Internet/Intranet Linux 伺服器
實驗手冊

Ⅰ. 實驗目的

瞭解常用的 Internet 及 intranet 服務，練習架設及管理 Linux 上各種伺服程式，其中包括：

Internet 服務

一、 HTTP: Apache server

二、 Database: MySQL

三、 mail: Qmail

四、 FTP: Wu-ftp

Intranet 服務

一、 file server: Samba

二、 proxy: Squid

三、 firewall: ipchains

實驗報告的內容應包含：實驗題目、參與人員及單位、目的、設備、方法、紀錄、問題討論、心得。**報告內容應是經討論、整理、濃縮後，重新詮釋而寫出，切勿全部剪貼、照單全貼。**

Ⅱ. 實驗設備

本實驗需要的硬體可自備，亦可至工三 229 室（機房）使用專屬實驗機器。

一、硬體

項目	數量	備註
個人電腦 PC	1	最好是 Pentium 以上，並具備 32MB 的記憶體
Linux 和 Windows 支援的網路卡	1	如果防火牆和其他伺服器要架設在不同的電腦上，則需要兩張以上的網路卡

二、軟體

項目	數量	備註
RedHat Linux 7	1	

Ⅲ. 背景資料

Linux 是一套 UNIX-like 的作業系統，可以在一般的 PC 上執行，不僅免費、可以任意下載複製，甚至它的原始程式碼也完全公開。Linux 最早起源自 1991 年由芬蘭赫爾辛基(Helsinki)大學的一位學生 Linus Torvalds，他撰寫 Linux 的核心並公佈在網路上後，熱心的網友們開發系統所需要的系統程式及應用程式，這些程式一樣大多是自由軟體，任何人都可以免費在網路上取得，不過自行去下載這些程式再一一安裝非常不便，於是有些公司或團體搜集、整合 Linux 上的程式，構成一套完整的作業系統，讓一般使用者可以方便地安裝，這就是所謂的安裝套件(distribution)。一般說的 Linux 系統便是針對這些安裝套件而言，同樣是 Linux 系統，卻分成不同公司、機構整合出來各式各樣的安裝套件。在這麼多安裝套件裡面，RedHat[1]由於安裝過程簡單，又提供了許多系統設定工具、加上使用 RPM(RedHat Package Manager)管理程式套件，系統易於維護與升級，目前已漸漸成爲最多人使用的 Linux 系統。表一列出目前 Red Hat Linux 7.0 版[1]所包含較常用的各類伺服器，本實驗從其中選出 Web server、Mail server、Database server、FTP server、File server、Firewall、Proxy server，介紹它們的功能及安裝方式。除了 Qmail 之外，所有的 rpm 檔案皆可在 RedHat 光碟中找到，需要注意的是原本 RedHat7.0 附的 MySQL 有問題，要另外再抓更新版。

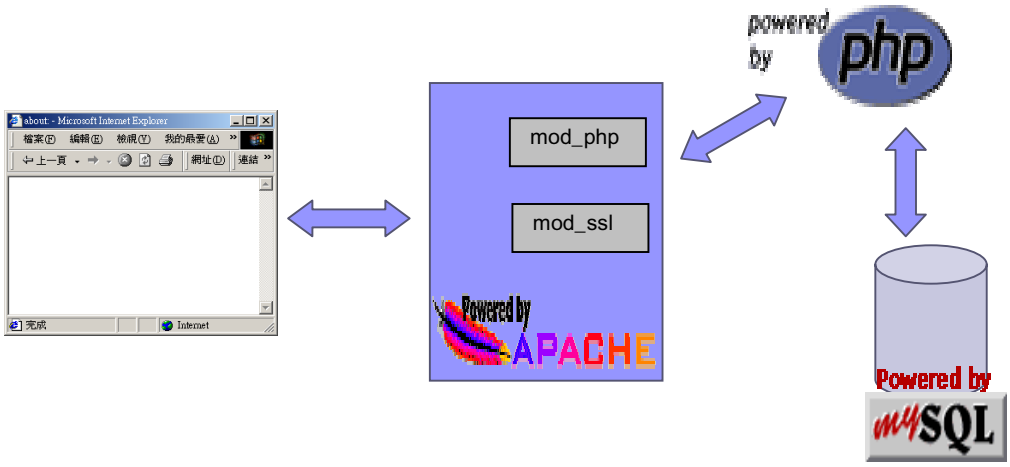
Server Type	***Package in Redhat 7***	***Server Type***	***Package in Redhat 7***
Web server	apache-1.3.12	News server	inn-2.2.3
Mail server	sendmail-8.11.0	LDAP server	openldap-1.2.11
FTP server	wu-ftpd-2.6.1	DHCP server	dhcp-2.0
Proxy server	squid-2.3.STABLE4	PPP server	ppp-2.3.11
DNS server	bind-8.2.2_P5	Kerberos server	krb5-server-1.2.1
Telnet server	telnet-server-0.17	Rsh server	rsh-server-0.17
Database	mysql-server-3.23.24, postgresql-server-7.0.2	File server	samba-2.0.7, nfs-utils-0.1.9.1
Version control	cvs-1.10.8, rcs-5.7	Firewall	ipchains-1.3.9, tcp_wrappers-7.6

