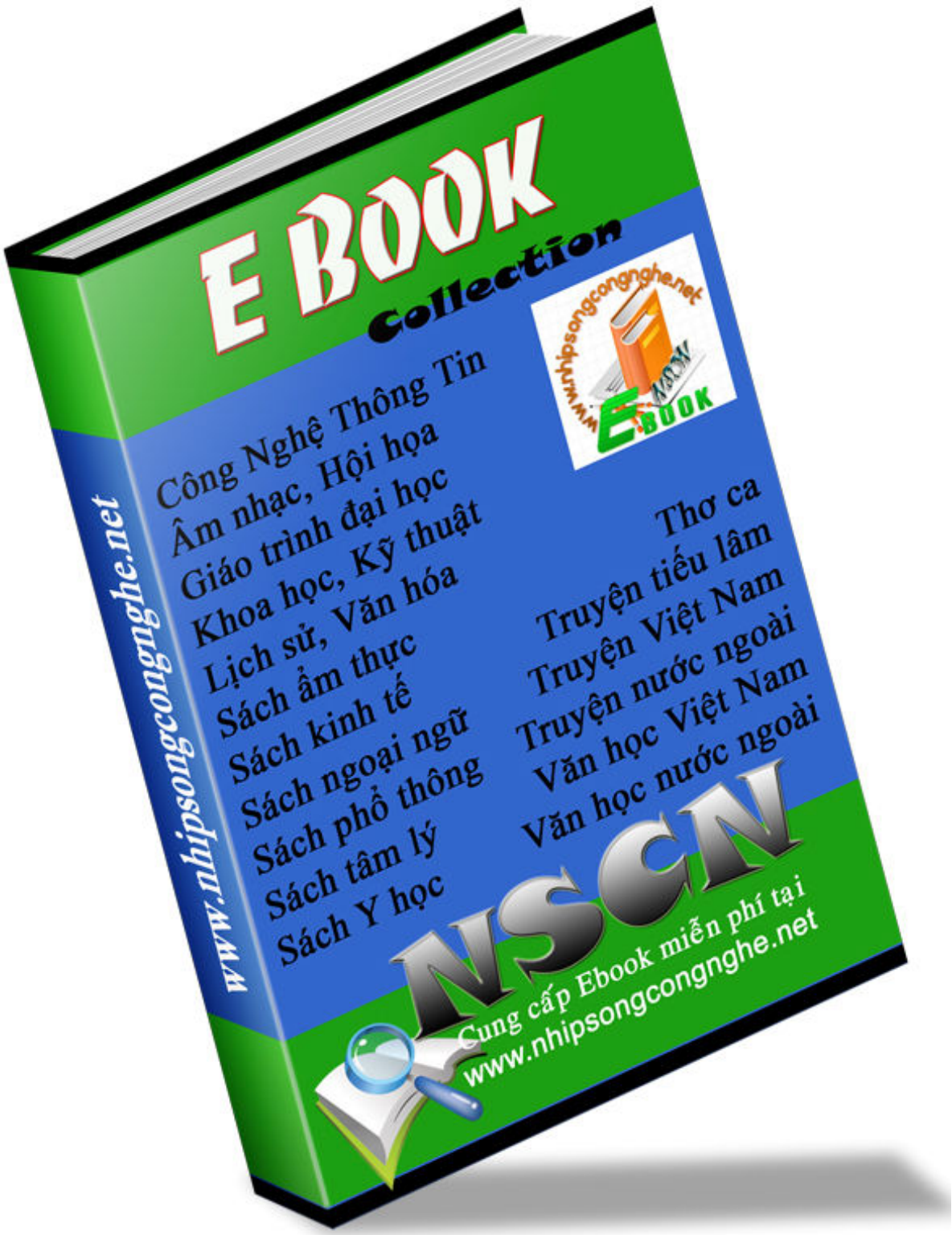

E BOOK
Collection
Công Nghệ Thông Tin
Âm nhạc, Hội họa
Giáo trình đại học
Khoa học, Kỹ thuật
Lịch sử, Văn hóa
Sách ẩm thực
Sách kinh tế
Sách ngoại ngữ
Sách phổ thông
Sách tâm lý
Sách Y học
Thơ ca
Truyện tiếu lâm
Truyện Việt Nam
Truyện nước ngoài
Văn học Việt Nam
Văn học nước ngoài
www.nhipsongcongnghe.net
NSCN
Cung cấp Ebook miễn phí tại
www.nhipsongcongnghe.net

# CÀI ĐẶT HỆ ĐIỀU HÀNH LINUX REDHAT 8.0

1. Một số điều lưu ý trước khi cài:

Để cài RedHat 8.0 chạy trơn tru thoải mái, bạn cần có hệ thống PII, 64MB Ram trở lên, và phân vùng ổ cứng dành để cài Linux cần khoảng 2GB trở lên. Tuy nhiên không có gì cản trở bạn cài Linux trên một hệ thống có cấu hình thấp hơn, nhưng khi đó bạn chỉ có thể chạy với các ứng dụng hạn chế trên hệ thống.

· Nên tìm hiểu thông số cấu hình của hệ thống trước khi cài đặt. Điều này rất quan trọng, giúp bạn thuận lợi trong quá trình cấu hình hệ thống sau khi cài đặt. Bạn sẽ phải lựa chọn cho đúng thông số của các linh kiện phần cứng trong quá trình cấu hình hệ thống như: loại card màn hình, loại màn hình( tần số quét ngang, dọc), card mạng, card âm thanh. v.v.

· Cần chuẩn bị phân vùng đĩa còn trống để cài Linux. Linux cần tối thiểu hai phân vùng là Linux Native (ext3) và Linux swap. Đơn giản, bạn có thể dùng Partition Magic để phân chia đĩa.

§ Một partition là Linux native ext3. Cần khoảng 2GB trở lên để cài Linux, bao gồm cả KDE và Gnome, các tiện ích đồ họa, multimedia, và lập trình. Tối thiểu bạn cần 400MB và cài toàn bộ là 4,5GB.

§ Một partition là Linux swap, là phân vùng tráo đổi của Linux dành cho việc sử dụng bộ nhớ ảo, làm không gian trao đổi. Thông thường, dung lượng bộ nhớ ảo tối ưu sẽ gấp đôi dung lượng bộ nhớ RAM của hệ thống.

2. Bắt đầu cài đặt:

Cách đơn giản và thông dụng nhất để cài Redhat Linux là cài đặt từ bộ CDROM:

Khởi động hệ thống từ bộ đĩa CD cài đặt ( CD số 1), và nhấn Enter từ dấu nhắc khởi động để mặc định cài đặt theo chế độ đồ hoạ. Chương trình cài đặt sẽ tự động dò thông số của bàn phím, chuột, card màn hình, màn hình và sau đó đi vào quá trình cài đặt. Thông qua từng bước wizard để bạn chọn các thông số về hệ thống như bàn phím, chuột, ngôn ngữ trong quá trình cài đặt, giờ hệ thống.

a. Chọn kiểu cài đặt:

- Personal Desktop: dành cho người mới bắt đầu với Linux hoặc cho những hệ thống desktop cá nhân. Chương trình cài đặt sẽ chọn lựa những gói phần mềm cần thiết nhất cho cấu hình này. Dung lượng đĩa cần cho kiểu cài đặt này chiếm khoảng 1,5GB, bao gồm cả môi trường đồ hoạ.

- WorkStation: dành cho những trạm làm việc với chức năng đồ hoạ cao cấp và các công cụ phát triển.

- Server: cài đặt hệ thống đóng vai trò máy chủ như webserver, ftpsever, SQL server.v.v.

- Custom: đây là lựa chọn linh hoạt cho bạn trong quá trình cài đặt. Bạn có thể chọn các gói phần mềm, các môi trường làm việc, boot loader tuỳ theo ý bạn.

b. Thiết lập phân vùng cài Linux:

Đây là quá trình nhạy cảm nhất và nguy hiểm nhất trong quá trình cài đặt, vì chỉ cần bất cẩn chọn sai thì dữ liệu trên ổ cứng của bạn có thể bị mất sạch.

Chức năng "automatic partition" sẽ giúp bạn tự động tạo các phân vùng cho Linux. Hãy cẩn thận nếu bạn chọn option "remove all partition on this system", vì như thế tất cả các phân vùng trên ổ cứng của bạn đều bị xoá. Option "remove all Linux partition on this system" sẽ chỉ xoá các phân vùng của Linux mà thôi

Ở đây, để thuận tiện thì bạn có thể dùng Partition Magic để phân chia đĩa trước. Tới giai đoạn này chỉ là công việc tạo định dạng cho phân vùng cài đặt mà thôi. Tuy nhiên bạn vẫn có thể thao tác phân chia phân vùng cài đặt dễ dàng với Disk Druid.

Thông thường, bạn nên chọn " Manually partition with Disk Druid " để tạo các phân vùng:

· Một phân vùng chứa mount point là "/", có kiểu file hệ thống là Linux Native ext3.

· Một phân vùng swap cho Linux, kiểu của phân vùng này là Linux swap, kích thước tối ưu là gấp đôi dung lượng RAM của hệ thống hiện tại.

Các button trên màn hình giao diện cho phép bạn thao tác phân chia và định dạng phân

vùng. Nút New, Delete để tạo mới hay xoá một phân vùng. Nút Edit để định dạng phân vùng đó, có kiểu là gì (ext3, swap, fvat…), qui định lại kích thước, là thư mục gì trong hệ thống phân cấp bộ nhớ.

