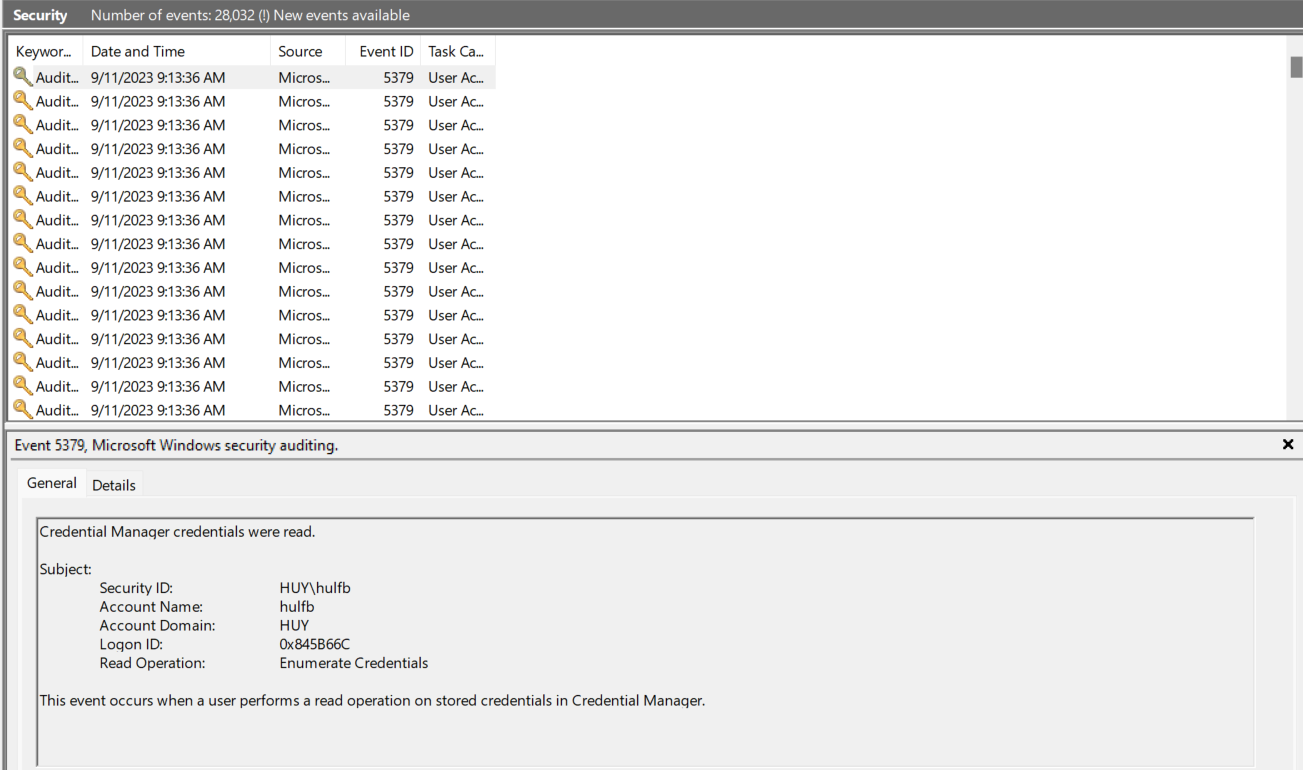
**1.Audit log ở trên 2 OS Windows và Linux.**

- Audit log trên OS Windows

Audit log ở trên OS Window là Security log ở trên Event Viewer được cho phép ghi lại các sự kiện của một hệ thống hoặc hành động của người dùng nhất định dựa trên các tiêu chí do audit policy đưa ra.Nó cung cấp các hành động khác nhau chẳng hạn như các lần login fail, folder access và những hành vi một người dùng cụ thể đã làm trên hệ thống xác thực.

(audit policy là những policy cho phép ta giám sát hoạt động của hệ thống , cũng như tương tác của người dùng, ghi nhận các hoạt động đó một cách có chọn lọc vào security log).



Và trong security log nó sẽ có những dạng Audit sau :

Audit account logon events: Kiểm tra từng trường hợp người dùng đăng nhập hoặc đăng xuất từ ​​một máy tính khác mà máy tính này được sử dụng để xác thực tài khoản.

Audit account management: Kiểm tra từng sự kiện account management trên máy tính. Chẳng hạn như password changes, user account và group modifications.

Audit directory service access: Kiểm tra sự kiện người dùng truy cập một đối tượng Active Directory có trong danh sách kiểm soát truy cập hệ thống (SACL).

Audit logon events: Kiểm tra từng trường hợp người dùng đăng nhập hoặc đăng xuất khỏi máy tính. Lưu ý rằng danh mục này khác với danh mục “S Audit account login events”. Nó theo dõi sự kiện đăng nhập vào một máy chủ cụ thể.

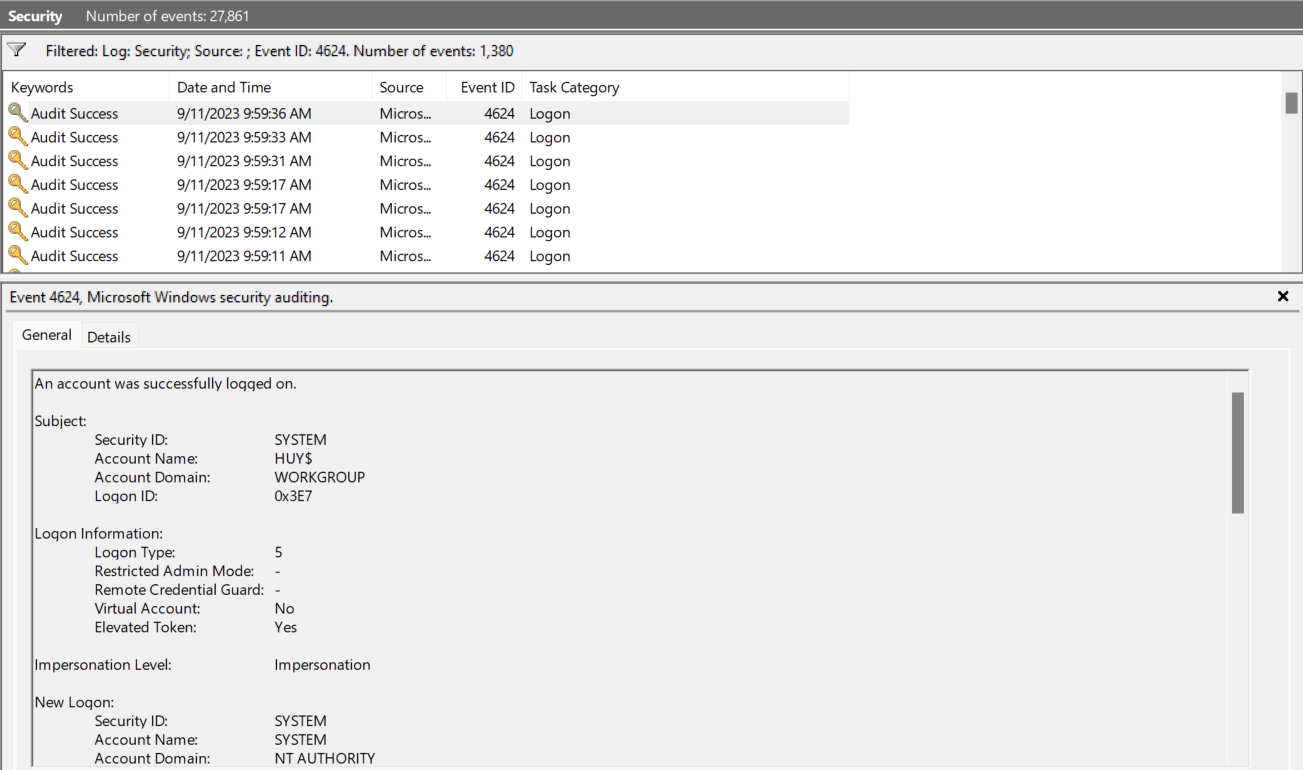
Audit object access: Kiểm tra sự kiện người dùng truy cập một đối tượng đã chỉ định danh sách kiểm soát truy cập hệ thống (SACL) của riêng nó. Ví dụ về các đối tượng là tệp, thư mục, registry, …

Ví dụ như :

