信祥事業群 Network 常識-資訊系統安全策略(Issue 01)

重要觀念：不管任何網路系統，均會有發信站與收信站。

入侵者的追蹤 (Intruder Tracing)

在區域網路上可能你聽過所謂「廣播模式」的資料發送方法，此種方法不指定收信站，只要和此網路連結的所有網路設備皆爲收信對象。但是這僅僅在區域網路上能夠實行，因爲區域網路上的機器不多(和 Internet 比起來)。如果想是 Internet 上有數千萬的主機，根本就不可能實施資料廣播(至於 IP Multicast 算是一種限定式廣播 Restricted Broadcast，唯有被指定的機器會收到，Internet 上其他電腦還是不會收到)。假設 Internet 上可以實施非限定廣播，那隨便一個人發出廣播訊息，全世界的電腦皆受其影響，豈不世界大亂？因此，任何區域網路內的路由器或是類似網路設備都不會將自己區域網路內的廣播訊息轉送出去。萬一在 WAN Port 收到廣播訊息，也不會轉進自己的 LAN Port 中。

而既然網路皆有發信站與收信站，用以標示資訊發送者與資訊接收者，除非對方使用一些特殊的封包封裝方式或是使用防火牆對外連線，那麼只要有人和你的主機進行通訊(寄信或是 telnet、ftp 過來都算)你就應該會知道對方的位址，如果對方用了防火牆來和你通訊，你最少也能夠知道防火牆的位址。也正因爲只要有人和你連線，你就能知道對方的位址，那麼要不要知道對方位址只是要做不做的問題而已。如果對方是透過一台 UNIX 主機和你連線，則你更可以透過 ident 查到是誰和你連線的。在實行 TCP/IP 通訊協定的電腦上，通常可以用 netstat 指令來看到目前連線的狀況。在下面的連線狀況中，netstat 指令是在 win95 上實行的，可以看到目前自己機器(Local Address 處)的 telnet port 有一台主機 workstation.variox.int 由遠端(Foreign Address 處)連線進來並且配到 1029 號 tcp port.而 ccunix1 主機也以 ftp port 連到 workstation.variox.int 去。所有的連線狀況看得一清二楚。(如 A、 B) A.在 UNIX 主機 (ccunix1.variox.int)看 netstat

B.另一端在 Windows 95(workstation.variox.int) 看 netstat

雖然是不同的作業系統，但 netstat 是不是長得很像

呢 ？

通 信 過 程 的 紀 錄 設 定

如 果 想 要 把 網 路 連 線 紀 錄 給 記 錄 下 來 ， 你 可 以 用 cron table 定 時 去 跑 ：

```
netstat > > filename
```

但 是 UNIX 系 統 早 已 考 慮 到 這 一 個 需 求 ， 因 此 在 系 統 中 有 一 個 專 職 記 錄 系 統 事 件 的 Daemon: syslogd，在 UNIX 系 統 的 /var/adm 下 面 有 兩 個 系 統 紀 錄 檔 案 ： syslog 與 messages，一 個 是 一 般 系 統 的 紀 錄 ， 一 個 是 核 心 的 紀 錄 。

系 統 的 紀 錄 基 本 上 都 是 由 syslogd(System Kernel Log Daemon) 來 產 生 ， 而 syslogd 的 控 制 是 由 /etc/syslog.conf 來 做 的 。 syslog.conf 以 兩 個 欄 位 來 決 定 要 記 錄 哪 些 東 西 ， 以 及 記 錄 到 哪 邊 去 。 下 面 是 一 個 Linux 系 統 所 附 上 的 syslog.conf 檔 案 ， 這 也 是 一 個 最 標 準 的 syslog.conf 寫 法 ： 格 式 就 是 這 樣 子 ， 第 一 欄 寫「 在 什 麼 情 況 下 」以 及 「 什 麼 程 度 」 。 然 後 用 TAB 鍵 跳 下 一 欄 繼 續 寫 「 符 合 條 件 以 後 要 做 什 麼 」 。 這 個 syslog.conf 檔 案 只 能 用 TAB 來 作 各 欄 位 之 間 的 分 隔。

