Nhóm 9.

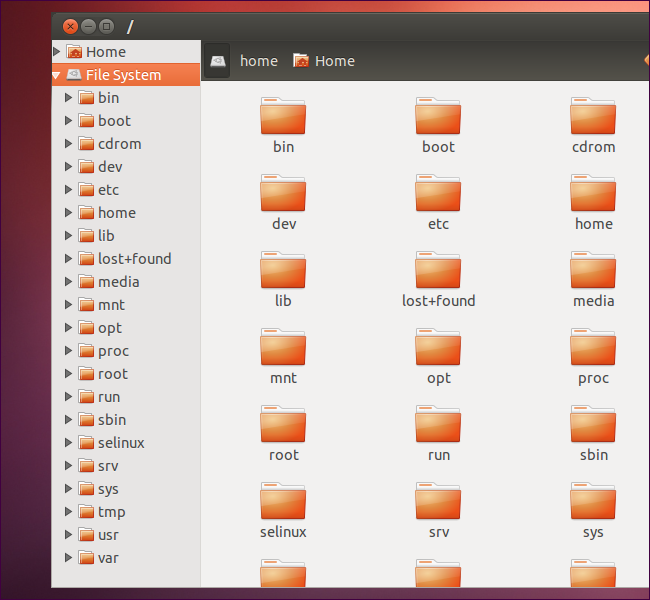
**Cấu trúc cây thư mục trên Linux.**

Linux quan niệm bất cứ thứ j tồn tại trong máy tính của bạn đều là FILE (tệp tin) cả. Ngay cả DIRECTORY (thư mục) cũng là 1 loại tệp tin. Do đó mà lệnh "file" luôn luôn tương thích với mọi thứ trong hệ thống. Nó sẽ cho ra kết quả là filetype (định dạng tệp tin) của file mà ta kiểm tra.

Cũng xin nói thêm rằng ngoài việc cung cấp thông tin về chức năng của từng thư mục trong hệ thống cây thư mục của Linux, ở từng phần, tôi cũng sẽ lồng ghép vào 1 số khái niệm về Security mà có liên quan đến thư mục đó. Tuy nhiên, trong khuôn khổ, tôi sẽ chỉ giới thiệu khái niệm; còn việc đi vào chi tiết thì sẽ ko trình bày. Mà thay vào đó, những j quan trọng và đáng lưu ý sẽ được trình bày cụ thể ở những bài viết sau.

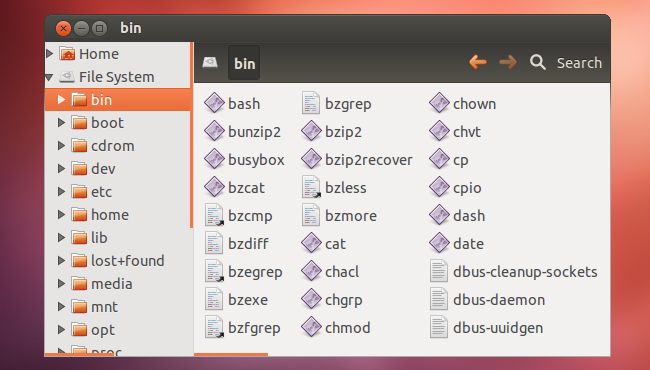
**/ - Thư mục ROOT.**

Đây là cái GỐC của hệ thống tệp tin trên Linux. Cũng giống như gốc của 1 ổ đĩa trên Windows là "C:/" hay "D:/" vậy. Nhưng trên Linux thì ko có khái niệm "ổ đĩa" này, mà mọi thứ đều nằm dưới ROOT. Thư mục ROOT này thuộc sở hữu của 1 User đặc biệt có tên là ROOT; và cũng thuộc Group đặc biệt có tên là ROOT.



Để truy cập đến ROOT, ta chỉ cần "cd /" là xong, quá là ez nhỉ! Sau đó "ls -la" 1 phát là ta có thể show ra toàn bộ thông tin và cấu trúc thư mục. Điều j sẽ xảy ra nếu 1 thằng tin tặc nào đó cũng xem được cái này? Đúng vậy, tôi chính là đang nói đến kỹ thuật **Directory Traversal Attack** giúp một anonymous (ai đó nặc danh) có thể list ra toàn bộ danh sách cây thư mục trên Server của bạn! Chưa cần biết là anonymous đó có thể thao túng được j từ việc này; chỉ biết là nếu họ có thể list ra những thông tin này thì coi như bạn đã để rò rỉ thông tin rồi; bị tấn công hay ko, chỉ còn là vấn đề thời gian  và nhân phẩm mà thôi!

