



Trần Thạch Tùng

Hiệu đính : Trần Tiến Dũng
Cố vấn khoa học : Đoàn Thiện Ngân



Bảo mật **và** **Tối ưu** **trong** **Red Hat Linux**

- Hướng dẫn chi tiết cài đặt Hệ điều hành và các ứng dụng chính của một máy Linux (6.x, 7.x).
- Đĩa mềm chứa đầy đủ các tập tin cấu hình chuẩn cho các ứng dụng chính trên Linux.

NHÀ XUẤT BẢN LAO ĐỘNG - XÃ HỘI



Trần Thạch Tùng

Hoàng Đức Hải

Hiệu đính : Trần Tiến Dũng

Cố vấn khoa học : Đoàn Thiện Ngân

Bảo mật và Tối ưu trong Red Hat Linux

**NHÀ XUẤT BẢN LAO ĐỘNG - XÃ HỘI
NĂM 2002**

GIỚI THIỆU

Giới thiệu về cuốn sách

Khi bắt đầu viết cuốn sách này, câu hỏi đầu tiên tôi đã tự hỏi mình là làm thế nào cài đặt Linux trên một server và đảm bảo rằng không một ai từ bên ngoài hoặc bên trong Linux có thể truy cập Linux mà không có sự cho phép. Kể đến tôi tự hỏi có bất kỳ phương pháp nào giống như trên windows dùng để cải thiện hiệu năng của máy tính. Sau đó tôi đã bắt đầu tìm kiếm trên Internet, đọc sách, thu thập thông tin về bảo mật, về cải thiện hiệu năng cho hệ thống của tôi. Sau nhiều năm nghiên cứu và học hỏi, cuối cùng tôi đã tìm được câu trả lời cho câu hỏi của tôi. Những câu trả lời đã được tìm thông qua tài liệu, bài báo, sách và Internet. Tôi đã viết tài liệu dựa trên những nghiên cứu của tôi và có thể giúp tôi trong công việc hằng ngày. Qua nhiều năm, tài liệu của tôi đã lớn dần và giống như một cuốn sách với nhiều ví dụ và những chú ý được phân bố theo từng chương. Tôi đã quyết định đưa cuốn sách này đến tay bạn đọc với hy vọng nó sẽ ít nhiều giúp ích cho các bạn đang làm việc với Linux.

Với việc chia sẻ thông tin này, tôi cảm thấy rằng tôi đã làm một việc có ích cho mọi người là trả lời nhiều câu hỏi về tính hấp dẫn, đáng tin cậy, ổn định, mạnh mẽ, nhanh chóng và miễn phí của hệ điều hành Linux. Tôi rất mong nhận được sự phản hồi và những góp ý chân thành về quyển sách này, nó sẽ giúp ích cho việc hoàn thiện trong thời gian tới, tôi cũng mong được mọi người đón nhận nó và sẽ tìm nhiều tiện ích của Hệ điều hành Linux.

Với nhiều thời gian cùng nhiều nỗ lực bản thân khi viết sách này chắc chắn rằng kết quả chính xác và khả thi. Tuy nhiên, sẽ không tránh khỏi những sai sót, nếu bạn tìm được những lỗi cũng như những thiếu sót ở bất kỳ chương nào trong cuốn sách này, làm ơn cho phép tôi biết để sửa đổi cho lần tái bản tiếp theo.

Độc giả

Cuốn sách này dành cho bất cứ những ai đã, đang và sẽ sử dụng Linux, đặc biệt dành cho các kỹ thuật viên, những người quản trị hệ thống Linux và cũng là tài liệu tham khảo rất tốt cho các sinh viên đang học Linux. Cuốn sách này sẽ trình bày cho các bạn làm thế nào để cài đặt và thiết lập một Red Hat Linux server, cùng những vấn đề bảo mật cần thiết và sự tối ưu hoá một Linux server ở mức cao. Vì chúng ta nói đến cấu hình của tối ưu hoá và bảo mật, chúng ta sẽ sử dụng các chương trình nguồn thường được phân phối dưới dạng .tar.gz chẳng hạn, như những gói chương trình nguồn của Apache, BIND/DNS, Samba, Squid, OpenSSL... Với những gói tài nguyên này, chúng ta có thể nhanh chóng tiến hành việc nâng cấp, cập nhật bảo mật khi cần thiết, ngoài ra với những gói tài nguyên trên, chúng ta sẽ có một sự biên dịch theo ý muốn và tối ưu hoá tốt hơn, so với bình thường chúng ta không thể sử dụng với những gói dữ liệu dạng RPM.