第 一 欄 包 含 了 何 種 情 況 與 程 度 ， 中 間 小 數 點 分 隔 。 另 外 ， 星 號 就 代 表 了 某 一 細 項 中 的 所 有 選 項 。 詳 細 的 設 定 方 式 如 下 ：

1. 在 什 麼 情 況 ： 各 種 不 同 的 情 況 以 下 面 的 字 串 來 決 定 。

auth	關 於 系 統 安 全 與 使 用 者 認 證 方 面
cron	關 於 系 統 自 動 排 程 執 行 (Cron Table)方 面
daemon	關 於 背 景 執 行 程 式 方 面
kern	關 於 系 統 核 心 方 面
lpr	關 於 印 表 機 方 面
mail	關 於 電 子 郵 件 方 面
news	關 於 新 聞 討 論 區 方 面
syslog	關 於 系 統 紀 錄 本 身 方 面
user	關 於 使 用 者 方 面

uucp	關於UNIX互拷(UUCP)方面

上面是大部份的UNIX系統都會有的情況，而有些UNIX系統可能會再分出不同的項目出來。

2. 什麼程度才記錄：下面是各種不同的系統狀況程度，依照輕重緩急排列。

none	不要記錄這一項
debug	程式或系統本身除錯訊息
info	一般性資訊
notice	提醒注意性
err	發生錯誤
warning	警告性
crit	較嚴重的警告
alert	再嚴重一點的警告
emerg	已經非常嚴重了

同樣地，各種UNIX系統可能會有不同的程度表示方式。有些系統是不另外區分crit與alert的差別，也有的系統會有更多種類的程度變化。在記錄時，syslogd會自動將你所設定程度以及其上的都一併記錄下來。

例如若你要系統去記錄info等級的事件，則notice、err.warning、crit、alert、emerg等在info等級以上的也會一併被記錄下來。把上面所寫的1、2項以小數點組合起來就是完整的「要記錄哪些東西」的寫法。例如mail.info表示關於電子郵件傳送系統的一般性訊息。auth.emerg就是關於系統安全方面相當嚴重的訊息。lpr.none表示不要記錄關於列表機的訊息(通常用在有多個紀錄條件時組合使用)。另外有三種特殊的符號可供應用：

1. 星號(*)

星號代表某一細項中所有項目。例如mail.*表示只要有關mail的，不管什麼程度都要記錄下來。而*.info會把所有程度爲info的事件給記錄下來。

2. 等號 (=)
等號表示只記錄目前這一等級，其上的等級不要記錄。例如剛剛的例子，平常寫下 info 等級時，也會把位於 info 等級上面的 notice、 err.warning、 crit、 alert、 emerg 等其他等級也記錄下來。但若你寫 =info 則就只有記錄 info 這一等級了。
3. 驚嘆號 (!)
驚嘆號表示不要記錄目前這一等級以及其上的等級。

記錄到哪邊去

一般的 syslogd 都提供下列的管道以供您記錄系統發生的什麼事：

1. 一般檔案
這是最普遍的方式。你可以指定好檔案路徑與檔案名稱，但是必須以目錄符號「/」開始，系統才會知道這是一個檔案。例如 /var/adm/maillog 表示要記錄到 /var/adm 下面一個稱爲 maillog 的檔案。如果之前沒有這個檔案，系統會自動產生一個。

2. 指定的終端機或其他設備
也可以將系統紀錄寫到一個終端機或是設備上。若將系統紀錄寫到終端機，則目前正在使用該終端機的使用者就會直接在螢幕上看到系統訊息 (例如 /dev/console 或是 /dev/tty1.可以拿一個螢幕專門來顯示系統訊息)。若將系統紀錄寫到印表機，則會有一長條印滿系統紀錄的紙 (例如 /dev/lp0)。

3. 指定的使用者
也可以在這邊列出一串使用者名稱，則這些使用者如果正好上線的話，就會在他的終端機上看到系統訊息 (例如 root，注意寫的時候在使用者名稱前面不要再加上其他的字)。