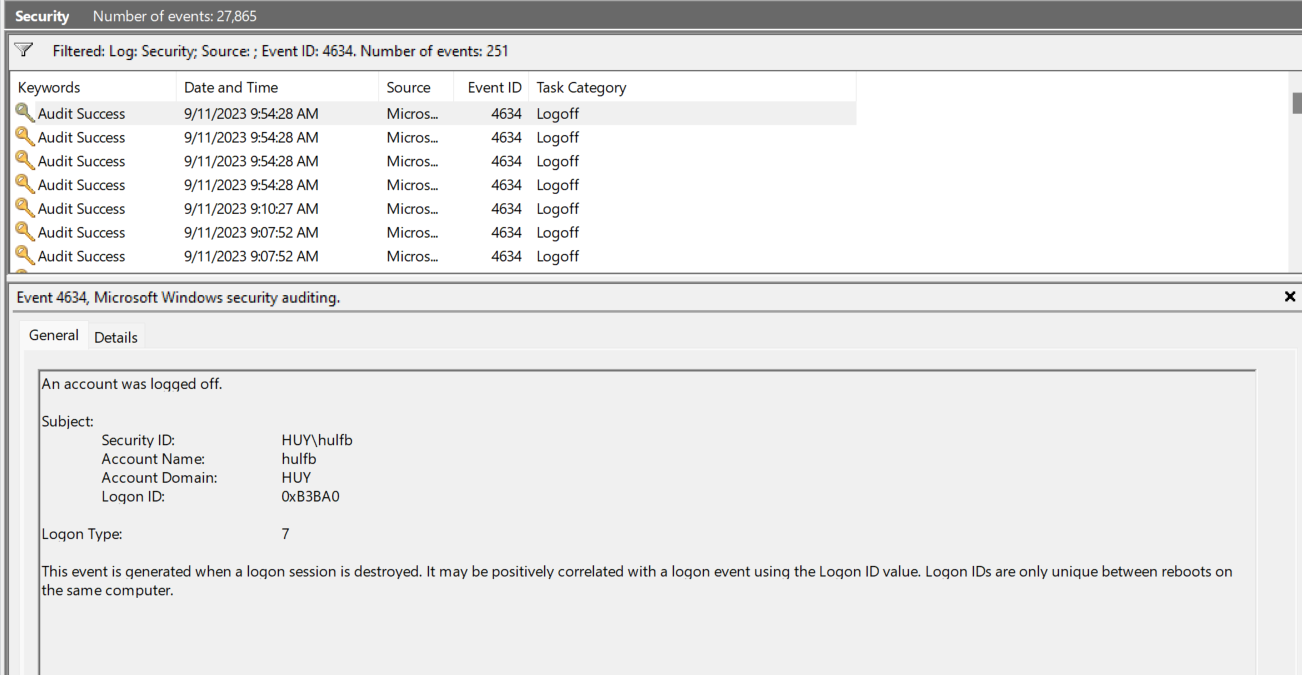
Khi phân tích các event logs , nó cho người điều tra về những chi tiết về các hoạt động của user nào đó. Việc biết tại thời điểm nào tài khoản người dùng đăng nhập vào hệ thống hay đăng xuất cung cấp bằng chứng vô cùng hữu ích và nó cũng là một trong những việc cần xác định ban đầu khi bạn gặp một sự cố nào đó. Nó có thể cung cấp bằng chứng  xem một sự cố xảy ra khi tài khoản nào đang được sử dụng hay tài khoản nào đang Remote logons cũng được ghi lại và cả thông tin về người dùng trái phép truy cập mạng và đang cố gắng xác thực.

