**Lab 6 - Giám sát thay đổi trái phép trong thư mục nhạy cảm bằng Auditd và Splunk**

**1. Mục tiêu**

* Cấu hình hệ thống để **giám sát thời gian thực** các thay đổi trái phép (sửa, xóa, thay đổi thuộc tính) trong thư mục quan trọng như /etc/.
* Sử dụng **Auditd** để ghi nhận sự kiện hệ thống liên quan đến thay đổi file.
* Dùng **Splunk** để thu thập, phân tích và trực quan hóa log từ Auditd.
* Mô phỏng các hành vi tấn công (ví dụ: sửa file /etc/passwd, xóa file) và từ đó rèn luyện kỹ năng điều tra, phản ứng sự cố và bảo vệ hệ thống.

**2. Sơ đồ mạng**

Ubuntu Server (Victim, SplunkUniversalForwarder): 192.168.56.105/24

Ubuntu (Splunk Server): 192.168.56.104/24

Kali (Attacker): 192.168.56.101/24

**3. Kiến thức nền**

**Auditd** (Linux Auditing System) là một dịch vụ giúp ghi nhận các hành vi xảy ra trên hệ thống:

* **Ghi log hành động**: Mọi thao tác như mở file, sửa đổi, xóa… sẽ được ghi lại.
* **Tùy biến luật kiểm soát**: Cho phép cấu hình để giám sát những file hoặc hoạt động cụ thể.
* **Hỗ trợ chuẩn an toàn**: Giúp đạt được các yêu cầu tuân thủ bảo mật (compliance).
* **Tích hợp với các công cụ SIEM**: Như Splunk để phân tích và cảnh báo.

**Splunk** và **Splunk Universal Forwarder**:

* **Splunk** là nền tảng phân tích log tập trung.
* **Splunk Universal Forwarder**: Gửi log từ server tới Splunk Server.
* Cho phép viết truy vấn, tạo dashboard, và cảnh báo khi có dấu hiệu bất thường.

**4. Các bước tiến hành**

**Bước 1: Chuẩn bị môi trường**

* Tải và cài đặt máy ảo Ubuntu Server 22.04 và Kali Linux 2025.1a qua VMware Player.
  + Ubuntu Server: <https://releases.ubuntu.com/jammy/ubuntu-22.04.5-live-server-amd64.iso>
  + Kali Linux: <https://cdimage.kali.org/kali-2025.1a/kali-linux-2025.1a-vmware-amd64.7z>
* Thực hiện cài đặt, cấu hình Splunk Server trên Windows và Splunk Universal Forwarder trên Ubuntu Server theo hướng dẫn tại: <https://github.com/0xrajneesh/90-days-security-challenge/blob/main/Challenge%231/Lab> Set up.md

**Bước 2: Cài đặt và cấu hình Auditd**

1. **Tải Auditd và mở Auditd**

sudo apt update

sudo apt install auditd -y

systemctl start auditd

sudo systemctl enable auditd

1. **Kiểm tra trạng thái của Auditd**

sudo systemctl status auditd

**Bước 3: Thiết lập luật giám sát File**

1. **Sửa file luật Audit:**

sudo nano /etc/audit/rules.d/audit.rules

1. **Thêm luật sau để giám sát thư mục /etc/**

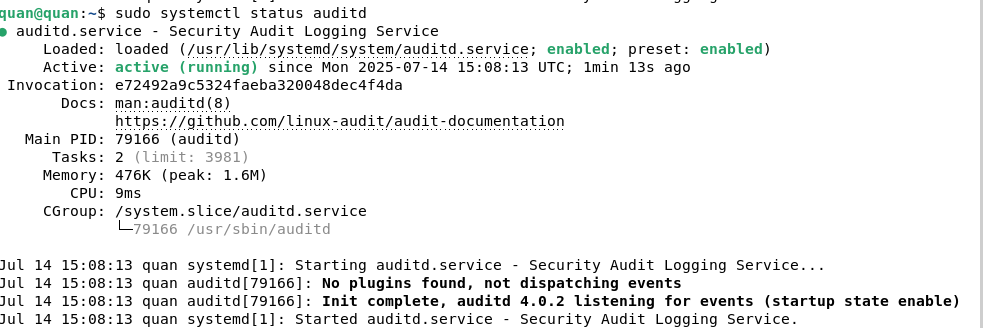
-w /etc/ -p wa -k file\_integrity

* Ý nghĩa:
  + -w: theo dõi thư mục /etc/
  + -p wa: giám sát quyền ghi (w) và thay đổi thuộc tính (a)
  + -k file\_integrity: keyword để gắn tag cho log