Những yêu cầu chung

Chúng ta cần một ổ CD-ROM trên máy tính và một bộ CD chứa chương trình cài đặt Linux mà ta hay gọi là chương trình nguồn, tốt nhất là nên dùng bộ “Official Red Hat Linux” (bộ “chính thống”-?-) thay vì dùng bộ tải xuống miễn phí (free download) vì trong bộ “chính thống”, các trình cài đặt đều đã được kiểm tra. Các hướng dẫn trong sách này đều đã được kiểm chứng với bộ “chính thống” phiên bản 6.1, 6.2, trong số này có những chương trình được kiểm tra trên Red Hat Linux 7.2.

Trước khi cài đặt Linux, bạn nên hiểu về các phần cứng có trong máy tính của bạn hoặc các thiết bị bạn sẽ cài thêm với Linux. Sau khi xem xét phần cứng máy tính, phần còn lại của tiến trình cài đặt sẽ được hướng dẫn trong cuốn sách này.

Những sản phẩm (chương trình) được đề cập trong cuốn sách

Có nhiều sản phẩm sẽ được đề cập trong cuốn sách này, chúng là những chương trình mang tính thương mại, nhưng cũng có nhiều sản phẩm không thương mại, tức là bạn được miễn phí khi sử dụng hoặc sửa đổi và phân phát cho người khác, do đó nhiều khi chúng ta cũng sẽ không xác định một cách chính xác nguồn gốc của những chương trình này. Tuy nhiên, chúng được sử dụng hằng ngày trong một số công ty kể cả những công ty lớn.

Tập tin cấu hình

Tất cả các phần mềm mà tôi mô tả trong cuốn sách này có một thư mục hoặc một thư mục con cụ thể trong tập tin được nén ở dạng lưu trữ tar có tên là “floppy.tgz” trong đĩa mềm kèm theo sách. Các thư mục đó chứa file cấu hình cho một phần mềm cụ thể nào đó. Ngoài việc bạn có thể có được các file cấu hình từ đĩa mềm, nếu bạn cần lấy một tập tin cấu hình nào đó, bạn có thể thực hiện việc cắt và dán chúng từ các phần cấu hình trong chương tương ứng trong sách. Dù bạn thực hiện bằng cách nào đi nữa, trách nhiệm của bạn là phải hiệu chỉnh chúng cho phù hợp với nhu cầu của bạn và đặt các tập tin cấu hình liên quan với các phần mềm tương ứng tới các nơi thích hợp trên máy server của bạn.

Lời cảm ơn:

Xin cảm ơn bố mẹ, người đã sinh ra và nuôi dưỡng con nên người, xin cảm ơn các bạn đồng nghiệp đặc biệt là anh Ngân và anh Dũng đã góp ý, bổ sung cho cuốn sách. Tôi cũng xin cảm ơn công ty Global Cybersoft Việt Nam và các đồng nghiệp trong phòng IT của công ty đã tạo điều kiện để tôi hoàn thành cuốn sách này.

Lời ngỏ

Kính thưa quý Bạn đọc gần xa, Ban xuất bản MK.PUB trước hết xin bày tỏ lòng biết ơn và niềm vinh hạnh trước nhiệt tình của đông đảo Bạn đọc đối với tủ sách MK.PUB trong thời gian qua.

Khẩu hiệu của chúng tôi là:

- * Lao động khoa học nghiêm túc.
- * Chất lượng và ngày càng chất lượng hơn.
- * Tất cả vì Bạn đọc.

Rất nhiều Bạn đọc đã gửi mail cho chúng tôi đóng góp nhiều ý kiến quý báu cho tủ sách.

Ban xuất bản MK.PUB xin được kính mời quý Bạn đọc tham gia cùng nâng cao chất lượng tủ sách của chúng ta:

Trong quá trình đọc, xin các Bạn ghi chú lại các sai sót (dù nhỏ, lớn) của cuốn sách hoặc các nhận xét của riêng Bạn. Sau đó xin gửi về địa chỉ:

E-mail: mk.book@cinet.vnnews.com; mk.pub@cinet.vnnews.com

Hoặc gửi về: Nhà sách Minh Khai

249 Nguyễn Thị Minh Khai, Q.1, Tp. Hồ Chí Minh

Nếu Bạn ghi chú trực tiếp lên cuốn sách, rồi gửi cuốn sách đó cho chúng tôi thì chúng tôi sẽ xin hoàn lại cước phí bưu điện và gửi lại cho Bạn cuốn sách khác.