Điển hình nhất là 2 dạng event id liên quan đền hành vi đăng nhập

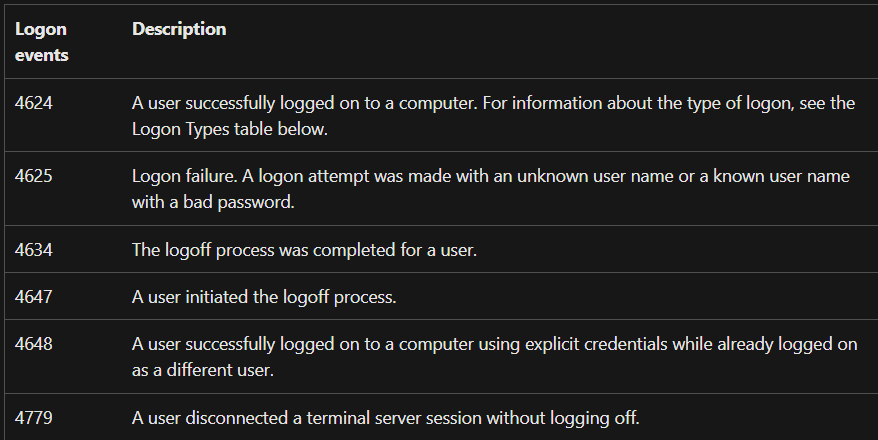
4624 - logon



4634 – logoff

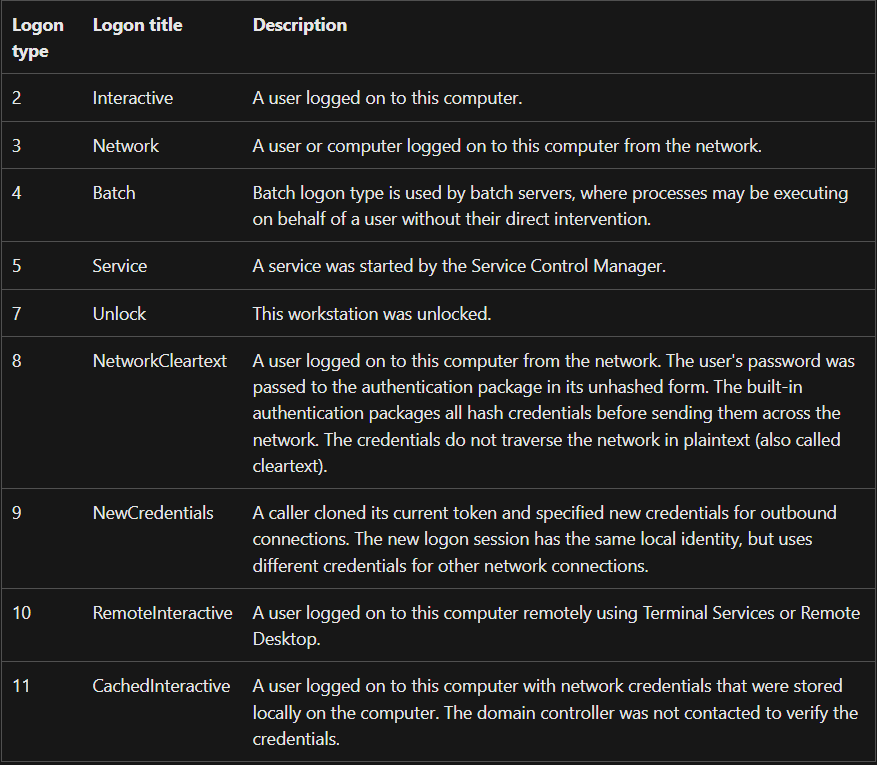


Và có nhiều các event id khác nữa

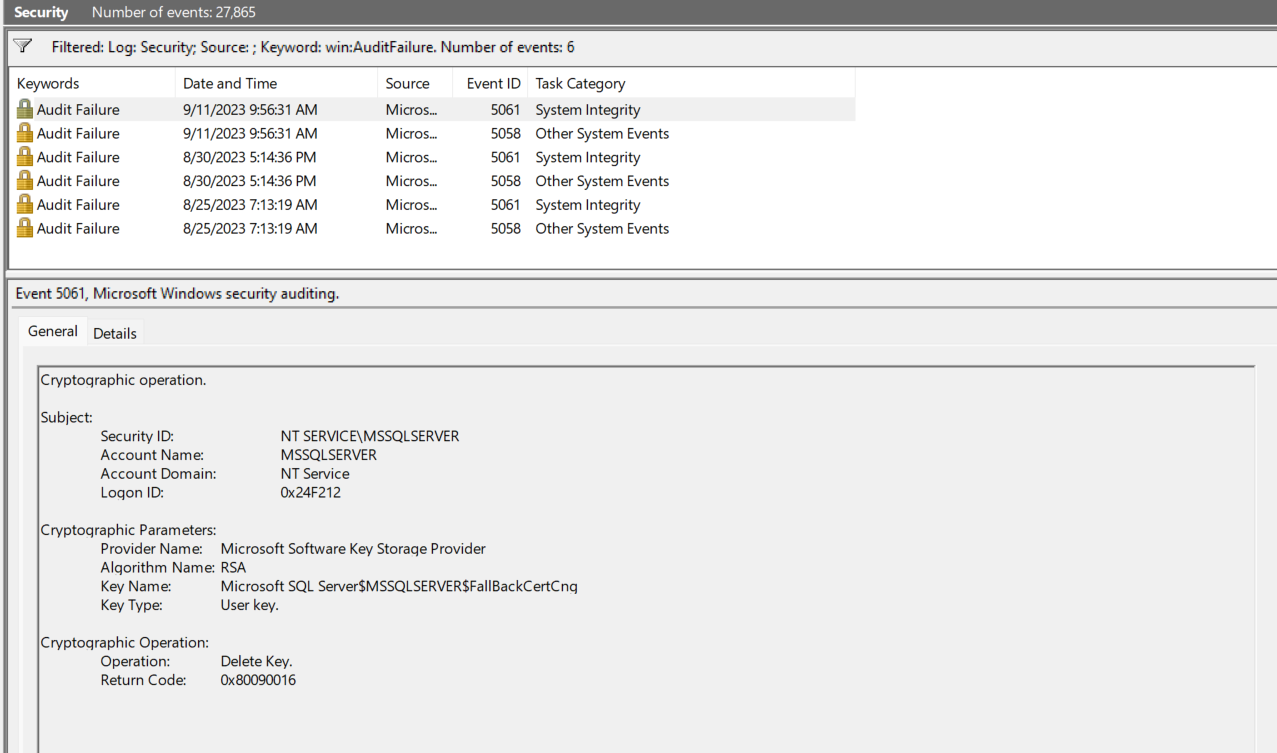


Và khi event 4624 được log , nó sẽ liệt kê những kiểu đăng nhập

Ví dụ người dung đăng nhập vào máy tính ,….

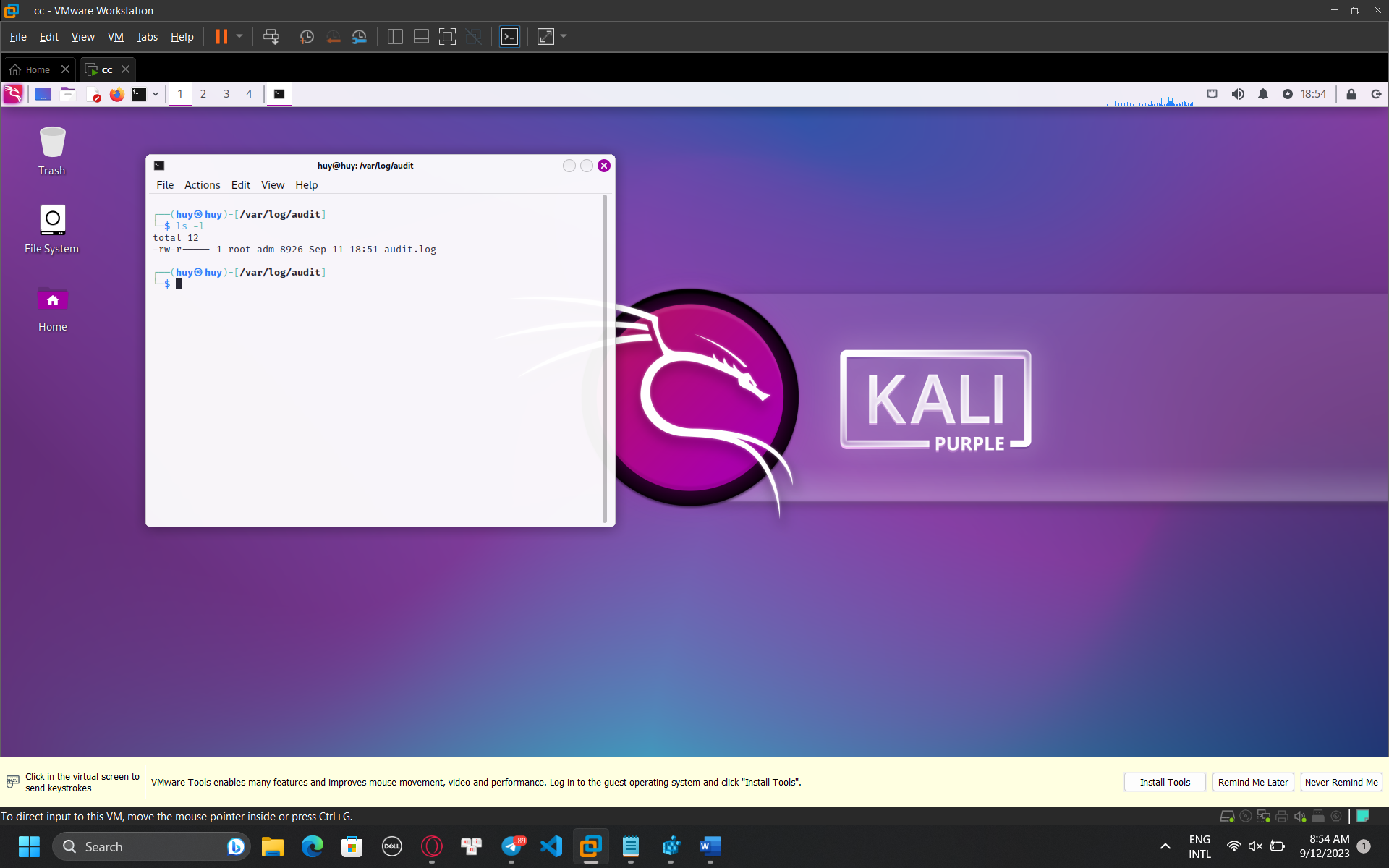


Không những thế đối với những người giám sát an toàn thông tin chúng ta cần phải chú ý tới Audit Failure khi mà các Lỗi kiểm tra thường được tạo ra khi yêu cầu đăng nhập không thành công, mặc dù chúng cũng có thể được tạo ra do các thay đổi đối với tài khoản, đối tượng, chính sách, đặc quyền và các sự kiện hệ thống khác. Chính sách kiểm tra xác định các loại sự kiện được ghi lại trong security log.



* Audit log trên OS Linux

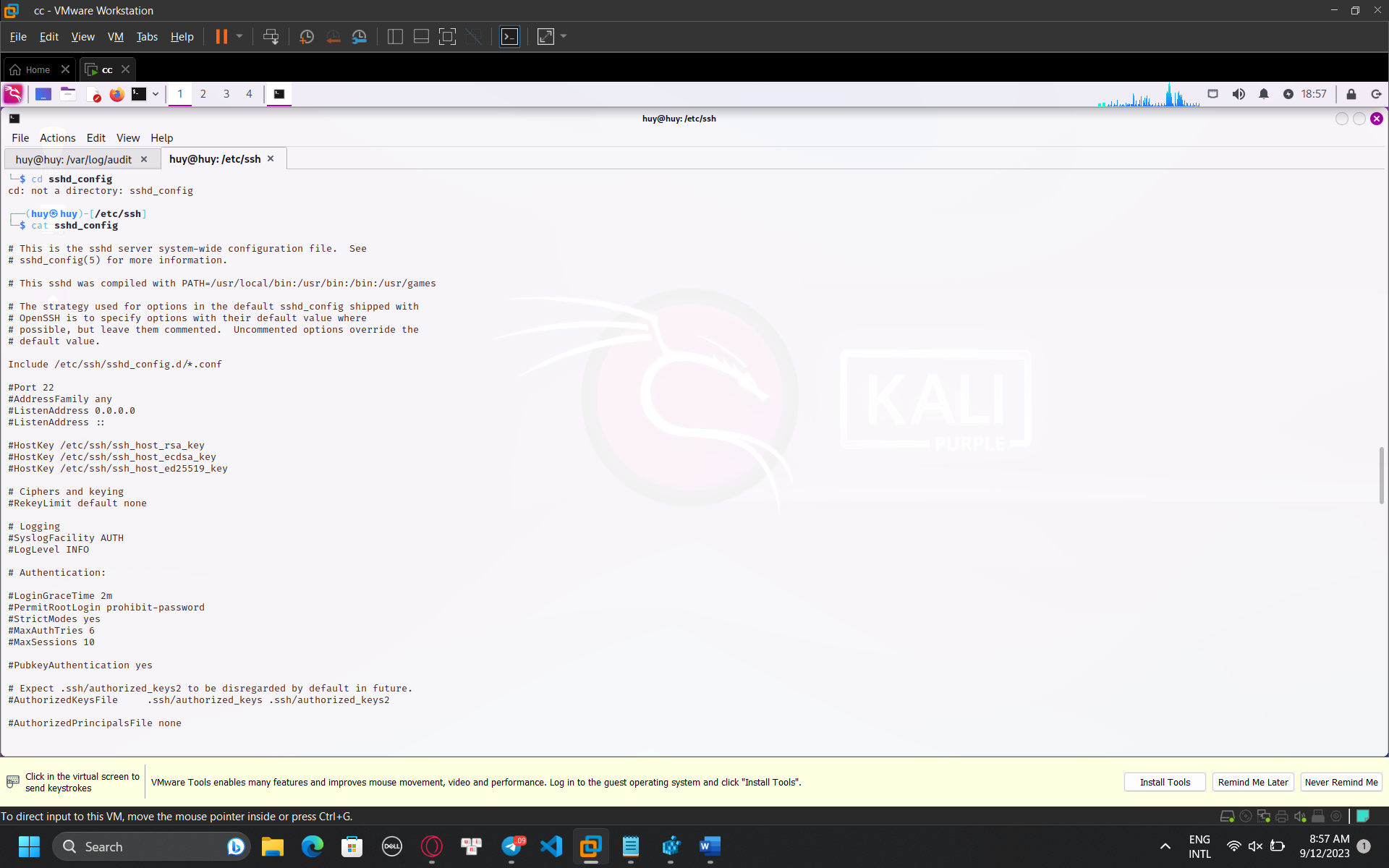
Audit system được kiểm tra lưu trữ trên các log entries ở trong /var/log/audit/audit.log file và các tệp audit.log và khi log rotation được enable thì file audit.log sẽ được lưu trữ ở trong cùng một thư mục