表一. RedHat Linux 7 內建伺服器

一、Internet 服務

1.Apache[2] + SSL[3,4] + PHP[5] + MySQL[6]

當 1993 年 World Wide Web(WWW)出現時，沒有人能料得到今日受歡迎的程度，WWW 已經成爲網際網路最大的應用，因爲簡單易用的瀏覽器，加上圖文並茂的網頁，成爲吸引許多人上網的主因。近年來電子商務興起， Apache web server 加上 SSL 模組加密傳輸內容，搭配 PHP 讓網頁更生動，後端配合 MySQL database，圖一的架構成爲愈來愈流行的電子商務網站套餐，本節將介紹如何安裝設定這些常見的伺服器。



圖一. Apache+SSL+PHP+MySQL 運作圖

相關檔案與指令	說 明
/etc/rc.d/init.d/httpd	控制 Apache 啓動與停止的 script 檔
/etc/httpd/conf/httpd.conf	Apache 設定檔
/etc/rc.d/init.d/mysqld	控制 MySQL 啓動與停止的 script 檔
mysqladm	MySQL 管理程式
mysqlshow	查詢 MySQL 資料庫
mysql	MySQL 用戶端程式

表二. Apache/MySQL 相關檔案與指令

重要設定：/etc/httpd/conf/httpd.conf

重 要 參 數	說 明
Port 80	Standalone 伺服器所接聽的 port
DocumentRoot "/var/www/html"	系統首頁放置的目錄
DirectoryIndex index.html index.htm	預設的首頁
UserDir public_html	使用者放置首頁的目錄

表三. Apache 重要參數

2. Qmail mail Server [7]

電子郵件(Email)現在也是網際網路上相當重要的服務，幾乎每個上網者都有自己的電子郵件信箱，可以每天和親友交換訊息。電子郵件相關的協定有兩個：

A. SMTP (Simple Mail Transfer Protocol)

用戶端連接郵件主機的 port 25，將信件送至郵件主機，一般主機與主機間交換信件大部份也都採用這種方式。

B. POP3 (Post Office Protocol)

用戶端連接郵件主機的 port 110 下載整批郵件，然後就可以在離線的狀況下閱讀自己的郵件，亦可以自行設定是否刪除郵件主機上的信件。

目前最廣泛使用的郵件伺服器當屬 sendmail，但是 sendmail 長久以來皆有重大的安全性問題，於是近年來 Qmail 漸漸嶄露頭角，許多著名郵件服務網站例如 Hotmail、Yahoo mail 皆改用 Qmail，主要因爲下列幾點特色：

1. **安全性**：Qamil 不像 sendmail 以 root 執行主程式，而改以特定 qmail 群組及 qmail 使用者來執行程式，加強系統的安全。
2. **效能**：Qmail 在執行效能上遠高於 sendmail。
3. **可靠性**：Qmail 在收信時，同時執行寫入硬碟的動作，不像傳統的 mail daemon 要等完整接收之後才寫入硬碟，因此，即使系統斷電，Qmail 也不會漏失訊息。
4. **管理便利**：相較於 sendmail 的複雜設定，Qmail 在系統管理上相對的便利許多。

設 定 檔	意 義
/var/qmail/control/me	包含本地端的機器名稱
/var/qmail/control/rcpthosts	Qmail 會寄送的位置
/var/qmail/control/locals	本地端的地址
/var/qmail/badmailfrom	拒收郵件來源地址