1. **Áp dụng luật**

sudo service auditd restart

sudo auditctl -l



**Bước 4: Cấu hình Splunk Universal Forwarder**

1. **Sửa file cấu hình inputs.conf để Splunk Forwarder theo dõi log của auditd và gửi tới Splunk Server**

* Mở file inputs.conf

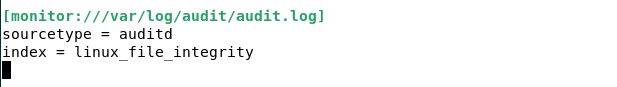
sudo nano /opt/splunkforwarder/etc/system/local/inputs.conf

* Thêm dòng sau

[monitor:///var/log/audit/audit.log]

sourcetype = auditd

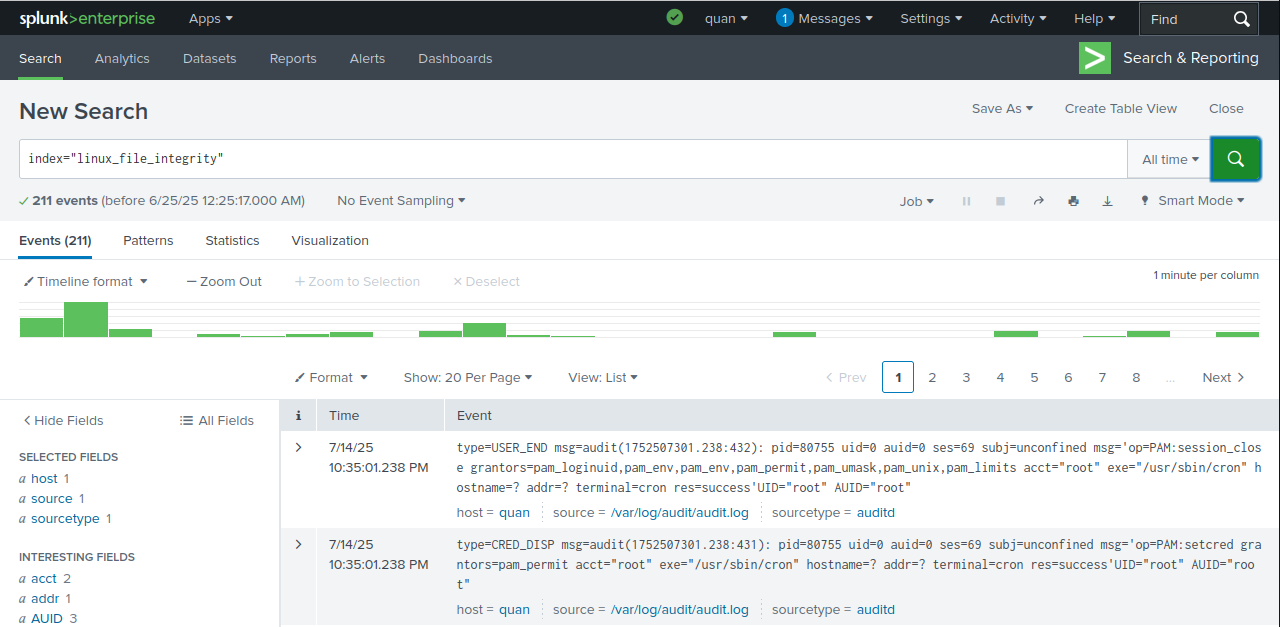
index = linux\_file\_integrity



* Khởi động lại Spunk Forwarder

sudo /opt/splunkforwarder/bin/splunk restart

1. **Kiểm tra xem log đã được đẩy lên Splunk Server chưa**



**Bước 5: Mô phỏng thay đổi trái phép trong thư mục /etc/**

1. **Thay đổi File**

* Tạo thay đổi tới file /etc/passwd để mô phỏng việc thay đổi trái phép

1. **Xóa File**

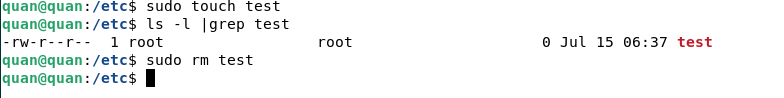
* Xóa 1 file trong thư mục /etc/

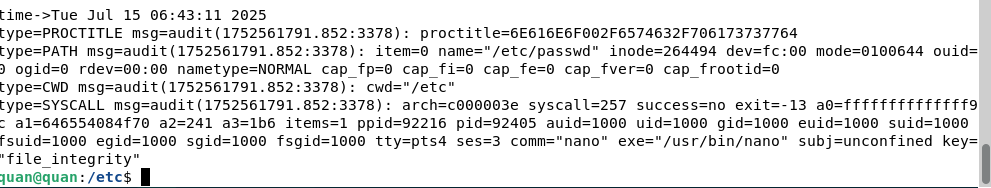
1. **Truy xuất log với Auditd**

* Dùng ausearch dể xem logs cho những hành động thay đổi trái phép trên

sudo ausearch -k file\_integrity