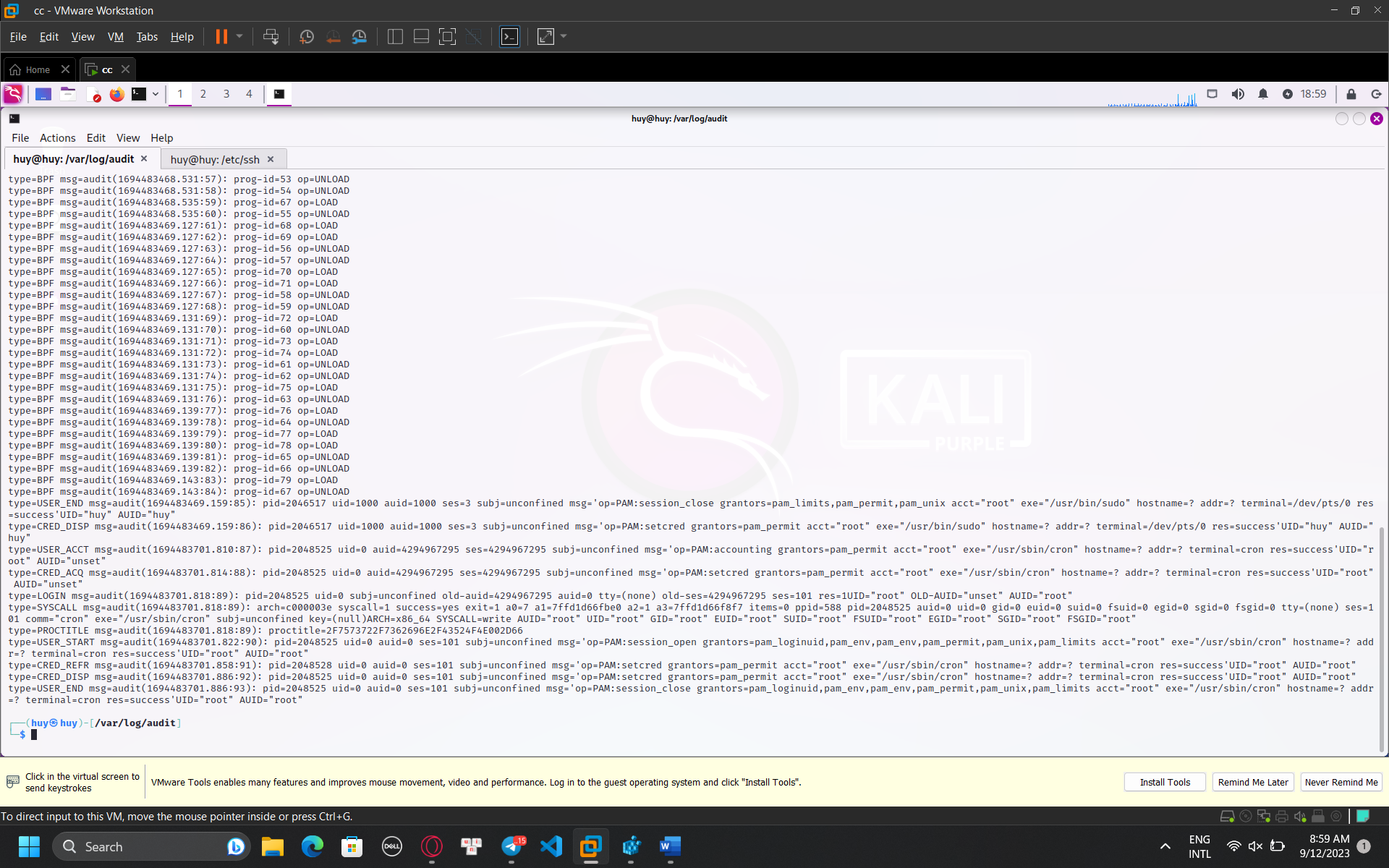
Audit rule log sẽ ghi lại những lần truy cập để đọc hoặc sửa đổi tệp ở file

/etc/ssh/sshd\_config

Và khi auditd daemon nó chạy chúng ta có thể sử dụng command để tạo ra một event mới trong audit log file



Và event trong audit.log sẽ trông như thế này



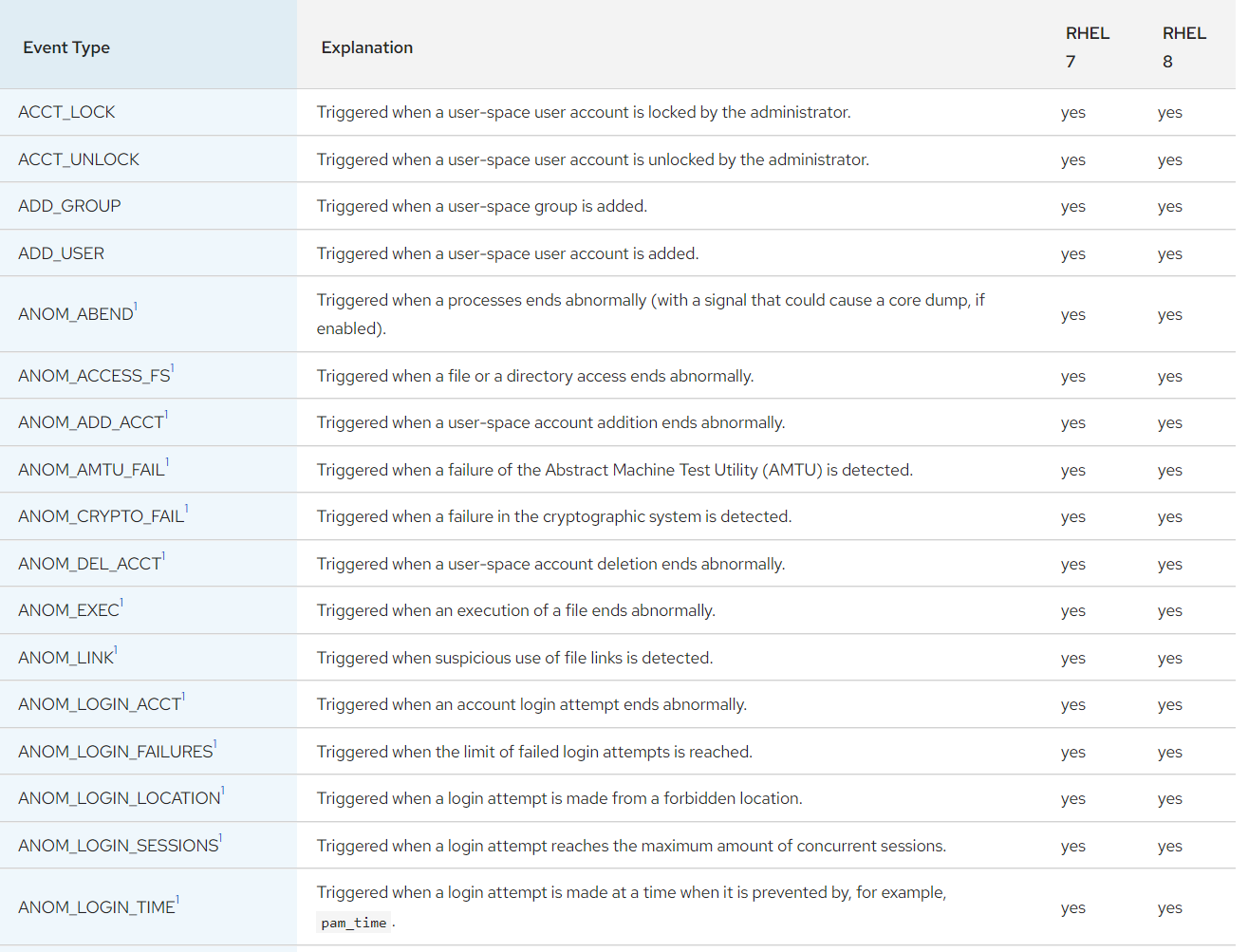
Tất cả các event trên bao gồm rất nhiều records, nó những mốc thời gian nói chung và số sê-ri.

