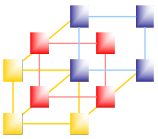
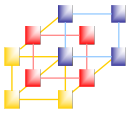


Unit 16
安全的威脅及弱點



安全威脅類型

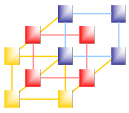
- 駭客取得網路的存取權後，就可能給網路帶來以下四種威脅
  - 資訊竊取
    - 闖入電腦以獲取機密信息
  - 身份竊取（冒用身份）
    - 是一種資訊竊取的形式，其中個人資訊會被竊取以接管某人的身份
  - 資料遺失及竄改
    - 破壞或更改數據記錄的計算機
    - 資料遺失：如威脅行動者傳送病毒，重新格式化電腦硬碟
    - 數据操作：如插入一個記錄系統來變更信息，比如物件的价格。
  - 服務阻斷（服務中斷）
    - 阻止合法用戶訪問他們有權使用的服務

安全性漏洞類型

- 技術弱點
- 組態弱點
- 安全策略弱點

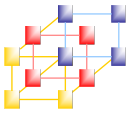
技術弱點

弱點	說明
TCP/IP 通訊協定弱點	•超文件傳輸協議 (HTTP), 檔案傳輸協議 (FTP), 和網際網路控制訊息協定(ICMP) 本質上都是不安全。 •簡單網路管理協定 (SNMP) 和簡單郵件傳輸 協定 (SMTP) 與TCP本身設計上不安全的結構有關。
作業系統缺陷	•每個作業系統都有必要解決的安全問題。 •UNIX、Linux、Mac OS、Mac OS X、Windows Server 2012、Windows 7、 Windows 8 •它們被記錄在電腦緊急應變小組 (CERT) 壓縮檔位於http://www.cert.org
網路設備缺陷	各種類型的網路設備，例如路由器、防火牆和 交換器具有安全弱點，必須識別和保護 防範他們的弱點包括密碼保護，缺乏驗證、路由通訊協定和防火牆漏洞。



組態弱點

弱點	說明
不安全的使用者帳號	使用者帳號資訊可能會不安全傳輸在網路中，而將帳號名稱和密碼暴露給威脅者。
系統帳戶使用容易猜測到的密碼	這個常見的問題是建立不良的使用者密碼所造成的結果。
網際網路服務設定錯誤	訪問不受信任的網站時，在 Web 瀏覽器中啟用 JavaScript 而開啟了一個由威脅者控制的攻擊的管道。 其他潛在弱點來源包括組態配置錯誤的終端機服務、檔案伺服器或網頁伺服器 (例如Microsoft Internet Information) Services (IIS), 和Apache網頁伺服器。
產品不安全的預設值	許多產品的預設設定可以產生或導致安全上的漏洞
設定錯誤的網路設備	設備本身的配置錯誤可能會導致嚴重的安全問題。例如，錯誤設定的存取清單、路由協定或簡單網路管理協定的community字串所產生的安全漏洞。

