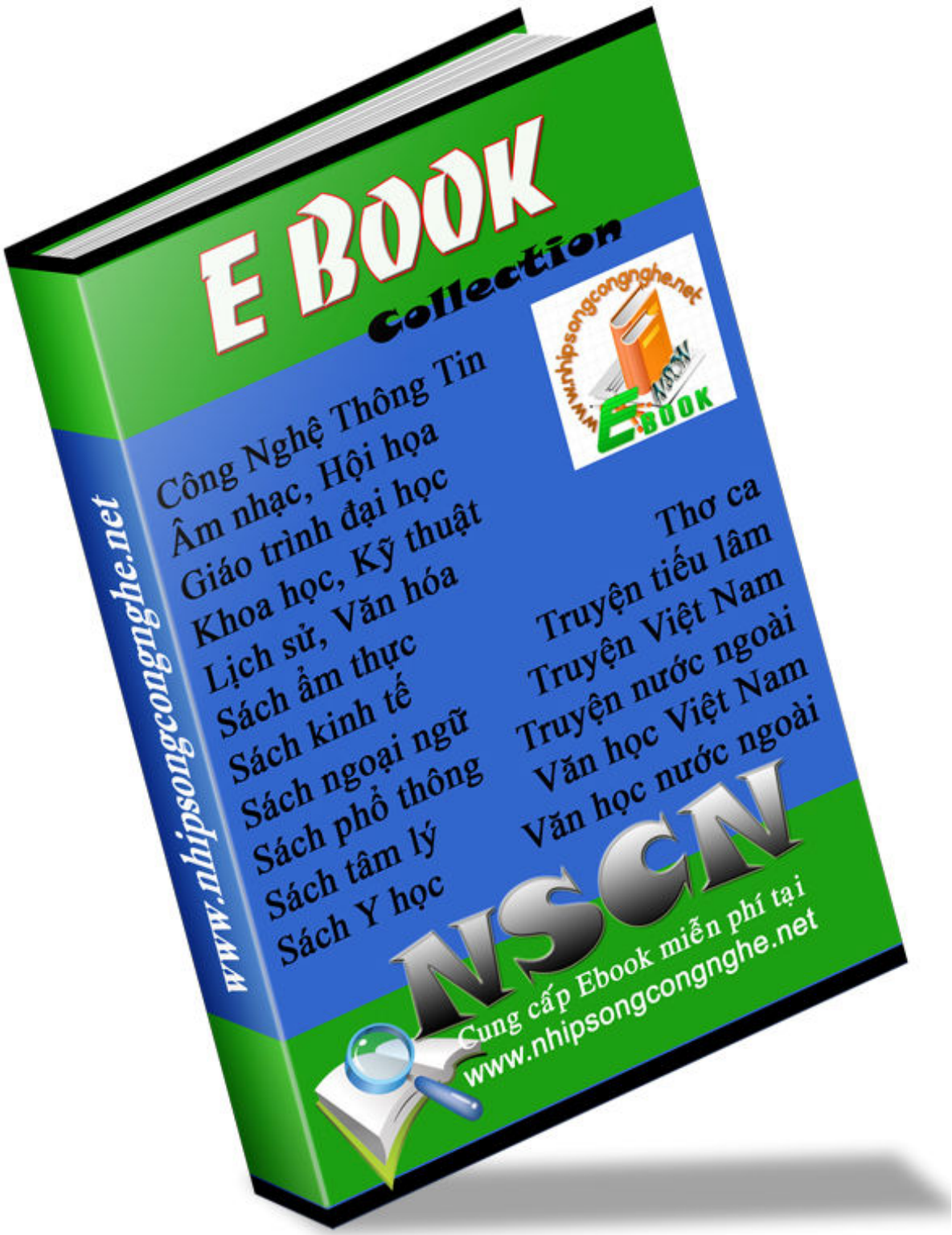
E BOOK
Collection
Công Nghệ Thông Tin
Âm nhạc, Hội họa
Giáo trình đại học
Khoa học, Kỹ thuật
Lịch sử, Văn hóa
Sách ẩm thực
Sách kinh tế
Sách ngoại ngữ
Sách phổ thông
Sách tâm lý
Sách Y học
Thơ ca
Truyện tiếu lâm
Truyện Việt Nam
Truyện nước ngoài
Văn học Việt Nam
Văn học nước ngoài
www.nhipsongcongnghe.net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

Security On Linux System

Power by: N.X.Bi O==(=========> ^($)^ Supporter Of VTF)
(E-mail: binhnx2000@yahoo.com | Home: http://www.vieteam.com/)

Mở đầu: Tôi là một Fan của Linux, một người yêu thích Security. Tôi rất thích Linux, đặc biệt là khả năng tuyệt vời của nó. Tôi viết tài liệu này chỉ với mục đích muốn chia sẻ với mọi người một chút hiểu biết ít ỏi của tôi về Security Linux...Không hề có bất cứ mục đích nào khác. Những gì tôi chia sẻ trong tài liệu này đều có nguồn gốc từ các: Magazine, Book, Site, Forum, List...về Linux Security trên thế giới. Những gì tôi cảm thấy hay và thực sự có ích, tôi đã thực hành thử và tìm cách ghi lại một cách ngắn gọn dễ hiểu nhất trong tài liệu này. Thiếu xót là điều không thể tránh khỏi, rất mong nhận được sự góp ý và chỉ bảo thẳng thắn từ phía các bạn. Đây chỉ là Version Demo của tài liệu. Nếu nhận được sự ủng hộ, đón nhận nhiệt tình cũng như sự góp ý và giúp đỡ thẳng thắn từ phía các bạn. Tôi sẽ tiếp tục hoàn thiện tài liệu này để phục vụ mọi người một cách tốt hơn.

