麟瑞科技
RING LINE CORPORATION

98年度TWAREN教育訓練

打造銅牆鐵壁-網路及系統安全面面觀

夏克強
麟瑞科技　技術顧問
CCNA, CCDA, CCNP, CQS
BS7799 Lead Auditor, CEH, OCA, OCP

Agenda

- Session 1
  - 資訊安全三要素(CIA Triad)
  - Risk Assessment
  - Web Hacking Techniques
  - Vulnerability Scan
  - Risk-aware Management System
- Session 2
  - Data Security and Hardening

Risk Concept

- **Risk**
  - a potential harm or loss to a system
  - the probability that a threat will materialize
- **Primary goal of RM is to mitigate risk**
  - reduce the risk until it reaches a level acceptable to an organization
  - the risk can never be totally eliminated
- RM is defined as the identification, analysis, control, and minimization of loss associated with events

CIA Triad

- **Confidentiality**
- **Integrity**
- **Availability**

- C.I.A's opposite is D.A.D
  - Disclosure
  - Alteration
  - Destruction

CIA Triad

- **Confidentiality**

– to prevent the intentional or unintentional unauthorized disclosure of data's contents.

– Network monitoring, shoulder surfing, steal password file, and social engineering are ways to thwart it.

– Encrypting, networking traffic padding, strict access control, data classification, and personnel's proper procedure training can help achieve confidentiality.

CIA Triad

- **Integrity**

– to ensure modifications not made to data by unauthorized personnel or processes

– to ensure unauthorized modifications not made to data by authorized personnel or processes

– to ensure the data internally and externally consistent

CIA Triad

- **Availability**

– to ensure the reliable and timely access to data or computing resources by appropriate personnel

– DoS attacks are methods to disrupt availability and productivity.

– Fault tolerance and backups should take place to provide availability and productivity of network, systems, and information.

Risk Triple

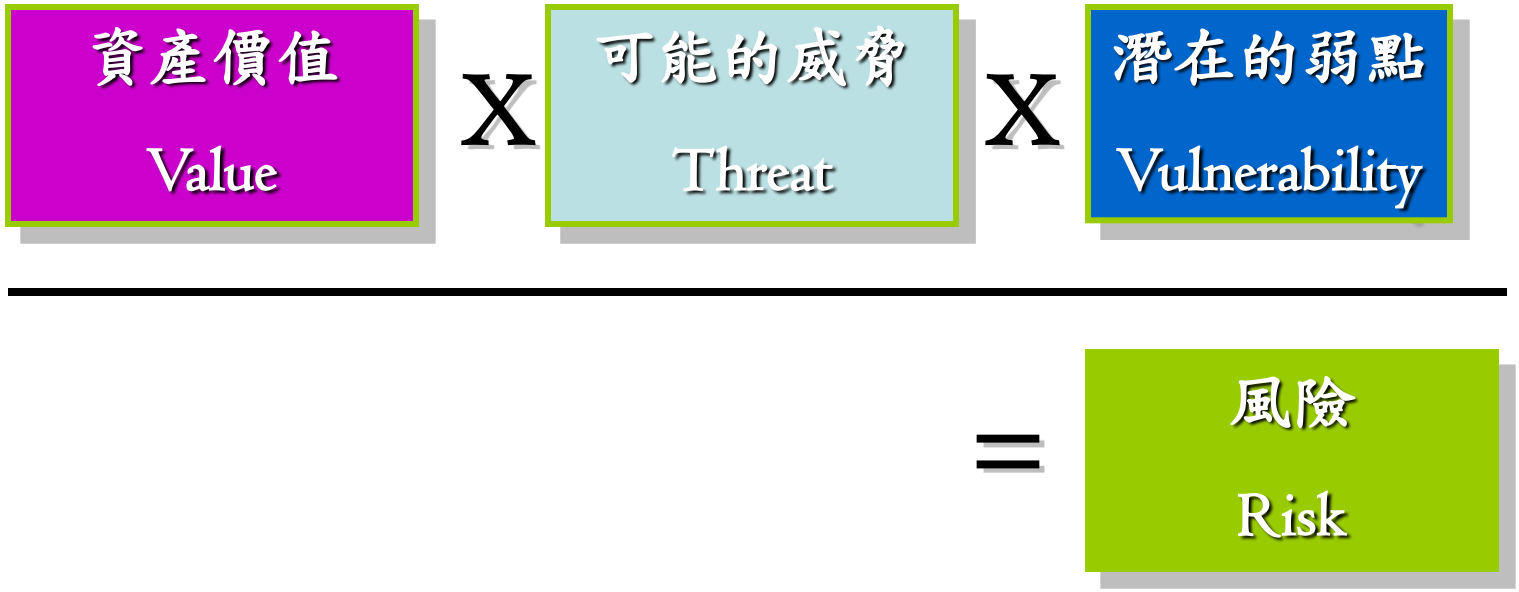
- **Asset** – a resource, process, product, computing infrastructure, etc.
- **Vulnerability** – Vulnerability is a software, hardware, or procedure weakness give attacker unauthorized access resources.
- **Threat** – Threat is any potential danger to resources. The company can't eliminate the threat.
- **Threat Agent** – Threat Agent is something or something that can make damage to resources.

Risk Triple

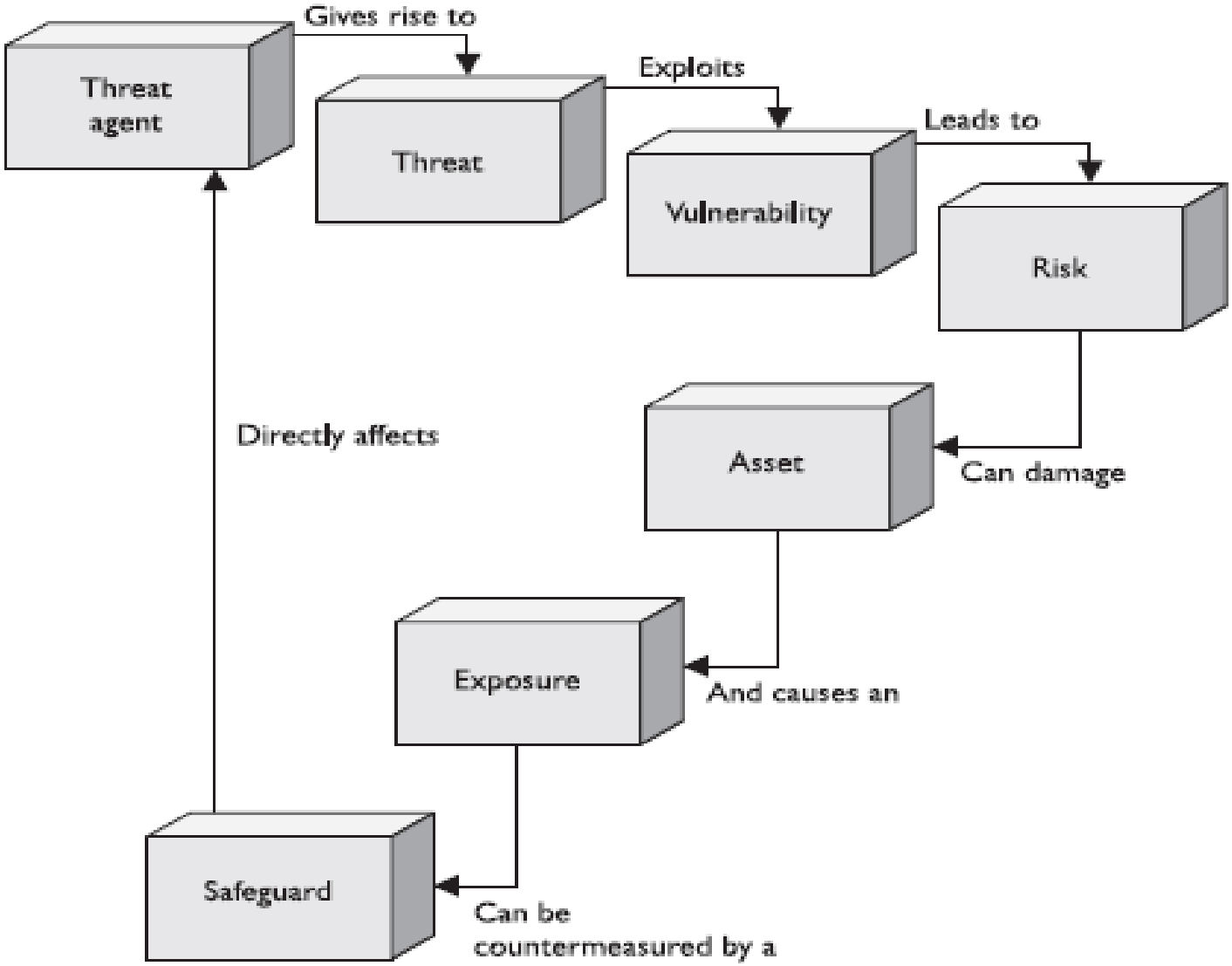
- **Exposure** – Exposure is an instance of be exposed to losses from a threat agent. Threat agent exploits vulnerability to damage assets is an exposure.
- **Countermeasure or Safeguard** – Countermeasure, or safeguard, mitigates the potential risk. It's a software configuration, hardware, or procedure that eliminates vulnerability or reduces the risk being able to exploit vulnerability.

Risk Triple

- **Risk** – Risk is the likelihood, potential, and probability of a threat agent taking advantage of vulnerability. Reducing vulnerability or threat agent reduces the risk.



Relationships among Security Factors



Risk Analysis

- **Quantitative vs. Qualitative**
- **Exposure Factor (EF)**

the percentage of loss a realized threat event would have on a specific asset

- EX. 30 %
- **Single Loss Expectancy (SLE)**

the dollar loss assigned to a single event

SLE = Asset Value ($) * EF

- EX. $50,000 * 30% = 15,000(SLE)

Risk Analysis

- **Annualized Rate of Occurrence (ARO)**

the estimated frequency in which a threat is expected to occur

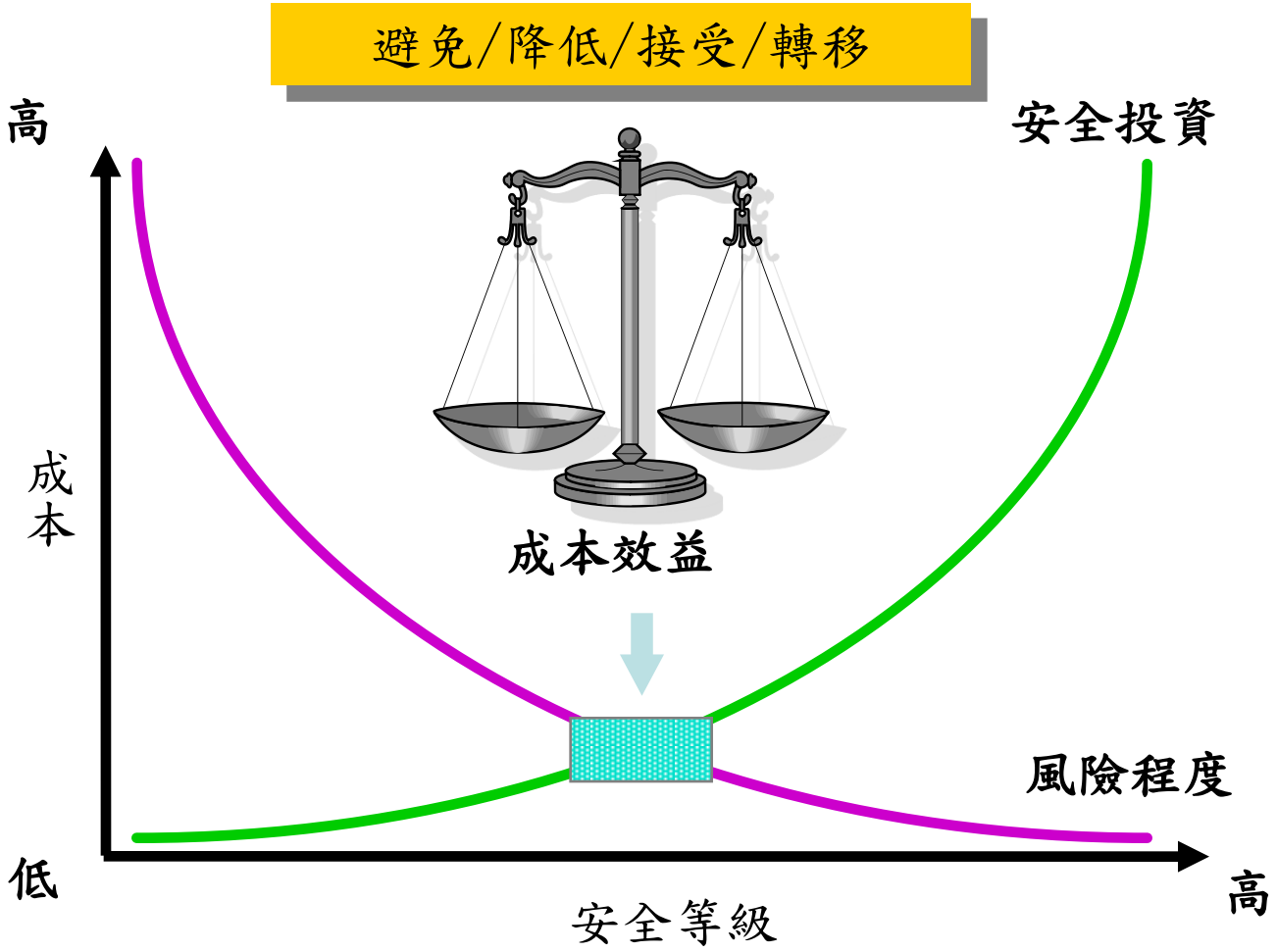
- **Annualized Loss Expectancy (ALE)**

the annual expected financial loss to an organization from a threat ALE = SLE * ARO

Qualitative RA

評鑑分組	資訊資產群組	總風險	風險計算				資安衝擊				風險發生率			
			機密性	完整性	可用性	適法性	機密性	完整性	可用性	適法性	機密性	完整性	可用性	適法性
1	[redacted]	A	D	A	D	D	0	3	1	0	0	4	1	0
1	行政規劃資訊	B	D	B	D	D	0	2	1	0	0	4	1	0
1	其他服務規劃及他機關委託	B	D	B	D	D	0	2	1	0	0	4	1	0
1	[redacted]	C	D	C	D	D	0	1	1	0	0	4	1	0
2	代施委外招標案件開標前資訊	B	C	C	B	D	2	2	2	0	1	1	3	0
2	[redacted]	C	D	C	D	D	1	2	2	0	1	1	0	0
2	[redacted]	B	B	B	D	D	3	3	2	0	1	1	0	0
2	[redacted]	B	B	B	C	D	3	3	2	0	1	1	1	0
2	[redacted]	B	D	B	B	D	1	2	2	0	0	3	3	0
3	涉違規，違規調查資料	B	B	B	D	D	3	2	1	0	1	4	0	0
3	電話，來函申訴(檢舉)紀錄及相關公文	B	B	C	D	D	3	2	1	0	1	1	0	0
3	局長電子信箱	B	B	C	D	D	3	2	1	0	1	1	0	0
3	其他機關轉來申訴檢舉案件 (涵蓋檢舉人資料)	B	B	C	D	D	3	2	1	3	1	1	0	0
3	比較試驗報告(未公佈者)及審查	B	B	B	C	D	3	3	2	0	1	1	1	0
3	比較試驗報告公佈	B	D	B	C	D	1	3	2	0	1	1	1	0
3	[redacted]	A	D	A	B	D	0	3	3	0	0	4	1	0
3	[redacted]	B	B	B	D	D	3	3	1	3	1	1	0	0

資訊安全 = 風險管理與控制



Agenda

- Session 1
  - 資訊安全三要素(CIA Triad)
  - Risk Assessment
  - Web Hacking Techniques
  - Vulnerability Scan
  - Risk-aware Management System
- Session 2
  - Data Security and Hardening

What malicious hackers do?