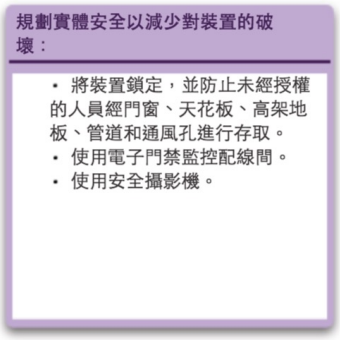


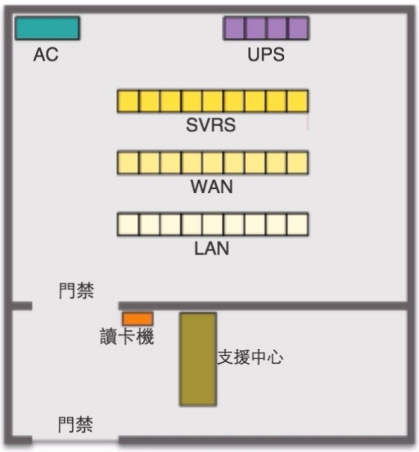
安全策略弱點

弱點	說明
缺乏書面安全策略	如果策略沒有被寫下來，安全性原則無法一致地套用或強制執行。
政治	政治上的鬥爭和搶奪地盤可能會使人們難以實現一致的安全性策略
缺乏驗證連續性	選擇不佳，容易破解，或預設密碼會導致未經授權的網路存取
未套用邏輯存取控制	監控和稽核不足，可允許攻擊和未經授權的使用，浪費公司資源。這可能導致法律行動或終止 IT 技術人員、IT 管理，甚至公司領導，使這些不安全的條件持續下去。
軟體和硬體的安裝和變更不遵循原則	未經授權的變更網路拓撲或安裝，未經批准的應用程序創建或啟用安全漏洞。
災難復原計劃是不存在的	缺乏災難復原計劃在發生自然災害或威脅者攻擊時可導致混亂恐慌和混亂

實體安全

- 實體威脅分為四類
  - 硬體威脅 - 對伺服器、路由器、交換器、佈線間和工作站的實體破壞
  - 環境威脅 - 指極端溫度（過熱或過冷）或極端溼度（過溼或過乾）
  - 電氣威脅- 電壓尖峰、電源電壓不足（電力管制）、不合格電源（雜訊），以及斷電
  - 維護威脅 - 指關鍵電力元件處理不當（靜電放電），缺少關鍵備用元件、佈線混亂和標識不明





電腦室防護計劃

漏洞和網路攻擊 – 病毒、蠕蟲和特洛伊木馬

- 病毒
  - 附加在其他程序上的惡意軟體，其目的是在工作站上執行特殊的惡意功能
- 蠕蟲
  - 一種獨立的程式，它會攻擊系統，並試圖利用目標中的特定漏洞。蠕蟲從攻擊主機上將自身程序複製到新發掘的系統中，然後使用相同的方式感染其他系統
- 特洛伊木馬
  - 整個應用程式經過偽裝，看似無害，但實際上是攻擊工具