Bạn có thể tham gia diễn đàn trao đổi, thảo luận về Unix/Linux với chúng tôi :

http://www.vieteam.com/vtf (Unix/Linux Section)

Lưu ý: Bài viết này chỉ mang tính chất học hỏi và trao đổi kinh nghiệm…Các bạn có thể tự do sử dụng nó, nhưng mong các bạn tôn trọng Copright một chút. Khi cần trích dẫn ở chỗ nào trong tài liệu. Vui lòng ghi rõ nguồn và tên người viết…Rất cảm ơn bạn đã quan tâm đến bài viết của tôi.

1) Về sự phân cấp, quyền hạn, sở hữu cho File

Sự phân cấp, quyền và sự sở hữu rõ ràng đơn giản đã tạo lên sức mạnh bảo mật của Unix/Linux. Vấn đề đầu tiên mà chúng ta cần kiểm tra có lẽ là sự phân cấp, quyền hạn, sở hữu các File trên hệ thống của bạn. Nếu không được cấu hình một cách chính xác điều này hết sức nguy hiểm. Cho lý do này bạn lên thường xuyên kiểm toán hệ thống File trên Server của bạn. Đặc biệt lên chú ý đến ID của root. Có một số chương trình cho phép người sử dụng trên hệ thống của bạn có thể tự do Set UID mà không cần root. Chắc tôi không cần nói, bạn cũng biết là phải làm gì với các chương trình loại này rồi chứ ? Bây giờ chúng ta tìm các File có sự phân cấp, quyền hạn không ổn định trên hệ thống của bạn và sau đó điều chỉnh lại giá trị an toàn cho chúng:

```
root@localhotst# find / -type f -perm +6000 -ls
59520 30 -rwsr-xr-x 1 root root 30560 Apr 15 1999 /usr/bin/chage
59560 16 -r-sr-sr-x 1 root lp 15816 Jan 6 2000 /usr/bin/lpq

root@localhotst# chmod -s /usr/bin/chage /usr/bin/lpq
root@localhotst# ls -l /usr/bin/lpq /usr/bin/chage
-rwxr-xr-x 1 root root 30560 Apr 15 1999 /usr/bin/chage
-r-xr-xr-x 1 root lp 15816 Jan 6 2000 /usr/bin/lpq
```

Các dòng lệnh trên tìm các File có UID root hay tương đương root. Tiếp đó gán thuộc tính chỉ cho phép root mới có quyền thực thi nó.

Chúng ta tiếp tục tìm những File cho phép ghi lại trên hệ thống của bạn. Điều gì sẽ xảy ra nếu kẻ tấn công có thể tự do thay đổi nội dung các File ?

root@localhost# find / -perm -2 ! -type l -ls

Trong các thao tác bình thường việc ghi, thay đổi nội dung File thường được thực hiện ở các thư mục như /**dev** và **/tmp**...Nếu bạn thấy ở các thư mục khác mà các File lại có thể tự do ghi lại được thì có lẽ là có vấn đề nảy sinh rồi đó.

Bạn cũng lên quan tâm đến các File không có chủ sở hữu (không thuộc bất cứ User hay Group nào). Tất nhiên là không ai sở hữu chúng thì kẻ tấn công rất có thể sẽ sở hữu chúng ;-(Để tìm các File không có chủ sở hữu bạn dùng lệnh:

root@localhost# find / -nouser -o -nogroup

Với việc sử dụng lệnh "**lsattr**" và "**chattr**" bạn có thể thay đổi đặc tính cho các File và thư mục dưới cấp độ cao cấp của một quản trị hệ thống như khả năng điều khiển quá trình xoá File, thay đổi File và với những tính năng khác mà lệnh "**chmod**" không thể thực hiện được.

Việc cấp phát quyền hạn sở hữu cho File theo một quy tắc thống nhất, trong suốt, không thay đổi...Tỏ ra có hiệu quả đặc biệt trong việc ngăn chặn quá trình xoá, thay đổi các tập tin Log của kẻ tấn công, hay việc cài đặt Trojan vào những File nhị phân Binnary trên hệ thống của bạn. Lệnh "**chattr**" được sử dụng để gán hay gỡ bỏ quyền hạn sở hữu cho File, thì lệnh "**lsattr**" được sử dụng để liệt kê chúng.