**/bin - Thư mục BINARY của USER chứa các command - line cho Users.**

Đây là thư mục chứa các chương trình thực thi dòng lệnh mà bất cứ User nào cũng sẽ sử dụng. Do đó Linux nhóm các chương trình đó vào /bin để tránh vấn đề duplicate. Ví dụ mấy command đơn giản như "bash, cat, cp, echo, grep, ls, ping, ..." thì User nào chả dùng. 

Ngoài ra, các command trong thư mục này ko những được các User thông thường sử dụng; mà còn được các System Admin sử dụng. Các command này thực sự rất cần thiết phải được đặt ở vị trí riêng biệt này, và được sử dụng bởi mọi User vì ko phải lúc lúc nào các User cũng luôn có thể truy cập vào thư mục "/bin" của User khác. Trường hợp này xảy ra khi bạn muốn fix lại j đó ở thư mục của User khác, nhưng lại bị hạn chế quyền truy cập, cộng thêm việc hệ thống của bạn mới chỉ xác định được mỗi thư mục ROOT.

**/boot - Thư mục BOOT LOADER chứa tệp tin khởi động.**

Đây là thư mục chứa các tệp tin cần thiết phục vụ cho quá trình khởi động hệ thống Linux, như GRUB và KERNEL; các dữ liệu này sẽ được lưu trữ tại đây trước khi Linux Kernel bắt đầu thực thi chế độ người dùng. Tuy nhiên, các tệp tin cấu hình việc khởi động lại ko được đặt ở thư mục này.

**/dev - Thư mục DEVICE chứa các tệp thiết bị.**

Đây là thư mục chứa các tệp tin đại diện cho các thiết gắn vào hệ thống của bạn. Các phân vùng ổ đĩa, ổ đĩa rời, ổ đĩa mềm, bàn phím, chuột, loa, ... Nói chung là mỗi thiết bị gắn vào hệ thống của bạn sẽ được đại diện bởi 1 tệp tin trong thư mục này. Và đương nhiên vì nó là FILE, nên có thể đọc và ghi (với ROOT).

Lấy ví dụ thế này, giả sử tệp tin dev/dsp là đại diện cho loa máy tính của bạn; mọi dữ liệu bạn truyền vào tệp tin này ngay lập tức sẽ được truyền đến loa máy tính. Nếu bạn chạy command "cat /boot/vmlinuz > /dev/dsp", ngay lập tức bạn sẽ nghe thấy 1 số âm thanh phát ra từ loa (đương nhiên là nếu hệ thống được cấu hình chuẩn).

Phần lớn các thiết bị trong /dev được phân ra thành 2 loại thiết bị là "block" và "character"; tuy nhiên các loại thiết bị khác cũng có thể ko thuộc loại nào trong 2 loại thiết bị này. Có thể hình dung rằng "block device" là các thiết bị lưu trữ dữ liệu; còn "character device" là các thiết bị truyền tải dữ liệu. Do đó có thể thấy các ổ đĩa cứng/mềm đều là "block device"; còn loa hay bàn phím/chuột j đó sẽ thuộc loại "character device".

Ngoài các thiết bị thực ra, thì trong /dev còn tồn tại 1 số file thiết bị ảo, tức là nó ko đại diện cho 1 thiết bị phần cứng thực sự nào được gắn vào máy tính. Mà các file thiết bị ảo này được Linux Kernel tạo ra để phục vụ hoạt động của hệ điều hành. Ví dụ thiết bị "/dev/null" là 1 cái hố đen sẽ triệt tiêu mọi output mà bạn truyền vào; hay như thiết bị "/dev/random" là 1 máy khởi tạo các giá trị số ngẫu nhiên.

