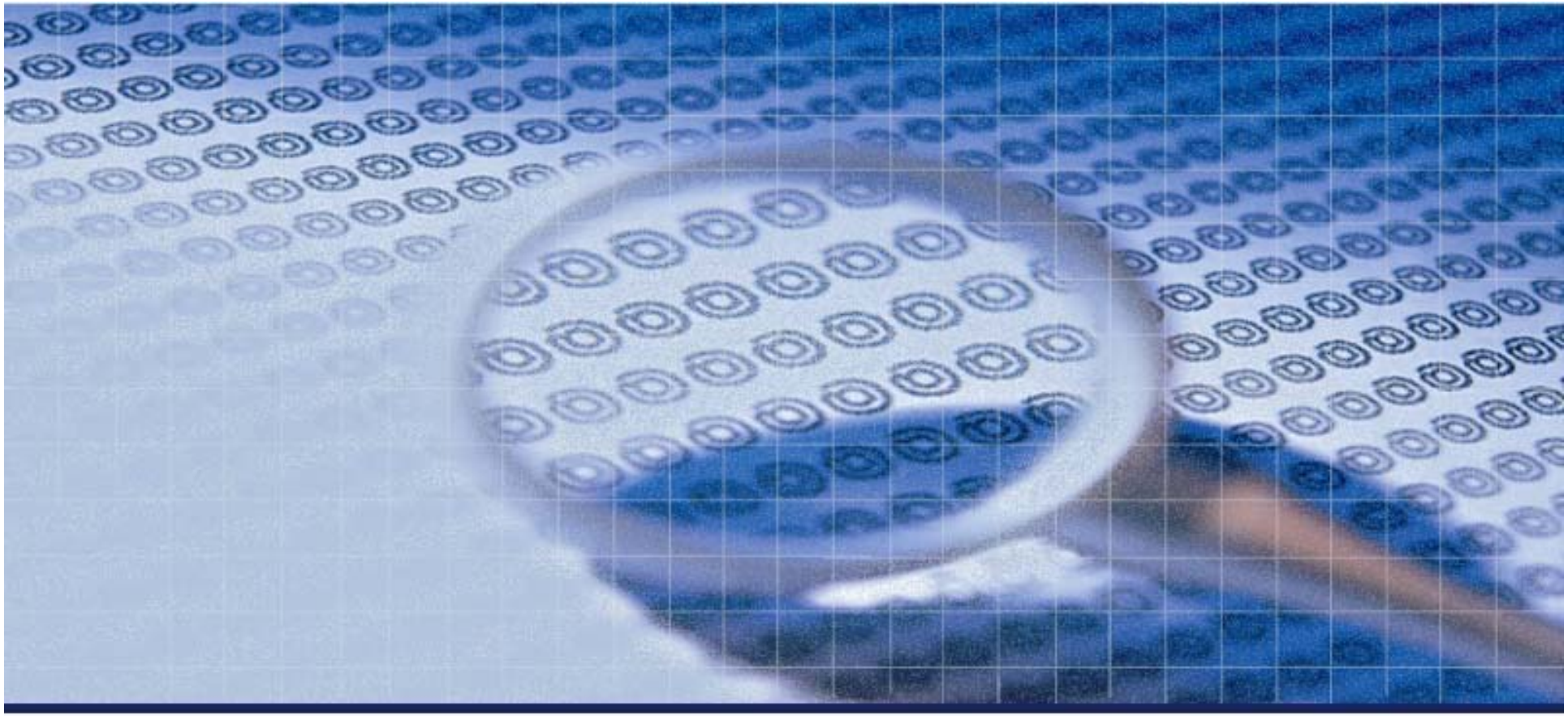
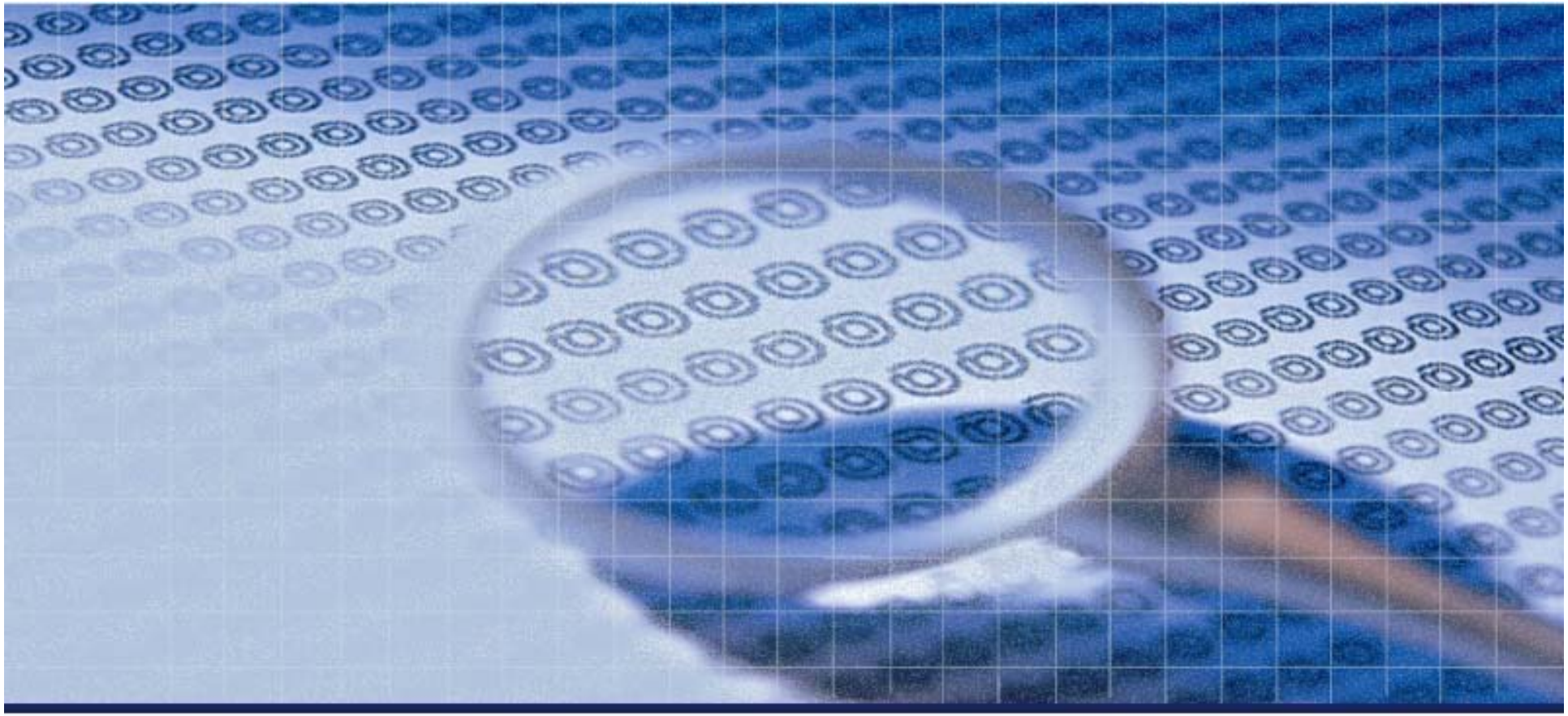


伺服器系統安全管理

敦陽科技

大綱

- 前言
- 入侵過程及事後處理
- General System Security
- Harden UNIX System
- Harden Windows System
- Q & A



前言

前言

- 關於我
- 資安領域概述
- **Trade-Off**
- 防禦的訣竅
- 迷思
- 妨害電腦使用罪

關於我

- 劉俊雄 <OuTian.Liu@sti.com.tw>
- 現任 敦陽科技 資安服務處 資安顧問
- 經歷 –
  - ✓2007/2008/2009 台灣駭客年會講師、0day發表者
  - ✓多次政府、金融、電信、教育、企業單位之滲透測試服務
  - ✓資安事件處理與蒐證
  - ✓資安設備規劃與建置
- 認證 –
  - ✓CEH (Certified Ethical Hacker)
  - ✓CCA (Citrix Certified Administrator)

