**Giám Sát Hoạt Động Và Kiểm Toán**

Với dịch vụ máy chủ, điều quan trọng với người quản trị là duy trì tình trạng hoạt động ổn định. Tuy nhiên một số ít khi máy chủ bị trục trặc và tạm dừng, người dùng cần phải được cảnh báo hay dự đoán trước để có biện pháp xử lý. Các công cụ giám sát và kiểm toán không chỉ giúp người quản trị được thông báo kịp thời về tình trạng chung của hệ thống mà còn có thông tin chính xác để khắc phục hay giúp cho các dịch vụ và hệ thống hoạt động được đảm bảo hơn.

**1. Giám Sát Hoạt Động**

Đối với hai hệ điều hành Windows và hệ điều hành Linux/Unix, giám sát và tinh chỉnh hiệu năng đều là quá trình theo dõi việc vận hành của hệ thống để xác lập tiêu chuẩn cơ sở, xác định và xử lý vấn đề tiềm năng. So sánh việc giám sát và hoạt động của hai hệ điều hành ta có bảng sau:

| **Hệ Điều Hành Windows** | **Hệ điều hành Linux/Unix** |
| --- | --- |
| Microsoft cung cấp một số công cụ cho người quản trị theo dõi hiệu năng và việc sử dụng tài nguyên hệ thống như giám sát hiệu năng (Performance Monitor), quản lý công việc (Task Manager), giám sát tài nguyên (Resource Monitor), và xem bản ghi sự kiện (Event Viewer). | Các file nhật ký cung cấp thông tin về tình trạng hoạt động chung của các dịch vụ và hệ thống máy chủ và được lưu trong thư mục “var/log/” như:  - syslog: nhật ký về hoạt động chung của hệ thống  - mail: nhật ký về hệ thống thư điện tử |
| Người quản trị có thể xác định được tình trạng chung của hệ thống thông qua chương trình quản lý nhiệm vụ theo dõi thông tin. Về chức năng, chương trình cung cấp các thông tin như sau:  - Mục ứng dụng: cho biết danh sách ứng dụng đang chạy và trạng thái tương ứng.  - Tiến trình: các tiến trình của người dùng đang chạy trong hệ thống.  - Dịch vụ : các dịch vụ Windows đang chạy.  - Hiệu năng : theo dõi việc sử dụng các tài nguyên phần cứng như bộ xử lý, bộ nhớ, ổ đĩa.  - Kết nối mạng: giám sát các giao tiếp mạng được cài đặt và việc sử dụng chung.  - Người dùng: thông tin về người dùng đăng nhập vào hệ thống.  Có hai kiểu file nhật ký sự kiện là:  - Nhật ký Windows: lưu lại các sự kiện hệ thống nói chung liên quan đến ứng dụng, an ninh, cài đặt và các thành phần hệ thống;  - Nhật ký dịch vụ và ứng dụng: lưu lại việc sử dụng của ứng dụng hay dịch vụ cụ thể.  Với nhật ký sự kiện, người quản trị sử dụng chương trình “Event Viewer”, mỗi sự kiện chương trình sẽ đánh dấu tương ứng như sau:  - Thông tin: Thông báo thông thường về thao tác được thực hiện thành công.  - Cảnh báo: Mô tả sự kiện không nghiêm trọng nhưng cần chú ý để tránh các vấn đề xa hơn.  - Lỗi: Cho biết một lối hay vấn đề không nghiêm trọng xảy ra.  - Nghiêm trọng: Cho thấy một lỗi nghiêm trọng hay vấn đề rất đáng kể xảy ra.  - Kiểm toán thành công: Mô tả sự kiện kiểm toán an ninh thành công như yêu cầu.  - Kiểm toán thất bại: Mô tả sự kiện kiểm toán an ninh không thành công như yêu cầu. | Linux/Unix cung cấp một số công cụ cho phép theo dõi tình trạng sử dụng các tài nguyên hệ thống của các chương trình và dịch vụ qua các câu lệnh:  - ps: liệt kê các chương trình đang hoạt động và số lượng tài nguyên hệ thống chúng sử dụng  - df: cho biết dung lượng lưu trữ đã được sử dụng trong hệ thống  - netstat: cho biết thông tin về các cổng và các giao thức mạng đang hoạt động của hệ thống  Sysstat là công cụ giám sát hiệu năng tốt cho môi trường Linux. Công cụ này cho phép ghi lại các thống kê tình trạng hệ thống tiêu biểu như:  - Tải của bộ xử lý  - Thao tác vào/ra và tốc độ truyền theo từng chương trình, ổ đĩa, kết nối mạng, …  - Sử dụng bộ nhớ và bộ nhớ hoán đổi, Bộ nhớ ảo, lỗi trang  - Sử dụng mạng, …  Để cài đặt công cụ này, người quản trị cần sử dụng câu lệnh *sudo apt-get install sysstat* và *sudo dpkg-reconfigure sysstat* để cấu hình. Để lấy thông tin về các thao tác vào/ra, người quản trị có thể sử dụng câu lệnh *sar –b*. |

