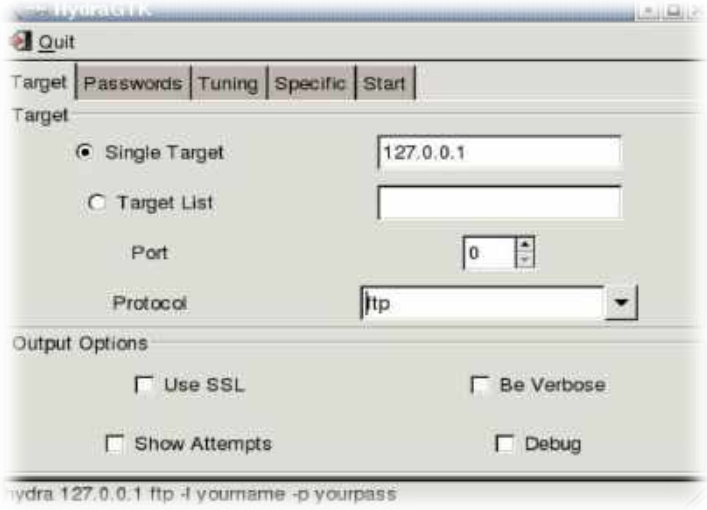


- 防護建議
  - 修補已知的DNS伺服器弱點
  - 區隔外部與內部DNS伺服器(不要forward到ISP的DNS)

應用層 – Brute force Login(1/2)

- 攻擊者透過通行碼猜測入侵應用系統的狀況相當常見，例如
  - TELNET login
  - SSH login
  - FTP login
  - SMTP AUTH
  - POP3 login
- 網路上有相當多的工具可自動進行通行碼猜測攻擊
  - Brutus
  - THC-Hydra





應用層 – Brute force Login(2/2)

- 建議防護
  - **限制同一帳戶連續簽入失敗之次數**，若超過次數則延遲簽入一段時間或關閉帳號，發出警告訊息
  - **強制使用者通行碼長度與複雜度**
  - **定期更換通行碼**

應用層 – SQL Injection

- 攻擊者可以將惡意之SQL指令插入程式碼的SQL指令中
- 資料庫之資料外洩、內容被修改、執行不當指令、植入後門...
- 弱點原理
  - 利用SQL語法漏洞
    - strSQL = "SELECT * FROM users WHERE (name = '" + userName + "') and (pw = '"+ passWord +"');"
    - 填入userName = "1 ' OR ' 1 '= '1 " 和 passWord = "1' OR '1'= '1";
    - 會變成： strSQL = "SELECT * FROM users WHERE (name = '1' OR '1'='1') and (pw = '1' OR '1'='1 ');"
    - 其實就是： strSQL = "SELECT * FROM users;"
- 防護建議
  - 過濾輸入值(例如：單引號與分號、限制長度等)
  - 採參數化查詢 (例：Prepared statement)
  - 網站應用程式源碼檢測

預備陳述

- Prepared statement
- 常態性執行效能會比較好
  - 因為SQL語句的分析，編譯，優化已經在第一次查詢前完成
- 參數化的查詢可以阻止大部分的SQL Injection
  - 語法：SELECT O FROM XXX WHERE id = ?
  - 在使用參數化查詢的情況下，資料庫系統（eg:MySQL）不會將參數的內容視為SQL指令的一部分來處理，而是在數據庫完成SQL指令的編譯後，才把輸入值當參數明用運行，因此就算參數中含有破壞性的指令，也不會被數據庫所運行

應用層 – Cross-Site Scripting

- 簡介
  - 簡稱XSS
  - 只用於客户端的攻擊方式，是攻擊者向有XSS漏洞的網站中輸入(傳入)惡意的HTML代碼(例如：JavaScript與VBScript)當其它用户瀏覽該網站時，這段HTML代碼會自動執行
  - 當其他使用者瀏覽到被置入惡意腳本的網頁時，使其瀏覽器執行惡意腳本 (HTML代碼會自動執行)

- 可能的損壞
  - 機密資訊被竊取(例如：Cookie與Session ID等)
  - 下載後門程式植入偽冒資訊
  - 重定向到其它網站等

應用層 – Cross-Site Scripting(續)

- **輸入字元檢查：**
  - 檢查該輸入字串是否含有可疑的 script 語法
  - 這邊要特別強調的是，XSS的防護不可以只靠輸入的檢查。
  - 要有效防止XSS一定要在輸出檢查並且做適當的 Encoding!

- **輸出檢查與 Encoding：**
  - 編碼後輸出，避免browser 執行不必要程式碼
  - 也就是將特殊的字元，特別是 < or > 轉換為 &lt or &gt
  - & → & (ampersand, U+0026)
  - < → < (less-than sign, U+003C)
  - > → > (greater-than sign, U+003E)

- **安裝防火牆：**
  - 透過防火牆，在 http communication protocol 過濾相關的 XSS

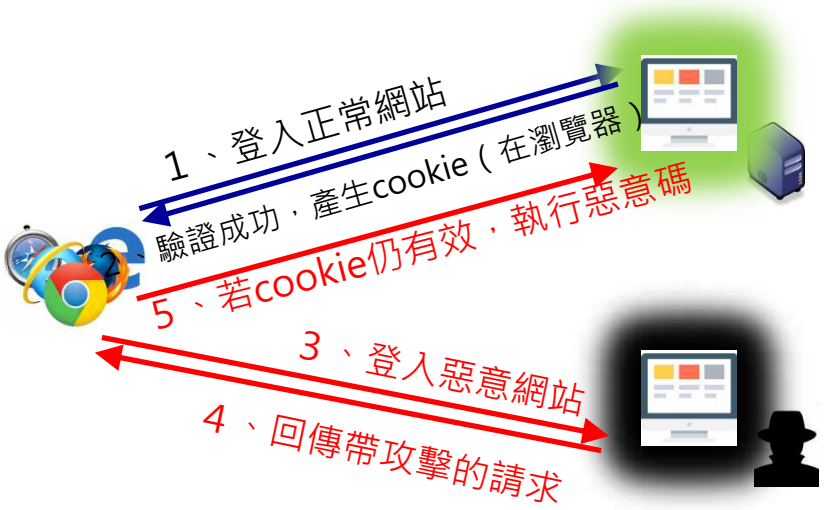
- **定期測試與驗證**
  - 可透過簡單下列語法，於網址、各個可以輸入的欄位與變數輸入下列值，
  - 若該網站有 XSS弱點，就會出現Test的視窗
  - <script>alert(‘test’)</script>