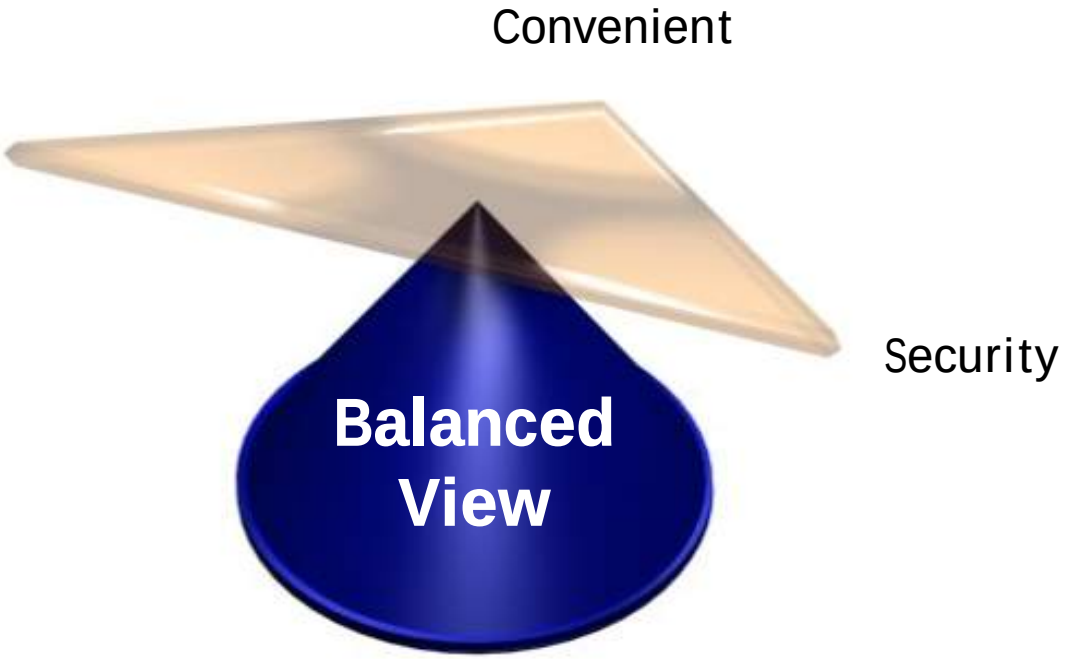
Stark Technology Inc. 敦陽科技股份有限公司

資安領域概述

- 通訊安全
- 存取控制
- 資料安全
- 內容管理
- 安全監控
- 資安稽核
- 安全管理

Stark Technology Inc.
敦陽科技股份有限公司

Trade-Off



防禦的訣竅

知彼知己，百戰不殆
不知彼而知己，一勝一負
不知彼，不知己，每戰必敗。

《孫子兵法・謀攻篇》

迷思

- **Windows 安全 ？ 還是 UNIX 安全 ？**

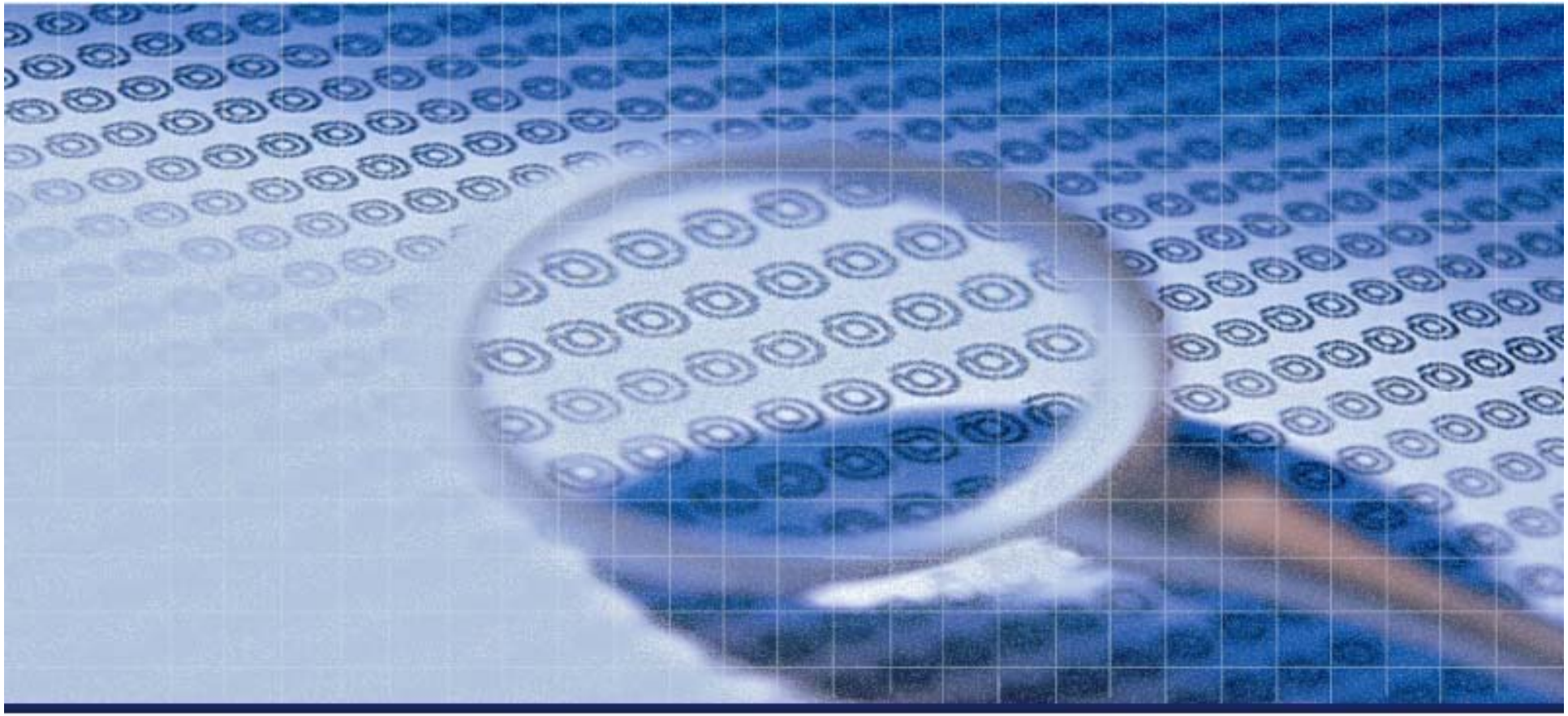
December 19, 2002

WINGGY：沒有不安全的系統，只有不安全的人

前些時日，一家資訊公司號稱從美國花大錢請來網路安
額爆滿，並且吸引香港人士前來研習。然而，台灣本地

妨害電腦使用罪

- 三百五十八條－入侵電腦或其相關設備罪
- 三百五十九條－破壞電磁紀錄罪
- 三百六十　條－干擾電腦或其相關設備罪
- 三百六十一條－加重其刑
- 三百六十二條－製作犯罪電腦程式罪
- 三百六十三條－告訴乃論



入侵過程及事後處理

一般入侵過程

- 資訊收集
- 弱點探測
- 侵入系統
- 提升權限
- 收集資料
- 植入後門

資訊收集

- 主機搜尋
  - ✓ICMP、TCP
  - ✓Zone Transfer
  - ✓Google
- 服務掃描 (Port Scan)
  - ✓nmap、Superscan、amap、scanrand
  - ✓FIN, Xmas , or Null scan
- 網路架構探測
  - ✓traceroute、tcptraceroute、paratrace
- 作業系統判斷
  - ✓xprobe、p0f、nmap
  - ✓由 TCP Fingerprint 辨識系統

