電子商務安全
Secure Electronic Commerce

電子金融安全控管機制
(E-Finance Security Control Mechanisms)

992SEC14
TGMXM0A
Fri. 6,7,8 (13:10-16:00) L526

Min-Yuh Day
戴敏育
Assistant Professor
專任助理教授
Dept. of Information Management, Tamkang University
淡江大學 資訊管理學系

http://mail.im.tku.edu.tw/~myday/

2011-06-03

Syllabus

週次	月／日	內容（Subject/Topics
1	100/02/18	電子商務安全課程簡介 (Course Orientation for Secure Electronic Commerce)
2	100/02/25	電子商務概論 (Introduction to E-Commerce)
3	100/03/04	電子市集 (E-Marketplaces)
4	100/03/11	電子商務環境下之零售：產品與服務 (Retailing in Electronic Commerce: Products and Services)
5	100/03/18	網路消費者行為、市場研究與廣告 (Online Consumer Behavior, Market Research, and Advertisement)
6	100/03/25	電子商務 B2B、B2C、C2C (B2B, B2C, C2C E-Commerce)
7	100/04/01	Web 2.0, Social Network, Social Media
8	100/04/08	教學行政觀摩日
9	100/04/15	行動運算與行動商務 (Mobile Computing and Commerce)
10	100/04/22	期中考試週

Syllabus (cont.)

週次	月／日	內容（Subject/Topics
11	100/04/29	電子商務安全 (E-Commerce Security)
12	100/05/06	數位憑證 (Digital Certificate) [Module 4]
13	100/05/13	網路與網站安全 (Network and Website Security) [Module 5]
14	100/05/20	交易安全、系統安全、IC卡安全、電子付款 (Transaction Security, System Security, IC Card Security, Electronic Commerce Payment Systems) [Module 6, 7, 8, 9]
15	100/05/27	行動商務安全 (Mobile Commerce Security) [Module 12]
16	100/06/03	電子金融安全控管機制 (E-Finance Security Control Mechanisms) [Module 13]
17	100/06/10	營運安全管理 (Operation Security Management)
18	100/06/17	期末考試週

教育部顧問室編輯 “電子商務安全”教材

委辦單位：教育部顧問室資通安全聯盟

執行單位：國立台灣科技大學管理學院

Module 13：
電子金融安控機制

學習目的

1. 電子金融系統架構與各種安控機制
2. 透過10個基本防範措施，瞭解如何更安全管理網路、網路設備、伺服器及應用系統
3. 透過相關法令規範說明，瞭解應用系統設計時應注意事項
4. 除伺服器端環境外，如何透過行為改善，增加客戶端環境安全

Module 13：電子金融安控機制

- Module 13-1：基本防範措施
- Module 13-2：網路應用系統規範
- Module 13-3：系統設計注意事項
- Module 13-4：客戶端使用注意事項
- 參考文獻

Module 13-1：
基本防範措施

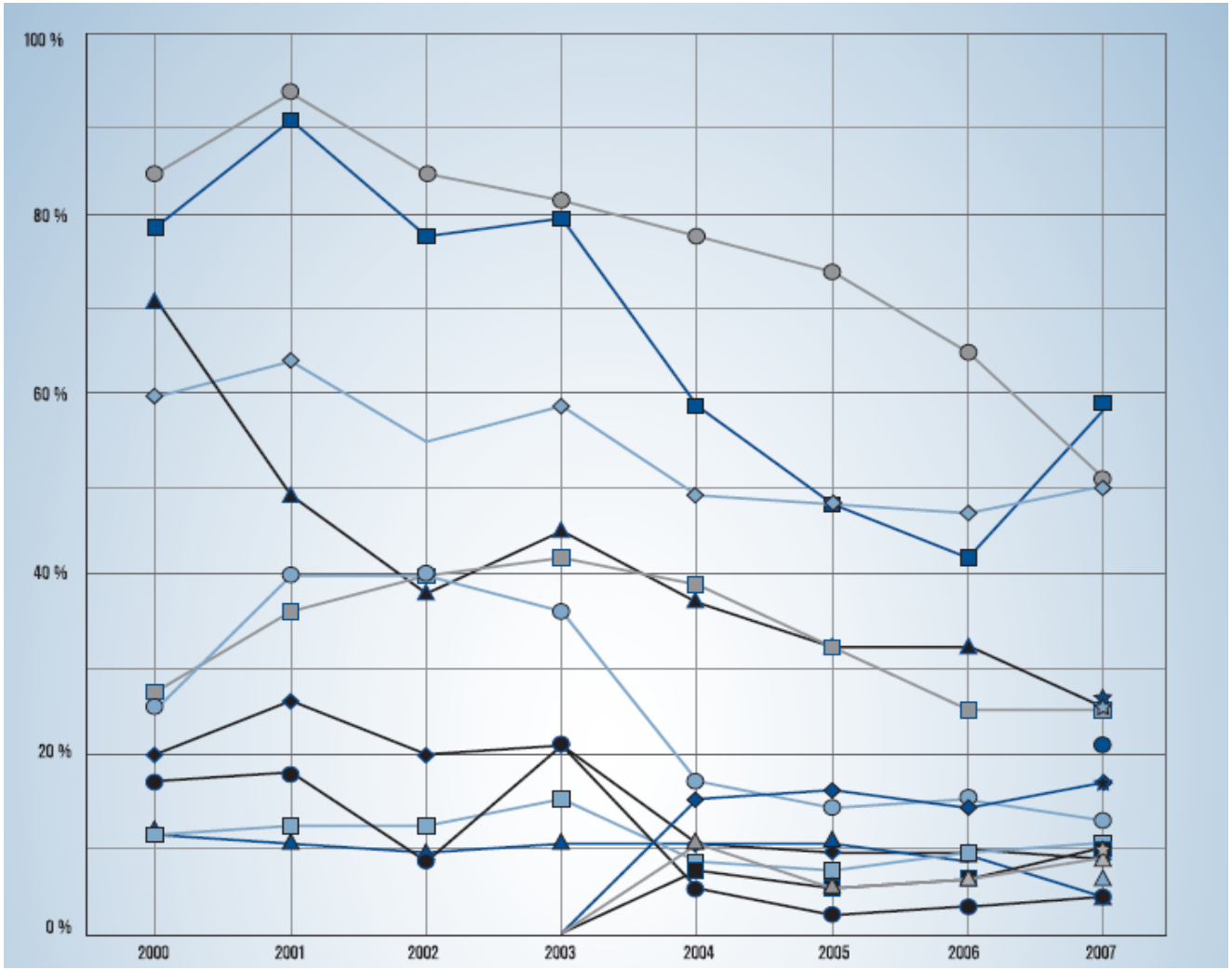
資安攻擊型態與演進

TYPE OF ATTACK	2007
Insider abuse of Net access	59%
Virus	52%
Laptop / mobile device theft	50%
Phishing where your organization was fraudulently represented as sender**	26%
Instant messaging misuse**	25%
Denial of service	25%
Unauthorized access to information	25%
Bots within the organization**	21%
Theft of customer / employee data**	17%

TYPE OF ATTACK	2007
Financial fraud	12%
Password sniffing**	10%
Web site defacement*	10%
Misuse of public Web application*	9%
Theft of proprietary information (intellectual property)	8%
Exploit of the organization's DNS server**	6%
Telecom fraud	5%
Sabotage	4%

CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

資安攻擊型態與演進



CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

- 內部不當網路存取(59%)
- 電腦病毒感染(52%)
- 行動裝置/電腦失竊(50%)
- 以合法身份發送釣魚台網站信件(26%)
- 即時通訊(IM)不當使用(25%)
- 阻絕服務(25%)
- 未授權資訊存取(25%)

基本防範措施

1. Port Scanning
2. SNMP Scanning
3. Enumeration & Banner Grabbing
4. Wireless Enumeration
5. Vulnerability Scanning
6. Host Evaluation
7. Network Device Analysis
8. Password Compliance Testing
9. Application Specific Scanning
10. Network Sniffing

基本防範措施

1. **Port Scanning**
   - Identify enabled network services on systems
   - Look for unauthorized services or backdoors
2. **SNMP Scanning**
   - Enumerate systems on the network
   - Identify community strings
3. **Enumeration & Banner Grabbing**
   - Verification of operating system
4. **Wireless Enumeration Tools**
   - Identify access points and potential exposures
5. **Vulnerability Scanning**
   - Identify well-known vulnerabilities on systems

基本防範措施

6. **Host Evaluation**
   - Analyze configuration, discretionary access control and policies
7. **Network Device Analysis**
   - Analyze security architecture for well-known vulnerabilities and insecure configurations
8. **Password Compliance Testing**
   - Evaluate adherence to password policy and determine whether password filters are being effectively implemented
9. **Application Specific Scanning**
   - Evaluate security configuration of critical applications
10. **Network Sniffing**
    - Identifies sensitive information traversing the network (log-in, passwords, server configurations via telnet, etc)

1. Port Scanning

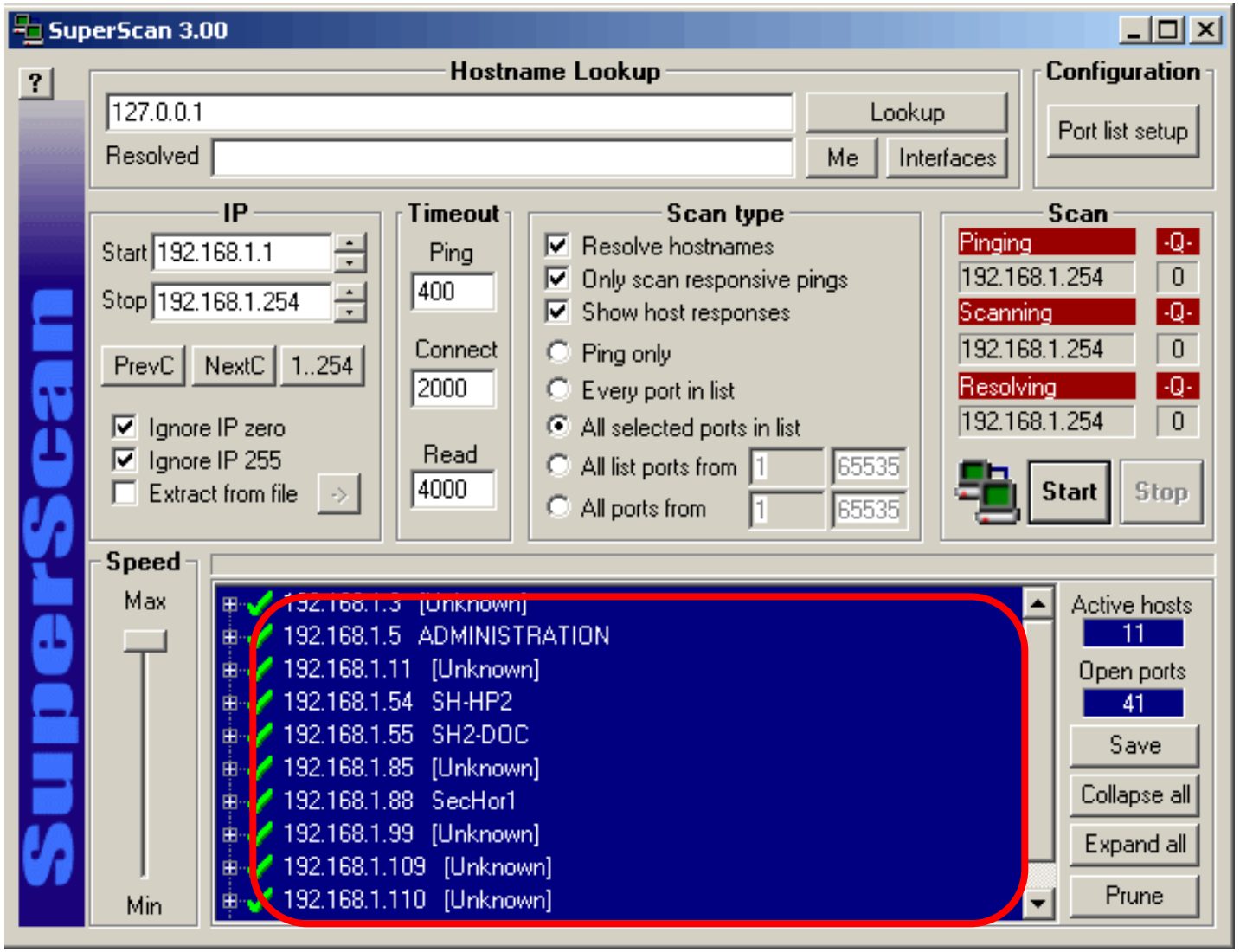
```
# nmap -v -sT 192.168.1.88

Starting nmap 3.20 ( www.insecure.org/nmap/ ) at 2003-04-17 13:29 MDT
Host 192.168.1.88 appears to be up ... good.
Initiating Connect() Scan against 192.168.1.88 at 13:29
Adding open port 139/tcp
Adding open port 445/tcp
Adding open port 135/tcp
Adding open port 5000/tcp
Adding open port 1025/tcp
The Connect() Scan took 5 seconds to scan 1611 ports.
Interesting ports on 192.168.1.88:
(The 1606 ports scanned but not shown below are in state: closed)
Port       State       Service
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
445/tcp    open        microsoft-ds
1025/tcp   open        NFS-or-IIS
5000/tcp   open        UPnP

Nmap run completed -- 1 IP address (1 host up) scanned in 5.268 seconds
#
```

Use nmap tool

1. Port Scanning



Use SuperScan tool

1. Port Scanning

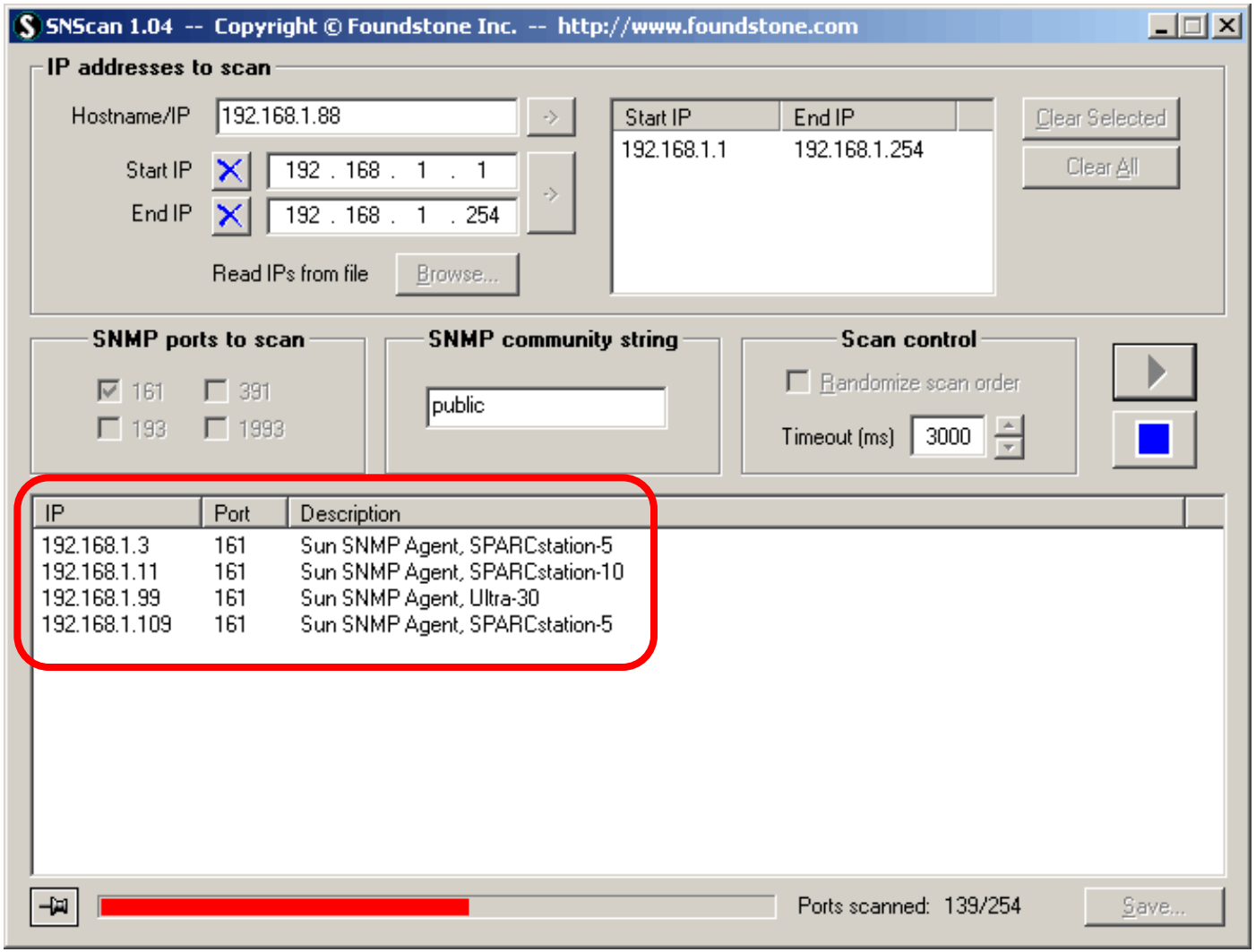
```
F:\Tools CD\FScan>fscan.exe -bep 1-1024 192.168.1.1-192.168.1.50
FScan v1.12 - Command line port scanner.
Copyright 2000 (c) by Foundstone, Inc.
http://www.foundstone.com

 Scan started at Fri Aug 29 08:19:08 2003

192.168.1.5         21/tcp  administration
   220 administration Microsoft FTP Service (Version 5.0).[0D][0A]
192.168.1.5         80/tcp  administration
   HTTP/1.1 400 Bad Request[0D][0A]Server: Microsoft-IIS/5.0[0D][0A]Date: Fri
   , 29 Aug 2003 14:18:34 GMT[0D][0A]Content-Type: text/html[0D][0A]Content-L
   ength: 87[0D][0A][0D][0A]
192.168.1.5         25/tcp  administration
192.168.1.5         42/tcp  administration
192.168.1.5        139/tcp  administration
   [83][00][00][01][8F]
192.168.1.5         88/tcp  administration
192.168.1.5        110/tcp  administration
192.168.1.5        135/tcp  administration
192.168.1.5        389/tcp  administration
192.168.1.5        443/tcp  administration
192.168.1.5        445/tcp  administration
192.168.1.5        515/tcp  administration
   [01]
192.168.1.5        464/tcp  administration
192.168.1.5        593/tcp  administration
   ncacn_http/1.0
192.168.1.5        636/tcp  administration
```

