

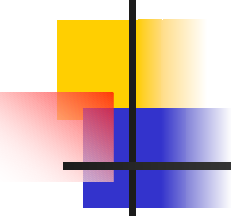
系統服務概念與安全弱點

主講人：林敬皇

密碼及網路安全研究室

URL: [HTTP://crypto.ee.ncku.edu.tw](http://crypto.ee.ncku.edu.tw)

Mail: gbox@crypto.ee.ncku.edu.tw

A decorative graphic on the left side of the slide, consisting of overlapping yellow, red, and blue squares with a black crosshair.

開始之前.....

- Process
- Server/Service
- 執行檔
- 程式
- 執行平台
- 啟動點
- Virus
- Worm
- Hacker Toolkits
- Trojan/back door
- Malicious code
- Exploit code



Process & Service

- 程序(Process)
 - 系統正在執行的程式
- 執行一次(Run Ones)
 - 只會在單一時間內佔用CPU資源用後即釋放
 - 大部分的命令屬於這樣的Process
- 常駐程式
 - Daemon
 - Super Daemon
 - Service (Windows 平台)



程序 (Process)

- process可以視為正在“執行”中的程式，一個process將會具有以下幾個屬性
 - exec thread
 - PID
 - Memory context
 - Environment
 - File descriptors
 - Security credential



常駐程式(Unix & Linux)

- Daemon
 - Server
 - 提供特定服務
 - Ex: web, smtp, ftp, ssh, vnc ...etc,.
- Super Daemon
 - 利用一程式來管理程序的啟動
 - Ex: ftp, telnet, pop3etc,.



常駐程式(Unix & Linux)

■ Daemon 啟動點

■ Runlevel

Run Level	說明
0	關機
1	單人模式 (single user mode) 除錯
2	多人使用模式，無網路功能 (關閉網路)
3	完整多人使用模式
4	未使用
5	完整多人使用模式，啟動圖形介面
6	重新開機 (reboot)



常駐程式(Unix & Linux)

- Super Daemon 啟動點
 - Inetd
 - /etc/inetd.conf
 - /etc/service
 - xinetd
 - /etc/xinetd.conf
 - /etc/xinetd.d



常駐程式(Unix & Linux)

■ Command

■ ps (System V / BSD)

- ps -elf/elf (System V)
- ps -aux/aux (BSD)

■ /Proc 虛擬目錄

- 儲存Process執行狀況
- 不是所有系統都有實作



```
gbox@cryptolab:~  
[gbox@cryptolab gbox]$ ps -aux  
Warning: bad syntax, perhaps a bogus '-'? See http://procps.sf.net/faq.html  
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND  
root         1   0.0   0.1   3048    464 ?        S      Aug20    0:06 init [3]  
root         2   0.0   0.0      0      0 ?        SWN    Aug20    0:00 [ksoftirqd/0]  
root         3   0.0   0.0      0      0 ?        SW<    Aug20    0:00 [events/0]  
root         4   0.0   0.0      0      0 ?        SW<    Aug20    0:00 [kblockd/0]  
root         6   0.0   0.0      0      0 ?        SW<    Aug20    0:00 [khelper]  
root         5   0.0   0.0      0      0 ?        SW     Aug20    0:00 [khubd]  
root         7   0.0   0.0      0      0 ?        SW     Aug20    0:02 [pdflush]  
root         8   0.0   0.0      0      0 ?        SW     Aug20    0:03 [pdflush]  
root        10   0.0   0.0      0      0 ?        SW<    Aug20    0:00 [aio/0]  
root         9   0.0   0.0      0      0 ?        SW     Aug20    0:04 [kswapd0]  
root       114   0.0   0.0      0      0 ?        SW     Aug20    0:00 [kseriod]  
root       153   0.0   0.0      0      0 ?        SW     Aug20    0:02 [kjournald]  
root       320   0.0   0.1   2644    292 ?        S<     Aug20    0:00 udevd  
root      1791   0.0   0.2   2584    596 ?        S      Aug20    0:00 syslogd -m 0  
root      1795   0.0   0.1   2516    456 ?        S      Aug20    0:00 klogd -x  
root      1894   0.0   0.5   5276   1472 ?        S      Aug20    0:03 /usr/sbin/sshd  
root      1907   0.0   0.4   5180   1196 ?        S      Aug20    0:00 /bin/sh /usr/bin/  
mysql     1932   0.0   2.6  31576   6696 ?        S      Aug20    0:00 /usr/libexec/mysq  
root     1954   0.0   6.4  32956  16108 ?        S      Aug20    0:02 /usr/sbin/httpd  
root     1965   0.0   0.2   2272    652 ?        S      Aug20    0:00 crond  
daemon   1984   0.0   0.2   3056    616 ?        S      Aug20    0:00 /usr/sbin/atd  
root     2005   0.0   0.1   2828    352 tty1     S      Aug20    0:00 /sbin/mingetty tt  
root     2012   0.0   0.1   2308    352 tty2     S      Aug20    0:00 /sbin/mingetty tt  
root     2013   0.0   0.1   2000    352 tty3     S      Aug20    0:00 /sbin/mingetty tt  
root     2014   0.0   0.1   2572    352 tty4     S      Aug20    0:00 /sbin/mingetty tt  
root     2015   0.0   0.1   2036    348 tty5     S      Aug20    0:00 /sbin/mingetty tt  
root     2016   0.0   0.1   2408    352 tty6     S      Aug20    0:00 /sbin/mingetty tt  
root    25392   0.0   0.2   2068    504 ?        S      Aug25    0:00 /usr/sbin/vsftpd  
apache    981   0.0   7.5  35028  18880 ?        S      04:05    0:00 /usr/sbin/httpd
```



```
gbox@cryptolab:/etc/xinetd.d
[gbox@cryptolab xinetd.d]$ pstree
init--+-atd
|   -crond
|   -events/0--+-aio/0
|               | -kblockd/0
|               | -khelper
|               `--2*[pdflush]
| -httpd---8*[httpd]
| -khubd
| -kjournald
| -klogd
| -kseriod
| -ksoftirqd/0
| -kswapd0
| -6*[mingetty]
| -safe_mysqld---mysqld
| -sshd---sshd---sshd---bash---pstree
| -syslogd
| -udevd
| `--vsftpd
[gbox@cryptolab xinetd.d]$
```



常駐程式(Windows)

■ 啟動點

■ 程式執行

- Windows Registry
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*
- HKEY_LOCAL_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- 啟動