弱點探測

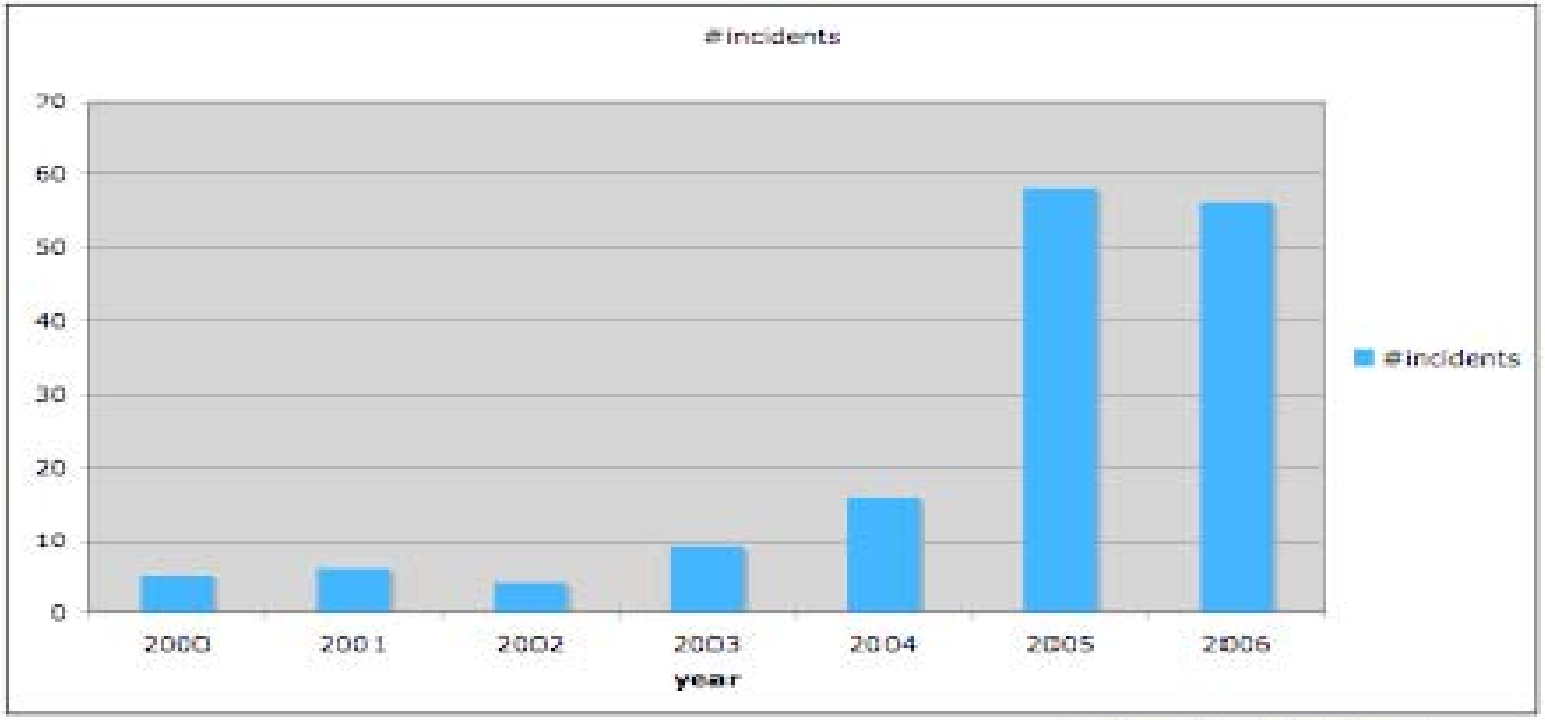
- 服務弱點掃描工具
  - ✓Nessus
  - ✓ISS Internet Scanner
  - ✓Foundstone FoundScan
  - ✓Dragonsoft Vulnerability Scanner
- 網頁弱點掃描工具
  - ✓HP WebInspect
  - ✓IBM AppScan
  - ✓Acunetix Web Vulnerabilisy Scanner
- 人為判斷

侵入系統

- 利用 Web 應用程式的漏洞
- 利用服務本身的弱點
- **Brute Force Attack**
- **Sniff**
- **Session Hijacking**
- **Man-in-the-Middle**
- **Social Engineering**

Web AP Security 共同的痛（一）

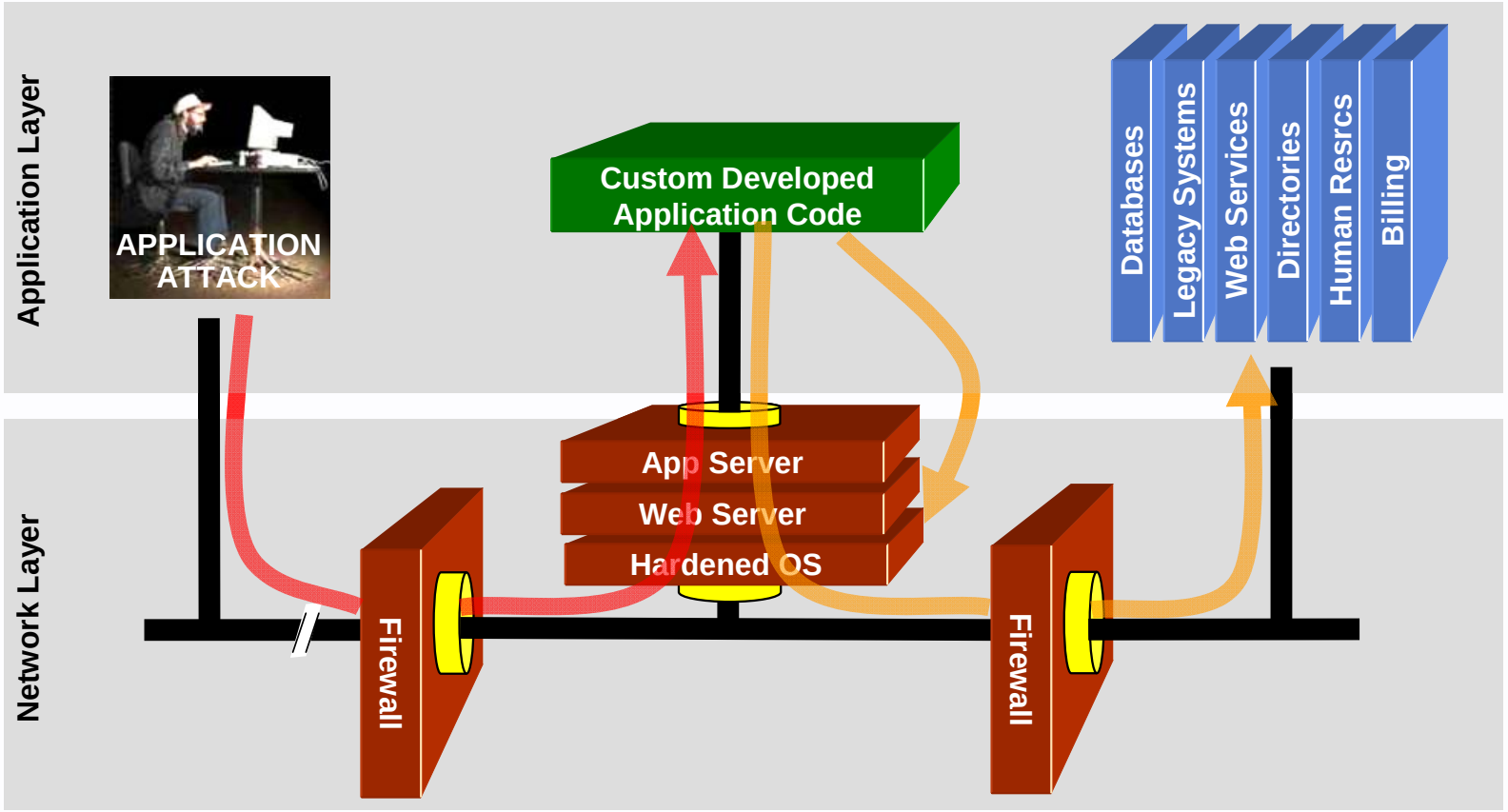
- Web AP 變成顧客 / 駭客共同入口
  - ✓根據Gartner統計：
    成功的惡意攻擊中，70% 都是針對 Web AP