防護方式

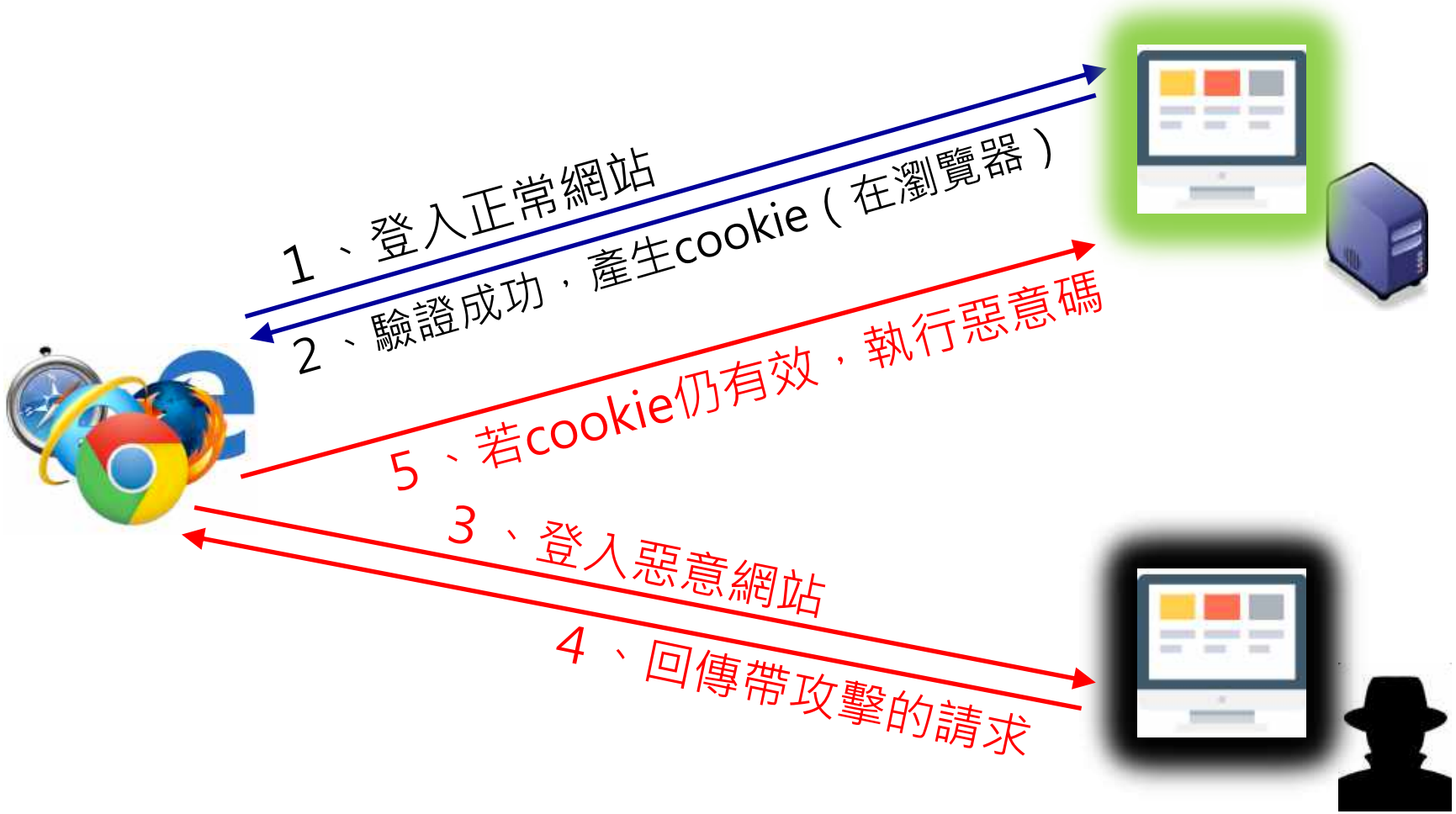
應用層 – SCRF

- Cross-site request forgery, SCRF of XSRF
- 也被稱為 one-click attack 或者 session riding
- 挾制用戶在當前已登入的Web應用程式上執行非本意的攻擊

- 防禦方式
  - 驗證HTTP Referer (檢查請求的來源地址)
  - 增加Token驗證(惡意站無法取得Token)，例如在server中隨意產生token值，存在Server 的session中
  - 驗證碼 (圖形、簡訊)



CSRF 示意

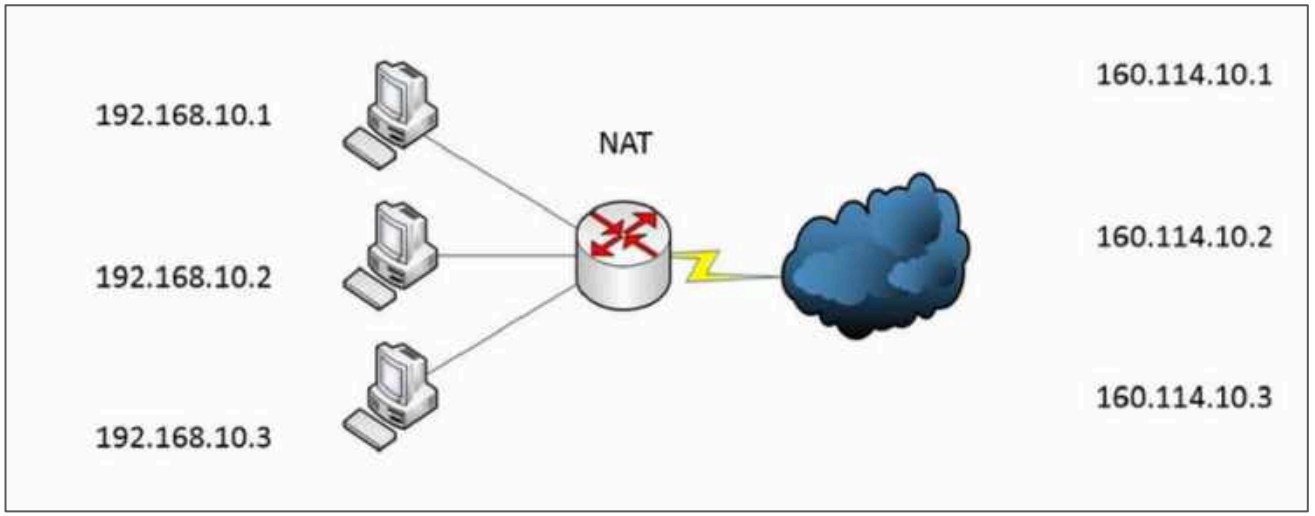

1、登入正常網站
2、驗證成功，產生cookie（在瀏覽器）
5、若cookie仍有效，執行惡意碼
3、登入惡意網站
4、回傳帶攻擊的請求

補充：私有IP (Private IP)

- 節省了IP位址資源
- 無法直接連接網際網路
- 需要使用網路地址轉換（Network Address Translator - NAT）或代理伺服器（proxy server）

IPv4 私有IP
10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

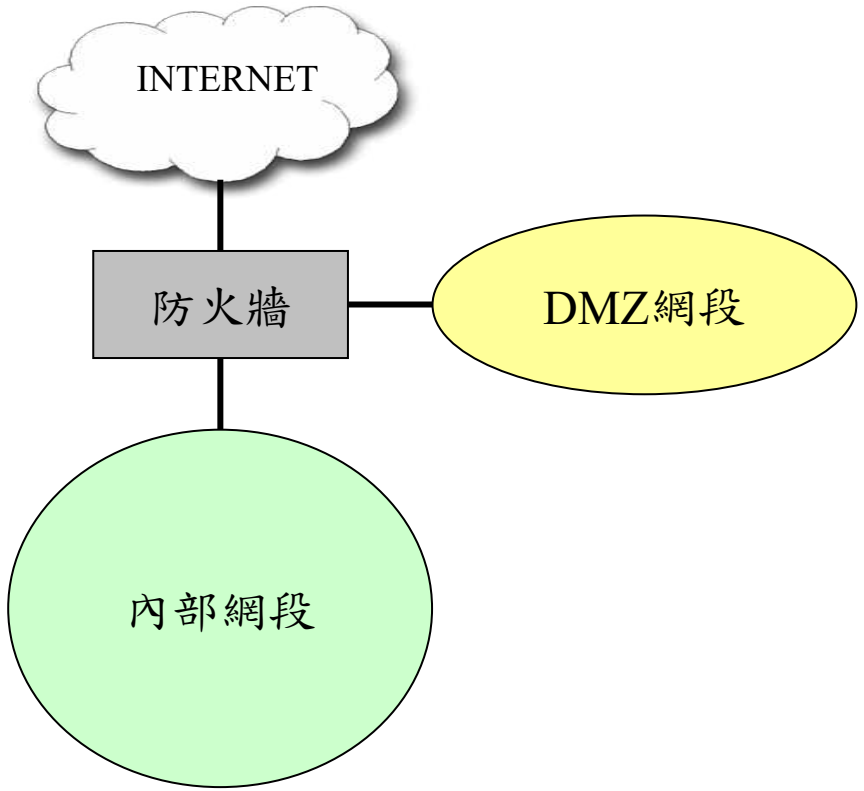
NAT



網路安全防禦系統

防火牆

- 主要用途
  - 區隔不同安全等級網段(例如：外部網路、內部網路及DMZ)
  - 偵測與阻擋網路層與連線層的攻擊
  - 落實網路存取政策



防火牆系統(續)

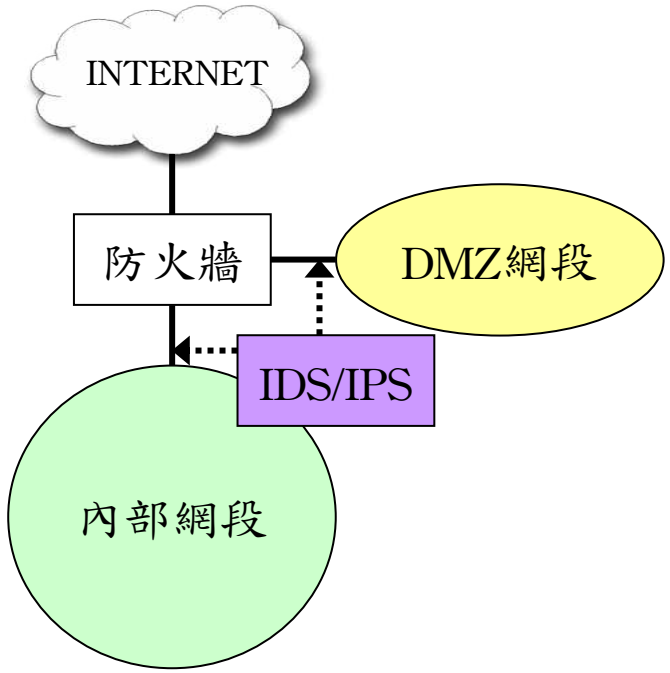
- 管理重點
  - 防火牆存取規則的變更應建立管理程序(變更申請、核准及記錄)
  - 防火牆存取紀錄應即時匯出存檔，並保留足夠的時間
  - 定期產出異常存取統計分析報表，進行異常處理
  - 防火牆存取控管規則應定期盤查(每年)
- 選購時重要規格
  - 防火牆本身的安全性(可參考Common Criteria EAL認證)、可區隔的網路區段數應符合組織需求(外、內及DMZ)、可支援的傳輸頻寬大小符合組織需求
  - 應可支援阻斷服務攻擊的偵測與防護

