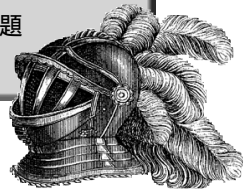


第二章

S A T A N 的 安裝

本章內容：

- * 如何取得 SATAN
- * 系統需求
- * 安裝與編譯
- * 懺悔吧！
- * 在 Linux 下執行 SATAN
- * 可能發生的問題



強烈建議你自己編譯 SATAN 的原始碼。因為 Internet 上提供 SATAN 二元碼的網站很多，尤其是 Linux 平台，你根本無從確認這些編譯好的程式是不是乾淨的版本。如果你想深入研究 SATAN，可以自己發展一些模組，自己編譯所花的功夫絕對是值得的。你可以更清楚其中運作的過程。

如何取得 S A T A N

最新版本的 SATAN 都是放在 <ftp.win.tue.nl> 的 `pub/security` (註) 目錄下。這是荷蘭艾荷溫科技大學數學與資訊系的伺服器，SATAN 原設計人之一的 Wietsje Venema 在最初公開這個軟體時還在這裡，目前他已經轉到 IBM 著名的華生實驗室工作。

註 本書寫作之時，SATAN 的版本是 1.1.1。

第二章

許多 CERT (電腦急救回應小組) 的 Web 與 FTP 伺服器也提供最新的 SATAN 原始碼。例如在德國，你可以透過德國研究網路 (DFN) 的 FTP 伺服器 ftp.cert.dfn.de 下的 /pub/tools/net 目錄找到。

為了保證你拿到的是最原始的 SATAN 程式碼，請務必透過這些管道。由於 SATAN 程式的特性，若是被有心人修改經過不知情的人編譯，後果可能難以收拾。網路安全工具通常是攻擊者安插病毒 (註1) 的目標，因為這類程式都會在最高權限的模式下執行，而且你以管理者身分執行這類程式，表示你賦予了最高的信任。

如果利用 PGP (註2)，你可以透過數位簽名驗證 SATAN 原始碼的真確性。Wietse 的 FTP 站目錄下的 satan-1.1.1.tar.Z.asc 檔包含數位簽名。你可以輸入下列指令來驗證原始碼：

```
#pgp satan-1.1.1.tar.Z.asc
```

附錄中有 Wietse Venema 的 PGP key 指紋。

系統需求

SATAN 不是一個單獨的程式，而是一群工具程式，有些是 C 寫成的，有些是 Perl，也有 RPC。這些工具的作用是偵測網路安全上的弱點，或是搜尋網路上的主機。其中有些 Perl 程式會分析偵測的結果，整理成小型的資料庫，進行格式化的螢幕輸出。SATAN 會產生 HTML 的輸出，讓你以瀏覽器觀察結果。

執行 SATAN 的系統需求如下：

支援網路存取的 Unix/Linux 系統，目前 SATAN 還沒有移植到其他作業平台。

主機上有一個 Web 瀏覽器。為了安全的顧慮，你不能透過遠端主機執行瀏覽器。

註1 在這裡，病毒程式的定義很廣泛，主要是所有能自我複製的程式。

註2 請參考 Simson Garfinkel 的著作 'PGP' (O'Reilly 出版)。

SATAN 的安裝

你必須具有 Unix 上的 root 使用權。某些 SATAN 程式需要超級使用者的權限。

Perl 5.0 以上的版本。

C 語言編譯器。

rpcgen。如果你的系統上沒有安裝 RPC 編譯器，可以利用 SATAN 本身提供的 rpcgen。

X Windows 系統。

基本上，SATAN 可以在簡陋的命令下執行，但這時只能利用部份的基本功能。若沒有瀏覽器，你無法檢視輸出結果，而且無法瀏覽 SATAN 的技術文件，所以即使發現問題也不知從何下手。

所以本書都假設你有 X Window 系統的圖形界面，這對大部分 Unix 的使用者應該不是問題。

安裝與編譯

SATAN 流傳的版本是 tar 型態的壓縮檔，你可以利用下列方式解壓：

```
# uncompress < satan-1.1.1.tar.Z | tar xvf -
```

解壓之後，satan-1.1.1 目錄下會產生許多子目錄、satan 與 reconfig 檔案、一個 Makefile、以及一個 README 檔案：

```
# cd satan-1.1.1
# ls -F
Changes      bin/         perl/        rules/       /src
Makefile*    config/     perllib/     satan
README       html/       reconfig*    satan.8
TODO         include/    repent*      satan.ps
```