Bạn có thể Reset quá trình thao tác nếu chưa thoả mãn yêu cầu của mình, chưa có một thay đổi nào được thực hiện cho đến khi bạn hoàn thành công việc với Disk Druid.

c. Cách quản lý đĩa trong Linux:

Trong cấu trúc cây thứ bậc của Linux, cao nhất là "/", dưới đó là /boot, /etc, /root, /mnt .v.v.

Đối với Linux, mọi thiết bị phần cứng đều được coi như file hoặc thư mục nằm trong hệ thống phân cấp cây thư mục. Chẳng hạn hệ thống của bạn có hai ổ cứng thì đĩa cứng thứ nhất là /dev/had, ổ cứng thứ hai là /dev/hdb. Trong cùng một ổ dĩa, các hệ thống file được chia thành các phân vùng khác nhau. Một ổ cứng có 4 phân vùng chính (primary) được đánh số thứ tự từ 1 đến 4. tương ứng với ổ cứng đầu tiên sẽ là hda1, hda2 .v.v, phân vùng thuộc phần mở rộng (extended) được đánh số bắt đầu từ số 5: ví dụ hda5, hda6 …

d. Cài đặt boot loader

Đây là chương trình dùng để khởi động Linux cũng như các hệ điều hành khác (dual boot) khi bạn có nhiều hơn một hệ điều hành được cài trên hệ thống. Grub là boot loader mặc định khi cài RedHat 8.0. Đây là chương trình rất mạnh và uyển chuyển. Grub tự động dò các hệ điều hành hiện có trên hệ thống và thêm vào trong danh sách khởi động. Các tuỳ chọn trên màn hình tương đối dễ hiểu.

Với tuỳ chọn " configure advance boot loader option" cho phép bạn chọn việc cài grub lên đâu trong ổ cứng:

Nếu chọn Grub để khởi động hệ thống , grub sẽ được cài lên Master boot record ( /dev/hda).

Nếu chọn một chương trình khác để khởi động như system commander chẳng hạn, bạn hãy chọn cài grub lên "first sector of boot partition". Như vậy, system commander sẽ tự động nhận ra Linux và thêm vào mục nhập khởi động cho Linux.

e. Cấu hình account:

Việc cấu hình acount dùng để thiết lập mật khẩu root và có thể tạo thêm các account khác để log in vào hệ thống khi việc cài đặt hoàn tất.

Tài khoản root là tài khoản có quyền cao nhất trong hệ thống. Bạn có thể cài đặt, cấu hình hệ thống hay làm mọi chuyện một khi đăng nhập vào hệ thống với tài khoản này.

f. Các lưu ý lựa chọn gói phần mềm cài đặt:

Với Redhat 8.0, việc chọn các gói phần mềm để cài đặt được thực hiện rất thuận tiên khi các gói phần mềm được gom lại thành nhóm. Có thể chọn cài các gói phần mềm ngay lúc này các gói cần thiết hoặc có thể cài thêm sau khi hoàn tất cài đặt.

Bạn chọn mục "select individual package" để cài thêm các gói mà mặc định sẽ không cài cho bạn. Ví dụ như mc (Midnight Commander, tương tự NC trong DOS). Sau khi lựa chọn xong, chương trình cài đặt sẽ duyệt các gói phụ thuộc để bạn cài thêm.

Trong suốt quá trình chọn gói phần mềm cài đặt, bạn được thông báo dung lượng cần để cài đặt. Nên chú ý để không vượt quá dung lượng phân vùng mà bạn đã dành cho Linux trong quá trình chọn lựa. Một điều chú ý là bạn nên cài các programming develop và kernerl source, các thư viện lập trình để thuận tiện cho việc sau này cần biên dịch lại nhân hệ điều hành hoặc cài đặt và biên dịch phần mềm và driver cho hệ thống.

g. Cấu hình X

Để làm việc được với giao diện đồ hoạ, bạn cần cấu hình cho X Window. Nếu may mắn, card đồ hoạ và màn hình của bạn sẽ nằm trong danh sách được Linux hỗ trợ. Còn nếu không, cách chắc chắn với loại card đồ họa để chạy được là chọn loại vesa. Về màn hình, Linux sẽ tự dò cho bạn hoặc bạn sẽ cấu hình bằng tay việc chọn tần số quét cho màn hình. Hãy cẩn thận vì quá trình này dễ làm hỏng màn hình và card đồ hoạ của bạn. Đây chính là lý do bạn cần nắm vững thông số của các linh kiện phần cứng.

Nếu không cần Linux tự dò tìm và cấu hình dùm bạn, bạn có thể mở file /etc/X11/XF86Config (hoặc XF86Config-4) để cấu hình bằng tay.

Sau khi nhấn nút test để kiểm tra hệ thống có chạy tốt với chế độ đồ họa chưa, nếu mọi việc suôn sẻ, chúc mừng bạn đã hoàn tất quá trình cài đặt Linux.

Lưu ý về card đồ họa

Mặc dù Linux nhận dạng và hỗ trợ đúng nhiều loại card đồ hoạ được sản xuất trong 2 năm gần đây, sau khi cấu hình, card đồ hoạ vẫn chạy với bus PCI cho dù card đồ họa của bạn là loại AGP, và bạn vẫn chưa tận dụng được các chứng năng đồ hoạ 3D cao cấp của nó. Lý do là các nhà sản xuất linh kiện vì lý do bảo mật và bản quyền nên chưa hỗ trợ cho các nhà phát triển Linux. Tuy nhiên, hiện nay nhiều nhà sản xuất phần cứng đã bắt đầu hỗ trợ driver cho các linh kiện của mình trên các hệ thống Linux. Chẳng hạn với nhà sản xuất Nvidia, bạn có thể tải driver của nó thông qua www.nvidia.com hoặc ftp://download.nvidia.com/XFree86_40/1.0-3123. Các game 3D chạy với hình ảnh rất mịn màng không thua kém gì trên MS Window sau khi bạn đã cài driver cho hệ thống.

# Cách cài đặt font và in ấn tiếng Việt trên Linux

Có 2 cách cài đặt Unicode fonts cho X Window.
1. Sử dụng ttmkfdir (cách cũ)
2. Sử dụng fontconfig (cách mới cho Mandrake-9.0, RedHat-8.0)

1. Sử dụng ttmkfdir (cách cũ):

a. Tạo /usr/share/fonts, nếu chưa có, bằng lệnh:
mkdir /usr/share/fonts

b. Mở utf8.tar.gz trong thư mục /usr/share/fonts bằng lệnh:
cd /usr/share/fonts && tar xvzf utf8.tar.gz

c. Tạo danh sách chứa fonts bằng lệnh:
cd utf8 && ttmkfdir > fonts.scale && mkfontdir

d. Báo cho fonts server biết địa điểm của Unicode fonts bằng lệnh:
chkfontpath --add /usr/share/fonts/utf8

e. Khởi động lại X font server bằng lệnh:
/etc/rc.d/init.d/xfs restart

2. Sử dụng fontconfig (cách mới cho Mandrake-9.0, RedHat-8.0):

a. Bỏ utf8.tar.gz vô /usr/share/fonts và mở nó ra bằng lệnh:
cp utf8.tar.gz /usr/share/fonts && cd /usr/share/fonts && tar xvzf utf8.tar.gz

b. Cập nhật danh sánch fonts bằng lệnh:
fc-cache

Chỉ vậy thôi không cần khởi động lại xfs hay X.

Bạn cũng có thể bỏ arial font (tải về địa chỉ ở dưới) vô trong ~/.fonts và không phải restart cái chi hết nếu bạn xài fontconfig (Red Hat 8 hoặc 9 hoặc Mandrake-9.1).

Ví dụ:

cd ~

mkdir ~/.fonts (nếu chưa có)

tar xvjf arial.tar.bz2

cp arialuni.ttf ~/.fonts

Xem trang web tiếng Việt và cách in tiếng Việt:

Thông thường nếu bạn xem trang web bằng Mozilla thì không cần phải set font gì cả. Nếu bạn xài Konqueror trên Red Hat 8.0 thì bạn phải set fonts trong Konqueror như hình ở đây thì mới xem và in được tiếng Việt.

Nếu bạn xài bản Mandrake mới nhất (9.1) thì bạn sẽ không cần làm gì hết. Việc hiển thị và in ấn tiếng Việt được hỗ trợ rất tốt.

Thêm chi tiết:

.Unicode fonts: có thể tải về từ http://www.vnlinux.org/fonts/utf8.tar.gz hoặc http://www.vnlinux.org/arial.tar.bz2 nếu bạn vẫn chưa hiển thị được tiêng Việt 100%
.fontconfig homepage tại http://www.fontconfig.org.
.ttmkfdir có thể tải về từ http://www.joerg-pommnitz.de/TrueType/xfsft.html
.mkfontdir nằm trong gói XFree86-3x (hoặc XFree86-4x)
. Viet Unicode có nhiều fonts http://sourceforge.net/project/showfiles.p...lease_id=132517

# Thủ thuật bảo mật cho Linux

**Trong bài viết này, chúng tôi xin giới thiệu một số kinh nghiệm nhằm nâng cao tính an toàn cho một hệ thống Linux (để dễ theo dõi cho bạn đọc, chúng tôi sẽ minh hoạ bằng RedHat, một phiên bản Linux rất phổ biến ở Việt Nam và trên thế giới).**

**Hiện nay, trên môi trường máy chủ, Linux ngày càng chiếm một vị trí quan trọng. Nguyên nhân khiến Linux dần trở thành một đối thủ tiềm năng của hệ điều hành Microsoft Windows là do tính ổn định, độ linh hoạt và khả năng chịu tải lớn: đây là những đặc điểm quan trọng hàng đầu của một hệ thống máy phục vụ.**