Các File Log cần phải được bảo vệ một cách hợp lý. Khi dữ liệu được ghi vào File Log một lần, nó sẽ không thể được phép chỉnh sửa hay thay đổi. Sở dỹ có nhu cầu này, bởi hiện tại có rất nhiều Script cho phép kẻ tấn công tấn công xoá bỏ, chỉnh sửa nội dung trên File Log. Để xiết chặt hơn an toàn cho File Log chúng ta cần sử dụng lệnh "**chattr**" và **"lsattr**" với một vài đối tượng:

root@localhost# chattr +i /bin/login
root@localhost# chattr +a /var/log/messages
root@localhost# lsattr /bin/login /var/log/messages
----i--- /bin/login
-----a-- /var/log/messages

Tóm lại! sau phần này bạn lên chú ý: Không bao giờ cho phép người sử dụng được phép chạy các chương trình Set UID, hay những chương trình khác có đặc quyền như root trên Home Directory của bạn. Luôn kiểm toán và quan tâm đến hệ thống File trên Server của bạn, đặc biệt là với những loại File có nguy cơ cao đã nêu ở trên.

- Bạn lên sử dụng tuỳ chọn **nouid** trong /**etc/fstab** để cho phép sự chỉnh sửa ghi lại ở các khu vực đã định với từng người sử dụng.
- Tính năng **noexec** và **nodev** cho các File trong Home Directory của người dùng để không cho phép họ tự động thực thi các chương trình hay tạo các thiết bị Block.

2) <u>Vô hiệu hoá các Service không sử dụng</u>

Để tránh tình trạng "đêm dài lắm mộng" bạn lên vô hiệu hoá và gỡ bỏ những chương trình, Service không dùng đến trên hệ thống của mình. Bạn có thể sử dụng các công cụ quản lý để

hiển thị danh sách những gói phần mềm nào đã được cài đặt để thực hiện việc này (Redhat Package Manager - Linux)

Về cơ bản! các Service được định nghĩa hoạt động bởi **inetd** (trên một số hệ thống Linux mới nó có thể là **xinetd**). Nội dung Service được định nghĩa hoạt động bởi **inetd** được chứa ở **/etc/inetd.conf** . Mỗi Service được định nghĩa đằng sau ký tự **"#"**...Bạn có thể vô hiệu hoá Service không sử dụng.

Thư mục **/etc/rc*.d** và **/etc/rc.d/rc*** là nơi chứa các Shell Script và các thông số để điều khiển sự thực hiện của Network và Service trong suốt thời gian nó hoạt động. Bạn có thể xoá bỏ hết những thứ liên quan đến những Service mà bạn không cần sử dụng. Đối với hệ thống Redhat, SuSE, Mandrake...bạn có thể sử dụng lệnh:

root@localhost#chkconfig --list
root@localhost#chkconfig --del <name>

Để hiển thị những Service nào đang hoạt động và xoá bỏ Service nào mà bạn muốn. Bạn muốn kiểm tra xem Service nào đó thực sự đã được gỡ bỏ khỏi hệ thống chưa ?

/bin/netstat -a -p --inet

Trên Redhat, SuSE, Mandrake...chương trình được sử dụng để quản lý các gói phần mềm là **/bin/rpm (Redhat Package Manager)**. Trên Debian là **/usr/bin/dpkg (Debian Package)**. Dưới đây là một số dòng lệnh cơ bản được dùng để quản lý các gói phần mềm. Dòng đầu sẽ là **rpm** và dòng thứ hai sẽ là **dpkg**:

Gỡ bỏ một gói phần mềm:

root@localhost# rpm -e <package-name>
root@localhost# dpkg -r <package-name>

Liệt kê danh sách những gói đã được cài đặt:

root@localhost# rpm -qvl <package-name.rpm>
root@localhost# dpkg -c <package-name.deb>

Liệt kê danh sách những gói đã được cài đặt với thông tin chi tiết cho mỗi gói:

root@localhost# rpm -qvia
root@localhost# dpkg -l

Liệt kê thông tin chính xác các File của gói đã được chỉ định:

root@localhost# rpm -qvpl <package-name.rpm>
root@localhost# dpkg -c <package-name.deb>

Hiển thị thông tin về một gói phần mềm:

root@localhost# rpm -qpi <package-name.rpm>
root@localhost# dpkg -l <package-name.deb>

Kiểm tra tính toàn vẹn cho một gói phần mềm:

root@localhost# rpm -Va
root@localhost# debsums -a

Cài đặt một gói phần mềm mới:

root@localhost# rpm -Uvh <package-name.rpm>
root@localhost# dpkg -i <package-name.deb>

3) Sự kiểm tra tính toàn vẹn của các gói phần mềm

Lệnh "**md5sum**" sự dụng thuật toán 128 bit để xác định chuỗi Finger Print của một gói phần mềm. Với mục đích đảm bảo sự toàn vẹn của các gói phần mềm từ nhà cung cấp đến người sử dụng. Nó có thể cho ta biết về sự thay đổi của các gói phần mềm trên hệ thống của bạn.

root@localhost# md5sum package-name
995d4f40cda13eacd2beaf35c1c4d5c2 package-name

Có lẽ bạn vẫn chưa hiểu được lợi ích thực sự của "**md5sum**" trong thế giới bảo mật. Tôi sẽ lấy một ví dụ đơn giản. Khi kẻ tấn công đã đột nhập được vào hệ thống của bạn, chúng sẽ cài đặt và sử dụng các Rootkit. Thực chất là các chương trình thông dụng của Admin như: netstat, ps, ls...đã được chỉnh sửa để cho ra thông tin sai che mắt bạn. Vậy làm thế nào để biết được điều này ?