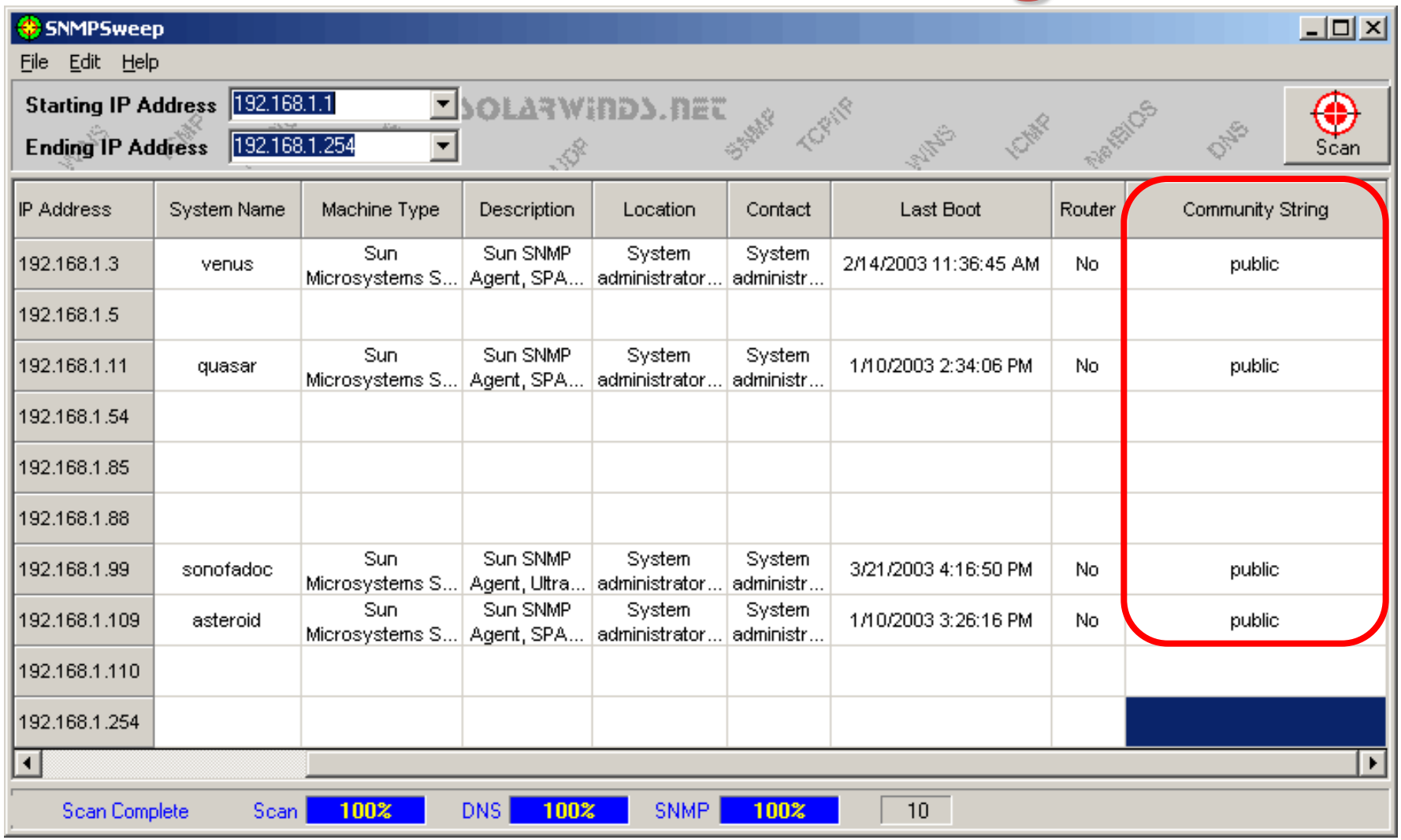
Use FScan tool

2. SNMP Scanning



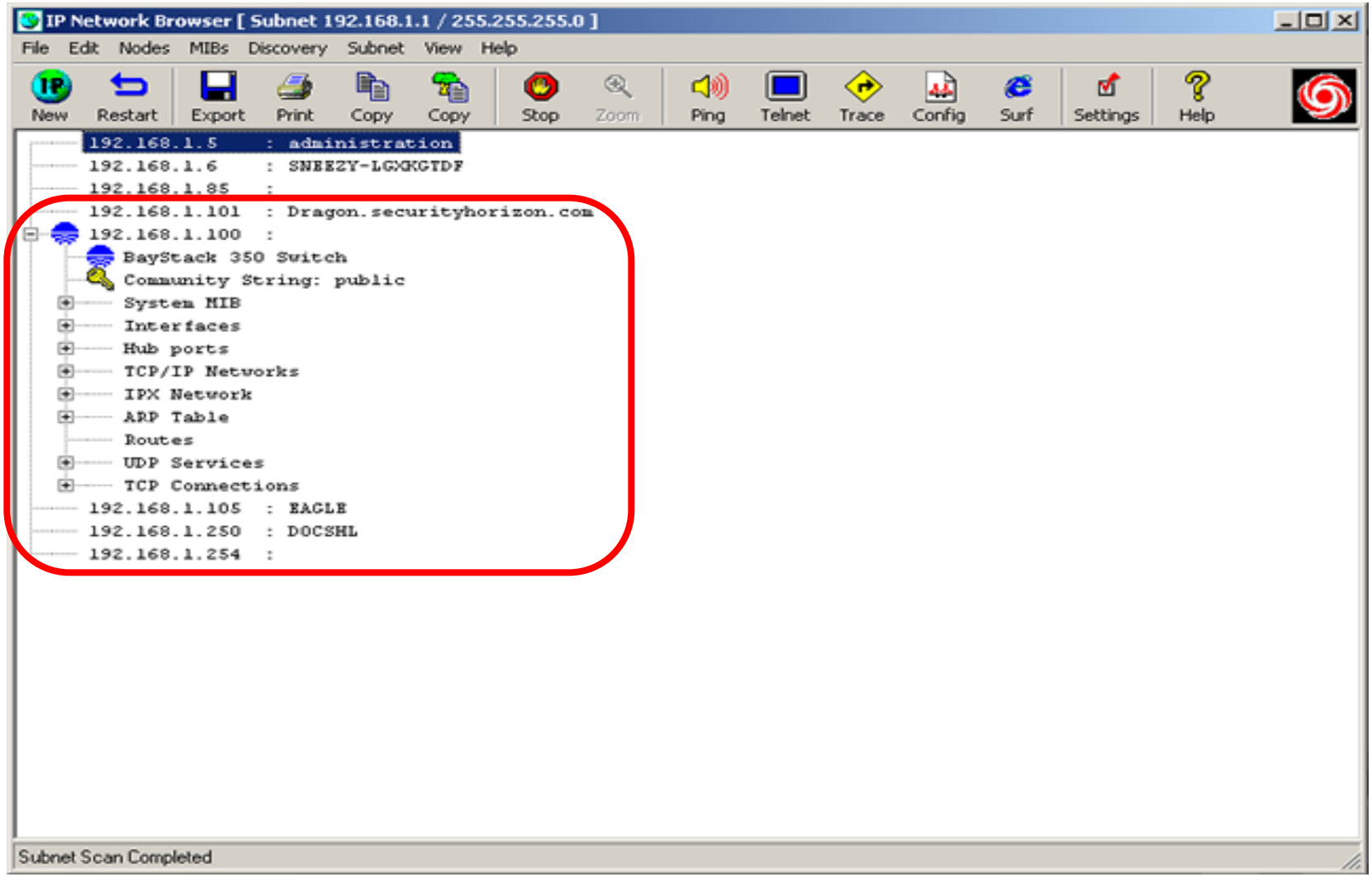
Use SNScan tool

2. SNMP Scanning



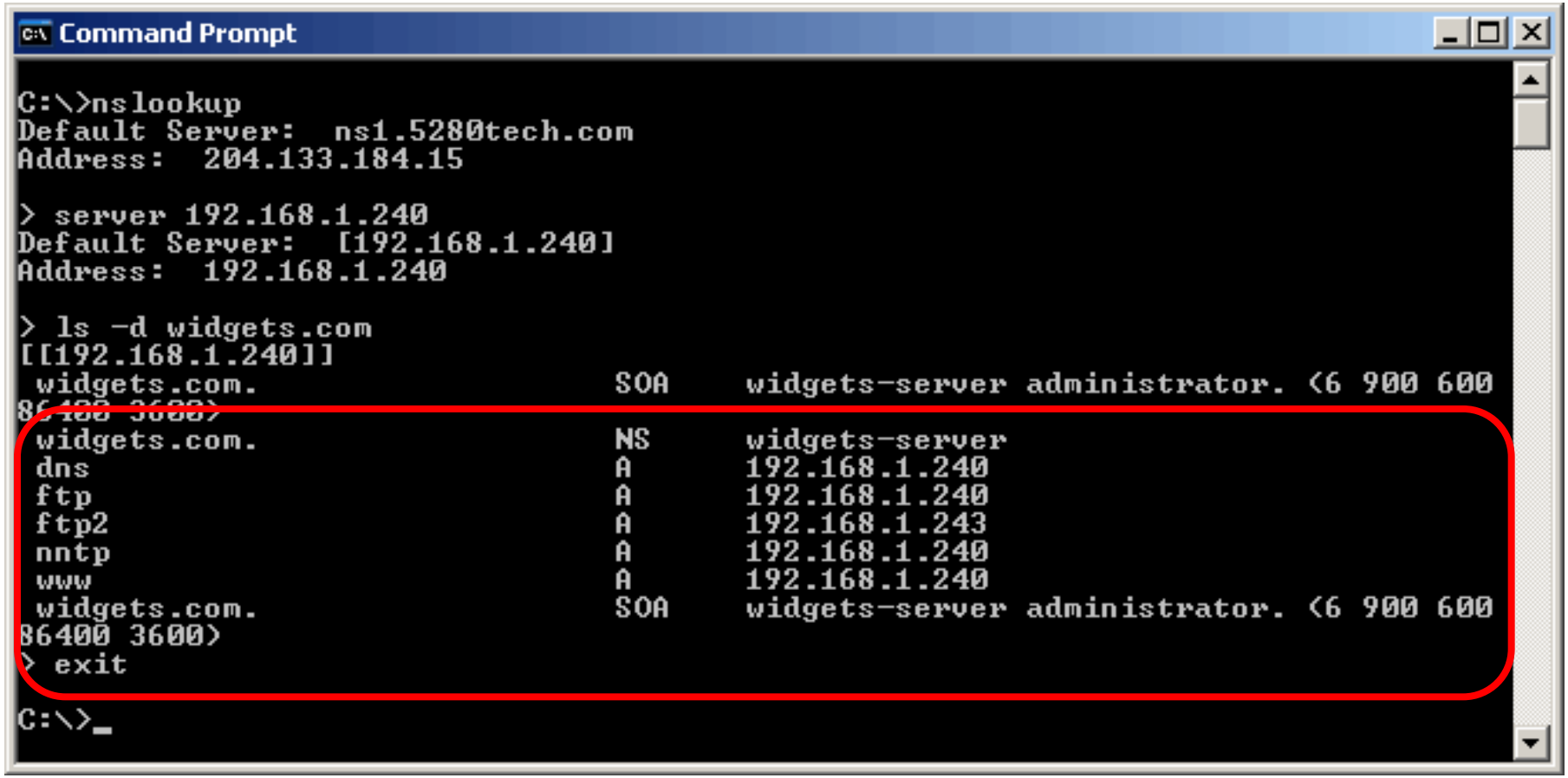
Use SolarWinds SNMPweep tool

2. SNMP Scanning



Use SolarWinds IP Network Browser tool

3. Enumeration



Use nslookup 自DNS Server 列出網路資訊

3. Enumeration

```
root@mercury:~# finger "a b c d e f g h i"@192.168.1.245
[192.168.1.245]
Login       Name                 TTY         Idle    When    Where
root     Super-User              console      <Jan  2, 2003> :0
daemon          ???                          < .   .   .   . >
bin             ???                          < .   .   .   . >
sys             ???                          < .   .   .   . >
adm      Admin                               < .   .   .   . >
lp       Line Printer Admin                  < .   .   .   . >
uucp     uucp Admin                          < .   .   .   . >
nuucp    uucp Admin                          < .   .   .   . >
listen   Network Admin                       < .   .   .   . >
nobody   Nobody                              < .   .   .   . >
noaccess No Access User                      < .   .   .   . >
nobody4  SunOS 4.x Nobody                    < .   .   .   . >
russr           ???              pts/1       <Jun 16 13:29> 192.168.1.88
tdykstra        ???                          < .   .   .   . >
rcallow         ???                          < .   .   .   . >
tpham           ???                          < .   .   .   . >
sturner         ???                          < .   .   .   . >
gnotske         ???                          < .   .   .   . >
ffranks         ???                          < .   .   .   . >
dbuffo          ???                          < .   .   .   . >
rking           ???                          < .   .   .   . >
```