偵察攻擊

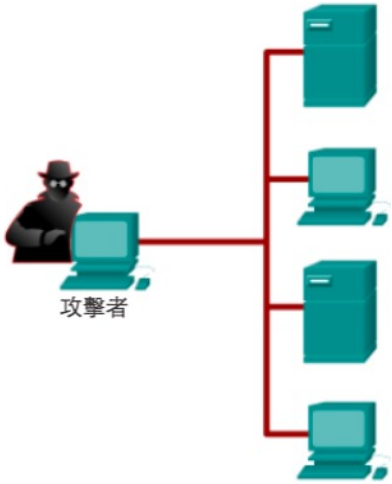
未經授權的搜索和映射系統、服務或漏洞

Internet 查詢

Ping 掃描

連接埠掃描

封包竊聽

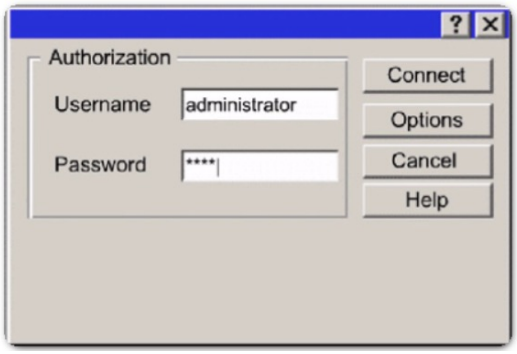


存取攻擊

未經授權的資料、系統存取或使用者權限操作

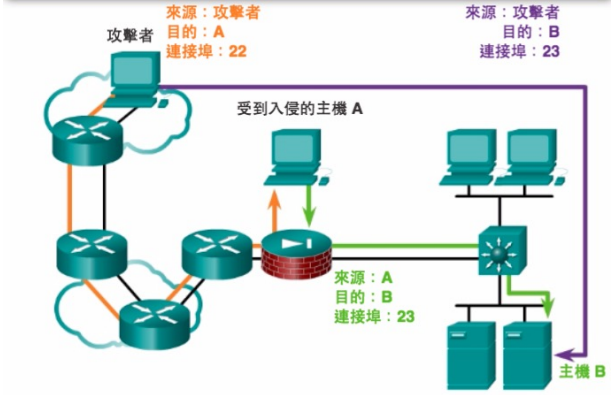
密碼攻擊

攻擊者可以使用多種方法實作密碼攻擊：
- 暴力攻擊
- 特洛伊木馬程式
- 封包竊聽



連接埠重定向

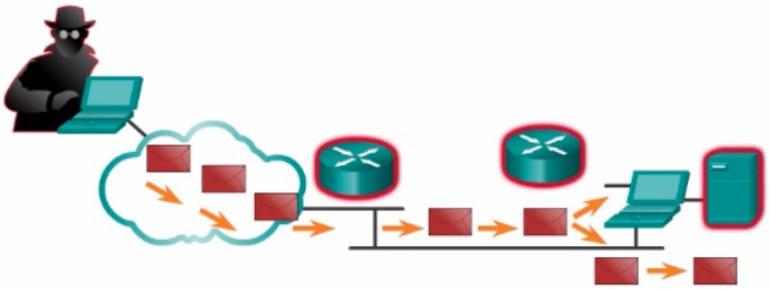
連接埠重定向是信任利用攻擊的一種，它使用被入侵的主機來傳遞正常情況下會被防火牆攔截的流量。它主要是使用適當的信任模型進行減輕。防毒軟體和基於主機的 IDS 可幫助檢測並阻止攻擊者在主機上安裝連接埠重定向公用程式。



DoS 攻擊(1/2)

DoS 攻擊

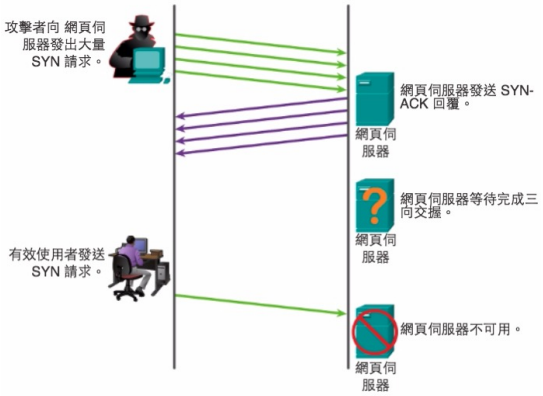
資源過載	異常資料
磁碟空間、頻寬、緩衝區	封包尺寸過大，例如大量 ping
Ping 泛洪，例如 smurf	封包重疊，例如 winuke
封包風暴，例如 UDP 炸彈和 fraggle	無法處理的資料，例如 teardrop



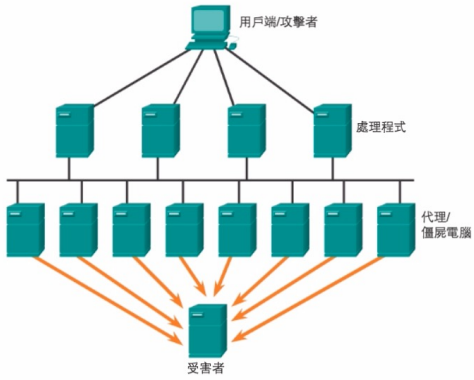
DoS 攻擊透過耗盡系統資源來阻止授權使用者存取。

DoS 攻擊(2/2)