- Reconnaissance
  - Active / passive
- Scanning
- Gaining access
  - Operating system level / application level
  - Network level
  - Denial of service
- Maintaining access
  - Uploading / altering / downloading programs or data
- Covering tracks

駭客攻擊網站的常見手法

傳統入侵網站的順序

1.蒐集資料 → 2.弱點探測 → 3.入侵系統 → 4.提升權限 → 5.竊取資料/竄改資料 → 6.植入後門

在弱點探測與入侵系統的過程中，SQL Injection是駭客第二步入侵點

1. 尋找檔案上傳(Upload Area)功能的漏洞
2. 再嘗試SQL Injection漏洞
3. 透過目錄遊走(Directory Traversal)，尋找檔案資訊漏洞
4. 瞄準設定檔，嘗試網站預設值漏洞
5. 最後嘗試其他Web弱點，如程式邏輯錯誤、Bug、緩衝區溢位(Buffer Overflow)弱點等

對SQL Injection再進化

新興自動化SQL Injection手法

自動化SQL Injection入侵程式

- 從資訊收集、弱點探測、侵入系統、提升權限到竊取資料或竄改資料，一氣呵成，程序和指令都可透過軟體全部自動化執行。
- 可自動依據不同的資料庫系統採取不同的入侵方式，以最近流行的P牌攻擊工具為例，可攻擊資料庫涵蓋Oracle、DB2、Informix、MySQL、SQL Server等。
- 通常是針對特定網站的目標式攻擊，較易留下一連串攻擊的Log記錄。

植入後門

不需要
蒐集網站資訊
與探測弱點

特定SQL Injection的無差別攻擊

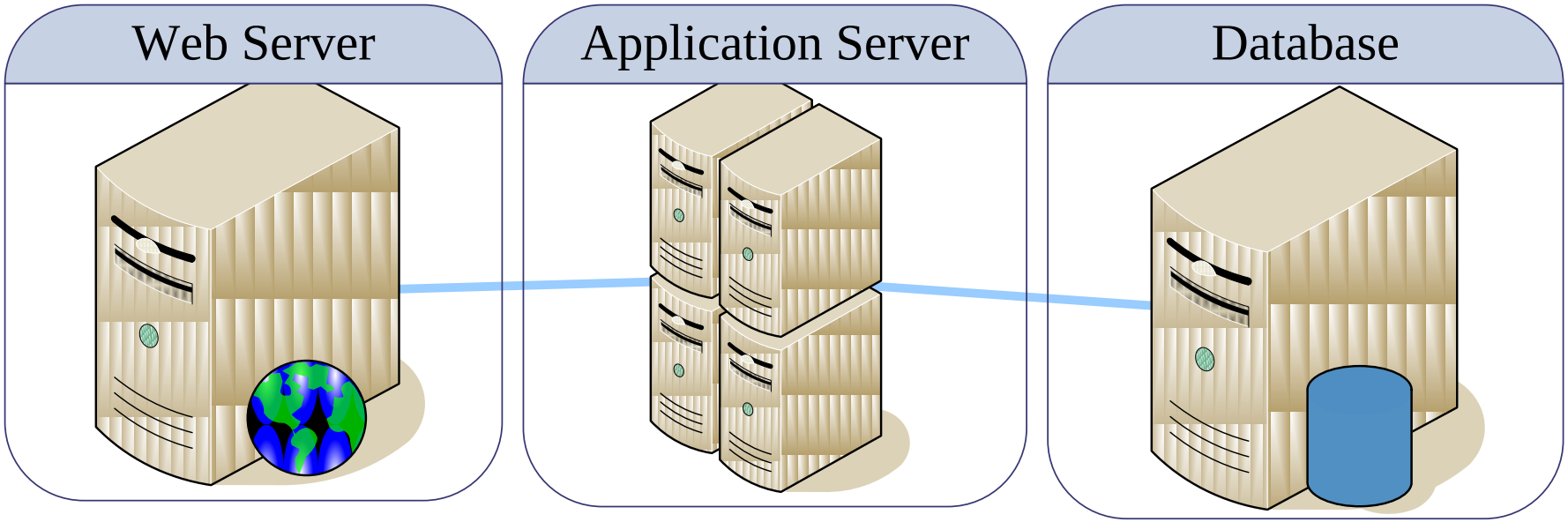
- 直接使用特定的SQL Injection指令，來攻擊任意網站，不論入侵成功與否，都立即離開，繼續攻擊下一個網站。
- 通常結合自動執行程式，快速攻擊大量網站。不需事先蒐集攻擊對象的資訊，屬於無差別式攻擊(盲打)。
- 入侵即離開，不會留下太多可追蹤的Log記錄。

入侵一次即離開，繼續攻擊下個網站

資料來源：OuTian、張裕敏，iThome整理，2008年9月

Targets being attacked

- Web Server – Apache, IIS, Netscape
- Application Server –Tomcat Servlet, PHP, ASP.NET
- Database – Oracle, MSSQL, DB2, Infomix, Sybase.



- *Security testing tools: Nmap, nessus, foundstone, acunetix, scuba, goolag and more*

Web App Hacking Methodologies

- Profile the Platform
- Survey the Application
- Attack Authentication Mechanism
- Attack Authorization Mechanism
- Attack Session Management
- Attack Input Validation
- Attack Client-side Security

Platform Profile Checklist

- Identify the server's role
- Determine the operating system and version
- Determine the operating system and application patch level
- Scan for open ports
- Record the web server type, patch level, and additional components
- Research known vulnerabilities.

Survey the Application

- The simplest way is click-through
- Documenting the application's structure in a well-ordered manner helps you track insecure pages
- Provides a necessary reference for piecing together an effective attack
- Use a matrix

Survey the Application

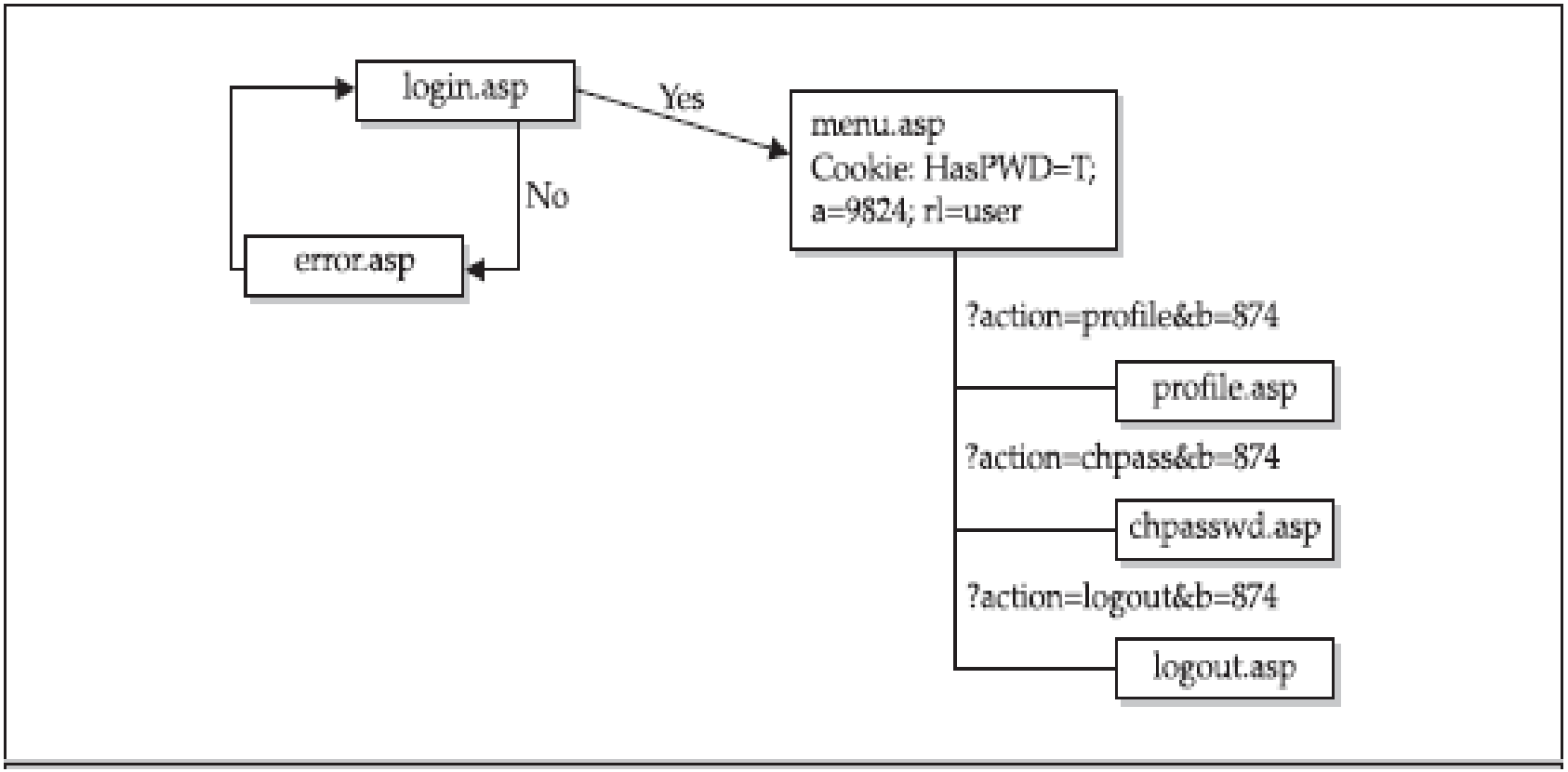
- Page Name (Static or Dynamic)
- Full Path to the Page
- Does the Page Require Authentication?
- Does the Page Require SSL?
- GET/POST Arguments
- Database Access Connection
- Other Optional Columns



Survey the Application

Page	Path	Auth?	SSL?	GET/POST	Comments
index.html	/	N	N		
login.asp	/login/	N	Y	POST	Main auth page password
company.html	/about/	N	N		Company info

Survey the Application



Surveying the Application

- Statically and dynamically generated pages
- Directory structure
- Helper files
- Java classes and applets
- HTML comments and content
- Forms
- Query strings
- Back-end connectivity

Directory Structure

- Parts visible through browsers
- Directories for obscurity : /admin, /adm
- Include files
- Log files
- old versions of the site
- backup directories
- data directories
- other directories that are not referenced in any HTML code

Forms

- Action file

(If you ever see a form call a script with a .sh extension (shell script), mark it. Shell scripts are notoriously insecure on Web servers)

- Methods
- Number of Parameters
- Login Information
  - username, password field
- Hidden fields
- sensitive information that the programmers explicitly did not want the browser to store
  - autocomplete field like

<input type=text name="val2" size="12" autocomplete=off>

Query Strings

- Collecting arguments is a complicated task
- User Identification /login?userid=24601
- Session Identification
/menu.asp?sid=89CD9A9347
- Database Queries
/dbsubmit.php?sTitle=Ms&iPhone=8675309
- Search Queries
/search?q=*&maxret=100&sort=true
- File Access /open.pl?template=simple

Using Google to Inspect an Application

- Google search operators
- Cached page

Case Study 1 for Attacking Authentication

Q: An application developer wishes to stop an attacker from performing brute-force attacks against the login function. Because the attacker may target multiple usernames, the developer decides to store the number of failed attempts in an encrypted cookie, blocking any request if the number of failed attempts exceeds five.

How can this defense be bypassed?

Case Study 2 for Attacking Authentication

Q: While testing a web application you log in using your credentials of joe and pass. During the login process, you see a request for the following URL appear in your intercepting proxy:
http://www.wahh-app.com/app?action=login&uname=joe&password=pass

What three vulnerabilities can you diagnose without probing any further?

Attack Authorization

- Why Access Control?
  - effects
    - illegitimate access to a harmless function
    - cannot be leveraged to escalate privileges any further
    - can quickly lead to a complete compromise of the application
  - sources of flaw
    - poor application unable to check unauthorized access
    - simple oversight may leave only one or two functions unprotected
    - defective assumptions about the way users will behave can leave the application undefended
  - ways to attack
    - look everywhere

Attack Authorization

- Vertical Privilege Escalation
  http://website/index.php?id=matt&isadmin=true&menu=full
  if the request succeeds, then the application is vulnerable to vertical privilege escalation

- Horizontal Privilege Escalation
  Otherwise, the application performs the authorization check based on the username, is vulnerable to horizontal and privilege escalation

- Arbitrary File Access (directory traversal)

Case Study 1 for Attacking Authorization

You log in to an application and are redirected to the following URL:
https://wahh-app.com/MyAccount.php?uid=1241126841

Hint:

- The application appears to be passing a user identifier to the MyAccount.php page.
- The only identifier you are aware of is your own.

Question:

- How can you test whether the application is vulnerable?

Attack Clide-side Security

- Why attack client-side browsers?

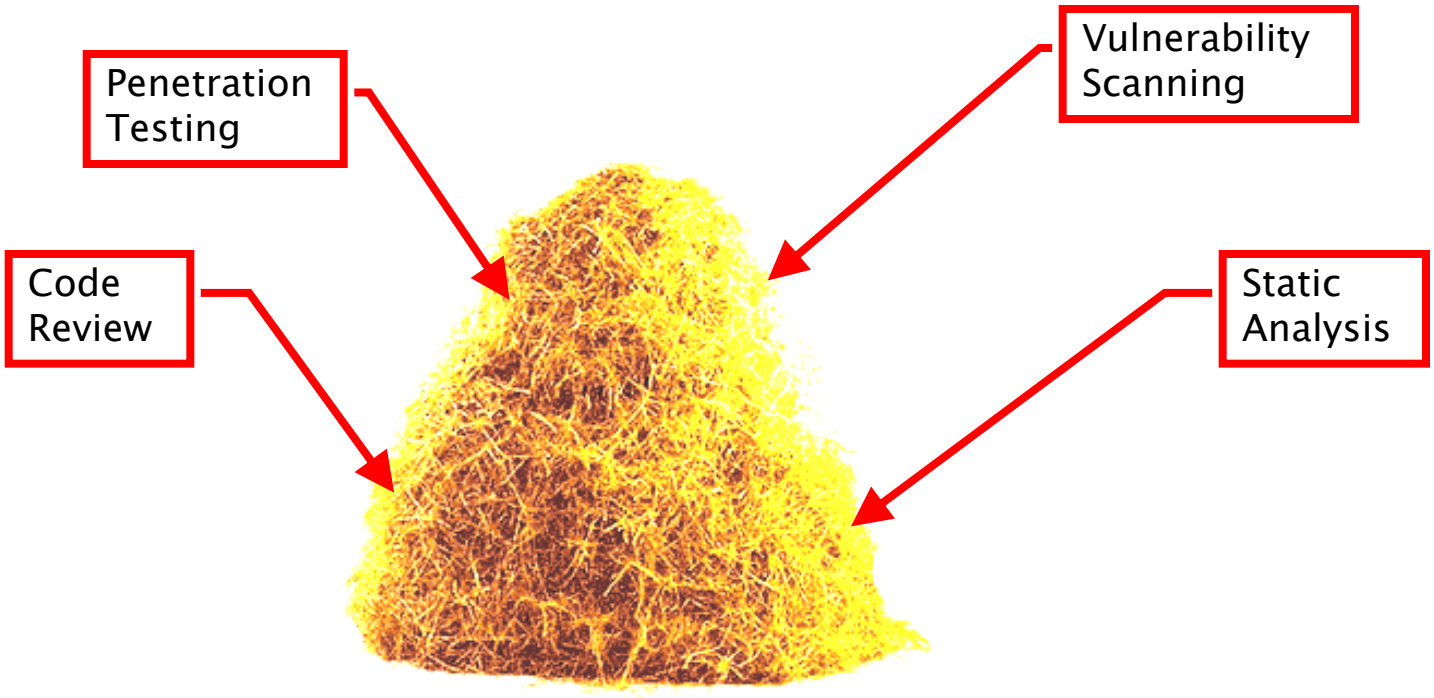
- Web browser security models
  - the same origin/domain policy (protocol+host+port)
  - the cookie security model

Attack Clide-side Security

- Countermeasures
  - Client Side
    - Never connect to Internet?
    - Use secure browsers (Firefox, Plug-in Noscript)
    - Disable Javascript and ActiveX capability
    - Keep up with security patches
    - Use Web Repudiation software
      - McAfee SiteAdvisor
      - Google Search