**Tính bảo mật tốt cũng là một trong những điểm nổi bật của Linux. Tuy nhiên, để một hệ thống Linux có khả năng chống lại các cuộc tấn công, người quản trị cũng cần phải nắm được một số kỹ năng nhất định. Trong bài viết này, chúng tôi xin giới thiệu một số kinh nghiệm nhằm nâng cao tính an toàn cho một hệ thống Linux (để dễ theo dõi cho bạn đọc, chúng tôi sẽ minh hoạ bằng RedHat, một phiên bản Linux rất phổ biến ở Việt Nam và trên thế giới).**

**1.1. Loại bỏ tất cả các account và nhóm đặc biệt**

**Ngay sau khi cài đặt Linux, người quản trị nên xoá bỏ tất cả các account và nhóm (group) đã được tạo sẵn trong hệ thống nhưng không có nhu cầu sử dụng, ví dụ như lp, sync, shutdown, halt, news, uucp, operator, games, gopher, v.v... (Tuy nhiên bạn đọc cần biết rõ những account và nhóm nào không cần cho hệ thống của mình rồi hãy xoá)**

**Thực hiện việc xoá bỏ account với lệnh :**

**# userdel**

**Ví dụ, nếu không có nhu cầu về in ấn trên hệ thống, có thể xoá account lp như sau:**

**# userdel lp**

**Tương tự như vậy, có thể thực hiện việc xoá bỏ các nhóm không cần thiết với lệnh**

**# groupdel**

**2.2. Che giấu file chứa mật khẩu**

**Từ lịch sử xa xưa của Unix và cả Linux, mật khẩu của toàn bộ các account đã từng được lưu ngay trong file /etc/password, file có quyền đọc bởi tất cả các account trong hệ thống! Đây là một kẽ hở lớn cho các kẻ phá hoại: Mặc dù các mật khẩu đều được mã hoá, nhưng việc giải mã ngược là có thể thực hiện được (và có thể thực hiện khá dễ dàng, đặc biệt vì cơ chế mã hoã mật khẩu không phải là khó phá và ngày nay khả năng tính toán và xử lý của máy tính rất mạnh). Vì lí do trên, gần đây các nhà phát triển Unix và Linux đã phải đặt riêng mật khẩu mã hoá vào một file mà chỉ có account root mới đọc được: file /etc/shadow. (Khi sử dụng phương pháp này, để đảm bảo tính tương thích, nơi vốn đặt mật khẩu trong file /etc/password người ta đánh dấu "x")**

**Nếu bạn đọc đang sử dụng các phiên bản RedHat gần đây (ví dụ RedHat 6.x hay 7.x) thì nhớ chọn lựa Enable the shadow password khi cài đặt RedHat để sử dụng tính năng che giấu mật khẩu này (Cũng thật may vì chọn lựa này là mặc định trong hầu hết các phiên bản Linux đang sử dụng rộng rãi hiện nay)**

**3.3. Tự động thoát khỏi shell**

**Người quản trị hệ thống rất hay quên thoát ra khỏi dấu nhắc shell khi kết thúc công việc. Bản thân tôi cũng đã từng nhiều lần khi đang thực hiện việc quản trị với account root thì bỏ đi vì một số công việc khác. Thật nguy hiểm nếu lúc đó có một kẻ phá hoại ở đó: Kẻ này có thể dễ dàng có quyền truy xuất hệ thống ở mức cao nhất mà chẳng cần tốn một chút công sức nào cả.**

**Để giảm nguy cơ này, người quản trị nên cài đặt tính năng tự động thoát ra khỏi shell khi không có sự truy xuất nào trong một khoảng thời gian định trước bằng cách đặt một tham số quy định khoảng thời gian hệ thống vẫn duy trì dấu nhắc shell.**

**Muốn cài đặt tham số này, người sử dụng biến môi trường TMOUT và gán cho nó một giá trị số thể hiện khoảng thời gian tính bằng giây hệ thống vẫn duy trì dấu nhắc. Để thực hiện điều này cho tất cả các account trong hệ thống, cách đơn giản nhất là đặt nó vào file /etc/profile dòng lệnh sau: (giả sử ta đặt khoảng thời gian là 600 giây)**

**TMOUT=600**

**Như vậy là nếu trong khoảng 10 phút người sử dụng không truy xuất shell, shell sẽ tự động thoát ra. Tuy nhiên cần chú ý: Mẹo này sẽ không "ăn" nếu lúc đó người dùng đang chạy một chương trình nào đó như vi hay mc,... Có nghĩa là người dùng phải đang làm việc trực tiếp với shell chứ không phải với bất kỳ một chương trình nào khác.**

**4.4. Loại bỏ các dịch vụ không sử dụng**

**Một điều khá nguy hiểm là sau khi cài đặt, hệ thống tự động bật chạy khá nhiều dịch vụ (và đa số là các dịch vụ không mong muốn), dẫn tới tốn tài nguyên và gây nên nhiều nguy cơ về bảo mật. Người quản trị nên loại bỏ ngay lập tức các dịch vụ không dùng tới ngay sau khi cài máy. Hoặc đơn giản bằng cách xoá bỏ các gói phần mềm/dịch vụ không sử dụng (qua công cụ quản trị gói phần mềm rpm của RedHat) hoặc sử dụng công cụ ntsysv để duyệt xem tất cả các dịch vụ đang cài đặt rồi vô hiệu hoá những dịch vụ không cần thiết (bằng cách bỏ đánh dấu các dịch vụ không sử dụng với phím Space). Sau khi thoát ra khỏi ntsysv thì khởi động lại máy: các dịch vụ không mong muốn sẽ không chạy nữa.**

**5.5. Không tiết lộ thông tin về hệ thống qua telnet**

**Dịch vụ cho phép truy xuất hệ thống từ xa telnet có khả năng tiết lộ thông tin về hệ thống, dễ tạo điều kiện cho những kẻ phá hoại tấn công dựa vào những điểm yếu đã biết. Điều này rất dễ nhận thấy: Mọi người dùng kết nối từ xa vào dịch vụ telnet đều nhận được thông tin về tên máy, phiên bản Linux và phiên bản của nhân (kernel) của máy chủ.**

**Để tránh điều này, ta cần thực hiện việc kích hoạt telnetd (telnet server) với tham số -h. (Tham số -h sẽ ngăn telnet tiết lộ các thông tin và chỉ in ra dấu nhắc "Login:" cho những người kết nối từ xa).**

**Do các phiên bản RedHat 7.x khi chạy telnetd không còn sử dụng inetd nữa (mà sử dụng xinetd - một phiên bản nâng cấp và có nhiều cải tiến so với inetd) nên cách cấu hình lại telnetd sẽ khác nhau tuỳ theo phiên bản RedHat đang sử dụng.**

**+ Với các phiên bản RedHat 6.x và trước đó, thực hiện các bước sau:**

**Trong file /etc/inetd.conf, thay đổi dòng**

**telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd**

**chuyển thành :**

**telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd -h**

**Tiếp theo, khởi động lại inetd bằng câu lệnh:**

**# /etc/rc.d/init.d/inetd restart**

**+ Với các phiên bản RedHat 7.x, thực hiện bước sau:**

**Trong file /etc/xinetd.d/telnet , thêm chọn lựa:**

**server_args = -h**

**File trên sẽ có dạng như sau;**

```
service telnet
{
disable = yes
flags = REUSE
socket_type = stream
wait = no
user = root
server = /usr/sbin/in.telnetd
log_on_failure += USERID
server_args = -h
}
```

**Tiếp theo, khởi động lại xinetd bằng câu lệnh:**

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

**6.6. Tránh sử dụng các dịch vụ không mã hoá thông tin trên đường truyền**

**Mặc dù ở trên chúng tôi đã trình bày cách ngăn dịch vụ telnet tiết lộ thông tin, nhưng chúng tôi xin có lời khuyên: Tuyệt đối tránh sử dụng những dịch vụ kiểu như telnet, ftp (ngoại trừ ftp anonymous) vì những dịch vụ này hoàn toàn không hề mã hoá mật khẩu khi truyền qua mạng. Bất kỳ một kẻ phá hoại nào cũng có**

**thể dễ dàng "tóm" được mật khẩu của bạn bằng những công cụ nghe lén kiểu như sniffer.**

**Ơ' những trường hợp có thể, nên sử dụng dịch vụ ssh thay thế cho cả ftp và telnet: dịch vụ SSH (Secure Shell) dùng cơ chế mã hoá công khai để bảo mật thông tin, thực hiện mã hoá cả mật khẩu lẫn thông tin chuyển trên đường truyền. Hiện đang được sử dụng khá rộng rãi, gói phần mềm của SSH cũng được đóng kèm trong hầu hết các phiên bản gần đây của Linux. Chẳng hạn, các phiên bản RedHat từ 7.0 trở lên mặc định đều cài OpenSSH, một sản phẩm mã nguồn mở có thể sử dụng hoàn toàn miễn phí. (Bạn đọc có thể tham khảo website www.openssh.org về sản phẩm này).**

**Ngoài ra, những dịch vụ "r" kiểu như rsh, rcp hay rlogin chúng tôi cũng khuyên nên tuyệt đối tránh sử dụng. Lý do là các dịch vụ này ngoài việc truyền mật khẩu không mã hoá còn thực hiện việc kiểm tra quyền truy xuất dựa trên địa chỉ máy kết nối, là một điều cực kỳ nguy hiểm. Các kẻ phá hoại sử dụng kỹ thuật spoofing đều có thể dễ dàng đánh lừa được cách kiểm tra này khi "làm giả" được địa chỉ của máy truy xuất dịch vụ hợp lệ.**

