**Lab 5 - Theo dõi tính toàn vẹn tệp của các thư mục quan trọng trên máy Windows**

**1. Mục tiêu**

* Mục tiêu của bài lab này là giám sát và điều tra các thay đổi trái phép đối với các tệp và thư mục quan trọng trên máy Windows bằng cách sử dụng Sysmon để ghi nhật ký chi tiết và Splunk để phân tích. Điều này bao gồm phát hiện việc tạo, sửa đổi và xóa tệp trong các thư mục nhạy cảm để xác định các sự cố bảo mật tiềm ẩn

**2. Sơ đồ mạng**

Ubuntu Server (Splunk Server): 192.168.56.105/24

Windows 10 (SplunkUniversalForwarder): 192.168.56.106/24

**3. Kiến thức nền**

* **Sysmon:** Là công cụ giám sát hệ thống nâng cao do Microsoft phát hành trong bộ Sysinternals, giúp ghi lại các sự kiện bảo mật chi tiết như tạo tiến trình, thay đổi file, kết nối mạng, và đặc biệt là các hành động liên quan đến Scheduled Tasks như tạo hoặc thực thi tác vụ. Với cấu hình phù hợp, Sysmon giúp phát hiện hành vi đáng ngờ mà các log mặc định của Windows có thể bỏ sót.
* **Splunk Universal Forwarder:** Là một lightweight agent được cài trên máy Windows (hoặc các hệ điều hành khác) để thu thập log theo thời gian thực và gửi về máy chủ Splunk. Trong môi trường giám sát bảo mật, nó thường được cấu hình để gửi log của Windows Event Log, Sysmon hoặc các file log tùy chỉnh về Splunk nhằm phục vụ việc phân tích tập trung.
* **Splunk:** Là một nền tảng SIEM mạnh mẽ hỗ trợ thu thập, tìm kiếm, phân tích, cảnh báo và trực quan hóa dữ liệu log từ nhiều nguồn. Với khả năng truy vấn linh hoạt bằng SPL (Search Processing Language), Splunk giúp các analyst nhanh chóng phát hiện các hành vi đáng ngờ, như việc tạo Scheduled Task bất thường hoặc hoạt động lateral movement, từ các log được gửi về.

**4. Các bước tiến hành**

**Bước 1: Chuẩn bị môi trường**

* Tải và cài đặt máy ảo Ubuntu Server 22.04 VMware Player.
  + Ubuntu Server: <https://releases.ubuntu.com/jammy/ubuntu-22.04.5-live-server-amd64.iso>
* Thực hiện cài đặt, cấu hình Splunk Server trên Ubuntu Server và Splunk Universal Forwarder trên Windows theo hướng dẫn tại: <https://github.com/0xrajneesh/90-days-security-challenge/blob/main/Challenge%232/Lab%20Set%20up%20.md>

**Bước 2: Cài đặt Sysmon trên máy Windows**

1. **Tải Sysmon**

* Truy cập: <https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon>
* Tải file .zip về và giải nén (thường sẽ có Sysmon.exe và Sysmon64.exe)

1. **Tải file cấu hình Sysmon**

* Dùng mẫu cấu hình từ SwiftOnSecurity (rất phổ biến): <https://github.com/SwiftOnSecurity/sysmon-config>

-> Tải file sysmonconfig-export.xml.

1. **Cài đặt Sysmon**

* Mở **Command Prompt với quyền Administrator**, điều hướng đến thư mục chứa Sysmon, rồi chạy:

sysmon64.exe -i sysmonconfig-export.xml

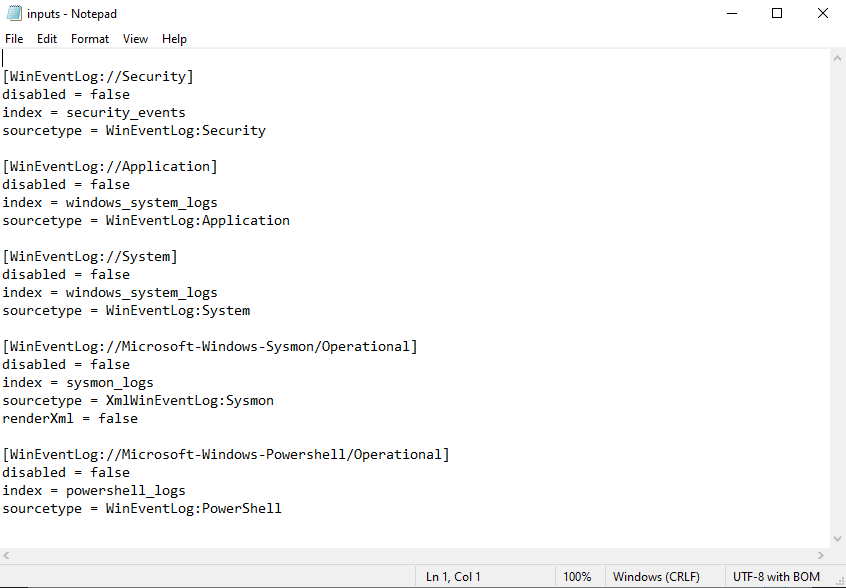
* Nếu thành công, Sysmon sẽ bắt đầu ghi lại các sự kiện vào Windows Event Log, mục **"Microsoft-Windows-Sysmon/Operational"**.
* **Kiểm tra:** Mở Event Viewer > Applications and Services Logs > Microsoft > Windows > Sysmon > Operational.