Chẳng hạn như chuỗi MD5 mặc định của "**netstat**" khi cài đặt hệ thống SuSE Linux của tôi là "**995d4f40cda13eacd2beaf35c1c4d5c2**"

Bây giờ khi tôi chạy "**md5sum**" với "**netstat**" **:**

root@localhost# md5sum /usr/bin/netstat
995d4f40cda13eacd2beaf35c1c7d8c1 /usr/bin/netstat

Thông tin về chuỗi không khớp nhau, điều gì đã xảy ra vậy ? Câu trả lời này dành cho bạn.

4) Sử dụng Tripwire

Tripwire một chương trình theo dõi nhằm đảm bảo tính toàn vẹn của File bởi việc duy trì sự hoạt động của một cơ sở dữ liệu những File được cài đặt trên hệ thống...Cũng như sẽ cảnh báo khi chúng có sự thay đổi.

Khi cài đặt Tripwire sẽ đọc, thu thập thông tin về trạng thái các File trên hệ thống của bạn và ghi chúng vào một cơ sở dữ liệu. Sau này khi Tripwire chạy nó sẽ đối chiếu các FIle trên hệ thống của bạn với cơ sở dữ liệu chuẩn. Nếu có sự thay đổi nó sẽ thông báo cho bạn.

Có một File chính được sử dụng để cấu hình hoạt động tổng thể cho Tripwire. Thông thường với thông số mặc định nó cũng đã tỏ ra khá hiệu quả. Nếu như bạn không rành về Tripwire, bạn lên sử dụng thông số mặc định của nó. Dưới đây là một số dòng lệnh thông dụng

Tạo File nội quy từ một Text File

root@localhost#: /usr/TSS/bin/twadmin -m P policy.txt

Khởi tạo cơ sở dữ liệu theo File nội quy chính:

root@localhost#: /usr/TSS/bin/tripwire -init

Hiển thị cơ sở dữ liệu:

root@localhost#: /usr/TSS/bin/twprint -m d

Tạo thông báo kết quả theo ngày:

root@localhost#: /usr/TSS/bin/tripwire -m c -t 1 -M

Cập nhật cơ sở dữ liệu theo File nội quy và báo cáo hàng ngày:

**root@localhost#: /usr/TSS/bin/tripwire --update --polfile policy/tw.pol **
--twrfile report/<hostname>-<date>.twr

5) Sử dụng giao thức SSH

Nếu có thể tôi khuyên bạn lên cho Service "**Telnet**" nghỉ hưu và thay vào đó bằng Service "**SSH**". Mặc dù Telnet rất tuyệt nhưng nó lại không cung cấp khả năng mã hoá dữ liệu trên đường truyền, điều gì sẽ xảy ra khi có một Sniffer đặt ở đâu đó trên đường truyền.

Để cài đặt OpenSSH bạn cần Down gói *.rpm từ Site của hãng cung cấp phiển bản Linux mà bạn đang dùng về. Việc cài đặt từ gói *.rpm khá đơn giản, tôi không đề cập đến.

Lưu ý: Nhớ Down và cài thêm OpenSSL, bởi để hoạt động OpenSSH cần một số Lib của OpenSSL.

Chi tiết về việc sử dụng OpenSSH bạn có thể tham khảo bài viết "Open SSH" của tôi ở http://www.polarhome.com/~vicki

Về căn bản OpenSSH sử dụng những Public Key để đảm bảo sự an toàn. Public Key được cấp phát cho bất cứ hệ thống nào mà bạn muốn truyền thông an toàn:

host2$ ssh-keygen
Generating RSA keys: ...ooooooO....oooooooO
Key generation complete.
Enter file in which to save the key (/home/binhnx2000/.ssh/identity):
Created directory '/home/binhnx2000/.ssh'.
Enter passphrase (empty for no passphrase): <passphrase>
Enter same passphrase again: <passphrase>
Your identification has been saved in /home/binhnx2000/.ssh/identity.
Your public key has been saved in /home/binhnx2000/.ssh/identity.pub.
The key fingerprint is:
ac:42:11:c8:0d:b6:7e:b4:06:6a:a3:a7:e8:2c:b0:12 binhnx2000@host2

Tiếp đến Copy các Key để sử dụng:

host2$ mkdir -m 700 ~dave/.ssh
host2$ cp /mnt/floppy/identity.pub ~binhnx2000/.ssh/authorized_keys

Bây giờ từ hệ thống của bạn, nếu muốn Login vào hệ thống này chỉ việc phát lệnh:

root@localhost$ ssh host2
Enter passphrase for RSA key 'binhnx2000@localhost': <passphrase>

Last login: Sat Aug 15 17:13:01 2000 from localhost
No mail.
host2$

Ngoài khả năng cung cấp Shell Login an toàn, OpenSSH còn cung cấp cho bạn công cụ Copy và FTP một cách an toàn. Chẳng khi tôi muốn Copy file từ hệ thống của mình sang một hệ thống khác đã được chấp nhận:

root@localhost$ scp /tmp/file.tar.gz host2:/home/binhnx2000
Enter passphrase for RSA key 'binhnx2000@localhost:
file.tar.gz 100% |***| 98304 00:00**

Nếu có thể lên hướng dẫn và khuyến khích các User trên hệ thống của bạn sử dụng: OpenSSH thay cho Telnet và FTP.