4. 指定的遠端主機
這種寫法不將系統訊息記錄在連接本地機器上，而記錄在其他主機上。有些情況系統碰到的是硬

碟錯誤，或是萬一有人把主機推倒，硬碟摔壞了，那你要到哪邊去拿系統紀錄來看呢？而網路卡只要你不把它折斷，應該是比硬碟機耐摔得多了。因此，如果你覺得某些情況下可能紀錄沒辦法存進硬碟裡，你可以把系統紀錄丟到其他的主機上。如果你要這樣做，你可以寫下主機名稱，然後在主機名稱前面加上「@」符號(例如@ccunix1.variox. int，但被你指定的主機上必須要有syslogd)。

在以上各種紀錄方式中，都沒有電子郵件這項。因爲電子信件要等收件者去收信才看得到，有些情況可能是很緊急的，沒辦法等你去拿信來看(BSD的Manual Page寫著「when you got mail, it’s already too late...」:-P)。

以上就是syslog各項紀錄程度以及紀錄方式的寫法，可以依照自己的需求記錄下自己所需要的內容。但是這些紀錄都是一直堆上去的，除非您將檔案自行刪除掉，否則這些檔案就會越來越大。有的人可能會在syslogd.conf裡面寫：

. /var/log/everything

要是這樣的話，當然所有的情況都被你記錄下來了。但是如果真的系統出事了，你可能要從好幾十MB甚至幾百MB的文字中找出到底是哪邊出問題，這樣可能對你一點幫助都沒有。因此，以下兩點可以幫助你快速找到重要的紀錄內容：

1. 定期檢查紀錄

養成每週(或是更短的時間，如果你有空的話)看一次紀錄檔的習慣。如果有需要將舊的紀錄檔備份，可以cp log log.1, cp log log.2...或是cp log log.971013, cp log log.980101...等，將過期的紀錄檔依照流水號或是日期存起來，未來考察時也比較容易。

2. 只記錄有用的東西

千萬不要像前面的例子一樣，記錄下*.*然後放在一個檔案中。這樣的結果會導致檔案太大，要找資料時根本無法馬上找出來。有人在記錄網路通訊時，連誰去ping他的主機都記錄。除非是系統已經遭到很大的威脅，否則這種小事可以不用記錄。可以提升些許系統效率以及降低磁碟用量(當然也節

省時間)。

地理位置的追蹤

如何查出入侵者的地理位置？光看 IP Address 可能看不出來，但常看的話，會發現 140.xxx 的很多都是台灣學術網路的主機，而 168.95. xxx.xxx 的一定是 HiNet 的主機 (168.95.0 爲 HiNet Class B 網路)。

在固接式的網路環境中，入侵者一定和網路提供單位有著密切的關係。因爲假設是區域網路，那麼距離絕對不出幾公里。就算是撥接好了，也很少人會花大筆錢去撥外縣市甚至國外的撥接伺服器。因此，只要查出連線的單位，入侵者必然離連線單位不遠。

撥接式的網路就比較令人頭疼了。ISP 爲了吸引客戶，賣了很多的所謂小時卡、記點卡……等等不需申請，帳號密碼就直接附在上面的卡片。User 這邊只要買了固定的小時數，不需須另外向 ISP 那邊提出申請，就可以按照卡片上的說明自行撥接上網。這樣當然可以吸引客戶，但是 ISP 就根本無從得知是誰在用他們的網路。

也就是說，雖然以小時卡提供撥接服務給撥接使用者帶來相當大的便利，但卻是系統安全的大敵，網路管理員的惡夢。如果入侵你的人是使用小時卡來上網，那……，要從撥號的地點查嗎？查到的發話來源絕不是入侵者自己的電話。

來話者電話偵測 (Caller ID)

ISDN 的 Caller ID 功能，對方的號碼馬上就顯示出來。但是 Caller ID 依然有失效的時候。要顯示來話方號碼的前提是，對方必須是透過數位交換機打到你這邊，在台灣有某些地區仍然使用機械式交換機，如果你打電話的交換路徑中，有經過這些機械式的交換機，那麼依然無法顯示出號碼來。