入侵偵測與防禦系統

- 主要用途
  - 識別網路的異常行為與攻擊行為(注意：SSL加密連線的內容無法識別)
  - 特定無誤判之攻擊行為可以立即阻擋
- 入侵偵測與防禦系統類型
  - 特徵碼比對
    - 比對攻擊特徵碼、判斷較精準
    - 只能偵測已知攻擊
  - 異常行為模式分析
    - 統計分析
    - 較易誤判
    - 能偵測未知類型攻擊

入侵偵測與防禦系統(續)

- 入侵偵測的反應方式
  - 被動方式：只將異常事件記錄下來，供日後稽核分析使用
  - 主動方式：立即將攻擊事件或攻擊來源進行封鎖
- 入侵偵測的部署
  - 監聽模式：不影響網路部署，但防禦效果較差
  - Bridge模式：防禦能力較強可以阻擋TCP/UDP類的攻擊
  - 主要偵測DMZ與內部網段進出口

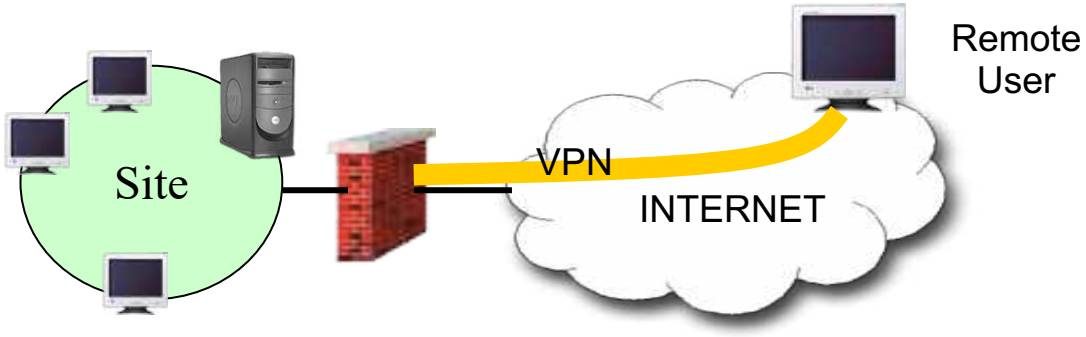


入侵偵測與防禦系統(續)

- 管理重點
  - 入侵行為特徵碼應隨時更新
  - 入侵偵測之異常事件應定期分析(每週)，或委由資安監控中心隨時監控
  - 入侵偵測存取紀錄應即時匯出存檔，並保留足夠的時間
- 選購時重要規格
  - 可偵測的網路區段數應符合組織需求(內與DMZ)
  - 可支援的頻寬大小符合組織現有網路狀況

虛擬私有網路系統

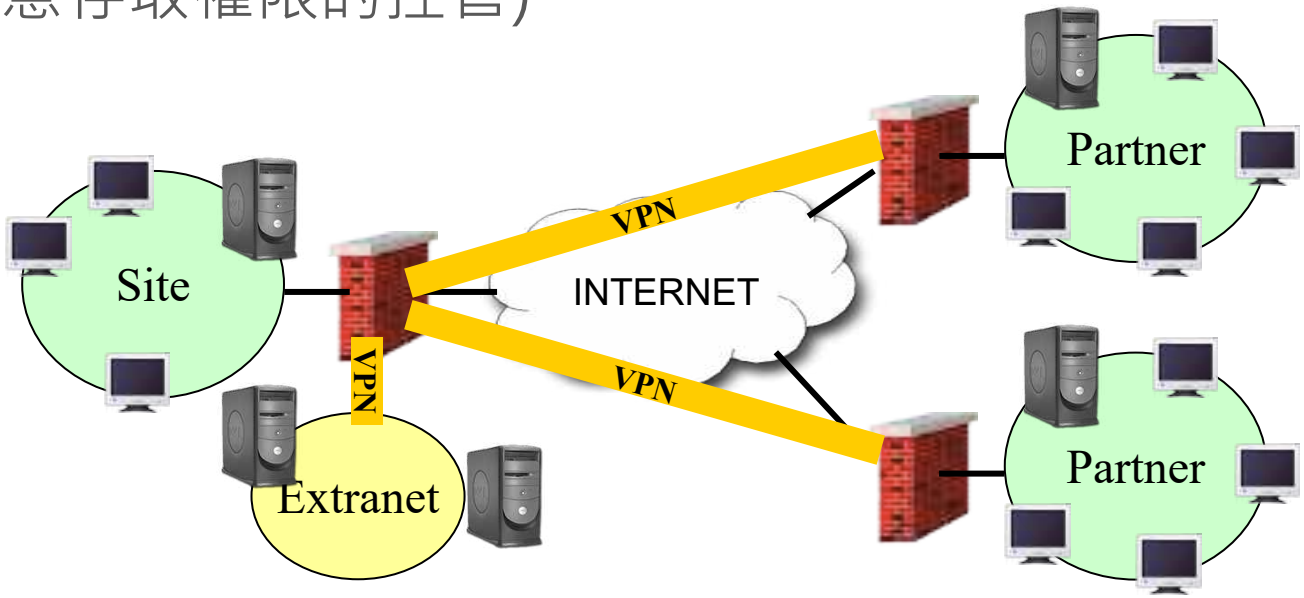
- 虛擬私有網路(Virtual Private Network，簡稱VPN)主要用途
  - 在公開的網路上建立私有的安全通道
  - 包含身分鑑別與加密以保護通訊資料的完整性與機密性
- VPN的類型
  - 遠端使用者存取VPN：外勤人員透過網際網路與內部網路建立的安全通道



虛擬私有網路系統(續)

- Site-to-Site VPN：總部與分點之內部網路透過網際網路建立安全通道

- Extranet VPN：與合作伙伴間透過網際網路建立安全通道(注意存取權限的控管)



虛擬私有網路系統(續)

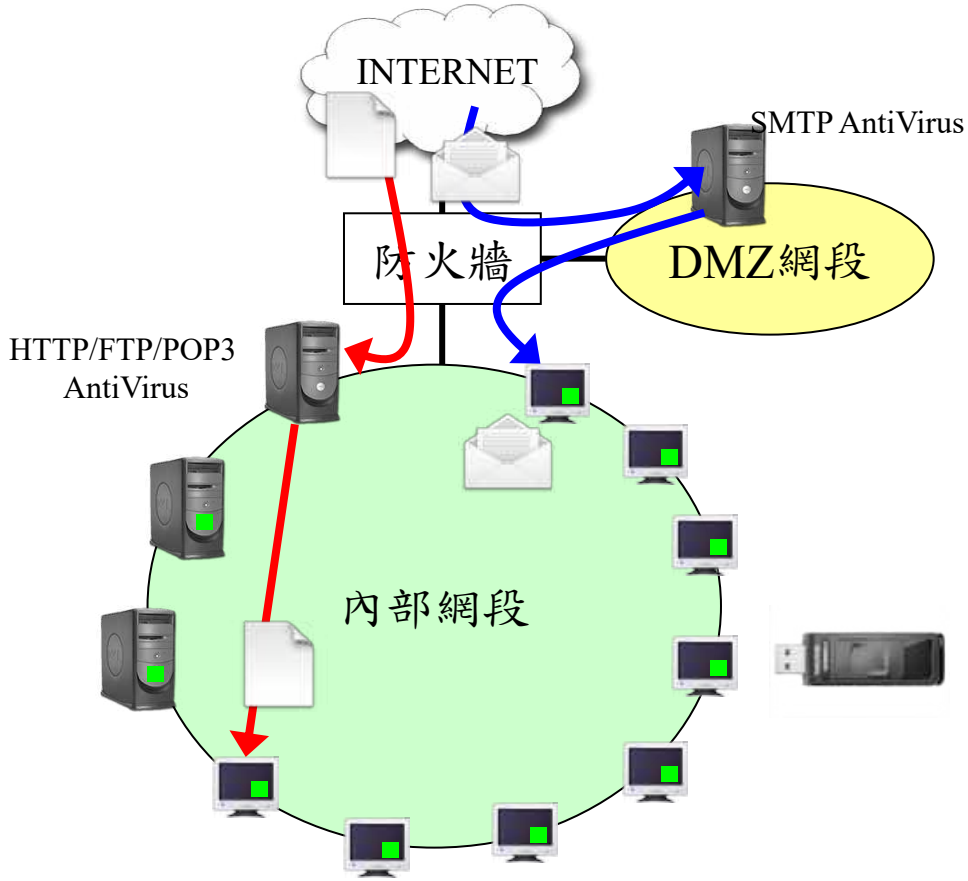
- 使用VPN的好處(與實體私有網路比較)
  - 部署較彈性
  - 可擴充性較高
  - 線路成本較低
- VPN協定
  - PPTP： Point to Point Tunnel Protocol (OSI L2)
  - L2TP： Layer 2 Tunneling Protocol (OSI L2)
  - IPSec：適用於遠端使用者存取VPN、Site-to-Site VPN及Extranet VPN
  - SSL：好處是不必裝任何用戶端軟體，瀏覽器幾乎都有支援
- 目前大部份防火牆產品已內建VPN功能