SYN 泛洪

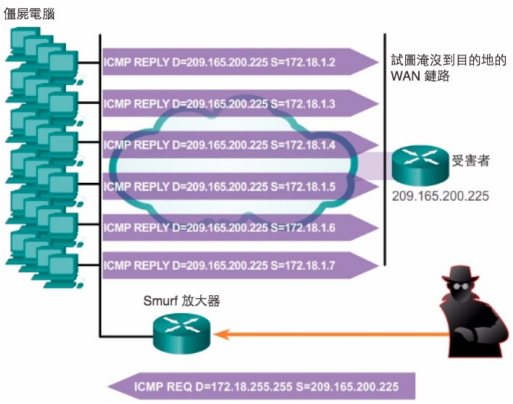


DDoS



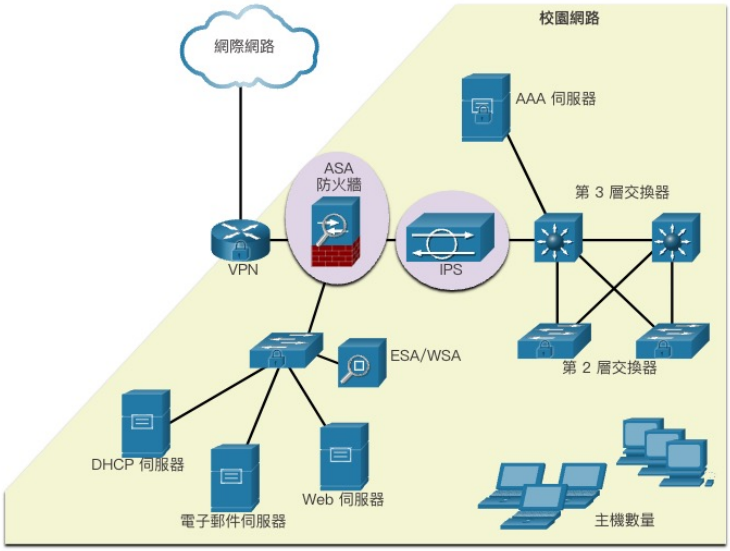
攻擊者使用多個中介主機（稱為僵屍電腦），發動攻擊。

Smurf 攻擊



減輕網路攻擊 –深度防護方法

- 大部分的組織都採用深度防禦方法（也稱為分層方法）來處理安全性。這需要結合網路裝置和服務

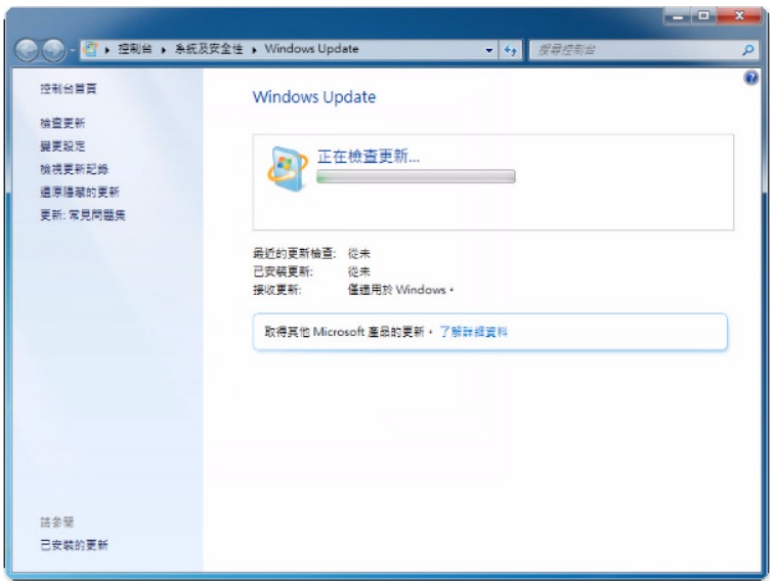


實作數個安全性裝置和服務來保護組織的使用者和資產免於 TCP/IP 威脅。

- **VPN** -路由器是用來為企業網站提供安全的 VPN 服務，並為使用安全加密通道的遠端使用者提供遠端存取支援。
- **ASA 防火牆** -此專用裝置提供狀態防火牆服務。它確保了內部流量可以出去和回來，但外部流量不能啟動連接到主機內部。
- **IPS** -入侵預防系統 (IPS) 可監控傳入和傳出流量，尋找惡意軟體、網路攻擊特徵等等。如果它識別威脅，它可以立即停止它。
- **ESA/WSA** -電子郵件安全設備 (ESA) 會過濾垃圾郵件和可疑電子郵件。網路安全裝置 (WSA) 會過濾已知和可疑的網際網路惡意程式網站。
- **AAA 服務器** -該服務器包含誰被授權訪問和管理網路設備的安全數據庫。網路裝置會使用此資料庫驗證系統管理使用者。