如何靠 IP Address 或 Domain Name 找出入侵者位置？

雖然電話不一定查得出來，但是至少你會知道他的 IP Address。IP Address 的使用必須向 InterNIC 登記，而 Domain Name 要向當地直屬的網路管理中心登記。在

Internet上的網路管理中心共有三個層級(單位性質一定爲NET)：

1. 國際等級
國際等級只有InterNIC一個，全球各國的NIC以及洲際NIC均由其管理。(http://www.internic%20.net/)。

2. 洲際等級
InterNIC並不直接管理整個Internet，其下的網路資源會再做分區。例如台灣、日本、香港等亞太地區國家，由亞太洲際網路管理中心(Asian-Pacific NIC, APNIC，位於日本)來管理，並不直接由InterNIC管理(http://www.apnic.net/)。

3. 國家等級
Domain Name後面不掛國碼的不是由InterNIC管理就是由洲際的NIC管理，但是有掛國碼的由當地國家之NIC管理，慣例是兩位國碼加上NIC就是該國NIC之名稱。例如台灣之國碼爲TW，則台灣網路管理中心爲TWNIC (http://www.twnic.net/)，但由於InterNIC位於美國，因此美國的Domain Name由InterNIC直轄。有一個特別的例外是掛.mil的美國軍方網路的資料是由ddn.mil(美國軍事防衛網路)來管理，不由InterNIC管理，當您得到某個Domain Name或是IP Address後，可以使用whois來查出資料，語法如下：

whois -h < whois 伺服器 > < 查詢對象 >

例如向whois.internic.net查詢hp.com，需輸入：

```
whois -h whois.internic.net hp.com
```

whois也可能使用下列語法：

whois < 查詢對象 > @< whois 伺服器 >

例如向whois.twnic.net查詢ntu.edu.tw需輸入：

```
whois ntu.edu.tw@whois.twnic.net
```

目前在Slackware Linux附上的爲後者。

Domain Name 命名的三種情況

雖然同樣是 Domain Name，可能你會遇到三種命名的不同情況。在許多國家 *.edu.*是由 NIC 以外的單位所管理 (如教育部)，而屬性也不一定是三個字母，甚至沒有屬性。在判斷單位性質時宜多加注意，以免找不到資料。

1.標準國碼＋三碼屬性碼 (或沒有國碼，僅有屬性碼)

普遍使用於歐洲，美洲國家以及部份東南亞國家。如台灣常見 *.edu.tw、 *.com.tw，美國的 *.com、 *.edu。

2.標準國碼＋二碼屬性碼

以離我國最近的日本、中華人民共和國爲例，公司屬性爲 co，社團屬性爲 or，和三碼定義的 com、org 略有不同。如日本萬代公司之 Homepage 爲 www.bandai.co.jp，如果讀者要使用公司名稱拼湊出完整主機名稱時，需注意日本爲僅有兩碼屬性碼之地區，否則若猜測其爲 www.bandai.com.jp 就會發生錯誤 (註：在國際通信範例中，無論是無線電通信、國際越洋電話、乃至於網際網路等，均將台灣與中國大陸劃分爲兩個不同國家。

3. 僅有標準國碼，未有任何屬性碼

如澳洲的主機均爲僅有 *.au 之主機名稱，未有任何其他的 com、co、或任何單位屬性碼後面直接接上單位名稱。

由 Domain Name 查出連線單位資料

在 Internet 上慣例由 whois 服務來查詢連線單位的登記資料，whois 本來應該是用來查某人的電話或是其他資料的，但是在 NIC 方面是用來查出連線單位的電話以及住址，技術聯絡人等。符合該 NIC 管理權限的單位資料會存放於該單位的 whois 主機中，慣例是 whois＋ NIC 名稱 ＋ net。例如亞太地區網路管理中心 whois server 爲 whois.apnic.net，台灣網路中心 whois server 爲 whois.twnic.net。