Stark Technology Inc.
敦陽科技股份有限公司

Web AP Security 共同的痛（二）

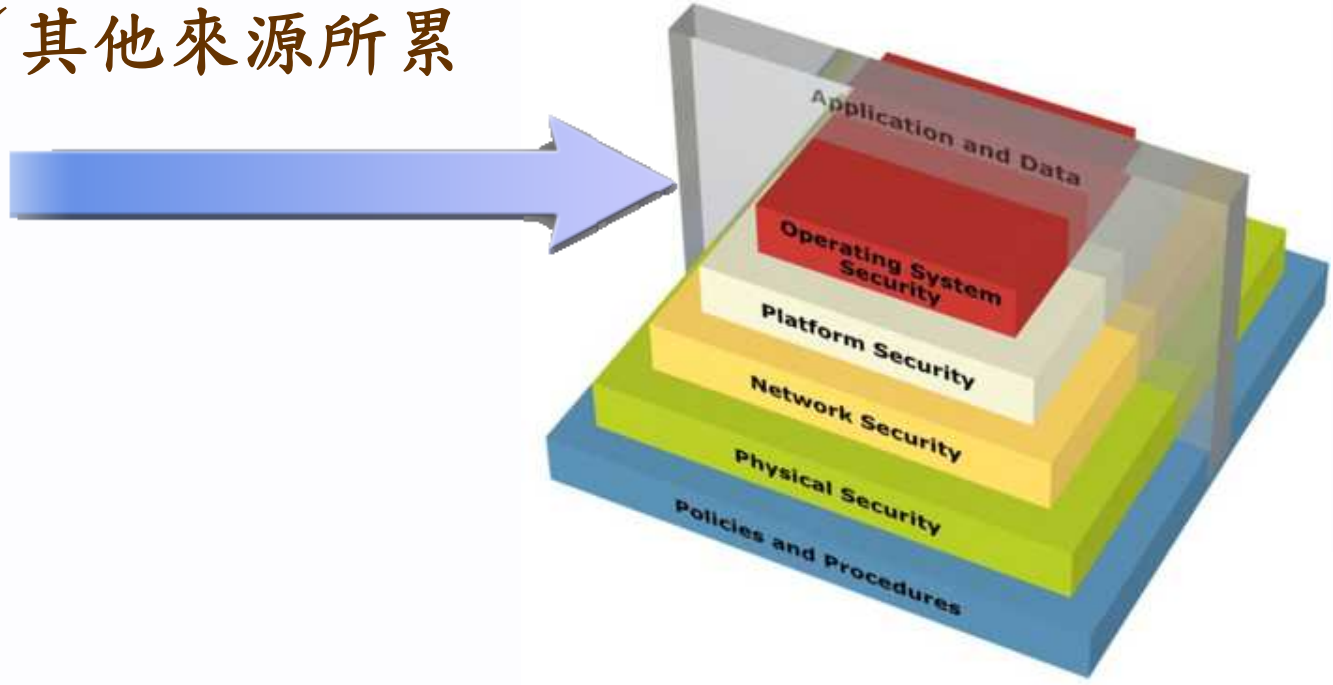
➢ 既有的資安設備無用武之地



你無法使用網路層的保護機制 **(firewall, SSL, IPS, hardening)**
來偵測或停止應用層的攻擊

Web AP Security 共同的痛（三）

- Web AP 安全問題來源的複雜與多樣性
  - ✓複雜之 AP Source Codes
  - ✓類似的安全問題重複發生
  - ✓誤用造成安全遺憾
  - ✓其他來源所累



網頁“應用程式”？？？

- 靜態網頁 ？
- HTML ?
- Javascript ?
- CSS ?
- DHTML ?
- XML ?

常見的網頁程式語言

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

常見的服務程式

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

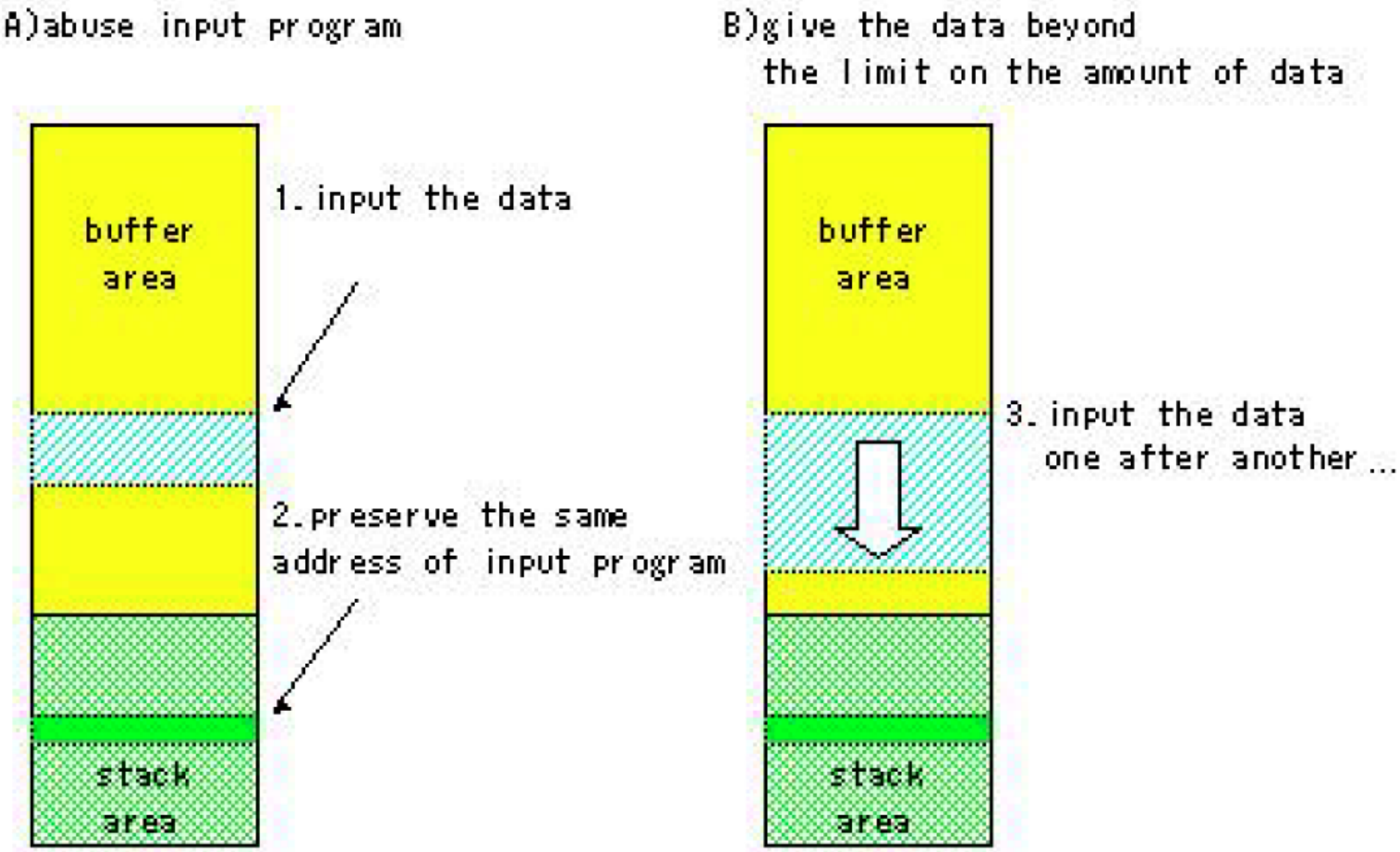
可用以入侵的 Web 弱點

- SQL Injection
- File Inclusion
- Command Injection
- Code Injection
- Directory Traversal
- Upload File Mis-Handling
- Buffer Overflow

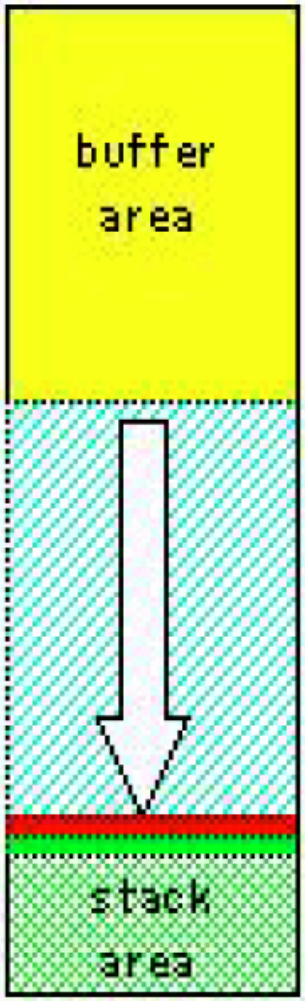
提升權限

- crack password
- vulnerable program/service
  - buffer overflow (stack/heap)
  - format string
  - race condition
  - design error
- Kernel Exploit
- Brute Force Attack

Buffer Overflow (Stack)

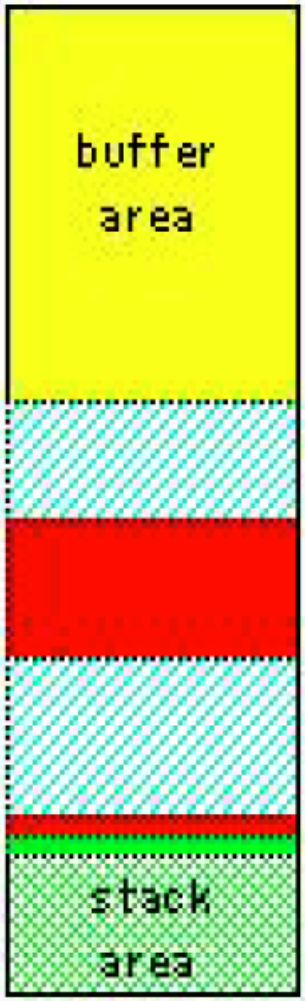


C)finally destroy
the stack



4.destroy the stack
and overwrite address

D)illegal program
is carried out



6.illegal program
is prepared in
overwritten addres:

5.back to
overwritten address

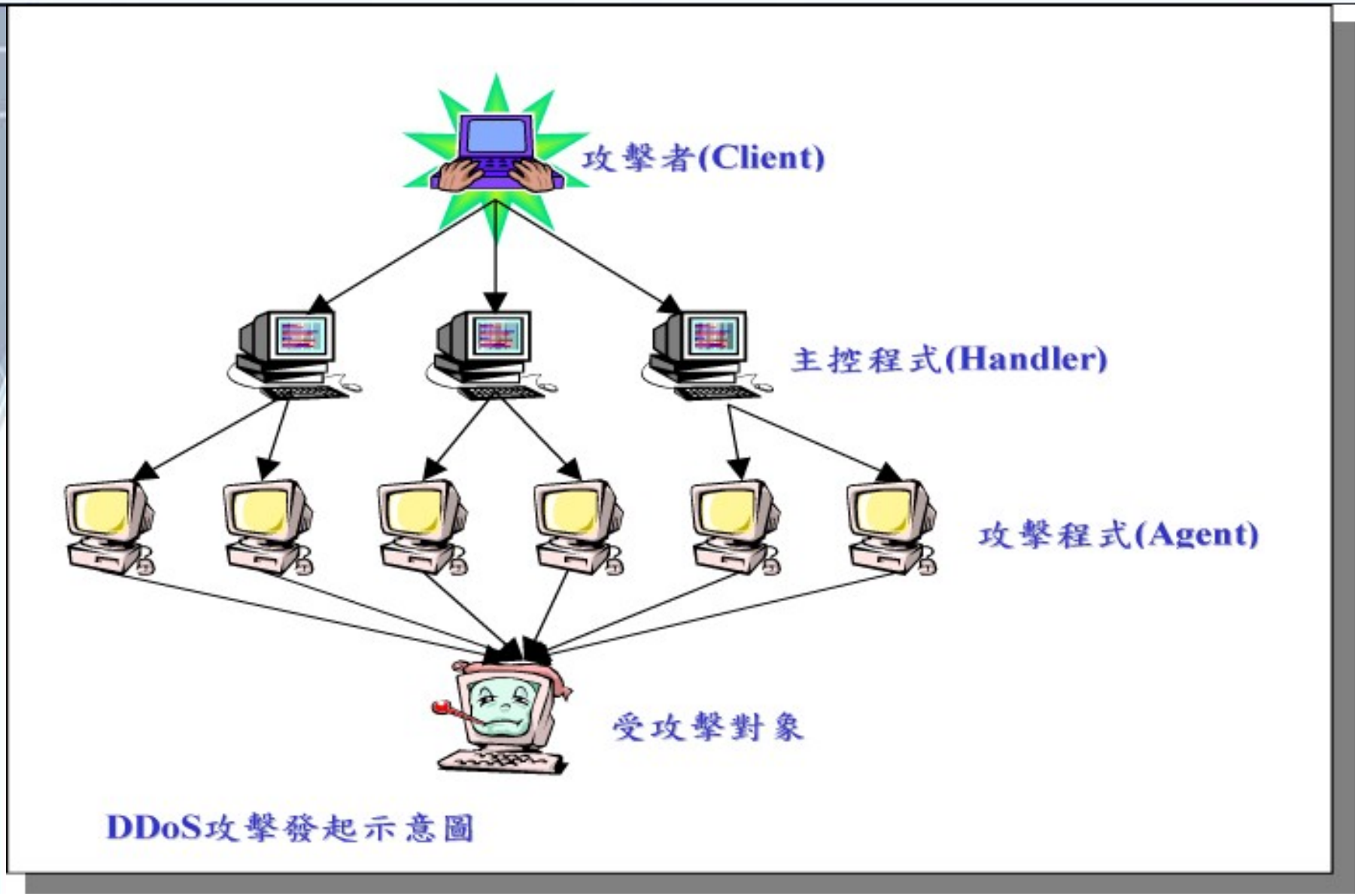
收集資料

- 破解使用者密碼
- 修改登入頁面取得密碼
- 啟動 sniffer 竊聽密碼
- "備份資料"
- 繼續尋找並攻擊內部網路中其他機器

植入後門

- 後門程式
- IRCbot
- TCP proxy
- 植入Rookit
  - ✓隱藏蹤跡及保留存取權限的工具"組“
  - ✓修改log紀錄
  - ✓置換系統工具
  - ✓後門程式

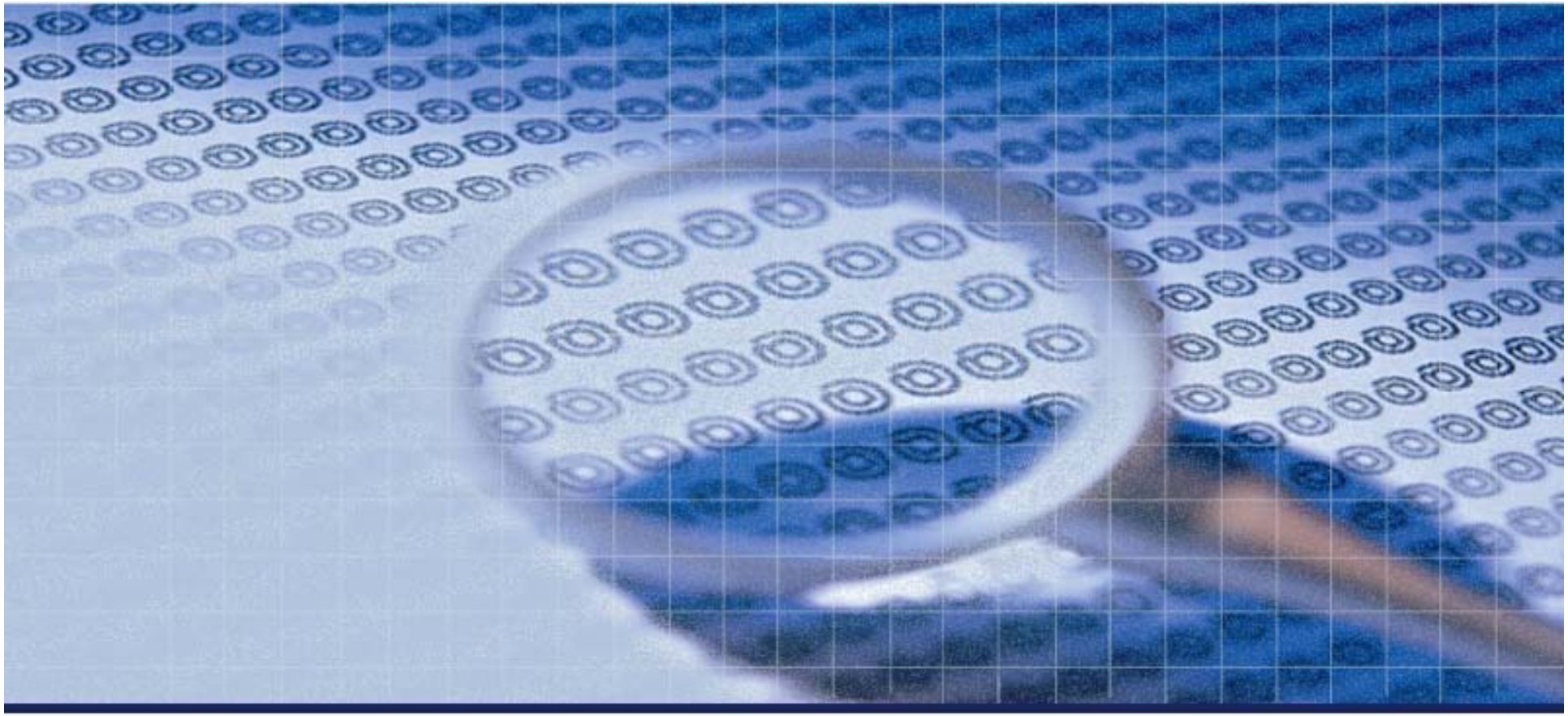
Botnet



DDoS攻擊發起示意圖

入侵徵兆

- 網頁遭更改
- 磁碟空間快速減少
- 網路流量提高
- 上游監控單位的通知
- 系統紀錄異常
- 系統中存在不明帳號
- 不明的 process
- 被破壞的 utmp/wtmp
- 「看起來古怪」的事情