**Bước 3: Cấu hình Splunk Forwarder theo dõi và gửi log của Sysmon**

1. **Mở file inputs.conf của Splunk Forwarder**

C:\\Program Files\\SplunkUniversalForwarder\\etc\\system\\local\\inputs.conf

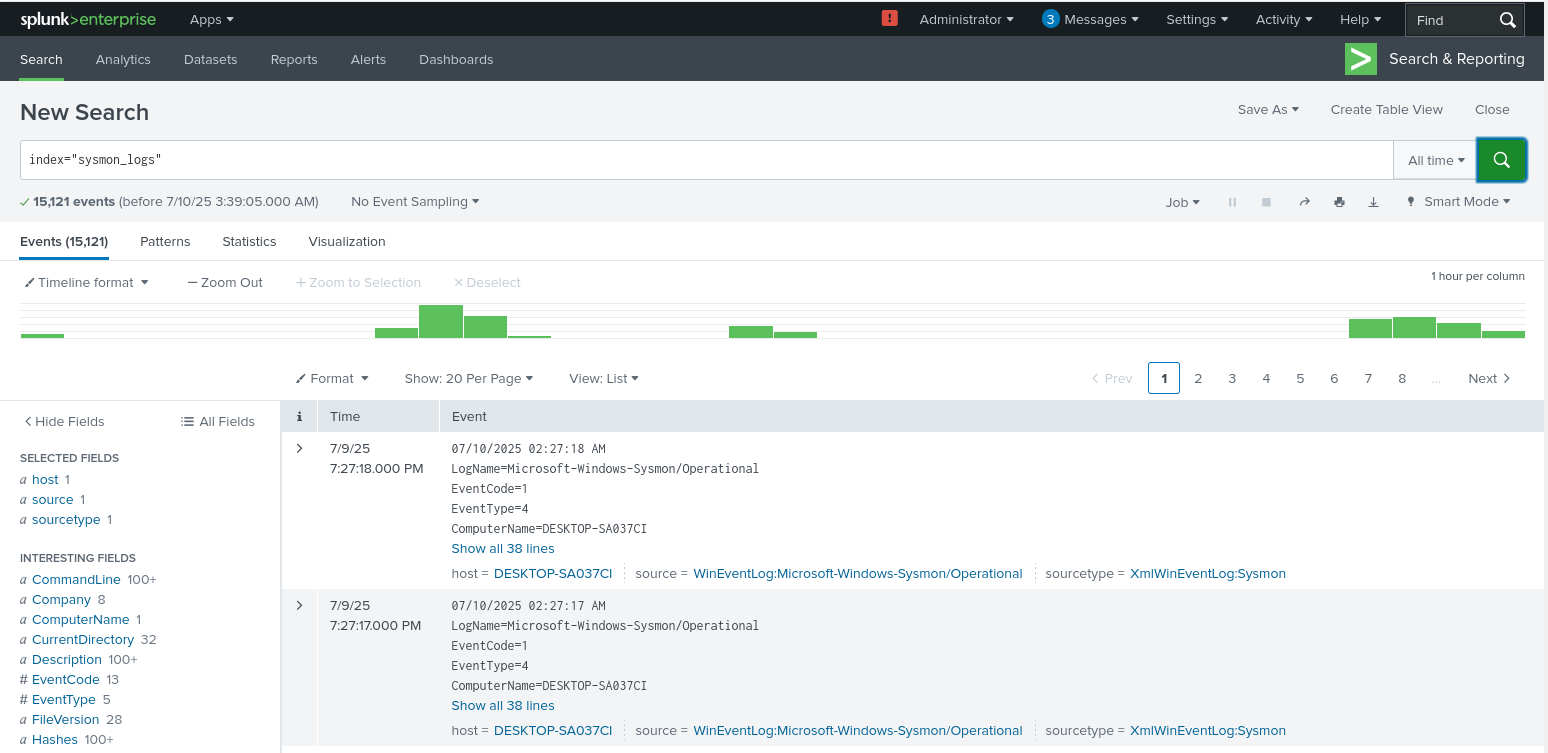
**Thêm dòng sau**



1. **Khởi động lại Splunk Forwarder**

C:\\WINDOWS\\system32>"C:\\Program Files\\SplunkUniversalForwarder\\bin\\splunk.exe" restart

1. **Kiểm tra xem Splunk nhận được log của Sysmon**



* **Lưu ý:** Nếu Splunk không nhận được log của **Sysmon** mà xem thủ công log của **Sysmon** trên máy Windows vẫn có thì khả năng là do Splunk Forwarder **không chạy bằng Local System Account** nên không đủ quyền đọc log Event Viewer ở Microsoft-Windows-Sysmon/Operational
* **Cách khắc phục:**
  + Kiểm tra lại account đang chạy Splunk Forwarder:
* Get-WmiObject win32\_service | Where-Object { $\_.Name -eq "SplunkForwarder" } | Select-Object StartName
* Nếu không thấy LocalSystem, bạn cần sửa:
  + - Nhấn Win + R, nhập: services.msc
    - Tìm dịch vụ **"SplunkForwarder"**
    - Chuột phải → Properties
    - Chuyển sang tab **Log On**
    - Chọn: Local System account
    - Khởi động lại Splunk Forwarder

**Bước 4: Mô phỏng thay đổi tệp trái phép**

1. **Tạo 1 tệp mới**

echo MaliciousContent > C:\\Windows\\System32\\malicious.exe

1. **Sửa đổi 1 tệp hiện có**

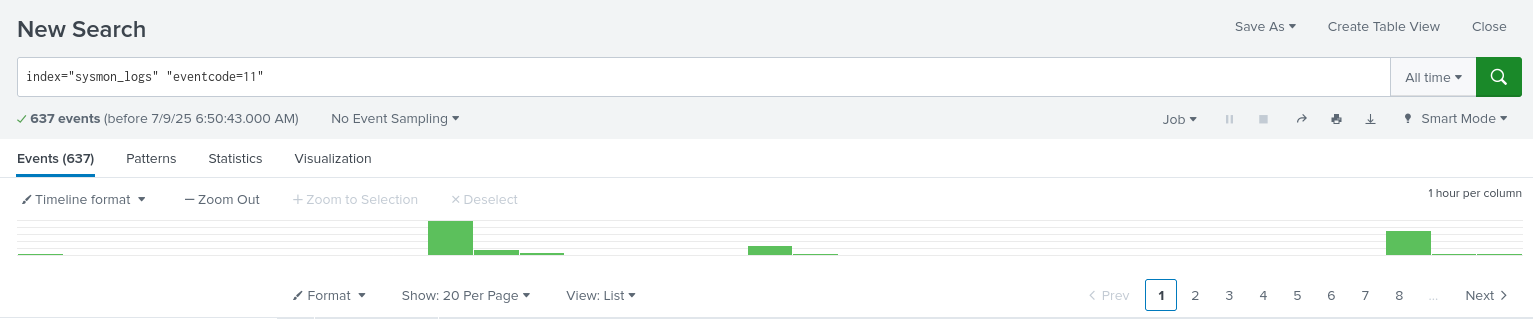
echo AlteredContent >> C:\\Windows\\System32\\config.sys