6) Sử dụng TCP Wrappers

Trước khi Server FTP được chạy. Đầu tiên **tcpd** sẽ xác định những địa chỉ nguồn được cho phép, các kết nối sẽ được gửi đến Syslog để đối chiếu sau này. Nếu bạn muốn vô hiệu hoá tất cả các Service, bạn chỉ việc thêm dòng sau vào File **/etc/host.denny**

ALL:ALL

Để gửi E-mail đến nhà quản trị hệ thống và thông báo những lần kết nối bị thất bại, bạn thêm vào các dòng sau:

**ALL: ALL: /bin/mail **
-s "%s connection attempt from %c" admin@mydom.com

Nếu bạn muốn cho phép những địa chỉ tin cậy chạy những dịch vụ mà họ được phép, bạn hãy chỉnh sửa nội dung File /**etc/host.allow**

sshd: magneto.mydom.com, juggernaut.mydom.com
in.ftpd: 192.168.1.

Để đảm bảo an toàn bạn lên kiểm soát và điều khiển quá trình truy nhập một cách cẩn thận hơn. Sử dụng **tcpdchk** để kiểm tra sự truy nhập File, sử dụng Syslog để ghi lại những lần đăng nhập thất bại...Bạn lên điều khiển sự truy nhập cho hệ thống của mình theo nguyên tắc:

Sự truy cập chỉ được thực hiện khi Client/Deadmon có địa chỉ phù hợp với nội dung được cho phép trong /**etc/hosts.allow**

7) Sử dụng chế độ bảo mật mặc định của Kernel

Trong Kernel của một số hệ thống Linux mới hiện giờ có cấu hình sẵn một vài Rules chuẩn với mục đích cung cấp những thông số căn bản nhất để cấu hình cho hệ thống dành cho những Admin không có nhiều kinh nghiệm về bảo mật hệ thống. Các File và thông số đó thường được chứa ở **/proc/sys**. Về căn bản giao thức IPV4, bên trong **/proc/sys/net/ipv4** cung cấp các tính năng căn bản:

icmp_echo_ignore_all: Vô hiệu hoá tất cả các yêu phản hồi ICMP ECHO. Sử dụng tuỳ chọn này nếu như bạn không muốn hệ thống của mình trả lời các yêu cầu Ping.

icmp_echo_ignore_broadcasts: Vô hiệu hoá tất cả các yêu cầu phản hồi ICMP ECHO trên Broadcast và Multicast. Tuỳ chọn này được sử dụng để ngăn chặn nguy cơ hệ thống của bạn có thể bị lợi dụng khai thác cho những cuộc tấn công DDOS.

ip_forward: Cho phép hay không cho phép sự chuyển tiếp IP giữa các giao diện mạng trong hệ thống của bạn. Tuỳ chọn này được sử dụng khi bạn muốn Server của mình hoạt động như Router.

ip_masq_debug: Kích hoạt hay vô hiệu hoá quá trình gỡ lỗi cho IP Masquerading

tcp_syncookies: Tuỳ chọn này được sử dụng để bảo vệ hệ thống của bạn chống các cuộc tấn công sử dụng kỹ thuật ngập SYN đã từng gây kinh hoàng một thời trên Internet.

rp_filter: Chứng thực và xác định địa chỉ IP nguồn hợp lệ. Tuỳ chọn này được sử dụng để bảo vệ hệ thống của bạn chống lại các cuộc tấn công giả mạo địa chỉ IP "IP Spoof".

secure_redirects: Chỉ chấp nhận chuyển tiếp những thông điệp ICMP cho những Gateway tin tưởng trong danh sách.

log_martians: Ghi lại những Packet không được xử lý bởi Kernel.

accept_source_route: Xác định xem liệu có phải những Source Routed Packet được chấp nhận hay từ chối. Để an toàn bạn lên vô hiệu hoá tính năng này.

Trong hệ thống Redhat, ở **/etc/sysctl.conf** chứa thông tin về những thiết bị mặc định được xử lý ngay khi khởi động hệ thống, những thông số đó được đọc, điều khiển và thực thi bởi **/usr/bin/sysctl**.

Nếu bạn muốn vô hiệu hoá tính năng **"ip_foward"** đơn giản bạn chỉ việc sử dụng lệnh:

root@localhost# echo “0” > /proc/sys/net/ipv4/ip_forward

Tương tự để kích hoạt tính năng nào bạn chỉ việc thay giá trị "0" bằng "1"…

8) Bảo mật cho Apache Server

Các thông tin về sự hoạt động Apache Server ở **/etc/httpd/conf/httpd.conf**. Bây giờ chúng ta cùng xem xét nội dung của nó.

Listen 127.0.0.1:80

Sử dụng thông số trên để vô hiệu hoá toàn bộ sự truy cập vào hệ thống File không được cho phép bởi kẻ tấn công. Để vô hiệu mức tối thiểu các thông tin về Server có thể bị rỉ ra ngoài khi kẻ tấn công sử dụng kỹ thuật chộp Banner. Nó được dùng rất rộng rãi trên các hệ thống lớn.