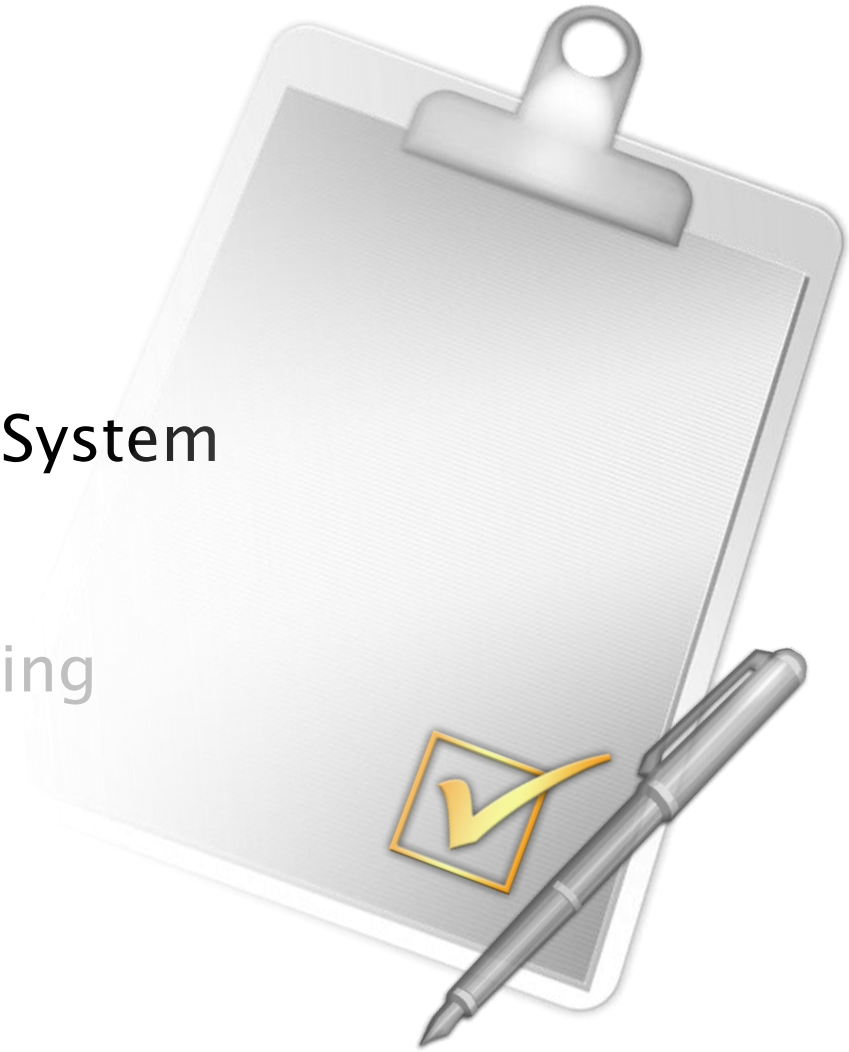
Attack Clide-side Security

- Countermeasures
  - Server Side
    - Harden your servers
    - Secure programming



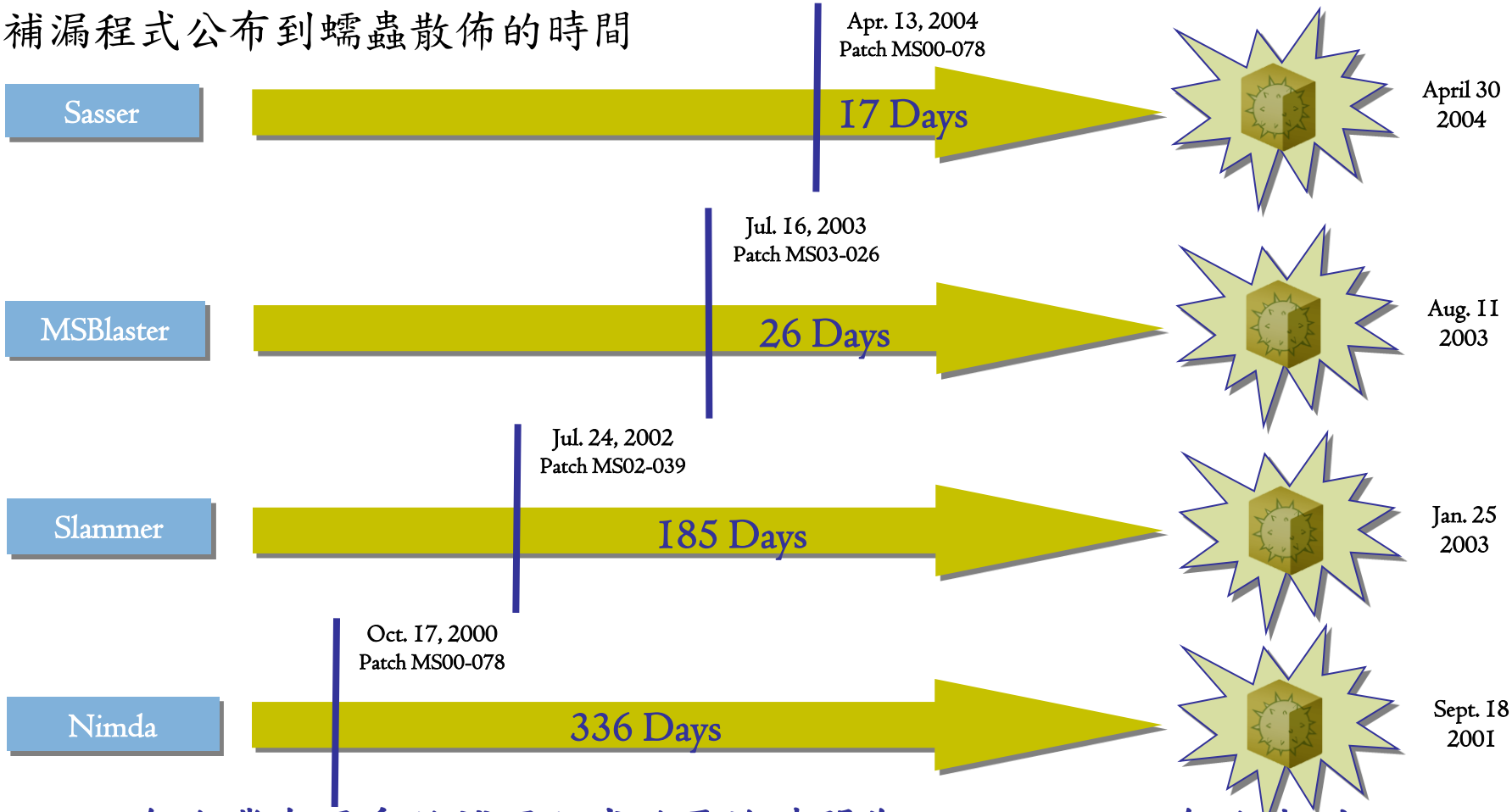
Agenda

- Session 1
  - 資訊安全三要素(CIA Triad)
  - Risk Assessment
  - Web Hacking Techniques
  - Vulnerability Scan
  - Risk-aware Management System
- Session 2
  - Data Security and Hardening



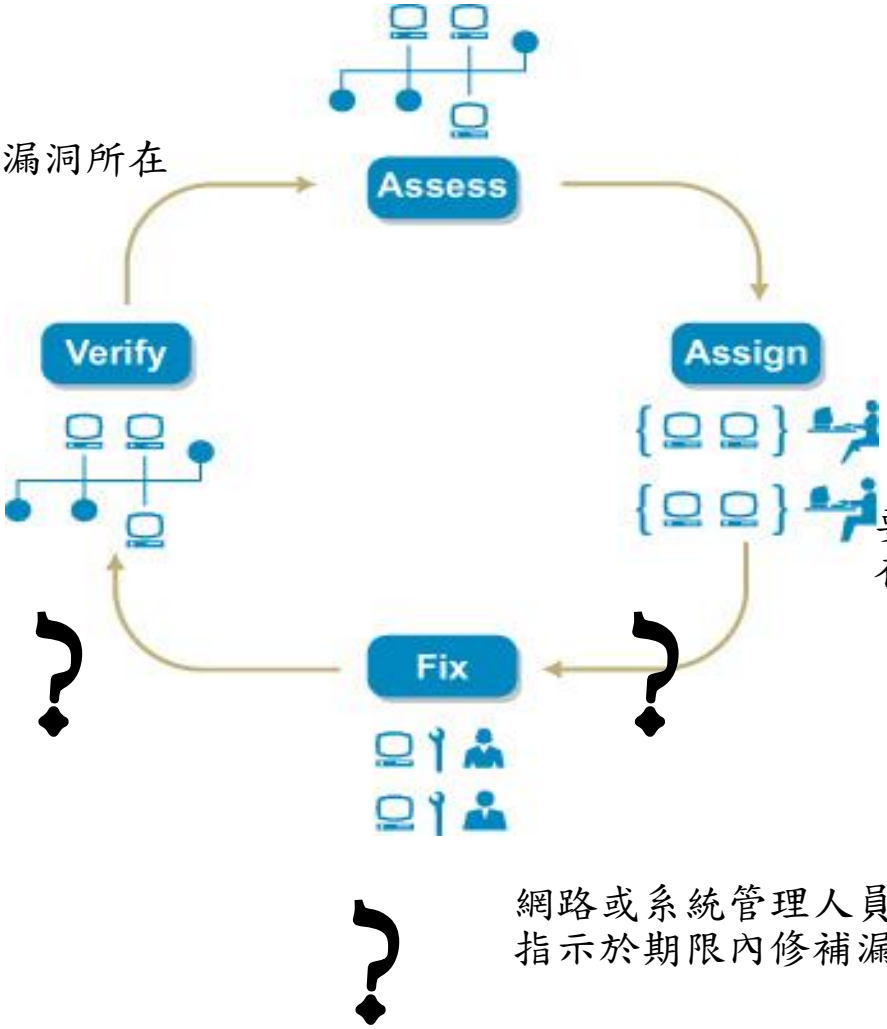
縮短的反應時間

從補漏程式公布到蠕蟲散佈的時間



2004 年企業套用系統補漏程式的平均時間為 30 天，2005 年進步到 21 天

到底管理流程中出了什麼問題?



為何要弱點掃瞄

- 雙面刃
  - 白帽駭客:幫助資訊安全人員了解到目前網路環境所曝露的漏洞，然後就可以利用修補或系統Hardening策略將漏洞所帶來的風險降到最低
  - 黑帽駭客:利用來發現你的網路環境的弱點的工具，一旦弱點被探測及列舉，駭客就可利用Internet上的一些exploit工具來對目標網路進行攻擊，進而獲取他想要的利益或成就感

弱點掃瞄的種類

- Network and System Level
  - Nessus
  - Foundstone
  - NMAP
  - MBSA
  - Superscan
  - 流光

- Web Application level
  - WebInsepect
  - Appscan
  - Acunetix
  - 網頁應用程式安全風險評鑑 – DREAD 模型

弱點掃瞄技術

- 弱點掃瞄通常分為3個階段：
  - Discovery Phase：發現目標主機或網路。使用之前所提的Port掃瞄技術
  - Fingerprint Phase：發現目標後進一步判斷作業系統類型、執行的服務以及版本等。使用之前所提的運行服務與作業系統辨識技術
  - Vulnerability Checking：根據前兩個phase及弱點檢測scripts所搜集到的訊息判斷目標主機是否存在弱點。針對Intrusive的弱點檢測例如buffer overflow或DoS, 有時必須將系統搞掛才可驗證系統是否存在此弱點

弱點掃瞄技術

- Port掃瞄技術
  - Port is a communication channel
  - Provide services to be accessed
  - Fingerprint target response through sending packets to the target
  - Scan technology includes TCP Connect, TCP SYN, UDP Scan, Stealth Scan, Xmas Scan and etc

- 弱點(Vulnerability)掃瞄技術
  - 弱點掃瞄技術是一種基於Internet遠端檢測目標網路或local主機安全弱點的技術。利用弱點掃瞄，系統管理員能夠發現各式網路設備及主機或伺服器上的各種TCP/IP port的status、開放的服務(如http、ftp或smtp等)、伺服器上的一些daemon的版本和這些daemon及軟體的安全漏洞
  - 可以採用Intrusive(侵入式)或Non-Intrusive(非侵入式)的方式來檢測系統是否有弱點存在。它利用了一系列的Scripts來模擬對系統進行攻擊的行為，並對結果進行分析

Port掃瞄技術

- TCP Connect Scan
  - 完成Three-way handshaking
  - 由掃瞄主機發出connect開始，如果port開放，被掃瞄主機發出SYN/ACK連接請求，則連接將建立成功，表明目標port處於Listen狀態；否則表示port關閉。如果目標port處於關閉狀態，則目標主機會向掃瞄主機發送RST/ACK的response。
  - NMAP -sT -O target

Port掃瞄技術

- TCP Connect Scan範例

```
C:\Program Files\Nmap>nmap -sT -PT -PI -T 3 172.18.2.32
Starting Nmap 4.20 ( http://insecure.org ) at 2007-09-14 11:48
Interesting ports on 172.18.2.32:
Not shown: 1686 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIS
3306/tcp  open  mysql
5800/tcp  open  vnc-http
5900/tcp  open  vnc
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
Nmap finished: 1 IP address (1 host up) scanned in 84.942 seconds
```

Port掃瞄技術

- TCP SYN Scan
  - 沒有完成Three-way handshaking
  - 由掃瞄主機發出connect開始，掃瞄主機在收到目標主機的SYN/ACK封包後不再回覆自己的ACK封包
  - TCP三次交握並沒有完成，正常的TCP連接無法建立，因此這個掃瞄訊息不會被記錄到Log。這種掃瞄技術一般不會在目標主機上留下記錄。所以TCP SYN掃瞄的優點是比TCP Connect掃瞄更隱蔽
  - 但缺點是在大部分的作業系統下，掃瞄主機需要自己建立這種適用於此類掃瞄的IP封包，但通常可以自己建構的SYN封包需要root權限
  - NMAP -sS -PT -PI －T 3 target

Port掃瞄技術

- Stealth Scan
  - 現在很多防火牆或路由器會對指定的port進行監視，將對這些port的連接請求全部進行記錄。這樣即使是使用TCP SYN掃瞄仍然會被防火牆或入侵偵測系統記錄到Log中，所以偷取掃瞄因此而生
  - 但現在的入侵偵測系統應該都可以發現偷取掃瞄
  - 雖然說偷取掃瞄可以躲過很多防火牆或路由器的監視，但這種掃瞄的缺點是掃瞄結果的不可靠性會增加，而且掃瞄主機也需要自己構建IP封包
  - 常見的偷取掃瞄有TCP FIN掃瞄、TCP ACK掃瞄、NULL掃瞄、XMAS掃瞄及SYN ACK掃瞄
  - NMAP -sF(-sX, -sN) -PT -PI target

Port掃瞄技術

- TCP FIN 、XMAS 、NULL Scan
  - 關閉的port會對你發送的探測封包返回一個RST，而打開的port則對其忽略不理。所以FIN掃瞄使用FIN封包作為檢測、Xmas tree使用FIN，URG，PUSH標記、Null掃瞄則不用任何標記
  - 不幸的是微軟以他們一貫的風格不理睬這一標準，所以這一掃瞄在WINDOWS下平台大都不能工作。從積極方面來講，這其實也是一個很好的區分兩種平台的辦法--如果這次掃瞄發現了打開的port，那你就能明白這台機器不是WINDOWS。如果-sF,-sX,-sN的掃瞄顯示所有port都是關閉的，但一個SYN(-sS)掃瞄卻顯示有打開port，那你就能大致推斷它是WINDOWS平台

Port掃瞄技術

- UDP Port Scan
  - 掃瞄主機發送UDP封包給目標主機的UDP port，等待目標port的ICMP Unreachable的ICMP訊息。若time out也不能收到port的ICMP Unreachable的ICMP訊息，則表明目標port可能處於listen狀態。若這個ICMP訊息及時收到，則表明目標port處於關閉的狀態
  - 這種方法十分不可靠，一方面UDP協議本身是不可靠，從local端發送的UDP封包可能在中途丟掉，再者，目標網路的防火牆設備也可能禁止任何ICMP封包通過，這樣，會讓掃瞄主機以為目標主機上開放了很多UDP ports，事實上這是防火牆造成的假象

Port掃瞄技術

- 運行服務的Fingerprint
  - 利用所掃瞄到目標主機的port號
  - 發送符合該協定的命令封包再比對回應結果, 例如SMTP HELLO
  - 比對系統的banner, 例如IIS Web Server的HTTP Response
  - 其他辨識方法, 例如察看Tomcat所回應的JSESSION等
- 作業系統的Fingerprint
  - 找出作業系統間不同的TCP Protocol Stack特性，就可以區分作業系統的類型或版本
  - NMAP中-O的選項就是告訴NMAP要對目標主機進行作業系統辨識, 例如: NMAP -sT -PT -PI -O target

Port掃瞄技術

TCP/IP fingerprint:

OS:SCAN(V=4.20%D=9/14%OT=80%CT=1%CU=38520%PV=Y%DS=3%G=Y%TM=46EA0C1E%P=i686-

OS:pc-windows-windows)SEQ(SP=106%GCD=1%ISR=10C%II=I%TS=0)OPS(O1=M5B4NW0NNT0

OS:0NNS%O2=M5B4NW0NNT00NNS%O3=M5B4NW0NNT00%O4=M5B4NW0NNT00NNS%O5=M5B4NW0NNT

OS:00NNS%O6=M5B4NNT00NNS)WIN(W1=4000%W2=4000%W3=4000%W4=4000%W5=4000%W6=400

OS:0)ECN(R=Y%DF=N%T=80%W=4000%O=M5B4NW0NNS%CC=N%Q=)T1(R=Y%DF=N%T=80%S=O%A=S

OS:+%F=AS%RD=0%Q=)T2(R=Y%DF=N%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=N%

OS:T=80%W=4000%S=O%A=S+%F=AS%O=M5B4NW0NNT00NNS%RD=0%Q=)T4(R=Y%DF=N%T=80%W=0

OS:%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=N%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6

OS:(R=Y%DF=N%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=N%T=80%W=0%S=Z%A=S+%

OS:F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%TOS=0%IPL=B0%UN=0%RIPL=G%RID=G%RIPCK=G%

OS:RUCK=G%RUD=G)IE(R=Y%DFI=S%T=80%TOSI=Z%CD=Z%SI=

Port掃瞄技術

- 作業系統的Fingerprint
  - 常用的TCP Protocol Stack Fingerprint技術有以下幾種:
    - FIN探測 -- 送一個FIN封包給一個打開的port並等待回應。正確的RFC行為是不會回應，但是例如Windows, CISCO, HP/UX, 和IRIX卻會回應一個FIN/ACK
    - BOGUS 標記探測 -- 設置一個未定義的TCP標記在SYN封包的TCP標頭裡。Linux機器到2.0.35之前的Kernel會在回應封包中保持這個標記。而對其他作業系統卻不做任何回應
    - TCP ISN取樣 -- 這種方法是找出當回應一個連接請求時，由TCP 實作中所選擇的初始化序列的模型

Port掃瞄技術

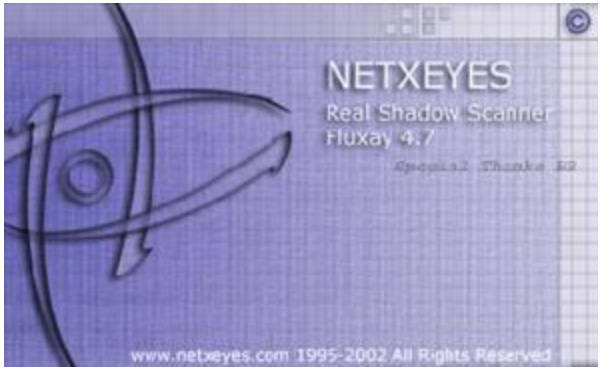
- TCP初始化窗口 -- 檢查返回封包的窗口(windows size)大小。有些作業系統會使用一些非常獨特的值，例如AIX是0x3F25，NT和BSD是0x402E

- ACK值 --不同實作中ACK值的實作也不同。例如，如果你送了一個FIN|PSH|URG 到一個關閉的TCP port。大多數實作會設置ACK 為初始序列數，而Windows會送出序列數加1 。若送一個SYN|FIN|URG|PSH到一個打開的端口，Windows的回應會非常不穩定

- ICMP錯誤訊息抑制 -- 一些遵循RFC 1812的作業系統會限制各種錯誤信息的發送率。例如，Linux限制ICMP unreachable訊息每4 秒鐘80個，通過對某選定的port發送一串封包並計算收到的unreachable訊息，統計出一段時間內收到的ICMP unreachable訊息，再與作業系統的預計值做比較

弱點掃瞄工具

- 基於弱點資料庫的弱點掃瞄，它大致上包括Database弱點掃瞄、CGI弱點掃瞄、DNS弱點掃瞄、POP3弱點掃瞄、SMTP弱點掃瞄、FTP弱點掃瞄、RPC弱點掃瞄、DOS弱點掃瞄、SSH弱點掃瞄、HTTP弱點掃瞄等。例如Nessus, Foundscan, 中華龍網, Reti及中國大陸著名駭客工具”流光”等



弱點掃瞄工具

- 漏洞掃瞄還包括使用Plug-in(如Nessus可使用Nikto及其他password cracking plug-in)進行模擬攻擊偵測(Intrusive及Non-Intrusive)，進而實際測試出目標主機的弱點資訊。有一些弱點資訊可能需要有privilege權限才能得到比較準確的結果

- 弱點掃瞄的關鍵其實就在於其核心的弱點資料庫，如同入侵偵測系統及防毒軟體的偵測方式，是採用比對match的方式(對弱點掃瞄來說是比對回應及Banner等)，即根據資訊安全專家對網路系統及主機的各種安全弱點輔以一些real case的攻擊案例的分析以及系統管理員對網路及系統設定的knowledge base及best of Practice，就可以形成我們所熟知的弱點資料庫(Vulnerability Database)，最後再由弱點掃瞄軟體進行弱點掃瞄及弱點結果match的工作

弱點掃瞄工具

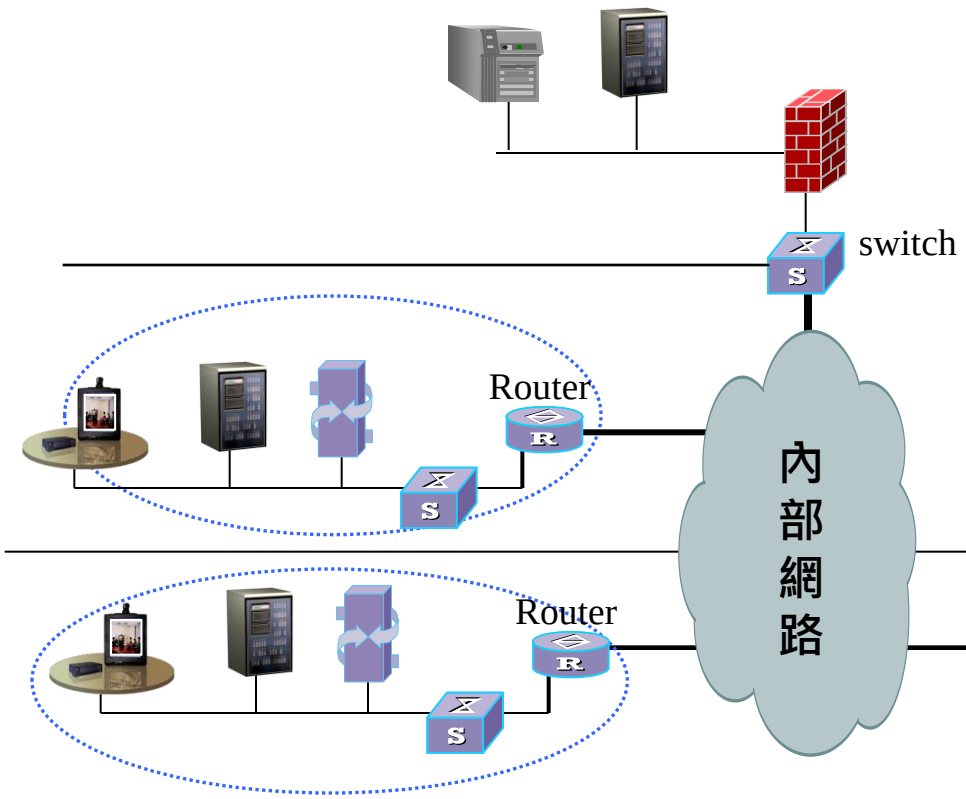
- Plug-in是由Scripts編寫的sub procedure，掃瞄軟體可以通過呼叫它來執行弱點掃瞄，檢測出系統中存在的一個或多個弱點。增加新的plug-in就可以使弱點掃瞄軟體增加新的弱點檢測功能，進而掃瞄出更多的弱點

- 以FoundScan為例，FoundScan使用統一的FSL(Foundstone Script Language)來撰寫plug-in，只要你有coding及具弱點相關能力，你自己就可以利用FSL自行設計Scripts編寫的plug-in來擴充弱點掃瞄檢測的功能。而專用Scripts的使用也簡化了編寫新plug-in的程式撰寫工作，使弱點掃瞄軟體具有很強的擴展性。Nessus亦有專用的Script語法(NASL)來讓它的開發者或使用者自己使用此Script來編寫適合本身環境使用的plug-in

弱點資料庫

- Connection with vendors
- Microsoft bulletin (Patch Tuesday)
  http://www.microsoft.com/technet/security/bulletin/notify.mspx
  - E-mail notification
  - RSS feed
  - Windows Live Alerts
- NTBugTraq.com
- mitre.org
- www.kb.cert.org
- www.dragonsoft.com
- www.icat.nist.org

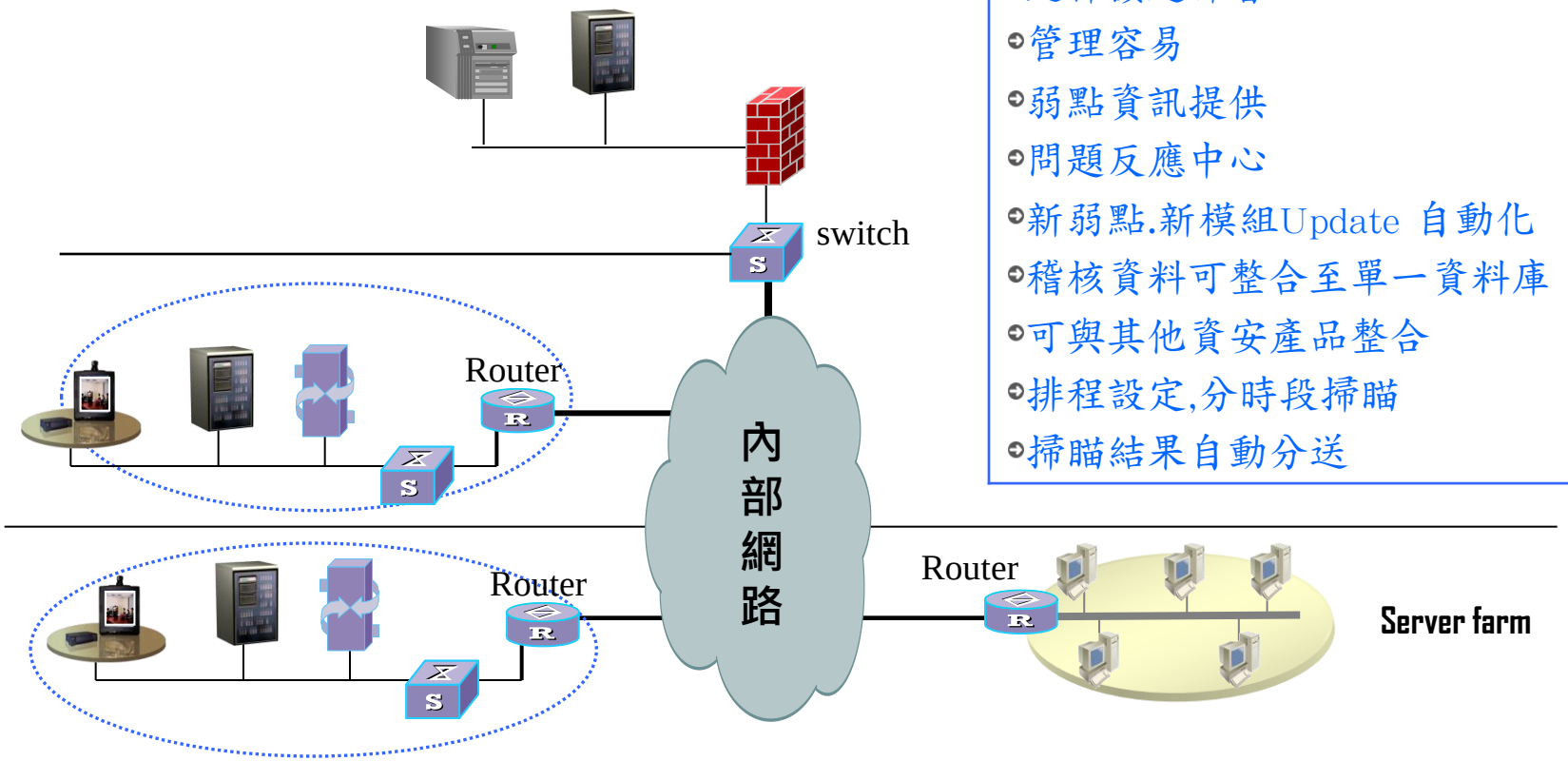
VA部署設計



需求分析: 1

- 徹底劃分各網路區塊及資產分級
- 簡化管理流程Ticket自動化
- 模擬各項資安狀況及Workaround
- 落實安全設備及內部稽核,檢測的多樣性
- 大幅減少支援成本
- 機動稽核各項端點(VPN, Wireless..),落實公司安全政策
- 弱點趨勢及差異分析,法規遵從,詳實的報表

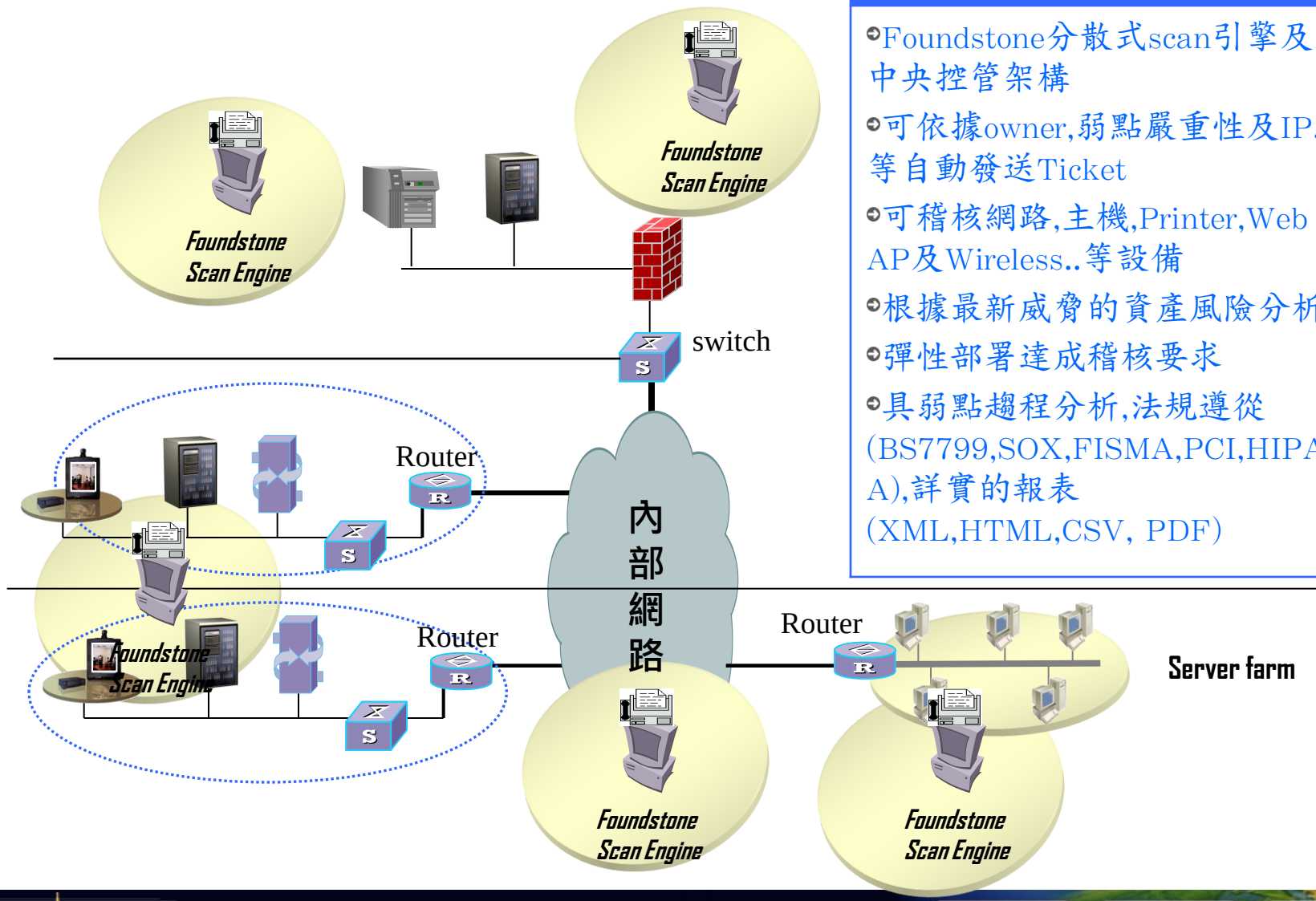
VA部署設計



需求分析: 2

- 介面操作簡單
- 報告清楚
- 符合歸範
- 延伸擴建部署
- 管理容易
- 弱點資訊提供
- 問題反應中心
- 新弱點.新模組Update 自動化
- 稽核資料可整合至單一資料庫
- 可與其他資安產品整合
- 排程設定,分時段掃瞄
- 掃瞄結果自動分送