執行 reconfig

輸入以下命令以執行 reconfig：

```
# ./reconfig
```

reconfig 會試圖在檔案系統中找出各種 Unix 命令、Perl、以及 Web 瀏覽器。假如找到了，reconfig 會將這些程式的路徑設定在 SATAN 的 Perl script 裡。你一定要執行 SATAN 本身所附的 reconfig，其他的程式如 Linux 的 X server Xfree 也包含一個 reconfig 命令，但它的作用是重新設定系統參數。執行 reconfig 之前先變更到 SATAN 所在的目錄。

有時候 reconfig 不見得會找到所有的工具，這是很可能發生的，例如 Perl 的檔名被改過了，或是存在其他遙遠的目錄底下。這時候你可以直接編輯 reconfig 的 script，將 Perl 的路徑名稱指定給 PERL 參數。

如果你用的瀏覽器不是 Netscape、Mosaic、或 Lynx，reconfig 會出現問題，你必須在 /config/path.pl 檔案中加入類似這樣一行：

```
$MOSAIC="/usr/bin/X11/chimera";
```

上一行將 Mosaic 改成 Chimera 瀏覽器，讓 SATAN 找到瀏覽器加以執行。

編譯所需要的工具

依據你所用的系統，編譯 SATAN 需要不同的準備工作，因為其中三個檔案需要的標頭檔 (header) 在某些系統中沒有提供，例如 Linux 上的 tcp_scan, udp_scan, 和 fping。tcp_scan 和 udp_scan 是掃描程式，用來偵測哪些 port 號上提供了哪些服務。fping 用來“ping”一個子網路上的所有主機，決定目前網路上正運作中的 IP 位址有哪些。在編譯過程中，這三個程式需要某些根據 BSD 4.4 定義的標頭檔。很不幸的，這些標頭檔在並非在所有系統上都相同。

SATAN 的安裝

在 SunOS, Solaris, 以及所有的 System V Unix (SINIX 5.42) 系統上, 編譯過程應該都沒什麼問題。請參照表 2-1 列出所有支援的作業系統。在其他系統上, 你必須自己修改這些標頭檔。例如 Linux, 你必須到 <http://recycle.cebaf.gov/~doolitt/satan> 去找修改過的標頭檔, 這個網頁也包含許多各種版本的 Linux SATAN 的注意事項。標頭檔必須解壓到 `~satan/include/netinet` 目錄。之後會對 Linux SATAN 有更深入的說明。

接下來, 輸入 `make systemtype`。在 SunOS 4.1.4 上, 輸入:

```
# make sunos4
```

根據引數所指定的作業系統型態, `make` 執行需要的指令以進行 SATAN 的編譯。Makefile 包含 SATAN 所需的程式庫資訊, 以及各種系統變數與編譯器命令列選項的定義。

表 2-1 列出了各種作業系統的 Makefile。

表 2-1 : 支援的作業系統

aix	IBM AIX
osf	DEC OSF
bsd	generic BSD 4.4
bsdi	BSDI
dgux	Data General UNIX
irix4	SGI IRIX 4
irix5	SGI IRIX 5
freebsd	FreeBSD
hpux9	HP-UX 9
linux	Linux[_F_]; [_F_] this might require some modifications; see the section [XREF "Running SATAN Under Linux_"] later in this chapter
sunos4	SunOS 4.1 x (Solaris 1)
sunos5	Solaris 2
sysv4	generic system V Release 4 (e.g., SINIX 5.42, Reliant Unix, ...)
ultrix4	Ultrix 4.x

第二章

除了 Linux 需要特殊的修改之外，這些作業系統上的編譯程序都不需其他修改。如果你用的是不同的作業系統，可能只要修改 Makefile 的編譯方式就可以了。至於需要哪些特定的修改，其實也很難講，大概多少需要一點程式設計的經驗。例如在 SCO Unix 上，必須進行下列修改：

```
sco:

    @$(MAKE) all LIBS="-lsocket -lnsl" \
        XFLAGS="-DAUTH_GID_T=gid_t -DTIRPC"
```