事後處理及蒐證

系統檢核與鑑識

- 蒐證原則
- 確認系統工具的正確性
- 檢查 log
- 檢查帳號
- 檢查 process
- 檢查檔案
- 檢查網路狀況
- 檢查 rootkit

蒐證原則

- 儘可能保留系統狀態，包含 Memory、Process、Open File、Network Connection、File System、…etc
- 複製重要的磁碟以防原資料損毀
- 在不破壞系統之情況下進行蒐證，例如使用著名的 Forensic Live CD – Helix (http://www.e-fense.com/helix/)

確認系統工具

- **UNIX**
  - ✓ls、find、ps、top、lsof、netstat
  - ✓比對 md5/sha1 checksum ,
    確認重要的系統工具是否被置換
  - ✓by Tripwire、AIDE
- **Windows**
  - ✓DIR、netstat
  - ✓Filemon、Regmon、PsTools、TcpView、
    Process Monitor、fport

檢查 log

- **UNIX –**
  - ✓**w**
  - ✓**last**
  - ✓**/var/log/**
- **Windows –**
  - ✓事件檢視器
  - ✓所有服務之日誌

檢查帳號

- 多出異常帳號？
- 所屬 group 改變？
- 權限改變 ？
- 密碼改變 ？

- **UNIX –**
  - ✓**Sudoers**
  - ✓**Shell 遭修改**

檢查 process

- **UNIX -**
  - ✓確認每一個 process
  - ✓ "不要"信任 ps 看到的名稱
  - ✓ check /proc/process_id for detail
  - ✓ strace -p process_id
  - ✓ lsof -p process_id
- **Windows –**
  - ✓工作管理員
  - ✓Process Monitor / Process Explorer
  - ✓PSTools

檢查檔案

- **UNIX –**
  - ✓ DocumentRoot、/tmp、/var/tmp
  - ✓ 「...」、「.. 」、「 」
  - ✓ find / -type f -ctime 1d -mtime 1d
  - ✓ touch -t 200702050000 /tmp/ox
    find / \(-newer /tmp/ox -o -cnewer /tmp/ox \) -ls
- **Windows –**
  - ✓dir /as 、 dir /ah
  - ✓attrib -s -h -r filename

Stark Technology Inc.
敦陽科技股份有限公司

檢查網路狀況

- **UNIX –**
  - ✓**nmap、netstat、lsof**
- **Windows –**
  - ✓**tcpview、fport、netstat**
- **確認每一連線是否正常**
  - ✓**normal web connection :**
    - **– local:80 <=> remote.clientport**
  - ✓ **reverse connect :**
    - **– local.clientport <=> remote.xx**
- **確認網卡是否處於 promiscuous mode**

檢查 rootkit

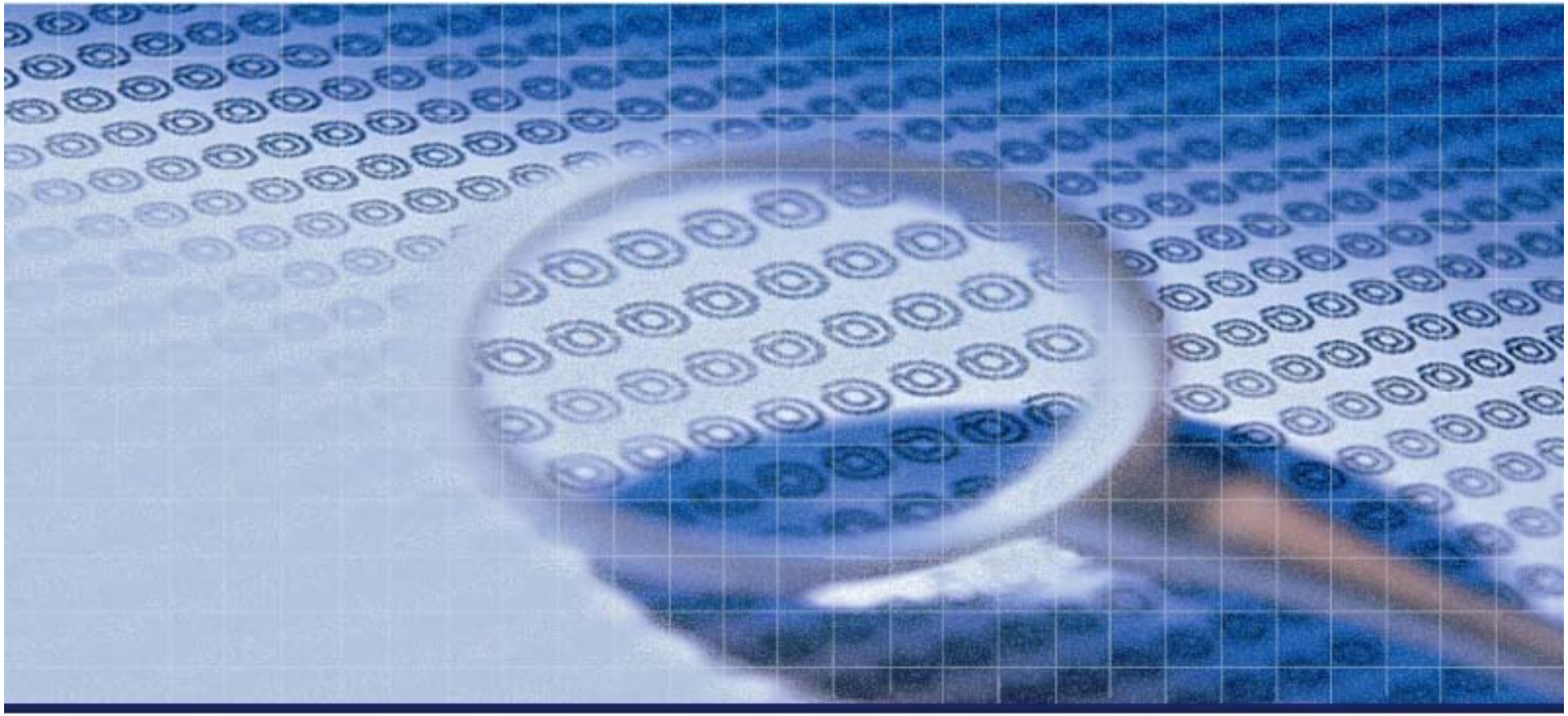
- **UNIX –**
  - ✓ **chkrootkit - http://www.chkrootkit.org/**
  - ✓ **rkhunter - http://www.rootkit.nl/**
- **Windows –**
  - ✓以兩套以上的掃毒、掃木馬軟體檢查
  - ✓anti-spyware.xls

入侵處理

- 由被植入的後門程式取得資訊 –
  - ✓從 **create time** 得知何時入侵
  - ✓從 **owner** 得知從哪個 **daemon** 侵入
- 找出駭客入侵的弱點，並修補
- 備份資料，重新安裝系統， **or -**

入侵處理(續)

- Windows - 檢查 Registry , autoexec.bat win.ini , system.ini , autorun.inf ... etc
- UNIX - 檢查 /etc/rc* , /etc/cron.* , /var/spool/cron , /etc/modprobe* , /proc/modules , /etc/ld.so.conf ... etc
- 比對並還原所有被修改過的檔案
- patch 所有的 package (包含kernel)
- 更換所有/重要使用者的密碼



General System Security

- **Keep System up to date**
- **Service**
- **Firewall**
- **Host-based IDS**
- **Vulnerability Scanner**

Keep System up to date

- 定時更新所有套件
  - ✓ Windows – Windows Update/自動更新
  - ✓ Linux – yum/apt/urpmi/yast/rhn-update
  - ✓ BSD – ports / portupgrade
  - ✓ Solaris – Sun Update Connection / pkg-get
- 必要時更新 kernel

Service

- 停止所有使用不到的服務
- 儘可能使用加密的協定
  - ✓ telnet => ssh
  - ✓ pop3 => pop3s
  - ✓ http => https
- 以最小權限運行服務
- 隱藏版本及設定
- chroot (if possible)