虛擬私有網路系統(續)

- 管理重點
  - 虛擬私有網路的建立與使用者帳號的申請，應建立管理程序(變更申請、核准及記錄)
  - 定期分析異常事件，例如：VPN使用者簽入失敗
  - VPN存取紀錄應即時匯出存檔，並保留足夠的時間
- 選購時重要規格
  - 可支援的VPN數量或使用者連線數量應滿足組織需求
  - 本身應具備防火牆功能，以控管VPN連線的存取
  - 與其他不同廠牌產品建立VPN連線的相容性

防毒系統

- 主要用途
  - 防止病毒、蠕蟲、間諜、後門及木馬等惡意程式入侵電腦系統
- 惡意程式的來源
  - 電子郵件
  - USB硬碟
  - 網站瀏覽
  - 即時通訊
  - 檔案傳輸/分享
- 全面防毒的部署
  - 個人電腦與伺服器防毒
  - 電子郵件防毒匣道
  - 上網防毒匣道



防毒系統(續)

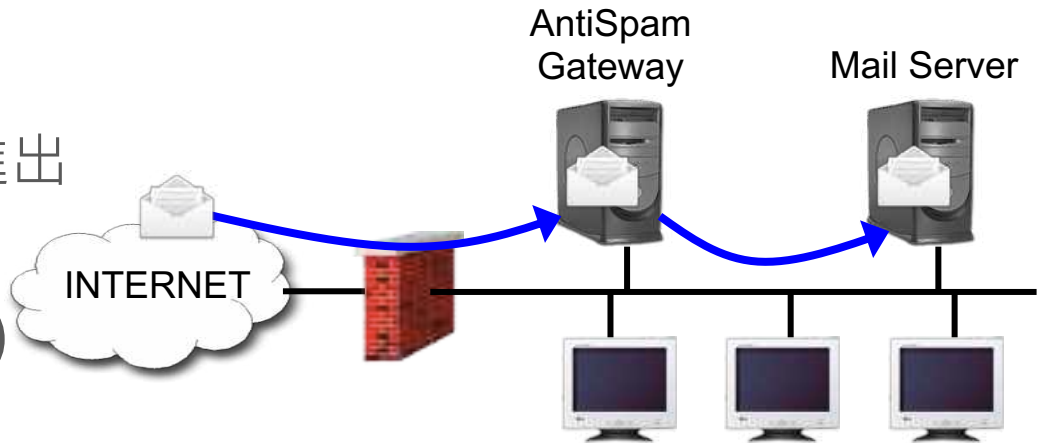
- 管理重點
  - 應定期自動更新病毒碼
  - 病毒感染的事件與趨勢應定期分析
  - 避免未安裝防毒軟體的電腦上線(配合上網管控設備)
  - 防火牆控管未經防毒匣道過濾的連線行為
  - 「個人電腦與伺服器防毒系統」與「防毒匣道系統」可採用不同廠牌
- 選購時之重要規格
  - 病毒偵測的精準度、對電腦效能的影響
  - 是否提供中央控管機制
  - 可支援的網路連線偵測能力(電子郵件與即時通訊)

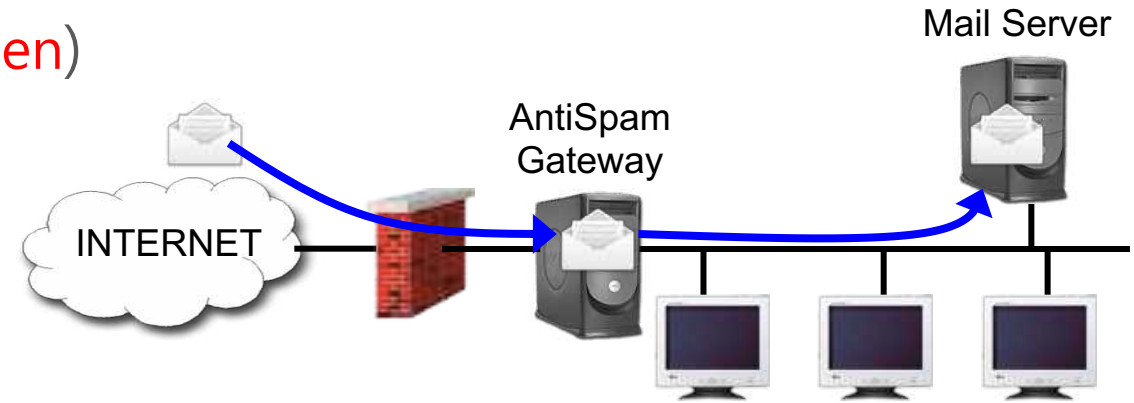
垃圾郵件過濾系統

- 主要用途
  - 過濾垃圾與廣告郵件
  - 避免電子郵件社交工程攻擊
  - 提升人員電子郵件使用安全
- 垃圾郵件的判斷技術
  - 關鍵字比對(中文字，包含附件)
  - 內容過濾條件
  - 外部資料庫比對(DCC、Razor、Pyzor)
  - 貝氏演算法(自動學習機制)
  - 圖片辨識技術

垃圾郵件過濾系統(續)

- 部署方式
  - 匣道模式(Mail Relay)
    - 不影響其他網路流量
    - 設備故障時信件無法進出
    - 安全性高(Fail Close)
  - Bridge模式(**目前較少見**)
    - 會影響其他網路流量
    - 設備故障時會自動Bypass流量
    - 安全性較低(Fail Open)



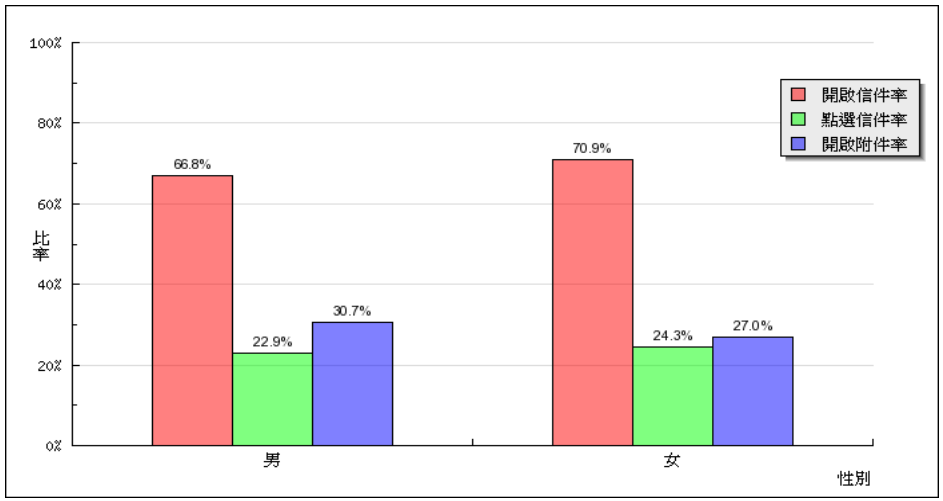


垃圾郵件過濾系統(續)

- 管理重點
  - 應定期自動更新垃圾郵件辨識特徵碼
  - 電子郵件過濾規則的變更應建立管理程序(變更申請、核准及記錄)
- 選購時之重要規格
  - 垃圾郵件判斷的精準度
  - 處理效能可符合組織需求
  - 對於中文信件或多國語言的支援能力
  - 全文檢索支援中文的能力與郵件附件的檢索能力
  - 圖片廣告信件的支援能力