■ C:\Documents and Settings\All Users\「開始」功能表\程式集\啟動

■ Service 啟動

- 註冊至Windows Registry
- HKEY_LOCAL_MACHINE\SYSTEM\Services



Windows 工作管理員

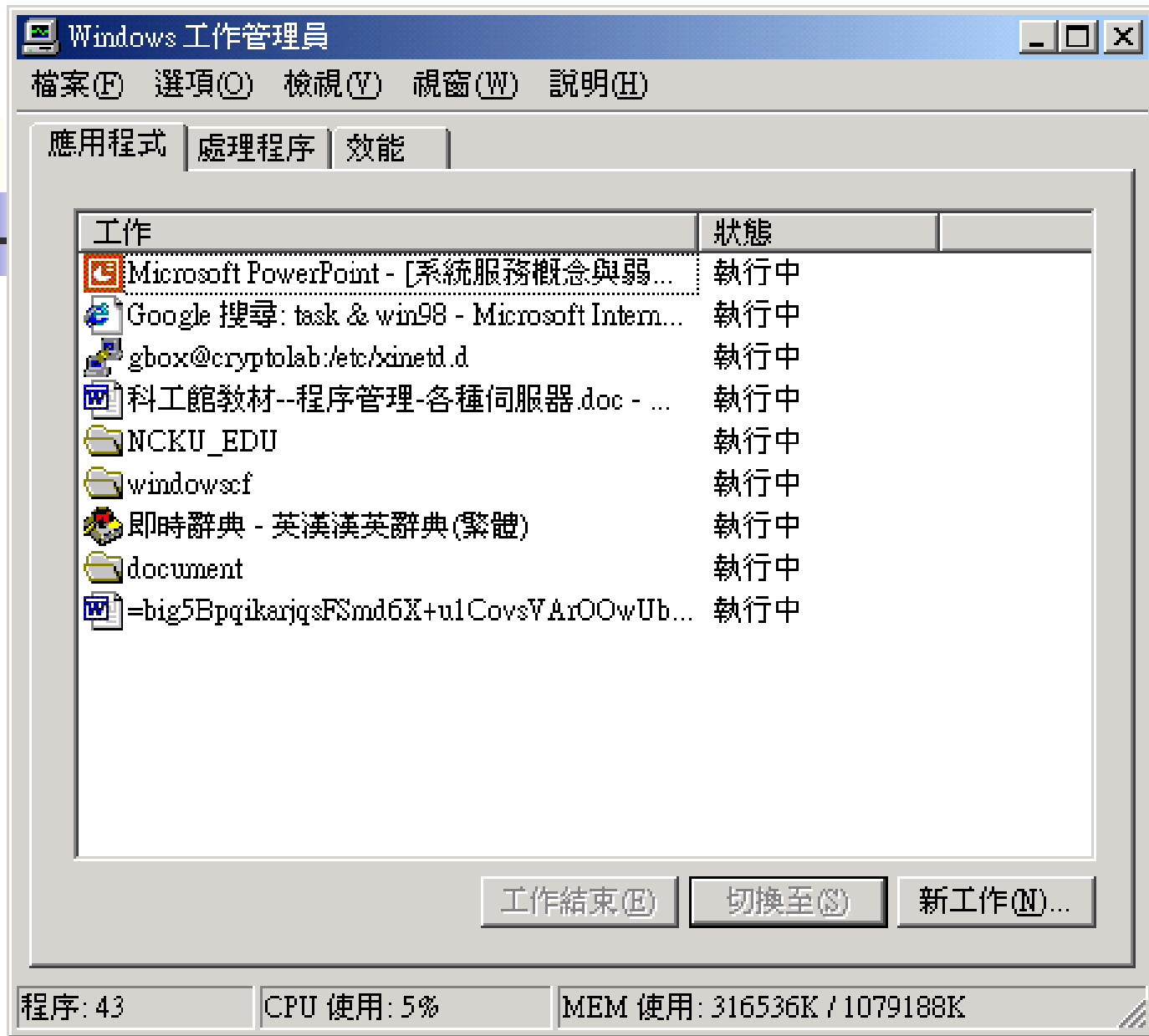
檔案(F) 選項(O) 檢視(V) 說明(H)

應用程式 處理程序 效能

影像名稱	PID	CPU	CPU 時間	記憶...
System Idle Process	0	99	2:50:16	16 K
System	8	00	0:00:20	276 K
SMSS.EXE	148	00	0:00:00	388 K
CSRSS.EXE	172	00	0:00:48	6,836 K
WINLOGON.EXE	192	00	0:00:02	560 K
SERVICES.EXE	220	00	0:00:03	6,844 K
LSASS.EXE	232	00	0:00:02	1,472 K
scardsvr.exe	368	00	0:00:00	1,352 K
svchost.exe	460	00	0:00:00	5,568 K
ccEvtMgr.exe	500	00	0:00:00	3,912 K
spoolsv.exe	584	00	0:00:01	5,732 K
svchost.exe	628	00	0:00:01	9,992 K
NAVAPSV.C.EXE	652	00	0:00:01	1,016 K
WINWORD.EXE	792	00	0:00:11	18,924 K
mstask.exe	804	00	0:00:00	5,040 K
stisvc.exe	816	00	0:00:00	1,764 K
vmware-authd.ex	904	00	0:01:06	3,476 K
vmnat.exe	912	00	0:00:00	2,836 K
vmtoolsd.exe	928	00	0:00:10	7,024 K

結束處理程序(E)

程序: 42 CPU 使用: 5% MEM 使用: 292460K / 1079188K





Windows Task Manager



File Options View Help

Applications

Processes

Performance

Networking

Image Name	User Name	CPU	Mem Usage
explorer.exe	dpouliot	01	15,184 K
svchost.exe	SYSTEM	00	11,276 K
WINWORD.EXE	dpouliot	00	10,428 K
IEXPLORE.EXE	dpouliot	00	10,192 K
taskmgr.exe	dpouliot	03	4,456 K
svchost.exe	LOCAL SERVICE	00	2,508 K
rtvscan.exe	SYSTEM	00	2,228 K
svchost.exe	SYSTEM	00	1,888 K
csrss.exe	SYSTEM	00	1,804 K
services.exe	SYSTEM	00	1,564 K
svchost.exe	NETWORK SERVICE	00	1,344 K
spoolsv.exe	SYSTEM	00	948 K
mdm.exe	SYSTEM	00	900 K
svchost.exe	SYSTEM	00	896 K
lsass.exe	SYSTEM	00	644 K
winlogon.exe	SYSTEM	00	624 K
ctfmon.exe	dpouliot	00	600 K
vptray.exe	dpouliot	00	476 K
evntsvc.exe	dpouliot	00	128 K
TaskSwitch.exe	dpouliot	00	104 K
MSGSYS.EXE	SYSTEM	00	76 K
defwatch.exe	SYSTEM	00	64 K
smss.exe	SYSTEM	00	48 K
System	SYSTEM	00	40 K
System Idle Process	SYSTEM	96	20 K

☐ Show processes from all users

End Process

Processes: 25

CPU Usage: 4%

Commit Charge: 126496K / 6318K



Close Program

Microsoft Word - Windows 98.doc [Not Responding]

Exploring - Lecture Notes

Explorer

Msimn

Lwpevntm

Avconsol

Reminder

Mswheel

Systray

Vsstat

Vshwin32

WARNING: Pressing CTRL+ALT+DEL again will restart your computer. You will lose unsaved information in all programs that are running.