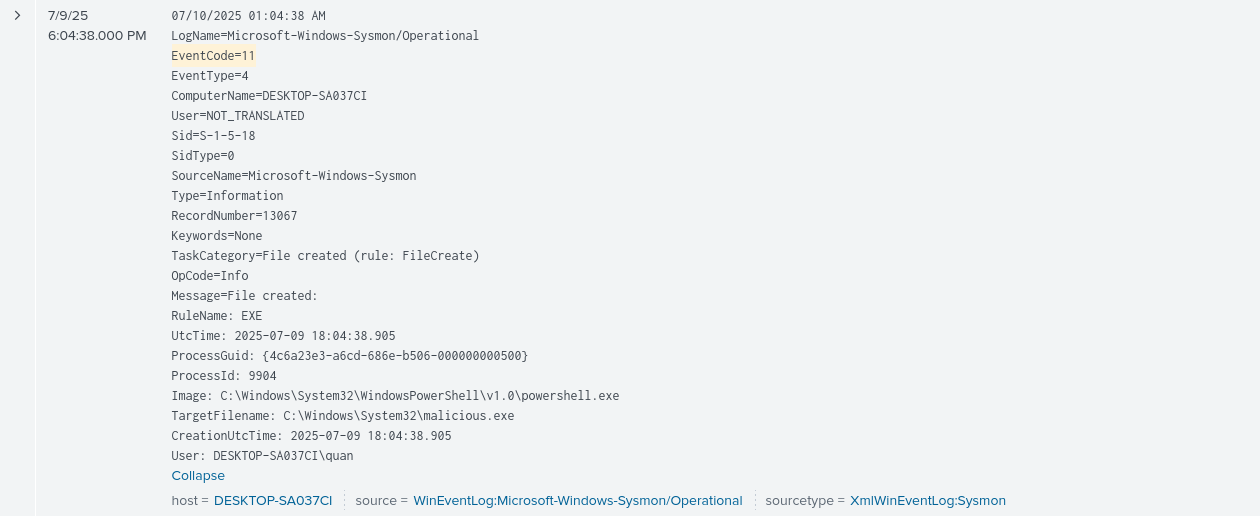
1. **Xóa 1 tệp quan trọng**

del C:\\Windows\\System32\\important.dll



**Bước 5: Phân tích log trên Splunk**

****

****

**🛡️ BÁO CÁO SỰ KIỆN AN NINH – TẠO FILE ĐÁNG NGỜ**

**🔹 Thời gian xảy ra:**

2025-07-09 18:04:38 UTC (01:04:38 Local time)

**🔹 Nguồn log:**

* Log Source: Sysmon – Microsoft-Windows-Sysmon/Operational
* Event ID: 11 (FileCreate)
* RuleName: EXE

**🔹 Nội dung log chính:**

File created:

RuleName: EXE

UtcTime: 2025-07-09 18:04:38

Image: C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe

TargetFilename: C:\\Windows\\System32\\malicious.exe

User: DESKTOP-SA037CI\quan

**📌 Miêu tả sự kiện:**

Hệ thống phát hiện một tệp thực thi (EXE) mới được tạo tại thư mục hệ thống quan trọng C:\\Windows\\System32\\. Tệp có tên malicious.exe, được tạo bởi tiến trình powershell.exe dưới quyền người dùng lab.

**🔍 Phân tích sự kiện:**

* **Vị trí file:** System32 là thư mục hệ thống có mức độ nhạy cảm cao. Việc xuất hiện một file .exe ở đây là **không bình thường** nếu không được cập nhật hệ thống hoặc cài phần mềm hợp lệ.
* **Tiến trình tạo file:** powershell.exe thường bị lợi dụng trong các cuộc tấn công nội bộ (living-off-the-land). Việc sử dụng PowerShell để tạo file .exe cho thấy khả năng có **script độc hại** hoặc tải mã độc từ xa.
* **Người dùng thực hiện:** DESKTOP-Lab\\lab

**⚠️ Đánh giá mức độ nghiêm trọng:**

**Cao** – Việc một file thực thi có tên nghi ngờ được tạo bởi PowerShell trong thư mục hệ thống là dấu hiệu của **hoạt động hậu khai thác** trong một cuộc tấn công.

**✅ Hành động đề xuất:**

1. **Cách ly ngay máy DESKTOP-Lab** khỏi mạng để tránh lây lan.
2. **Xác minh file malicious.exe** qua hash và gửi đến VirusTotal hoặc sandbox.
3. **Kiểm tra toàn bộ lịch sử hành vi của tiến trình powershell.exe** vào thời điểm trên (Sysmon Event ID 1 - ProcessCreate).
4. **Xem lại toàn bộ log đăng nhập** từ xa liên quan đến tài khoản lab, xác minh địa chỉ IP truy cập.
5. **Thực hiện quét toàn bộ hệ thống** bằng công cụ EDR hoặc antivirus nâng cao.
6. **Thay đổi mật khẩu khẩn cấp** cho các tài khoản quản trị.
7. **Tăng cường FIM (File Integrity Monitoring)** cho thư mục hệ thống