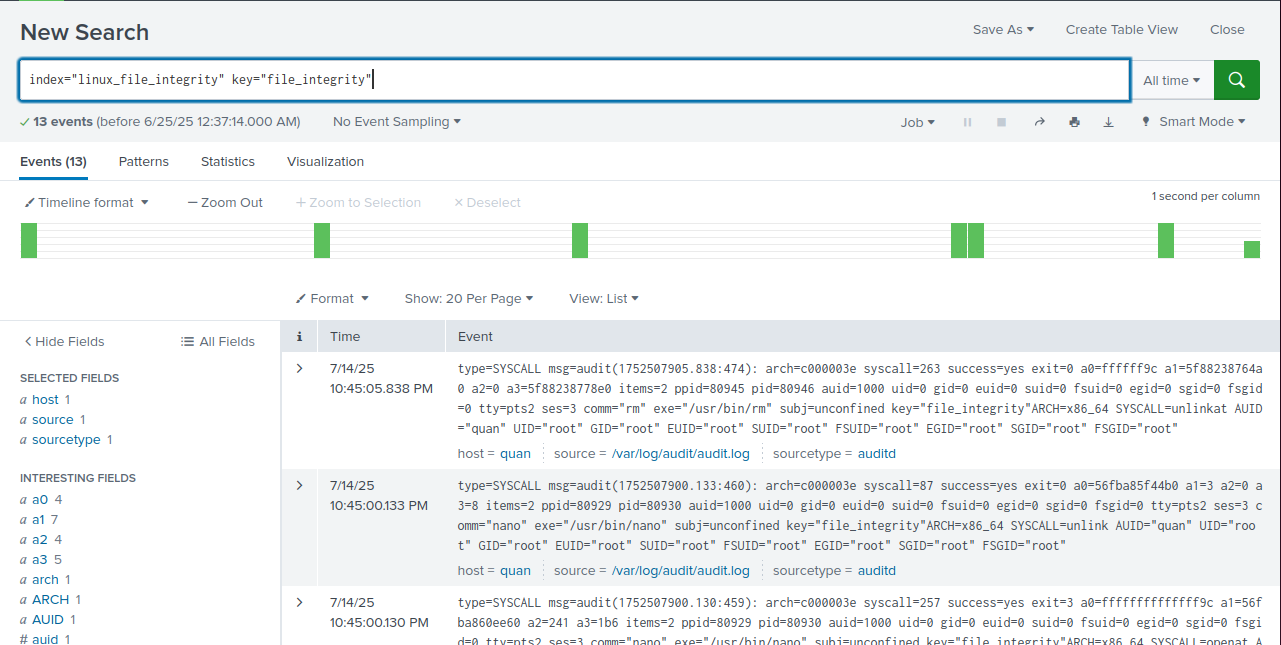


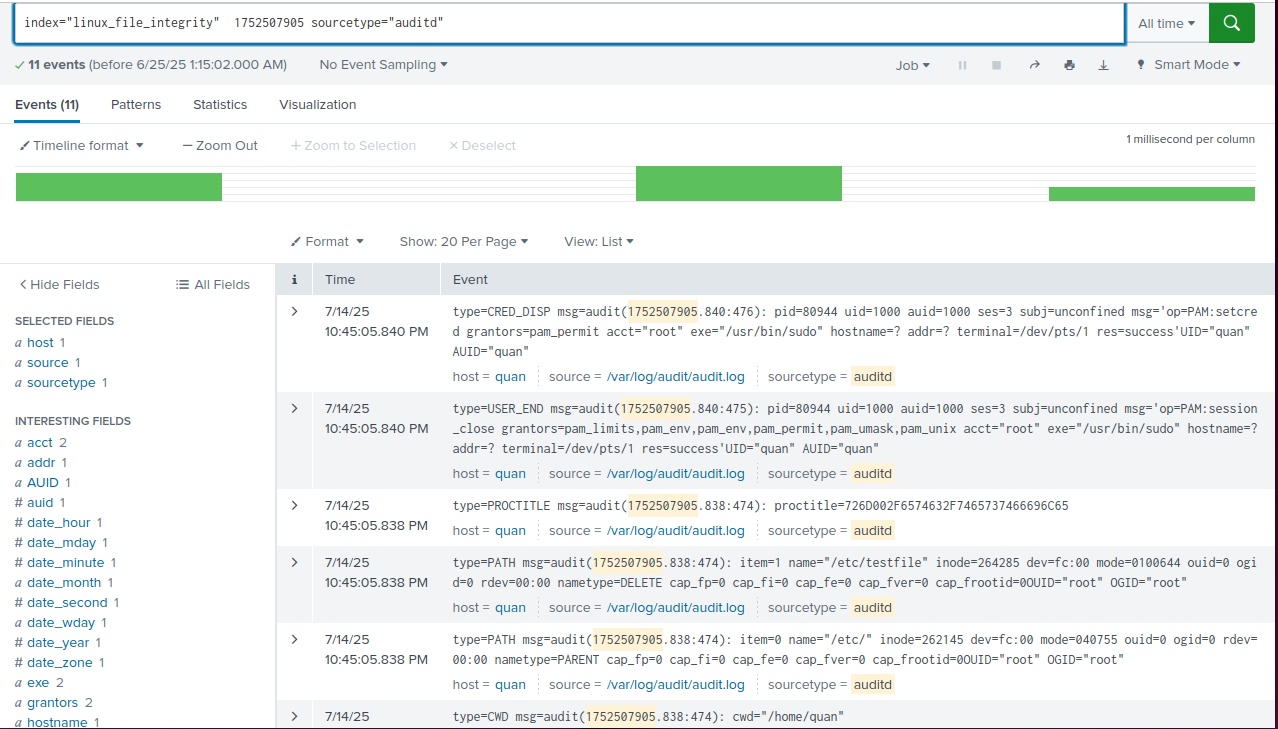


**Bước 6: Phân tích log trong Splunk**

1. **Truy vấn tìm sự kiện integrity:**

index="linux\_file\_integrity" key="file\_integrity"





**HOẠT ĐỘNG XÓA FILE**

**Thời gian sự kiện:** 14-07-2025 10:45:05.939 PM

**Nguồn log:**

Auditd – syscall unlinkat

**1. Tóm tắt sự kiện**

Vào thời điểm được ghi nhận, một tiến trình do người dùng muoi khởi tạo đã thực thi lệnh **rm** để xóa file có tên **test** trong thư mục **/etc**. Lệnh được thực thi với quyền **root** (UID 0), và hoạt động xóa đã **thành công** (success=yes, exit=0).

**2. Chi tiết kỹ thuật**

* **Lệnh thực thi:** /usr/bin/rm
* **Tên tiến trình:** rm
* **PID:** 80946 (cha: 80945)
* **Đường dẫn hiện tại:** /etc
* **File bị xóa:** /etc/test
* **syscall:** unlinkat (syscall=263)
* **Người dùng thật (AUID):** quan (auid=1000)
* **Người thực thi:** root (uid=0, euid=0, fsuid=0)

**3. Phân tích và đánh giá**

* **Quyền xóa file được thực hiện bởi user root**, tuy nhiên **người dùng khởi tạo phiên là muoi**, tức là có thể đã dùng **sudo hoặc có đặc quyền root**.