<Directory />
Options None
AllowOverride None
Order deny,allow

Deny from all
</Directory>

Bây giờ đến phần giới hạn những địa chỉ IP được phép, không được phép. Bạn đọc file **/etc/httpd/conf/access.conf** :

<Directory /home/httpd/html>
 # Deny all accesses by default
Order deny,allow
 # Allow access to local machine
Allow from 127.0.0.1
 # Allow access to entire local network
Allow from 192.168.1.
 # Allow access to single remote host
Allow from 192.168.5.3
 # Deny from everyone else
Deny from all
</Directory>

Để an toàn bạn lên sử dụng mật khẩu chứng thực cho việc truy cập đến tập tin **/etc/httpd/conf/access.conf** (tập tin chứa đựng thông tin cho phép, không cho phép giới hạn các IP truy cập):

<Directory /home/httpd/html/protected>
Order Deny,Allow
Deny from All
Allow from 192.168.1.11
AuthName "Private Information"
AuthType Basic
AuthUserFile /etc/httpd/conf/private-users
AuthGroupFile /etc/httpd/conf/private-groups
require group <group-name>
</Directory>

TạoFile chứa thông tin về người được phép truy nhập vào khu vực trên bằng lệnh "**htpasswd**". Chẳng hạn như bạn muốn add vào danh sách những User được phép truy nhập vào khu vực trên:

root@localhost# htpasswd -cm /etc/httpd/conf/private-users binhnx2000
New password: <password>
Re-type new password: <password>
Adding password for user binhnx2000

Đừng quên Set quyền hạn hợp lý cho nó:

root@localhost# chmod 700 /etc/httpd/conf/private-users
root@localhost# chown root /etc/httpd/conf/private-users

Khởi động lại Apache Server và kiểm tra xem nó đã làm việc chưa ? Nếu bạn muốn Add thêm User vào file private-user...Bạn có thể sử dụng nguyên câu lệnh ở trên nhưng bỏ đi tuỳ chọn "**c**"

9) <u>Bảo mật cho DNS Server (BIND Server)</u>

Zone Transfer phải được cho phép bởi Master Name Server với mục đích cập nhật những thông tin trên Slave Server. Các yêu cầu phục vụ DNS thất bại có thể để lộ ra thông tin về những IP và Hostname của những người sử dụng không hợp pháp. Cho lý do này, bạn cần hạn chế những phản hồi trên Domain Public:

```
// Allow transfer only to our slave name server. Allow queries
// only by hosts in the 192.168.1.0 network.
zone “mydomain.com” {
type master;
file “master/db.mydomain.com”;
allow-transfer { 192.168.1.6; };
allow-query { 192.168.1.0/24; };
};
```

Vô hiệu hoá và ngăn chặn việc rò rỉ thông tin từ DNS Server:

```
// Disable the ability to determine the version of BIND running
zone “bind” chaos {
type master;
file “master/bind”;
allow-query { localhost; };
};
```

Để bổ xung thêm tính năng bảo mật cho DNS Server. File **./master/bind** chứa đựng thông tin:

```
$TTL 1d
@ CHAOS SOA localhost. root.localhost. (
1 ; serial
3H ; refresh
15M ; retry
1W ; expire
1D ) ; minimum
NS localhost.
```

Điều khiển và chỉ định rõ giao diện mạng phục vụ cho DNS Server. Việc hạn chế những giao diện mạng không cần thiết đó có thể giảm bớt nguy cơ tấn công vào DNS Server của bạn:

```
listen-on { 192.168.1.1; };
```

Sử dụng User Access Control List để điều khiển sự truy cập, sửa đổi cho những người sử dụng đáng đáng tin cậy trên phạm vị mạng:

```
acl “internal” {
{ 192.168.1.0/24; 192.168.2.11; };
};
```

Thiếp lập User của DNS Server như một User bình thường trên hệ thống của bạn. Không lên thiết lập cho nó nhiều đặc quyền...Tránh tính trạng nó sẽ có thể bị kẻ tấn công lợi dụng để thực thi các cuộc tấn công "Get Root"

```
root@localhost# useradd -M -r -d /var/named -s /bin/false named
root@localhost# groupadd -r named
```

10) <u>Bảo mật cho Syslog</u>

Syslog được ví như một Camera ghi lại gần như toàn bộ hoạt động. Nếu là một Admin chắc tôi không phải nêu lên chức năng và tầm quan trọng thực sự của Syslog.