**7. 7. Cấm sử dụng account root từ consoles**

**Có thể bạn đọc đều nhận thấy, ngay sau khi cài đặt RedHat, account root sẽ không có quyền kết nối telnet vào dịch vụ telnet trên hệ thống (chỉ những account thường mới có thể kết nối). Nguyên nhân là do file /etc/securetty quy định những console được phép truy nhập bởi root chỉ liệt kê những console "vật lý" (tức là chỉ truy xuất được khi ngồi trực tiếp tại máy chủ) mà bỏ qua những kết nối qua mạng. Dịch vụ ftp cũng sẽ bị hạn chế này: account root không được phép truy xuất ftp qua mạng.**

**Để tăng tính bảo mật hơn nữa, soạn thảo file /etc/securetty và bỏ đi những console bạn không muốn root truy nhập từ đó.**

**8.8. Cấm "su" lên root**

**Trong Linux, lệnh su (Substitute User) cho phép người dùng chuyển sang một account khác. Nếu không muốn một người bất kỳ "su" thành root, thêm hai dòng sau vào nội dung file /etc/pam.d/su**

```
auth sufficient /lib/security/pam_rootok.so debug
auth required /lib/security/Pam_wheel.so group=wheel
```

**Như vậy, chỉ có những người có đăng ký là thành viên của nhóm wheel mới có quyền "su" thành root. Để cho phép một người dùng có quyền này, người quản trị chỉ việc gán account của người này vào nhóm wheel (qua file /etc/group)**

**9.9. Hạn chế các thông tin ghi bởi bash shell**

**Thông thường, tất cả các lệnh được thực hiện tại dấu nhắc shell của các account đều được ghi vào file ".bash_history" nằm trong thư mục cá nhân của các account. Điều này cũng gây nên những nguy hiểm tiềm ẩn, đặc biệt với những ứng dụng đòi hỏi phải gõ các thông mật như mật khẩu trên dòng lệnh. Người quản trị nên hạn chế nguy cơ này dựa trên 2 biến môi trường HISTFILESIZE và HISTSIZE: Biến môi trường HISTFILESIZE xác định số lệnh (gõ tại dấu nhắc shell) sẽ được lưu lại cho lần truy nhập sau, còn biến môi trường HISTSIZE xác định số lệnh sẽ được ghi nhớ trong phiên làm việc hiện thời. Ta có thể giảm giá trị của HISTSIZE và đặt bằng 0 giá trị HISTFILESIZE để giảm tối đa những nguy hiểm đã nêu trên.**

**Để thực hiện việc này, chỉ cần đơn giản thay đổi giá trị hai biến này trong file /etc/profile như sau:**

```
HISTFILESIZE=0
HISTSIZE=20
```

**Như vậy, tại phiên làm việc hiện thời, shell chỉ ghi nhớ 20 lệnh gần nhất, đồng thời không ghi lại các lệnh người dùng đã gõ khi người dùng thoát ra khỏi shell.**

**10.10. Cấm nhòm ngó tới những file script khởi động Linux**

**Khi khởi động Linux, các file script được đặt tại thư mục /etc/rc.d/init.d sẽ được thực hiện. Để tránh những sự tò mò không cần thiết, người quản trị nên hạn chế quyền truy xuất tới những file này chỉ cho account root bằng lệnh sau:**

```
# chmod -R 700 /etc/rc.d/init.d/*
```

**11.11. Xoá bỏ những chương trình SUID/SGID không sử dụng**

**Thông thường, những ứng dụng được thực hiện dưới quyền của account gọi thực hiện ứng dụng. Tuy nhiên, Unix và Linux sử dụng một kỹ thuật đặc biệt cho phép một số chương trình thực hiện dưới quyền của người quản lý chương trình (chứ**

**không phải người thực hiện). Đây chính là lý do tại sao tất cả mọi user trong hệ thống đều có thể đổi mật khẩu của mình trong khi không hề có quyền truy xuất lên file /etc/shadow: Nguyên nhân vì lệnh passwd có gán thuộc tính SUID và được quản lý bởi root, mà chỉ có root mới có quyền truy xuất /etc/shadow.**

**Tuy nhiên, khả năng này có thể gây nên những nguy cơ tiềm tàng: Nếu một chương trình có tính năng thực thi được quản lý bởi root, do thiết kế tồi hoặc do được cài đặt cố tình bởi những kẻ phá hoại mà lại có thuộc tính SUID thì mọi điều tồi tệ đều có thể xảy ra. Thực tế cho thấy, khá nhiều kỹ thuật xâm nhập hệ thống mà không có quyền root được thực hiện nhờ kỹ thuật này: kẻ phá hoại bằng cách nào đó tạo được một shell (ví dụ bash) được quản lý bởi root, có thuộc tính SUID. Sau đó mọi truy xuất phá hoạt sẽ được thực hiện qua shell này vì mọi lệnh thực hiện trong shell sẽ được thực hiện dưới quyền của root.**

**Thuộc tính SGID cũng tương tự như thuộc tính SUID: các chương trình được thực hiện với quyền nhóm là nhóm quản lý chương trình chứ không phải nhóm của người chạy chương trình.**

**Như vậy, người quản trị sẽ phải thường xuyên kiểm tra xem trong hệ thống có những ứng dụng nào có thuộc tính SUID hoặc SGID mà không được phép không?**

**Để tìm tất cả các file có thuộc tính SUID/SGID, sử dụng lệnh find như sau:**

**# find / -type f \( -perm -04000 -o -perm -02000 \) \-exec ls ưlg {} \;**

**Nếu phát hiện được một file có thuộc tính SUID/SGID một cách không cần thiết, có thể loại bỏ các thuộc tính này bằng lệnh:**

**# chmod a-s**

**12.12. Tăng tính bảo mật cho nhân (kernel) của Linux**

**Thực tế cho thấy, Linux không hẳn được thiết kế với các tính năng bảo mật thật chặt chẽ: khá nhiều lỗ hổng có thể bị lợi dụng bởi những tin tặc thông thạo về hệ thống. Do đó, việc sử dụng một hệ điều hành với nhân được củng cố là rất quan trọng: Một khi nhân - phần cốt lõi nhất của hệ điều hành - được thiết kế tốt thì nguy cơ bị phá hoại sẽ giảm đi rất nhiều.**

**Bạn đọc có thể xem xét việc củng cố nhân Linux thông qua các miếng vá (patch). Tôi xin giới thiệu một trong những website tốt nhất chuyên cung cấp các miếng**

**vá bổ sung cho nhân Linux về bảo mật tại địa chỉ www.grsecurity.net. Tại đây bạn đọc có thể tìm hiểu thông tin hữu ích và tải xuống các miếng vá bổ sung cho hệ thống Linux của mình.**

# Bảo mật hệ thống *nix với PAM

1. Đặt vấn đề

Chắc hẳn bạn đã từng tự hỏi tại sao các chương trình ftp, su, login, passwd, sshd, rlogin … lại có thể hiểu và làm việc với shadow password; hay tại sao các chương trình su, rlogin lại đòi hòi password; tại sao một số hệ thống chỉ cho một nhóm nào đó có quyền su, hay sudo, hay hệ thống chỉ cho phép một số người dùng, nhóm người dùng đến từ các host xác định và các thiết lập giới hạn cho những người dùng đó, …Tất cả đều có thể lý giải với PAM. Ứng dụng của PAM còn nhiều hơn những gì tôi vừa nêu nhiều, và nó bao gồm các module để tiện cho người quản trị lựa chọn.

2. Cấu trúc PAM

- Các ứng dụng PAM được thiết lập trong thư mục /etc/pam.d hay trong file /etc/pam.conf ( login, passwd, sshd, vsftp, …)
- Thư viện các module được lưu trong /lib/security ( pam_chroot.so, pam_access.so, pam_rootok.so, pam_deny.so, … )
- Các file cấu hình được lưu trong /etc/security ( access.conf, chroot.conf, group.conf ,… )
+access.conf – Điều khiển quyền truy cập, được sử dụng cho thư viện pam_access.so.
+group.conf – Điều khiển nhóm người dùng, sử dụng bởi pam_group.so
+limits.conf – thiết lập các giới hạn tài nguyên hệ thống, được sử dụng bởi pam_limits.so.
+pam_env – Điều khiển khả năng thay đổi các biến môi trường, sử dụng cho thư viện pam_env.so .
+time – Thiết lập hạn chế thời gian cho dịch vụ và quyền người dùng, sử dụng cho thư viện pam_time.so.

3. Cách hoạt động của PAM

Thuật ngữ
- Các chương trình login, pass, su, sudo, … trên được gọi là privilege-granting application ( chương trình trao đặc quyền ).

- PAM-aware application: là chương trình giúp các privile-granting application làm việc với thư viện PAM.

Các bước hoạt động:

1. Người dùng chạy một ứng dụng để truy cập vào dịch vụ mong muốn, vd login.

2. PAM-aware application gọi thư viện PAM để thực hiện nhiệm vụ xác thực.
3. PAM library sẽ dựa vào file cấu hình của chương trình đó trong /etc/pam.d ( vd ở đây là login -> file cấu hình /etc/pam.d/login ) xác định loại xác thực nào được yêu cầu cho chương trình trên. Trong trường hợp không có file cấu hình, thì file /etc/pam.d/other sẽ được sử dụng.
4. PAM library sẽ load các module yêu cầu cho xác thực trên.
5. Các modules này sẽ tạo một liên kết tới các hàm chuyển đổi ( conversation functions ) trên chương trình.
6. Các hàm này dựa vào các modules mà đưa ra các yêu cầu với người dùng, vd chúng yêu cầu người dùng nhập password.
7. Người dùng nhập thông tin vào theo yêu cầu.
8. Sau khi quá trình xác thực kết thúc, chương trình này sẽ dựa vào kết quả mà đáp ứng yêu cầu người dùng ( vd cho phép login vào hệ thống ) hay thông báo thất bại với người dùng.