* File test nằm trong thư mục nhạy cảm /etc, nơi chứa các file cấu hình hệ thống → cần xác minh mục đích và nội dung của file test trước khi bị xóa.
* Không phát hiện dấu hiệu lỗi hay từ chối truy cập – hành động hoàn tất thành công.

**4. Kiến nghị**

* **Kiểm tra lịch sử sudo (/var/log/auth.log)** để xác nhận hành vi sử dụng đặc quyền.
* **Xác minh nội dung file /etc/test trước đó**, nếu có bản sao lưu hoặc qua hệ thống giám sát integrity.
* Nếu hành động không nằm trong kế hoạch hệ thống:

→ **Tăng cường giám sát hoạt động người dùng muoi** và xem xét **hạn chế quyền sudo nếu không cần thiết.**

* **Bổ sung cảnh báo real-time** với từ khóa như unlinkat, rm, chmod, chown khi tác động đến /etc/\*.

**5. Kết luận**

Hành vi xóa file /etc/test bằng lệnh rm dưới quyền root được khởi tạo bởi người dùng muoi đã diễn ra thành công. Tuy không có dấu hiệu tấn công rõ ràng, đây là hành vi nhạy cảm do liên quan đến thư mục hệ thống. Đề xuất đánh giá lại quyền truy cập và chính sách giám sát người dùng.