**Lab 3 - Điều tra hoạt động PowerShell đáng ngờ trên máy Windows bằng Sysmon và Splunk**

**1. Mục tiêu**

* Mục tiêu của lab này là phát hiện, điều tra và phản ứng với các hoạt động PowerShell độc hại hoặc trái phép trên máy Windows bằng cách sử dụng Sysmon và Splunk.
* Tập trung vào việc xác định các lệnh PowerShell đáng ngờ, các script được mã hóa và các hoạt động như tải xuống hoặc thực thi tệp từ các đường dẫn không chuẩn.

**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**

* **PowerShell:** Là một shell dòng lệnh mạnh mẽ được tích hợp trong Windows, có thể bị tin tặc lợi dụng để tải mã độc, thực thi script hoặc giao tiếp C2.
* **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

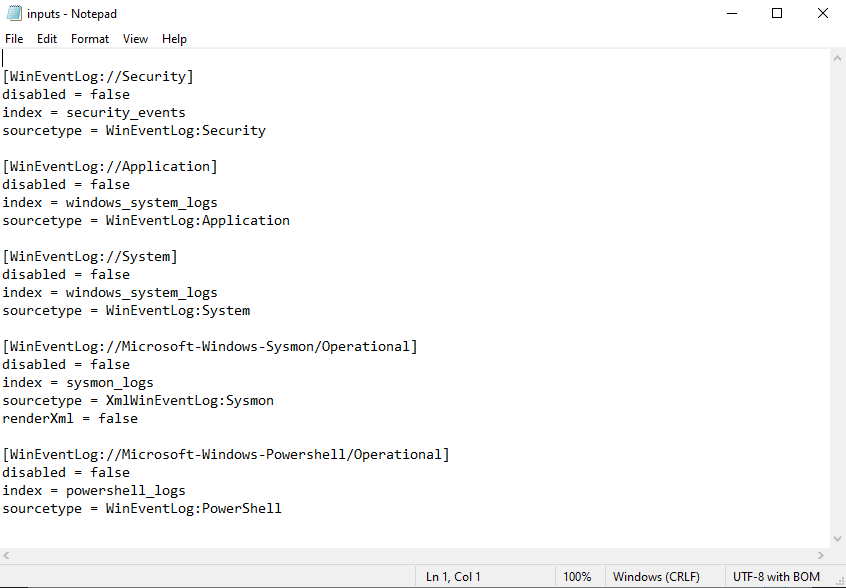
* Nếu thành công, Sysmon sẽ bắt đầu ghi lại các sự kiện vào Windows Event Log, mục **"Microsoft-Windows-Sysmon/Operational"**.
* **Kiểm tra:** Mở Event Viewer > Applications and Services Logs > Microsoft > Windows > Sysmon > Operational.