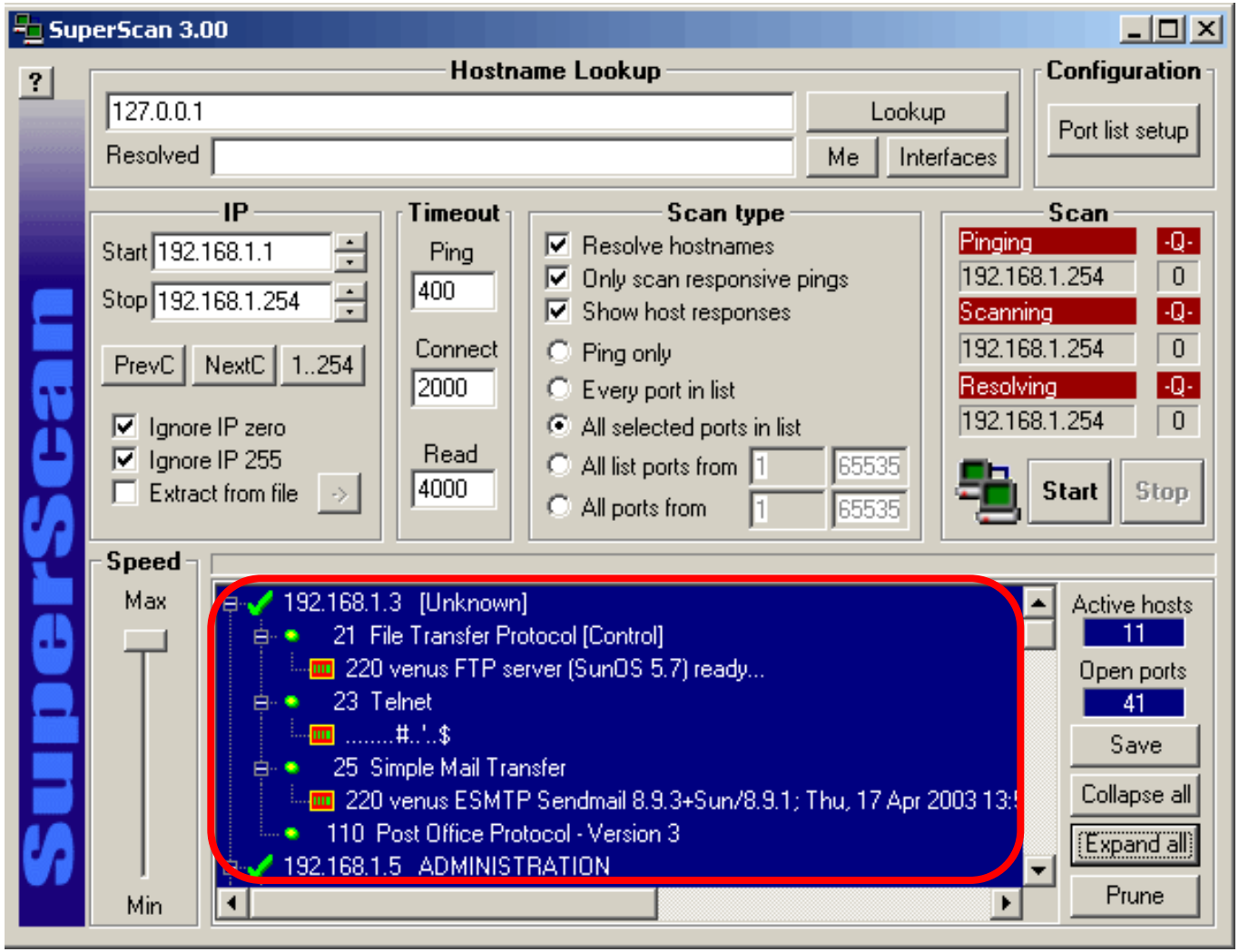
Use finger tool on UNIX

3. Enumeration

```
root@mercury:~# rpcinfo -p 192.168.1.110
   program vers proto   port
    100000    4   tcp    111  portmapper
    100000    3   tcp    111  portmapper
    100000    2   tcp    111  portmapper
    100000    4   udp    111  portmapper
    100000    3   udp    111  portmapper
    100000    2   udp    111  portmapper
    100083    1   tcp  32775
    100068    2   udp  32776
    100068    3   udp  32776
    100068    4   udp  32776
    100068    5   udp  32776
    100024    1   udp  32778  status
    100024    1   tcp  32777  status
    100133    1   udp  32778
    100133    1   tcp  32777
    100021    1   udp   4045  nlockmgr
    100021    2   udp   4045  nlockmgr
    100021    3   udp   4045  nlockmgr
    100021    4   udp   4045  nlockmgr
    100021    1   tcp   4045  nlockmgr
    100021    2   tcp   4045  nlockmgr
    100021    3   tcp   4045  nlockmgr
```