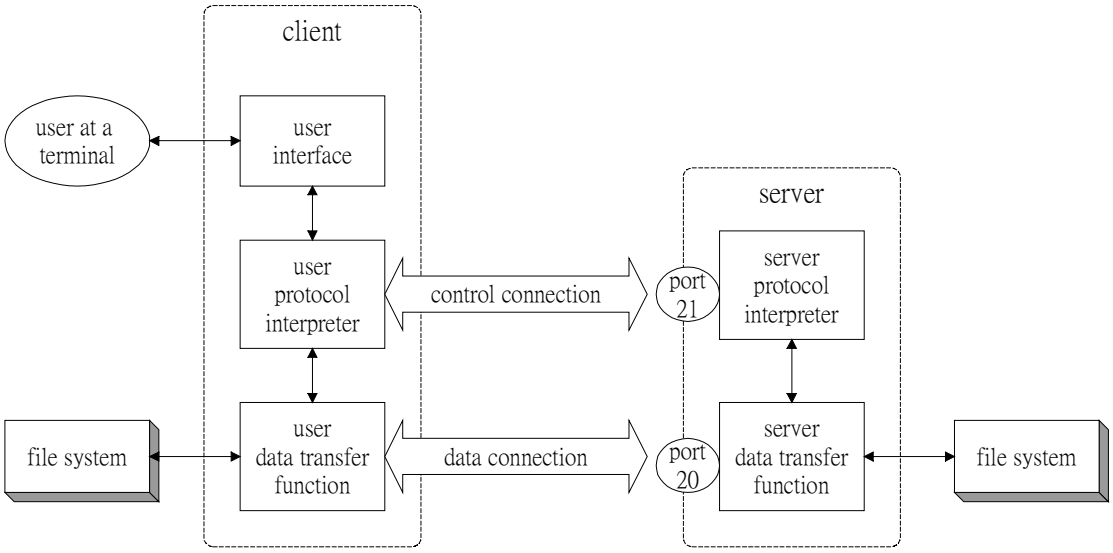
表四. Qmail 重要設定檔

三、wu-ftpd FTP Server[8]

當有需要提供下載檔案服務時，除了使用 http 的方式連結外，另外一種常用的方法就是 ftp 直接下載。FTP(File Transfer Protocol, RFC 959)的設計是用來傳輸兩台電腦之間的資料，如圖二所示，用戶端和伺服器端會有兩個不同的連線，伺服器的 port 21 負責 FTP 指令的傳送，而 port 20 則負責資料的傳送。

Ftp Server 服務的對象可區分爲兩類:

- 認證式 FTP：對象是在該主機上有帳號的使用者，當使用者以帳號登入時，其登入的目錄就是其帳號目錄 (home directory)，使用者有權對檔案做讀寫。
- 匿名式 FTP：對象是網路上任何一位使用者，他們可以使用匿名帳號如 ftp 或 anonymous 登入有提供該服務的主機，這些使用者只能抓取檔案，不過有些站台也提供上傳的目錄。



圖二. FTP protocol (RFC 959)

相關檔案與指令	說　明
ftpwho	檢視有哪些使用者登入 ftp server
ftpshut	暫時關閉 ftp server，會根據給的參數產生一個 /etc/shutmsg 檔案，若要啓動只需刪除該檔案。
/etc/ftpaccess	設定 ftp server 的存取控制及基本設定
/etc/ftpconversions	設定 ftp 傳輸時，壓縮/解壓的處理
/etc/ftpgroups	設定哪些群組不能登入
/etc/ftphosts	設定哪些網路主機不能登入
/etc/ftpusers	設定哪些帳號不能登入
/var/ftp/pub/	此目錄放置供匿名使用者下載的檔案

表五. wu-ftpd 相關檔案與指令

重要設定：/etc/ftpaccess

重 要 參 數	說 明
`banner /var/ftp/banner.msg`	登入前顯示歡迎訊息 banner.msg
`deny *.edu.tw /var/ftp/deny.msg`	拒絕 edu.tw 網域的連線，並顯示 deny.msg
`limit all 20 any /etc/limit.msg`	限定 all 類別在任何時間最多可以有 20 個人登入，若超過則顯示 limit.msg
`loginfails 5`	登入時容許密碼輸入錯誤 5 次

表六. wu-ftpd 重要參數

二、Intranet 服務

1.Samba file server[9]

架設區域網路的主要目的，在於能夠彼此共享資源。例如有一份通訊錄放在伺服器上，當資料更動時，自行 ftp 回來修改再放回去，但資料常常需要異動時，這樣的手續顯得相當麻煩，於是在 Unix 系統下的解決方案是 NFS(Network File System)，而 Windows 系統使用「網路上的芳鄰」，皆是可以直接存取共享遠端的檔案，形成快速有效率的工作環境。

Samba 能讓 Linux 系統整合到 Windows 的網路系統成爲用戶端與伺服器端。當成伺服器時，能提供其他 Windows 系統檔案存取與列印等服務；當成用戶端時也可以存取分享出來的 Windows 檔案系統。本文僅就伺服器端的設定加以說明。

相關檔案與指令	說 明
smbd	提供用戶端 SMB 服務的程式(daemon)
nmbd	負責 Netbios name 查詢
/etc/samba/smb.conf	Samba 的設定檔
/etc/rc.d/init.d/smb	控制 Samba 啓動與停止的 script 檔
/etc/lmhosts	記載 Netbios name 與 IP 對應的檔案
testparm	測試 Samba 的 smb.conf 設定是否正確
testprns	測試印表機在/etc/printcap 設定是否正確

表七. Samba 相關檔案與指令

重要設定：/etc/samba/smb.conf

Samba 所有的設定皆在此檔，內文中以「#」符號或「;」符號開頭的整行文字是註解，通常「;」符號是用來暫時關閉該選項。整個檔案內容可分 Global Setting 和 Share Definition 兩大部份，再細分爲幾個區段，每個區段都以[區段名稱]開頭，並有相關的設定：

