弱點掃描技術

rk87 @ NSC

raykhor [at] gmail

Agenda

- Introduce
- Technology
- Pen Test
- Tools

Introduce

- **WHAT**
  - 針對已知的系統弱點，對該系統進行掃描、攻擊、測試
- **WHO**
  - 攻擊：攻擊他人系統，已達到入侵
  - 防護：發掘系統漏洞
- **WHY**
  - 攻擊：竊取資料，以利益爲主、造成破壞
  - 防護：進行漏洞修補，減少損失、預防破壞

Introduce

- HOW
  - 輔助工具
  - 追蹤最新的弱點 milw0rm.com
    - Exploits , Vulnerabilties, 0 days
  - 瞎猜　　Let's Demo
    - 管理弱點(密碼過於簡單)
    - 系統弱點(權限過大)
    - 入侵成功(免費的肉雞....^.^)
    - 以上示范作爲學術研究，以不竊取資料或構成威脅。主動通知受害者，以避免下一次攻擊！

Technology

- 這不是一項新技術，而是基於其他技術的弱點，讓弱點更爲突顯...
- **混合型弱點攻擊(早期2002~2003)**
  - 混合型主動攻擊是結合病毒、蠕蟲、木馬，並利用作業系統/程式漏洞
  - **Blaster** 利用 Microsoft RPC DCOM漏洞
  - **SQL Slammer** 利用 Microsoft SQL漏洞
  - **Nimda & Code Red** 利用Microsoft IIS漏洞