電子郵件社交工程攻擊與防護

- 技術面防護
  - 建置垃圾郵件過濾系統(預估可過濾90%的垃圾信件)
  - 用戶端郵件收發軟體(例如：Outlook)的安全設定
    - 以文字模式閱讀信件
    - 關閉自動下載外部元件
    - 關閉「收件匣」預覽視窗
- 管理面防護
  - 訂定使用者電子郵件使用規範
  - 定期實施電子郵件安全宣導課程
  - 定期實施電子郵件社交工程演練，並針對未符合使用規範的人員進行宣導或訓練



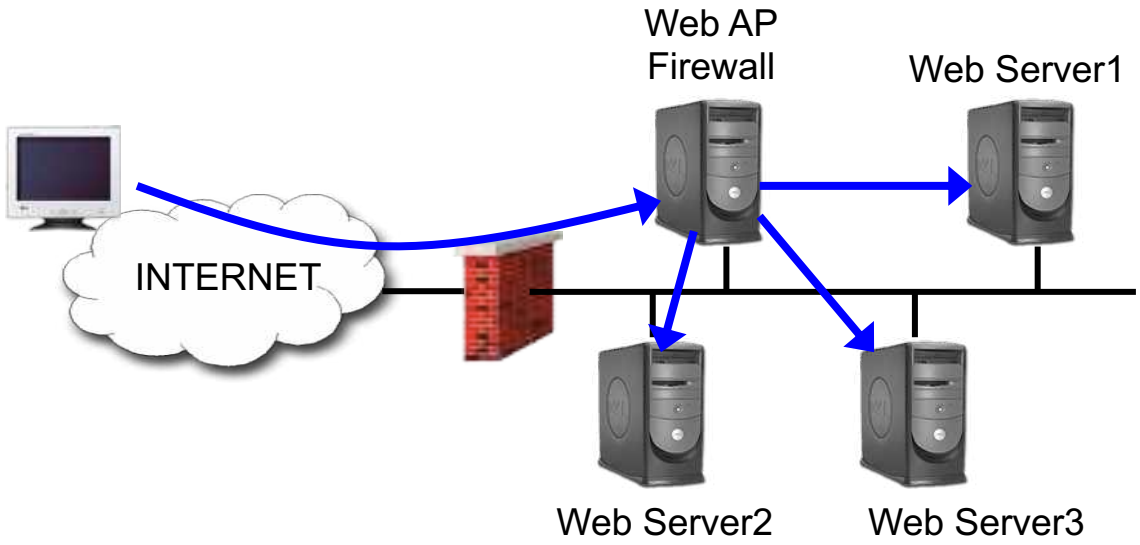
網站應用程式防火牆

- 主要用途
  - Web Application Firewall，簡稱WAF
  - 偵測與防禦針對網站應用程式之攻擊行為
  - 例如：SQL Injection 與 Cross-Site Scripting等

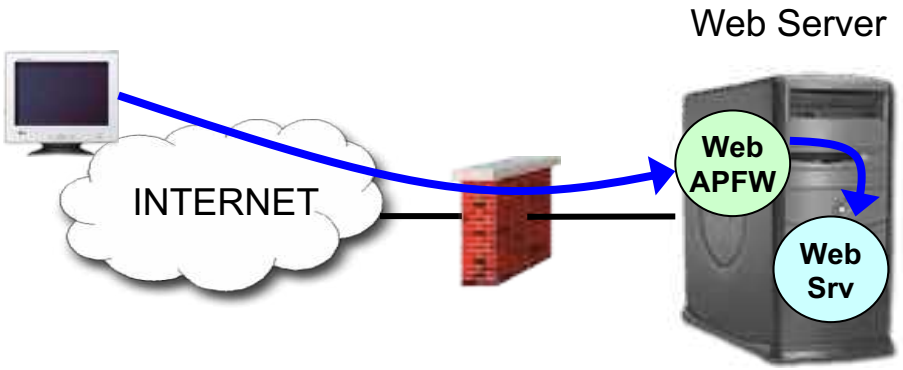
- 偵測與過濾技術
  - 白名單(自動學習)，只有列在白名單的網頁與參數才能通過，其他一律拒絕。
  - 攻擊特徵判斷是目前較常用的作法，但會有誤判與漏判的問題

網站應用程式防火牆(續)

- 類型與部署方式
  - 硬體式



  - 軟體式



網站應用程式防火牆(續)

- 管理重點
  - 存取規則的變更應建立管理程序(變更申請、核准及記錄)
  - 異常的網站應用程式攻擊事件應立即匯出，並保留足夠的時間
  - 異常的網站應用程式攻擊事件應定期分析，並進行異常的處理
- 選購時之重要規格
  - 處理效能應符合組織網站流量需求
  - 中文URL及傳輸內容的判斷能力
  - HTTPS的加密連線可先在網站應用程式防火牆解密過濾後，再轉到後端真正的網站(IDS/IPS無法判斷HTTPS連線)

範例考題

下列何者非社交工程攻擊方式？

- (A) 利用電子郵件誘騙使用者登入偽裝之網站以騙取帳號及通行碼
- (B) 利用程式設計缺陷，向程式寫入錯誤的內容
- (C) 利用即時通訊軟體如LINE，偽裝親友來訊，誘騙點選來訊中之連
- 結後中毒
- (D) 利用電話佯裝資訊人員，騙取帳號及通行碼

下列哪個協定較為安全？

- (A)HTTP
- (B) FTP
- (C)SSL
- (D)TELNET

短時間內傳送大量的封包給另一部電腦的攻擊方式，稱之為？

(A)木馬程式或殭屍病毒

(B)釣魚郵件攻擊

(C)阻斷服務攻擊

(D)中間人攻擊

請問SSH常見的服務Port為？

- (A)22
- (B)23
- (C)24
- (D)25

在未經授權的情況下取得網路傳輸資料，或者針對傳輸網路進行流量分析，請問上述行為屬於下列何者常見的網路威脅？

- (A) 截斷（Interruption）
- (B) 竊取（Interception）
- (C) 偽造（Fabrication）
- (D) 篡改（Modification）

網際網路中主要的通訊協定模式有兩種OSI 7層及TCP/IP協定組，請問在這兩個通訊協定模式中，負責傳輸封包（Packet）及選擇路徑（Routing），是那一層的工作？

- (A)實體層（Physical Layer）
- (B) 資料鏈結層（Data-Link Layer）
- (C)網路層（Network Layer）
- (D)應用層（Application Layer）

下列何者不是應用在「虛擬私有網路」（VPN）上的通訊協定？

- (A)TFTP
- (B) PPTP
- (C)IPSEC
- (D)SSL

請問TCP/IP通訊協定中，負責提供分段排序、錯誤控制、流量控制等工作是哪一層之任務？

- (A)應用層
- (B) 會議層
- (C) 傳輸層
- (D)網路層

公司的資安人員想要安全性的監控網路上所有的交換器和路由器的狀態，請問他需要在每個設備上設定哪個協定？

- (A)STP (spanning tree protocol)
- (B) VLAN (Virtual LAN)
- (C) MPLS (Multi-Protocol Label Switching)
- (D)SNMPv3 (Simple Network Management Protocol)