VA部署設計

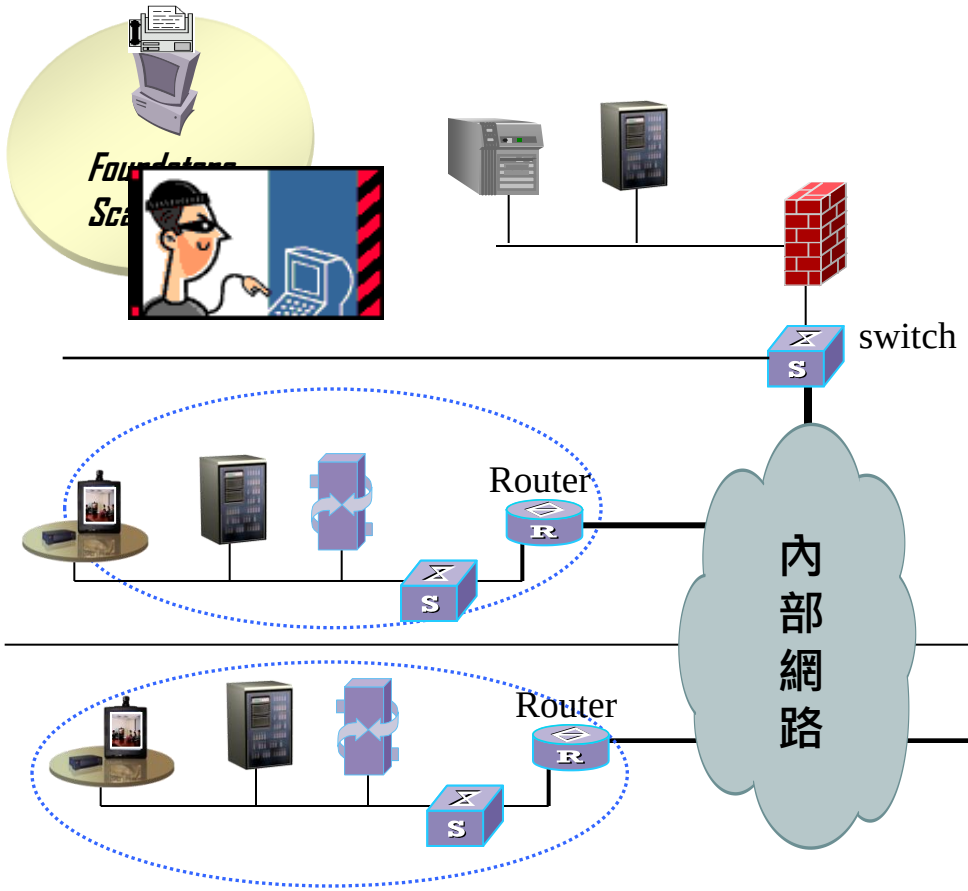


產品解決方案

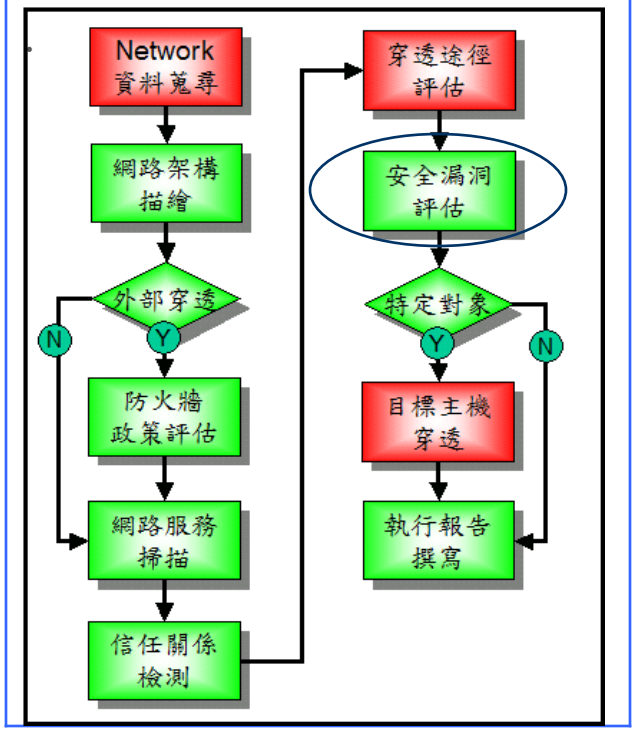
- Foundstone分散式scan引擎及中央控管架構
- 可依據owner,弱點嚴重性及IP..等自動發送Ticket
- 可稽核網路,主機,Printer,Web AP及Wireless..等設備
- 根據最新威脅的資產風險分析
- 彈性部署達成稽核要求
- 具弱點趨程分析,法規遵從(BS7799,SOX,FISMA,PCI,HIPAA),詳實的報表(XML,HTML,CSV, PDF)

VA部署設計

進行遠端滲透測試，採取駭客攻擊模式，遠端偵測貴單位網路系統安全強度；也經由內部網路進行滲透測試，繞過防火牆之過濾與阻擋，蒐集必要之安全資訊，彰顯測試效益及弱點發掘



功能設計: 模擬駭客



RPC攻擊案例

: SPARC Solaris remote root exploit for /usr/sbin/sadmind

```
solaris [/export/home/kuang/demo] -kuang- ./sadmindex-brute-lux 2 192.168.129.21

Alright... sit back and relax while this program brute forces the sp.

%esp 0x08041798 offset 572 --> return address 0x080419d4 [0+536]
clnt_call: RPC: Timed out
now check if exploit worked; RPC failure was expected
%esp 0x0804179c offset 572 --> return address 0x080419d8 [0+536]
clnt_call: RPC: Timed out
now check if exploit worked; RPC failure was expected
%esp 0x08041794 offset 572 --> return address 0x080419d0 [0+536]
clnt_call: RPC: Timed out
now check if exploit worked; RPC failure was expected
%esp 0x080417a0 offset 572 --> return address 0x080419dc [0+536]
clnt_call: RPC: Timed out
now check if exploit worked; RPC failure was expected
%esp 0x08041790 offset 572 --> return address 0x080419cc [0+536]
clnt_call: RPC: Timed out
now check if exploit worked; RPC failure was expected

Now telnet to 192.168.129.21, on port 1524... be careful
solaris [/export/home/kuang/demo] -kuang- telnet 192.168.129.21 1524
Trying 192.168.129.21...
Connected to 192.168.129.21.
Escape character is '^]'.
# id;
uid=0(root) gid=0(root)
^M: not found
# _
```

執行入侵

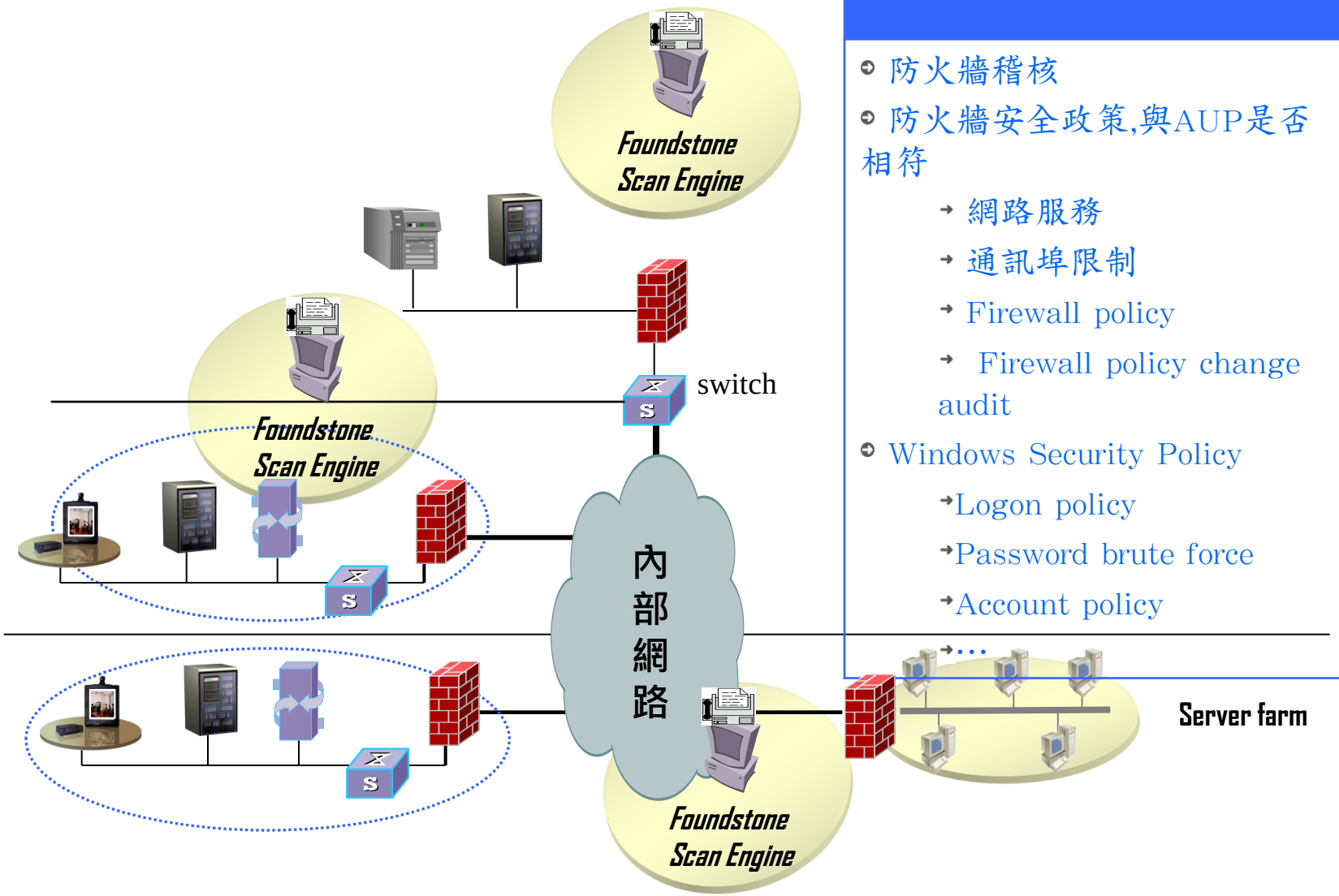
入侵過程

入侵完成(port number可更改)

執行telnet

取得root權限

VA部署設計



功能設計: Firewall and Security Policy Audit

- 防火牆稽核
- 防火牆安全政策,與AUP是否相符
  - 網路服務
  - 通訊埠限制
  - Firewall policy
  - Firewall policy change audit
- Windows Security Policy
  - Logon policy
  - Password brute force
  - Account policy
  - ...

法規要求

功能設計: Regulatory Compliance

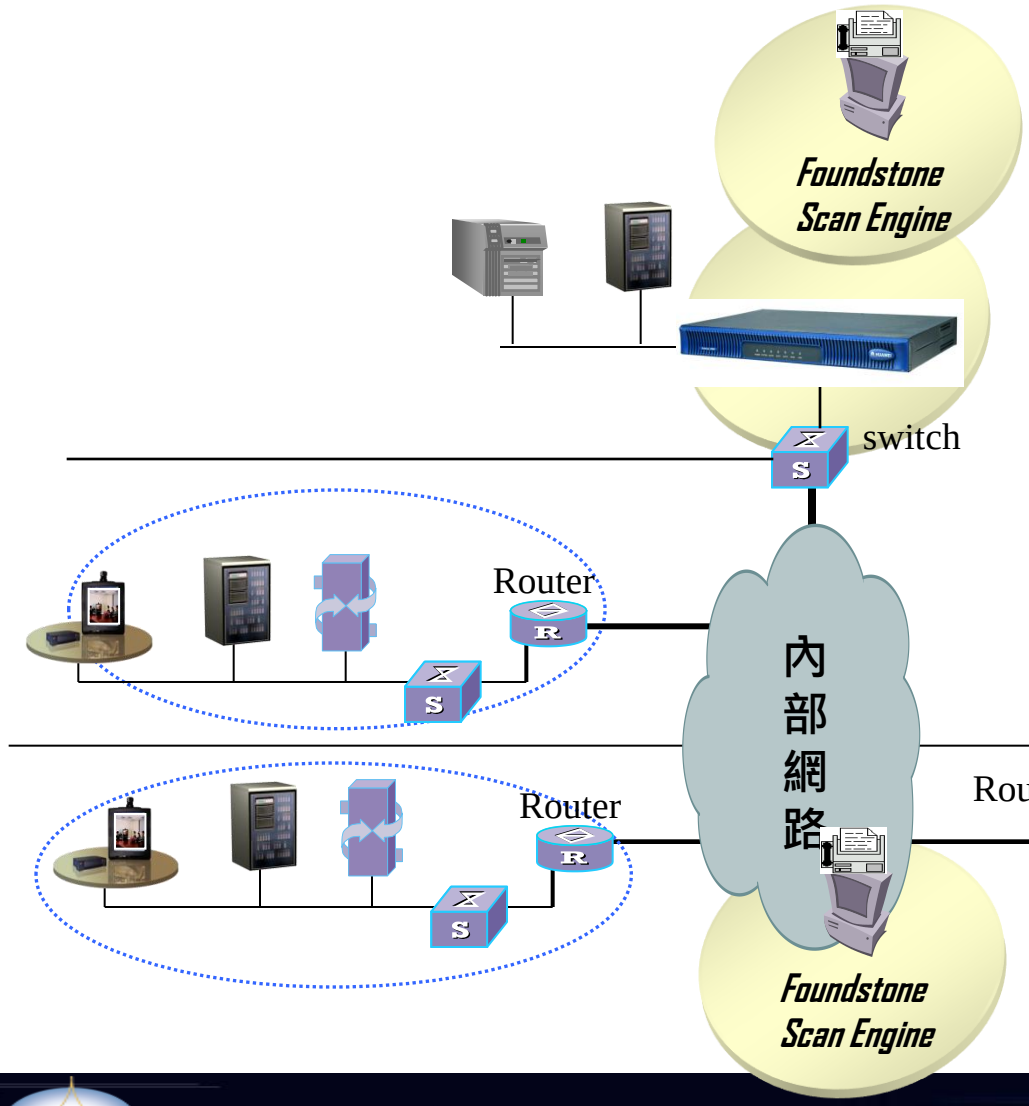
ISO 27001

12.6.1 Control of technical vulnerabilities Control- Timely information about technical vulnerabilities of information systems being used should be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.
g) patches should be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, other controls should be considered, such as 1) turning off services or capabilities related to the vulnerability; 2) adapting or adding access controls, e.g. firewalls, at network borders; 3) increased monitoring to detect or prevent actual attacks; 4) raising awareness of the vulnerability;