Chúng tôi xin gửi tặng một cuốn sách của tủ sách MK.PUB tùy chọn lựa của Bạn theo một danh mục thích hợp sẽ được gửi tới Bạn.

Với mục đích ngày càng nâng cao chất lượng của tủ sách MK.PUB, chúng tôi rất mong nhận được sự hợp tác của quý Bạn đọc gần xa.

" MK.PUB và Bạn đọc cùng làm !"

MK.PUB

Tổng quan

Giới thiệu

Phần 1 - Cài đặt Linux

Chương 1 - Giới thiệu về Linux

Chương 2 - Cài đặt server Linux của bạn

Phần 2 - Các vấn đề liên quan về bảo mật và tối ưu

Chương 3 - Tổng quan về bảo mật hệ thống

Chương 4 - Tổng quan về tối ưu hệ thống

Chương 5 - Cấu hình và xây dựng một kernel bảo mật và được tối ưu

Phần 3 - Liên kết mạng

Chương 6 - Quản lý hệ thống mạng Linux TCP/IP

Chương 7 - Liên kết Firewall

Chương 8 - Liên kết Firewall với hỗ trợ giả lập IP và chuyển tiếp

Phần 4 - Sự tham khảo các phần mềm liên quan

Chương 9 - Chức năng biên dịch

Chương 10 - Phần mềm bảo mật (Công cụ giám sát)

Chương 11 - Phần mềm bảo mật (Các dịch vụ mạng)

Chương 12 - Phần mềm bảo mật (Tính toán vận hệ thống)

Chương 13 - Phần mềm bảo mật (Sự quản lý và sự giới hạn)

Chương 14 - Phần mềm server (Dịch vụ mạng BIND/DNS)

Chương 15 - Phần mềm server (Dịch vụ Mail)

Chương 16 - Phần mềm server (Dịch vụ mã hóa)

Chương 17 - Phần mềm server (Dịch vụ cơ sở dữ liệu)

Chương 18 - Phần mềm server (Dịch vụ Proxy)

Chương 19 - Phần mềm server (Dịch vụ về Web)

Chương 20 - Cài đặt Apache với các thành phần tùy chọn

Chương 21 - Phần mềm server (Dịch vụ chia sẻ tập tin)

Phần 5 - Các vấn đề liên quan về sao lưu dữ liệu

Chương 22 - Các thủ tục về sao lưu và khôi phục dữ liệu

Phần 6 - Cài đặt và cấu hình một số phần mềm trên Red Hat Linux 7.2

Chương 23 - Cài đặt WEB SERVER APACHE 1.3.20

Chương 24 - Cài đặt LINUX FREES/WAN

Chương 25 - Cài đặt Squid Proxy Server

Chương 26 - Cài đặt OpenSSH Client/Server

Chương 27 - Cài đặt và sử dụng Samba

Phần 7 - Các phụ lục

Phụ lục A - Những lát léo, mẹo và công việc của người quản trị

Phụ lục B - Các RFC đang tồn tại

MỤC LỤC

GIỚI THIỆU	3
Giới thiệu về cuốn sách.....	3
Độc giả.....	3
Những yêu cầu chung.....	4
Tập tin cấu hình.....	4
Lời ngỏ.....	5
Tổng quan.....	7
PHẦN 1 : HƯỚNG DẪN CÀI ĐẶT LINUX.....	17
Chương 1: GIỚI THIỆU VỀ LINUX	19
Linux là gì?.....	20
Một vài nguyên nhân dẫn đến việc sử dụng Linux.....	20
Xua tan đi sự lo ngại, sự không chắc chắn và sự nghi ngờ về Linux.....	21
Chương 2: CÀI ĐẶT SERVER LINUX.....	23
Hướng dẫn cài đặt Linux	24
Sự hiểu biết về phần cứng trong server.....	24
Tạo đĩa boot và tiến trình boot.....	25
Các cách cài đặt và phương pháp của chúng.....	26
Cài đặt đĩa (Disk setup).....	26
Sự chọn lựa những package (gói dữ liệu) riêng lẻ.....	32
Các gói chương trình không nên cài đặt do các nguyên nhân bảo mật.....	34
Làm thế nào sử dụng những lệnh RPM.....	38
Khởi động và dừng những dịch vụ daemon	39
Các phần mềm cần phải loại bỏ sau khi tiến trình cài đặt của server hoàn thành.....	40
Các phần mềm phải được cài đặt sau sự cài đặt của server.....	43
Những chương trình được cài đặt trên server của bạn.....	46
Định màu trên terminal của bạn.....	51
Cập nhật phần mềm mới nhất	52
PHẦN 2 : CÁC VẤN ĐỀ LIÊN QUAN VỀ BẢO MẬT VÀ TỐI ƯU ..53	
Chương 3: TỔNG QUAN VỀ BẢO MẬT LINUX.....	55