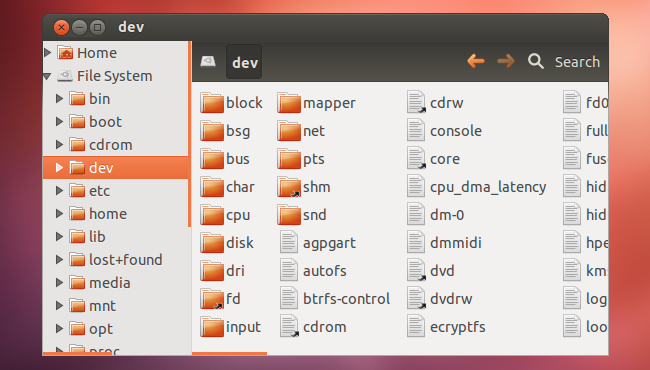
Về mặt Security, vì đặc tính nội tại là đại diện cho các thiết bị được gắn vào máy tính, nên "/dev" cũng là nơi dữ liệu có thể bị thay đổi. Do đó, trong nhiều tình huống, cần ngăn chặn ảnh hưởng xấu của đặc tính này bằng việc cấu hình các tùy chọn về thư mục cho "/dev"; nhằm hạn chế sự thay đổi dữ liệu dẫn đến việc tin tặc có thể khai thác được hệ thống thông qua dữ liệu trong "/dev".

**/etc - Thư mục chứa các tệp tin cấu hình hệ thống.**

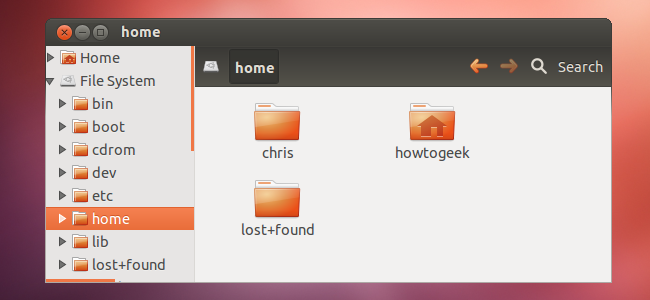
Thư mục này có thể nói là "trung tâm thần kinh hệ thống" của Linux. Thư mục này chứa tất cả mọi tệp tin cấu hình của hệ thống. Đương nhiên các tệp tin cấu hình này có thể nằm ngay dưới thư mục này, hoặc cũng có thể nằm trong thư mục con của thư mục này.

Một "tệp tin cấu hình" được định nghĩa là tệp tin cục bộ, lưu trữ thông tin dạng TEXT, được Linux Kernel sử dụng để kiểm soát mọi hoạt động của chương trình và hệ thống. Thông tin biểu thị dưới dạng TEXT của tệp tin này không được phép thay đổi trong quá trình hệ thống hoạt động; và tệp tin này ko được phép tăng permission (quyền) lên EXECUTE.

Ví dụ lệnh "cat /etc/passwd" sẽ hiển thị file nằm ở đường dẫn "/etc/passwd". Đây là tệp tin cấu hình lưu trữ thông tin về tất cả các User trong hệ thống. Đương nhiên những thông tin nhạy cảm (như password chẳng hạn) đều đã được băm.

Vì đặc tính chứa toàn bộ quy định cấu hình hệ thống, do đó "/etc" ngoài việc đơn giản hóa quá trình làm việc cho System Admin, thì nó còn là vị trí mà các tin tặc luôn muốn nhắm vào bất cứ khi nào có thể. Tại vì chỉ cần thay đổi 1 byte ký tự trong 1 tệp tin nào đó thôi, có khi cũng làm thay đổi hoàn toàn việc kiểm soát hệ thống của Linux Kernel. 

**/home - Thư mục HOMEPAGE.**

Linux là hệ điều hành hỗ trợ đa người dùng; vì vậy mỗi người dùng sẽ được cấp 1 thư mục cụ thể mà chỉ có họ và ROOT là được phép truy cập vào thư mục đó. Các thư mục này đều được tập hợp lại trong "/home". Ví dụ nếu Username của bạn là "cuongbv" thì thư mục HOME của bạn sẽ có đường dẫn là "/home/cuongbv". Đây là "sân chơi" của bạn; bạn có full quyền với mọi tài nguyên (thư mục/file) nằm trong sân chơi này. Ngoài bạn và ROOT có full quyền với nó ra, thì các User khác ko thể truy cập vào. 