**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

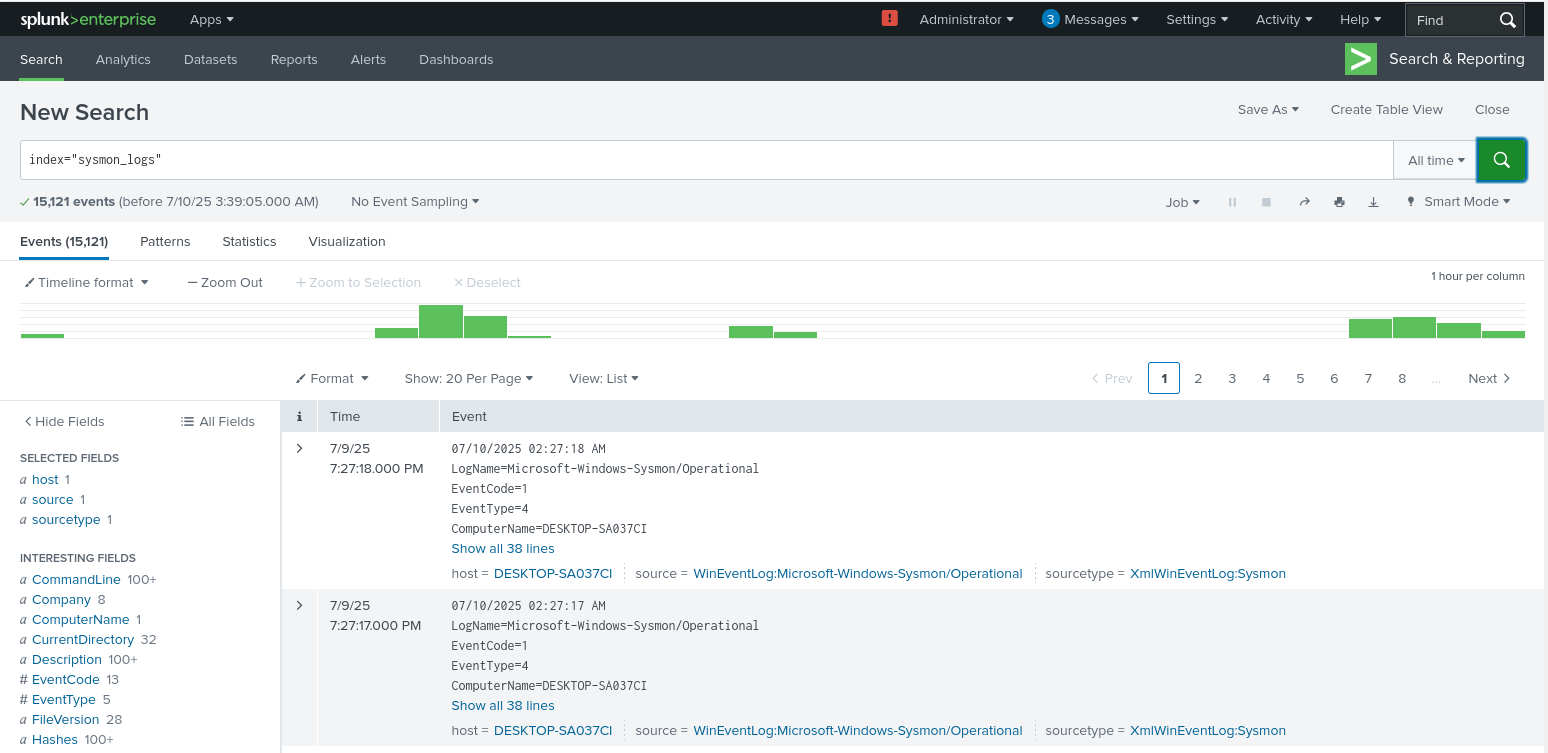
**Thêm dòng sau**



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 hoạt động đáng ngờ trên PowerShell**

1. **Tải 1 file đáng ngờ từ internet**

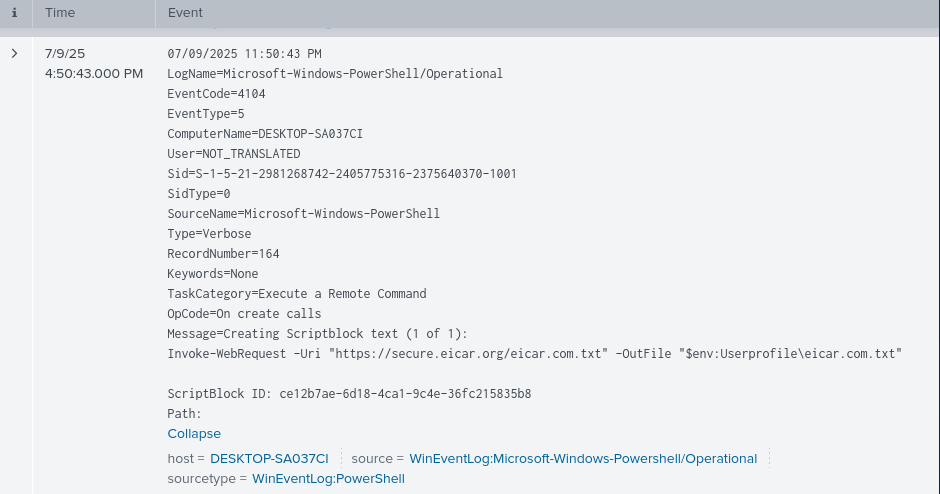
Invoke-WebRequest -Uri "<https://secure.eicar.org/eicar.com.txt>" -OutFile "$env:USERPROFILE\\eicar.com.txt"