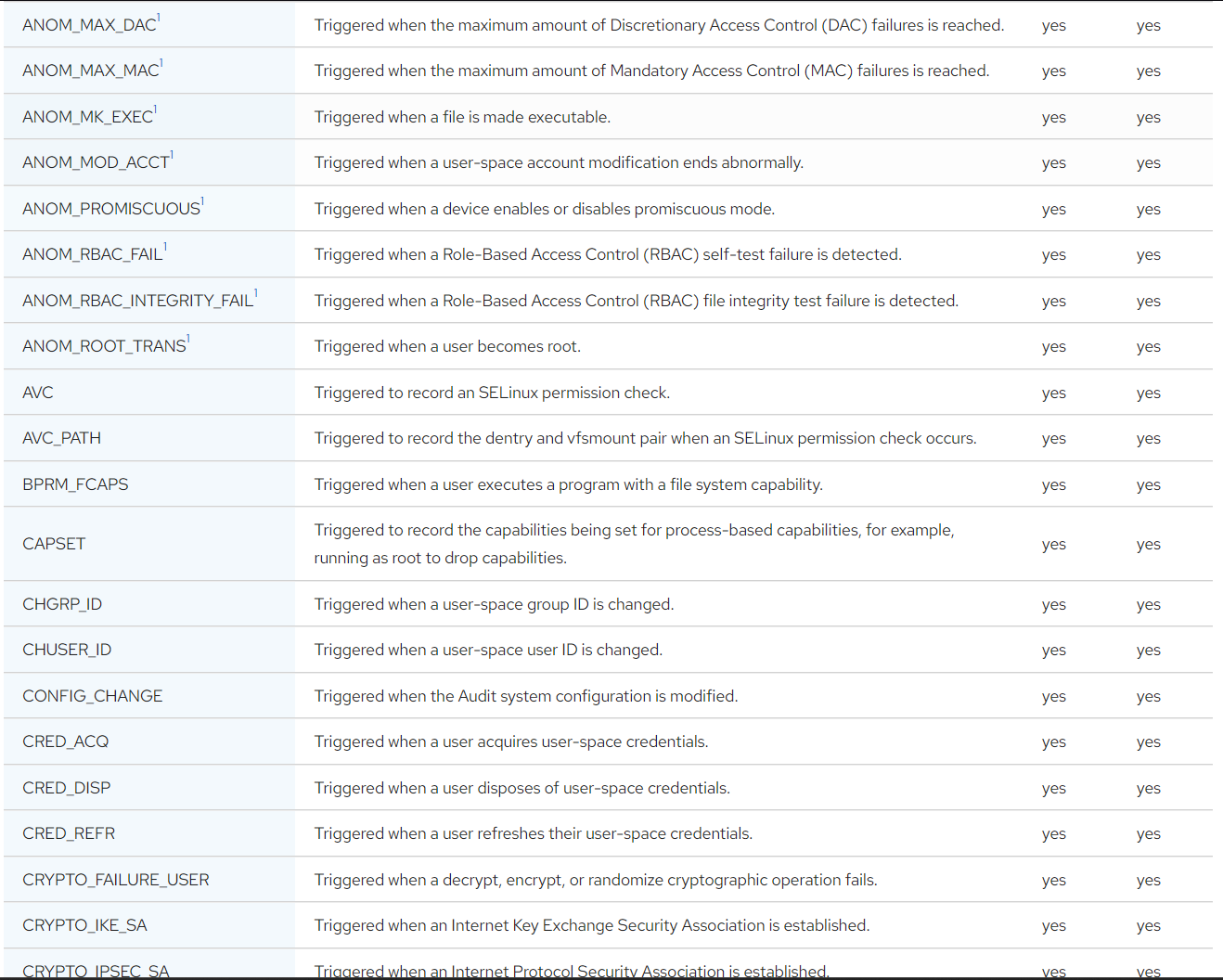
Record luôn được bắt đầu bằng từ khóa type=.

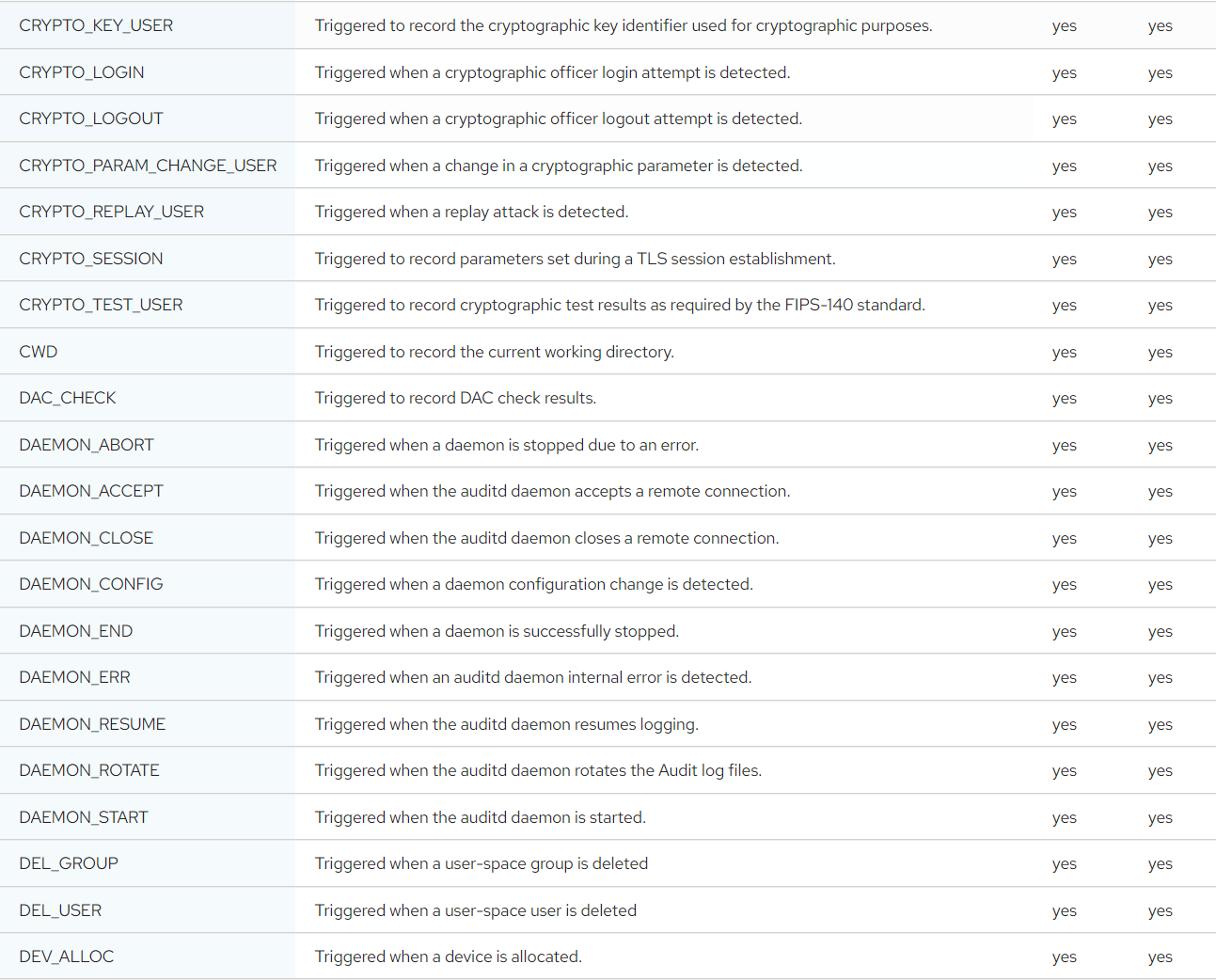
Mỗi bản record đều có một cặp name=value được phân tách bằng những khoảng trắng hoặc dấu phẩy