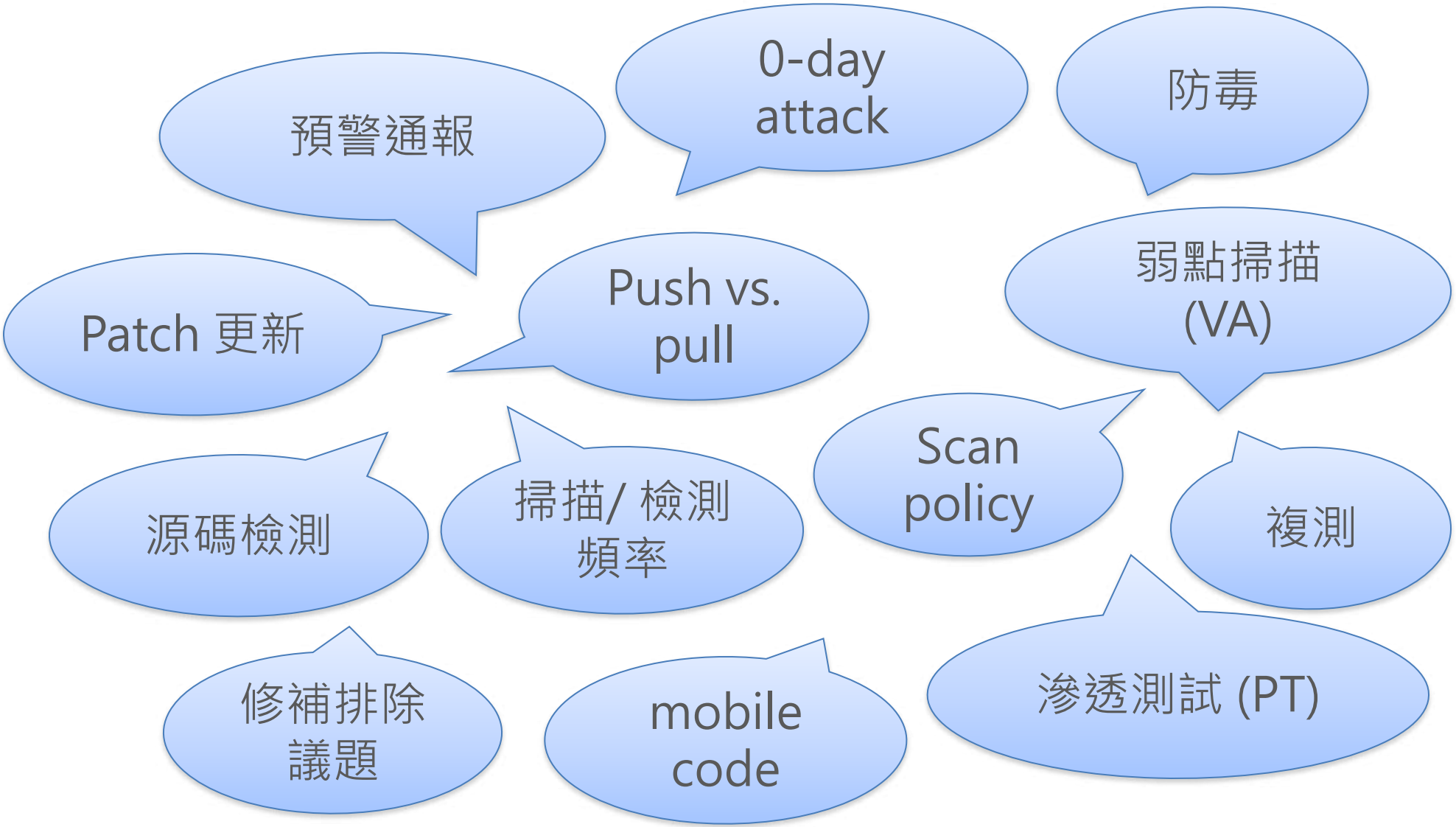
網頁中使用驗證碼(CAPTCHA)主要可防禦下列何種攻擊？

- (A)SQL注入攻擊(Injection)。
- (B) 跨站腳本攻擊(XSS)。
- (C) 緩衝區易位攻擊(Buffer Overflow)。
- (D)跨站偽造請求攻擊(CSRF)。

評鑑主題八
資安維運技術

1. 惡意程式防護與弱點管理
2. 資料安全及備份管理
3. 日誌管理

重要字辭與定義


預警通報
0-day attack
防毒
Patch 更新
Push vs. pull
弱點掃描 (VA)
源碼檢測
掃描/ 檢測頻率
Scan policy
複測
修補排除議題
mobile code
滲透測試 (PT)

重要字辭與定義


日誌啟用vs
存放空間
日誌審查
(SOD)
False
negative/
positive
關聯分析
異質正規化
SOC
SIEM

重要字辭與定義


RPO與備份頻率
分級(機密等級/可用性等級)
備份時間/回復時間
銷毀
完整、差異、增量備份
實體傳送安全
備份資料存放安控等級
留存時間
上鎖/分持
回復測試/可讀測試

常見議題

- 分類與標示
- 可移除試媒體管理
  - 擺渡計畫
- 媒體汰除報廢
- 實體媒體傳送
- 惡意軟體防護
- 備份

- 使用者管理
  - 註冊、註銷、異動
- 使用者鑑別資訊管理
- 特殊權限管理
- 權限審查
- 電子傳訊安全
- NDA
- 脆弱性管理
- 技術性審查
- 日誌管理

弱點掃描 Vulnerability Scan

- **系統弱點掃描 (VA)**
  - 針對作業系統的弱點、網路服務的弱點、作業系統或網路服務的設定、帳號密碼設定及管理方式等進行檢測
    - 可分為到場服務與遠端服務
    - 弱點掃描服務報告 (掃描與複掃均需提供)
- **網站弱點掃描(Web VA)**
  - 係針對組織對外主機網頁安全弱點進行掃描
    - 可分為到場服務與遠端服務
    - 弱點掃描服務報告 (掃描與複掃均需提供)

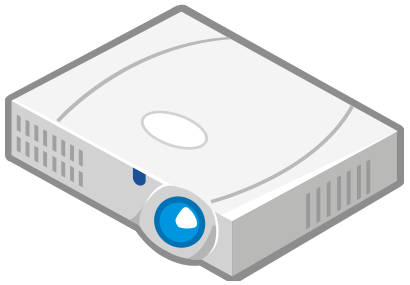
滲透測試 Penetration Test

- 利用各**伺服器 / 主機**的作業系統、應用軟體、網路服務等系統設備之安全弱點與漏洞，進行滲透或穿透跳躍主機之入侵測試，設法取得未經授權之存取權限，並測試內部資訊是否有遭受不當揭露、竄改或竊取之可能性

測試類型	測試類別
作業系統	遠端服務、本機服務
網站服務	設定管理、使用者認證、連線管理、使用者授權、邏輯漏洞、輸入驗證、Web Service、Ajax
應用程式	電子郵件服務套件、網站服務套件、檔案傳檔服務套件、遠端連線服務套件、網路服務套件、其它常見應用程式或網路套件之弱點測試項目
密碼破解	密碼強度測試

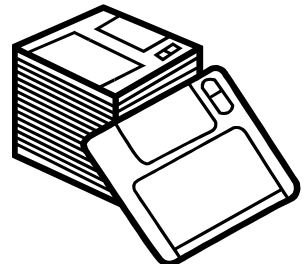
資料備份

- 資料備份的目的為對抗資料毀損的威脅，以保護資料的可用性
- 檔案資料的備份
  - 個人使用者可為自己的重要資料進行備份
  - 備份媒介可為光碟、行動碟或其他電腦
  - 組織應有系統人員對內部重要系統與檔案統一進行備份
  - 備份媒體多為大型備份設備或系統，速度快且穩定性高
- 資料庫資料備份
  - 由系統人員定期備份



資料備份(續)

- 備份方式
  - 完整備份（Full Backup）
  - 差異備份（Differential Backup）←和full 差別
  - 增量備份（Incremental Backup）←和前次差別
- 備份模式
  - 異地與本地兩種
- 備份頻率
  - 與回復點目標 RPO (Recovery Point Objective)
- 回復測試

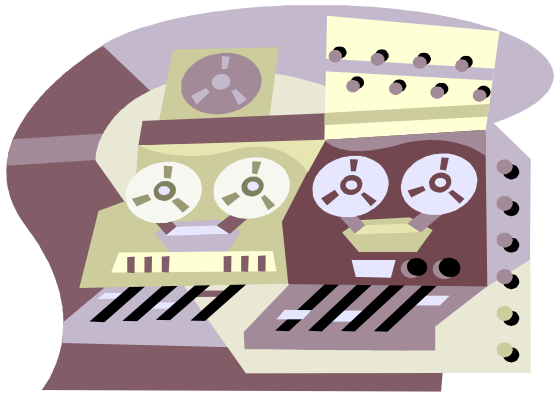


資料備份(續)

- **應備份的範圍與設定應該事先評估審慎取捨**
- 備份媒體的問題
  - 資訊設備變化甚快，應定期檢驗備份媒體是否仍有合適的存取設備
- 檔案格式的問題
  - 備份檔案的格式，可能因年代久遠而找不到相容的工具可以開啟，應定期檢查備份檔案，確認仍有合適的應用軟體或工具可開啟
- 儲存相同檔案之一致性問題
  - 在不同電腦中使用相同檔案時，應盡量使用單一版本。例如透過檔案伺服器提供多人存取
  - 如電子檔案需儲存於多處時，則須作好版本管理

電子資料儲存之安全威脅

- 電子檔案存放主機受攻擊
  - 主機遭入侵或植入後門
  - 使用者不當安裝具有安全威脅的軟體(例如：可進行電子檔案分享的P2P傳檔軟體)
  - 導致電子檔案遭竊、竄改或破壞
- 資料庫資料遭到刪除、竄改或竊取
- 系統弱點漏洞的管理不當也會造成電子資料儲存之安全威脅



