DÒ TÌM DẤU VẾT CHỈNH SỬA ĐƯỢC THỰC HIỆN TRÊN HỆ THỐNG LINUX

Hoạt động xâm phạm có thể đến từ cả hai phía: người dùng đã biết (nội bộ) và người dùng không xác định (từ bên ngoài). Kinh nghiệm cá nhân của tôi chỉ ra rằng những người không hạnh phúc hay không bằng lòng với cuộc sống thường gây nguy hiểm cho hệ thống của bạn, nhất là khi họ có lớp vỏ bọc truy cập hợp pháp. Một số người khá thông minh, loại bỏ file history (như: ~/.bash_history) hòng tránh bị phát hiện. Nhưng bạn vẫn hoàn toàn có thể giám sát tất cả lệnh thực thi của người dùng.

Lời khuyên ở đây là bạn nên kiểm soát hoạt động người dùng bằng cách sử dụng chương trình xử lý accounting. Chương trình xử lý accounting cho phép bạn xem xét mọi lệnh do người dùng thực thi với thời gian sử dụng CPU và bộ nhớ. Nhờ chương trình này, người quản trị sẽ luôn tìm ra được mọi lệnh thực thi ở bất kỳ thời gian nào.

Gói xử lý accounting gồm một số tiện ích giám sát các hoạt động chương trình như ac, lastcomm, accton và sa.

• Câu lệnh "ac" thể hiện lượng thời gian người dùng đăng nhập hệ thống.
• Câu lệnh "lastcomm" cho biết thông tin của các lệnh thực thi trước đó.
• Câu lệnh "accton" bật tắt chương trình xử lý accounting.
• Câu lệnh "sa" tóm tắt thông tin về các lệnh được thực thi trước đó.

Cài đặt gói psact hoặc acct

Dùng lệnh up2date nếu bạn đang dùng RHEL:

up2date psacct

Dùng lệnh yum nếu bạn đang dùng nhân Linux CentOS/Fedora:

yum install psacct

Dùng lệnh apt-get nếu bạn đang dùng Linux Ubuntu / Debian:

$ sudo apt-get install acct OR # apt-get install acct

Khởi động dịch vụ psacct/acct

Mặc định, dịch vụ này khởi động trên Ubuntu / Debian Linux bằng cách tạo ra file "/var/account/pacct". Nhưng ở hệ điều hành Red Hat /Fedora Core/Cent OS, bạn cần tự khởi động "psacct". Gõ hai lệnh sau để tạo file "/var/account/pacct" và khởi động các dịch vụ:

chkconfig psacct on
/etc/init.d/psacct start

Nếu bạn đang dùng Suse Linux, tên của dịch vụ là "acct". Gõ các lệnh sau:

chkconfig acct on
/etc/init.d/acct start

Bây giờ chúng ta hãy xem cách khai thác các tiện ích này để giám sát lệnh và thời gian người dùng.

Hiển thị số liệu thời gian kết nối của người dùng

Câu lệnh "ac" đưa ra số liệu thời gian kết nối theo giờ dựa trên các lệnh login/logout. Số lượng tổng cộng cũng được đưa ra. Nếu bạn gõ lệnh "ac" không có bất kỳ tham số nào, nó sẽ đưa ra lượng thời gian kết nối tổng:

$ ac

Xuất ra:

total 95.08

Hiển thị lượng tổng cộng theo từng ngày tốt hơn là chỉ có một kết quả tổng lớn vào thời điểm cuối cùng:

$ ac -d

Xuất ra:

Nov 1 total 8.65
Nov 2 total 5.70
Nov 3 total 13.43
Nov 4 total 6.24
Nov 5 total 10.70
Nov 6 total 6.70
Nov 7 total 10.30
.....
..
...
Nov 12 total 3.42
Nov 13 total 4.55
Today total 0.52

Hiển thị thời gian tổng cộng của từng người dùng để thêm vào giá trị "mọi thứ trong một" thông thường:

$ ac -p

Xuất ra:

vivek87.49
root7.63
total 95.11

Tìm ra thông tin các lệnh người dùng thực thi trước đó

Sử dụng câu lệnh lastcomm để đưa ra thông tin các lệnh người dùng thực thi trước đó. Bạn có thể tìm kiếm lệnh bằng cách sử dụng username (tên người dùng), tty name, hoặc bằng tên của chính câu lệnh.

Ví dụ hiển thị lệnh do người dùng "vivek" sử dụng:

$ lastcomm vivek

Xuất ra:

userhelper S X vivek pts/0 0.00 secs Mon Nov 13 23:58
userhelper S vivek pts/0 0.00 secs Mon Nov 13 23:45
rpmq vivek pts/0 0.01 secs Mon Nov 13 23:45
rpmq vivek pts/0 0.00 secs Mon Nov 13 23:45
rpmq vivek pts/0 0.01 secs Mon Nov 13 23:45
gcc vivek pts/0 0.00 secs Mon Nov 13 23:45
which vivek pts/0 0.00 secs Mon Nov 13 23:44
bashF vivek pts/0 0.00 secs Mon Nov 13 23:44
ls vivek pts/0 0.00 secs Mon Nov 13 23:43
rm vivek pts/0 0.00 secs Mon Nov 13 23:43
vi vivek pts/0 0.00 secs Mon Nov 13 23:43
ping S vivek pts/0 0.00 secs Mon Nov 13 23:42
ping S vivek pts/0 0.00 secs Mon Nov 13 23:42
ping S vivek pts/0 0.00 secs Mon Nov 13 23:42
cat vivek pts/0 0.00 secs Mon Nov 13 23:42
netstat vivek pts/0 0.07 secs Mon Nov 13 23:42
su S vivek pts/0 0.00 secs Mon Nov 13 23:38

Thông tin được đưa ra theo từng dòng. Ví dụ với dòng đầu tiên:

userhelper S X vivek pts/0 0.00 secs Mon Nov 13 23:58

Trong đó:

- userhelper: là tên lệnh chương trình

- S và X: là các cờ, ghi lại bởi kiểu định tuyến tài khoản hệ thống. Ý nghĩa của các cờ gồm:

S - câu lệnh thực thi bởi siêu người dùng.