Risk Mgt

workaround

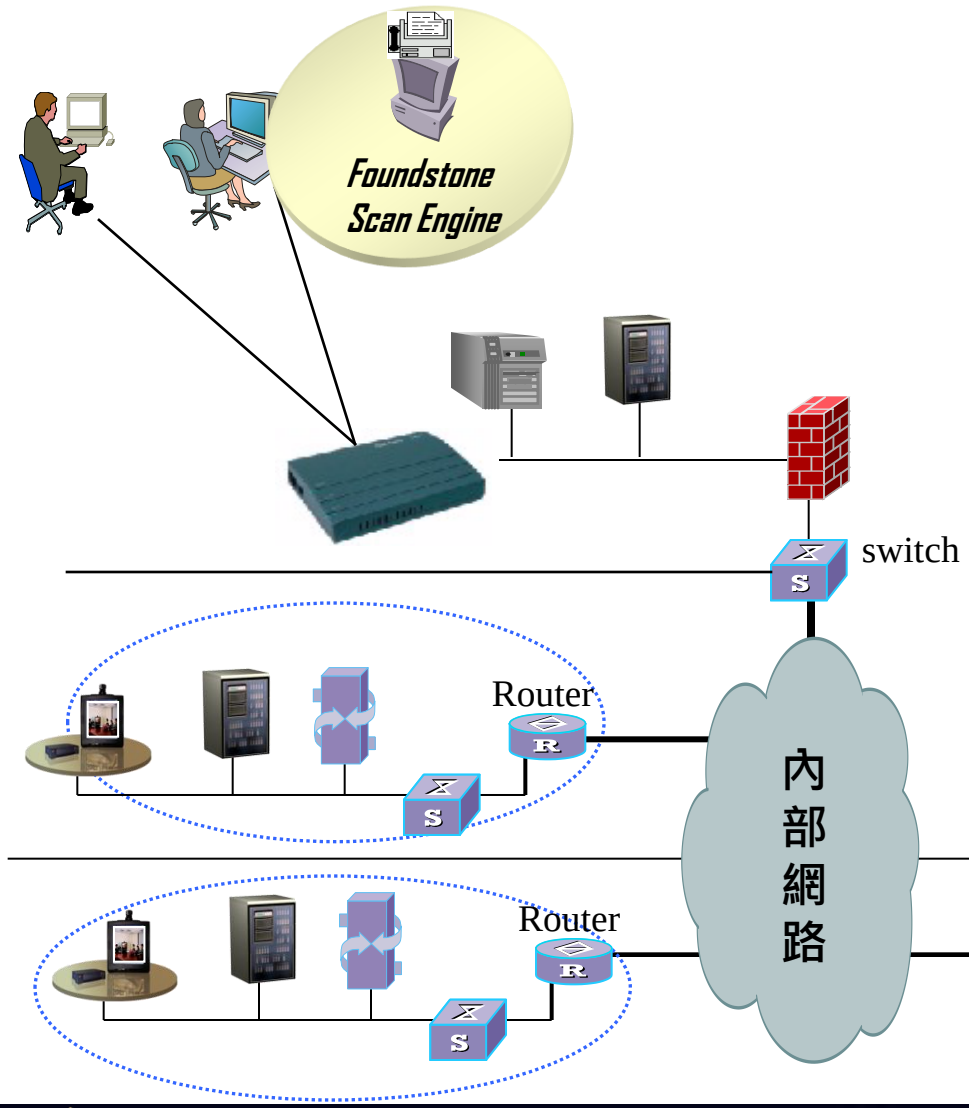
VA部署設計



功能設計: 與IPS協同合作

- IDS若測到某一IP的攻擊訊息則檢查該IP是否存在相關弱點.並透過整合過之資料庫進行其他類似之比對
- 如果被攻擊IP..經快速比對.確認是可承受.則只需紀錄存證,反之,若可被攻擊成功,除紀錄外,尚需第一時間通知管理者,啟動資安事件通報程序及由資安事件處理小組接手

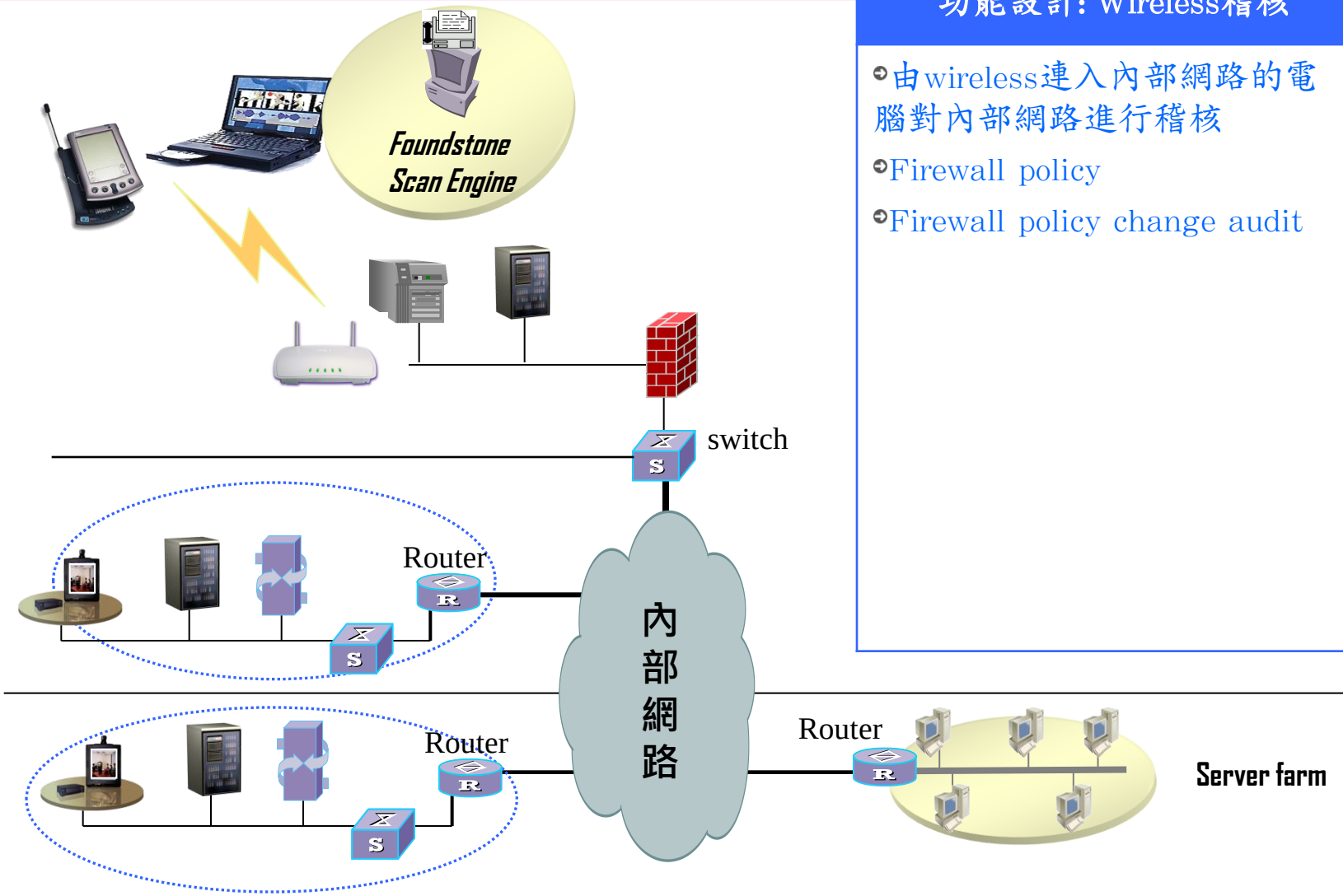
VA部署設計



功能設計: VPN稽核

- 由連入VPN的電腦對內部網路進 行稽核
- Firewall policy
- Firewall policy change audit

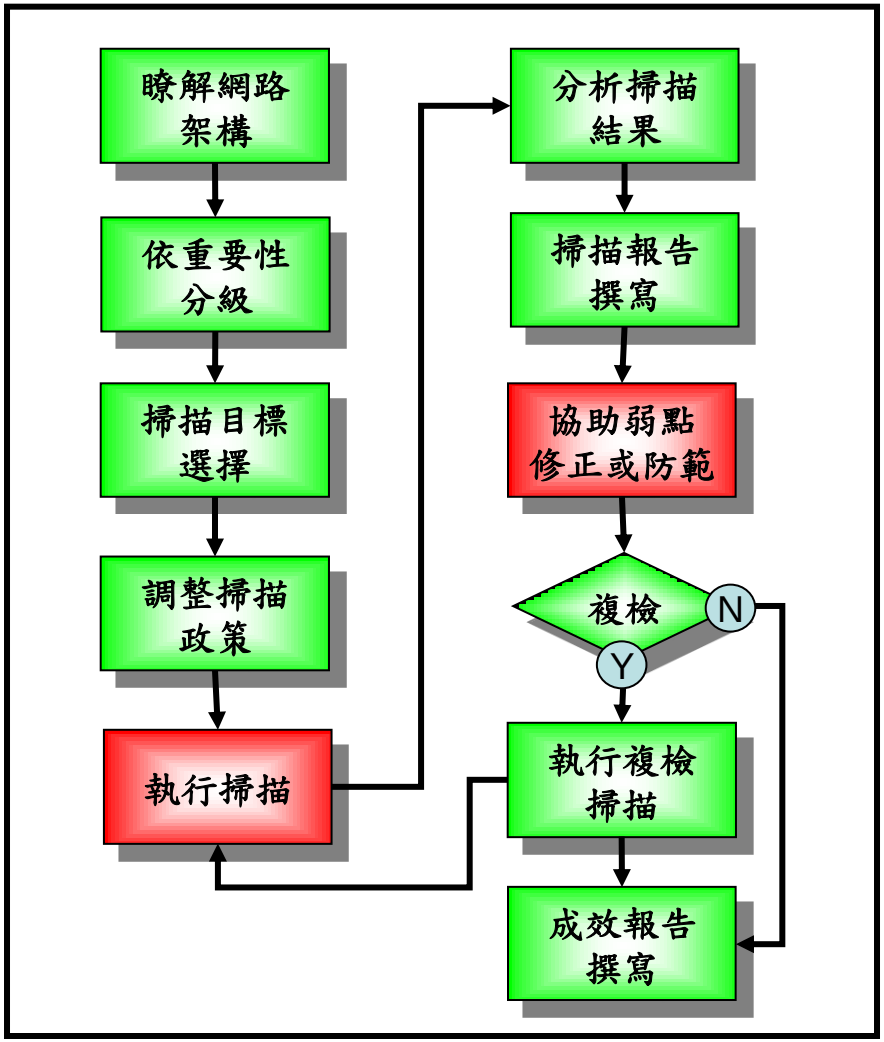
VA部署設計



功能設計: Wireless稽核

- 由wireless連入內部網路的電腦對內部網路進行稽核
- Firewall policy
- Firewall policy change audit

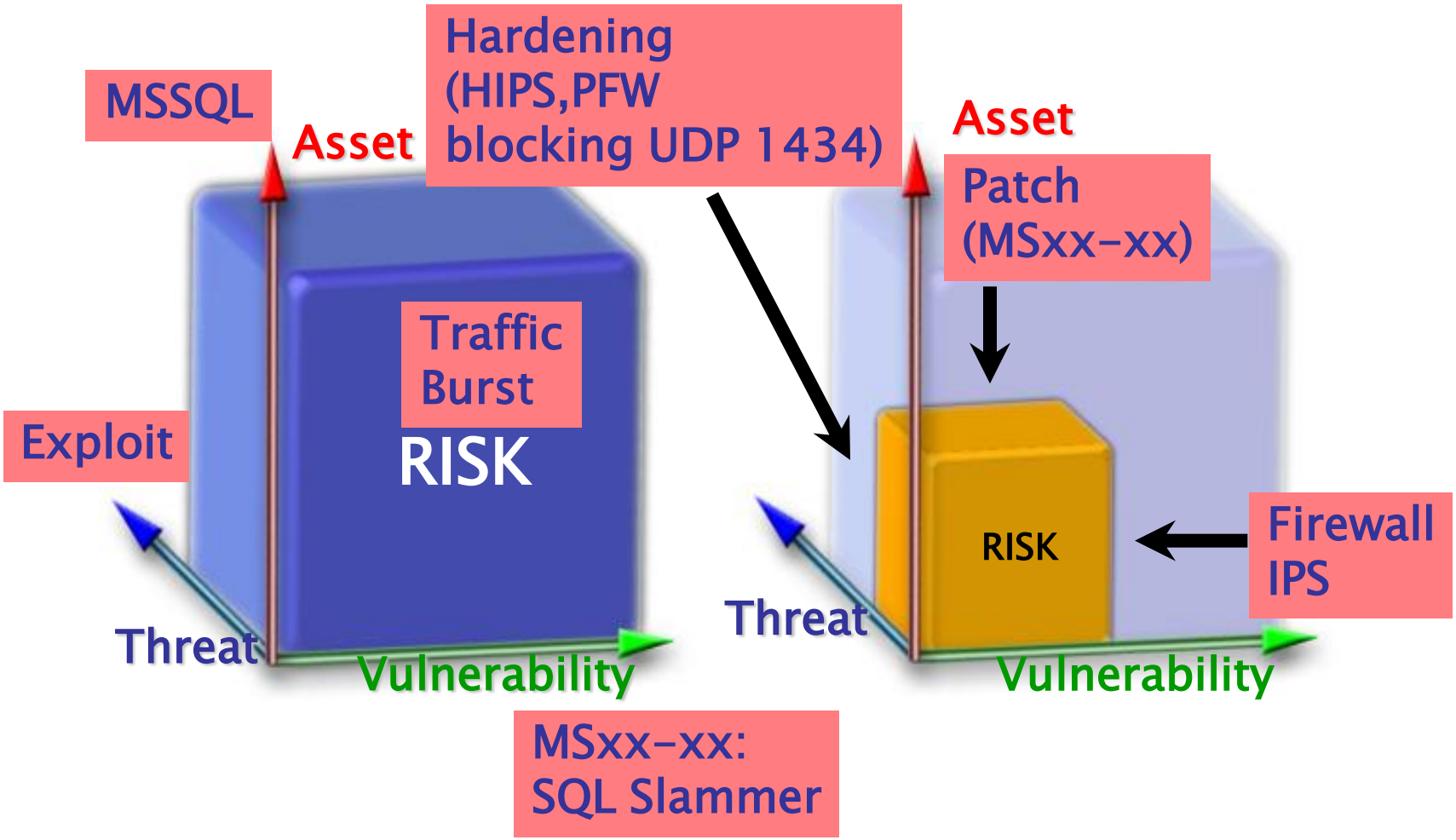
弱點掃瞄標準作業程序


瞭解網路架構
依重要性分級
掃描目標選擇
調整掃描政策
執行掃描
分析掃描結果
掃描報告撰寫
協助弱點修正或防範
複檢
N
Y
執行複檢掃描
成效報告撰寫

風險等級(Risk Level)分類

Foundstone是根據Foundstone Best Practice及弱點本身能被利用的難易程度(Simplicity), 攻擊者利用此弱點進行攻擊的技術水準(Popularity)及對此系統所造成的衝擊(Impact)來計算弱點所屬風險等級
高風險(High Risk) 弱點若被利用可能讓不具經驗的攻擊者直接取得管理者權限,導致系統中斷,拒絕服務攻擊,執行命令,敏感資訊的揭露等.
中風險(Medium Risk) 弱點若被利用可能讓稍有經驗的攻擊者直接取得非管理者層級權限,但攻擊者可利用進一步的hacking技術來取得管理者權限.
低風險(Low Risk) 弱點若被利用可能讓具有經驗的攻擊者間接取得某種等級的使用者存取權.
一般資訊(Information Risk) 此類弱點僅揭露不具價值的資訊,或是根本無法利用來進行攻擊

弱點及修補分類

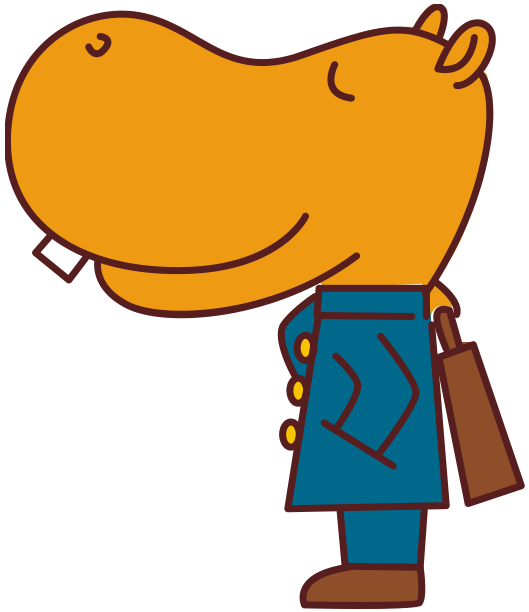

MSSQL
Asset
Hardening
(HIPS,PFW
blocking UDP 1434)
Traffic
Burst
RISK
Exploit
Threat
Vulnerability
MSxx-xx:
SQL Slammer
Asset
Patch
(MSxx-xx)
RISK
Firewall
IPS
Threat
Vulnerability

弱點及修補分類

- 軟體的bug
  - 尋求協力廠商的補丁進行修補
  - 作業系統補丁
  - 套件的補丁
  - Workarounds
    - 防毒軟體 (緩衝區溢位保護, HIPS等)
    - 防火牆, IPS, SELinux
    - 移除不使用的軟體
- 不安全的設定
  - 系統管理員強化安全的設定
  - 參考Foundstone的弱點資料庫
  - 參考Security Checklist (Windows, Linux, MSSQL, Oracle等)
  - 使用Tools (如Basetille, MBSA, MSSQL BPA, Scuba等)
- 不需要的服務
  - 關閉或移除