減輕網路攻擊 – 備份、升級、更新和修補程式

- 保持當前的防毒軟體為最新版本
- 安裝已經過更新的安全修補程式



減輕網路攻擊 – 驗證、授權和計量

- 驗證(Authentication)、授權(Authorization)和計量(Accounting)（AAA 或“三 A”）
  - 驗證 - 用戶和管理者必須證明其身份。身份驗證可以結合使用用戶名和密碼組合、提示問題和回應問題、權杖卡以及其他方法
  - 授權 - 用戶可以存取那些資源以及允許用戶執行那些操作
  - 計量 - 記錄使用者存取的資源、存取資源的時間以及所做的任何更改

防火牆

- 防火牆駐留在兩個或多個網路之間。它將控制流量並幫助阻止未授權的訪問。所用方法包括
  - 封包過濾
  - 應用程式過濾
  - URL 過濾
  - 狀態封包檢視 (SPI) — 傳入封包必須是對內部主機所發出請求的合法回應


Cisco 安全裝置


基於伺服器的防火牆


整合防火牆的 Linksys 無線路由器

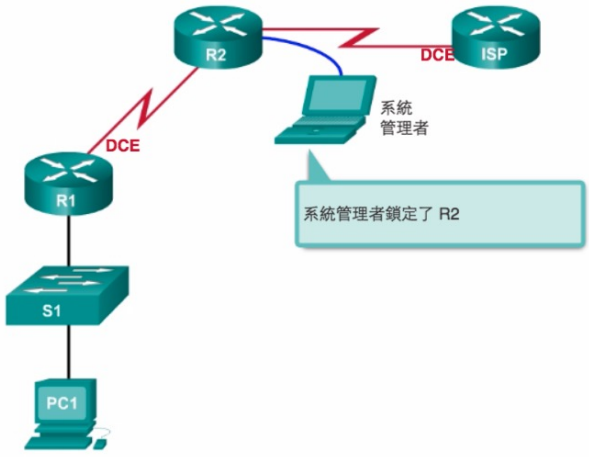

個人防火牆

終端安全

- 常見終端包括筆記型電腦、桌上型電腦、伺服器、智慧型手機和平板電腦
- 員工必須遵守公司制定的安全政策以保護其設備
- 政策通常包括防毒軟體的使用和主機入侵防禦

保護設備簡介

- 網路安全的一部分就是保護設備，包括終端設備和中介設備
  - 立即更換預設用戶名稱和密碼
  - 限制對系統資源的存取，只有授權使用者才可以存取
  - 盡可能關閉和卸載任何不必要的服務和應用程式
  - 當安全修補程式可用時更新安全修補程式



密碼

- 為了保護網路裝置，需使用強密碼。以下是需要遵循的標準原則：
  - 使用的密碼長度至少為 8 個字元，最好是 10 個或更多字元。密碼越長越好
  - 使用複雜密碼。如果條件允許，密碼中混合使用大寫和小寫字母、數字、符號和空格
  - 密碼中避免使用重複的常用字詞、字母或數字順序、用戶名稱、親屬或寵物的名字、個人傳記資訊（例如出生日期、身份證號碼、祖先的名字）或其他易於識別的資訊
  - 故意將密碼拼錯。例如，Smith = Smyth = 5mYth 或 Security = 5ecur1ty
  - 定期更改密碼。如果密碼不知不覺地泄露，那麼攻擊者使用該密碼的機會就會受到限制
  - 請勿將密碼寫出來並放在顯眼位置上，比如桌面上或螢幕上

基本安全實踐

- 加密密碼
- 要求密碼的最小長度
- 阻止暴力攻擊
- 使用標語訊息
- 設置 EXEC 逾時

```
Router(config)#service password-encryption
Router(config)#security password min-length 8
Router(config)#login block-for 120 attempts 3 within 60
Router(config)#line vty 0 4
Router(config-vty)#exec-timeout 10
Router(config-vty)#end
Router#show running-config
-more-
!
line vty 0 4
 password 7 03095A0F034F38435B49150A1819
 exec-timeout 10
 login
```

啟用 SSH


```
R1#conf t
R1(config)#ip domain-name span.com
R1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#
*Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#username Bob secret cisco
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
```

第 1 步：設定 IP 網域名稱。
第 2 步：產生 RSA 金鑰對。
第 3 步：檢驗或新增本地資料庫項目。
第 4 步：啟用 VTY 入站 SSH 會談。