**/lib - Thư mục LIBRARY chứa các tệp tin thư viện.**

Đây là thư mục chứa các tệp tin thư viện cần thiết cho các chương trình trong "/bin" cũng như các chương trình của Linux Kernel (ví dụ như bộ thư viện lập trình C chẳng hạn). Các tệp tin thư viện trong Linux có phần mở rộng (định dạng) là "\*.so"; tương đương với các tệp tin thư viện liên kết động trong Windows là ".dll".

**/media - Thư mục MEDIA chứa các tệp tin phương tiện.**

Đây là thư mục chứa các thư mục con, mà mỗi thư mục con là đại diện cho 1 thiết bị đa phương tiện đang được kết nối vào hệ thống Linux của bạn. Ví dụ khi bạn nhét 1 đĩa CD vào, 1 thư mục sẽ tự động xuất hiện bên trong "/media"; bạn có thể truy cập vào tài nguyên đang lưu trữ trên đĩa CD đó bằng cách "cd" vào thư mục này.

Lưu ý, phân biệt sự khác nhau giữa "/media" và "/dev" nhé! "/dev" chứa mọi thiết bị ngoại vi được kết nối với hệ thống của bạn; còn "/media" chỉ chứa thư mục các tệp tin đa phương tiện thôi. Ví dụ khi bạn cắm cái USB vào, trong "/dev" sẽ xuất hiện 1 FILE chứa thông tin về cái USB đó; còn trong "/media" sẽ xuất hiện 1 FOLDER chứa các tệp tin trong USB. Khi bạn cắm 1 cái loa vào, chỉ có trong "/dev" sẽ xuất hiện 1 FILE đại diện cho cái loa đó; còn trong "/media" sẽ ko xuất hiện thêm bất cứ FILE hay FOLDER nào cả.

**/mnt - Thư mục MOUNT để gắn kết tạm thời các thư mục khác.**

Đây là người ae có kHá nhiều điểm tương đồng với "/media". "/mnt" là nơi các System Admin "gắn" (mount) các FILE vào hệ thống cây thư mục của Linux. Mount là quá trình bạn tạo 1 FILESYSTEM (hệ thống tệp tin) cho hệ thống. FILESYSTEM là tập hợp các phương pháp và cấu trúc dữ liệu mà OS sử dụng để theo dõi các tệp tin trên ổ đĩa, phân vùng. Ví dụ, nếu trong hệ thống của bạn có 2 filesystems, điều này đồng nghĩa rằng trong hệ thống đang có 2 **phân vùng** riêng biệt, kiểu như 2 ổ (C và D) trong Windows chẳng hạn.

Và đương nhiên, chỉ khi hoàn thành việc mount filesystem mới vào đâu đó (vào "/mnt" chẳng hạn), thì bạn mới có thể truy cập vào nội dung bên trong filesystem đó. Thư mục "/mnt" này thường sẽ chứa các điểm gắn kết cho các filesystem như đĩa CD, USB, ... Ví dụ, Linux Subsystem for Windows định nghĩa các phân vùng ổ đĩa trên máy Windows của bạn là các filesystems; và mount chúng vào bên trong "/mnt". Bạn có thể

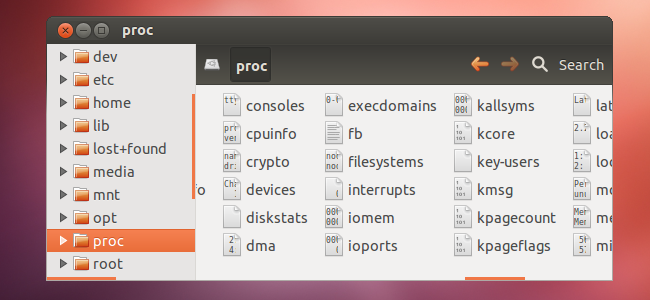
Ko có quy tắc yêu cầu bạn chỉ được phép mount các filesystems mới vào "/mnt"; tuy nhiên, cũng đừng "xả rác" ra hệ thống thông qua việc mount lung tung rồi tự bóp bản thân. Thường thì hệ thống của bạn sẽ định nghĩa sẵn 1 số filesystems được mount sẵn trong "/mnt" (như "/mnt/floppy" hay "/mnt/cdrom" chẳng hạn). Tuy nhiên một số bản phân phối Linux như Debian thực hiện cấp phát "/floppy" hay "/cdrom" trực tiếp ngay dưới "/" (ROOT), chứ ko mount chúng vào bên dưới "/mnt".