資訊安全監控中心(SOC)

- SOC(Security Operation Center)一種集中式的安全監控機制，目的在於整合並管理組織各種不同環境下的資安訊息，並且對安全事件做出對應的機制
- SOC可以**即時收集**可能危害組織網路安全的的事件，加以整合及分析，並提出解決的方法，以確保組織單位網路安全

為什麼需要SOC

- 數量龐大的資安事件及系統紀錄等需要被處理或管理，讓網管或資安人員難以逐一處理
- 單一的資安產品無法提供完整的資安防護功能。應將資安防護視為一服務流程(service process)
- 將安全需求訂定成資安政策，並整合相關資安技術產品和緊急應變中心，而架構成的**資訊安全監控中心(Security Operation Center, SOC)**，為整體資安防護的趨勢

為什麼需要SOC？(續)

- 為了防護多變且組織化的駭客攻擊，如進階持續性威脅(Advanced Persistent Threat)，應利用資安防護中心協助蒐集及分析資安事件，找出有用的或是被駭客攻擊的相關資訊，來加強網路攻擊防禦

SOC的主要功能

- 基本功能
  - 資安警訊管理
  - 資安弱點管理
  - 資安設備管理
  - 資安事件監看
  - 資安事故處理
- 一個SOC 會對多個監看區域以分散收集、集中管理方式達成上述功能

範例考題

**

關於系統日誌的管理與分析，下列敘述何者不正確？

- (A)每天不斷產生的日誌，資料量龐大，往往超出人力可以判讀的範圍
- (B) 預設的Syslog本身沒有加密，但是不會遭到偽冒攻擊
- (C)混合式攻擊手法普遍，很難從單一設備上解讀出攻擊手法的資訊
- (D)不同設備所產生的日誌格式可能不一樣，會造成彙整上的困難

請問2017年的Wannacry攻擊是攻擊哪個服務？

- (A)SMB
- (B) SMTP
- (C)HTTP
- (D)FTP

勒索軟體對於資料安全的傷害極大，請問下列敘述何者不正確？

- (A)勒索軟體感染方式，利用加密方式將電腦資料加密勒索
- (B) 勒索軟體是透過網頁瀏覽或郵件感染造成，與網路無關
- (C) 勒索軟體會造成備份成本增加
- (D)勒索軟體會感染一般電腦也會感染到網路主機

下列何者不是常見的弱點掃描工具之一？

- (A)Open Vulnerability Assessment System (OpenVAS)
- (B) Nessus
- (C) MegaSploit
- (D)Nmap

當系統或應用程式上被發現具有弱點，但是在修補程式未發佈之前，或是使用者更新前所進行的惡意攻擊行為，稱之為？

- (A)釣魚(phising)
- (B) 零時差攻擊(zero day attack)
- (C) 暴力攻擊(brute-force attack
- (D)重送攻擊(replay attack)

下列哪個檔案最可能內含巨集型病毒（Macro Virus）？

- (A)staff.doc
- (B) cmd.exe
- (C)command.dll
- (D)device.drv

關於備份，下列敘述何者正確？

- (A) 差異備份係指與增量備份完成後之索引檔進行比對，只要發生過變化之文件都會再備份一次
- (B) 完全備份係指與差異備份完成後之索引檔進行比對，只要發生過變化之文件都會再備份一次
- (C) 差異備份係指與增量備份完成後之索引檔進行比對，只要發生過變化之文件都會再備份一次
- (D) 差異備份係指與完全備份完成後之索引檔進行比對，只要發生過變化之文件都會再備份一次

關於系統日誌的管理與分析，下列敘述何者不正確？

- (A)每天不斷產生的日誌，資料量龐大，往往超出人力可以判讀的範圍
- (B) 預設的Syslog本身沒有加密，但是不會遭到偽冒攻擊
- (C) 混合式攻擊手法普遍，很難從單一設備上解讀出攻擊手法的資訊
- (D)不同設備所產生的日誌格式可能不一樣，會造成彙整上的困難

Windows作業系統中的事件檢視器，有三個較為重要之日誌檔，請問此三個日誌檔分別為下列何者？

- (A)連結性日誌、系統日誌、應用程式日誌
- (B)安全性日誌、網路日誌、應用程式日誌
- (C)安全性日誌、系統日誌、本機防毒日誌
- (D)安全性日誌、系統日誌、應用程式日誌

Bob 過去兩週一直在試圖滲透一個遠端的生產系統，某一次，他能夠進入系統，並使用該系統三週的時間。殊不知，執法機構也正在記錄他的每一項活動，並在後來成為證據。該組織使用一種虛擬環境來捕獲 Bob。這種虛擬環境是什麼？

- (A) 一種用來誘騙駭客的蜜罐技術
- (B) 一種使用特洛伊木馬的命令系統
- (C) 一種用來困住登入後使用者的環境
- (D) 一種用來困住登入前使用者的環境

請問系統管理人員登入成功或失敗，是否需留存相關紀錄？

- (A)登入成功不需要，登入失敗需要
- (B) 登入成功需要，登入失敗不需要
- (C) 登入成功和失敗都需要
- (D)登入成功和失敗都不需要

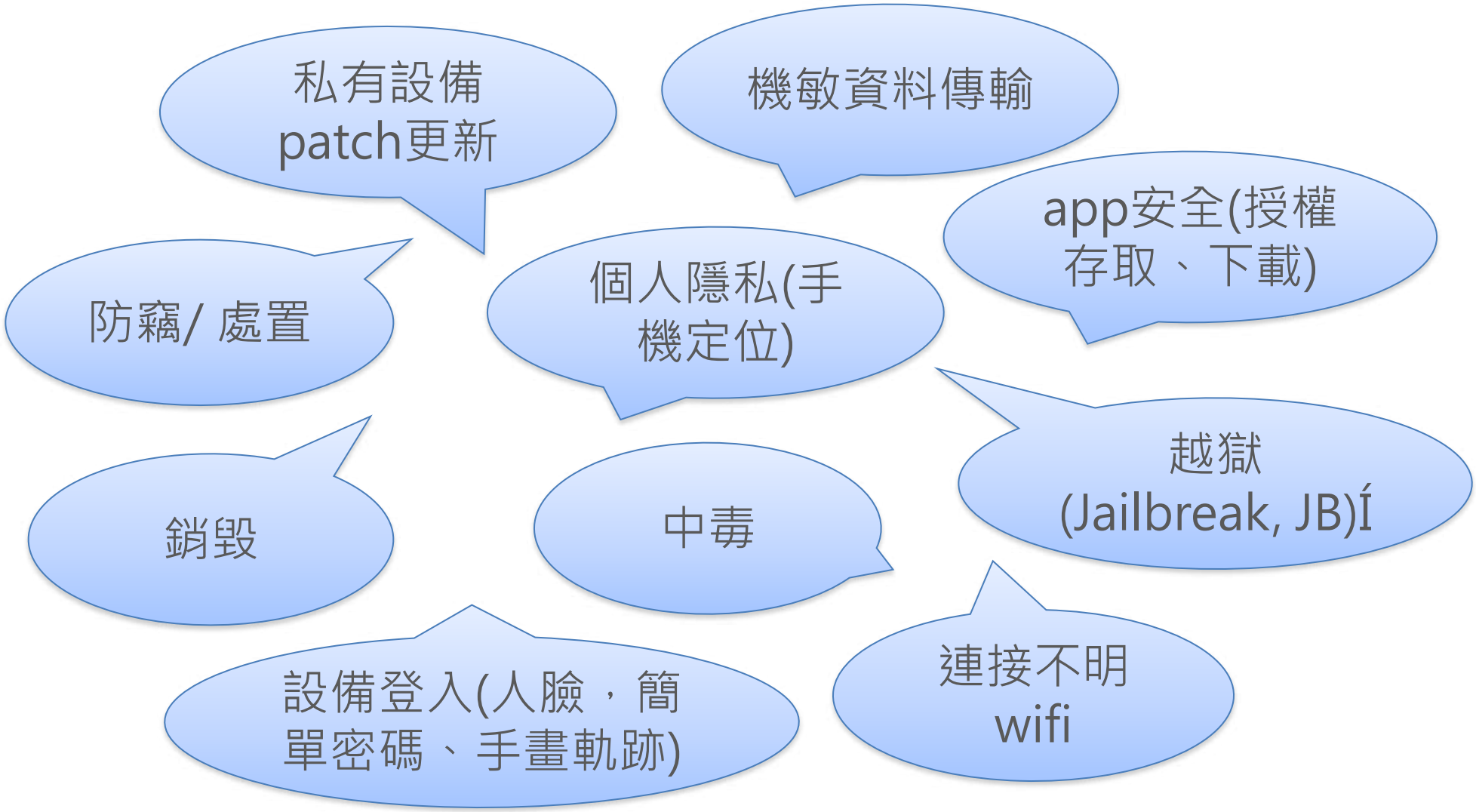
評鑑主題九
新興科技安全

1. 雲端安全概論
2. 行動裝置安全概論
3. 物聯網安全概論

重要字辭與定義


雲端認證
公有雲
私有雲
Hybrid
(cloud+IDC)
雲端委外
安全議題
信任度
雲端事故
處理
雲端日誌留
存、查詢
雲端服務合約
議題
(難以修改)