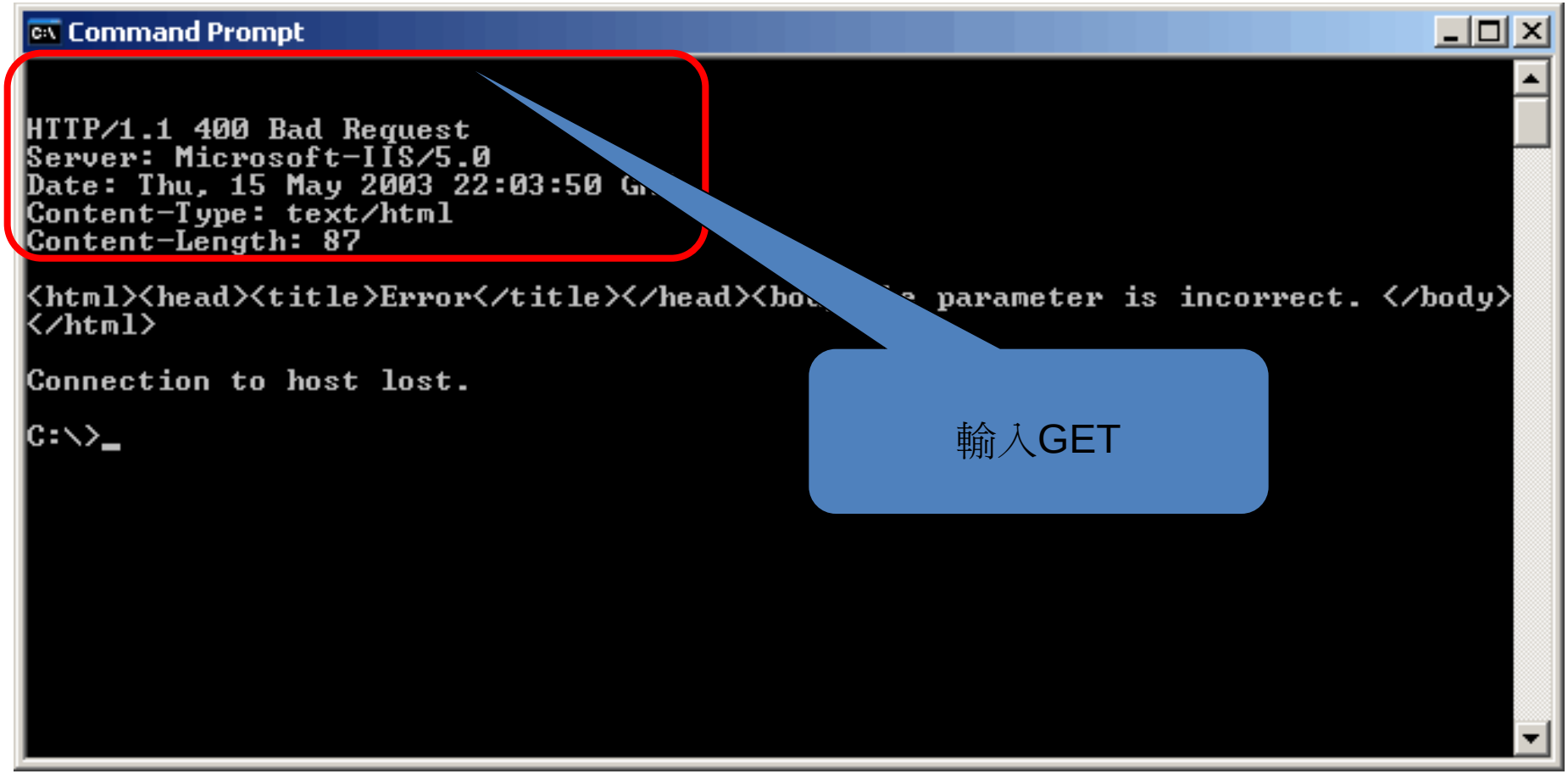
Use rpcinfo tool on UNIX

3. Banner Grabbing



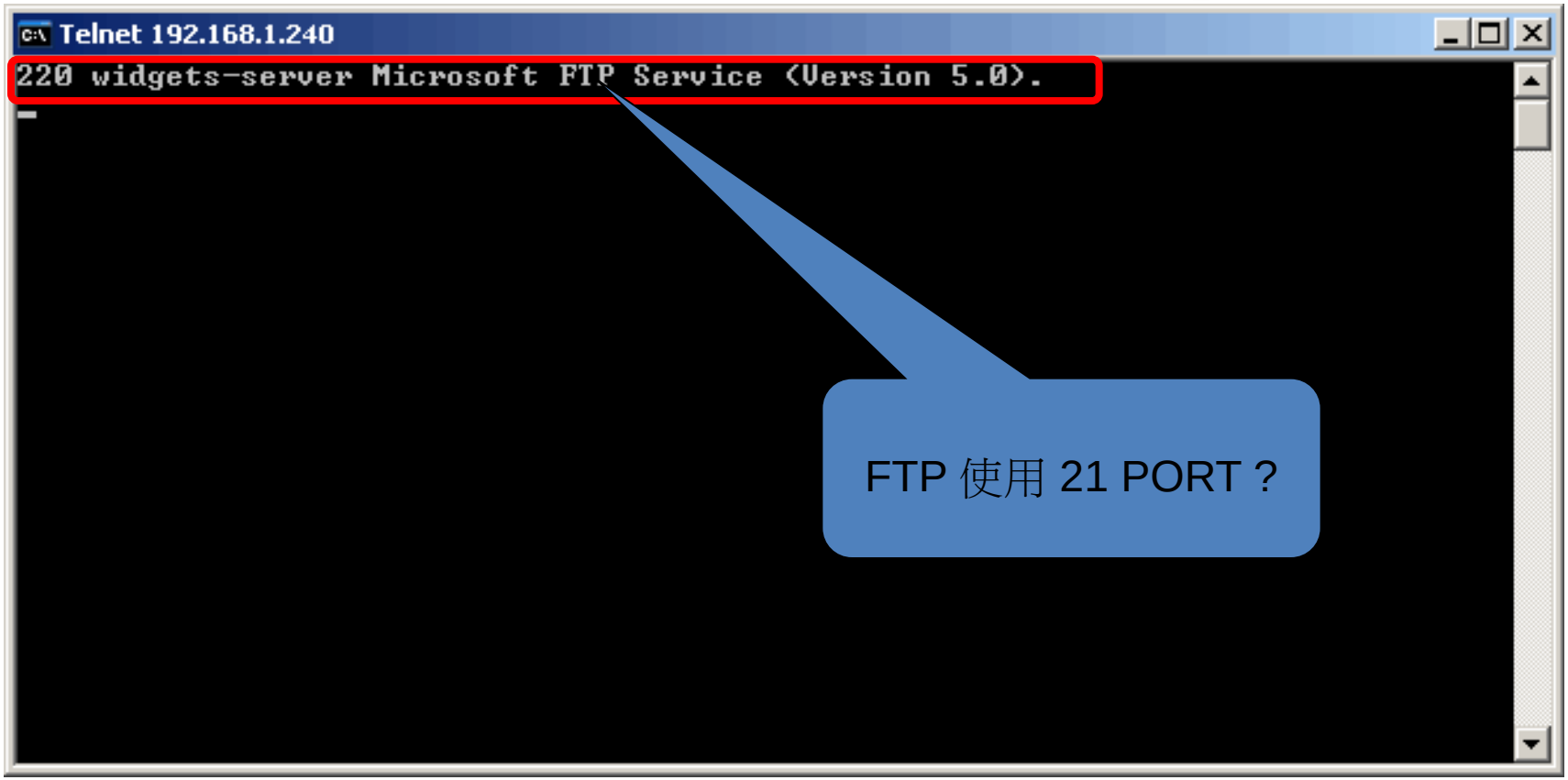
Use SuperScan tool

3. Banner Grabbing



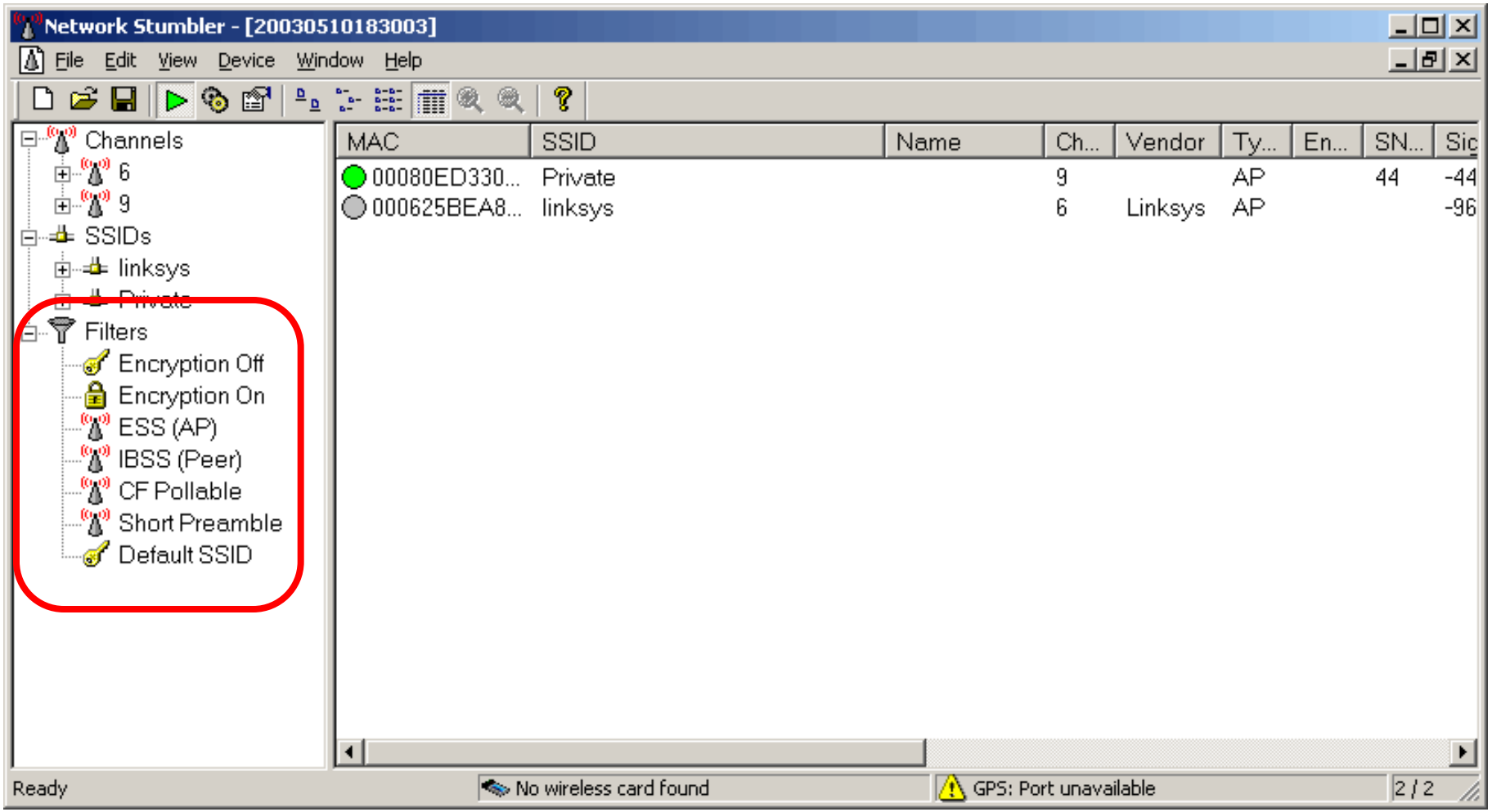
Use telnet (80) tool

3. Banner Grabbing



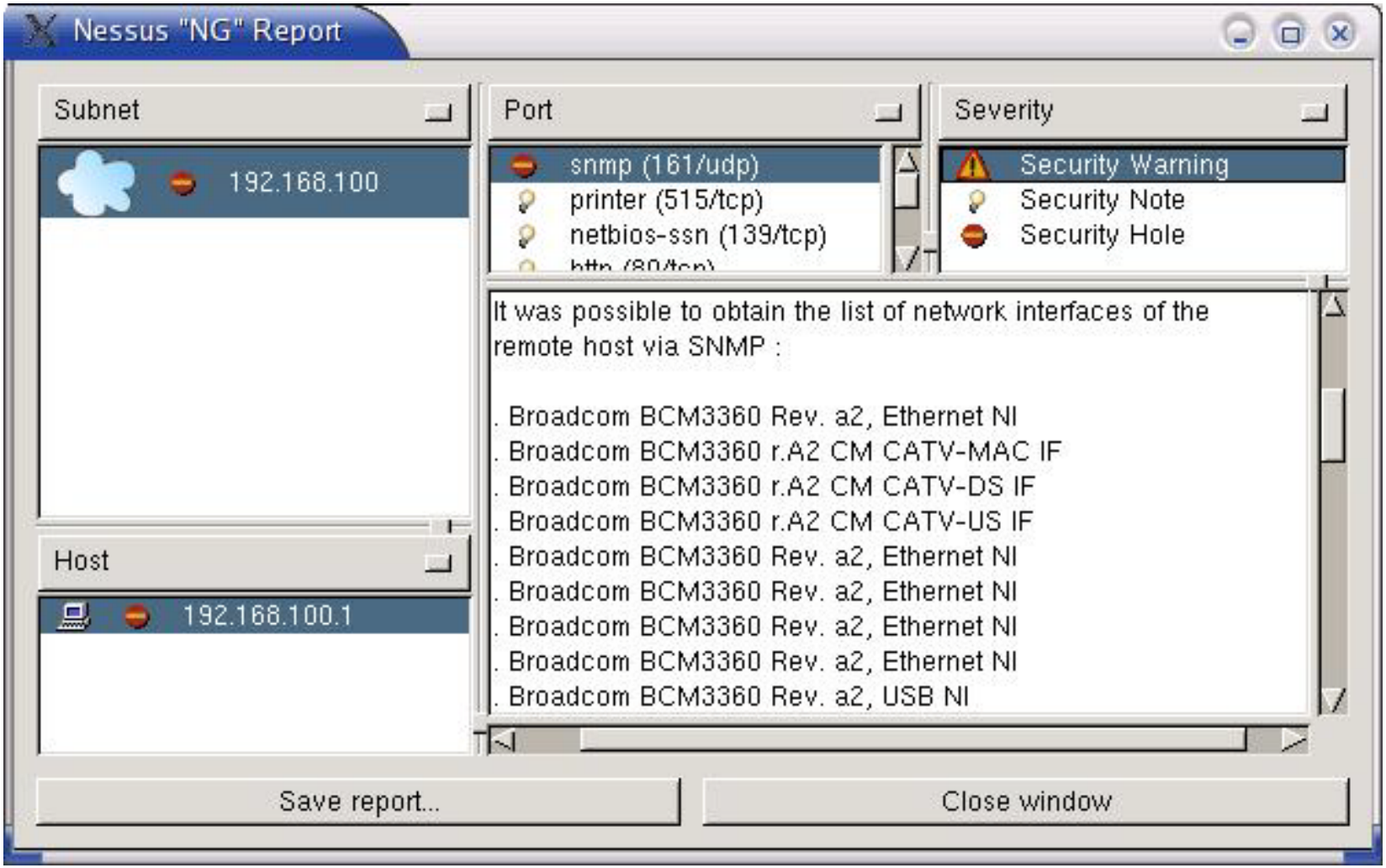
Use telnet (21) tool

4. Wireless Enumeration



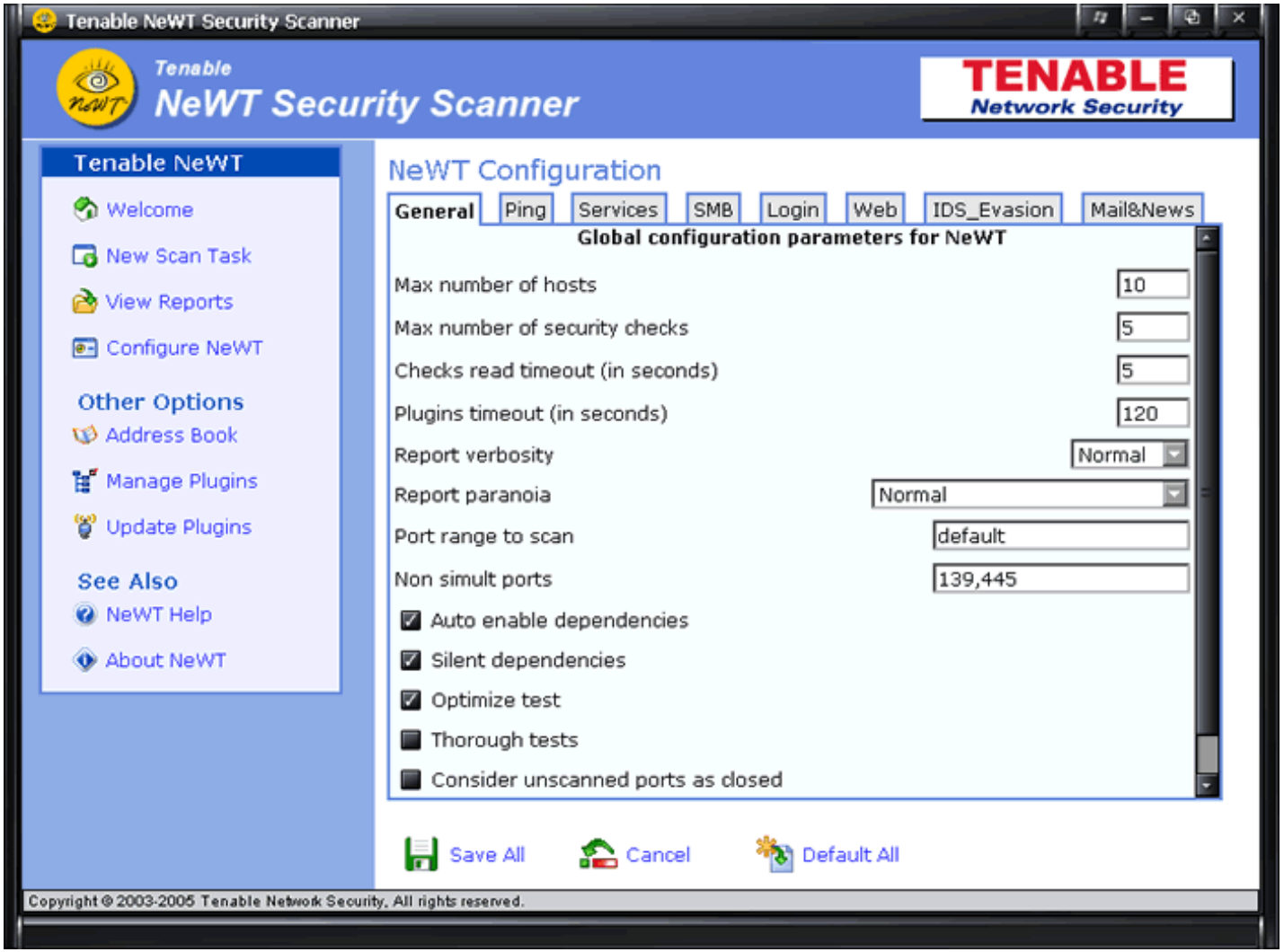
Use Network Stumbler tool

5. Vulnerability Scanning



Use Nessus tool

5. Vulnerability Scanning

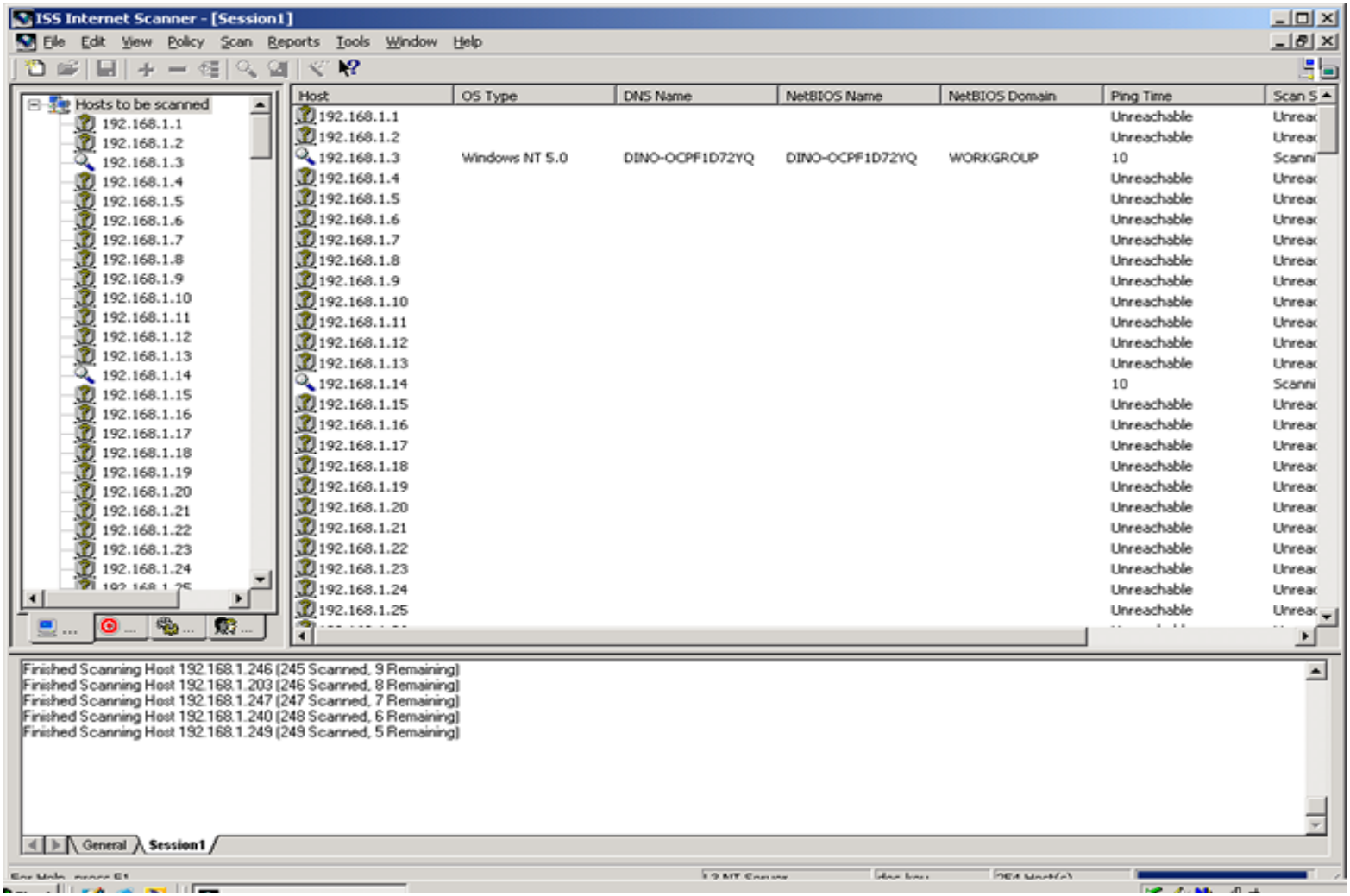


Use NeWT Security Scanner tool

5. Vulnerability Scanning

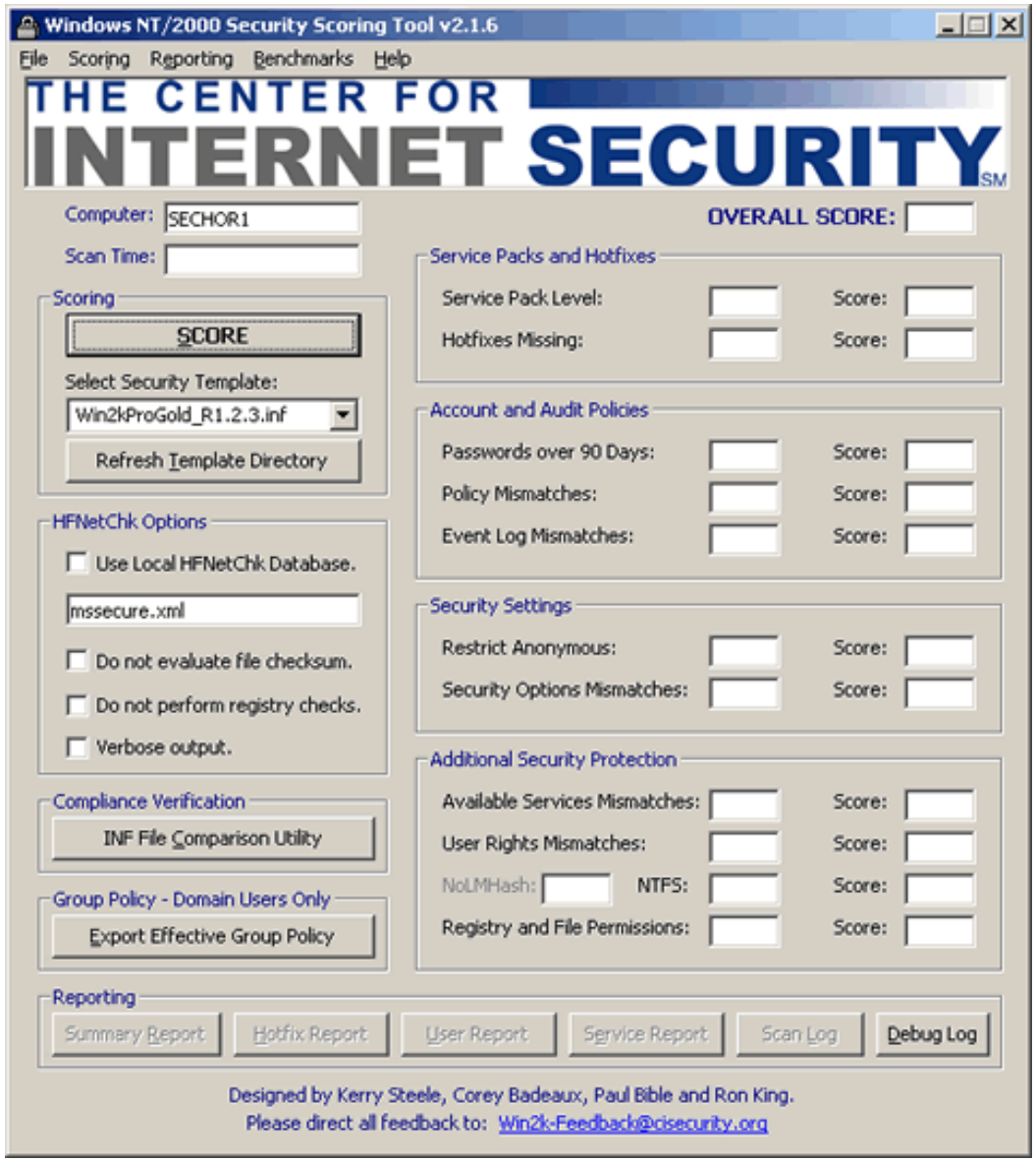
Use Saint tool

5. Vulnerability Scanning



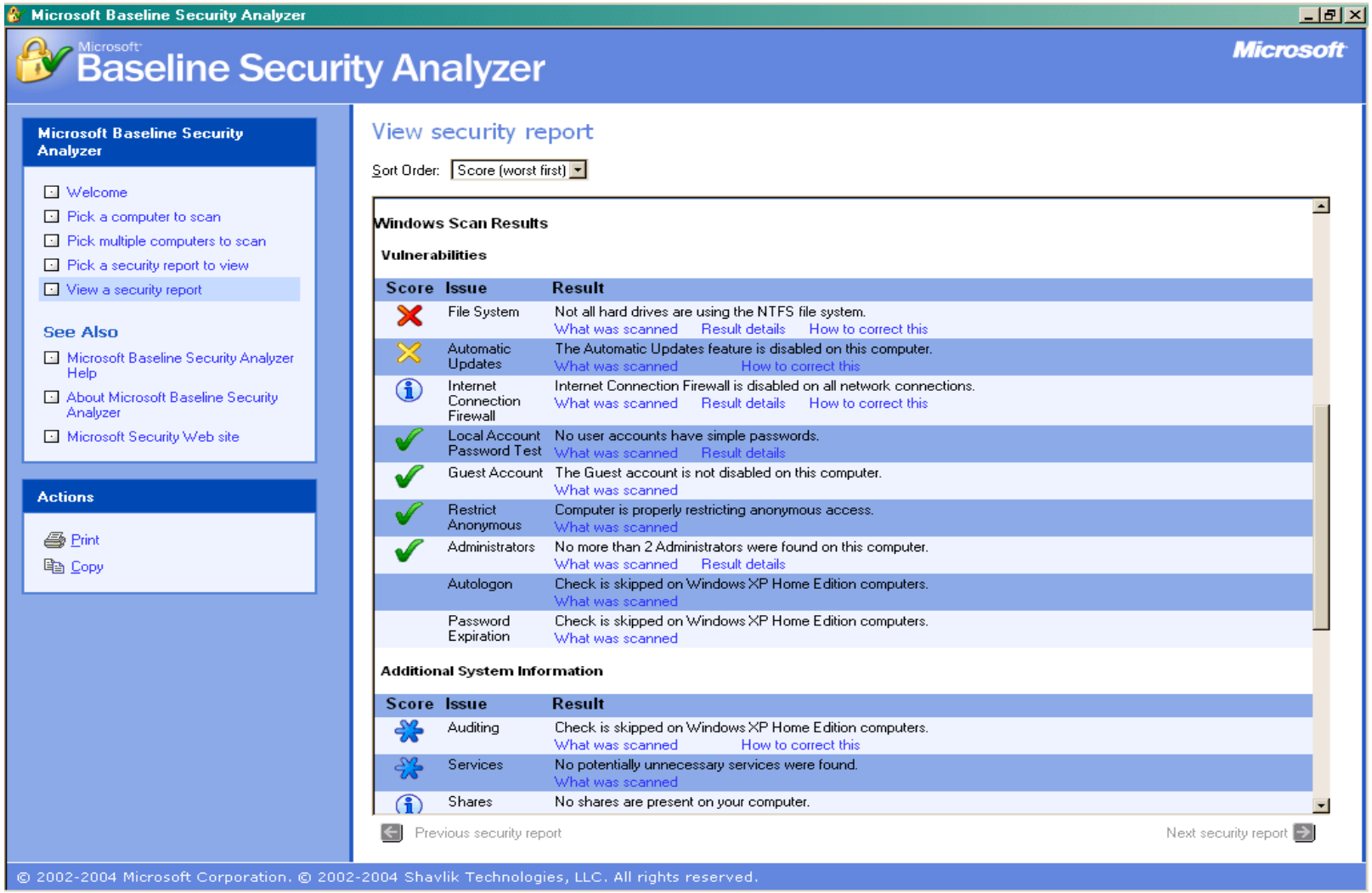
Use IBM Internet Security Scanner tool

6. Host Evaluation



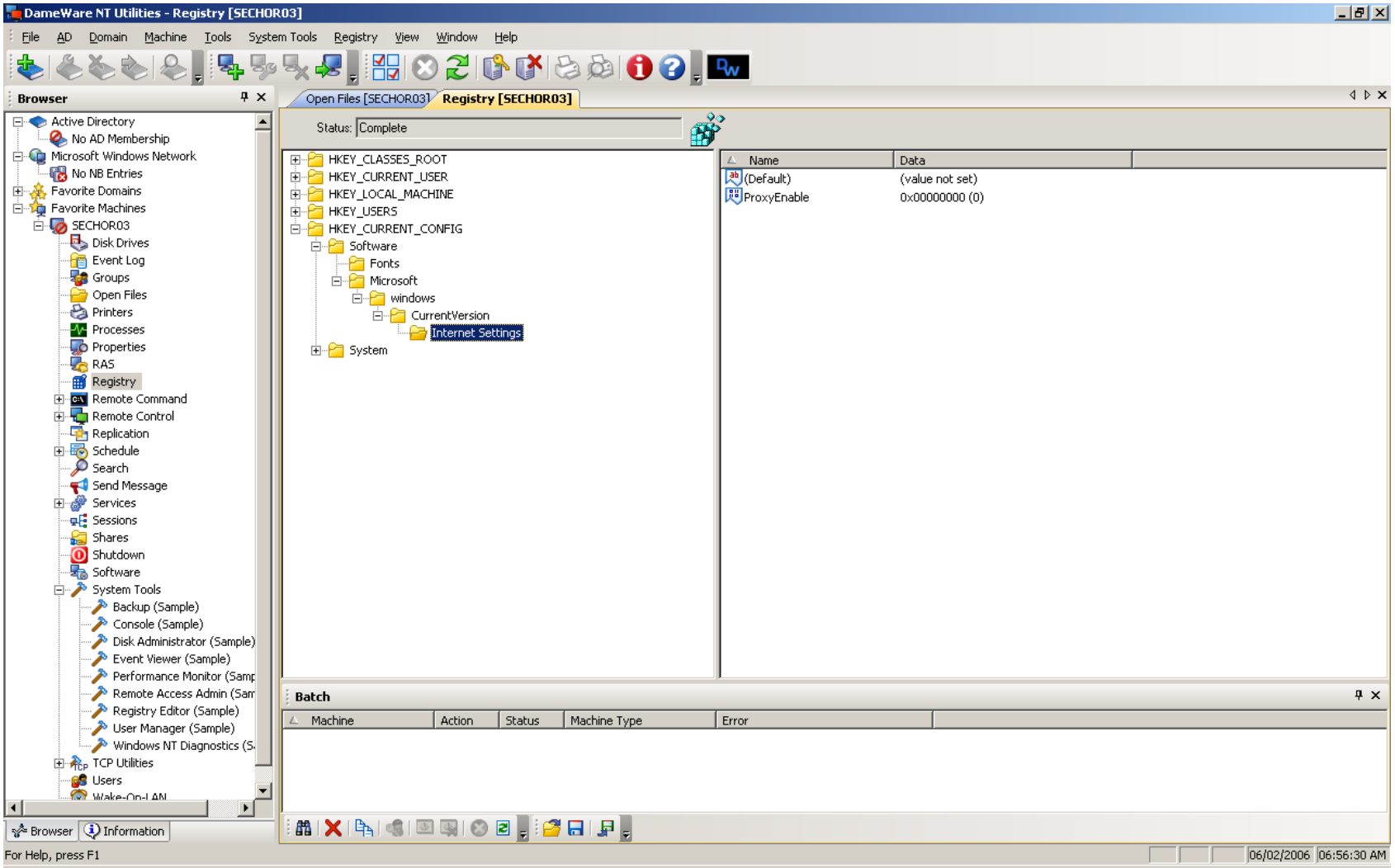
Use CIS Windows Benchmark tool

6. Host Evaluation



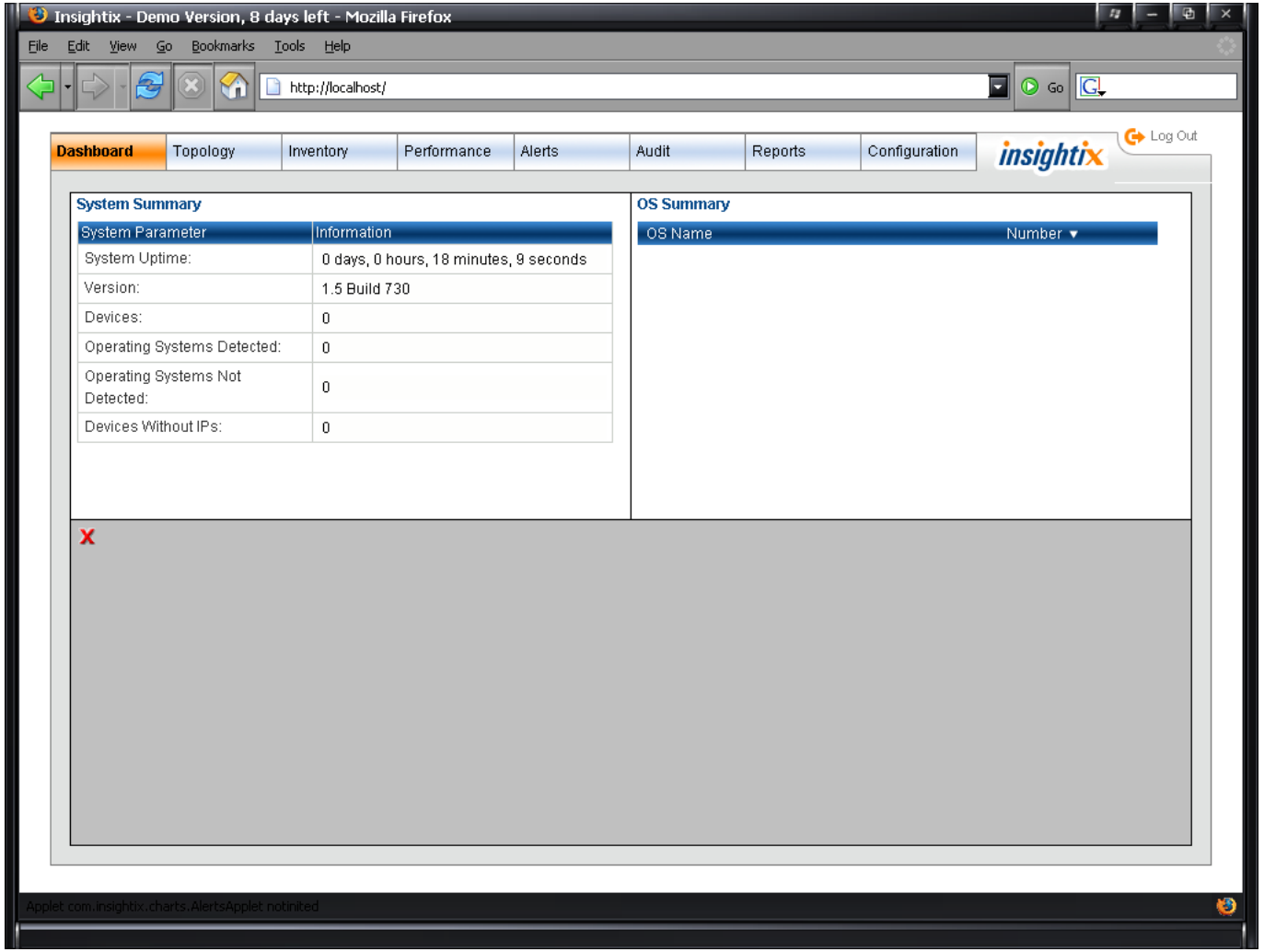
Use MS-Baseline Security Analyzer tool

6. Host Evaluation



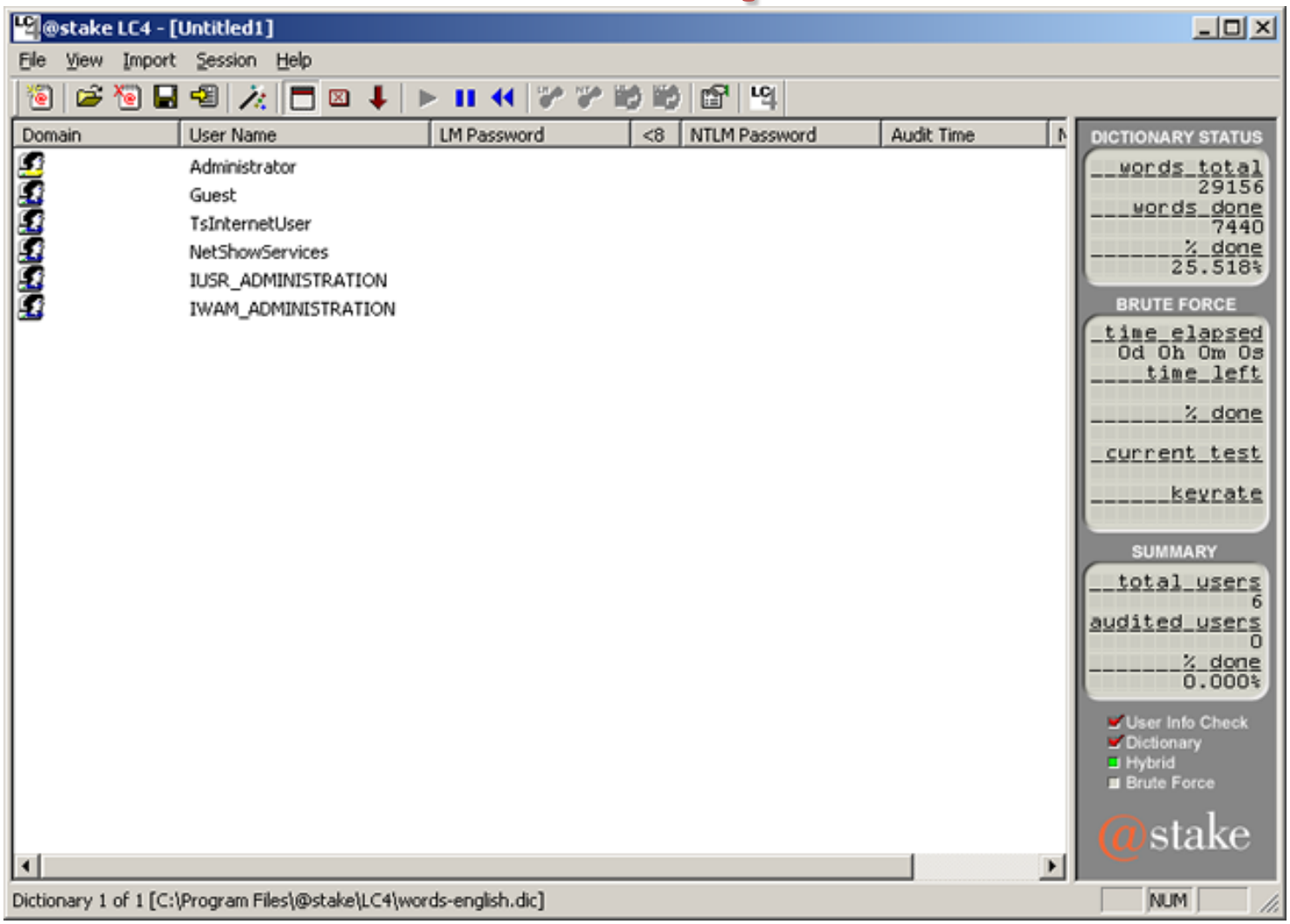
Use DameWare NT Utility tool

7. Network Device Analysis



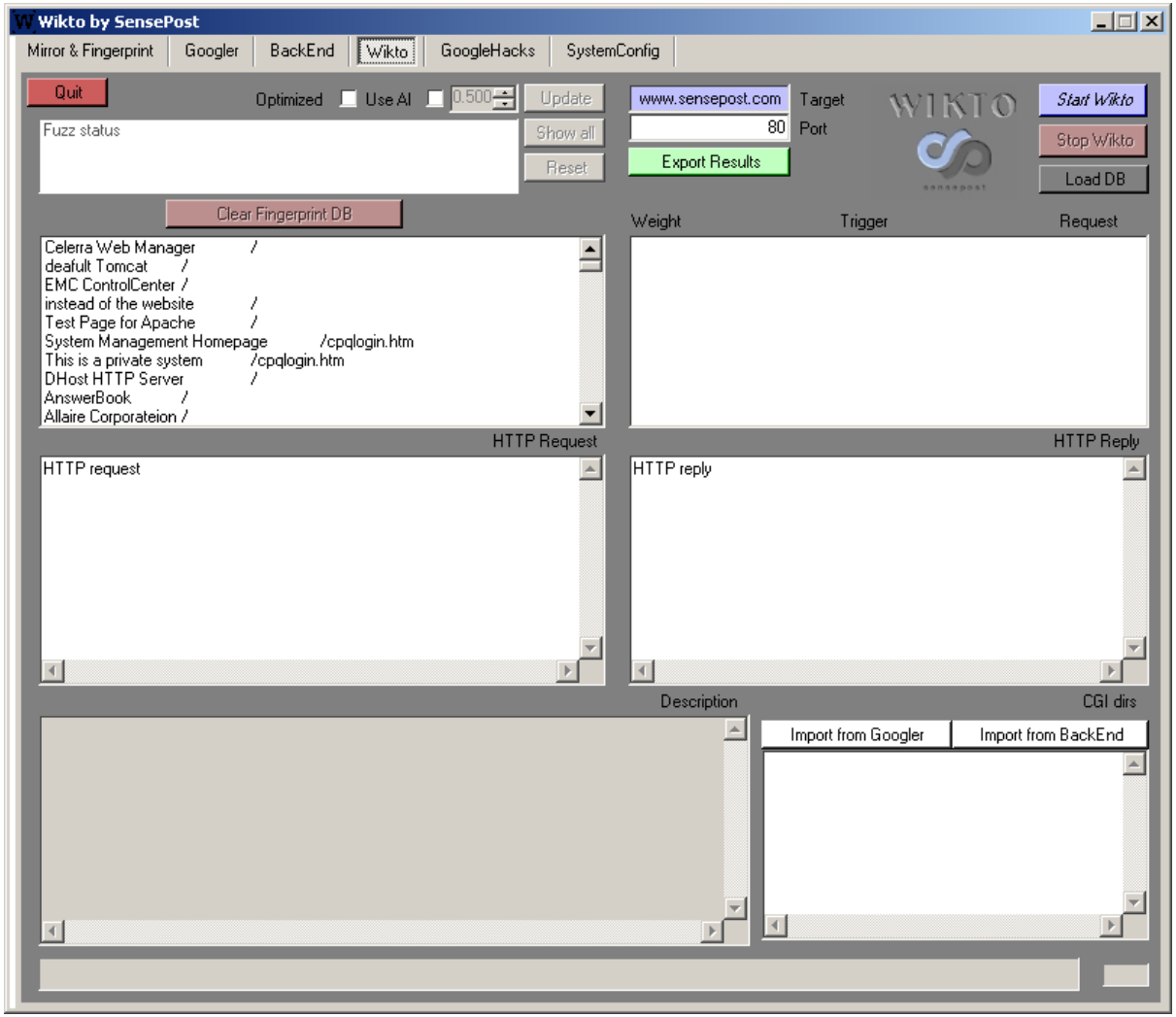
Use Insightix tool

8. Password Compliance Testing



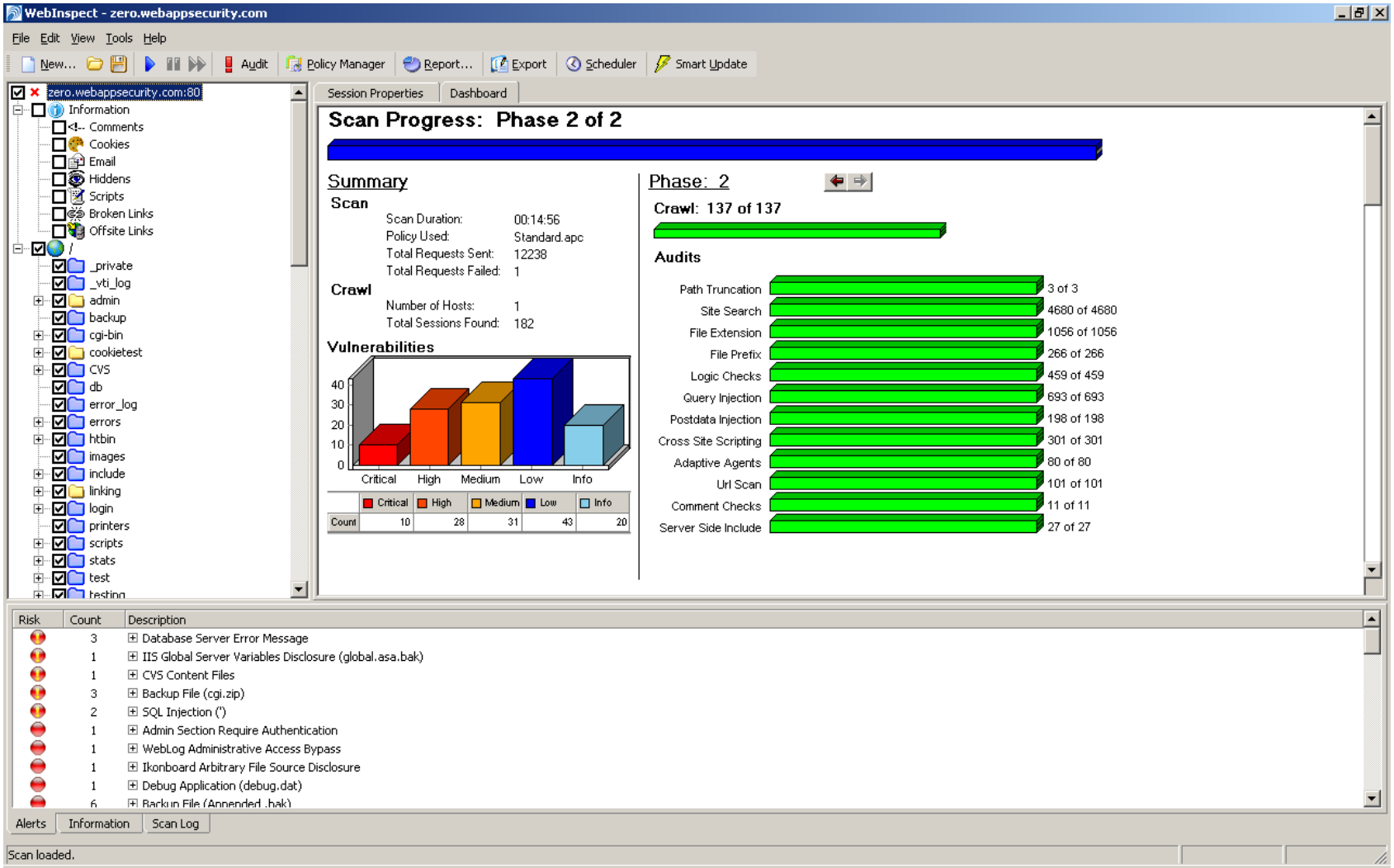
Use L0phtcrack tool

9. Application Specific Scanning