4. Bây giờ chúng ta sẽ nghiên cứu file config

Listing 10-1: The /etc/pam.d/rlogin file

```
#%PAM-1.0
auth required /lib/security/pam_securetty.so
auth sufficient /lib/security/pam_rhosts_auth.so
auth required /lib/security/pam_stack.so service=system-auth
auth required /lib/security/pam_nologin.so
account required /lib/security/pam_stack.so service=system-auth
password required /lib/security/pam_stack.so service=system-auth
session required /lib/security/pam_stack.so service=system-auth
```

Các dòng trong file config có dạng sau:

module-type control-flag module-path module-args

----MODULE TYPE
auth: thực hiện xác thực. Thông thường, một auth module sẽ yêu cầu password để kiểm tra, hay thiết lập các định danh như nhóm người dùng, hay thẻ kerberos.

Account điều khiển sự kiểm tra "bề mặt" với yêu cầu xác thực. Ví dụ, nó có thể kiểm tra người dùng truy cập dịch vụ từ một host và trong thời gian cho phép hay không.

Password: thiết lập password. Thông thường, nó luôn có sự tương ứng giữa một module auth và một module password..

Session: điều khiển các nhiệm vụ quản lý session. Được sử dụng để đảm bảo rằng người dùng sử dụng tài khoản của họ khi đã được xác thực..

----PAM MODULE CONTROL FLAGS

Require: cờ điều khiển này nói với PAM library yêu cầu sự thành công của modules tương ứng, vd "auth required /lib/security/pam_securetty.so" à module pam_securetty.so phải thành công. Nếu module đó không được thực hiện thành công thì quá trình xác thực thất bại. Nhưng lúc đó, PAM vẫn tiếp tục với các module khác, tuy nhiên nó chỉ có tác dụng nhằm tránh khỏi việc người dùng có thể đoán được quá trình này đã bị thất bại ở giai đoạn nào.

Sufficient: cờ này khác với cờ trên ở chỗ, khi có một module thực hiện thành công nó sẽ thông báo hoàn thành ngay quá trình xác thực, mà không duyệt các module khác nữa.

Requisite: cờ này có ý nói PAM library loại bỏ ngay quá trình xác thực khi gặp bất kỳ thông báo thất bại của module nào.

Optional: cờ này ít khi được sử dụng, nó có ý nghĩa là module này được thực hiện thành công hay thất bại cũng không quan trọng, không ảnh hưởng quá trình xác thực.

----MODULE-PATH – Đường dẫn đên thư viện PAM.
----ARGUMENTS – Các biến tùy chọn cho các module.

Các module ( auth, account, password, session ) được thực hiện trong stack và chúng được thực hiện theo thứ tự xuất hiện trong file config.

Các chương trình yêu cầu xác thực đều có thể sử dụng PAM.

5.Sau đây tôi xin giới thiệu chức năng của một số module

_ pam_access.so:

- Support module type :account
- Module này sử dụng file thiết lập trong etc/security/access.conf .

File cấu hình này có dạng như sau:
< + or - > : : + : grant permission
- : deny permission
Với username list là người dùng hay nhóm người dùng, tty list là login qua console, host list xác định các host hay domain. Chúng ta có thể sử dụng các từ khóa ALL=tất cả, EXCEPT=trừ, LOCAL=cục bộ.
Ví dụ sau cho cấm osg login từ tất cả, và cho phép linet login từ xa.
account required pam_access.so
-:osg:ALL
+:linet:ALL EXCEPT LOCAL

pam_chroot.so:
Support module type :account; session; authentication

Dùng để chroot cho các user thiết lập trong /etc/security/chroot.conf
Ví dụ, tôi thực hiện chroot cho sshd để người dùng linet chỉ có quyền truy cập trong /home/osg mà không có quyền truy cập đến các thư mục home của người dùng khác
Thêm dòng sau trong /etc/pam.d/sshd ( lưu ý trong /etc/sshd/sshd_config phải thiết lập UsePAM = yes )
session required pam_chroot.so

_ pam_deny.so:

Support module type: account; authentication; password; session
Module này luôn trả về giá trị false. Vd nó được dùng trong /etc/pam.d/other để từ chối mọi truy cập của người dùng khi truy cập vào các PAM-aware program mà không có file cấu hình PAM

- Acount module type: Từ chối người dùng quyền truy cập vào hệ thống

#add this line to your other login entries to disable all accounts
login account required pam_deny.so

- Authentication module type: từ chối truy cập, thiết lập giá trị mặc định. vd trong /etc/pam.d/other. Khi người dùng login vào hệ thống, đầu tiên sẽ gọi các module trong /etc/pam.d/login ra và yêu cầu người dùng nhập thông tin tương ứng ( username, password ), nếu các thông tin này không đáp ứng thì PAM sẽ gọi /etc/pam.d/other ra để deny quyền truy cập.

#/etc/pam.d/other

auth required /lib/security/$ISA/pam_deny.so
account required /lib/security/$ISA/pam_deny.so
password required /lib/security/$ISA/pam_deny.so
session required /lib/security/$ISA/pam_deny.so

- Password module type: Không cho phép change password

ví dụ không cho phép người dùng đổi passwd
Thêm dòng sau vào /etc/pam.d/passwd
password required pam_deny.so

_ pam_limits.so
- Support module type: session
Thiết lập các giới hạn tài nguyên trong /etc/security/limit

username|@groupname type resource limit.

A resource can be one of these keywords:
· core - Limits the size of a core file (KB).
· data - Maximum data size (KB).
· fsize - Maximum file size (KB).
· memlock - Maximum locked-in memory address space (KB).
· nofile - Maximum number of open files.
· rss - Maximum resident set size (KB).
· stack - Maximum stack size (KB).
· cpu - Maximum CPU time in minutes.
· nproc - Maximum number of processes.
· as - Address space limit.
· maxlogins - Maximum number of logins allowed for this user.

Thông tin chi tiết ở trong /etc/security/limits.conf

Vd dưới đây, tất cả user giới hạn 10 MB mỗi session và cho phép max là 4 logins đồng thời. ftp được cho phép 10 login đồng thời ( hứu ích cho anonymous ftp ); thành viên của nhóm manager giới hạn 40 process, nhóm developers giới hạn 64MB bộ nhớ, và các user thuộc wwwusers không thể tạo files lớn hơn 50 MB = 500000 KB.

Listing 3. Setting quotas and limits

* hard rss 10000
* hard maxlogins 4
* hard core 0
bin -
ftp hard maxlogins 10
@managers hard nproc 40
@developers hard memlock 64000
@wwwusers hard fsize 50000

Để active các limits này, bạn cần thêm dòng sau vào cuối /etc/pam.d/login:

session required /lib/security/pam_limits.so.

_ pam_listfile.so

Module này đọc thông tin trong file và thực hiện hành động được thiết lập ( như cho phép hay không cho phép truy cập ) dựa vào sự tồn tại hay không của các nhân tố như username, host, groups, …

Ví dụ trong vsftpd
auth required /lib/security/pam_listfile.so item=user \
sense=deny file=/etc/ftpusers onerr=succeed

Yêu cầu PAM load pam_listfile module và đọc trong /etc/ftpusers, nếu /etc/ftpusers chứa các dòng username, thì PAM sẽ sử dụng sense=deny để quyết định ngăn cản các user này truy cập vào. Vậy các user trong /etc/ftpusers sẽ ko có quyền truy cập vào ftp.

_ pam_rootok.so

Sử dụng module này để yêu cầu root không cần nhập password khi thực hiện chương trình, vd nó được gán vào su để chi rằng root không cần gõ passwd khi đánh lệnh su

_pam_wheel.so
Chỉ cho phép quyền truy cập root với group wheel. Ví dụ chỉ cho phép những người thuộc nhóm wheel có quyền su lên root.

#
# root gains access by default (rootok), only wheel members can
# become root (wheel) but Unix authenticate non-root applicants.

```
#
auth sufficient pam_rootok.so
auth required pam_wheel.so
auth required pam_unix_auth.so
```

----------> Tham khảo

Document: http://www.kernel.org/pub/linux/libs/pam/pre/doc/

Mã nguồn module:

http://cvs.sourceforge.net/viewcvs.py/pam/Linux-PAM/modules/

# Cách biên dịch nhân (kernel)

**1. Lấy kernel về:**

**Kernel source có thể tải về từ http://www.kernel.org . Bản stable hiện tại là 2.4.21 và developer là 2.5.73. Nếu bạn không muốn test những chức năng mới của kernel thì nên sử dụng 2.4.21 cho công việc hàng ngày.**

**2. Bung nén và chuẩn bị kernel: giả sử bạn vừa tải về linux-2.4.21.tar.bz2, sau khi chạy các dòng lệnh dưới bạn sẽ sắn sàng cho việc compile kernel**

**2a. $mv linux-2.4.21.tar.bz2 /usr/src/**

**2b. $cd /usr/src && tar -xvjf linux-2.4.21.tar.bz2**

**2c. $ln -s linux-2.4.21 linux**

**Đến đây bạn đã sẵn sàng cho việc compile nhưng đôi lúc có lẽ bạn sẽ cần apply một patch nào đó thì có thể chạy lệnh sau trong thư mục /usr/src/linux**

**$patch -p1 --dry-run < /địa điểm/và tên/của patch**

**Lưu ý: --dry-run sẽ 'giả đò' apply cái patch nhưng thực sự chưa làm gì hết. Bạn nên xài --dry-run trước khi apply để phòng hờ cái patch không phải cho kernel bạn đang xài hoặc patch còn bị lỗi. Sau khi chạy --dry-run và không thấy báo lỗi gì thì bạn có thể thật sự apply patch bằng lệnh $patch -p1 < /địa điểm/và tên/của patch**