- Global Setting:
  - [global]: Samba server 的基本設定。
- Share Definition:
  - [home]:設定存取 Samba server 的使用者 home directory。
  - [printers]:設定分享的印表機。
  - [分享名稱]:設定其他的共享目錄，可以自行定義多個。

global、home、printers 是固定的基本區段，共享目錄則是依需求自行增加，表八介紹每個區段的重要參數設定。

smb.conf—[global]

重 要 參 數	*說 明*
workgroup = MYGROUP	相當於 Windows 中的工作群組
server string = Samba Server	伺服器的說明
hosts allow = 192.168.1. hosts deny = 192.168.2.	允許或不允許進入 samba server 的 IP 位置範圍，注意是網路位址，最後必須加上一個「.」
load printers = yes	是否要將印表機分享出去
printcap name = /etc/printcap	印表機設定檔
security = user	設定 samba 的安全性等級，目前有四種選擇 share: 對各目錄設不同密碼分享，或讓 guest 進入 user: 讓有帳號的使用者輸入密碼登入 server: 由別台機器驗證密碼 domain: 登入 NT 網域
password server = <NT-Server-Name>	如果 security 設爲 server，必須指定驗證主機名
encrypt passwords = yes	傳送資料加密
smb passwd file = /etc/smbpasswd	如果驗證的主機是 samba server，指定密碼檔案
username map = /etc/smbusers	Linux 使用者名稱對應到不同的 SMB 使用者名稱
interfaces = 192.168.12.2/24 192.168.13.2/24	如果 Samba server 主機有多片網路卡，可以在此設定
name resolve order = wins lmhosts bcast	設定 NetBios 主機名稱與 IP 位址對應的查詢順序
client code page = 950	可以使用中文檔名

smb.conf—[home]

參 數	*說 明*
comment = Home Directories	目錄的說明
browseable = no	設定可否瀏覽
writable = yes	設定可否寫入

smb.conf—[printers]

參 數	*說 明*
comment = All Printers	印表機的說明
path = /var/spool/samba	設定 spool 目錄
browseable = no	設定可否瀏覽

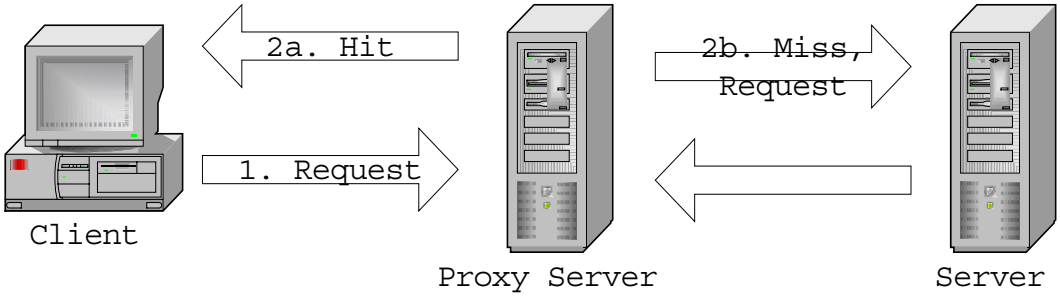
smb.conf—[分享名稱]

參 數	*說 明*
comment = Share	分享的說明
path = /tmp	開放/tmp 目錄
readonly = no	設定可否唯讀或可寫入
public = yes	設定是否共享

表八. Samba 重要參數

◆ Squid Proxy Server[10]

在網際網路上，當用戶端向伺服器要求資料時，伺服器立即傳回所需的資料。但這個伺服器可能距離很遠，資料傳送必須花很多時間，而且很可能同一網域內多個用戶端大老遠去要求同一份資料，於是 proxy 在這種情況下應運而生。當客戶端要向伺服器要求資料時，會如圖三所示，(1.)先詢問 proxy server 是否已經有這一筆資料，(2a.)如果有的話 proxy server 會立刻傳回給客戶端，(2b.)如果沒有的話，proxy server 再代替客戶端到伺服器抓取資料回來。



圖三. Proxy server 運作原理

相關檔案與指令	說 明
squid	squid 主程式
/etc/rc.d/init.d/squid	控制 squid 啓動與停止的 script 檔
/etc/squid/squid.conf	squid 設定檔