Vậy có thể tổng kết lại ví dụ như sau; khi bạn cắm USB vào máy tính Linux, 1 tệp tin cấu hình đại đại diện cho cái USB đó sẽ tự động xuất hiện trong "/dev"; 1 thư mục đa phương tiện sẽ tự động xuất hiện trong "/media"; và 1 phân vùng mới đại diện cho ổ USB đó sẽ tự động xuất hiện trong hệ thống. Nhiệm vụ của 1 System Admin khoa học là phải mount cái phân vùng này ("media/usb") vào bên dưới "/mnt".

**/opt - Thư mục OPTION chứa các gói tùy chọn.**

Thư mục này chứa các thư mục con lưu trữ các package mà bạn tải về hệ thống (thông qua "sudo apt install ..." chẳng hạn). Vai trò của nó kiểu kiểu như thư mục "C:\Windows\Program Files\" trên Windows vậy.

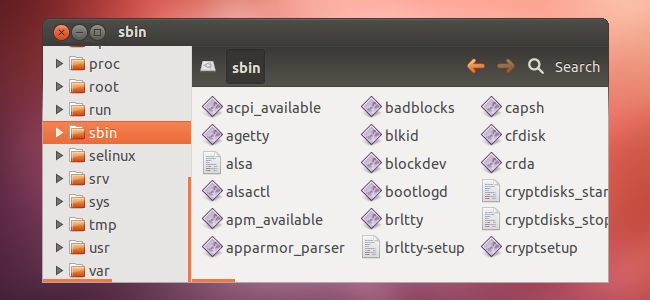
**/proc - Thư mục PROCESS chứa các tệp tin tiến trình.**

Linux hiểu mọi thứ chứa trong nó đều là FILE; do đó các tiến trình cũng được Linux định nghĩa là FILE; và đây là các tệp tin ảo. Ví dụ, khi có 1 tiến trình đang chạy trên hệ thống Linux của bạn, ngay lập tức 1 giả tệp tin sẽ xuất hiện bên trong "/proc" và lưu trữ mọi thông tin liên quan đến tiến trình đó (như ID tiến trình, vị trí tệp thực thi, bộ nhớ chiếm dụng, cấu hình phần cứng, ...). Vì tính kiểm soát cao như vậy, nên "/proc" cũng được coi là trung tâm giám sát/điều khiển thông tin cho Kernel. 

**/run - Thư mục RUN chứa các tệp tin trạng thái ứng dụng đang hoạt động.**

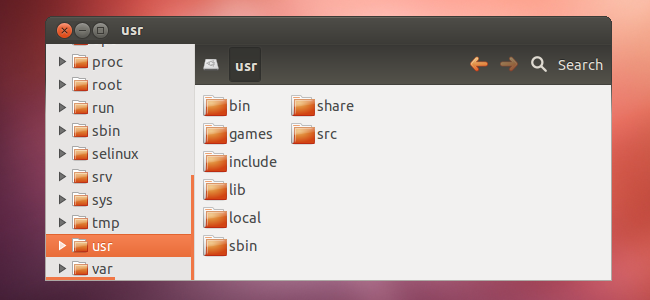
Đây là thư mục khá mới, là thư mục cung cấp cho các chương trình ứng dụng một vị trí tiêu chuẩn để lưu trữ các tệp dữ liệu tạm thời mà chúng yêu cầu trong quá trình hoạt động. Như bên trên tôi đã nói, các tệp tin trong "/tmp" có thể bị xóa khi khởi động lại hệ thống, hoặc thông qua dịch vụ "tmpwatch", do đó các chương trình này cần 1 vị trí cứng hơn để tránh khả năng tệp tin tạm của mình bị xóa trong quá trình hoạt động.  
  
Thông tin thêm rằng thư mục mới này được tạo ra thông qua sự trao đổi và thảo luận giữa các nhà phát triển hệ thống Linux - based (như Fedora, Debian, ...)