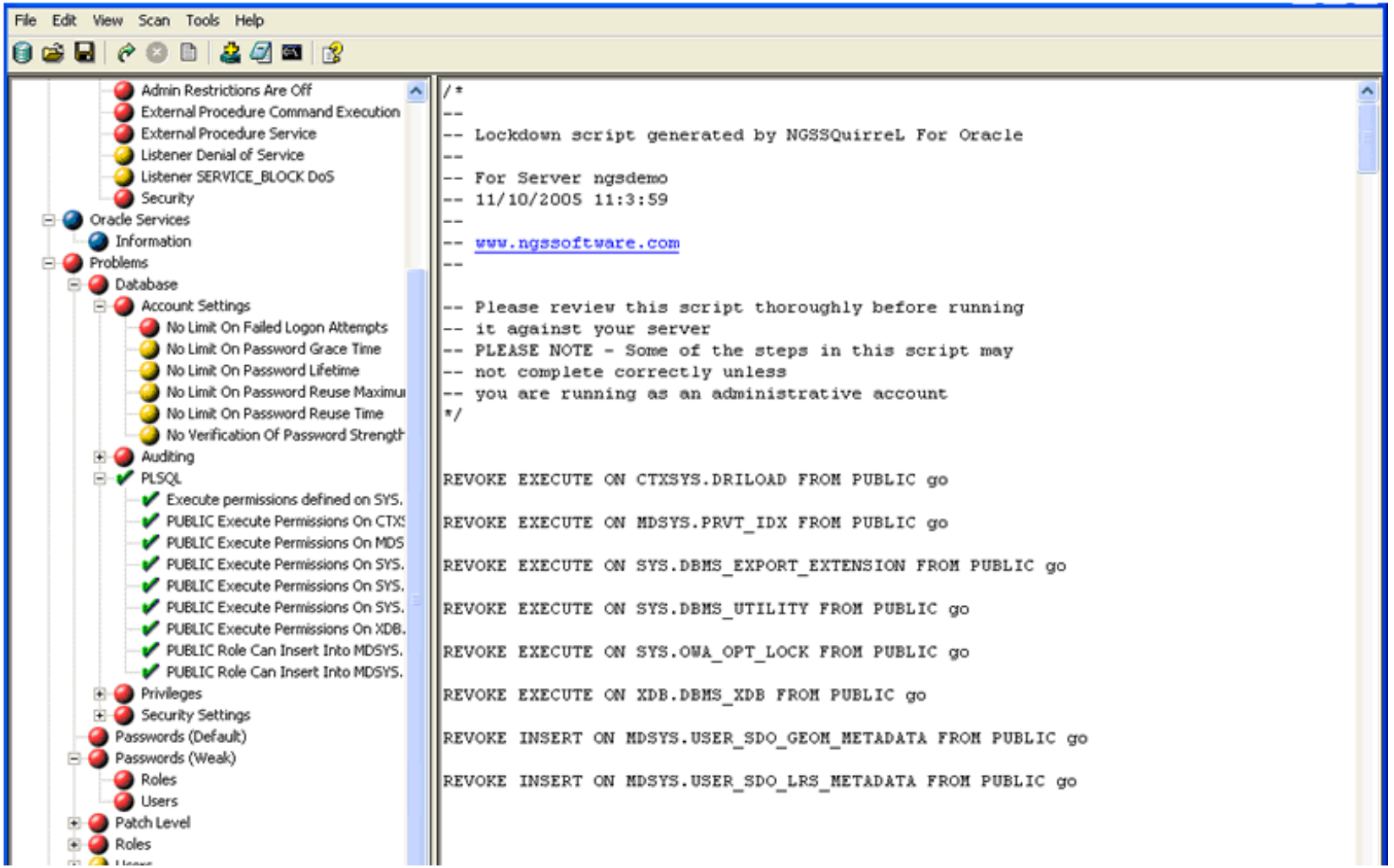
Use Wikto tool

9. Application Specific Scanning



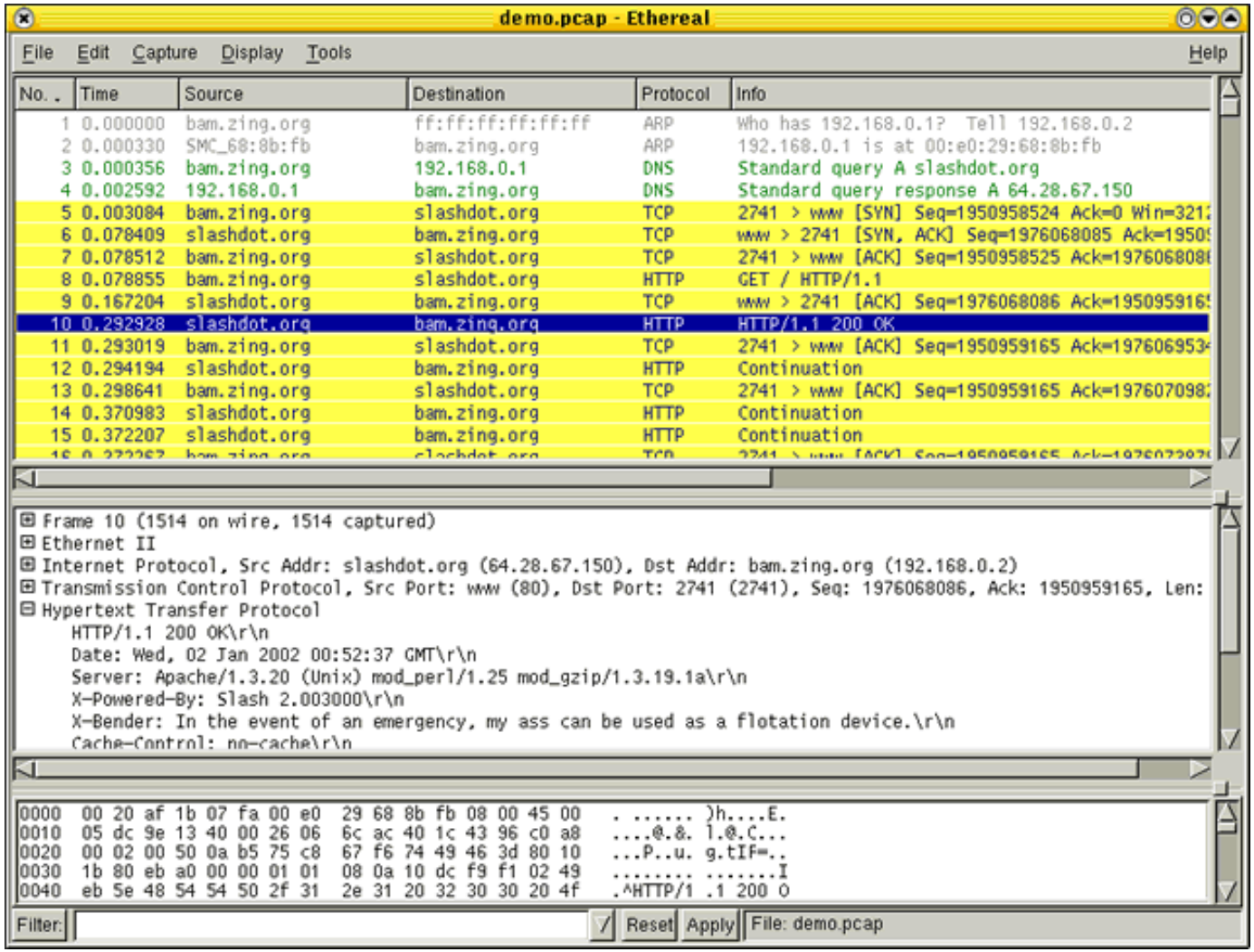
Use WebInspect tool

9. Application Specific Scanning



Use NGS Squirrel tool

10. Network Sniffing



Use Ethereal tool

其他防範措施

- 使用防火牆管理多個出入口
  - Internet (B2C)
  - Extranet (B2B)
  - Cross Domain Intranet (HK, VN, JP, US…etc)
- 使用防火牆將內部區分多個網段
  - Web Zone
  - Application / Database / Testing Zone
  - Transaction / Mainframe Zone
- 使用IDS / IPS入侵偵測與防護設備管理外部攻擊
- 使用工具軟體限制員工存取不當網站, 接收垃圾郵件
- 使用工具限制敏感性資料傳送與存取
- 使用BIOS, HDD, USB加密方式防止設備遺失, 導致資料外洩

其他防範措施

- **網站應用系統弱點**
  - http://www.owasp.org
  - Top 10 in 2007

A1 – Cross Site Scripting (XSS)

A2 – Injection Flaws

A3 – Malicious File Execution

A4 – Insecure Direct Object Reference

A5 – Cross Site Request Forgery (CSRF)

A6 – Information Leakage and Improper Error Handling

A7 – Broken Authentication and Session Management

A8 – Insecure Cryptographic Storage

A9 – Insecure Communications

A10 – Failure to Restrict URL Access

其他防範措施

- **網站應用系統弱點**
- https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- The OWASP Top 10 Web Application Security Risks for 2010
- A1: Injection
- A2: Cross-Site Scripting (XSS)
- A3: Broken Authentication and Session Management