表九. squid 相關檔案與指令

重要設定：/etc/squid/squid.conf

重 要 參 數	說 明
http_port 3128	squid 使用的 port
cache_peer hostname type http_port icp_port	當 squid 中沒有查詢的資料時，可以向其它的 peer proxy server 查詢。其中 type 分爲兩種：1. parent, 2.sibling，若 peer proxy server 皆沒有資料時，會再要求最快回應的 parent proxy sever 取回資料。
cache_peer_domain cache-host domain [domain ...]	指定 domain 的資料向 cache-host 查詢，如果 domain 前加上「!」符號表示這個網域不向 cache-host 查詢。
cache_mem 8 MB	設定處理資料的記憶體大小，通常專職的 proxy server 可以設爲全部記憶體的 3/4，如果主機同時執行其它的伺服器，可以設爲 1/3。
maximum_object_size 4096 KB	如果查詢的資料大於這個值就不會儲存到磁碟上
cache_dir Type Directory-Name Mbytes Level-1 Level-2	可以設定多行來指定不同的 cache 目錄。Type 一般設爲 ufs，Directory-Name 爲存放暫存資料的目錄，Mbytes 爲這個目錄所使用的容

	量，Level-1 是第一層的子目錄數量，Level-2 爲第二層子目錄數量。
reference_age 1 year	設定資料最長的保留時間
http_access allow|deny [!]aclname ...	設定 proxy server 開放的對象

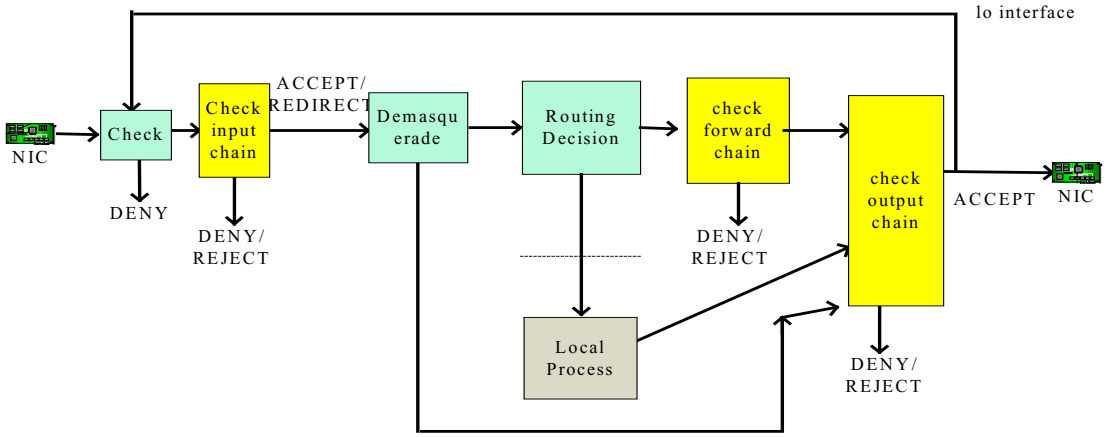
表十. squid 重要參數

◆ Ipchains Firewall[11]

網路上的防火牆能夠將內部區域網路與外界隔離，避免遭受到外界的攻擊，本節介紹的是目前 Linux 核心內建的 Ipchains。Ipchains 是封包過濾型的防火牆，它依據一些預先設定好的規則(rules)，來決定是否讓封包進出。

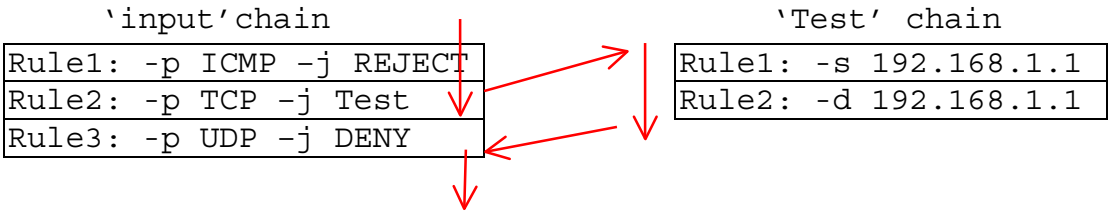
所謂的 chain 就是一些規則的集合，在 Ipchains 中有三個內建的 chains，分別用於封包進入(input)、送出(output)、轉送(forward)時的封包處理。如圖四所示，封包由左邊的網路卡進來後會經過 input chain，若是轉送的封包則會經過 forward chain，封包要送出時則會經過 output chain。每個 chain 按照規則的順序逐一比對封包，若符合任一條規則就依指定的方式處理 (以 -j 參數指定)，目前有六種內建的處理方式：

- ACCEPT: 讓封包通過
- DENY: 丟棄封包
- REJECT: 丟棄封包，並回覆 host unreachable 的 ICMP 封包
- MASQ: masquerade 封包可以做 NAT，僅用於 forward chain
- REDIRECT: 轉送到特定的 port，僅用於 input chain
- RETURN: 直接跳到 chain 的結尾



圖四. 封包的處理流程

除了上述的處理方式之外，如圖五所示，也可以跳到另一個使用者自行定義的 chain，比對有沒有符合的規則，若沒有的話再跳回原來的 chain 的下一條規則。若內建的 chain 沒有符合的規則，則執行該 chain 的預設處理方式(policy)，可以是上述的前四種之一。