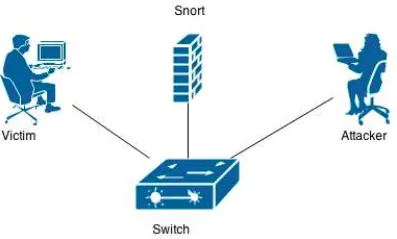
1. **Kiểm toán**

Việc kiểm toán cho phép người quản trị theo dõi cả truy nhập thực tế và cố thử truy nhập hay các sửa đổi các đối tượng và chính sách của hệ thống. Các đối tượng có thể là thư mục và file cũng như các đối tượng an ninh của hệ thống. Mục tiêu cơ bản của việc kiểm toán là đảm bảo hệ thống được vận hành một cách an toàn, giảm thiểu các rủi ro, và ứng phó một cách hữu hiệu khi có trục trặc xảy ra. Cụ thể:

| **Hệ Điều Hành Windows** | **Hệ điều hành Linux/Unix** |
| --- | --- |
| Cách chính sách kiểm toán hỗ trợ việc đảm bảo an toàn cho hệ thống, theo dõi các sửa đổi các dữ liệu nhạy cảm hay các tài khoản cần để ý:  - Đăng nhập: theo dõi việc xác thực thông tin đăng nhập  - Quản lý tài khoản: theo dõi các thao tác thay đổi tài khoản như người dùng, máy tính…  - Theo dõi chi tiết: theo dõi việc chạy chương trình, các lời gọi hàm từ xa…  - Truy nhập thư mục động: theo dõi việc truy nhập hay các chức năng của thư mục động.  - Truy nhập đối tượng: theo dõi việc truy nhập các file, thư mục hay ứng dụng. | Việc kiểm toán hệ thống cho phép người quản trị thực hiện các nhiệm vụ tiêu biểu như sau:  - Theo dõi truy nhập file và thay đổi  - Giám sát các lời gọi và chức năng hệ thống  - Phát hiện các bất thường như các tiến trình bị hỏng/ngưng.  - Các câu lệnh thực hiện bởi người dùng |
| Người dùng có thể sử dụng chương trình Group Policy Management Editor để giúp dễ dàng hiểu, triển khai, quản lý, khắc phục sự cố triển khai Group Policy, cũng như tự động hóa các hoạt động Group Policy thông qua tập lệnh. | Người quản trị có thể thao tác kiểm toán bằng bộ công cụ auditd được cài đặt qua câu lệnh *udo apt-get install auditd.*  Một số tình huống cụ thể:  - Giám sát các thay đổi trong việc truy nhập file và thư mục.  + File: sử dụng câu lệnh: *sudo auditctl -w/etc/passwd -p rwxa*  + Thư mục: sử dụng câu lệnh *sudo auditctl -w /var/www/html*  ***-*** Giám sát các tiến trình: sử dung câu lệnh:  *sudo autrace –r /bin/ls*  - Báo cáo giám sát: sử dụng tiện ích *aureport* |

1. **Xây dựng kịch bản và phát hiện tấn công vào máy chủ**

3.1 Mô hình demo:

Mô hình hệ thống trong mạng LAN gồm 3 thành phần chính:

- Victim: đại diện cho người dùng hoặc máy chủ trong hệ thống mạng LAN

- Snort: thiết bị phát hiện xâm nhập chạy Snort

- Attacker: đối tượng tấn công mạng LAN, có thể là hacker, virus, trojan, worm, …

- Switch: để snort có thể lắng nghe được các cuộc tấn công, switch hoặc thiết bị chuyển mạch phải cài đặt hỗ trợ forward các gói tin trong mạng về Snort Sensor.

3.2 Kịch bản thử nghiệm phát hiện xâm nhập bằng Snort IDS:

Bước 1: Cài đặt và cấu hình Snort IDS

Snort được cài đặt trên máy ảo Ubuntu, đồng thời chạy bổ sung các công cụ cho phép theo dõi và giám sát các cảnh báo từ snort gồm: Sguil, Snortby, Squert

Bước 2: Thêm rule để thử nghiệm, ở đây ta chỉ thêm một rule đơn giản để đánh giá khả năng phát hiện của Snort:

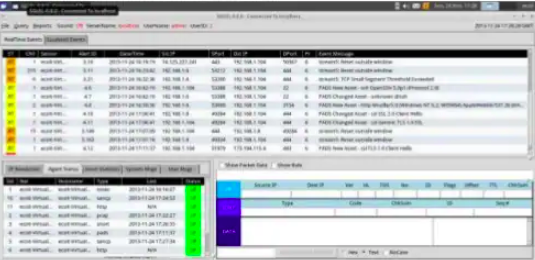
- Sửa file: */etc/nsm/rules/local.rule và thêm vào rule sau:*

*dert iamp 192.168.1.6 any → any any (msg: “ping of dead”; sid: 100009;)*

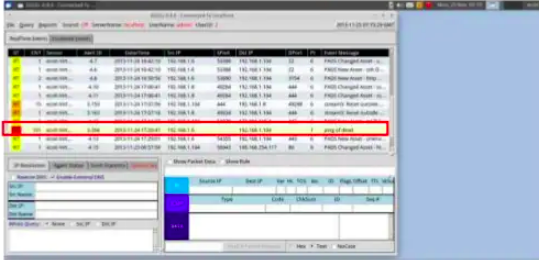
- Khởi động lại Snort bằng lệnh: “/etc/init.d/nsm restart”

Bước 3: Từ máy tính attacker thực hiện lệnh ping đến máy victim: “ping 192.168.1 -t”

Buớc 4: Theo dõi cảnh báo của Snort từ giao diện Sguil



*Màn hình theo dõi realtime dùng Sguil*



Cảnh báo có tấn công “Ping of dead”

TÀI LIỆU THAM KHẢO

[1] Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix,

Học viện Công Nghệ Bưu Chính Viễn Thông, 2016.

[2] Tom Carpenter, Microsoft

Windows Server Operating System Essentials, Sybex, 2011.

[3] Wale Soyinka, Linux

Administration A Beginners Guide, McGraw-Hill Osborne Media, 2012.