Các thông số hoạt động của Syslog khá dễ hiểu và được cấu hình ở **/etc/syslog.conf**, dưới đây là một phần của File cấu hình:

```
# Monitor authentication attempts
auth.*;authpriv.* /var/log/authlog

# Monitor all kernel messages
kern.* /var/log/kernlog

# Monitor all warning and error messages
*.warn;*.err /var/log/syslog

# Send a copy to remote loghost. Configure syslogd init

# script to run with -r -s domain.com options on log
# server. Ensure a high level of security on the log
# server!
*.info @loghost
auth.*;authpriv.* @loghost
```

Có lẽ tôi sẽ không nêu lên toàn bộ những tính năng của Syslog, cái này bạn có thể tự tìm hiểu. Tôi chỉ nêu qua cách thức giúp bạn bảo vệ nội dung của Syslog. Tránh tình trạng nó bị chỉnh sửa bởi kẻ tấn công. Bạn cần hạn chế sự truy cập đến thư mục, File của Syslog đối với những User bình thường:

```
root@localhost# chmod 751 /var/log /etc/logrotate.d
root@localhost## chmod 640 /etc/syslog.conf /etc/logrotate.conf
root@localhost## chmod 640 /var/log/*log
```

10) <u>Một số kinh nghiệm</u>

Dưới đây là một số kinh nghiệm vụn vặt mà tôi thu lượm được sau khi lê la ở một vài Site/Forum chuyên về Security Unix/Linux. Tôi quyết định sẽ tổng hợp chúng và viết lại một cách dễ hiểu nhất.

Số lượng các Bug được phát hiện ngày càng nhiều. AutoRPM (Redhat) và app-get (Debian) có chức năng theo dõi và tự động Down xuống các bản Update, Patch của Package từ Server của nhà cung cấp. Tôi nghĩ tính năng này rất hữu ích cho hệ thống của bạn. Nếu có thể tôi khuyên bạn lên bỏ nhiều thời gian quan tâm đến hệ thống của mình hơn, bạn có thể đăng ký vào danh sách các Mail List chuyên về Bug, Security...Để chủ động hơn trong các tình huống.

Cài đặt một vài chương trình Scanner nhanh gọn như nmap chẳng hạn. Nó có thể Scan công khai, Port, Service, OS...ẩn trên 2 giao thức TCP/UDP...Rất tiện lợi.

Bạn cũng đừng quên có một cơ chế bảo vệ hợp lý cho LiLo (trình quản lý khởi động trên Linux). Thiết lập một cơ chế chứng thực quyền hạn hợp lý bằng cách thêm những dòng sau vào File /etc/lilo.conf:

/sbin/lilo:
image = /boot/vmlinuz-2.2.17
label = Linux
read-only
restricted
password = your-password

Kernel OpenWall tỏ ra rất hữu ích trong việc ngăn ngừa các cuộc tấn công tràn bộ đệm Buffer Overflow, cảnh báo, ngăn chặn và hạn chế những sự thay đổi được thực hiện bởi các User trên hệ thống của bạn. Để sử dụng Kernel OpenWall bạn phải Compli lại Kernel.

Đảm bảo rằng các thông tin về thời gian trên hệ thống của bạn phải hoàn toàn chính xác và hợp lý. Sẽ có rất nhiều rắc rối xảy ra khi thời gian trên hệ thống của bạn không chính xác. Nó sẽ gây rất nhiều khó khăn cho việc kiểm toán hệ thống sau này: Như phân tích nội dung, sự kiện của các Log File chẳng hạn. Để đảm bảo thời gian trên hệ thống của bạn luôn chính xác. Bạn chỉ việc Add thêm vào Crontab một lệnh với chức năng đối chiếu, so sánh thời gian trên hệ thống của bạn với một Host Time chuẩn:

0-59/30 * * * * root /usr/sbin/ntpdate -su time.timehost.com

Sử dụng Sudo để thiết lập quyền hạn thực hiện câu lệnh của User trên hệ thống của bạn. Có thể thiết lập quyền hạn cho một User bình thường thực hiện các lệnh như root. Tiếp đó bạn có thể dùng chính User này để điều khiển hệ, quản hệ thống của bạn mà không cần phải sử dụng đến Acc root. Mặc dù những lợi ích mà Sudo đem lại là rất lớn, nhưng nếu không được cấu hình một cách cẩn thận. Sudo có thể phá vỡ hoàn toàn khái niệm phân quyền, cấp vốn được coi là yếu tố tạo lên sức mạnh của Unix/Linux

Đừng quên chọn cho mình một Antivirus thích hợp. Nó có nhiệm vụ quét, cảnh báo, ngăn chặn, tiêu diệt các Virus khi chúng có ý định tấn công vào hệ thống của bạn. Mặc dù khả năng bị tấn công bởi Virus trên Linux là rất ít nhưng không phải không có. Lợi ích to lớn thực sự mà các Antivirus đem lại cho bạn có lẽ là việc nó sẽ phát hiện và ngăn chặn các Virus ngay từ Mail Server của bạn trước khi người sử dụng nhận được chúng. Hệ thống của bạn có thể sử dụng Unix/Linux, nhưng đâu phải tất cả các User trong hệ thống của bạn đều sử dụng Unix/Linux ? Nếu như không muốn nói rằng 90 % họ sử dụng Windows. Hay trường hợp các User ác ý muốn Up lên Server của bạn các Script, Tools cỡ như: PHP Bomb, CGI Telnet, DDOS Zombine...Tất cả chúng đều được liệt vào hàng Malicious Code và có thể dễ dàng bị phát hiện bởi Antivirus. Có rất nhiều Antivirus nhưng bản thân tôi thích sử dụng Kapersky Antivirus (KAVP) nhất.