圖五. chain 的規則比對流程

基本操作：以 root 的身份執行

- 處理 chains (下列[chain]若未指定則代表所有的 chains)
  1. 建立新的 chain：ipchains -N chain
  2. 刪除 chain： ipchains -X chain
  3. 改變 chain 的 policy： ipchains -P chain policy
  4. 列出 chain 的 rule：ipchains -L [chain]
  5. 刪除 chain 的所有 rule： ipchains -F [chain]
- 更改 chains 的規則：
  1. 增加一條新的規則：ipchains -A chain
  2. 刪除第一個符合的規則：ipchains -D chain
  3. 刪除某個位置的規則：ipchains -D chain rulenum
  4. 在某位置加入一條新的規則：ipchains -I chain [rulenum]
  5. 替換某個位置的規則：ipchain -R chain [rulenum]
- 規則的語法
  1. -s:指定來源，-d:指定目的：可用 domain name 或 ip 指定單一的目標，或是以 IP/netmask 的方式指定一網域，例如 192.168.1.0/24 或 192.168.1.0/255.255.255.0 皆是代表從 192.168.1.0 到 192.168.1.255 所有的機器。
  2. 指定 port：例如-s 192.168.0.1 3000:3010 代表從 192.168.0.1 機器上的 3000 至 3010 這 11 個 ports。若是 port 指定範圍少了其中一個的話，下界預設值是 0，上界預設值是 65535。
  3. -p：指定協定，例如 TCP,UDP,ICMP。
  4. -i：指定介面，例如 eth0, ppp0。
  5. -y：指定建立 TCP 連線封包(SYN)
  6. -j：指定符合此條規則時的處理方式(ACCEPT,DENY,…)或跳到另一個 chain
  7. !：代表否定，例如 -p ! TCP，表示非 TCP 的連線，注意「!」前後都必須留空白。

IV. 實驗方法

本實驗的安裝方式以 RPM 爲主，RPM 是由 RedHat 公司所開發的一個程式管理套件，

使用 RPM 套件管理系統具有下列優點：

一、易於安裝與升級。

二、有強大的查詢功能。

三、可以驗證套件完整性。

四、支援以原始碼發行的套件。

RPM 套件命名的格式大都依循一致的慣例，以 apache-1.3.12-25.i386.rpm 爲例，它包含了套件名稱(apache)、版本(1.3.12)、發行編號(25)和平台(i386)，並且以 rpm 結尾。要安裝此套件也相當簡單

```
# rpm -Uvh apache-1.3.12-25.i386.rpm
```

-U 參數代表昇級原有的套件，若原本未安裝則進行安裝。

-v 參數代表在安裝過程中提供更多訊息。

-h 參數會在安裝過程中印出「#」符號。

要移除套件則只需一行指令:

```
# rpm -e apache
```

V. 實驗步驟

一、架設 Internet 服務

注意，以下的步驟需要以 root 的身份執行。

1.架設 Apache+SSL+PHP+MySQL

A.準備檔案：

php-4.0.1pl2-9.i386.rpm	*PHP scripting language*
php-mysql-4.0.1pl2-9.i386.rpm	*以 php 連結 MySQL 資料庫*
mysql-3.23.24-1.i386.rpm	*MySQL 用戶程式及 shared library*
mysql-server-3.23.24-1.i386.rpm	*MySQL 伺服器*
apache-1.3.12-25.i386.rpm	*Apache 網頁伺服器*
openssl-0.9.4-3.i386.rpm	*Secure Sockets Layer Toolkit*
mod_ssl-2.6.6-25.i386.rpm	*Apache 的 SSL 模組*
mod_php-4.0.1pl2-9.i386.rpm	*Apache 的 PHP 模組*

B.安裝所有套件

```
# rpm -Uvh php-4.0.1pl2-9.i386.rpm
# rpm -Uvh mysql-3.23.24-1.i386.rpm
# rpm -Uvh mysql-server-3.23.24-1.i386.rpm
# rpm -Uvh php-mysql-4.0.1pl2-9.i386.rpm
# rpm -Uvh apache-1.3.12-25.i386.rpm
# rpm -Uvh openssl-0.9.4-3.i386.rpm
# rpm -Uvh mod_ssl-2.6.6-25.i386.rpm
```

```
# rpm -Uvh mod_php-4.0.1pl2-9.i386.rpm
```

C.執行 Apache 與 MySQL

```
# /etc/rc.d/init.d/httpd start
# /etc/rc.d/init.d/mysqld start
```

D.設定 MySQL root 密碼爲 passwd (讀者可以自己選擇適當的密碼)

```
# /usr/bin/mysqladmin -u root password 'passwd'
```