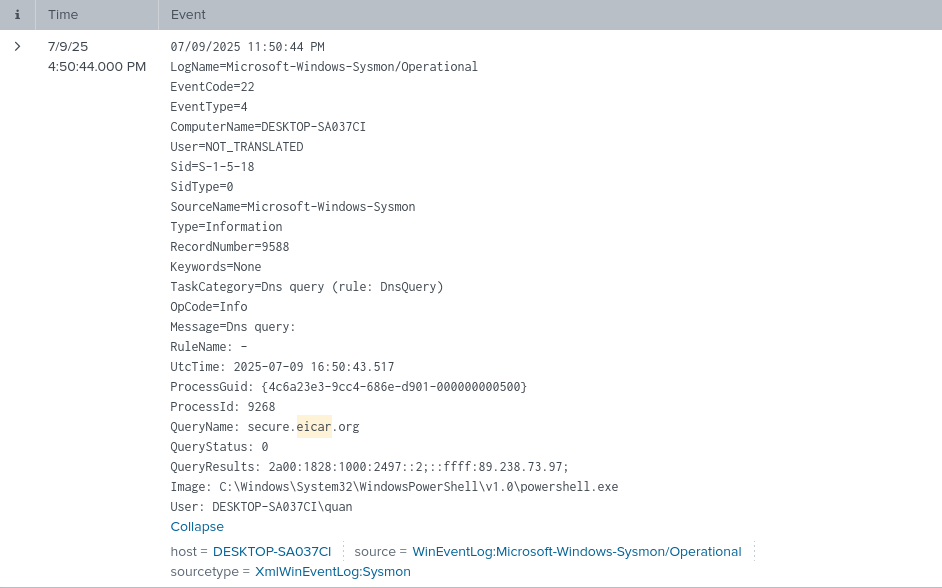
**Bước 5: Phân tích Log trên Splunk**

1. **Truy vấn log**

index="powershell\_logs"



index="sysmon\_logs" eicar



1. **Ngày giờ sự kiện:** 07/09/2025 11:50:44
2. **Máy chủ:** DESKTOP-SA037CI
3. **Người dùng:** DESKTOP-SA037CI\quan
4. **Quản lý sự kiện:** Microsoft-Windows-PowerShell/Operational, Microsoft-Windows-Sysmon/Operational
5. **Mô tả sự kiện:**

Một tiến trình powershell.exe (PID: 11232) đã tạo và thực thi một đoạn mã PowerShell (ScriptBlock) thực hiện tải file từ internet về máy cục bộ. Đoạn mã sử dụng lệnh Invoke-WebRequest để tải file eicar.com.txt từ URL https://secure.eicar.org/eicar.com.txt và lưu tại thư mục người dùng với đường dẫn $env:USERPROFILE\\eicar.com.txt.

1. **Chi tiết sự kiện PowerShell:**
   * Sự kiện được ghi lại trong log PowerShell EventCode=4104, TaskCategory=Execute a Remote Command.
   * ScriptBlock ID: ce12b7ae-6d18-4ca1-9c43-36fc215835b8
   * Lệnh thực thi:
2. Invoke-WebRequest -Uri "<https://secure.eicar.org/eicar.com.txt>" -OutFile "$env:USERPROFILE\\eicar.com.txt"
3. **Chi tiết sự kiện DNS Query:**
   * Ngay sau đó, tiến trình powershell.exe đã thực hiện truy vấn DNS tới domain secure.eicar.org để phân giải địa chỉ IP.
   * Kết quả truy vấn DNS trả về IP: 89.238.73.97
   * Sự kiện được ghi nhận trong log Sysmon EventCode=22, TaskCategory=Dns query.
4. **Phân tích và đánh giá:**
   * Hành vi tải file từ URL bên ngoài qua **PowerShell** có thể được coi là hoạt động đáng ngờ, đặc biệt nếu file được tải về có thể chứa mã độc hoặc được dùng cho thử nghiệm an ninh mạng (trong trường hợp này, file eicar.com.txt là file test virus chuẩn dùng để kiểm tra phần mềm diệt virus).
   * Việc theo dõi kết hợp giữa **PowerShell ScriptBlock** tạo ra và **DNS Query** giúp xác định chính xác mục tiêu tải file, phục vụ điều tra sâu hơn nếu cần.
   * Sự kiện này phù hợp với MITRE ATT&CK kỹ thuật T1105 - Ingress Tool Transfer, tức việc chuyển tải công cụ/mã độc vào hệ thống mục tiêu.
5. **Đề xuất:**
   * Theo dõi các hoạt động **PowerShell** tương tự để phát hiện các tải về đáng ngờ.
   * Kiểm tra nội dung file tải về và xác định mục đích sử dụng.
   * Nếu đây là hoạt động không mong muốn, cân nhắc thực thi các biện pháp ngăn chặn tải file không được phép qua PowerShell hoặc thiết lập chính sách chặt chẽ hơn cho PowerShell logging và thực thi.