弱點掃瞄報表

- Nessus
- Nessus Report Demo
- Foundstone風險管理系統介紹
- Foundstone Report 分析



弱點修補管理5大招

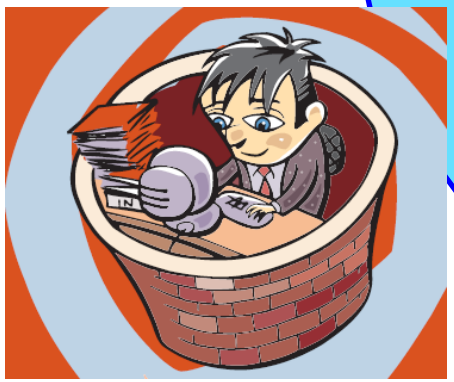
Discovery & Assessment

Security Officer:

- Be informed (Patch Tuesday) and assess potential vulnerabilities
- Identify those available for your systems
- Identify risk and priority level
- Whether to use automated patch system or partners
- Alert users if required

弱點修補管理5大招

Preparation & Testing



Administrators:

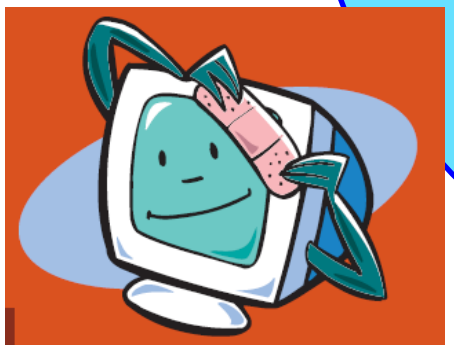
- Patching should be written to your security policy and stick to your change mgt plan
- Define patching workflow for patch testing, rollout and rollback
- Use standardized and repeatable procedure for non-critical patches and based on a regular cycle
- Use conscious and specially crafted procedures for critical patch

弱點修補管理5大招

Deployment

Technicians:

- Dangerous patch and dangerous exploit is a real Catch-22
- Do nothing
  - If an exploit targets something you don't use, there is no need to patch
- Implement a workaround
  - Multi-tiers and in-depth defense such as firewall, IPS and other security measures can reduce the pressure to rush out the patches.
- Patch & Harden
  - Mimic the production environment as possible
  - Use VM to test



弱點修補管理5大招

Validate & Report

Security Officer and Administrators:

- Acceptance Test
  - Patch is working (Re-scan, Pen Test)
  - Operation is not disrupted
- Status Report
  - How many systems got fixed
- Repeat
  - If you got right, back to the beginning

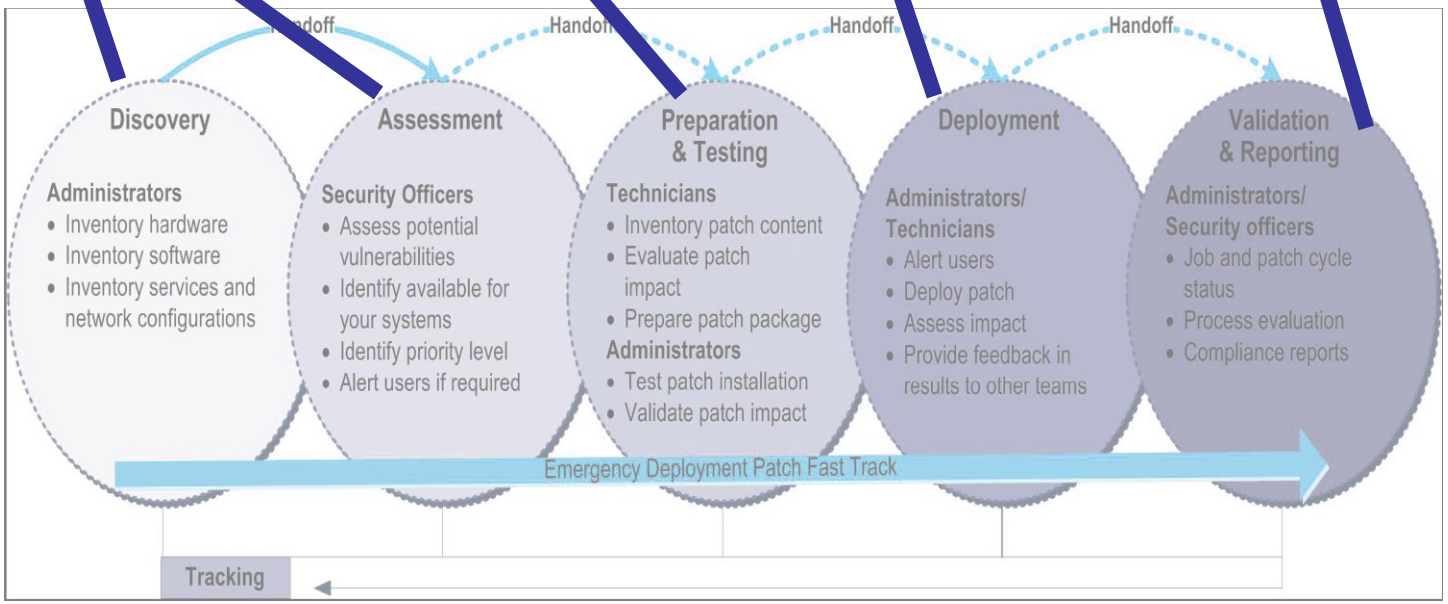
弱點管理策略

資產清冊
弱點掃瞄
弱點公告

備份,測試機
WSUS

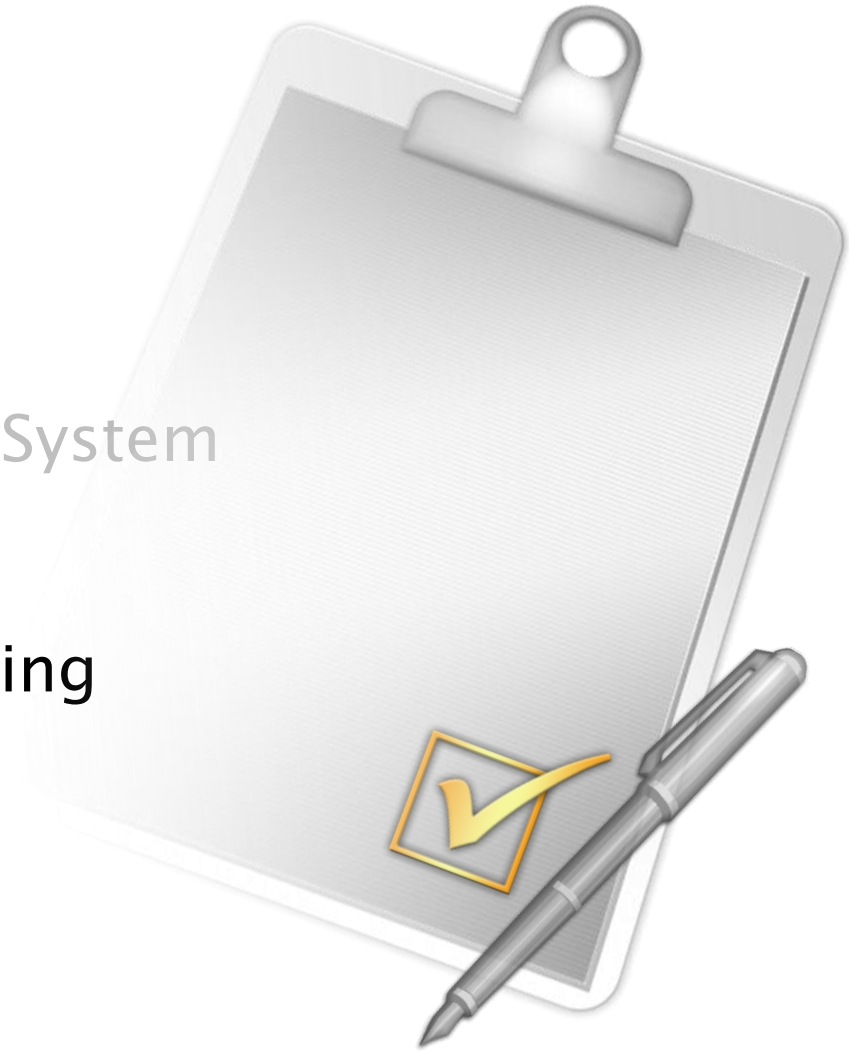
WSUS,Rollback

複掃,滲透測試
記錄及報告



Agenda

- Session 1
  - 資訊安全三要素(CIA Triad)
  - Risk Assessment
  - Web Hacking Techniques
  - Vulnerability Scan
  - Risk-aware Management System
- Session 2
  - Data Security and Hardening

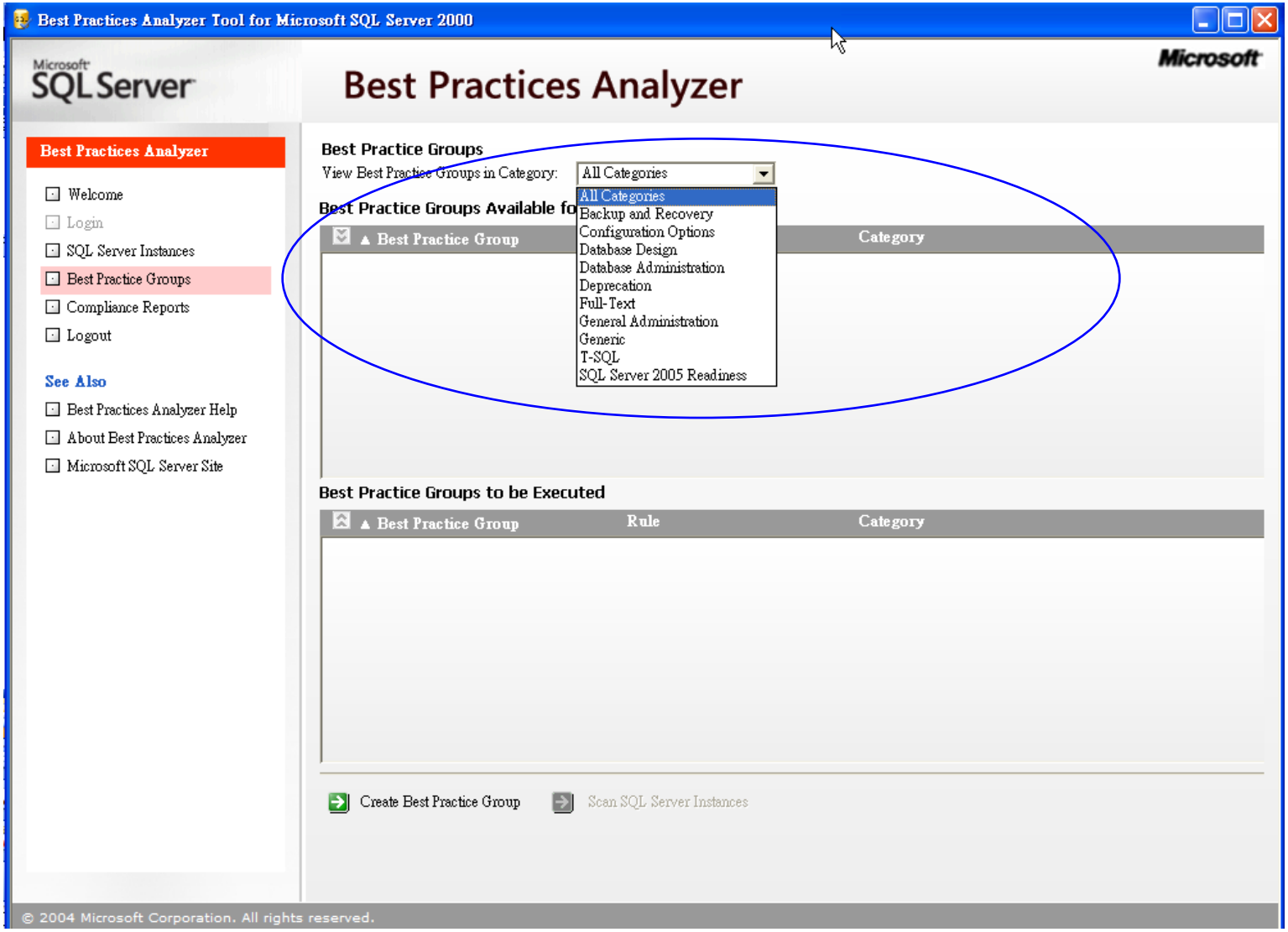


Database Security Checklist

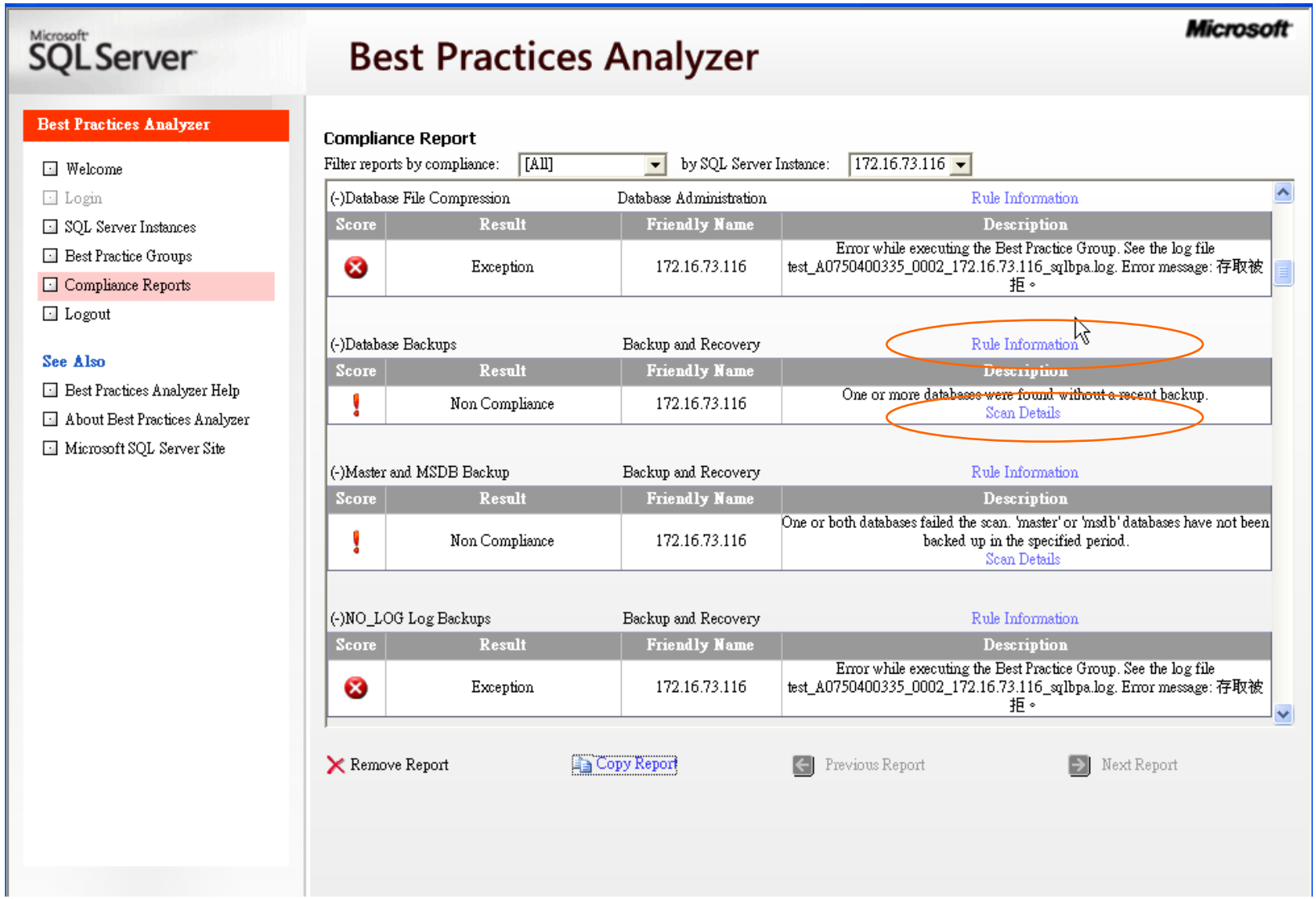
保護SQL Server十大措施

1	安裝最新的Service Pack
2	使用MBSA檢查系統安全漏洞, 並加以修補
3	採用Windows Authentication Mode身分驗証模式
4	不要讓SQL Server直接連上網際網路, 並定期備份
5	爲sa帳號設定複雜的密碼
6	降低SQL Server Service Account的權限
7	利用防火牆封鎖未使用的通訊埠
8	將SQL Server安裝在NTFS檔案系統上, 並管制取用權限
9	刪除安裝記錄檔和範例資料庫
10	稽核使用者的活動