End Task

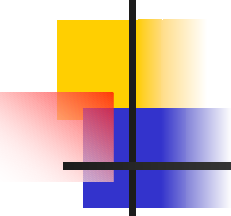
Shut Down

Cancel



Server (伺服器)& Service(服務)

- Server (伺服器)
 - 應用套件
 - 提供處理及回應的程式
- Service(服務)
 - 特定的處理作業
 - 完整的處理程序
 - 可能包含許多Server

A decorative graphic on the left side of the slide, consisting of overlapping yellow, red, and blue squares with a black crosshair.

常見的服務

- Web
 - Would Wide Web
- Mail
 - SMTP
 - POP 2/3
 - IMAP
- NFS
- DNS
- Remote Control
- SNMP



Windows process manager

- 工作管理員(Taskmgr)
- Other Tools
 - Pstools-pslist
 - <http://www.sysinternals.com/ntw2k/freeware/pstools.shtml>
 - Process Explorer
 - <http://www.sysinternals.com/ntw2k/freeware/processexp.shtml>



Process status

■ ALT + CTRL + DEL 呼叫工作管理員

Windows 工作管理員

檔案(F) 選項(O) 檢視(V) 說明(H)

應用程式 處理程序 效能

影像名稱	PID	CPU	CPU 時間	記憶...
System Idle Process	0	97	2:19:39	16 K
System	8	01	0:00:23	276 K
SMSS.EXE	148	00	0:00:00	388 K
CSRSS.EXE	172	00	0:01:02	5,780 K
WINLOGON.EXE	192	00	0:00:01	404 K
SERVICES.EXE	220	00	0:00:04	6,860 K
LSASS.EXE	232	00	0:00:02	1,432 K
scardsvr.exe	368	00	0:00:00	1,352 K
svchost.exe	460	00	0:00:00	5,632 K
ccEvtMgr.exe	492	00	0:00:00	3,916 K
spoolsv.exe	576	00	0:00:01	5,344 K
svchost.exe	620	00	0:00:01	9,980 K
svchost.exe	636	00	0:00:00	7,316 K
NAVAPSWC.EXE	644	00	0:00:02	4,612 K
TASKMGR.EXE	656	02	0:00:00	5,232 K
explorer.exe	684	00	0:00:29	3,852 K
LTSMMSG.exe	728	00	0:00:00	1,604 K
mstask.exe	780	00	0:00:00	5,076 K
ctfmon.exe	792	00	0:00:00	1,764 K

結束處理程序(E)

程序: 34 CPU 使用: 7% MEM 使用: 259032K / 1079176K

試著關閉正在執行的
應用程式測試是否有
異常的process

System Idle Process
正常應保持在95以上



Process status

- Pstools-pslist

- <http://www.sysinternals.com/ntw2k/freeware/pstools.shtml>

- Process Explorer

- <http://www.sysinternals.com/ntw2k/freeware/procexp.shtml>



Pstools-pslist

```
C:\WINNT\system32\cmd.exe
PsList 1.24 - Process Information Lister
Copyright (C) 1999-2002 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for ALLEN-NB:

Name           Pid Pri Thd  Hnd      Mem      User Time      Kernel Time      Elapsed Time
Idle            0   0   1    0        16      0:00:00.000      2:29:18.121      2:52:08.401
System          8   8  37  314       276      0:00:00.000      0:00:23.964      2:52:08.401
SMSS           148  11   6   33       388      0:00:00.010      0:00:00.761      2:52:08.401
CSRSS          172  13  10  445      6188      0:00:01.341      0:01:13.345      2:51:58.337
WINLOGON       192  13  19  409       772      0:00:00.270      0:00:01.231      2:51:54.391
SERVICES       220   9  35  557      6924      0:00:02.002      0:00:02.523      2:51:51.727
LSASS          232   9  16  313      1400      0:00:01.412      0:00:01.311      2:51:51.627
scardsvr       368   8   5   64      1352      0:00:00.020      0:00:00.420      2:51:47.681
svchost        460   8  10  308      5632      0:00:00.320      0:00:00.570      2:51:45.278
ccEvtMgr       492   8  17  293      3916      0:00:00.120      0:00:00.500      2:51:36.225
spoolsv        576   8  14  185      5344      0:00:00.160      0:00:01.261      2:51:33.921
svchost        620   8  30  495     10036      0:00:00.330      0:00:01.231      2:51:30.557
NAVAPSUC       644   8   9  113      6588      0:00:00.941      0:00:01.832      2:51:29.495
mstask         780   8   7  128      5076      0:00:00.040      0:00:00.470      2:51:20.142
stisvc         792   8   4   56      1764      0:00:00.030      0:00:00.380      2:51:19.591
vmware-auth    880   8   5  109      3476      0:00:13.970      0:00:36.322      2:51:18.659
vmnat          904   8   4   82      2832      0:00:00.020      0:00:00.340      2:51:17.077
WinMgmt        952   8   4  121       572      0:00:05.918      0:00:00.590      2:51:14.824
```



Process Explorer

Process Explorer - Sysinternals: www.sysinternals.com				
File Options View Process Find Handle Help				
Process				
PID	C...	Description	Company Name	
0	91			
Interrupts	n/a	Hardware Interrupts		
DPCs	n/a	Deferred Procedure Calls		
8				
System				
SMSS.EXE	148	Windows NT Session Manager	Microsoft Corporation	
CSRSS.EXE	172	Client Server Runtime Process	Microsoft Corporation	
WINLOGON.E...	192	1 Windows NT Logon Application	Microsoft Corporation	
SERVICES.E...	220	Services and Controller app	Microsoft Corporation	
260				
Type	Name	Handle	Access	
Desktop	\Default	0x12C	0x000F01FF	
Desktop	\Default	0x440	0x000F01FF	
Desktop	\Default	0x6B8	0x000F01FF	
Directory	\KnownDlls	0x14	0x00000003	
Directory	\Windows	0x1C	0x000F000F	
Directory	\BaseNamedObjects\Restricted	0x2C	0x000F000F	
Directory	\BaseNamedObjects	0x30	0x000E000E	
CPU Usage: 9% Commit Charge: 29.66% Own Commit Charge: 14.72%				