**/sbin - Thư mục SYSTEM BINARY, giống mà khác BINARY.**

Linux phân biệt giữa quá trình thực thi thông thường và quá trình thực thi để kiểm soát hệ thống. Nếu như "/bin" là nơi lưu trữ các chương trình thực thi thông thường; thì thư mục này có chức năng tương tự thư mục "/bin"; trong đây chứa các chương trình command - line dành riêng cho System Admin. Để thực thi các chương trình trong thư mục này, bạn phải leo thang đặc quyền lên ROOT. 

**/srv - Thư mục SERVICE chứa các tệp tin dịch vụ.**

Thư mục này chứa các dữ liệu dịch vụ được cung cấp bởi hệ thống Linux. Ví dụ nếu bạn đang sử dụng Linux để cung cấp dịch vụ máy chủ Apache cho 1 website, bạn có thể lưu trữ toàn bộ các file của máy chủ Apache đó vào 1 thư mục ngay dưới "/srv" (như "/srv/httpd" chẳng hạn).

Vì đây là nơi chứa dữ liệu dịch vụ đang chạy trên hệ thống Linux, nên các thư mục trong "/srv" sẽ ko thuộc quyền sở hữu của User nào cả ngoài ROOT. Các dịch vụ do đơn người dùng cung cấp ko nên đặt vị trí lưu trữ ở đây. Trong thực tế, với các hệ thống dịch vụ lớn, các dịch vụ cũng phải thực hiện kiến trúc phân tầng thành nhiều sub - directory (thư mục con) như tại "/home" vậy. 

**/tmp - Thư mục TEMPORARY chứa các tệp tin tạm.**

Đây là thư mục lưu trữ mọi tệp tin tạm trong quá trình Linux hoạt động; và chính vì nó là nơi lưu trữ mọi thứ tạm bợ nên nó còn được gọi là thư mục quốc dân; vì bất cứ ai, bất cứ chương trình hay tiến trình nào cũng có thể ghi dữ liệu vào đây. Mọi thứ trong "/tmp" sẽ bị xóa bỏ ngay khi Linux được khởi động lại; hoặc khi ta sử dụng dịch vụ "tmpwatch".

Lưu ý rằng tuy nó là nơi lưu trữ mọi thứ tạm bợ, nhưng có một khuyến cáo là bạn ko nên xóa bất cứ thứ j tồn tại trong thư mục này trừ khi bạn hiểu mình đang làm j, sẽ dẫn đến kết quả là j; vì 1 số tệp tin trong này đang phục vụ quá trình hoạt động của 1 chương trình/tiến trình quan trọng nào đó.

Do đặc tính cho phép ai cũng có thể ghi vào, nên đây cũng là 1 trong những thư mục cần phải để tâm rất nhiều nếu bạn muốn hệ thống của mình ko bị tin tặc khai thác.

**/usr - Thư mục USER chứa các tệp tin dành riêng cho Users.**

Thường thì đây là thư mục có kích thước lớn nhất trong hệ thống Linux. Dữ liệu chứa trong thư mục này là các tệp tin/chương trình đang được User sử dụng. Ví dụ như các tệp thực thi của User, các tệp tài liệu, thư viện ko phục vụ cho hệ thống; hoặc các chương trình như FTP, TELNET, ...

Ban đầu, vai trò của "/user" này chính là vai trò mà "/home/$USER" đang đảm nhận; tuy nhiên vai trò của nó đã bị thu hẹp lại. Và cho đến nay, thư mục này được coi là nơi lưu trữ "tài nguyên hệ thống dành cho người dùng", chứ ko phải "tài nguyên dành cho người dùng".

**/var - Thư mục VARIABLE chứa các tệp tin động.**

Đây là thư mục có thể được ghi với các chương trình/dịch vụ xuất phát từ thư mục "/use"; và ở chế độ READ ONLY với các tác vụ bình thường. Nơi đây lưu trữ rất nhiều thông tin có ích cho System Admin; tiêu biểu có thể kể đến cache, databases, library, log, ...

Vì lợi ích lớn lao mà nó đem lại, đây cũng là 1 trong những vị trí mà các tin tặc luôn thèm muốn khai thác.