Unix/Linux 系統入侵檢測管理流程

TACERT 臺灣學術網路危機處理中心團隊編譯

資料來源： **CERT SOCIETE GENERALE**

http://cert.societegenerale.com/en/publications.html

目錄

這份資安事件應變小抄，專給想要調查安全事件的網管人員。記住：面對事件時，跟著資安事件應變方法的流程，記下記錄不要驚慌。如果需要請立刻聯絡臺灣學術網路危機處理中心(TACERT)。

1. 準備((Preparation)

1-1. 執法調查員應該要能實際接觸可疑的系統。

1-2. 為了當作法庭證據可能需要將硬碟做實體備份。最後，如果需要，切斷所有與可疑的機器接觸的網路連結。

1-3. 一台機器或是伺服器平常的網路活動知識是必要的，應該要在安全的地方保有一個記錄平時通訊埠活動的檔案，才能有效率的比較目前的情況。

1-4. 如果能具備平時在機器上運作服務的知識將會有很大的幫助。有需要時不要猶豫向 Unix/Linux 專家請求幫助。一個好意見對於機器上的服務或是執行的程序也能有所了解。

1-5. 你應該要固定更新重要檔案(尤其是具有 SUID 和 GUID 的檔案)，且它應該被存放在遠離網路的地方。有了這個列表，你可以輕易地分開正常的 SUID 檔案並偵測異常的部份。

2. 確認

■ **不尋常的帳戶(Unusual Accounts)**

– 在/etc/passwd 裡尋找任何可疑的帳戶，尤其是 UID 為 0 的(root 帳戶)。另外也要檢查/etc/group 和/etc/shadow 兩個檔案

– 尋找被刪除的帳戶留下的檔案，這些檔案可能被用在攻擊

上

```
#find /   \( -nouser   -o   -nogroup\) -print
```

■ **不尋常的檔案(Ususual Files)**

– 尋找所有的 SUID 和 GUID 的檔案：

```
#find / -uid 0 \( -perm -4000 -o -perm 2000 \) -print
```

– 尋找怪異的文件名，例如開頭為 ”.” , ”..” 或 ” ”：

```
#find / -name “ *” -print
#find / -name “. *” -print
#find / -name “.. *” -print
```

– 尋找大型檔案(大於 10MB)

```
#find / -size   +10MB   -print
```

– 尋找正在運行的程序或是已被取消鏈結的文件：

```
#lsof   +L1
```

– 尋找在/proc 和/tmp 中的異常檔案。/tmp 是駭客選擇儲存惡意檔案的地方之一。

■ **不尋常的服務(Unusual Services)**

– (Linux 限定)執行 chkconfig(假如有安裝)去檢查所有服務：

```
#chkconfig -list
```

– 查看執行中的程序(記住：一個 rootkit 可能改變本文裡你的

一切結果，尤其是這裡)

```
#ps -aux
```

– 使用 lsof -p [pid]查詢不知道的程序

你必須知道平常運行的程序，並且能指出哪個程序是被駭客加進去的。注意 UID 為 0 的程序。

■ **不尋常的網路活動(Unusual Network Activity)**

利用以下幾種方法，去查看網路的嗅探器（sniffers）：

查看 kernel 紀錄，尋找像是:"*kernel: device eth0 entered promiscuous mode*"的關鍵字

使用#ip link 去檢測"PROMISC"標籤，和 ifconfig 比這種方法較好，因為 ifconfig 指令並非所有 kernel 都支援。

– 尋找異常的埠活動：

利用指令：#netstat -nap 和 #lsof -i 去得到更多的網路埠號活動的資訊

– 尋找平常在你的區域網路中的 MAC #arp -a

– 尋找任何未預期出現在網路活動上的 IP 地址

■ 異常的自動化任務

– 尋找在/etc/cron.allow 出現的異常排程。這邊必須特別注意 UID 為 0 的帳號(root)所安排的工作

```
#crontab -u root -l
```