Unix/Linux process manager

- Process Status
 - ps command (ps package)
 - ps -elf (SystemV)
 - Ps aux (BSD)
- lsof
- /proc
 - Cmdline



ps command

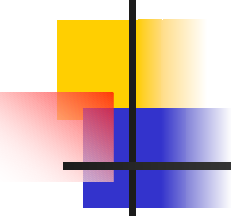
```
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1   0.8   0.3  1372   472 ?        S      02:48    0:05 init
root         2   0.0   0.0     0     0 ?        SW     02:48    0:00 [keventd]
root         3   0.0   0.0     0     0 ?        SW     02:48    0:00 [kapmd]
root         4   0.0   0.0     0     0 ?        SWN    02:48    0:00 [ksoftirqd_CPU0]
root         9   0.0   0.0     0     0 ?        SW     02:48    0:00 [bdflush]
root         5   0.0   0.0     0     0 ?        SW     02:48    0:00 [kswapd]
root         6   0.0   0.0     0     0 ?        SW     02:48    0:00 [kscand/DMA]
root         7   0.0   0.0     0     0 ?        SW     02:48    0:00 [kscand/Normal]
root         8   0.0   0.0     0     0 ?        SW     02:48    0:00 [kscand/HighMem]
root        10   0.0   0.0     0     0 ?        SW     02:48    0:00 [kupdated]
root        11   0.0   0.0     0     0 ?        SW     02:48    0:00 [mdrecoveryd]
root        19   0.0   0.0     0     0 ?        SW     02:48    0:00 [kjournald]
root        77   0.0   0.0     0     0 ?        SW     02:48    0:00 [khubd]
root       1178   0.0   0.0     0     0 ?        SW     02:49    0:00 [kjournald]
root       1525   0.0   0.4   1444   536 ?        S      02:49    0:00 syslogd -m 0
root       1529   0.0   0.3   1364   416 ?        S      02:49    0:00 klogd -x
root       1579   0.0   1.1   3508  1496 ?        S      02:49    0:00 /usr/sbin/sshd
root       1590   0.0   0.6   2028   800 ?        S      02:49    0:00 xinetd -stayalive
      -reuse -pidfile /var/run/xinetd.pid
root       1599   0.0   0.4   1420   564 ?        S      02:49    0:00 crond
root       1608   0.0   0.4   1392   604 ?        SN     02:49    0:00 anacron -s
root       1614   0.0   0.7   2260   976 ?        S      02:49    0:00 login -- root
```

:_



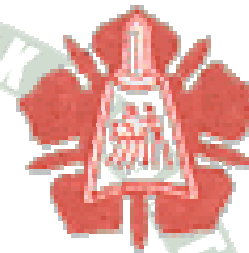
Isof command

```
syslogd 1525 root rtd DIR 8,3 4096 2 /
syslogd 1525 root txt REG 8,3 27424 319639 /sbin/syslogd
syslogd 1525 root mem REG 8,3 103044 239633 /lib/ld-2.3.2.so
syslogd 1525 root mem REG 8,3 52472 239654 /lib/libnss_files-
2.3.2.so
syslogd 1525 root mem REG 8,3 1531064 415303 /lib/tls/libc-2.3.
2.so
syslogd 1525 root 0u unix 0xc7fe0a80 1657 /dev/log
syslogd 1525 root 1w REG 8,3 15787 419390 /var/log/messages
syslogd 1525 root 2w REG 8,3 146 419409 /var/log/secure
syslogd 1525 root 3w REG 8,3 0 419411 /var/log/maillog
syslogd 1525 root 4w REG 8,3 764 419414 /var/log/cron
syslogd 1525 root 5w REG 8,3 0 419412 /var/log/spooler
syslogd 1525 root 6w REG 8,3 840 419413 /var/log/boot.log
klogd 1529 root cwd DIR 8,3 4096 2 /
klogd 1529 root rtd DIR 8,3 4096 2 /
klogd 1529 root txt REG 8,3 22332 319638 /sbin/klogd
klogd 1529 root mem REG 8,3 103044 239633 /lib/ld-2.3.2.so
klogd 1529 root mem REG 8,3 1531064 415303 /lib/tls/libc-2.3.
2.so
klogd 1529 root 0r REG 0,2 0 4113 /proc/kmsg
klogd 1529 root 1u unix 0xc7faa580 1667 socket
sshd 1579 root cwd DIR 8,3 4096 2 /
sshd 1579 root rtd DIR 8,3 4096 2 /
```

A decorative graphic on the left side of the slide, consisting of overlapping yellow, red, and blue squares with a black crosshair.

Ref.

- Windows XP服務功能詳解
 - <http://www.msservermag.com.tw/>
- Windows Server 2000 Security Guide
 - <http://www.microsoft.com/windowsserversystem/default.mspx>



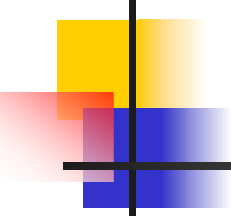
安全弱點 Security Vulnerability





大綱

- 安全弱點?
- 安全弱點分類
 - 形成原因
 - 弱點運用方式
 - 結果
- 弱點資料庫
- 弱點命名與編號
- 修正方式

A decorative graphic consisting of overlapping yellow, red, and blue squares with a black crosshair is positioned to the left of the title.

什麼是安全弱點？

- A flaw in a computer or network allowing unauthorized use or unauthorized access.
- Ignorance or errors in process of programming or configurations which lead to security problems



安全弱點分類

- 便於

- 了解原因
- 解決問題

- 依據

- 形成原因
- 弱點運用(攻擊)的方法
- 可能造成的結果



形成原因(1)

■ Design Phase

- 脆弱的演算法(Weak algorithm)
- 設計錯誤(Design error)

■ Implementation Phase

- 輸入驗證的錯誤 (Input validation error)
- 界限(範圍)檢查的錯誤 (Boundary check error)
- 競爭情況(Race condition)



形成原因(2)

- Operation Phase
 - 設定錯誤(Configuration error)
- Human Nature
 - 脆弱的密碼(Weak Passwords)
 - 不良的使用習慣(Unsafe habits)
 - Etc.....,



脆弱的演算法(Weak algorithm)

- 設計時
 - 忽略的
 - 未考慮
- Eg:
 - TCP CheckSums
 - 早期的密碼演算法
 - Etc.,



設計錯誤(Design error)

- 設計時
 - 疏忽的
 - 未考慮的
- E.g:
 - 錯誤的資料型態
 - 無窮迴圈
 - Etc,.