Firewall

- UNIX – ipchains/iptables/ipfw/ipf/pf/sunscreen
- Windwos – Default/Norton/Kaspersky/…etc
- DROP 所有對本機的連線，僅開放必要服務的 port
- 限制本機對外部的連線，僅開放必要的 程式/目標機/目的埠
- nmap -p 1-65535 target

Firewall Example (TCP)

- Mail + Web + POP3 Server

- Allow TCP from any to any ESTABLISHED
  Allow TCP from any to me port 25 SYN
  Allow TCP from any to me port 80 SYN
  Allow TCP from any to me port 110 SYN
  Deny TCP from any to me SYN
  Deny TCP from me to any

Firewall Example (UDP)

- DNS + NTP + SNMP Server

- Allow UDP from any to me port 53 keep-state
  Allow UDP from any to me port 123 keep-state
  Allow UDP from any to me port 161 keep-state
  Deny UDP from any to me

Host-based IDS

- AIDE (UNIX)
- AFICK (Win/UNIX)
- Archon (Win)
- OSIRIS (Win/UNIX)
- OSSEC (Win/UNIX)
- Samhain (UNIX)
- Tripwire (Win/UNIX)

Vulnerability Scanner

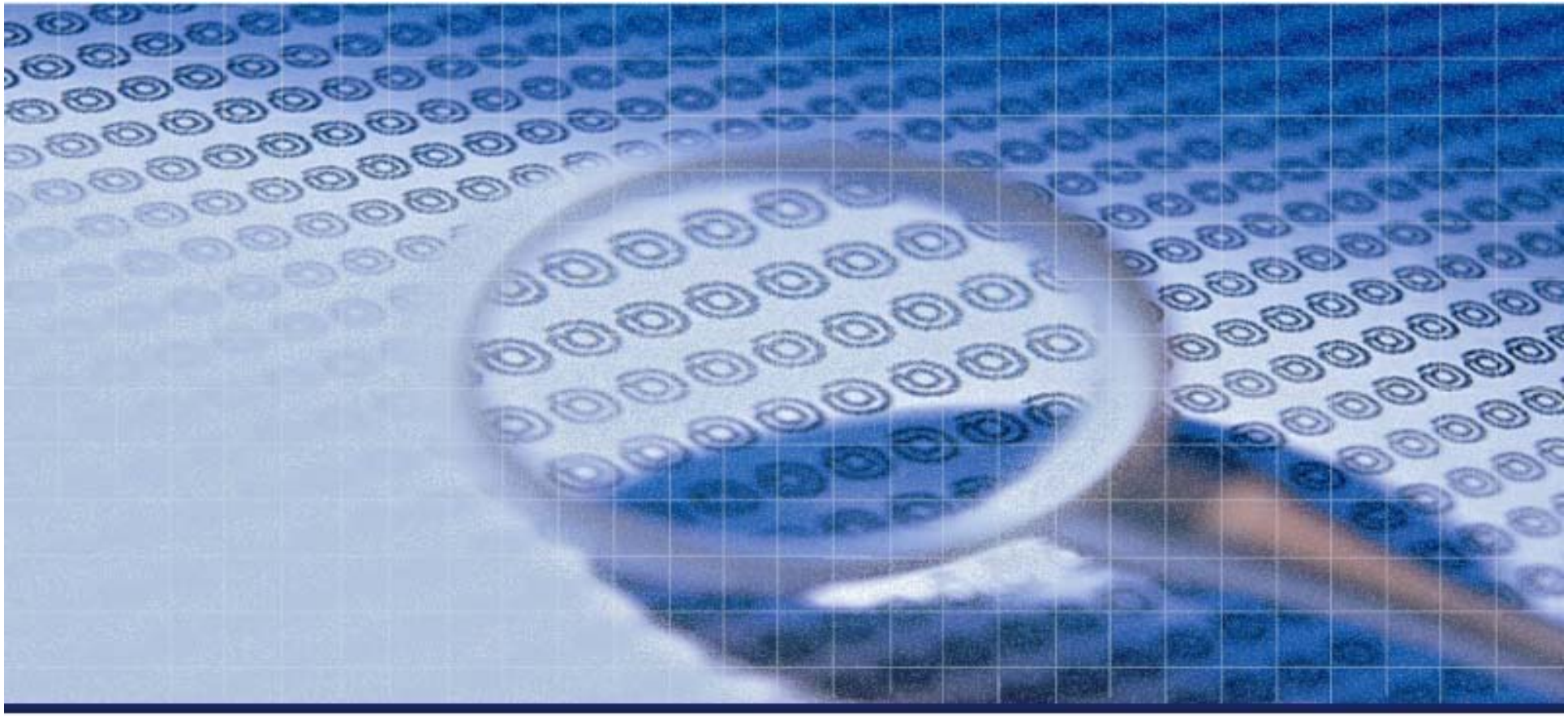
- **Free**
  - ✓Nessus
  - ✓SATAN
  - ✓Microsoft Baseline Security Analyzer
- **Commercial**
  - ✓ISS Internet Scanner
  - ✓DragonSoft Secure Scanner
  - ✓Foundstone Foundscan
  - ✓eEye Retina

Stark Technology Inc.
敦陽科技股份有限公司

Web Vulnerability Scanner

- **Free**
  - ✓Nikto
  - ✓Wikto
- **Commercial**
  - ✓IBM Rational AppScan
  - ✓HP WebInspect
  - ✓Acunetix – Web Vulnerability Scanner

Stark Technology Inc.
敦陽科技股份有限公司



Harden UNIX System

Harden UNIX System

- **System**
  - ✓ Harden System
  - ✓ Account
  - ✓ Avoid backdoor program
  - ✓ Harden kernel
- **Service**
  - ✓ telnet
  - ✓ sshd
  - ✓ smtp
  - ✓ apache

Harden system

- **Harden Package**
  - ✓**Tiger – (AIX/HPUX/IRIX/Linux/SunOS)**
  - ✓**Bastille Linux – (Linux)**
  - ✓**LSAT – (Linux)**
- **Check files with setuid root permission**

Account

- mail/ftp only 的帳號，使用其他認證方式取代 (ldap/mysql/...etc) 系統帳號
- 關閉非管理者的登入權限
- 定期更換密碼
- 規範密碼強度

Avoid backdoor program

- chroot 所有的 daemon
- 除了 /、/usr外，把其他 partitions (/var 、/tmp、/home、...) 的 mount option 加上 nosuid,noexec
- 一般 user 不需使用的話，把gcc、perl 及 python 改成限 root 執行 (或移除)

Harden Linux Kernel

- **Pax/Exec-Shield**
  - ✓ **kernel.randomize_va_space = 1**
  - ✓ **kernel.exec-shield = 1**
- **APParmor**
- **SELinux**
- **GRsecurity kernel module**
- **RSBAC (Rule Set Based Access Control)**

Stark Technology Inc.
敦陽科技股份有限公司

Linux Kernel Patches

名稱	安全性	安裝容易度	設定難度	Linux 套件支援
Pax/Exec-Shield	***	***	*	Fedora/RHEL
APPArmor	***	**	***	Suse/Ubuntu/ Slackware
SELinux	***	**	*********	Fedora/RHEL
Grsecurity	****	***	***	MDV/Gentoo /Debian
RSBAC	***	***	*****	MDV/Gentoo

Stark Technology Inc.
敦陽科技股份有限公司

telnet

- … Forget it !
- 明碼傳輸，導致不論由外向內、或由內向外，均可能遭竊聽內容
- CVE-2007-0956 (2007/02/14)、CVE-2007-0882 (2007/02/12) – bypass authentication in Solaris 10/11 telnetd

ftp

- wu-ftpd、proftpd、pureftpd、vsftpd
- chroot
- 限制登入的 user – ftpusers
- 關閉 anonymous login
- 以 sftp 取代

sshd

- 限制連接的來源
  - ✓Firewall
  - ✓TCP Wrapper (hosts.allow & hosts.deny)
- Ban 掉不斷嚐試登入的來源 –
  - ✓BlockHosts - http://www.aczoom.com/cms/blockhosts/
  - ✓DenyHosts - http://denyhosts.sf.net/
  - ✓Daemon Shield - http://daemonshield.sf.net/
  - ✓Fail2ban - http://fail2ban.sf.net/

sshd (續)

- in /etc/ssh/sshd_config :
  - ✓禁止 root login - PermitRootLogin no
  - ✓更改至別的連接埠 - Port xxx
  - ✓只使用 ssh v2 - Protocol 2
  - ✓關閉 ssh port forwarding -
    AllowTcpForwarding no
    GatewayPorts no
  - ✓允許/禁止哪些用戶或群組連接 sshd -
    AllowGroups、AllowUsers、
    DenyGroups、DenyUsers