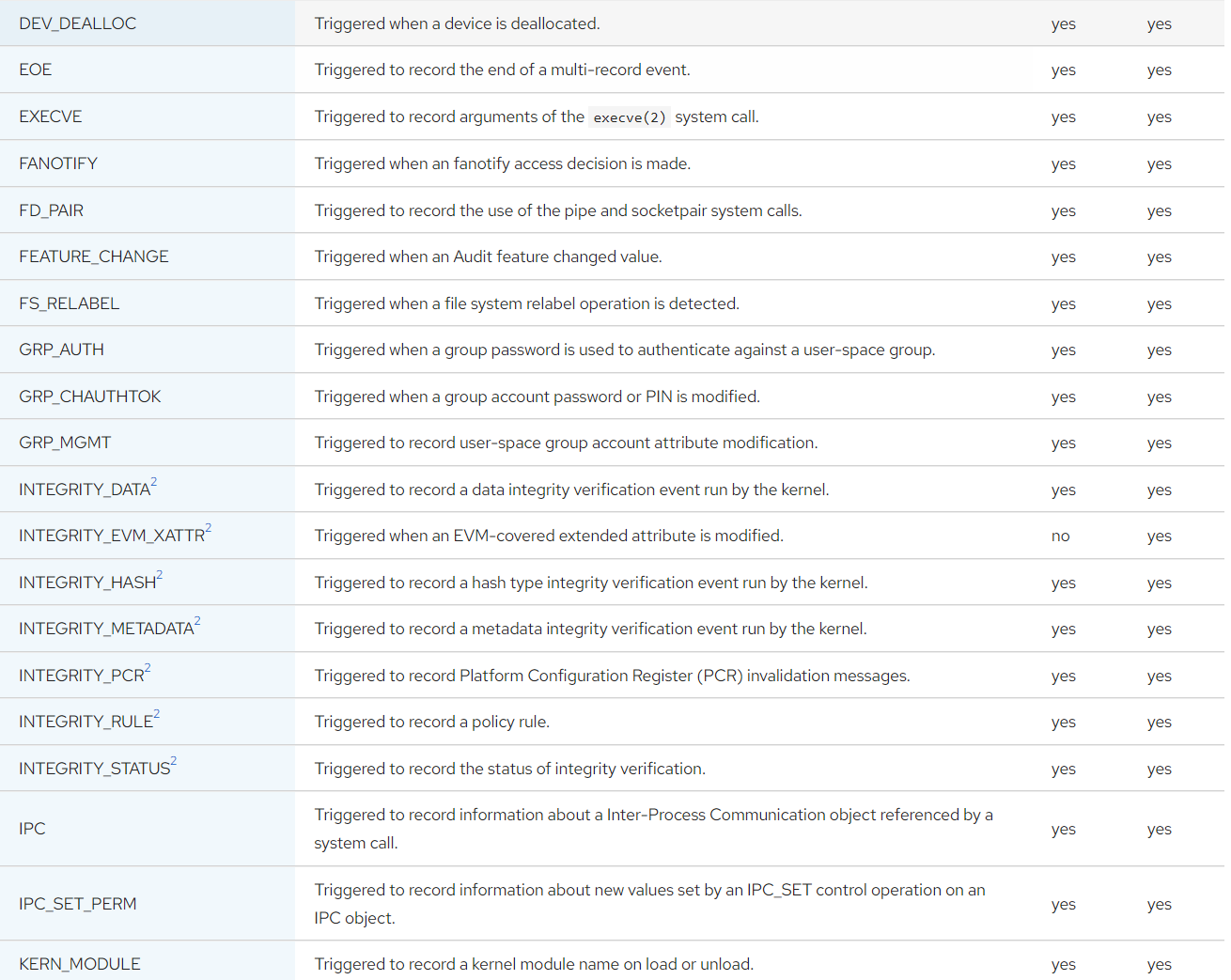
Lấy ví dụ

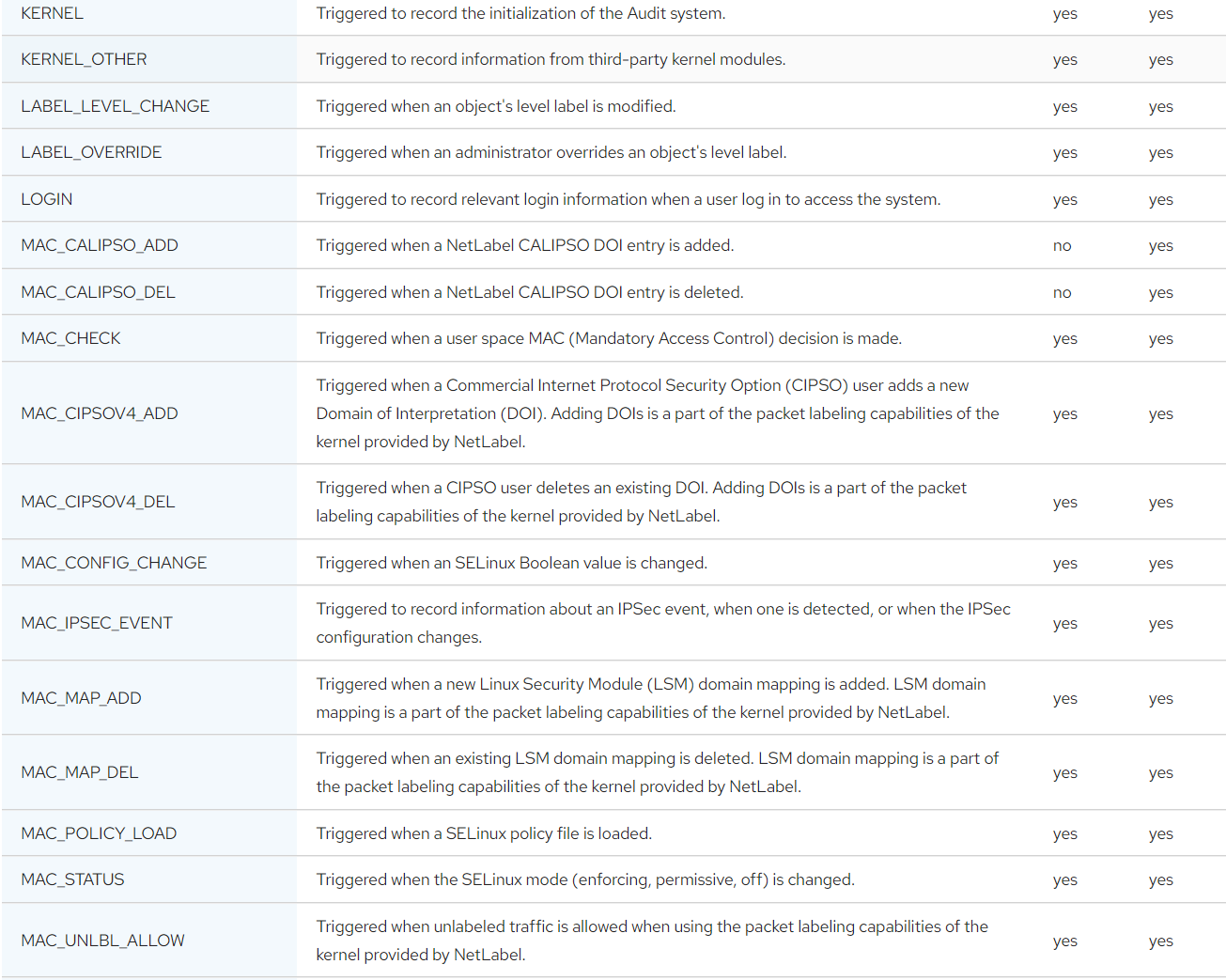
type=SYSCALL thì giá trị SYSCALL này được triggered bởi hệ thống tới kernel và để biết xem trong danh sách có những giá trị values nào có thể bị loại hoặc có thể giải thích của chúng chúng ta có thể biết được qua thông qua Audit Record Types