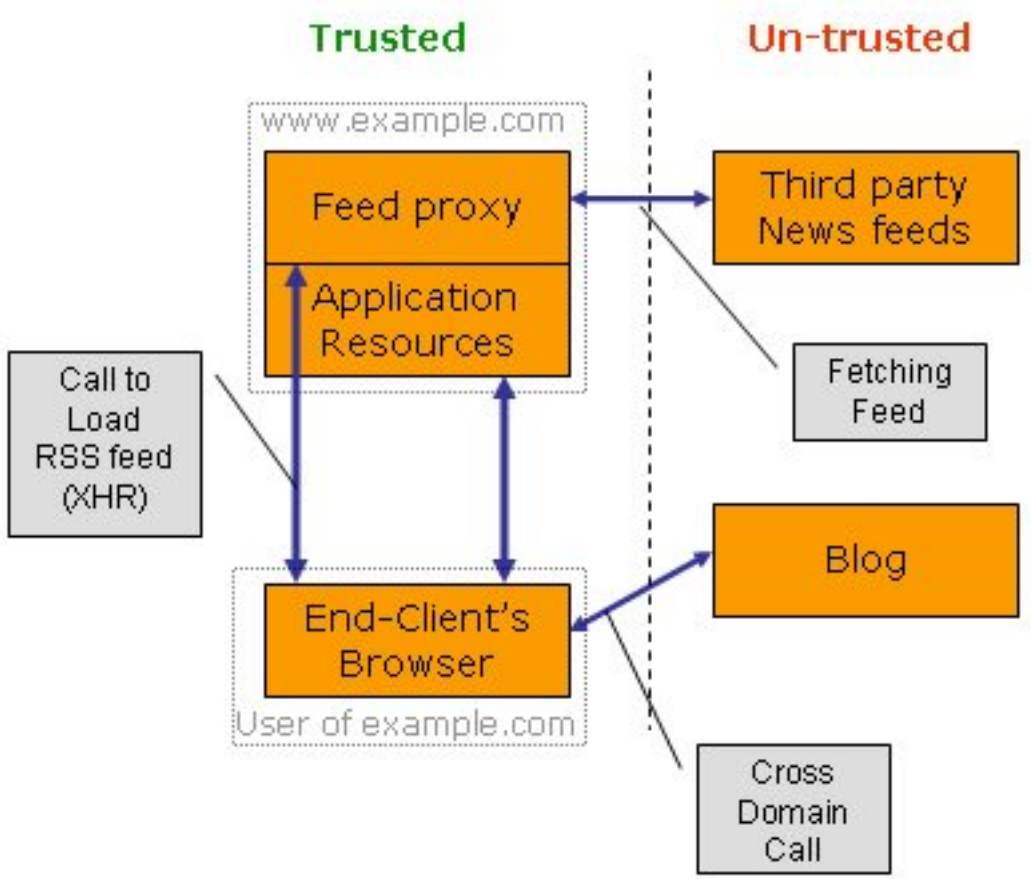
Micro$oft

- 好像都針對微軟... @.@
- 使用者有付錢買license,好像也不能改變事實
- 使用者不能預防...無法評估何時會照成損失
- 只能等無數的patch,還有很多service pack.
- Patch, Service pack ....都不用錢, 哈哈
- 使用者只能默默的接受
- 只要心臟夠強，弱點掃描是可以忽略...

Technology

- WEB 2.0 Application 正夯
  - Ajax
  - Json, XML, JavaScript
  - RSS feed
  - Flash
- 絕大部分都是open source, 那弱點就是開發人員留下來的
- 需要面對的風險
  - Cross Site Scripting (XSS)
  - SQL Injection

Web 2.0


Trusted
Un-trusted
www.example.com
Feed proxy
Application Resources
Third party News feeds
Fetching Feed
Call to Load RSS feed (XHR)
Blog
End-Client's Browser
User of example.com
Cross Domain Call