**3. Compile kernel: sẽ được thực hiện với các lệnh sau đây:**

**3a. $make menuconfig (hoặc make config, hoặc make xconfig) sẽ hỏi bạn một loạt câu hỏi cho kernel phù hợp với máy của bạn. Nếu bạn biết chắc mình sẽ xài một chức năng nào đó thì nên trả lời Y còn không thì trả lời N, trả lời M (module) nếu bạn lưỡng lự không biết cái phần cứng của mình sẽ xài driver này hay driver khác, nhất là phần cho network card hay sound card. Nếu bạn không rõ câu hỏi này hỏi cái gì thì gõ h sẽ có phần giải thích khá rõ ràng.**

**Bạn có thể tải về một bản config mẫu mà mình xài cho máy Pentium3, Tekram SCSI card, SB Live! sound card, bt848 Haupauge TV card, ext2/ext3/reiserfs/jfs/tmpfs/iso9660/vfat/ntfs và ipsec VPN compiled vô kernel, tulip, intel, realtek modules cho network cards, iptables và wireless modules. Nếu bạn không cần cái nào thì chỉ việc comment out (bỏ cái dấu # ở phía trước) cái hàng đó. Chẳng hạn máy bạn là Petium4 thì nên thay đổi với giá trị tương ứng. Sau đó chạy lệnh $make oldconfig thay vì $make menuconfig như ở trên.**

**3b. $make dep sẽ chuẩn bị các dependencies cần thiết**

**3c. $make clean sẽ dọn dẹp .o files mà developers để quên và tạo các source tree.**

**3d. $make bzImage sẽ bắt đầu thật sự compile kernel. Nếu mọi chuyện suôn sẽ bạn sẽ có bzImage nằm trong thư mục /usr/src/linux/arch/i386/boot**

**3e. $make modules sẽ compile các modules bạn chọn trong lúc chạy $make menuconfig ở trên.**

**3f. $make modules_install sẽ cài các modules vào thư mục /lib/modules/2.4.21**

**3g. $cp /usr/src/linux/arch/i386/boot/bzImage /boot/mykernel-2.4.21 sẽ cp kernel image bạn mới compile vô thư mục /boot.**

**Nếu bạn có SCSI card và compile SCSI card hoặc filesystem (ext3, reiserfs,..v..) mà máy sử dụng dưới dạng module thì bạn phải tạo initial ramdisk với lệnh $mkinitrd -o /boot/initrd-2.4.21.img /lib/modules/2.4.21. Còn nếu bạn đã compile SCSI card và filesytem vô luôn kernel thì bái bai initrd.**

**:**

**4. Chuẩn bị boot loader**

**4a. Nếu bạn dùng GRUB: tạo hẳn một section mới cho kernel của bạn bằng cách sửa menu.lst với lệnh $vi /boot/grub/menu.lst giả sử / của bạn nằm trên /dev/hda3 và /boot nằm trên /dev/hda1, thêm vào những hàng sau:**

**title MyKernel-2.4.21**

**kernel (hd0,0)/boot/mykernel-2.4.21 root=/dev/hda3**

**initrd (hd0,0)/boot/initrd-2.4.21.img**

**Nếu bạn không xài initrd thì không cần hàng cuối ở trên.**

**4b. Nếu bạn dùng LILO: tạo hẳn một section cho kernel của bạn bằng cách sửa file lilo.conf với lệnh $vi /etc/lilo.conf thêm vào những hàng sau:**

**image=/boot/mykernel-2.4.21**

**label=MyKernel-2.4.21**

**root=/dev/hda3**

**initrd=/boot/initrd-2.4.21.img**

**read-only**

**Nhớ chạy lệnh $lilo nếu không bạn sẽ không thấy kernel mới của mình khi reboot.**

**Bạn nên giữ lại /usr/src/linux/.config để mai này nếu bạn muốn compile 2.4.22 chẳng hạn thì có thể xài lại nó bằng cách chạy $make oldconfig thay vì $make menuconfig. Lưu ý: $make mrproper sẽ xóa đi /usr/src/linux/.config file và dọn dẹp sạch sẽ các .o files và symlinks (ln -s command). Bạn sẽ không thể dùng config file của kernel 2.4 cho kernel 2.5 được.**

**Hy vọng bài viết này sẽ giúp bạn hiểu rõ hơn quá trình cập nhật kernel từ source. Như thường lệ, cám ơn các bác trên #unixcircle đã cho feedback. Mọi góp ý xin gửi về em_mê_compile_kernel@vnlinux.org**

# Làm reverse proxy với Linux + Apache, Bảo vệ máy chủ

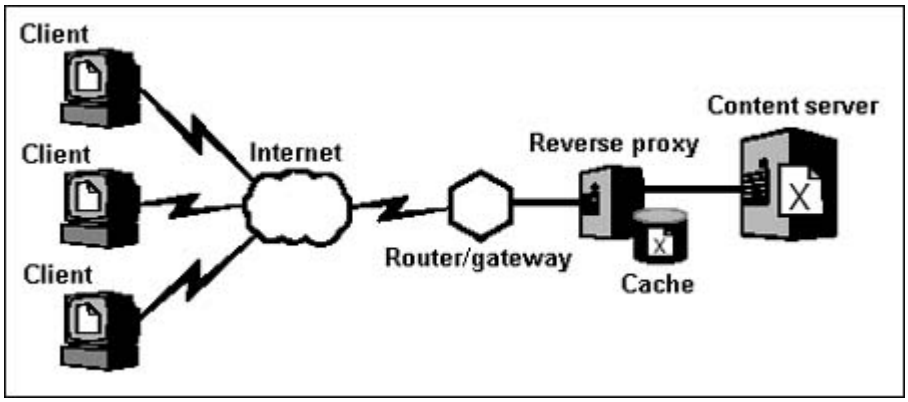
1. Giới thiệu

Chào các fan hâm mộ Linux,

Bài viết này chủ yếu dựa trên hai tài liệu là "Web Security Appliance With Apache and mod_security" của Ivan, tác giả mod_security và "Securing Apache 2: Step-by-Step" của Artur Maj. Bà con có thể xem đây là một bản dịch tiếng Việt của hai tài liệu trên, kèm theo những suy nghĩ riêng của bản thân tôi dựa vào kinh nghiệm thực tế khi triển khai reverse proxy -0-. Bài viết này có thể xem là một case study thuộc tập tài liệu "Bảo vệ máy chủ an toàn với phần mềm tự do".

Nhiệm vụ của chúng ta là bảo vệ một hay nhiều content web-server -1- nằm trong vùng Internal -2-, các web-server này có thể là Apache httpd, hoặc Microsoft IIS, hoặc có thể chỉ là một web-server đơn giản được embedded vào một ứng dụng nào đó. Để hoàn thành nhiệm vụ, chúng ta sẽ tập trung vào xây dựng một firewall/ids hoạt động ở tầng application, trong tài liệu này gọi là reverse-proxy, sử dụng Apache httpd -3- trên nền Linux.

2. Reverse proxy là gì?




Một proxy, theo định nghĩa, là một thiết bị đứng giữa server và client, tham gia vào "cuộc trò chuyện" giữa hai bên. Khái niệm proxy mà chúng ta thường dùng hàng ngày tốt hơn nên được gọi là một forward proxy: một thiết bị đứng giữa một client và tất cả server mà client đó muốn truy cập vào. Một reverse proxy làm công việc hoàn toàn ngược lại: nó đứng giữa một server và tất cả client mà server này phải phục vụ. Reverse proxy giống như một nhà ga kiêm một trạm kiểm soát, các request từ client, bắt buộc phải ghé vào reverse proxy, tại reverse proxy sẽ kiểm soát, lọc bỏ các request không hợp lệ, và luân chuyển các request hợp lệ đến đích cuối cùng là các server. Chú ý là một reverse proxy có thể luân chuyển request cho nhiều server cùng lúc.

Lợi thế lớn nhất của việc sử dụng reverse proxy là ở khả năng quản lí tập trung. Một khi đã đẩy được tất cả traffic đi qua một trạm kiểm soát duy nhất (là reverse proxy), chúng ta có thể áp dụng nhiều "đồ nghề" khác để tăng cường an ninh cho hệ thống của mình. Dĩ nhiên, bất kì sản phẩm hay công nghệ nào cũng có ưu và khuyết điểm của nó, đi cùng với single point of access bao giờ cũng là "bóng ma" single point of failure. Single point of failure có thể được giải quyết bằng cách xây dựng cluster. Đây là một vấn đề hoàn toàn vượt qua khỏi phạm vi của bài viết này, tôi chỉ xin giới thiệu bồ nào muốn tìm hiểu về cluster trên Linux thì thử ghé vào http://www.linux-ha.org. Ngoài ra áp dụng reverse proxy đúng cách sẽ giúp tăng cường performance cũng như nâng cao scalability của các web-application chạy trên các content server. Chút xíu nữa, tôi sẽ đi vào chi tiết các ưu điểm của reverse proxy cũng như làm thế nào để khai thác các ưu điểm đó.