– 尋找不尋常的系統排程：

```
#cat /etc/crontab 和#ls -la /etc/cron. *
```

■ 主機異常記錄

查看系統上的記錄檔案找出可疑事件，包括：

– 大量的認證失敗（sshd, ftpd 等服務）

– Remote Procedure Call (RPC)的程式紀錄條目包括了大量的奇怪符號

– Apache log 中大量的 error

– 重新啟動（硬體重新啟動）

– 重新啟動應用程式（軟體重新啟動）

在大部分的 Linux 發行版中，幾乎所有的記錄檔皆放在/var/log 目錄底下，以下為主要的幾個：

- /var/log/message：一般信息和系統相關的東西
- /var/log/auth.log：認證記錄
- /var/log/kern.log：kernel 記錄
- /var/log/cron.log：crond 工作記錄
- /var/log/maillog：mail server 記錄
- /var/log/httpd/：Apache log
- /var/log/boot.log：系統啟動記錄
- /var/log/mysqld.log：MySQL 資料庫伺服器記錄
- /var/log/secure：身分認證記錄
- /var/log/utmp or /var/log/wtmp：登入記錄檔

要查看這些記錄檔，一些工具像 cat 和 grep 可能有用：

```
cat /var/log/httpd/access.log | grep “GET /signup.jsp"
```

■ **異常 kernel log**

- 透過 kernel log 去找出系統上的可疑事件

```
#dmesg
```

- 列出所有重要的內核和系統資訊

```
# lsmod
# lspci
```

– 尋找已知的 rootkit(使用 rkhunter 和相關工具)

■ **檔案 hash(雜湊函式)**

驗證所有二進制的 MD5 hash，這些檔案位於/bin, /sbin, /usr/bin, /usr/sbin 或是其他二進制存儲的地方(使用 AIDE 或相關工具)

警告：這個操作將會改變檔案的時間戳。所以這項動作必須等其他檢查都已經做完才能操作。

– 能使用 PRM 的系統，可以用下列指令查看安裝的套件：

```
#rpm -va | sort
```

– 在有些 Linux 上，有個名為 check-packages 可以使用

– 在 Solaris 上：

```
#pkg_chk -vn
```

– 在 Debian：

```
debsums -ac
```

– 在 Openbsd

```
pkg_delete -vnx
```

3. 遏止(Containment)

從受到感染的機器上備份所有的資料，如果可以，對整個硬碟

bit-by-bit 的實體拷貝，也可以對記憶體(RAM)做拷貝。

假如機器對公司而言不是相當重要的話，可以拔除電源插頭強迫將其關機，假如是使用電池的筆電，則按壓”off”數秒直到電腦關機。

假如鑑定的步驟沒有任何發現，而系統仍舊是被入侵狀態，則需要離線進行調查。

嘗試去找出駭客每一個動作的證據：(使用取證工具像是 Sleuth Kit/Autopsy)

- **找出所有被攻擊者使用的檔案**，包括被刪除的檔案，並且看他們做了什麼或是評估威脅。
- **檢查最近有被更改的檔案**
- **檢查記錄檔**
- 試著找出攻擊者如何進入系統。所有的線索都必須去考慮。假如沒有找到入侵電腦的證據，不要忘記問題有可能發生在內部人員。
- 更新系統，以防同樣的漏洞又被使用

4. 修正(Remediation)

暫時移除與事件有關的帳戶和調查發現的惡意檔案

5. 復原(Recovery)

無論駭客入侵系統到何種程度，或是你對事件的調查有多仔細，只要系統被入侵了，最好的方法還是重灌系統，並且更新。如果不能重灌，你應該：

- 更改所有系統的帳戶密碼並且讓使用者在安全的管道下這樣做：他們必須使用有大小寫，特殊符號，數字及至少 7 個符號長的密碼
- 檢查所有系統資料的完整性，可以使用 MD5 hash
- 還原所有被更改的二進制文件(例如： /bin/su)

6. 後續情況(Aftermath)

報告

下列的主題應該要記錄下來：

- 初步檢測
- 每個重要事件的行為與時間軸
- 什麼是適當的行為
- 什麼地方出了問題

■ 事件成本

資料來源：CERT SOCIETE GENERALE

http://cert.societegenerale.com/en/publications.html