FTP伺服器介紹

陳柏愷

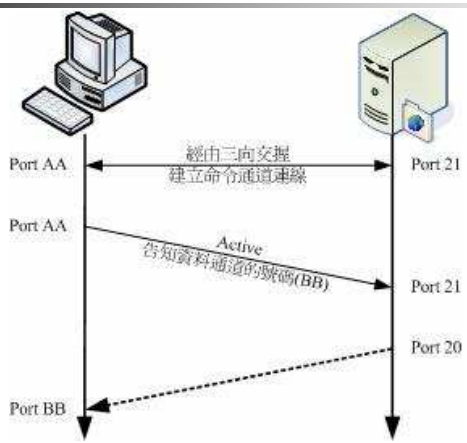
FTP簡介

- FTP（File Transfer Protocol），是一個用來在網路上傳輸檔案的協定，方便簡單而且普及
- 常見的FTP server軟體
  - wuftp：早期最知名的ftp，但因安全上的問題，現在已較少人使用
  - proftpd:功能強大且較安全的ftp server
  - vsftpd:以安全性為主要考量，重新設計的ftp server
- 常見的ftp client軟體
  - Filezilla:自由軟體，有windows跟Linux版，圖形操作介面，功能強大且易於使用
  - ncftp:功能強大的指令式軟體

FTP協定簡介

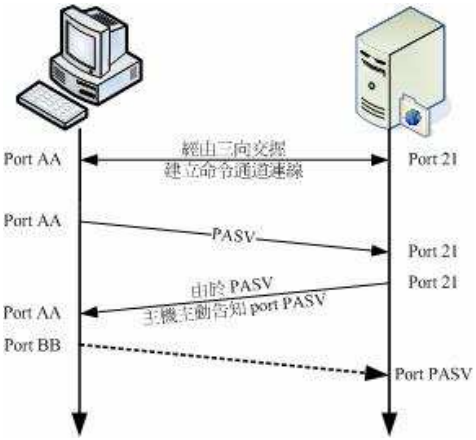
- FTP在網路上是以明碼傳輸，使用者的帳號密碼都可以被竊聽，傳輸的檔案也可以被竊取
  - 如果可以的話，盡量以sftp來取代ftp
  - sftp是由ssh所提供的加密型檔案傳輸服務
- FTP使用兩個通道來傳輸資料
  - 命令通道：用來下指令與溝通。ftp server永遠開啟port 21，等待使用者連線
  - 資料流通道:用來傳輸檔案或傳輸指令的執行結果。連線方式有主動模式(Active Mode)與被動模式(Passive Mode)兩種

FTP主動模式連線



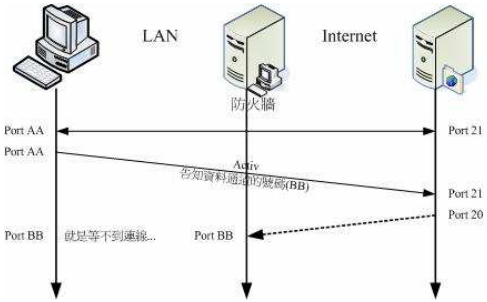
- 資料流通道是由Server端主動發出
- Server 端固定由Port 20連向Client端動態開啟的port

FTP被動模式連線



- 資料流通道是由Client端主動發出，Server被動接收
- Server端動態開啟新的port，供資料流通道使用

FTP連線時的防火牆問題



- 若Client端位於防火牆(NAT)底下，則他無法動態開啟port給外面的人(FTP Server)連線
- 故不能使用Active Mode，只能使用Passive Mode

VSFTPD的安全性設計

- vsftpd 這個服務的不使用完全的root權限來啟動，僅在有需要的地方採取高權限，因此即使遭受攻擊，影響的層面也比較小。
- 使用chroot來縮限這隻程式可以接觸到的檔案目錄。
- 絕大部分 ftp 會使用到的額外指令功能 (dir, ls, cd ...) 都已經被整合到 vsftpd 主程式當中。

VSFTPD使用者分級

- 實體用戶 (Real user)
  - 一般可以透過ssh等方式登入，操作伺服器的人
  - 因為FTP協定會將帳號密碼以明碼傳輸，很容易被竊取，因此建議不開放real user使用ftp，而改用sftp
- 訪客身份 (Guest)
  - 特別針對vsftpd用途開放的帳號，其他服務都不可用
- 匿名登入使用者 (anonymous)
  - 不需帳號密碼即可登入

vsftpd安裝(Fedora 11)

- yum install vsftpd
- 或自行下載安裝
  - wget http://ftp.twaren.net/Linux/Fedora/linux/updates/11/i386/vsftpd-2.1.2-2.fc11.i586.rpm
  - rpm -ivh vsftpd-2.1.2-2.fc11.i586.rpm
- Client端請在windows上下載Filezilla安裝
  - http://filezilla-project.org/
- ftp client
  - yum install ftp

vsftpd開機自動啟動設定

- 使用指令ntsysv，打開vsftpd
- 使用指令serviceconf，打開vsftpd
- 或
  - su
  - cd /etc/rc3.d
  - ln –s ../init.d/vsftpd S98vsftpd
  - cd /etc/rc5.d
  - ln –s ../init.d/vsftpd S98vsftpd
- 手動啟動: /etc/init.d/vsftpd start
- 手動停止: /etc/init.d/vsftpd stop
- 記得要打開防火牆
- 記得打開SELinux
  - setsebool –P allow_ftpd_full_access on
  - 或修改/etc/selinux/config,重新開機

vsftpd主要的設定檔

- /etc/vsftpd/vsftpd.conf
  - vsftpd最主要的設定檔
- /etc/vsftpd/user_list
  - 預設不可登入的帳號，可改設定為可登入，建議不更動
- /etc/vsftpd/ftpuser
  - 預設不可登入的帳號，建議不更動
- /etc/pam.d/vsftpd
  - 進階的使用者認證設定檔，建議不更動

vsftpd.conf重要參數

- anonymous_enable
  - 允許匿名登入
- local_enable
  - 實體使用者登入
- write_enable
  - 允許使用者上傳資料
- anon_upload_enable
  - 允許匿名者上傳
- anon_mkdir_write_enable
  - 允許匿名者建立目錄
- listen
  - YES: standalone mode
  - NO:使用super daemon(inetd)

練習一:開放匿名用戶登入

- 允許匿名登入且讀取
  - anonymous_enable=YES
- 不允許匿名寫入
  - anon_upload_enable=NO
- 不允許匿名創造目錄
  - anon_mkdir_write_enable=NO
- 放一個檔案到/var/ftp/pub底下供讀取

練習二:開放實體用戶登入

- 允許實體使用者登入
  - local_enable=YES
- 允許實體使用者寫入
  - write_enable=YES
- 限制實體使用者只能在自己目錄下
  - chroot_local_user =YES
- 限制個人最大流量(Bps)
  - local_max_rate=100000
- 限制同時上線人數
  - max_clients=10
- 限制同一個IP同時連線數
  - max_per_ip=2