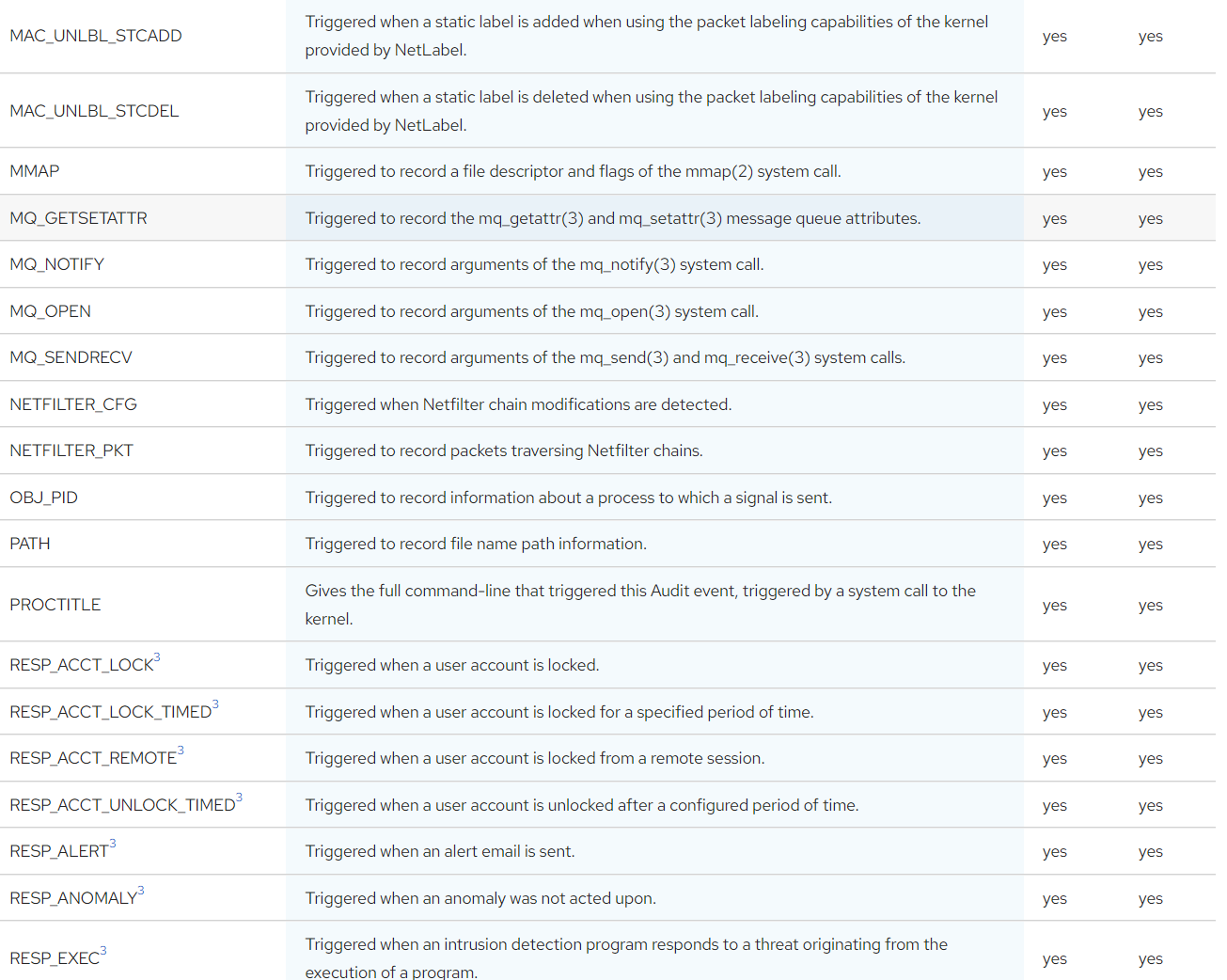


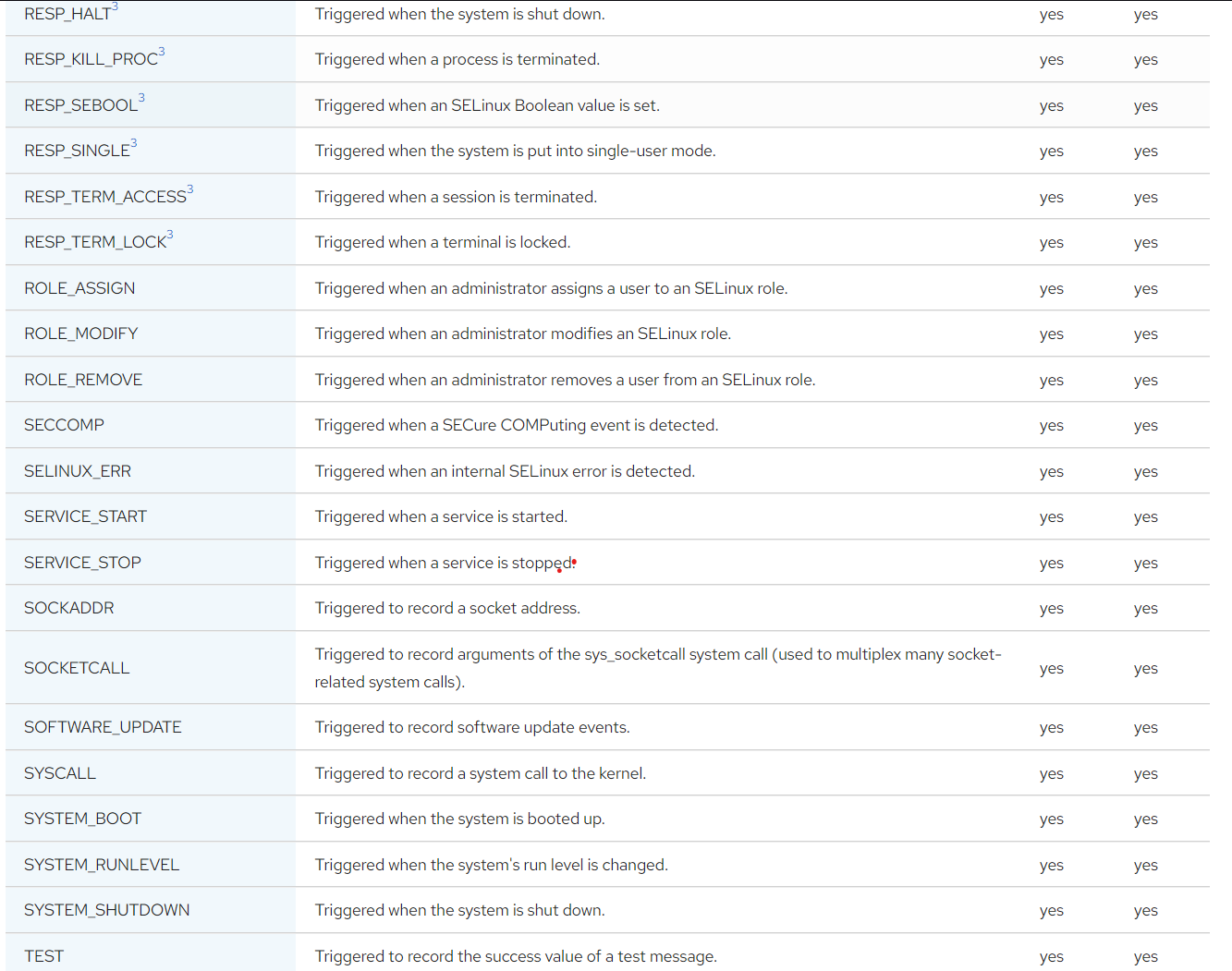


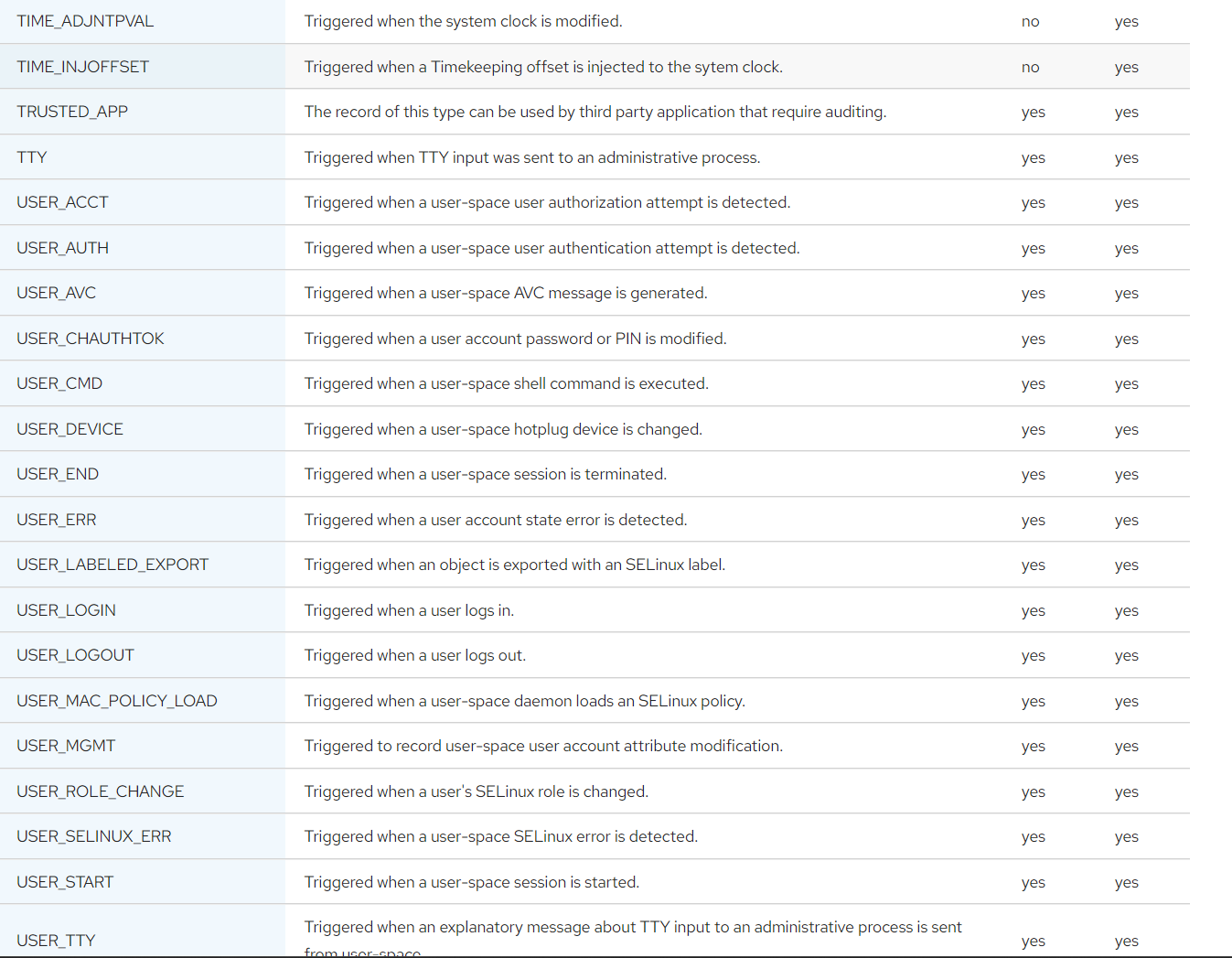


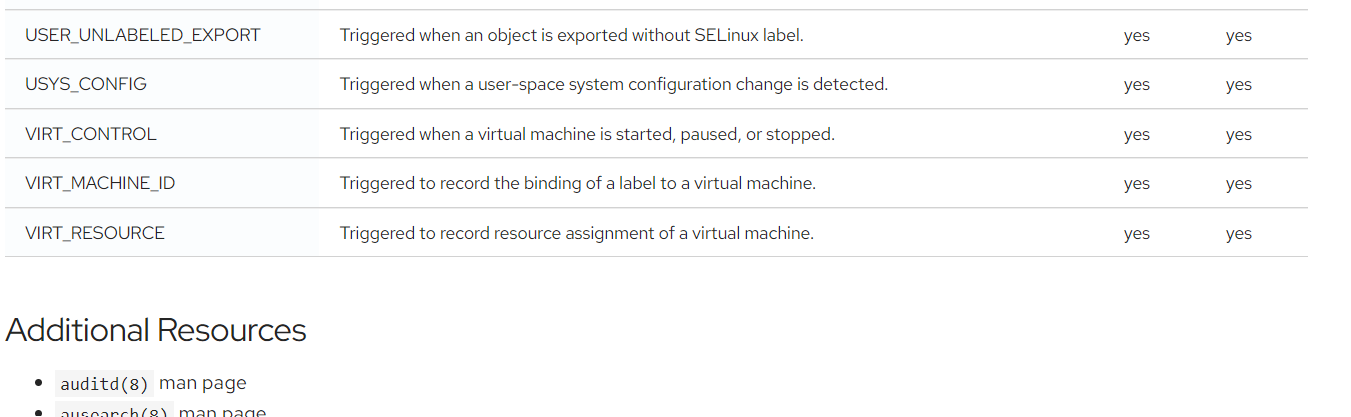












msg=audit(1694483451.987:3)

nó là 1 một mốc thời gian và 1 id duy nhất ở trong record ở trong form audit(time\_stamp:ID).

và nhiều bản records khác cũng có thể chi sẻ những time stamp cũng như id nếu như chúng được generated ở cùng một Audit event.

Và time stamp được sử dụng định dạng thời gian Unix – giây kể từ 00:00:00 UTC vào ngày 1/1/1970

arch=c000003e

Chứa các thông tin CPU của hệ thống.Giá trị arch được mã hóa dưới dạng thập lục phân . Và khi chúng ta muốn tìm kiếm trong Audit records bằng những lệnh ausearch, chúng ta có thể dung -I hoặc –interpret để có thể tự động chuyển đổi giá trị thập lục phân thành giá trị tương đương mà con người có thể đọc được

Giá trị c000003e con được hiểu là x86\_64

syscall=44

syscall field records là một kiểu system call được gửi tới kernel

giá trị 44 được gọi là hệ thống mở .không những thế chúng ta cần phải lưu ý rằng ausyscall cho phép bạn chuyển dổi số cuộc gọi trong hệ thống thành số mà chúng ta có thể đọc được .

Chúng ta cũng có thể sử dụng syscall dưới dang lệnh ausyscall –dump để hiển thị nội dung trong danh sách tất cả các system calls với số của chúng

Success=yes

Ghi lại system call trong sự kiện này có thành công hay không .ở trường hợp này là có

Exit=60

Ghi lại những giá trị được trả về bởi system call.Và giá trị này thay đổi đối với các system call khách nhau

Item= 1

Chứa những number of PATH phụ trợ cho records theo syscall record

Ppid=2046342

Đại diện cho những Parent ProcessID (PPID)

Pid = 3538

Đại diện cho proceesID(pid)

auid=1000