- A4: Insecure Direct Object References
- A5: Cross-Site Request Forgery (CSRF)
- A6: Security Misconfiguration
- A7: Insecure Cryptographic Storage
- A8: Failure to Restrict URL Access
- A9: Insufficient Transport Layer Protection
- A10: Unvalidated Redirects and Forwards

其他防範措施

- **網站應用系統弱點**

  A1: Injection Flaws

  - http://www.owasp.org
  - Source Code Secure Review
  - 建置Web Application Firewall (WAF)
  - 依據銀行公會安控基準建置相關應用系統

Module 13-2：
網路應用系統規範

金融機構規範

- **中華民國銀行公會** http://www.ba.org.tw/

宗旨：

協助政府推行金融政策

協調同業關係及增進同業之共同利益

任務：

推行財經金融政策及商業法令，配合經濟發展研商各業資金之供需調劑，協調同業間各項業務規章之釐訂及編纂，增進國內外金融業務之聯繫、調查、統計、諮詢、研究、發展及發行刊物，維護會員合法權益及調處同業間業務爭執，促進會員間徵信資料之交流、研析、編報及建立重要授信客戶資料，整合會員間資訊系統之策劃，加強會員單位員工之互助、救濟、進修、聯誼及公益事業之舉辦暨服務道德自律規範之推行，參加國際性金融組織會議，增進與各國銀行公會之聯繫與合作，推展國民外交，接受政府或團體委託辦理與研究建議事項，以及參與各項社會公益活動等。

會員：

國內銀行

台北市/台灣省/高雄市銀行公會之會員

金融機構規範

- **金融機構辦理電子銀行業務安控作業基準**
  - 由銀行公會制定提供會員遵循
  - 非法令
  - 非行政命令
  - 為會員自約條款
  - 提供辦理電子銀行業務之安控作業基準

電子銀行

- **定義**

  電子銀行(Electronic Banking)業務係指在金融機構與客戶(自然人及法人)間，透過各種電子設備及通訊設備，客戶無須親赴金融機構櫃台，即可直接取得金融機構所提供之各項金融服務。

- **訊息傳輸途徑**

  係指客戶端利用電子設備及通訊設備與金融機構進行交易時所使用的網路型態。

  - 金融機構專屬網路(Dial-Up, Lease-Line, VPN)
  - 加值網路(Value Added Network，VAN)
  - 網際網路(Internet)
  - 行動網路

電子交易類別

- **轉帳及交易指示**

  涉及資金轉移或直接影響客戶權益

  (如：存/提款、轉帳、匯兌/款、消費、投資、繳款、授信、基金/債票券下單、信用狀申請/修改)