再輸入 sco 就可以順利編譯了！

大概差不多就這樣了，還有兩件事要注意一下。

解除你的 Proxy Server

如果你的網路安裝了防火牆，Web 瀏覽器必須設定為解除 proxy 服務。因為如果用了防火牆，Web 瀏覽器通常和 Internet 的連線是間接的，必須透過 proxy server。Proxy 是防火牆上一種特殊的程序，它會把本地瀏覽器請求的頁面轉送到發出請求的主機。經由這種過程，躲在防火牆後面的主機不需直接與 Internet 連線，也同時增加了安全性。

同樣為了安全的理由，SATAN 不允許利用 proxy 伺服器。SATAN 與 Web 伺服器之間的資料傳輸必須是直接的，中間不能被攔截。在 Netscape 中關掉 proxy 服務的方式是：

```
Mosaic*httpProxy:  http://www.dg5kx.de/
Mosaic*ftpProxy:   http://www.dg5kx.de/
Mosaic*waisProxy:  http://www.dg5kx.de/
Mosaic*gopherProxy: http://www.dg5kx.de/
Mosaic*newsProxy:  http://www.dg5kx.de/
Mosaic*fileProxy:  http://www.dg5kx.de/
```

SATAN 的安裝

使用 DNS

如果你的工作站沒有使用 DNS，將 `~satan/config/satan.cf` 檔案中的的這筆資料從 0 改成 1：

```
$dont_use_nslookup = 0;
```

改成這樣：

```
$dont_use_nslookup = 1;
```

如果這個檔案中有一筆資料是名稱伺服器，基本上就可以用 DNS。利用 `nslookup` 測試 DNS 是否在執行。你應該盡量使用 DNS，讓 SATAN 的輸出結果比較看得懂，否則一堆 IP 位址會讓你頭昏腦脹。

當然，你可以之後透過 SATAN 的設定選項關閉或開啟 DNS，但若這筆資料錯誤會讓 SATAN 無法啟動。SATAN 本身提供了 Web 伺服器來輸出結果，但只允許 SATAN 啟動的那台工作站與伺服器連線。如果 DNS 沒有作用，即使在 `satan.cf` 檔案中開啟了 DNS，SATAN 也無法確定本身工作站的 IP 位址，造成 Web 伺服器也無法啟動。

啟動 SATAN

設定完成之後，從 X Windows 中啟動 `./satan`。SATAN 會自動啟動指定的 Web 瀏覽器與其他工具程式。你不需要事先啟動瀏覽器。

如果你指定的瀏覽器是 Netscape 3.0 以上的版本，必須稍作修改，本章之後會提到。

懺悔吧！

如果你對 SATAN (撒旦) 這個名稱很感冒，可以換個名字。你可以執行 `repent` 程式，它會改變所有出現 SATAN 的地方，包括文件的內容，讓你舒服一點。但你必須在執行 `make` 之前先執行 `repent`。

但在這本書裡，我們還是持續用 SATAN 這個名稱，因為這是大家熟知的名詞。看吧！連 SATAN 的圖片都換成了 SANTA (耶誕老人)！

在 Linux 下執行 SATAN

除了缺少 BSD 4.4 標準的標頭檔之外，Linux 系統還有些問題。這不是 SATAN 的問題，而是 Linux 的錯。由於 Linux 的版本眾多，它的核心 (kernel) 也非傳統的 Unix 架構，我們沒辦法歸納出一個標準的安裝方式，這裡只提出一些常見的問題。

例如，`reconfig` 往往無法啟動而且 `shell` 會產生執行錯誤。這是因為 `bash` 的問題，`bash` 是 Linux 的預設外層，`bash` 無法處理關於 `reconfig` 對於是在 Perl 還是在 `shell` 下執行的判定。這個好解決：在 Perl 下面執行 `reconfig`，而不要透過 `shell`：

```
# perl ./reconfig
```

你也可以將 `#` 符號放在 `reconfig` 第一行的前面。

小心和 `Xfree` 任何一個檔同名的程式！在安裝過程中，由 `./reconfig` 啟動 `reconfig` (如果你在正確目錄下)或是輸入絕對路徑，否則你可能啟動的是別的 `reconfig`！

Linux 的 `select()` 函式和其他 Unix 系統有些差別，可能造成與 `tcp_scan` 的衝突。可以在下列網站找到修正程式：

```
http://recycle.crba.gov/~doolitt/satan/tcp\_scan.diff2
```

