伺服器安全防護

為有效管理伺服器，減少系統因軟體漏洞或遭受外部攻擊造成損失，以下介紹各種系統安全設定方式及步驟，提供伺服器管理者參考，本範例以 CentOS 5.9 (Kernel 2.6.18) 為例。其管理方式大致可分為以下三個階段：

1. 事前防範：針對伺服器的功能及服務對象，提供基本的開放權限設定，其餘則加以限制。
2. 及時分析：對於必要開放的服務功能，及時的分析客戶端不當的使用行為，給予適時的阻擋或限制。
3. 事後稽查：定期的檢視系統紀錄，對於未能加以防範的部份，尋求可以改善的方式。

系統基礎設定

1. 防火牆

近來許多網路作業系統都以搭配防火牆當作基礎功能，常見如下：

作業系統	防火牆
GNU/Linux	W netfilter/iptables
FreeBSD	W IPFilter、W pfSense、W ipfirewall
Solaris	W IPFilter

建議系統管理者**開啟防火牆功能**，針對所需要提供的服務給予開放連線，其餘部份則透過防火牆的條件設定限制連線或訪問，形成伺服器的第一道防護。避免有心人士嘗試猜測系統漏洞，降低被攻擊之可能。

2. ACL 設定

W TCP Wrapper 是一個 host-based 的網路存取控制，它的設定通常包含客戶端與伺服器端 (client-server) 的對應關係，客戶端資訊通常有「主機名稱 (host name)、主機位址 (host address)」及「使用者名稱 (user name)」；而伺服器端的資訊通常有「程序名稱 (process name)、伺服器名稱 (host name)」及「伺服器位址 (host address)」
而目前多數的網路應用程式，大多支援 TCP Wrapper 功能，如：vsftpd (FTP)、OpenSSH (SSH)、xinetd 等。

- 檢查應用程式是否支援 TCP Wrapper 功能，以確認是否可以使用 ACL 設定。以下透過檢查應用程式是否有使用 libwrap.so 函式庫，判斷是否支援 TCP Wrapper 功能。

```
# ldd /usr/sbin/vsftpd | grep -i wrap
    libwrap.so.0 => /lib/libwrap.so.0 (0x00ad5000)
```

- TCP Wrapper 的主要設定檔大致上有兩個，分別是 hosts.allow 與 hosts.deny (檔案名稱請依實際安裝為主)。而系統則採 first-match 方式比對設定條件，首先是比對 hosts.allow 然後給予提升權限，再者比對 hosts.deny 限制權限，最後未滿足前二者的設定則全部開放。
- 以下範例僅開放 140.114.0.0/16 網段連線至 SSH 服務，其餘連線來源都限制。

```
# vim /etc/hosts.allow
sshd : 140.114.0.0/255.255.0.0
```

```
# vim /etc/hosts.deny
```

```
sshd : ALL
```

3. 即/及時防護

對於伺服器必須提供給所有使用者的服務功能，如 HTTP (port 80) 或是 FTP (port 21) 等服務，因為無法完全使用防火牆或是 TCP Wrapper 加以限制，則容易成為有心人士加以攻擊的管道或對象，此時仍可透過一些即/及時防護的軟體加以限制，如 Fail2ban、DenyHosts。該類軟體的運作原理是透過即/及時分析 log 紀錄檔，過濾一些可疑的使用行為紀錄，再針對這些來源作一適當的處置，如「通知管理者異常行為」、「透過防火牆或 TCP Wrapper 加以阻擋」等。其特色是，可以適性的針對不當用戶或來源加以阻擋，而非阻擋整個網段或是限制全部的服務功能，提供伺服器動態的防護需求。

- 本站另有撰文 Fail2ban 的說明文件。

系統更新

套件管理

定期的更新系統與修補漏洞，是維持系統安全的最基本工作。善用套件管理系統 (Package management system) 可以協助管理者有效的更新作業系統與應用程式。在軟體的安裝使用上，常見的問題有以下：

- **軟體來源**：使用來路不明或未受信賴的軟體來源，您就必須承擔惡意軟體或是病毒程式的威脅。不論您是使用開放原始碼軟體 (Source) 或是已編譯過的程式 (Binary)，從信賴的來源取得軟體安裝，則可降低該風險。
- **維護不易**：若軟體不易取得或更新，將造成管理者疏於修補系統漏洞與修正軟體瑕疵。因此選擇合適的套件管理系統，不僅可以輕鬆的更新軟體，也可以及時掌握版本更新資訊。
- **功能相依問題**：如 A 軟體已經安裝，但卻少安裝 B 軟體，以致於 A 軟體無法使用。
- **未完全更新**：如 A 軟體已更新至較新的版本，但 B 軟體卻是未更新的舊版本，如此將造成軟體運作上的錯誤或無法預期的功能缺失。
- **重複安裝**：如原先已安裝某軟體的 v1.0 版，但又另外安裝 v1.1 版，原本應是從 v1.0 更新至 v1.1，結果卻是重複安裝同一套軟體。
- **其他問題**：如軟體未能完全移除、軟體重新安裝後設定檔遺失、軟體升級後設定檔未能更新等。

而透過設計良好的套件管理系統則可以減少上述的問題發生，常見的套件管理系統如下：

作業系統	套件管理系統
CentOS / Fedora	YUM
Debian	APT
FreeBSD	FreeBSD Ports
Solaris	Image Packaging System、OpenCSW

紀錄檔分析

適當的開啟系統紀錄 (Syslog)，其中包含系統異動資訊、使用者登出或登入事件、各類軟體的除錯或警告資訊等，藉以紀錄重要事件的發生時間和內容，提供日後稽核使用。另外，透過定期的分析與統計系統紀錄，可以觀察伺服器的使用情形，也可以了解服務的營運狀況，除了使用既有的軟體自動分析外，也可以手動方式過濾一些錯誤訊息，以了解異常的使用行為。

- 紀錄檔自動分析與統計

    - logwatch
    - AWStats
- 手動判斷，如以下範例以 Wegrep 工具過濾出紀錄檔中包含有 `fail`、`error` 或 `crit` 字樣的內容。

```
# egrep -i -n '(fail|error|crit)' /var/log/secure
```

- 手動判斷，以下範例使用 grep 工具過濾出含有 404 字樣的內容 (因 HTTP 當中的 WHTTP 404 錯誤訊息)。

```
# grep 404 /var/log/httpd/access_log
```

其他的系統防護資訊

- Top 20 OpenSSH Server Best Security Practices
- 20 Linux Server Hardening Security Tips
- Linux: 25 PHP Security Best Practices For Sys Admins
- 20 Linux System Monitoring Tools Every SysAdmin Should Know
- E-mail Alert on Root SSH Login
- ModSecurity: Open Source Web Application Firewall
- WSecurity-Enhanced Linux
- WAppArmor
- Wsudo