- **非轉帳及交易指示**

  與資金轉移無關或不直接影響客戶權益

  (如：存放款餘額查詢、交易明細查詢、額度查詢、歸戶查詢、託收票據查詢、匯入匯款查詢、信用狀查詢、匯率查詢、利率查詢、共同基金查詢、金融法規查詢、股市行情查詢、投資理財資訊查詢、業務簡介查詢、入扣帳通知、存款不足通知、存放款到期通知、放款繳息通知、託收票據狀況通知、消費通知)

電子交易風險

- **高風險**

  訊息執行結果，對客戶權益有重大影響之各類電子轉帳及交易指示

- **低風險**

  訊息執行結果，對客戶權益**無重大影響**之各類電子轉帳及交易指示

  - 事先約定轉入帳戶
  - 概括約定及限定性繳費繳稅之稅費轉帳
  - 非約定轉入帳戶

    每戶每筆＜5萬、每天累積＜10萬、每月累積＜20萬
  - 採用動態密碼(OTP), 憑證為簽入密碼，可取代前項安全要求

電子金融交易

資料來源：(銀行公會)金融機構辦理電子銀行業務安全控管作業基準

訊息傳輸途徑	金融機構專屬網路 (Lease-Line, VPN)		加值網路 (VAN)		網際網路 (Internet)	
交易類別	轉帳及交易指示	非轉帳及交易指示	轉帳及交易指示	非轉帳及交易指示	轉帳及交易指示	非轉帳及交易指示
訊息隱密性	*非必要*	*非必要*	*非必要*	*非必要*	*必要*	*非必要*
訊息完整性	*必要*	*非必要*	*必要*	*非必要*	*必要*	*非必要*
訊息來源辨識	***高-必要*** *低-非必要*	*非必要*	***高-必要*** *低-非必要*	*非必要*	***高-必要*** *低-非必要*	*非必要*
訊息不可重複性	*必要*	*非必要*	*必要*	*非必要*	*必要*	*非必要*
無法否認訊息	***高-必要*** *低-非必要*	*非必要*	***高-必要*** *低-非必要*	*非必要*	***高-必要*** *低-非必要*	*非必要*

註：高 – 高風險，低 – 低風險

支付工具安控機制

- 帳號密碼(ID and Password)
- 晶片金融卡(FISC Card)
- 一次性動態密碼(One Time Password)
- 數位簽章(Digital Signature)

帳號密碼安控機制

- **安全設計與要求**
  - 帳號(未搭配其他驗證機制)
    - 不得為顯性資料(如：統編、身分證號), 要另行增設代號
    - 不得少於六位、相同英數字、連續英文、連號數字
    - 首次申請須於一個月內強迫變更密碼
  - 代號(帳號為顯性資料時, 增設)
    - 不得為顯性資料
    - 新建立時，不得與帳號及密碼相同
    - 連續錯誤達五次，應妥善處理
  - 密碼
    - 不得少於六位、相同英數字、連續英文、連號數字
    - 不得與帳號及代號相同、不得與前次密碼相同
    - 連續錯誤達五次，不得交易
    - 首次登入應強迫變更預設密碼

帳號密碼安控機制

- **使用範圍(低風險)**
  - 事先約定轉入帳戶
  - 概括約定及限定性繳費繳稅之稅費轉帳
  - 非約定轉入帳戶

    每戶每筆＜5萬、每天累積＜10萬、每月累積＜20萬
  - 採用動態密碼(OTP), 憑證為簽入密碼，可取代前項安全要求
- **控管點**
  - 臨櫃約定
  - ATM約定
  - OTP約定？安全嗎？
  - 電話約定？安全嗎？

晶片金融卡安控機制

- **安全設計與要求**
  - 訊息傳輸應採用56位元DES或1024位元RSA以上加密
  - 網站應檢查資料來源網站或網頁正確性
  - 伺服器端限定網頁過期時間(TimeOut)
  - 伺服器端檢查網頁合法性(Session)
  - 網頁應加入操作者回應事項
  - 網頁應設計動態物件呈現
  - 網頁重要變數應隨機變動或亂碼化保護
  - 元件於帳務交易時, 每次輸入卡片密碼產生交易驗證碼
  - 元件應檢查網站正確性
  - 元件應經過作業系統被認可之數位憑證簽章
  - 元件應於存取卡片時限定為獨占模式
  - 元件應設計經由人工抽拔卡片動作後才回傳交易驗證碼

  - 建議採用經銀行公會審核通過之確認型讀卡機

晶片金融卡安控機制

- **使用範圍(低風險)**
  - 事先約定轉入帳戶
  - 概括約定及限定性繳費繳稅之稅費轉帳
  - 非約定轉入帳戶

    每戶每筆＜5萬、每天累積＜10萬、每月累積＜20萬

- **控管點**
  - 客戶應妥善保管卡片
  - 客戶完成交易後應立即自讀卡機移除
  - 銀行應確認付款指示來源資訊的正確性
  - 銀行應確認產生交易認證碼資訊的正確性

數位簽章安控機制

- **安全設計與要求(研議中)**
  - 訊息傳輸應採用56位元DES或1024位元RSA以上加密
  - 網站應檢查資料來源網站或網頁正確性
  - 伺服器端限定網頁過期時間(TimeOut)
  - 伺服器端檢查網頁合法性(Session)
  - 網頁應加入操作者回應事項
  - 網頁應設計動態物件呈現
  - 網頁重要變數應隨機變動或亂碼化保護
  - 元件於帳務交易時,每次輸入卡片密碼產生數位簽章
  - 元件應檢查網站正確性
  - 元件應經過作業系統被認可之數位憑證簽章
  - 元件應設計經由人工抽拔卡片動作後才回傳數位簽章或於同筆交易搭配額外硬體設備驗證機制
  - 建議採用經銀行公會審核通過之確認型讀卡機或載具

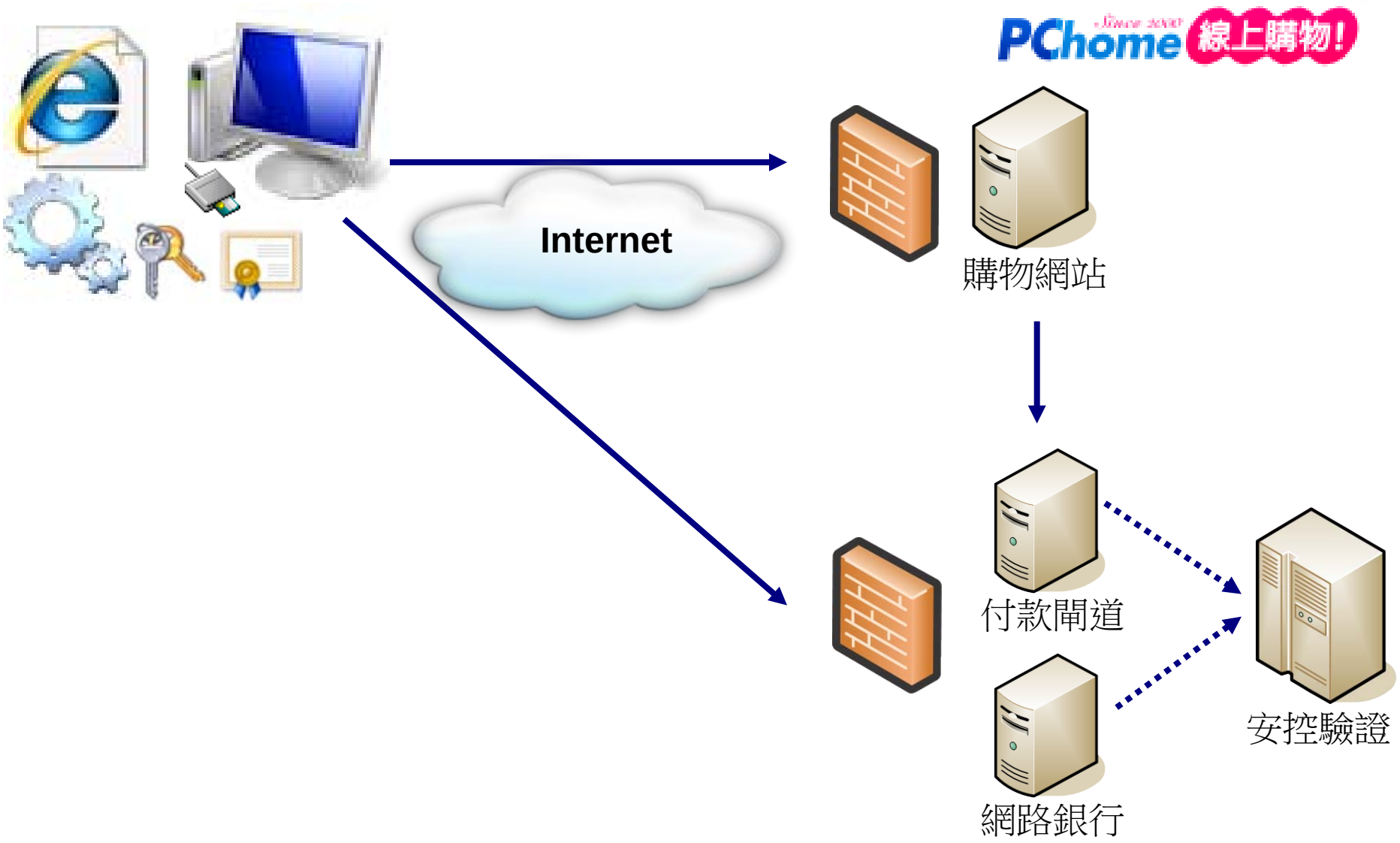
數位簽章安控機制

- **使用範圍(高風險)**
  - 不須事先約定轉入帳戶
  - 概括約定及限定性繳費繳稅之稅費轉帳
  - 不限定交易金額
  - 須具備不可否認傳送/接收訊息之交易類型

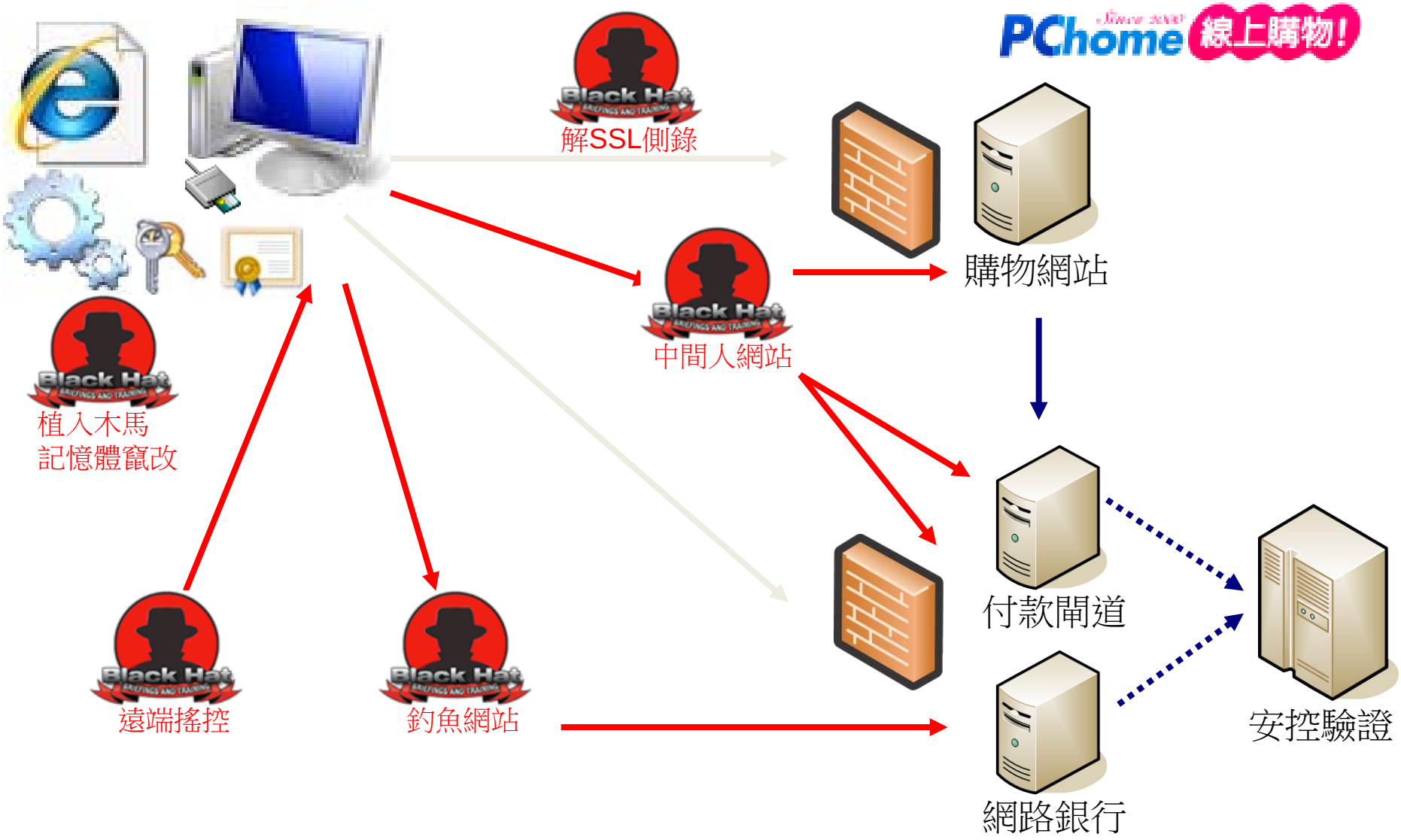
- **控管點**
  - 客戶應妥善保管載具(e.g. IC Card, USB Token)
  - 客戶完成交易後應立即自讀卡機或USB移除
  - 銀行應確認付款指示來源資訊的正確性
  - 銀行應確認載具安全性
  - 銀行應確認金鑰產製與客戶正確性
  - 銀行應確認驗證數位簽章正確性、憑證有效性、CPS適用性

Module 13-3：
系統設計注意事項

電子交易架構



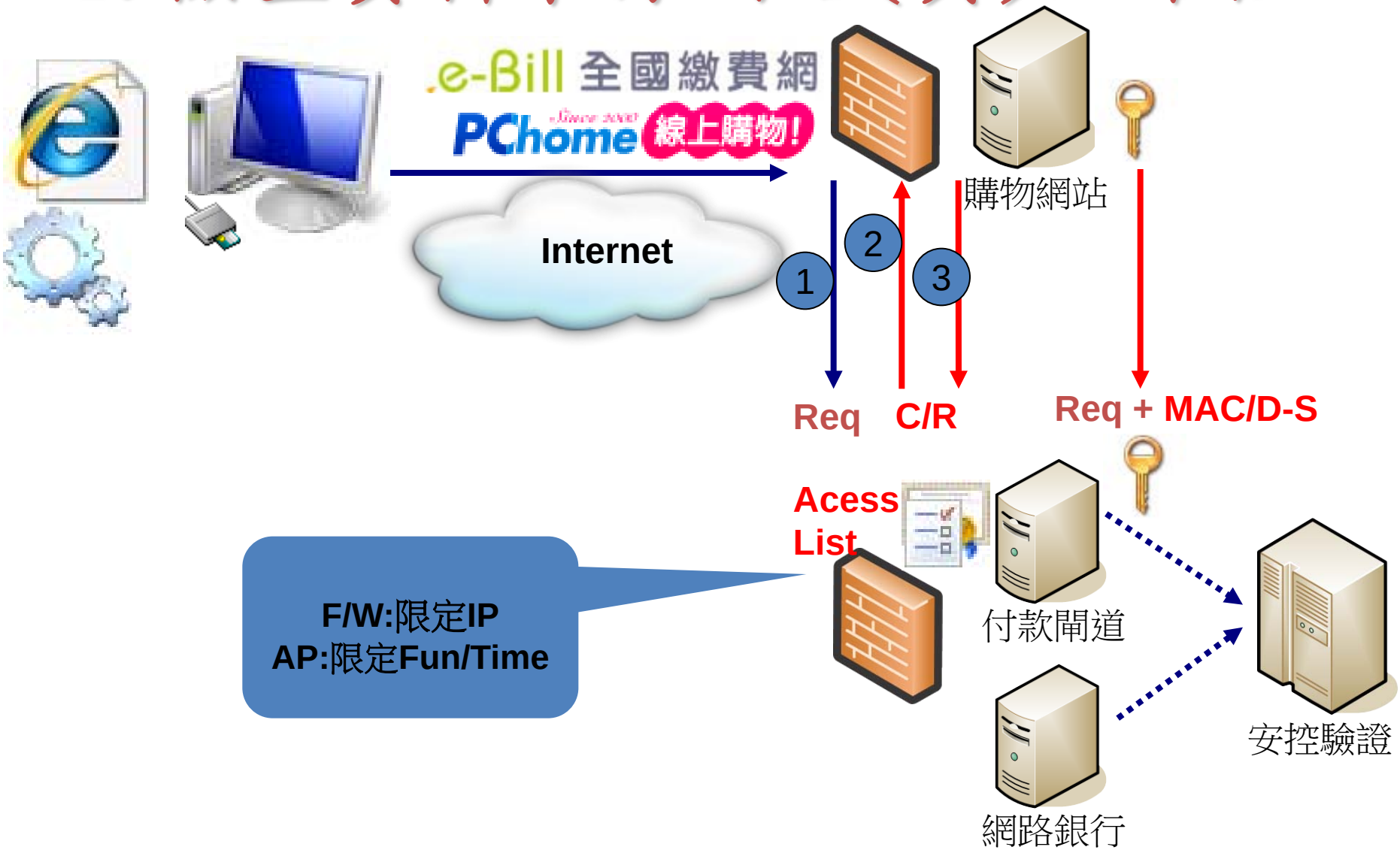
電子交易風險


e-Bill 全國繳費網
PChome 線上購物!
解SSL側錄
植入木馬
記憶體竄改
中間人網站
購物網站
遠端搖控
釣魚網站
付款閘道
網路銀行
安控驗證

系統設計注意要項

1. 轉帳及交易指示
2. 檢查資料來源網站(頁)正確性
3. 檢查網頁合法性
4. 操作者回應事項
5. 動態物件呈現
6. 元件檢查網站正確性
7. 檢查元件數位簽章
8. 元件設計抽拔機制
9. 支援確認型讀卡機(載具)
10. 額外載具輔助認證