auid ghi lại ID người dùng Kiểm tra, đó là loginuid. ID này được gán cho người dùng khi đăng nhập và được kế thừa bởi mọi quy trình ngay cả khi danh tính của người dùng thay đổi, ví dụ: bằng cách chuyển đổi tài khoản người dùng bằng lệnh su - john.

uid=1000

uid ghi lại ID người dùng của người dùng đã bắt đầu quá trình phân tích. ID người dùng có thể được hiểu thành tên người dùng bằng lệnh sau: ausearch -i --uid UID.

gid=1000

gid ghi lại ID nhóm của người dùng đã bắt đầu quá trình phân tích. euid=1000

euid ghi lại ID người dùng hiệu quả của người dùng đã bắt đầu quá trình phân tích.

Suid=1000

suid ghi lại ID người dùng đã đặt của người dùng đã bắt đầu quá trình phân tích.

Fsuid=1000

fsuid ghi lại ID người dùng hệ thống tệp của người dùng đã bắt đầu quá trình phân tích.

ví dụ=1000 egid ghi lại ID nhóm hiệu quả của người dùng đã bắt đầu quá trình phân tích.

sgid=1000

sgid ghi lại ID nhóm đã đặt của người dùng đã bắt đầu quá trình phân tích.

fsgid=1000

fsgid ghi lại ID nhóm hệ thống tệp của người dùng đã bắt đầu quá trình phân tích.

tty=0

tty ghi lại thiết bị đầu cuối mà quy trình phân tích được gọi.

ses=1

ses ghi lại ID phiên của phiên mà quy trình phân tích được gọi.

comm=”cat”

comm ghi lại tên dòng lệnh của lệnh được sử dụng để gọi quy trình được phân tích. Trong trường hợp này, lệnh cat được sử dụng để kích hoạt sự kiện Kiểm tra này.

exe="/bin/cat"

exe ghi lại đường dẫn đến tệp thực thi được sử dụng để gọi quy trình được phân tích. subj=unconfined\_u:unconfined\_r:unconfined\_t:s0-s0:c0.c1023

subj ghi lại bối cảnh SELinux mà quá trình phân tích tại thời điểm labeled thực thi.

key = "sshd\_config"

key ghi lại chuỗi do quản trị viên xác định liên quan đến quy tắc đã tạo ra sự kiện này trong Audit log.