Thật là thiếu xót nếu như không nhắc đến 2 "bảo kê" tin cậy của hầu hết các mạng máy tính. Đó là tường lửa (Firewall) và hệ thống dò xâm nhập (Network Instrution Detection). Trên môi trường Unix/Linux có rất nhiều Soft loại này. Nhưng có lẽ có 2 ông kẹ được sử dụng khá rộng rãi vì tính an toàn và sự phổ cập là: Ipchains/Iptables (Firewall) và Snort (Network Instrution Detection)... Để viết chi tiết và tỉ mỉ về Firewall và Network Instrution Detection thì có lẽ không biết sẽ phải tốn bao nhiêu trang…

Do khuôn khổ của bài viết, với mục đích điểm qua các chỉ mục về bảo mật cần lưu ý lên tôi không thể nào hướng dẫn cụ thể cách cài đặt, cấu hình, sử dụng các Tools/Soft đã nêu như: Sudo, Ipchains/Iptables, Snort, OpenSSH...Mong các bạn thông cảm.

P/S: Trước thời điểm khi bài viết này được hoàn thành...Tôi đã hoàn thành xong các bài viết chi tiết hướng dẫn sử dụng chúng. Tôi sẽ xem xét và Update trực tiếp nó vào tài liệu này trong thời gian sớm nhất.

Một sồ File về Security cần lưu ý trong Unix/Linux:

Vị Trí	Permission	Chức Năng
/var/log	**751**	Thực mục chứa tất cả Log File của hệ thống
/var/log/message	**644**	Những thông báo của hệ thống
/etc/crontab	**600**	Thư mục chứa các File liên quan đến Crontab
/etc/syslog.conf	**640**	File cấu hình của Syslog
/etc/logrotate.conf	**640**	File cầu hình điều khiển sự luân phiên của các File Log
/var/log/wtmp	**660**	Hiển thị thông tin về những ai đã Logged vào hệ thống
/var/log/lastlog	**640**	Ai đã Log vào hệ thống trước đây
/etc/ftpusers	**600**	Danh sách những User không được phép sử dụng FTP
/etc/passwd	**644**	Danh sách các User trên hệ thống
/etc/shadow	**600**	Danh sách các Password được mã hoá cho các User
/etc/pam.d	**750**	File cấu hình cho PAM
/etc/hosts.allow	**600**	File điều khiển sự cho phép các địa chỉ, Host…
/etc/hosts.denny	**600**	File điều khiển sự ngăn cản các địa chỉ, Host…
/etc/lilo.conf	**600**	File cấu hình trình quản lý khởi động trên Linux
/etc/securetty	**600**	TTY Interface mà root được phép đăng nhập
/etc/shutdown.allow	**400**	Danh sách những User được phép sử dụng tổ hợp phím: Ctrl + Alt
/etc/security	**700**	File thiết lập quy tắc an toàn chung cho hệ thống
/etc/rc.d/init.d	**750**	Thư mục chứa các File chương trình khởi động cùng hệ thống (Redhat)
/etc/init.d	**750**	Thư mục chứa các File chương trình khởi động cùng hệ thống (Debian)
/etc/sysconfig	**751**	Thư mục chứa các File cấu hình hệ thống và Network (Redhat)
/etc/inetd.conf	**600**	File định nghĩa các Service trên hệ thống
/etc/cron.allow	**400**	Danh sách các User được phép sử dụng Cron
/etc/cron.denny	**400**	Danh sách các User không được phép sử dụng Cron
/etc/ssh	**750**	Thông tin cấu hình SSH

11) Nguồn các Secuurity Tools được ưa chuộng trên Linux.

- **Ipchains/Iptables Firewall**
  http://www.iptbales.org/

- **Open SSH Secure Remote Access Tool**
  http://www.openssh.com/

- **Nmap Port Scanner**
  http://www.insecure.org/nmap

- **Sudo Root Access Control Tool**
http://www.sudo.ws/

- **Snort Network Intrusion Detection System**
http://www.snort.org/

- **Tripwire File Integrity Tool**
http://www.tripwiresecurity.com/

- **OpenWall Security Project**
http://www.openwall.com/

- **Network Time Protocol information**
http://www.ntp.org/

- **Kapersky AntiVirus Pro**
http://www.avp.ch

12) Lời kết

Security luôn là một lĩnh vực nóng bỏng, cuộc chiến dai dẳng giữa các Admin và Intruder dường như không bao giờ kết thúc. Bạn càng bỏ nhiều thời gian, có những chính sách bảo mật hợp lý cho hệ thống của mình…Thì khả năng bị tấn công càng thấp…Tuy nhiên tỷ lệ thấp không có nghĩa là không thể xảy ra. Không có một Firewall, Security Tools nào được coi là an toàn một cách tuyệt đối. Con người luôn luôn là yếu tố quyết định tất cả.

Như đã nói ở phần đầu, đây chỉ là Version Demo của tài liệu. Thiếu xót là điều không thể tránh khỏi, rất mong nhận được sự góp ý và chỉ bảo thẳng thắn từ phía các bạn.

Bạn có thể liên hệ với tôi:

My E-mail: binhnx2000@yahoo.com
My GPG Public Key: http://www.polarhome.com/~binhnx/contact/binhnx2000.asc
My Site & Group: http://www.vieteam.com/ **(VTF Forum)**
http://www.polarhome.com/~vicki **(Vicki Group H/C/A)**
http://binhnx.hypermart.net/ **(My Site)**