E.設定開機自動執行

```
# ntsysv; 勾選 httpd, mysqld ; 選 OK
```

F.測試 Apache

以瀏覽器連上伺服器 https://*your.domain.name*(讀者 Linux 伺服器的網址)【紀錄 1】

G.測試 MySQL

```
/usr/bin/mysqlshow -u guest【紀錄 2】
```

H.測試 PHP&MySQL:編輯一測試檔 test.php3，內容如下

```
<? mysql_connect("localhost") && print "MySQL and PHP work"; ?>
```

【紀錄 3】

2.架設 Qmail 郵件伺服器

A.準備檔案：

http://cr.yp.to/software/qmail-1.03.tar.gz *qmail 主程式*

http://cr.yp.to/software/checkpassword-0.81.tar.gz *使 qmail pop3 server 支援系統密碼檔*

B.建立安裝目錄、2 個群組與 7 個使用者

```
# mkdir /var/qmail
# groupadd nofiles
# useradd -g nofiles -d /var/qmail/alias alias
# useradd -g nofiles -d /var/qmail qmaild
# useradd -g nofiles -d /var/qmail qmaill
# useradd -g nofiles -d /var/qmail qmailp
# groupadd qmail
# useradd -g qmail -d /var/qmail qmailq
# useradd -g qmail -d /var/qmail qmailr
# useradd -g qmail -d /var/qmail qmails
```

C.解開並安裝 Qmail

```
# tar zxvf qmail-1.03.tar.gz
# cd qmail-1.03
# make setup check
```

D.設定(your.domain.name, your.email 須換爲讀者自己的 domain,email)

```
# ./config-fast your.domain.name
```

```
# cd ~alias
# echo your.email > .qmail-postmaster
# echo your.email > .qmail-mailer-daemon
# echo your.email > .qmail-root
# chmod 644 .qmail*
```

E.建立使用者郵件目錄(Maildir)

爲每個現有的使用者(以 luke 爲例)建立郵件目錄

```
# su luke
$ /var/qmail/bin/maildirmake $HOME/Maildir
$ echo $HOME/Maildir/ > $HOME/.qmail
$ exit
```

爲以後加入的使用者準備郵件目錄

```
# /var/qmail/bin/maildirmake /etc/skel/Maildir
# echo ./Maildir > /etc/skel/.qmail
```

F.建立啓動檔 /var/qmail/bin/rc

```
# cp /var/qmail/boot/home /var/qmail/bin/rc
```

修改 /var/qmail/bin/rc，將 Mailbox 改爲 Maildir

```
qmail-start ./Maildir splogger qmail
```

G. 停止 sendmail 服務，以 qmail 取代 sendmail

```
# ntsysv; 取消選取 sendmail; 選 OK
# kill `echo /var/run/sendmail.pid`
# mv -f /usr/lib/sendmail /usr/lib/sendmail.old
# mv -f /usr/sbin/sendmail /usr/sbin/sendmail.old
# ln -s /var/qmail/bin/sendmail /usr/lib/sendmail
# ln -s /var/qmail/bin/sendmail /usr/sbin/sendmail
```

H.安裝 Pop-3 服務

```
# tar zxvf checkpassword-0.81.tar.gz
# cd checkpassword-0.81
# make
# make setup check
```

I.增加 smtp,pop3 服務至 xinetd (RedHat 7.0 預設的超級伺服器，作用和常見的 inetd 一樣，但功能和安全性較強，當接收到連結要求時，xinetd 才起始適當的伺服器，例如此節是 Qmail)

增加檔案/etc/xinetd.d/smtp，內容如下：

```
service smtp
{
        disable         = no
        socket_type     = stream
```

```
        protocol        = tcp
        wait            = no
        user            = qmaild
        server          = /var/qmail/bin/tcp-env
        server_args     = /var/qmail/bin/qmail-smtpd
        log_on_failure  += USERID
}
```

增加檔案/etc/xinetd.d/pop-3，內容如下：(server_args 與下行爲同一行)

```
service pop-3
{
    disable = no
    socket_type     = stream
    protocol        = tcp
    wait            = no
    user            = root
    server          = /var/qmail/bin/qmail-popup
    server_args     = your.domain.name /bin/checkpassword
  /var/qmail/bin/qmail-pop3d Maildir/
    log_on_failure  += USERID
}
```

J.重新執行 xinetd 和 Qmail

```
# /etc/rc.d/init.d/xinetd restart
# /var/qmail/bin/rc &
```

K.檢查/var/log/maillog 的內容【紀錄 4】

L.由此機器寄一封電子郵件給助教。

3.架設 wu-ftp 伺服器

A.準備檔案

wu-ftpd-2.6.1-6.i386.rpm	*wu-ftpd 主程式*
anonftp-3.0-9.i386.rpm	*anonymous ftp 套件*

B.安裝所有套件

```
# rpm -Uvh wu-ftpd-2.6.1-6.i386.rpm
# rpm -Uvh anonftp-3.0-9.i386.rpm
```