1. 檢查資料來源網站(頁)正確性



2. 檢查網頁合法性


中華民國銀行公會 - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
新增(N)
開啓舊檔(O)... Ctrl+O
使用 Microsoft Office Word 編輯(D)
儲存檔案(S) Ctrl+S
另存新檔(A)...
設定列印格式(U)...
列印(P)... Ctrl+P
預覽列印(V)...
傳送(E)
匯入和匯出(I)...
內容(R)
離線工作(W)
關閉(C)
視窗(W) Ctrl+N
郵件(M)
公佈(P)
連絡人(C)
網際網路通話(I)
New Window
s Association Of The Republic Of China
回首頁 網站導覽 本會簡介
法規與指引
會員專區
委員會專區
The Bankers Association Of
The Republic Of China

3. 操作者回應事項

遠端遙控

人工判讀

OCR判讀

4. 動態物件呈現

轉帳 輸入交易資料

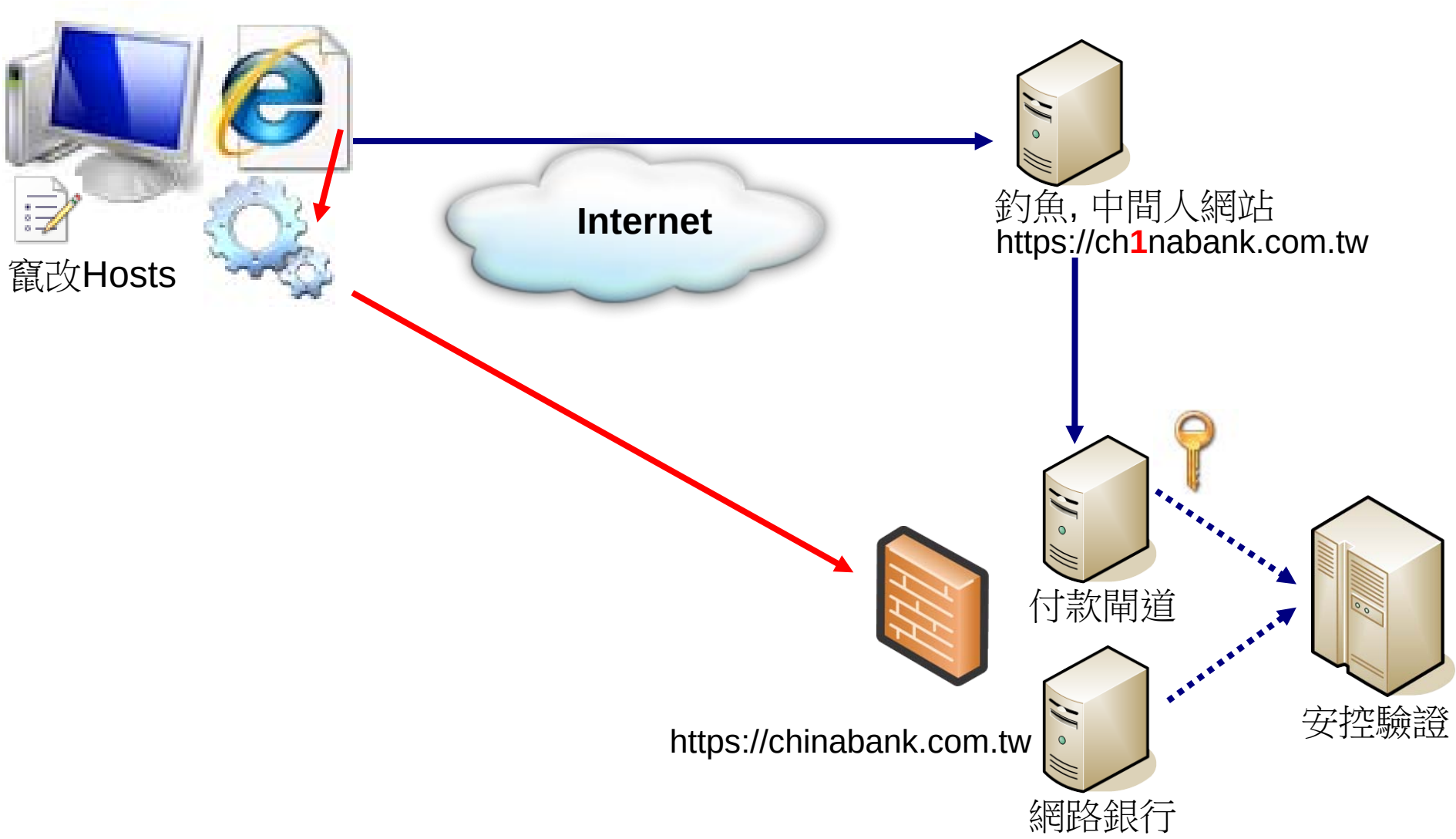
轉出帳號	822 - 中國信託商業銀行 0000901530757401
轉入帳號	◉ 約定帳號： 請選擇
	○ 常用帳號： 請選擇
	○ 其他帳號：
	銀行代號： 822 - 中國信託商業銀行
	帳號 加入常用帳號
轉出金額	新台幣 元
晶片卡密碼	請在螢幕鍵盤中輸入您的密碼
螢幕鍵盤	6 1 4 8 3 5 9 7 2 0 清 除
交易備註	
交易成功通知	請輸入要通知的Email,2個以上以分號隔開

轉帳 輸入交易資料

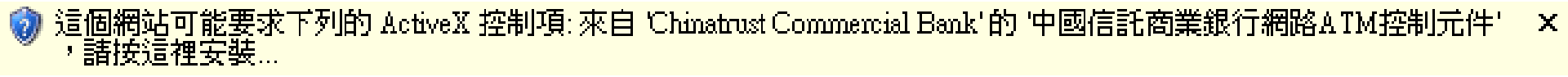
轉出帳號	822 - 中國信託商業銀行 0000901530757401
轉入帳號	◉ 約定帳號： 請選擇
	○ 常用帳號： 請選擇
	○ 其他帳號：
	銀行代號： 822 - 中國信託商業銀行
	帳號 加入常用帳號
轉出金額	新台幣 元
交易備註	
交易成功通知	請輸入要通知的Email,2個以上以分號隔開
晶片卡密碼	請在螢幕鍵盤中輸入您的密碼
螢幕鍵盤	6 1 4 8 3 5 9 7 2 0 清 除

IE Embeded in WebBrowser Controler

5. 元件檢查網站正確性


竄改Hosts
Internet
釣魚, 中間人網站
https://ch1nabank.com.tw
付款閘道
安控驗證
https://chinabank.com.tw
網路銀行

6. 檢查元件數位簽章



SHA1驗證— 下列SHA1驗證檔，只供驗證安裝程式是否被竄改，申報人可不需下載。若想驗證由其它網站下載之申報程式，請使用SHA1 指紋碼工具 。SHA1工具使用方式，請詳見說明

- 下載 SHA1 工具驗證程式 windows-kb841290-x86-enu.exe

7. 元件設計抽拔機制

防止木馬假交易

防止遠端遙控

還有漏洞？

使用者確認交易

8. 支援確認型讀卡機(載具)

顯示交易內容

按鈕確認交易

已通過銀行公會認證

閃燈提示

按鈕確認交易

產品設計中

顯示交易內容

按鈕確認交易

9. 額外載具輔助認證


Authenex
123456 123456 123456
123456 123456 123456
123456 123456 123456
123456 123456 123
342601
Nordea
Java Card
中國信託
MENU
ON

Module 13-4：
客戶使用注意事項

客戶使用電子金融注意事項

- **確認網站網址**
  - 如果您不清楚銀行的正確網址，交易前請先打電話查詢，千萬不要透過其他不明網頁或是電子郵件連結，以免被偽造網站詐騙。
  - 因使用網路服務，而須輸入您的個人資料前，請先確認該服務的安全性及合法性，避免進行未經授權的交易，而承擔損失風險。
  - 隨時核對銀行帳戶明細，做好帳單管理，交易完成後，應儘速登入網路銀行檢核是否正確，一旦發覺或懷疑帳戶、密碼未經授權而被他人使用時，立即以電話或其他約定方式通知。

客戶使用電子金融注意事項

- **網路密碼的設定**
  - 請勿使用「懶人密碼」（如：出生年月日、身分證字號或電話），儘量使用英文字母、數字及特殊符號的組合來設定密碼，此外，也請注意要定期更改密碼。
  - 請勿將所有帳號都設定同樣的密碼，最好每個帳號都有單獨的密碼及登入資料，以減低被盜用的風險。
  - 不要以個人相關資料（如：出生年月日、身分證字號或電話）做為密碼提示的問題或答案，避免犯罪集團蒐集個人相關資料後，即可利用密碼提示猜到密碼。

客戶使用電子金融注意事項

- **網路密碼的保管**
  - 不要透過未加密的電子郵件寄送網路密碼及個人資料，以免遭駭客截取；且勿將個人隱私資料過度於網路上曝光，以免成為有心人士覬覦之對象。
  - 儘量記住密碼及個人資料，不要寫在記事本、提款卡或存摺等上面，更不要將密碼與存摺、卡片等置放於同一處，避免因未收妥疏忽而被竊取或窺視。
  - 應提高警覺防範詐騙集團套取密碼及個人資料，例如：詐騙集團假冒銀行人員套問金融卡密碼，或假藉通知使用者資料過期需更新，以基於安全考量進行身分驗證為由，而套取帳號、密碼等個人資料。
  - 使用網路服務時，千萬不要因懶惰或怕忘記密碼，而將密碼及登入資料儲存在電腦中，最好每次都自行鍵入較為安全。

客戶使用電子金融注意事項

- **使用晶片金融卡及網路自動櫃員機(Web ATM)加強網路交易**
  - 民眾應於網路ATM交易完成後即取出卡片並妥善保管，避免因忘記取出造成卡片遺失與後門程式有機可趁之風險。
  - 民眾可選用確認型讀卡機進行交易，以硬體設備確認交易內容與行為，降低後門程式與遠端遙控之攻擊。

客戶使用電子金融注意事項

- **使用行動電話、個人數位助理(PDA)及無線網路應注意事項**
  - 使用行動電話及個人數位助理(PDA)進行網路交易前，請安裝防火牆及防毒軟體，並設定一個不易被猜解的密碼，同時請記得開啟加密功能，並備份資料，且於不使用或不需要藍芽功能（個人裝置間短距離通訊之無線傳輸技術）時，予以關閉，以避免他人意圖連結您的行動電話及PDA，進而竊取您的個人資料。
  - 設定您的無線網路基地台時，請記得更改預設的密碼和使用者名稱，開啟加密功能，並請小心使用無線網路名稱及廣播網路名稱(SSID)，以減少每個有相容裝置的人可能和您的無線網路建立連結，截取您傳輸資料的風險。
  - 使用公用的無線網際網路前，請關閉「檔案和印表機共享」及「電腦對電腦（點對點）傳輸網路」功能，清除「我的最愛」網路清單，加密所有檔案，且不要傳送敏感性的資料。

總結Summary

- **資安攻擊型態與演進Types of Attacks**
  - 內部不當網路存取(59%)
    Insider abuse of Net access
  - 電腦病毒感染(52%)
    Virus
  - 行動裝置/電腦失竊(50%)
    Laptop / Mobile device theft
  - 以合法身份發送釣魚台網站信件(26%)
    Phishing where your organization was fraudulently represented as sender
  - 即時通訊(IM)不當使用(25%)
    Instant messaging misuse

總結Summary

- **基本防範措施**
  - 掃瞄Scanning
    Port / SNMP / Vulnerability / Application
  - 列舉Enumeration
    Wireless Enumeration
  - 探索Grabbing
    Banner Grabbing
  - 分析Analysis
    Network Device Analysis
  - 評估Evaluation
    Host Evaluation
  - 測試Testing
    Password Compliance /滲透Penetration
  - 發覺Sniffing
    Network Sniffing

總結Summary

- **網路應用系統規範**

訊息傳輸途徑	金融機構專屬網路 (Lease-Line, VPN)		加值網路 (VAN)		網際網路 (Internet)	
交易類別	轉帳及交易指示	非轉帳及交易指示	轉帳及交易指示	非轉帳及交易指示	轉帳及交易指示	非轉帳及交易指示
訊息隱密性	*非必要*	*非必要*	*非必要*	*非必要*	*必要*	*非必要*
訊息完整性	*必要*	*非必要*	*必要*	*非必要*	*必要*	*非必要*
訊息來源辨識	***高-必要*** *低-非必要*	*非必要*	***高-必要*** *低-非必要*	*非必要*	***高-必要*** *低-非必要*	*非必要*
訊息不可重複性	*必要*	*非必要*	*必要*	*非必要*	*必要*	*非必要*
無法否認訊息	***高-必要*** *低-非必要*	*非必要*	***高-必要*** *低-非必要*	*非必要*	***高-必要*** *低-非必要*	*非必要*

總結Summary

- **網路應用系統規範**
  - 帳號密碼 ID & Password
    - 密碼若被竊, 帳戶資料及歷史交易恐亦被竊??
    - 交易型態限制(約定帳號, 繳費稅, 概括性約定)
    - 非約定帳號金額限制
  - 晶片金融卡 IC Card
    - 可跨行
    - 非約定帳號金額限制
    - 於國外預借現金時, 遇到ATM側錄??
  - 數位簽章 Digital Signature
    - 驗CRL
    - 驗憑證鍊
    - 驗註冊銀行RA
    - 簽章時, 你知道內容嗎？沒被改嗎？
  - 一次性密碼One Time Password
    - 產生密碼後, 可放多久再用? 遇到Man In The Middle?

總結Summary

- **系統設計注意要項**
  - 來源正確性
  - 網頁合法性
  - 操作者回應
  - 動態物件呈現
  - 網站正確性
  - 程式碼簽章
  - 元件抽拔
  - 確認型讀卡機
  - 額外輔助載具

總結Summary

- 你可以…
  - 允許於交易進行前, 由銀行針對你的PC掃毒
  - 允許於交易進行時, 由銀行限制其他連網
  - 採用確認型讀卡機或載具, 透過硬體設備確認交易內容與行為
  - 作業系統安全性更新

參考文獻Reference

- 銀行公會,金融機構辦理電子銀行業務安控作業基準(2008/10)
- 金管會銀行局, 客戶使用網路銀行注意事項(2008/9)
- IATRP, The 10 Baseline Activities of INFOSEC Evaluation Methodology(2008/10)

References

- 教育部顧問室編輯 “電子商務安全”教材
- Turban et al., Introduction to Electronic Commerce, Third Edition, 2010, Pearson