重要字辭與定義


私有設備
patch更新
機敏資料傳輸
app安全(授權
存取、下載)
防竊/ 處置
個人隱私(手
機定位)
越獄
(Jailbreak, JB)Í
銷毀
中毒
連接不明
wifi
設備登入(人臉，簡
單密碼、手畫軌跡)

重要字辭與定義


物聯網中間人攻擊
傳輸安全 (利用wifi等)
認證強度 (密碼)
訊號蓋台 (DoS)
Sinffer 議題
設備安全設定(完整性不足)
金鑰管理
預防無用論
加密強度
漏洞修補 (意識不足)

雲端運算的資訊安全

- 雲端運算的特性產生額外的安全問題，而且由於分責架構使得資安問題的處理變複雜了
- 不同的雲端服務模式衍生不同類型的安全問題
- 不同的部署方式面臨不同類型的安全問題
- 雲端運算的資源分配彈性可能會使資安問題的擴大加速，產生更大的危害
- 雲端運算的環境衍生出更多有關於**隱私、合規**與**稽核**的問題

雲端系統安全問題的源起

- 接受並採用雲端運算技術的企業越來越多
- 企業開始依賴虛擬化環境的應用
- 傳統的防火牆難以監控**虛擬機器（virtual machine）間的網路流量和安全**
- 這些網路流量未直接在實體網路留下足跡，實體網路的監控工具不易監控

從不同的角度看雲端資安的問題-1

- 用戶端
  - 資料竊取
  - 資料可用性
  - 網路封包竊聽
  - 資料內容加密保護
  - 共用環境的系統安全防護
  - 退租後資料完整刪除
- 供應商(CSP)
  - 惡意程式攻擊
  - 虛擬化環境的系統與網路安全
  - 僵屍網路
  - 提供透明化的安全管理資訊
  - 即時阻絕資安威脅

從雲端服務的特性來看安全問題-2

- 因應需求的自主服務(on-demand self-service)：自主服務的調配是否會超出資安容許的範圍
- 廣泛的網路存取(broad network access)：採用的各種設備是否安全
- 資源的共享(resource pooling)：動態的資源分配是否可靠、是否衍生多租戶干擾的問題、區域屬地要求是否合規
- 高度的彈性化(rapid elasticity)：是否造成資源預估困難
- 可度量的服務(measured service)：是否侵犯隱私

從雲端服務的特性來看安全問題-3

- 傳統的防護
- 虛擬平台與主機的弱點更新（Patch）
- 遠端存取的安全
- 虛擬化安全
- 虛擬主機的入侵偵測與防護技術
- 運作時的資料完整性
- 隔離技術
- 虛擬主機映像檔的安全保護
- **安全遷移(migration)**的技術

物聯網的資訊安全

- 非傳統的物件透過網路相連並且互相交換資料
- 物聯網中的物件數量龐大，代表可能受到資安攻擊的目標越多，**容易成為資安的弱點**
- 物聯網容易成為駭客橫行的天堂
- 物聯網的威脅更多元化，例如車載加入物聯網之後，就有可能成為駭客控制與操控的目標，對生活的環境產生危害

物聯網(IoT)的定義

- 物聯網是由多個實體物件所形成的網路
- 這些物件內有電子裝置、軟體、感測器與網路連接的能力，目的是讓物件本身產生更高的價值與服務
- 達到這個目的的方式是與製造商、電信業者或是其他連接的裝置交換資料
- 每個物聯網的物件都能透過其內部的運算系統被辨識，等於有個別唯一的身份，而且能夠在目前的網際網路的架構下相容地運作

物聯網的安全威脅

- 相連的物件在設計之初很可能完全沒有考量資安的問題
- 內含的作業系統與軟體可能極為老舊或是有許多弱點與漏洞
- 物聯網可能存在著眾多脆弱的資安物件與漏洞
- 傳統的攻擊手法很容易移植到物聯網中作用

行動裝置與物聯網安全防護

- 對於具備藍牙、NFC (Near-field communication)功能的行動裝置，應具備**開啟、關閉藍牙、NFC等連接介面之功能**
- 應用程式啟用無線介面連接功能，應在用戶確認之情況下，無線介面連接功能才可以被啟用
- 當行動裝置的無線介面**藍牙**或是**NFC**已啟動，行動裝置應在用戶主介面上，提供給用互相對應之提示

行動裝置與物聯網安全防護(續)

- 當行動裝置的無線介面-藍牙已建立數據連接，行動裝置應在用戶主介面上，提供給用互相對應之提示。當行動裝置的無線介面-NFC已建立數據連接，行動裝置應在用戶主介面上，提供給用互相對應之提示(圖示、聲音或震動)
- 針對機敏作業場所，於人員進出或是舉行機敏會議時，可以採用**電子圍籬(Electronic fences)**安全管理機制，當行動裝置進入管制處所時，可以限制特定硬體或是軟體之執行專屬Apps等

範例考題

下列哪種行為可能會威脅雲端帳號的安全？

- (A)使用有公信力的服務
- (B) 在不同網站使用不同帳號與密碼
- (C) 避免使用陌生電腦登入雲端服務帳號
- (D)使用瀏覽器會記錄帳號密碼的便利功能

雲端運算透過許多應用程式來提供服務，如果在身分驗證方面不夠嚴謹或是應用程式存在安全漏洞，可能就會造成使用時的安全問題。下列何者為所描述的安全威脅？

- (A)惡意的內部員工
- (B) 不安全的介面與APIs
- (C) 資源共享的技術問題
- (D)濫用與非法使用

隨雲端服務時代來臨，網路及系統架構逐漸擴張，安全控制議題也被彰顯。請問下列何者不屬於安全控制中的認證方法？

- (A)驗證（Authentication）
- (B)帳號管理（Accounting）
- (C)授權（Authorization）
- (D)加密（Encryption）

關於提高行動裝置（如手機）本身的安全性，下列敘述何者不正確？

- (A)開啟並設定開機密碼
- (B) 開啟並設定解鎖密碼
- (C) 加大電池容量
- (D)開啟並設定手機自動鎖定功能

關於行動裝置上的應用程式軟體安全，下列敘述何者不正確？

- (A)僅安裝可信賴來源之軟體
- (B)定期更新軟體
- (C)安裝防毒軟體
- (D)可安裝破解版軟體節省荷包

當兩個物聯網裝置在通訊過程中，傳遞的憑證訊息遭攔截並透過此憑證模擬合法身分達到存取特定服務。請問以上描述屬於下列哪種攻擊手法？

- (A)中間人攻擊
- (B) 重送攻擊
- (C)冒充攻擊
- (D)監聽攻擊

問題與討論

敬請指教

以下空白

OWASP Top 10 2007與2010

OWASP Top 10 – 2007 (Previous)		OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	↑	A1 – Injection
A1 – Cross Site Scripting (XSS)	↓	A2 – Cross Site Scripting (XSS)
A7 – Broken Authentication and Session Management	↑	A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	=	A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	=	A5 – Cross Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	+	A6 – Security Misconfiguration (NEW)
A10 – Failure to Restrict URL Access	↑	A7 – Failure to Restrict URL Access
<not in T10 2007>	+	A8 – Unvalidated Redirects and Forwards (NEW)
A8 – Insecure Cryptographic Storage	↓	A9 – Insecure Cryptographic Storage
A9 – Insecure Communications	↓	A10 – Insufficient Transport Layer Protection
A3 – Malicious File Execution	-	<dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	-	<dropped from T10 2010>

資料來源: OWASP

駭客手法演變

- Web 1.0 (1990 至 2000)
  - 駭客為了知名度
    - ➢網頁置換
- Pre-Web 2.0 (2000 至 2004)
  - 駭客為了控制網頁伺服器
    - ➢用戶資料庫、信用卡號碼及交易紀錄
  - 對個人電腦沒興趣
- Web 2.0 (2004 至 2009)
  - 人人是高度網路化的世界公民，從電腦可找出生活足跡
  - 駭客對於個人電腦更有興趣
- 擴展到**行動載具與社交軟體**的攻擊