F - câu lệnh thực thi sau khi rẽ nhánh nhưng sau đó không làm gì nữa.

D - câu lệnh kết thúc bằng một file lõi chung.

X - câu lệnh được kết thúc bằng dấu hiệu SIGTERM.

-vivek: tên người dùng chạy chương trình này.

- prts/0: tên mở rộng.

- 0.00 secx: thời gian thực thi chương trình.

Tìm kiếm các file log tính toán bằng tên lệnh:

$ lastcomm rm
$ lastcomm passwd

Xuất ra:

rm S root pts/0 0.00 secs Tue Nov 14 00:39
rm S root pts/0 0.00 secs Tue Nov 14 00:39
rm S root pts/0 0.00 secs Tue Nov 14 00:38
rm S root pts/0 0.00 secs Tue Nov 14 00:38
rm S root pts/0 0.00 secs Tue Nov 14 00:36
rm S root pts/0 0.00 secs Tue Nov 14 00:36
rm S root pts/0 0.00 secs Tue Nov 14 00:35
rm S root pts/0 0.00 secs Tue Nov 14 00:35
rm vivek pts/0 0.00 secs Tue Nov 14 00:30
rm vivek pts/1 0.00 secs Tue Nov 14 00:30

rm vivek pts/1 0.00 secs Tue Nov 14 00:29
rm vivek pts/1 0.00 secs Tue Nov 14 00:29

Tìm kiếm các file log tính toán bằng tên mở rộng pts/1

$ lastcomm pts/1

Tóm tắt thông tin tính toán

Dùng lệnh sa để đưa ra thông tin tóm tắt về các lệnh được thực thi trước đó. Hơn nữa các thông tin này còn ép dữ liệu để đưa vào một file tóm tắt có tên "savacct", gồm thời gian lệnh được gọi và tài nguyên hệ thống được dùng. Thông tin cũng có thể được tóm tắt theo từng người dùng cơ sở. "sa" sẽ ghi thông tin vào một file có tên "usracct".

sa

Xuất ra:

579 222.81re 0.16cp 7220k
40.36re0.12cp 31156k up2date
8 0.02re0.02cp 16976k rpmq
8 0.01re0.01cp 2148k netstat
11 0.04re0.00cp 8463k grep
18 100.71re0.00cp 11111k ***other*
8 0.00re0.00cp 14500k troff
5 12.32re0.00cp 10696k smtpd
2 8.46re0.00cp 13510kbash
8 9.52re0.00cp 1018k less

Ví dụ với dòng đầu tiên:

40.36re0.12cp 31156k up2date

Trong đó:

• 0.36re: "thời gian thực" (theo phút của đồng hồ treo tường).
• 0.12cp: tổng thời gian sử dụng CPU của hệ thống và người dùng (theo phút).
• 31156k: thời gian sử dụng CPU trung bình (theo đơn vị k).
• up2date: tên lệnh.

Hiển thị thông tin với từng người dùng:

sa -u

Xuất ra:

root0.00 cpu 595k mem accton
root0.00 cpu 12488k mem initlog
root0.00 cpu 12488k mem initlog
root0.00 cpu 12482k mem touch
root0.00 cpu 13226k mem psacct
root 0.00 cpu 595k mem consoletype
root 0.00 cpu 13192k mem psacct *
root 0.00 cpu 13226k mem psacct
root 0.00 cpu 12492k mem chkconfig
postfix 0.02 cpu 10696k mem smtpd
vivek 0.00 cpu 19328k mem userhelper
vivek 0.00 cpu 13018k mem id
vivek 0.00 cpu 13460k mem bash*
lighttpd 0.00 cpu 48240k mem php *

Hiển thị số lượng chương trình và số phút sử dụng CPU ở từng người dùng cơ bản:

sa -m

Xuất ra:

667231.96re0.17cp 7471k
root 54451.61re0.16cp 7174k
vivek 103 17.43re0.01cp 8228k
postfix 18 162.92re0.00cp7529k
lighttpd 20.00re 0.00cp 48536k

Tìm ra ai là người đang chiếm lĩnh CPU

Bằng cách nhìn vào thành phần thời gian "re, k, cp/cpu" (xem phần giải thích ở trên), bạn có thể tìm ra hoạt động đáng ngờ hoặc tên của người dùng, tên lệnh đang chiếm lĩnh toàn bộ CPU. Thời gian cũng như dung lượng sử dụng CPU (hoặc bộ nhớ) tăng lên tức là có vấn đề xuất hiện.

Hãy lưu ý các lệnh ở trên cũng như các gói ở nhiều hệ điều hành tựa UNIX khác (như Sun Solaris và *BSD chẳng hạn).

T.Thu