輸入驗證的錯誤

- 沒有檢查輸入的值
- 資料型態
- E.g:
 - SQL Injection
 - ISC BIND 4 - nslookupComplain()問題



界限(範圍)檢查的錯誤

- 未正確檢查傳入資訊的長度，導致換衝區溢位或程式計算錯誤
- E.g:
 - Fetchmail - header parsing function readheaders()問題



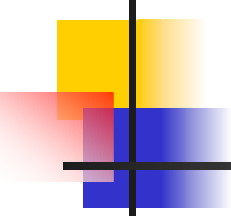
競爭情況

- 指多個處理元同時並行（**Concurrent**）存取共用資源，系統依排程次序執行，而造成資源內的資料不正確的問題發生。
- E.g:
 - Redhat LogWatch新增暫存目錄時 race condition
 - *Linux 核心 2.2.x ~ 2.4.x - kmod.c 有競行(race condition)的安全漏洞 ptrace*



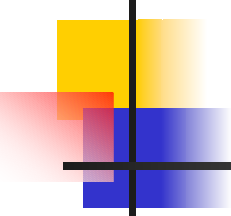
設定錯誤

- 疏忽
- 不知道
- E.g:
 - Web Server 設定可瀏覽檔案
 - 所有人都可寫入權限(Would witted)

A decorative graphic on the left side of the slide, consisting of overlapping yellow, red, and blue squares with a black crosshair.

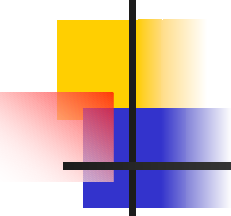
Human Nature

- 脆弱的密碼(Weak Passwords)
 - Username
 - 生日
 - 1234
 - 1111
- 不良的使用習慣(Unsafe habits)
 - 將密碼告訴別人
 - 寫下貼在桌面上
- Etc.,

A decorative graphic on the left side of the slide, consisting of overlapping yellow, red, and blue squares with a black crosshair.

弱點運用方式

- Bruce Force,
 - Resource Exhausting,
 - Buffer Overflow
 - Format String
 - TCP Spoofing
 - TCP Hijacking, ...etc.
-
- Social Engineering

A decorative graphic consisting of overlapping yellow, red, and blue squares with a black crosshair is positioned to the left of the title.

Bruce Force

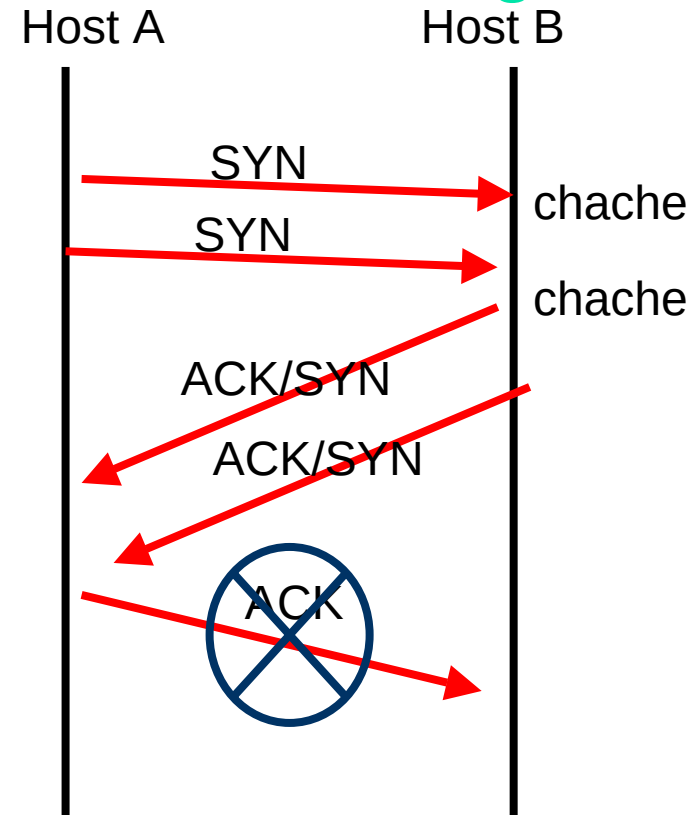
- 攻擊密碼機制
- 演算法弱點
- 實體入侵破壞
- Etc,.



Resource Exhausting

- SYN Flooding..
- 耗盡運算資源
- 耗盡記憶體資源
- 網路無法連接
- 程式執行緩慢
- 填滿硬碟空間
- Etc,.