3. Cài đặt máy chủ reverse-proxy

3.1. Chọn và cài đặt hệ điều hành cho reverse proxy

Dĩ nhiên là tôi sử dụng linux cho máy chủ reverse proxy. Tôi không mô tả quá trình cài đặt linux ở đây bởi có rất nhiều tài liệu hay trên Internet nói về đề tài này, và hơn nữa tôi nghĩ là một khi đã nghĩ đến chuyện làm reverse proxy thì chắc chắn chuyện cài đặt Linux không là vấn đề.Linux có quá trời distro, thế mrro chọn distro nào? Theo tôi thì distro nào cũng như nhau cả thôi, nhưng nếu ai đó hỏi tôi câu hỏi trên thì câu trả lời sẽ là Trustix -4-. Bất kể chọn distro nào, nhớ là sau khi cài đặt xong, hãy dành một chút thời gian để secure cái distro của mình lại trước khi đọc tiếp -5-. Phần tiếp theo chúng ta sẽ bàn về việc cài đặt Apache httpd cũng như các module kèm theo của nó.

3.2. 1.3.x hay 2.x?

Trước tiên, tôi nghĩ cần phải trả lời câu hỏi là chúng ta sẽ chọn phiên bản Apache nào để làm reverse proxy đây, 1.3.x hay 2.x? Tôi chọn 2.x vì ba lý do: thứ nhất là tôi "nghe đồn" là có rất nhiều 0-day trong phiên bản 1.3.x  . Lý do thứ hai là Apache 2.x cung cấp một bộ filtering API tốt hơn so với phiên bản 1.3.x, cho phép các module có thể nhìn thấy và tương tác với nội dung của các request cũng như các response tương ứng từ trả lời từ server. Điều này rất quan trọng đối với một reverse proxy đóng vai trò là một application gateway bởi vì nó phải kiểm tra tất cả thông tin đi xuyên qua nó trước khi chuyển giao cho bên nhận. -6-. Lý do cuối cùng là Apache httpd 2.x có performance cao hơn hẳn 1.3.x khi phục vụ các static content như file HTML và file hình ảnh. Tôi quan tâm đến vấn đề này là vì tôi có ý định giảm tải cho các content server bên trong bằng cách tách content ra làm hai loại là dynamic (các loại file CGI/Perl, PHP) và static (các file HTML và file hình ảnh), các content server chỉ phục vụ dynamic content, còn tất cả static content thì đưa qua máy chủ reverse proxy luôn. Lúc đó khi các request của client đi vào reverse proxy, nếu request đó có đích đến là một static content, máy chủ reverse proxy sẽ trả lời luôn cho client mà không cần forward request đó đến content server ở phía sau, chỉ những request đến các dynamic content mới được forward để các content server xử lí. Tôi sẽ đi vào chi tiết vấn đề này ở phần sau, chỉ lưu ý một điều là cuối cùng tôi lại không dùng Apache httpd cho mục đích này mà lại sử dụng một máy chủ web khác chuyên trị static content.

3.3. Chọn module cho Apache httpd

Ngoài những module mà tài liệu "Securing Apache 2: step by step" đề nghị, chúng ta phải chọn thêm các module sau đây:

-mod_rewrite, mod_proxy, mod_proxy_http: các module này sẽ hỗ trợ chúng ta trong việc thiết lập reverse proxy.

-mod_security: module này giúp chúng ta cấu hình reverse proxy thành một application firewall để chống lại các dạng tấn công thường thấy vào các web-application chạy trên content server. -7-

-mod_ssl: module này giúp chúng ta mã hóa dữ liệu của các kết nối từ client đến server thông qua giao thức SSL và TLS, biến giao thức HTTP không an toàn thành giao thức HTTPS rất bảo mật. -8-

Phần quan trọng tiếp theo là chọn một MPM phù hợp với mục đích làm reverse proxy của chúng ta. MPM là viết tắt của cụm từ Multi-Processing Module, là một cải thiện đáng kể của Apache httpd 2.x so với Apache 1.x. Trong kiến trúc của Apache 2.x, MPM đóng vai trò hết sức quan trọng, nó chịu trách nhiệm lắng nghe trên các cổng mạng, chấp nhận các yêu cầu kết nối từ phía client, và chuyển các yêu cầu đó vào bên trong để Apache httpd xử lí -9-. Trong trường hợp này tôi chọn MPM worker. MPM worker sử dụng thread để phục vụ các request, do đó nó có khả năng phục vụ một lượng lớn các request nhưng lại tốn rất ít tài nguyên so với các process-based MPM khác như prefork. Đồng thời MPM worker vẫn khai thác đặc tính ổn định của cá process-based MPM bằng cách tạo ra nhiều process để trước, mỗi process có nhiều thread để sẵn sàng phục vụ client -10-.

3.4. Biên dịch và cài đặt Apache httpd

Câu hỏi kế tiếp là biên dịch các module theo kiểu nào. Như chúng ta đều biết, có hai cách

biên dịch các module trong Apache httpd. Cách thứ nhất, gọi là phương pháp động, là biên dịch các module thành các thư viện liên kết chia sẻ (tương tự như các thư viện DLL trên Windows). Với cách này, các module sẽ được biên dịch thành các file .so, và sẽ được tải lên khi Apache httpd khởi động nếu cần (tùy theo các câu lệnh LoadModule trong file cấu hình conf/httpd.conf). Cách biên dịch thứ hai, gọi là phương pháp tĩnh, là gom tất cả module nhét vào trong file bin/httpd luôn (link statically). Khi khởi động và trong quá trình chạy, Apache httpd không cần phải tải thêm module nào nữa. Phương pháp tĩnh được xem là lựa chọn tốt hơn hết. Chọn phương pháp tĩnh, chúng ta không cần dùng đến module mod_so (module cần thiết để tải các file .so trong phương pháp động). Hơn nữa, theo khuyến cáo của Apache, sử dụng phương pháp tĩnh sẽ giúp tăng 5% về mặt performance so với phương pháp động.

Chúng ta tải Apache httpd 2.x ở http://httpd.apache.org/download.cgi và tải mod_security tại http://www.modsecurity.org sử dụng các lệnh sau:

CODE
```
localhost$ wget http://www.tux.org/pub/net/apache/dist/htt...d-2.0.54.tar.gz
localhost$ wget http://www.modsecurity.org/download/modsecurity-1.8.7.tar.gz
localhost$ tar -xzf httpd-2.0.54.tar.gz -C /usr/local/src
localhost$ tar -xzf modsecurity-1.8.7.tar.gz -C /usr/local/src
```

Tài liệu kèm theo của mod_security chỉ hướng dẫn cách biên dịch mod_security thành một thư viện chia sẻ của Apache httpd, do đó chúng ta cần phải chuẩn bị đôi chỗ để có thể biên dịch tĩnh mod_security:

CODE
```
localhost$ cd /usr/local/src
localhost$ mkdir -p httpd-2.0.54/modules/security
localhost$ cp modsecurity-1.8.7/apache2/mod_security.c httpd-2.0.54/modules/security
localhost$ cp httpd-2.0.54/modules/echo/Makefile.in httpd-2.0.54/modules/security
```

Okay, xong xuôi, bắt đầu biên dịch như sau:

CODE
```
localhost$ cd /usr/local/src/httpd-2.0.54
localhost$ ./configure \
--with-mpm=worker \
--disable-charset-lite \
--disable-include \
--disable-env \
--disable-status \
--disable-autoindex \
--disable-asis \
--disable-cgid \
--disable-cgi \
--disable-negotiation \
--disable-imap \
--disable-actions \
--disable-userdir \
--disable-alias \
--disable-so \
--with-module=security:mod_security.c \
--enable-modules='ssl rewrite proxy proxy_http'
```

Nếu quá trình biên dịch thành công, chúng ta sẽ tiếp tục như sau để cài Apache httpd vào hệ thống (tại thư mục mặc định là /usr/local/apache):

CODE
```
localhost$ make
localhost$ su
localhost# umask 022
localhost# make install
localhost# chown -R root:sys /usr/local/apache
```

3.5. Đổi "root" của server

Phần này xin vui lòng tham khảo tài liệu "Securing Apache 2:Step by Step."

-m

(còn tiếp)

Phần sau:
4. Cấu hình Apache httpd làm reverse proxy

---
-0-: Thực tế phần tiếng Việt của tài liệu "Securing Apache 2: Step-by-Step" tôi sao chép khá nhiều từ bản dịch và mở rộng tài liệu "Securing Apache: Step-by-Step" (http://www.securityfocus.com/infocus/1694) của hnd aka conmale. Tham khảo thêm về bản dịch và mở rộng của anh conmale tại http://www.hvaonline.net/forum/index.php?a...T&f=161&t=46199

-1-: ngoài web-server ra, giải pháp reverse proxy (hoặc tương tự) có thể áp dụng cho các dịch vụ khác như VNC (xem thử http://sourceforge.net/projects/vnc-reflector/), mail (xem thử tài liệu "Qmail as the mail gateway" của hnd@diendantinhoc.org). Chỉ duy nhất một dịch vụ tui chưa làm được reverse proxy là FTP, bồ nào có thông tin về ftp reverse proxy thì cho tui vài xu.

-2-: chúng ta vẫn có thể thiết lập reverse proxy để bảo vệ cho các web-server nằm ở ngay vùng DMZ, hoặc thiết lập một reverse-proxy đặt ngay trong vùng Internal để bảo vệ các web-server ở vùng Internal từ các mối hiểm họa đến từ bên trong.

-3-: Ngoài Apache httpd ra, còn có rất nhiều software khác có thể được ứng dụng để làm reverse proxy mà đáng kể nhất là pound. Thao khảo thêm tại địa chỉ http://www.apsis.ch/pound/.

-4-: Trustix là một distro nhỏ gọn (trọn bộ cài đặt chỉ có một CD duy nhất) được xây dựng dựa trên RedHat với hai mục tiêu chính là bảo mật và ổn định. Phiên bản stable mới nhất của Trustix là 2.2, phiên bản unstable là 3.0 RC2. Tham khảo thêm tại www.trustix.org.