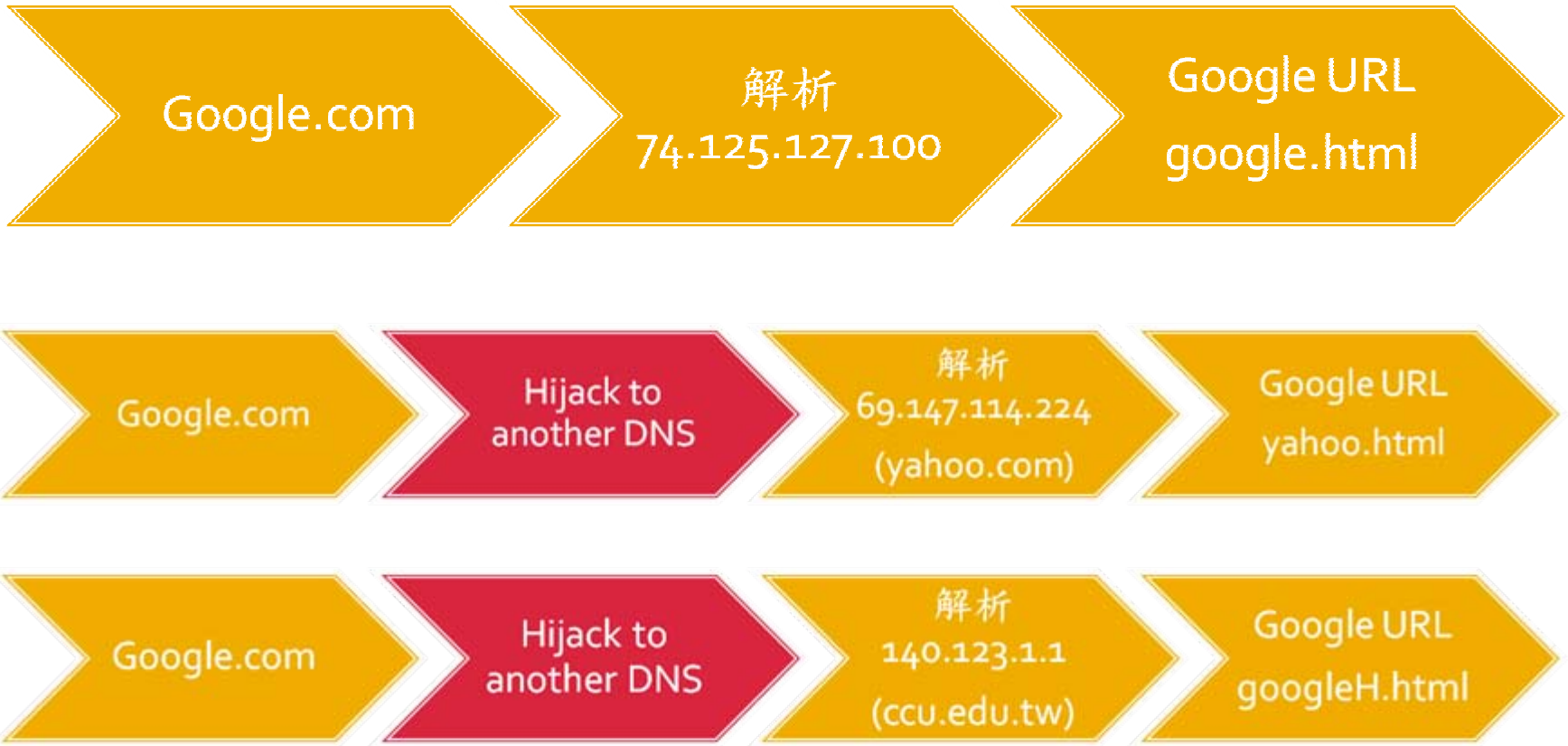
Web 2.0


所有網頁 圖片 影片 地圖 新聞 書籍 Gmail 更多 ▼
raykhor@gmail.com | 傳統首頁 | 我的帳戶 | 登出
iGoogle
進階搜尋
搜尋偏好設定
語言選項
Google 搜尋
好手氣
所有網頁
搜尋繁體中文網頁
把World of War...主題換掉 | 新增小工具 »
Home
Gmail
頭條報導
Gmail
日期和時間
Google Reader
天下雜誌精選內容
Bookmarks
即時通訊
搜尋、新增或邀請
Ray Khor
Google Reader (828)
All items (828)
refresh
mark all as read
網際網路40歲 出現中年危機
from UDN數位資訊
雜誌裡的電視廣告
from UDN數位資訊
Opera 10 全世界最快的瀏覽器
from UDN數位資訊
HWiNFO32 超強力系統資訊檢視軟體
from UDN數位資訊
跨傳統與數位 IOGEAR數位手寫筆幫你Key in
from UDN數位資訊
天下雜誌精選內容
夏日啤酒大戰，3大關鍵決勝500億商機
書包不見了...新聞熱潮過，災區學童怎麼辦？
人才養成7招，「膽識」造就頂尖企業
Jack's space
人生的十句话
頹廢
龍貓其實是死神
Tracy's space
start of something new
無題
Alan & Tracy
Ray
高雄
夜景
日記

Technology

- 網絡設備
  - Router, Switch, Firewall
- 作業系統
  - Microsoft Windows NT/ME/2000/XP/2003,Netware
  - Unix/Linux
- 資料庫
  - MSSQL, MySQL,…
- 網絡服務
  - Sendmail, Microsoft IIS, Apache, BIND(dns hijack),…
- 遠端管理
  - PCAnywhere, VNC, 遠端桌面

Dns Query


Google.com
解析
74.125.127.100
Google URL
google.html
Google.com
Hijack to another DNS
解析
69.147.114.224
(yahoo.com)
Google URL
yahoo.html
Google.com
Hijack to another DNS
解析
140.123.1.1
(ccu.edu.tw)
Google URL
googleH.html

弱點、漏洞

- 微軟的洞，微軟補
- 哪開發人員的洞，誰補.....?
  - 身爲Web 2.0 時代開發人員必須要有基本資安知識
  - 花錢請資安公司做滲透測試
  - 最壞的打算
    - 等有良心的使用者回報bug
    - 等免費的駭客幫你測試，順便把資料撈走 ^.^
- OWASP
  - Open Web Application Security Project
  - http://www.owasp.org/index.php/Taiwan

滲透測試技術
Penetration Test

Penetration Test

- 簡稱Pen Test, PT
- 採用一些 Hacking Methodology 來進行測試
- 檢驗資訊資產是否有落實資訊安全政策

- EX:
  - 某系統應進行漏洞維修，但未落實。可以利用Pen-Test檢驗該弱點是否可以被攻擊成功，造成系統被 compromise.
  - Ref: http://forum.icst.org.tw