Chương 4: TỔNG QUAN VỀ SỰ TỐI ƯU LINUX	91
Chương 5: CẤU HÌNH VÀ XÂY DỰNG MỘT KERNEL	109
Linux Kernel.....	110
Làm một đĩa mềm boot cấp cứu.....	111
Bảo mật Kernel.....	114
Cấu hình Kernel.....	117
Cài đặt Kernel mới.....	124
Xóa những chương trình, tập tin, dòng có liên quan tới các module.....	127
Tạo một đĩa cứu nguy mới (rescue floppy):.....	129
Tạo đĩa mềm boot cấp cứu (emergency boot floppy disk).....	129
Cập nhật thư mục "/dev".....	130
PHẦN 3 : LIÊN KẾT MẠNG	131
Chương 6: QUẢN LÝ HỆ THỐNG MẠNG LINUX TCP/IP	133
Cài đặt nhiều card mạng trên một máy.....	134
Các tập tin liên quan đến chức năng của mạng.....	135
Cấu hình mạng TCP/IP bằng tay với giao diện dòng lệnh.....	140
Chương 7: LIÊN KẾT FIREWALL	145
Linux IPCHAINS.....	146
Xây dựng một nhân của hệ thống (Kernel) với sự hỗ trợ IPCHAINS Firewall.....	150
Một vài sự giải thích về các nguyên lý được sử dụng trong các tập tin firewall script.....	150
Các tập tin firewall scripts.....	153
Cấu hình tập tin script "/etc/rc.d/init.d/firewall" cho Web Server.....	154
Cấu hình tập tin script "/etc/rc.d/init.d/firewall" cho Mail Server.....	167
Tóm tắt về IPCHAINS.....	178
Chương 8: LIÊN KẾT FIREWALL VỚI HỖ TRỢ TÍNH NĂNG GIẢ MẠO (MASQUERADING) IP VÀ CHUYỂN TIẾP (FORWARDING)	185
Giả mạo và chuyển tiếp IP trong Linux.....	186
Xây dựng một Kernel với Firewall hỗ trợ giả mạo IP và chuyển tiếp.....	186
Sự cấu hình tập tin script cho Gateway Server.....	189
Từ chối truy nhập vào hệ thống từ một vài địa chỉ IP.....	203
Công cụ quản trị IPCHAINS.....	204

PHẦN 4 : SỰ THAM KHẢO CÁC PHẦN MỀM LIÊN QUAN205**Chương 9: CHỨC NĂNG BIÊN DỊCH.....207**

Chức năng biên dịch trong Linux	208
Các gói dữ liệu cần thiết.....	208
Tại sao chúng ta chọn sử dụng tarballs?.....	210
Biên dịch các phần mềm trên hệ thống của bạn	210
Xây dựng và cài đặt phần mềm trên hệ thống của bạn	212
Soạn thảo các tập tin với trình soạn thảo vi.....	213
Một vài ghi chú sau cùng.....	213

Chương 10: PHẦN MỀM BẢO MẬT (Công cụ giám sát).....215

Linux sXid	216
Cấu hình.....	217
Các công cụ quản trị sXid.....	219
Linux Logcheck.....	221
Giới thiệu.....	221
Cấu hình.....	223
Linux PortSentry.....	225
Cấu hình.....	227
Khởi động PortSentry.....	233

Chương 11: PHẦN MỀM BẢO MẬT (Các dịch vụ mạng).....235

Linux OpenSSH Client/Server.....	236
Cấu hình.....	239
Cấu hình OpenSSH để dùng TCP-Wrappers inetd super server.....	245
Cấu hình OpenSSH cho mỗi người sử dụng	246
Các công cụ OpenSSH cho người sử dụng.....	248
Linux SSH2 Client/Server.....	251
Cấu hình.....	252
Cấu hình Sshd2 để dùng TCP-Wrappers inetd super server	260
Cấu hình SSH2 cho mỗi người sử dụng	261
Các công cụ SSH2 cho người sử dụng.....	262

Chương 12: PHẦN MỀM BẢO MẬT (Tính toàn vẹn hệ thống).....265

Linux Tripwire 2.2.1	266
Cấu hình.....	271
Bảo vệ Linux với Tripwire	278
Các lệnh	279