SYN Flooding

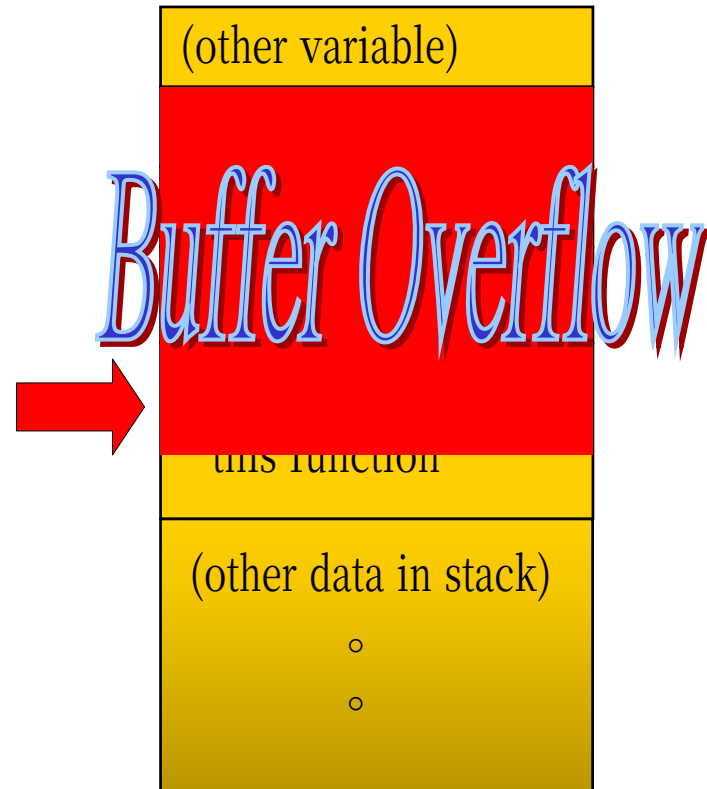




Buffer Overflow

function 被呼叫時

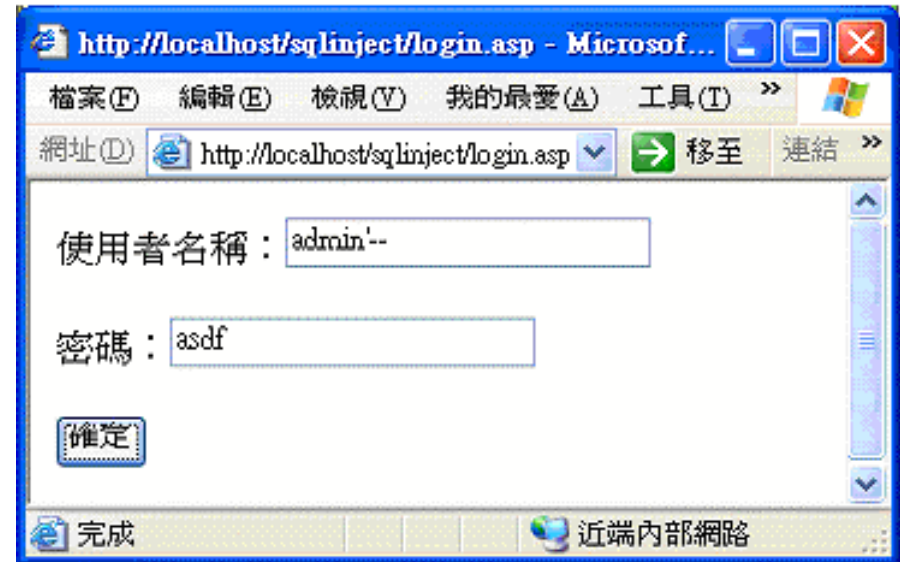
```
int func() {  
    int i, j, k;  
    char buf[16];  
    struct abc *x, *y, *z;  
    ... }  
}
```





Format String

■ 以 SQL Injection為例



'利用使用者輸入的資料來組合 SQL 語法

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

```
Set rec=.Execute(strSQL)
```



Format String

■ 以 SQL Injection為例

- 原來正常輸入語法

```
strSQL="SELECT * FROM tblUser WHERE UserName='admin' AND  
Password='1234 '"
```

Set rec=.Execute(strSQL) ➔ 執行正常

在使用者名稱處輸入：admin '--
會變成

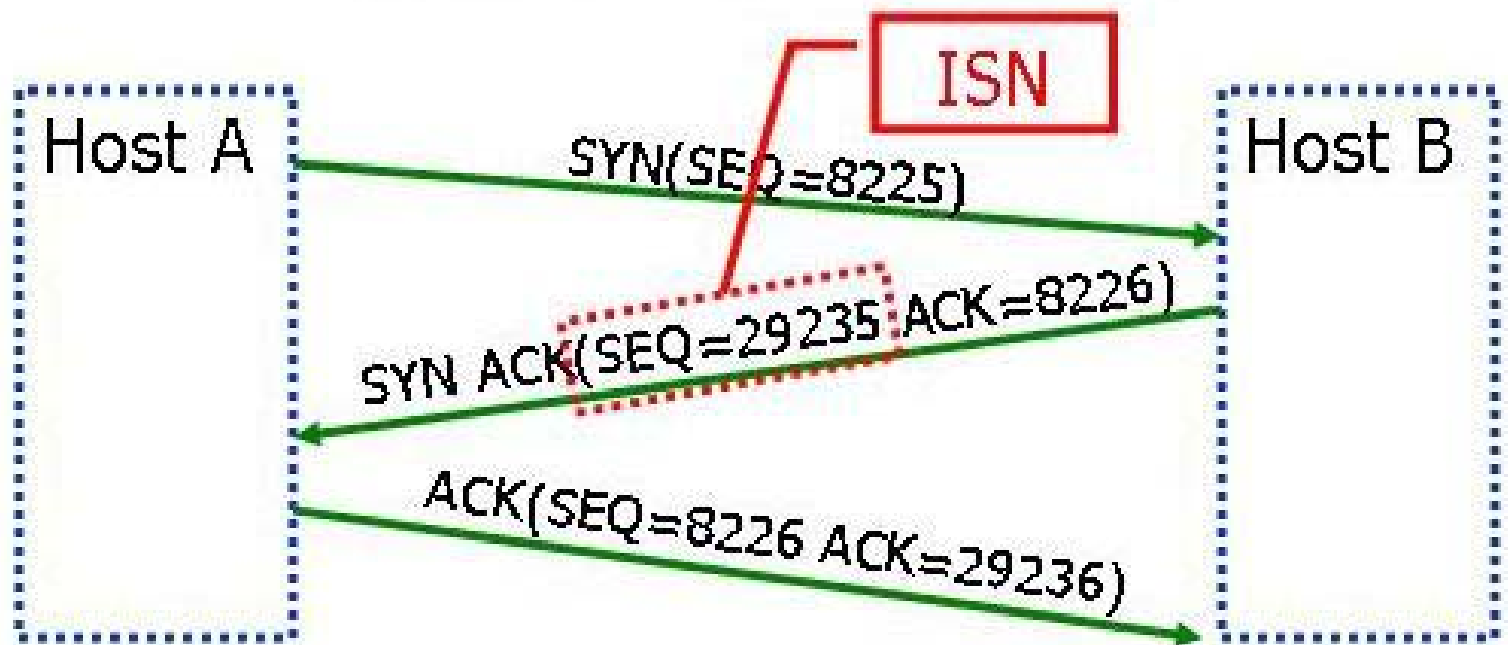
```
strSQL="SELECT * FROM tblUser WHERE UserName='admin'--' AND  
Password='1234'"
```