Penetration Test 意義&目的

1. 了解入侵者可能利用的途徑，提出改善方法與建議
2. 找出IT人員未能掌握的伺服器或主機加以調查
3. 找出現行資訊安全政策之盲點
4. 對於重要主機的安全性提供專業資訊安全的評估與建議
5. 了解系統及網路的安全狀態
6. 稽核資安整體規劃佈置的安全性
7. 檢驗現行的資訊安全政策
8. 檢驗現行的網路設備(路由器、交換器…)安全政策
9. 檢驗現行的資訊安全設備(防火牆、IDP…)安全政策
10. 驗證現有系統安全性

Ref: http://forum.icst.org.tw

Penetration Test 意義&目的

發現弱點是可以被利用

至於防治是另一個議題

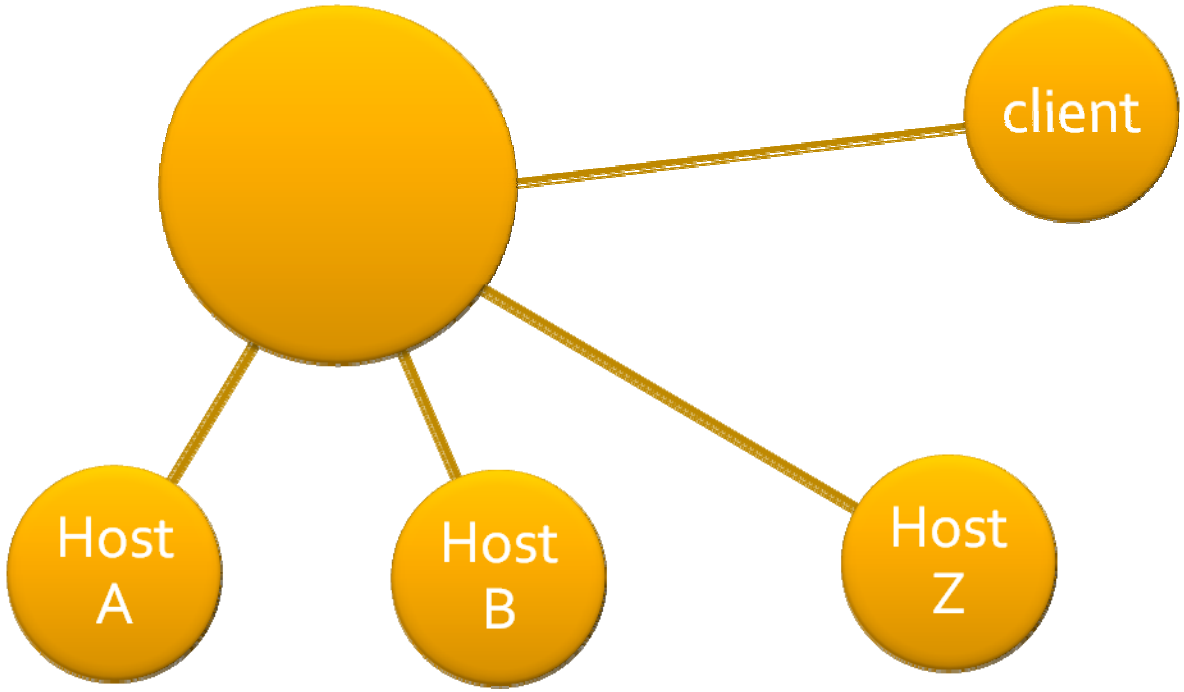
滲透測試 (Penetration Test) 討論版

http://forum.icst.org.tw/phpbb/viewforum.php?f=14

Ref: http://forum.icst.org.tw 行政院 國家資通安全會報

輔助工具
Nice Tools

Nessus / Paros Proxy



Question and Answer

弱點掃描技術

滲透測試技術

Thanks you.