-5-: Tham khảo tài liệu Linux Security HOWTO có tại http://www.tldp.org để biết thêm chi tiết. Phần mềm Bastille-Linuxcũng sẽ rất hữu dụng trong việc secure cho các Linux server.

-6-: Chỉ có sử dụng Apache 2.x thì những luật cản lọc OUTPUT của mod_security mới có tác dụng.

-7-: Tham khảo thêm tài liệu về mod_security tại địa chỉ http://www.modsecurity.org và loạt kí sự của conmale về các vụ tấn công DDoS vào HVA.

-8-: Kể từ phiên bản Apache httpd 2.0, mod_ssl đã được chính thức đưa vào Apache httpd. Tham khảo thêm tài liệu về mod_ssl tại địa chỉ http://www.modssl.org.

-9-: Chọn lựa MPM cho Apache 2.x là một vấn đề cực kì quan trọng, ảnh hưởng rất nhiền đến performance của server, do đó tôi đề nghị những ai quan tâm đến Apache 2.x, nên tham khảo thêm tài liệu về MPM tại http://httpd.apache.org/docs-2.0/mpm.html

-10-: Tại sao thread lại "ngon" hơn process về performance? Những ai quan tâm đến vấn đề này xin tìm các tìm đọc các tài liệu sau đây:
Advanced Linux programming (http://www.advancedlinuxprogramming.com)
Understanding the Linux kernel.

Tác giả Mrro - Nhóm HVAonline

# Ứng dụng tập tin htaccess trên máy chủ Apache

**Ứng dụng tập tin htaccess trên máy chủ Apache - 15/11/2004 12h:37**
**Bạn đã từng nghe về tập tin .htaccess trên các máy chủ hệ Unix (FreeBSD, Linux, Solaris, True64...)? Bạn biết rằng tập tin này có thể điều khiển được khá nhiều thứ, thậm chí thay đổi được cả thiết lập mặc định của máy chủ Apache http://apache.org/. Thế nhưng bạn đã tận dụng được bao nhiêu lệnh trong tập tin này để làm cho website của mình mạnh mẽ, an toàn hơn?**
**Trong bài viết tổng hợp này, tác giả sẽ cùng bạn nghiên cứu, ứng dụng một số lệnh thông dụng nhất để thực hiện các tác vụ bảo vệ, điều khiển website theo ý bạn muốn. Nào, xin mời bạn!**
**Tạo trang báo lỗi mang màu sắc cá nhân**
**Trong quá trình làm việc với client, nếu có lỗi xảy ra (ví dụ như không tìm thấy tập tin) thì Apache sẽ báo lỗi bằng một trang có sẵn hiển thị mã số của lỗi đó, rất không đẹp và khó hiểu.**
**Với .haccess thì bạn có thể tự tạo các trang báo lỗi hay hơn. Để làm được điều này thì trong tập tin .htaccess bạn thêm dòng sau:**

ErrorDocument mã số lỗi /trangloi.html

Trong đó mã số lỗi là mã số của lỗi phát sinh, sau đây là những lỗi hay gặp:

- 401 - Authorization Required (cần password để truy nhập)
- 400 - Bad request (Lỗi do yêu cầu)
- 403 - Forbidden (không được vào)
- 500 - Internal Server Error (lỗi server)
- 404 - Wrong page (lỗi trang, không tìm thấy...)

còn trangloi.html là trang web mà bạn muốn hiển thị khi lỗi phát sinh, có thể đưa vào tập tin này nội dung hay đồ hoạ gì tùy bạn, chẳng hạn liên kết trở về trang chính của trang web. Ví dụ: ErrorDocument 404/trangloi.html hoặc: ErrorDocument500/loi/500.html

Bây giờ bạn hãy tải (upload) 2 tập tin .htaccess và trangloi.html lên hosting của mình.

Chống ăn cắp băng thông (bandwidth)

Thông thường những dịch vụ lưu trữ web chỉ cung cấp cho bạn một lượng dữ liệu luân chuyển (data transfer) nhất định hàng tháng và khi bạn sử dụng hết lượng dữ liệu này, website của bạn sẽ tự động bị đóng cửa. Bạn sẽ phải trả thêm tiền cho lượng băng thông vượt quá hoặc phải buộc lòng chờ đến tháng sau.

Nếu hình ảnh, dữ liệu, … của bạn bị các website khác "ăn trộm" (bằng các thủ thuật đơn giản) làm cho lượng dữ liệu luân chuyển của bạn tăng lên, thì có nghĩa là bạn sẽ phải trả tiền cho cái mà bạn không sử dụng. Sử dụng tập tin .htaccess là một giải pháp hoàn hảo, để ngăn chặn việc sử dụng hình ảnh trái phép trên website của bạn. Bạn chỉ việc đưa vào tập tin .htaccess nội dung sau :

```
RewriteEngine on
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{HTTP_REFERER} !^http://(www\.)?trangweb\.com/.*$ [NC]
RewriteRule \.(gif|jpg)$ - [F]
```

Ở đoạn mã trên tôi sử dụng module Rewrite của máy chủ Apache, bạn chỉ việc thay đổi trangweb.com thành địa chỉ website của mình.

Có thể sử dụng một hình ảnh nào đó cảnh cáo những kẻ "ăn trộm" băng thông, bạn dùng dòng lệnh sau:

```
RewriteEngine on
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{HTTP_REFERER} !^http://(www\.)?trangweb\.com/.*$ [NC]
RewriteRule \.(gif|jpg)$ http://www.trangweb.com/diehotlinker.jpg [R,L]
```

Không cho hiện danh sách tập tin trong thư mục

Trong trường hợp một thư mục nào đó không có tập tin index hoặc default, Apache sẽ hiển thị một danh sách liệt kê những tập tin có trong thư mục đó. Tuy nhiên nếu đây là những tài liệu nhạy cảm, bạn không muốn người khác thấy, hãy thêm lệnh sau vào tập tin .htaccess

```
Options –Indexes
```

Thay thế trang index

Thông thường khi truy nhập vào một trang web, Apache sẽ tìm tập tin index.htm hoặc default.htm trả kết quả về cho trình duyệt, bạn có thể dùng .htaccess thay đổi mặc định này.

```
DirectoryIndex index.php index .php3 messagebrd.pl index.html index.htm
```

Với dòng lệnh này thì tất cả các tập tin được liệt kê sẽ được tìm theo thứ tự khi có yêu cầu tới thư mục hiện hành, trang nào được tìm thấy đầu tiên sẽ thành trang index của thư mục.

Cấm/hạn chế IP truy nhập

Một số người muốn làm ngập (flood) trang web của bạn, việc cần làm là ngăn cấm những IP của những người này truy nhập vào trang web, bạn thêm đoạn mã sau vào .htaccess: deny from 203.262.110.20; cho phép IP truy nhập: allow from 203.262.110.20.

Nếu bạn chỉ viết IP dưới dạng: 203.262.110 thì sẽ cấm tất cả IP trong dải từ 203.262.110.1 đến 203.262.110.254.

Sử dụng dòng lệnh sau: Deny from all sẽ cấm tất cả mọi truy nhập đến các trang web trong thư mục, tuy nhiên các tập tin trong đó vẫn có thể được sử dụng từ bên ngoài thông qua các lệnh dạng require hay include (trong lập trình PHP), có thể xem thêm mã nguồn của PHPBB forum,IBF... để hiểu rõ hơn.

Tự động chuyển đến địa chỉ mới (Redirection)

Bạn chuyển trang web của mình đến địa chỉ mới nhưng không phải ai cũng biết điều này, redirect truy nhập từ xa một cách đơn giản bằng lệnh sau:

```
Redirect/olddirectory http://www.trangwebmoi.com/thumucmoi ;
```

Tuỳ biến đuôi tập tin

Thông thường, tuỳ thuộc vào ngôn ngữ lập trình web mà bạn sử dụng tập tin sẽ có phần mở rộng khác nhau như: html, htm, asp, aspx, php, cgi, …Tuy nhiên nếu sử dụng .htaccess bạn có thể tác động vào máy chủ Apache, Apache sẽ gọi đến tập tin của bạn và trả về cho trình duyệt web của người dùng với phần mở rộng do bạn quy định trong .htaccess. Bạn sử dụng đoạn lệnh sau trong tập tin .htaccess:

```
RewriteEngine on
RewriteRule (.*)\.dll$ $1.html
```

Html là phần mở rộng thực sự của những tập tin trên website, dll là phần mở rộng do bạn lựa chọn. Lưu ý trong liên kết trên trang web, bạn phải gọi đúng đường dẫn đến tập tin với phần mở rộng mới (ở trên là dll), ví dụ http://www.trangweb.com/in dex.dll

Lưu ý khi sử dụng tập tin .htaccess:

- Chỉ áp dụng trên máy chủ Apache đã bật chế độ .htaccess, nếu chưa bạn hãy thử liên hệ với nhà cung cấp dich vụ hosting.

- Để tạo ra tập tin này bạn có thể sử dụng ngay chương trình Notepad của Windows: chọn chế độ save as với tên .htaccess, nhưng khi lưu nhớ bỏ đuôi txt.

-.htaccess chỉ có tác dụng đối với những tập tin ngang hàng (trong cùng thư mục với nó) hoặc thư mục con. Với thư mục, nó chỉ có tác dụng trong thư mục chứa nó và thư mục con, còn vô tác dụng với thư mục mẹ (parent directory).

- Bạn có thể dùng một số chương trình FTP (Leaf FTP, WS FTP, Cute FTP) để tải tập tin .htaccess lên hosting của mình với chế độ ASCII, nếu nó không hoạt động bạn thử CHMOD với giá trị 644.