Set rec=.Execute(strSQL) ➔ 原先的 AND 子句被 "--" 標示成說明也就是只執行

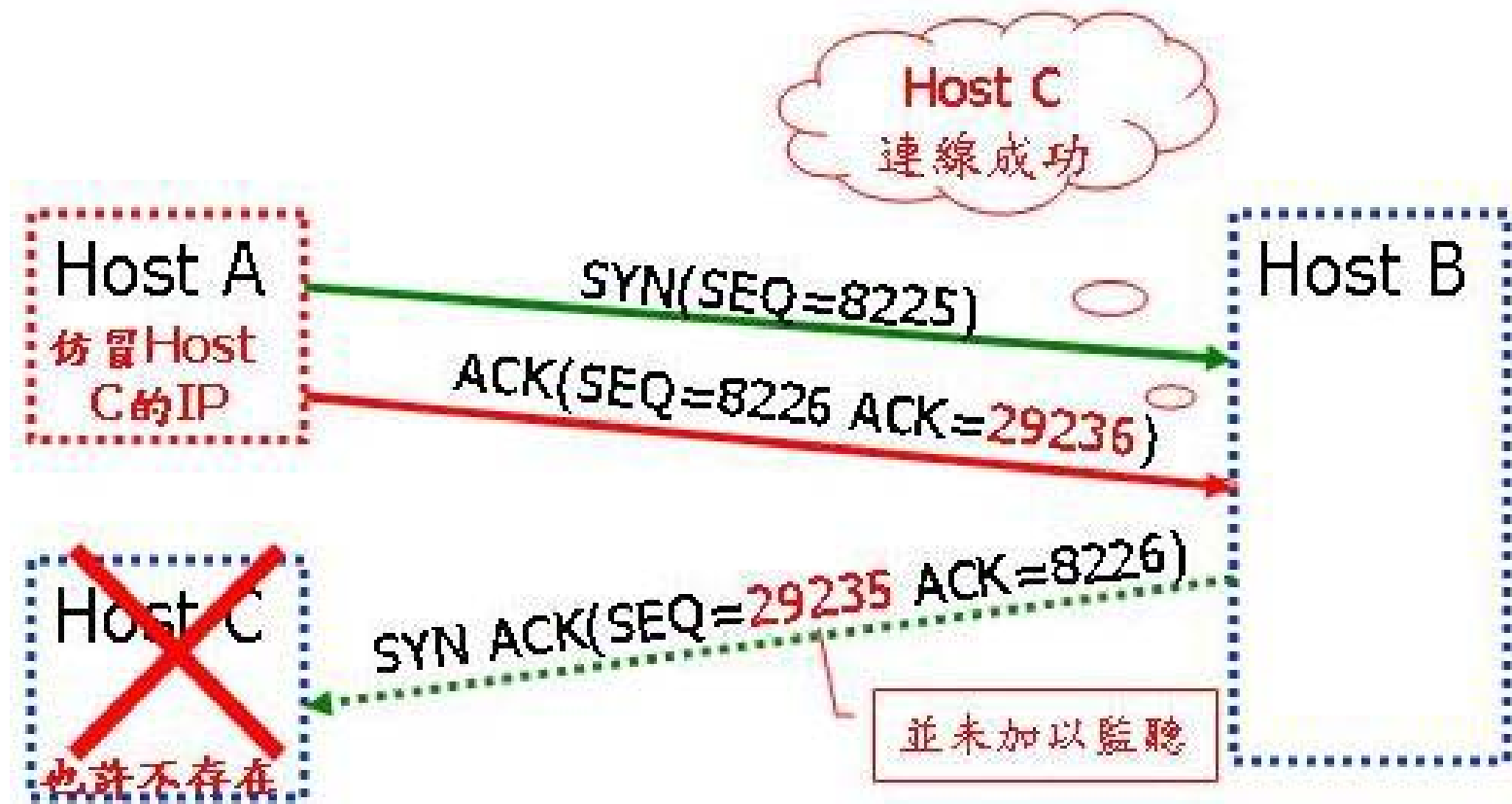
SELECT * FROM tblUser WHERE UserName='admin'