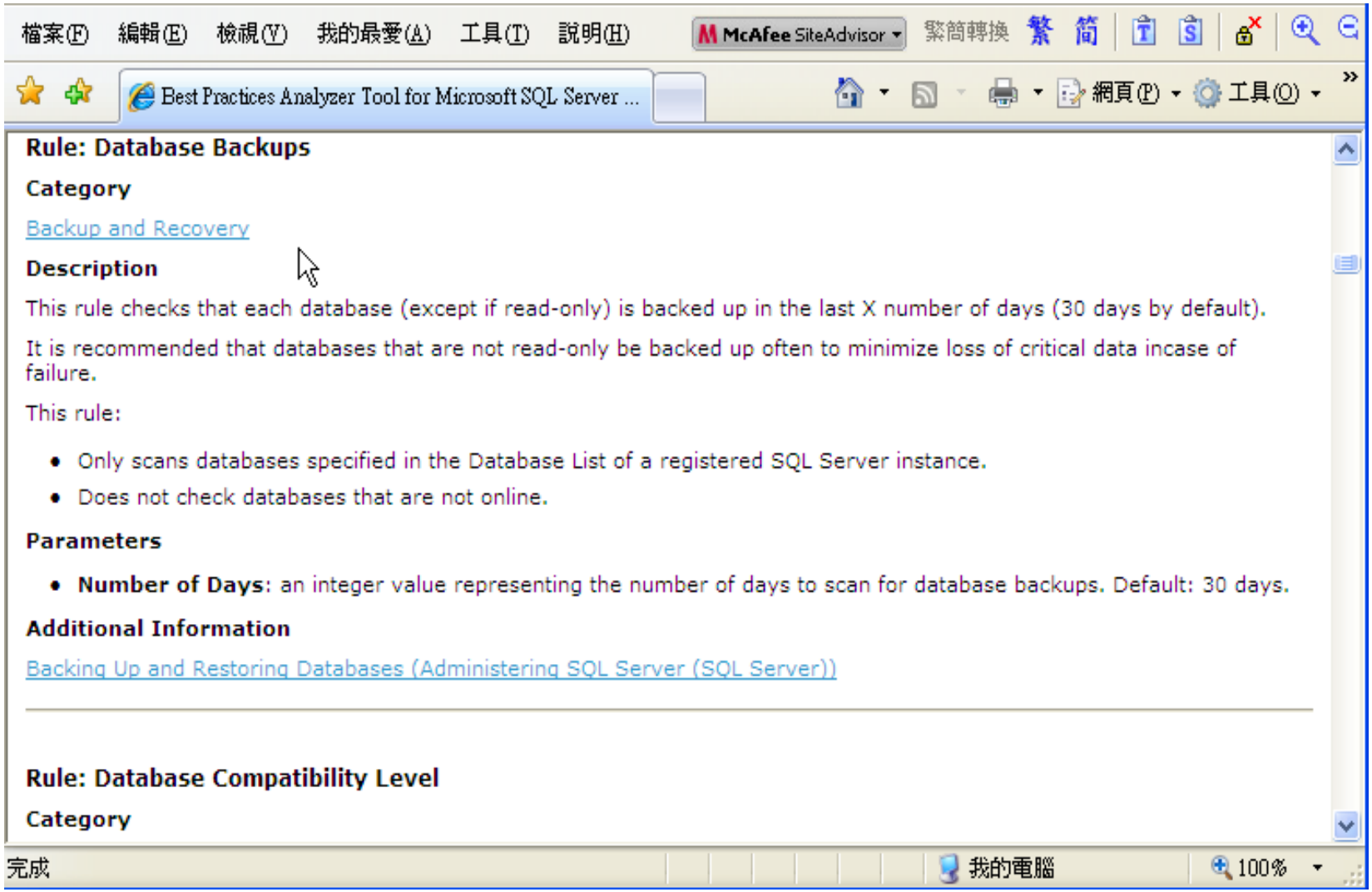
MSSQL 2000 BPA Scan setting



MSSQL 2000 BPA Compliance Report

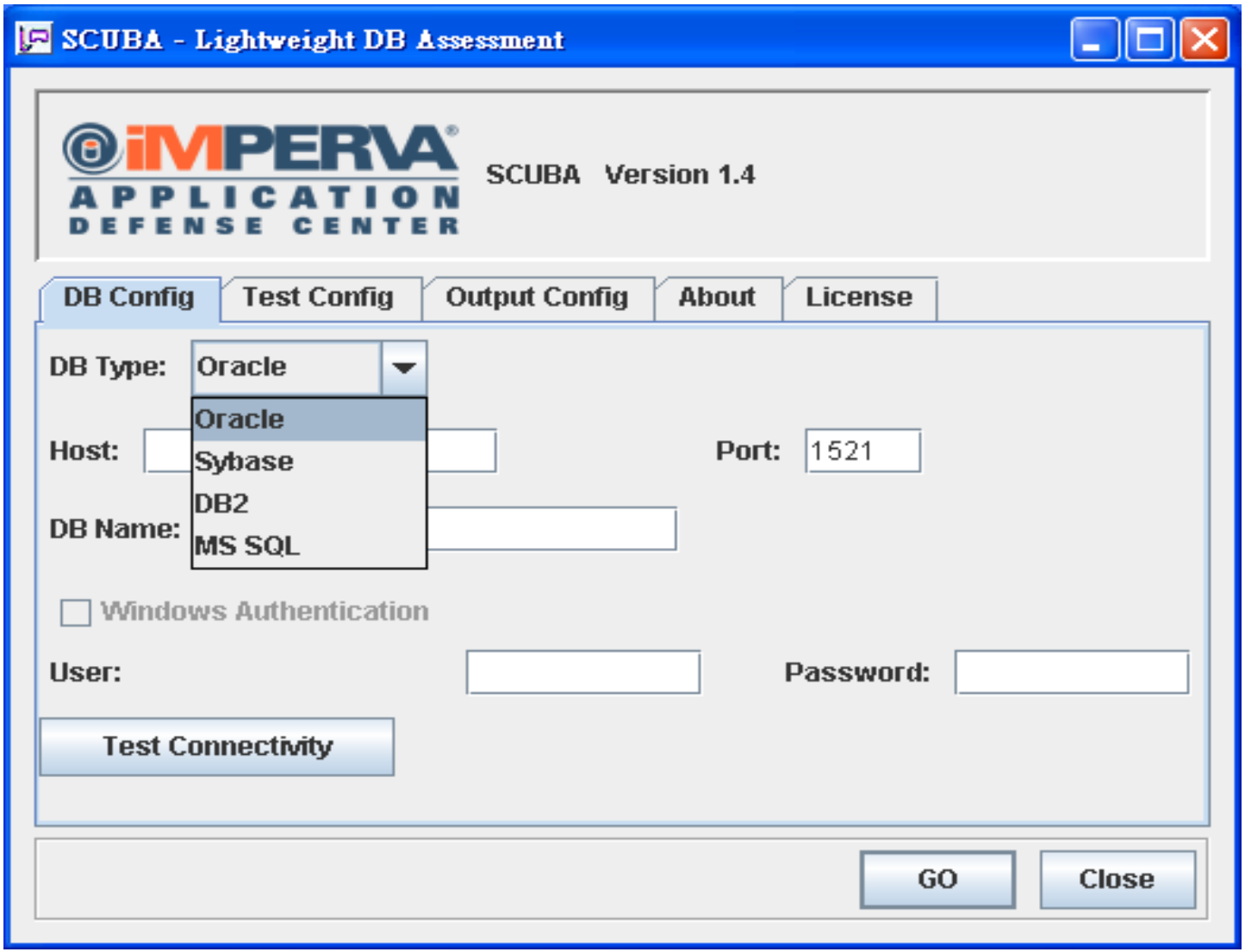


MSSQL 2000 BPA Rule Information

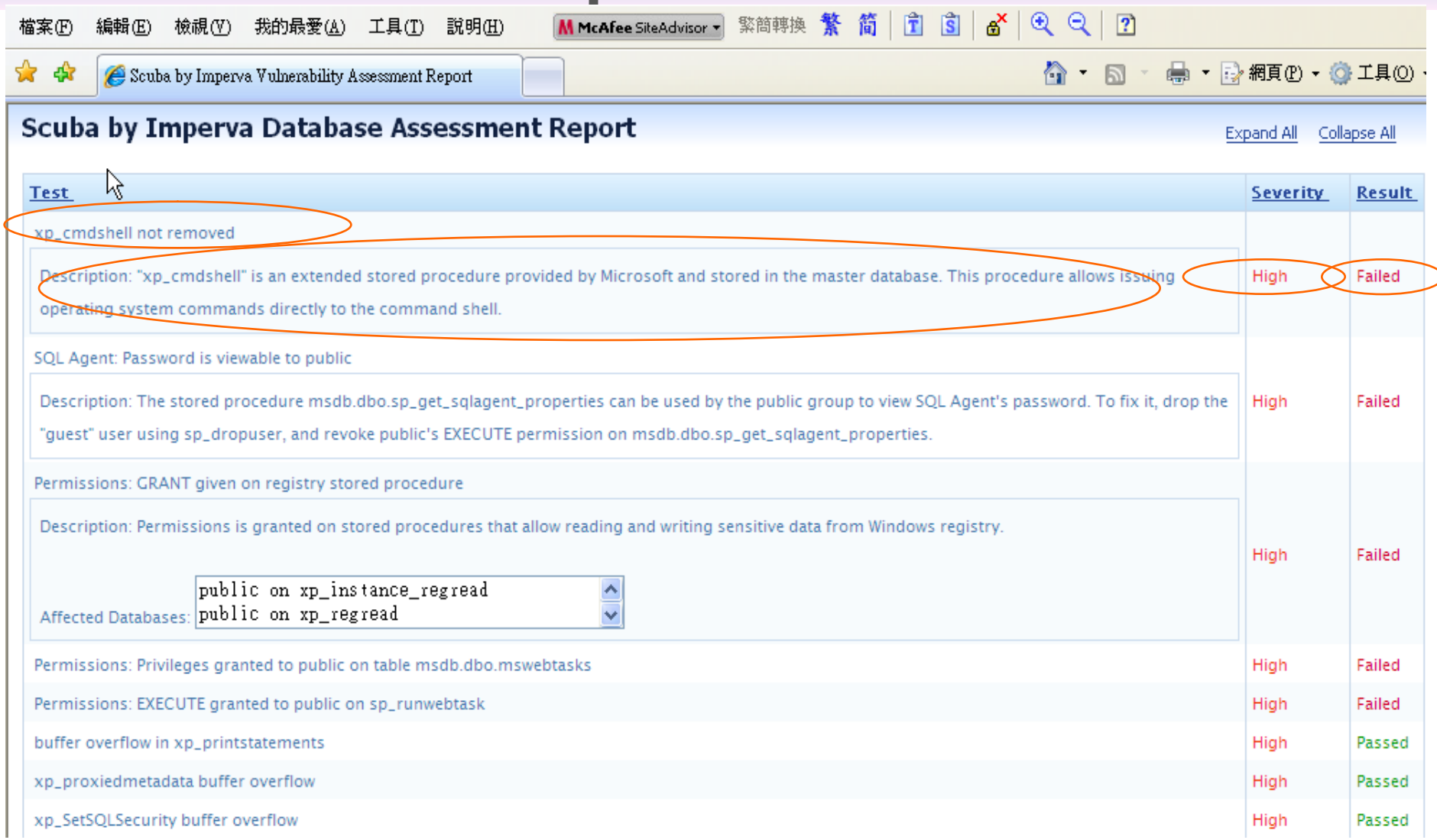


MSSQL 2000 BPA Scan Detail

Scuba Scan Setting



Scuba Scan Report


檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H) McAfee SiteAdvisor 繁簡轉換 繁 简 網頁(P) 工具(O)

Scuba by Imperva Vulnerability Assessment Report

Scuba by Imperva Database Assessment Report

Expand All Collapse All

Test	Severity	Result
xp_cmdshell not removed		
Description: "xp_cmdshell" is an extended stored procedure provided by Microsoft and stored in the master database. This procedure allows issuing operating system commands directly to the command shell.	High	Failed
SQL Agent: Password is viewable to public		
Description: The stored procedure msdb.dbo.sp_get_sqlagent_properties can be used by the public group to view SQL Agent's password. To fix it, drop the "guest" user using sp_dropuser, and revoke public's EXECUTE permission on msdb.dbo.sp_get_sqlagent_properties.	High	Failed
Permissions: GRANT given on registry stored procedure		
Description: Permissions is granted on stored procedures that allow reading and writing sensitive data from Windows registry. Affected Databases: public on xp_instance_regread public on xp_regread	High	Failed
Permissions: Privileges granted to public on table msdb.dbo.mswebtasks	High	Failed
Permissions: EXECUTE granted to public on sp_runwebtask	High	Failed
buffer overflow in xp_printstatements	High	Passed
xp_proxiedmetadata buffer overflow	High	Passed
xp_SetSQLSecurity buffer overflow	High	Passed

Solutions to Accountability

Comparison of different ways of covering user accountability

	Performance	User Mgt	Cost	3rd Party software limitation	Risk	Time	Real-time
External Audit Device	No Impact	No Impact	Low	No	None	Short	Yes
Rewriting Application – user mgt	Minimal Impact	More efforts	High	Yes	High	Long	Yes
Rewriting Application – set user context	Minimal Impact	More efforts	High	Yes	High	Long	Yes
Proprietary database solutions	Minimal Impact	Not all support	High	Yes	High	Long	Yes
Web App Audit Data	No Impact	Comple x	High	No	Low	Long	No

What does IDS / IPS do for DB Security?

- Traditional IDS / IPS / Firewall relay mostly on signature to detect threats against database system.
- Can not fully understand SQL statements when they see it.
- So… What do IDS / IPS / Firewall see?

```
00000000 : 00 53 d0 51 00 01 00 4d 20 0d 00 44 21 13 53 41
.S.Q...M ..D!.SA
00000010 : 4d 50 4c 45 20 20 20 20 20 20 20 20 20 20 20 20 MPLE
00000020 : 4e 55 4c 4c 49 44 20 20 20 20 20 20 20 20 20 20 NULLID
00000030 : 20 20 54 4f 4f 4c 33 45 30 30 20 20 20 20 20 20
TOOL3E00
00000040 : 20 20 20 20 41 41 41 41 41 61 48 53 00 01 00 05
AAAAAaHS....
00000050 : 21 16 f1 00 29 d0 03 00 01 00 23 24 14 00 00 00
!...).....#$....
00000060 : 00 19 73 65 6c 65 63 74 20 2a 20 66 72 6f 6d 20
..select * from
00000070 : 52 75 6c 65 31 44 72 6f 70 20 20 ff
Employee
```

What we should see…

- Now… let's see if we can understand this…

```
UPDATE TEST_SQL SET TEXT='SELECT * FROM USER_OBJECTS UNION
SELECT * FROM USER_OBJECTS WHERE ID=11;
```

- That is a lot more better then IDS / IPS, isn't it?
- So which solution on the market delivers

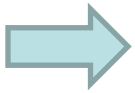
This….

```
Dsfrgdfgw4tsf
   dfsgsdfgfd
   gsdfg

Ooxxjr0172-
   gfhfhsfhsd
   fhhgsfgh50
   =jdsfh'ads
   f-815

Asdl54k;sadfu
   8-asdf

Lkasdjflasdf8
   0732-58-
   adsfpkasdf
```



into

```
Who :  guest
What : SAP ERP SYSTEM
Where :200.151.21.103
When : 2007/01/02 22:14:23
How : update "account" set
   "amount" =  '10000000'
   where name  like 'John Doe'
```

Native DBMS Logging Again

- Cumbersome to configure & manage
  - Impacts performance of production systems
  - Does not provide level of detail required by auditors
  - Generates large amounts of unfiltered data
  - Requires changes to databases (change control issue)
  - Does not provide separation of duties

Requirements: Must Haves

- Integrates with our existing infrastructure
- Single solution for all our DBMS platforms
- Minimal impact on DBMS performance
- Scales across multiple DB servers & locations
- Produces detailed information required by auditors (who, what, when, how, etc.)
- Generates real-time alerts in standard format
- Creates secure audit trail (can't be modified by privileged users)

Requirements: Nice-to-Haves

- Can also be implemented as database firewall (blocking)
- Includes templates for SOX, PCI, …
- Eliminates need to manually manage audit trail and oversight process
- Installs with minimal professional services
- Requires minimal ongoing IT resources

問題與討論

Thank you!

Michael_Shiah@ringline.com.tw

02-26512340#699