SATAN 的安裝

我建議你不要用太慢的機器跑 Linux，這會產生 SATAN 一堆莫名其妙的問題，尤其是 fping。舉例來說，就算網路電腦明明是啟動的，SATAN 結束子網路掃描之後居然會下列訊息：

```
get_targets failed - unable to expand subnet
```

你可以只掃描個別主機而不是整個網路，避開這個問題。當然，這實在划不來，還不如增加 timeout 數值。在 `~satan/perl/targets.pl` 檔案的 `target_acquisition` 函式中增加 timeout：

```
sub target_acquisition
{
    local($target, $proximity, $level) = @_;
    local($targets_found);

    # Expand and then collect. Pass results through new_target() for
    # consistent handling of constraints and policies.
    &open_cmd (TARGETS, 120, "$GET_TARGETS $target");
    while (<TARGETS>) {
        ...
    }
}
```

在 `open_cmd` 命令中，第二個參數的預設值是 120 秒的常數值。最好將這個值改成變數 `$value_timeout`。之後可以透過 Web 瀏覽器或在設定檔中直接更改這個值。關於設定檔 `satan.cf` 的更改，請參照第五章。

網路上的新聞群組常提出一些疑難雜症，例如 `showmount` 的解析 (`showmount` 是顯示 NFS 伺服器輸出到哪個檔案系統的工具程式)，以及 Linux 網路程式的緩衝區溢出 (`overflow`)。不過新的 Linux kernel (2.0 以上) 顯然已經排除了這些問題。

可能發生的問題

下面提一些使用 SATAN 時常發生的問題。

使用 Netscape

許多人提出使用 Netscape 搭配 SATAN 的問題通常出現的徵狀是 Netscape 啟動沒問題，但按下任何一個連結都連不上那個位址，反而會出現訊息問你要把網頁存到哪裡。

問題是由於大部分 SATAN 透過瀏覽器顯示的不是靜態的 HTML 網頁。SATAN 是利用可產生即時 HTML 輸出的 Perl script。在 Netscape 的預設情況下，它認出 pl 副檔名，然後試圖儲存這個網頁，而不是執行 script 及顯示輸出。

要改變這種情況，可透過 Edit->Preferences->Navigator->Applications->Helpers。表格的左欄是檔案型態，找到 application/x-perl 這筆記錄，用滑鼠點選，再點選右邊的 Edit 按鈕。出現對話方塊之後，刪掉包含“pl”的記錄，按下 OK 按鈕就行了。在新版的 Netscape Communicator 中，修改的步驟為 Edit->Preferences->Navigator->Applications。

找不到網路位址

啟動 SATAN 之後，你的螢幕出現這樣的訊息：

```
# ./satan
SATAN is starting up...
Unable to find all my network addresses
#
```

問題可能出在你的 DNS 設定、NIS、或是 /etc/hosts 內容設定。

SATAN 的安裝

為了安全的因素，SATAN 只會與本地主機 WWW 瀏覽器溝通。要確定瀏覽器是否真的在本地區域，SATAN 裡面有一個 Perl 程式會負責判斷你本地工作站的所有 IP 位址。如果某個企圖與 SATAN 伺服器建立連線的對方位址不屬於本地位址，SATAN 會認為有人想竊取資訊，先中斷連線再顯示警告訊息。

確定你的 DNS 與 NIS 設定無誤。如果這些方法都沒用，可以將 `~satan/config/nslookup` 中的 `dont_use_nslookup` 設為 1，讓 SATAN 不使用 DNS：

```
$dont_use_nslookup = 1;
```

確定 `/etc/hosts` 檔案中包含你的 IP 位址及主機名稱。

找不到我的主機

若在啟動階段出現下列訊息：

```
# ./satan
SATAN is starting up...
Can't find my own hostname: set $dont_use_nslookup in config/satan.cf
#
```

表示 SATAN 無法判斷你的工作站的主機名稱。假使你的主機名稱有出現在 `/etc/hosts` 中，把 DNS 關掉就可以解決這個問題。

SATAN 是利用 `hostname`、`uname` 和 `uuname` 這些指令搜尋你的主機名稱。或許這些指令在你的機器上是放在某些偏僻的目錄底下，可以查看 `~/perl/hostname.pl` 檔，修改這些指令的路徑。

第二章