並且通過驗證

TCP Spoofing

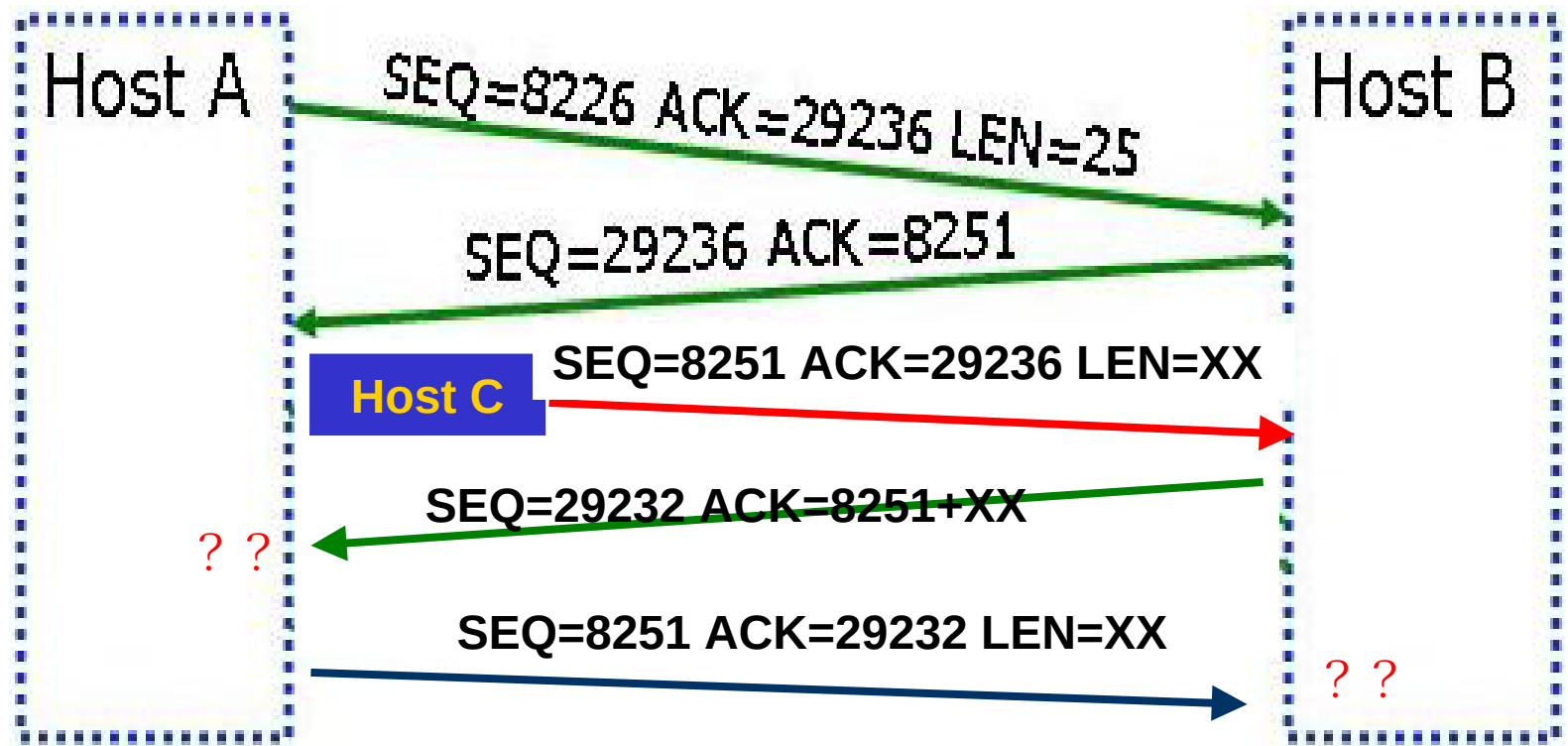


TCP Spoofing





TCP Hijacking





Social Engineering

- 利用人性上的弱點
 - 同情心
- 利用心理上的弱點
 - 欺騙
 - 偽裝
 - 其它...等



造成的結果

- 程式錯誤(Program Error)
- 取得權限(Gain Privilege)
- 阻斷服務攻擊(Denial of Service)
- 資訊洩漏/竊取/破壞/竄改
(Information Leakage / Corruption)
- 後門/木馬
(Backdoor / Trojan)



弱點資料庫

- 蒐集整理安全弱點相關資料
 - 發生原因
 - 攻擊方法
 - 造成的結果
 - 修正方式....等等.
- E.g.
 - CERT Advisory-包含弱點的 描述、重要性、影響系統、如何修補 ...等,.
 - Whithats- Snort IDS偵測的特徵
 - Nessus plugins archives – Nessus 掃描的稽核檔



弱點命名與編號

- 便於索引、搜尋、描述弱點
- 編號種類
 - CERT/CC Vulnerability Note;
 - Bugtraq ID,
 - ISS X-Force: Name& number, ...etc.
- CVE 編號 (Common Vulnerabilities and Exposures)
 - 起源:編號種類繁多，不易對照
 - Dictionary
 - CVE Compatible
 - <http://cve.mitre.org/>



弱點資料庫

- Common Vulnerabilities and Exposures
 - <http://cve.mitre.org/>
- SecurityFocus Vulnerabilities
 - <http://www.securityfocus.com/bid>
- X-Force™ Database
 - <http://xforce.iss.net/xforce/search.php>
- Whitehats arachNIDS
 - <http://whitehats.com/ids/index.html>
- CERT/CC Vulnerability Notes Database
 - <http://www.kb.cert.org/vuls>



Top Vulnerabilities to Windows Systems

- W1 Internet Information Services (IIS)
- W2 Microsoft SQL Server (MSSQL)
- W3 Windows Authentication
- W4 Internet Explorer (IE)
- W5 Windows Remote Access Services
- W6 Microsoft Data Access Components (MDAC)
- W7 Windows Scripting Host (WSH)
- W8 Microsoft Outlook and Outlook Express
- W9 Windows Peer to Peer File Sharing (P2P)
- W10 Simple Network Management Protocol (SNMP)





Top Vulnerabilities to UNIX Systems



- U1 BIND Domain Name System
- U2 Remote Procedure Calls (RPC)
- U3 Apache Web Server
- U4 General UNIX Authentication Accounts with No Passwords or Weak Passwords
- U5 Clear Text Services
- U6 Sendmail
- U7 Simple Network Management Protocol (SNMP)
- U8 Secure Shell (SSH)
- U9 Misconfiguration of Enterprise Services NIS/NFS
- U10 Open Secure Sockets Layer (SSL)



弱點修正方式(1)

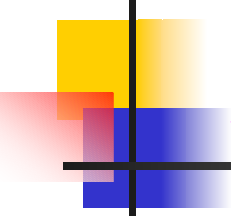
■ 軟體

- 安裝修補軟體
- 安全的設定
- 關閉不必要的服務
- 升級正確的軟體



弱點修正方式(2)

- 安全的使用習慣
 - 強韌的密碼
 - 不要開啟來路不明的郵件檔案
 - 不要將密碼寫下
- 軟體發展流程 — 減少軟體發展時所產生的弱點

A decorative graphic on the left side of the slide, consisting of overlapping yellow, red, and blue squares with a black crosshair.

Antivirus software

- 保持防毒軟體的開啟
- 保持防毒軟體病毒碼的更新



MBSA

- Microsoft Baseline Security Analyzer
- 最新版本 MBSA Version 1.2
- 特色：
 - 檢查安全不當設定，檢查安全更新
- 支援產品平台
 - Windows XP Home Edition/Professional
 - Windows 2000 Professional/Server
 - Windows Server 2003
- 可同時掃描一部或多部電腦
 - 可指定IP 網段或網域或電腦名稱
- 免費下載
 - <http://www.microsoft.com/technet/security/tools/mbsahome.msp>
 - 透過圖形化界面及圖示顯示分析結果

掃描我的電腦有哪些安全弱點？



Microsoft Baseline Security Analyzer

Microsoft
Baseline Security Analyzer

Microsoft Baseline Security Analyzer

- ☐ Welcome
- ☐ Pick a computer to scan
- ☐ Pick multiple computers to scan
- ☐ Pick a security report to view
- ☒ View a security report

See Also

- ☐ Microsoft Baseline Security Analyzer Help
- ☐ About Microsoft Baseline Security Analyzer
- ☐ Microsoft Security Web site

Actions

- Print
- Copy

View security report

Sort Order:

Score	Issue	Result
	Office Security Updates	2 security updates are missing. What was scanned Result details How to correct this
	MSXML Security Updates	1 security updates are out-of-date. What was scanned Result details How to correct this
	Windows Security Updates	3 security updates could not be confirmed. What was scanned Result details How to correct this
	IIS Security Updates	No critical security updates are missing. What was scanned
	Windows Media Player Security Updates	No critical security updates are missing. What was scanned
	MDAC Security Updates	No critical security updates are missing. What was scanned

Previous security report [Next security report](#)

© 2002-2004 Microsoft Corporation. © 2002-2004 Shavlik Technologies, LLC. All rights reserved.



弱點修補

■ Unix/Linux

- Tar ball recompiler
- Package manager Update

■ Windows

- Windows Update
- Auto Update(win98SE,W2K sp4,WinXP,Win 2003)
- Download patch