當你知道某台主機的 Domain Name 以後，可以依照下

面順序查出連線單位的電話住址等資料。第一步，先看有沒有國碼。沒有國碼的，向 whois.internic.net 問；有國碼的，向 whois.國碼 nic.net 問 (ex. whois.twnic.net)。
另外，如果你要查美國軍事單位的聯絡明細則你需要向 nic.ddn.mil 查詢，方可查到資料。例如查出美國陸軍的資料：但 FBI 等調查機構屬政府單位，非軍事單位，查詢時需注意：

由 Domain Name 查出資料
如您能從 nslookup 查出某一 IP Address 之 FQDN，則可以直接向當地 NIC 查出入侵者網路之資料：

1.由美國入侵的例子：
由 xxx.aol.com 入侵由主機名稱發現未有國碼，因此直接向 InterNIC 查詢。由此我們可以查到 America Online 的技術負責人以及電話、傳真等資料。

2.由台灣入侵的例子：
由 Hope Net 入侵 (cded1. hope.com.tw) 由於 TWNIC 目前 whois 資料庫不知怎麼的不見了，故請改由 dbms.seed.net.tw 查出 hope.com.tw 之中文名稱，再打 104 詢問該公司的電話！(圖一) 現在如果直接由 whois.twnic.net 查詢會這樣：

只有 IP Address 的查法
假設 168.95.109.222 有人入侵，不知道這是 HiNet 的網路，而這個 IP Address 也沒有 Domain Name 的話，則須先將 IP Address 分等級，再向 InterNIC 查詢：

1.由 15.4.75.2 入侵的例子：
此 IP Address 是 15 開頭，爲一個 Class A 網路，故向 InterNIC 查詢 15.0：查出此 IP Address 爲惠普公司所有

2.由 140.111.32.53 入侵的例子：
此 IP Address 爲 Class B，需查詢兩次。先向 InterNIC 查詢 140.111.0：查出爲中華民國教育部所有。再向 whois.twnic.net 查詢 140.111.32.0

3. 由 203.66.35.1 入侵的例子
這是一個 Class C IP，因此必須查詢至少二次，一般是

三次。順序爲國際－＞洲際－＞所屬國家。先查203.0：出來一大堆，怎麼辦？有的情況只好再追問Class B。由於InterNIC將部份Class C交給洲際管理機構來負責配給，因此有些Class C的資料會在洲際管理機構，此時先向InterNIC查出所屬洲際管理機構(用Class B問)。問到203.66爲亞太地區洲際網路，於是向whois.apnic.net詢問203.66.35.0：查了三次以後，終於查到203.66.35.0爲：在一堆資料中查到203.66.35.1，此一IP Address爲Forwardness Technology Co. Ltd.所有，電話地址也一併附在上面。

由以上的查法，可以由任一主機名稱或IP Address查到連線者網路單位的資料，如果您發現該網路單位下屬主機對您的網路有攻擊行爲，請檢具資料告訴對方的系統管理員。

下面是Windows 95的hosts檔案：當您沒有DNS的時候，您可以拿這個來將Domain Name＜－＞IP Address的對應工作做好。寫法就和UNIX一樣。Microsoft的這個hosts檔案寫的是給chicago用的，原先的hosts檔案檔名是hosts.sam，您要自己將檔名改成hosts才能用。

註一：

幾乎所有使用TCP/IP通訊協定的機器都會有hosts、network等檔案。這是所有TCP/IP系統的共通習慣(但只有Microsoft的軟體會有lmhosts來配合Microsoft自己的wins域名解譯系統)。

註二：

長途台號碼爲108，轉發國內長途電話用，並可要求對方付費(就像國際台一樣)，因爲台灣早期交換機無法讓用戶直撥外縣市電話，故需由長途台人工轉接。現在有了長途直撥，除非您有需要對方付費，否則不需要用長途台了，因爲人工轉接還要另外支付人工轉接費用。當您在打國內長途電話而有對方付費的需求時，就可以打108然後要求值機人員替您轉接，然後由受話者來付電話費。國內其他的人工轉接台還有103船舶台(轉發船舶無線電話，NAVTEX航務情報電訊等)以及100國際台。