C.設定開機自動執行

```
# ntsysv; 選取 wu-ftpd; 選 OK
```

D.執行 xinetd

```
# /etc/rc.d/init.d/xinetd restart
```

E.上傳檔案至自己的目錄下，抓取此螢幕畫面【紀錄 5】

二、架設 Intranet 服務

1.架設 Samba 檔案伺服器

A.準備檔案

samba-common-2.0.7-21ssl.i386.rpm　*Samba 伺服器及用戶端皆會使用的檔案*

samba-2.0.7-21ssl.i386.rpm　*Samba 伺服器*

samba-client-2.0.7-21ssl.i386.rpm　*Samba 用戶端程式*

B.安裝所有套件

```
# rpm -ivh samba-common-2.0.7-21ssl.i386.rpm
# rpm -ivh samba-2.0.7-21ssl.i386.rpm
# rpm -ivh samba-client-2.0.7-21ssl.i386.rpm
```

C.設定開機自動執行

```
# ntsysv;勾選 smb;選 OK
```

D.設定使用者密碼登入，修改/etc/samba/smb.conf 使用下列參數

```
security = user
encrypt passwords = yes
smb passwd file = /etc/samba/smbpasswd
```

設定使用者 luke 的密碼，重覆輸入兩次新的密碼

```
# smbpasswd -a luke
```

E.執行

```
# /etc/rc.d/init.d/smb start
```

F.測試連接 Samba 伺服器

方法一：以 Window98, 2000 選取「網路上的芳鄰」→選取讀者您的工作群組→選取您的機器，輸入帳號及密碼，抓取整個過程的螢幕畫面【紀錄 5】

方法二：「開始」→「執行」→輸入「\\your.domain.name」(your.domain.nam 需換爲讀者自己的伺服器位置)

2.架設 Squid proxy 伺服器

A.準備檔案(以 root 的身份執行下列入步驟)

```
# squid-2.3.STABLE4-1.i386.rpm
```

B.以 root 安裝

```
# rpm -Uvh squid-2.3.STABLE4-1.i386.rpm
```

C.設定開機自動執行

```
# ntsysv; 選取 squid; 選 OK
```

D.更改存取控制(此處設爲任何人可以使用此 proxy server，可依讀者需要自行設定)

修改/etc/squid/squid.conf，將 http_access　deny all 改爲

```
http_access allow all
```

E.執行 squid

```
# /etc/rc.d/init.d/squid start
```

F.設定瀏覽器使用此 proxy 伺服器(以 IE5 爲例)

開啓 IE5，選取「工具」→「Internet 選項」→「連線」→「區域網路設定」，勾選「使用 proxy 伺服器」，網址填入 `http://your.domain.name`(讀者 Linux 伺服器的網址)，「連接埠」填 `3128`

G.測試

在任一台裝有 PHP 的伺服器上，準備一個測試網頁 info.php，內容如下

```
<? phpinfo(); ?>
```

以瀏覽器連上此網頁，檢查 Apache Environment 中 HTTP_VIA 的值【紀錄 7】

3.測試 ipchains 防火牆

測試在 input chain 擋住所由本機發送的 ICMP 封包：

```
# ping -c 1 127.0.0.1
# ipchains -A input -s 127.0.0.1 -p icmp -j DENY
# ping -c 1 127.0.0.1
```

觀查發生的現象【紀錄 8】

VI. 實驗紀錄

紀錄	內容
1	
2	
3	
4	
5	
6	
7	
8	

VII. 問題與討論

注意：請針對問題中每一項目回答，並避免引述「太」多資料。

1. 請解釋 [紀錄 1] 的結果，以及該如何處理？

2. 在 Qmail 中如何設定 Relay 以防止廣告信？

3. 若想開放匿名使用者上傳檔案，wu-ftp 伺服器該如何設定？

4. 在[紀錄五]的步驟中，該如何設定才可以不用輸入帳號密碼？

5. 在用戶端要求資料時，Squid 如何辨別本身的資料是最新的？

6. 試著列出在架設 Intranet 環境時，ipchains 該設定哪些規則？

7. 自問自答，即自己發掘問題，自己找出答案（給分將根據題目設計的「嚴謹程度」、「難度」與「作答的品質」）。

Ⅷ. 參考文獻

[1] Red Hat, http://www.redhat.com/
[2] The Apache Software Foundation, http://www.apache.org/
[3] mod_ssl: The Apache Interface to OpenSSL, http://www.modssl.org/
[4] OpenSSL: The Open Source toolkit for SSL/TLS, http://www.openssl.org/
[5] PHP: Hypertext Preprocessor, http://www.php.net/
[6] MySQL, http://www.mysql.com/
[7] The qmail home page, http://www.qmail.org/
[8] WU-FTPD Development Group, http://www.wu-ftpd.org/
[9] SAMBA, http://www.samba.org/
[10] Squid Web Proxy Cache, http://www.squid-cache.org
[11] Linux IP Firewalling Chains, http://netfilter.filewatcher.org/ipchains/