SMTP

- sendmail、**postfix**、**qmail**
- 常見弱點 – 不恰當的組態檔權限、資料檔權限、目錄權限
- **VRFY**、**EXPN**
- **.forward**
- **TLS/SSL support**

Apache

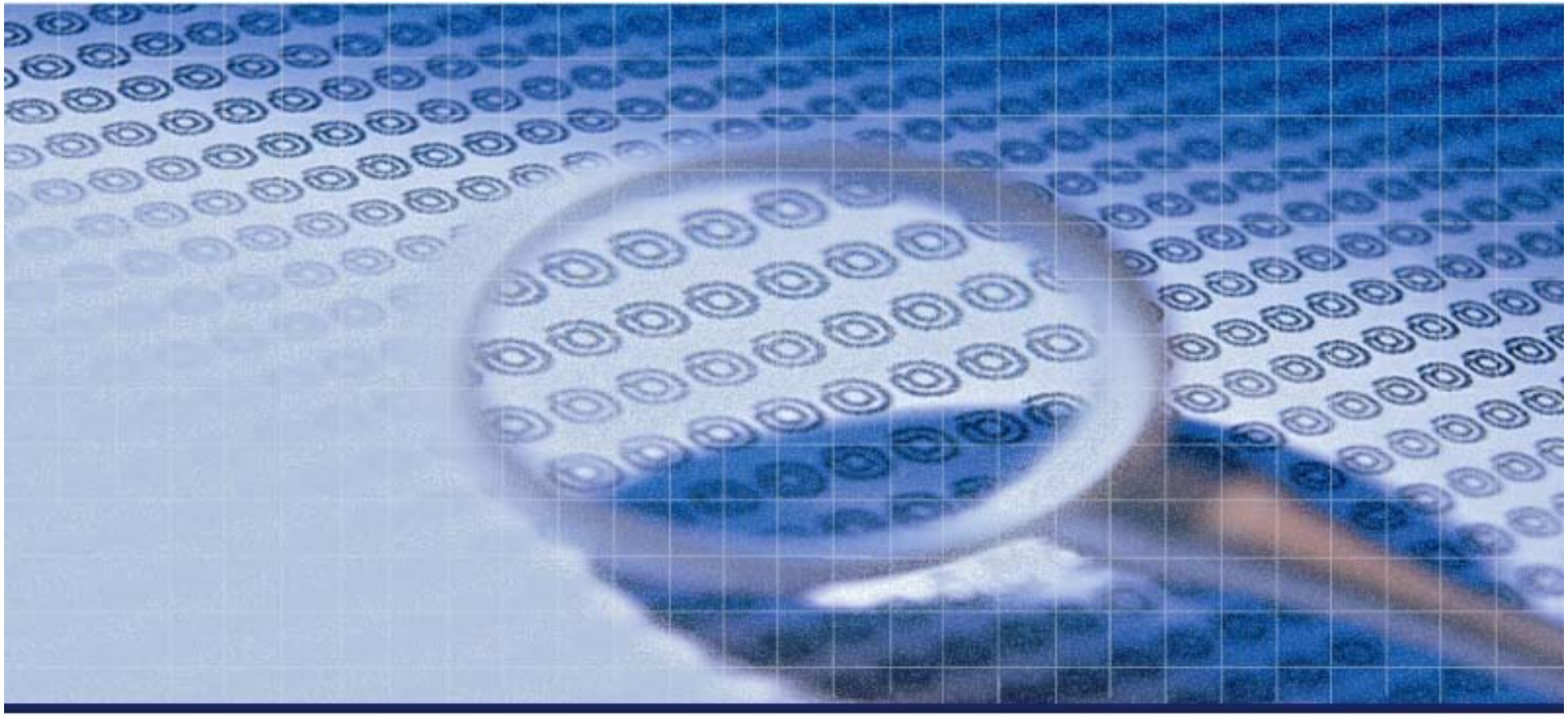
- Chroot if possible
- cgi control
- Logs
- DocumentRoot permission
- Run as separate user (suEXEC)
- Protect Auth password file
- Be careful about MIME file handling
- Mod_security

php config

- in php.ini –
  - ✓ register_global = off (全域變數)
  - ✓ magic_quotes_gpc = on (特殊字元轉換)
  - ✓ display_error = off (在網頁上顯示錯誤訊息)
  - ✓ log_error = on (紀錄錯誤訊息)
  - ✓ allow_url_fopen = off (可開啟遠端網頁)
  - ✓ expose_php = off (顯示 PHP 版本資訊)
  - ✓ open_basedir = (允許開啟的目錄)
  - ✓ safe_mode = on (安全模式)
  - ✓ safe_mode_include_dir = (允許引入的目錄)
  - ✓ disable_function = (禁止使用的函數)

php (續)

- **Encode php source / config –**
  - ✓ionCube Standalone Encoder
  - ✓PHP Encoder
  - ✓PHTML Encoder
  - ✓SourceCop
  - ✓SourceGuardian
  - ✓Zend Encoder + Optimizer



Harden Windows System

Harden Windows System

- **System**
  - ✓File System
  - ✓Account
  - ✓Anti-Virus / Anti-Spyware
  - ✓Useful Tools
- **Service**
  - ✓IIS
  - ✓FTP
  - ✓DNS
  - ✓Terminal Service、VNC
  - ✓SQL Server

Stark Technology Inc.
敦陽科技股份有限公司

File Sysem

- NTFS only !
- 針對重要的目錄及執行檔設定權限
  - ✓%SYSTEMROOT%\System32
  - ✓Inetpub
- at、regedit、cacls、regedt32、rdlin、cscript、wscript、ftp、runas、net、netsh、tskill、regsvr32、tftp、netstat、runonce、telnet、debug

Account

- 規範密碼強度
- 定時更改密碼
- 更改 Administrator 帳號名
- 禁止預設的若干帳號登入
  - ✓Guest
  - ✓IIS 新增的 TsInternetUser
  - ✓ASP.NET 新增的 ASPNET

Anti-Virus / Anti-Spyware

- 至少安裝一套防毒軟體，並定時更新病毒碼
- 避免使用伺服器上網、處理郵件或開啟來路不明的檔案
- 定時以手動方式做其他檢核

Useful Tools

- **Default –**
  - ✓ dir
  - ✓ netstat
  - ✓ arp
  - ✓ 工作管理員
- **Sysinternal**
  - ✓ Strings
  - ✓ TcpView
  - ✓ Filemon、Regmon
  - ✓ PsTools 、Process Monitor

IIS

- FTP、Web、SMTP、NNTP – 關閉、或移除其中不需要的服務
- IIS Lockdown
- URLScan

IIS (續)

- 更改預設的 Web 存放目錄
- 更改預設的 Log 存放位置
- 移除預設的 Web 站台
- 刪除不必要的預設目錄 (IISHelp、IISAdmin、IISSample、MSADC)
- 嚴格設定目錄權限(尤其是”寫入”)

FTP

- **Serv-U、G6、Filezilla、RaidenFTPD**
- **另外安裝的 FTP 服務，常成為主機遭入侵的入口**
- **權限限制**
- **加密**
- **帳戶分離**

DNS

- **Disable Zone Transfer**

- **CVE-2007-1748 (2007/03/29) – Buffer Overflow in Microsoft DNS Service, affect to**
  - ✓ **Microsoft Windows 2000 Server sp4**
  - ✓ **Microsoft Windows 2003 Server sp1 / sp2**

Terminal Service、VNC

- **Terminal Service –**
  - ✓ 限制可登入的帳號
  - ✓ 限制可登入的來源
  - ✓ 若要暴露在 Internet 上，則建議修改 Port (in registry)
- **VNC –**
  - ✓ 修改預設 Port
  - ✓ 加密
  - ✓ **CVE-2006-2369 (2006/05/15) – Bypass Authentication in RealVNC <= 4.1.1**

SQL Server

- **Service Pack**
- **僅可能切割各 DB 的讀、寫權限**
- **將一般用不到但功能強大的延伸程序刪除或限制操作者身份，如 sp_addextendedproc、sp_addlogin、sp_password、sp_addsrvrolemember、xp_cmdshell、xp_availablemedia、xp_dirtree、xp_servicecontrol、xp_subdirs ……等。**

問題與討論