**Lab 4 - Giám sát thay đổi Windows Registry bằng Sysmon và Splunk**

**1. Mục tiêu**

* Mục tiêu của lab này là giám sát và phát hiện các thay đổi trái phép hoặc đáng ngờ đối với Windows Registry, đặc biệt là các hành vi liên quan đến cài đặt malware, cơ chế duy trì quyền truy cập (persistence), hoặc thay đổi cấu hình bảo mật. Sử dụng công cụ **Sysmon** và **Splunk** để giám sát các thay đổi này.

**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**

* **Windows Registry:** Là một cơ sở dữ liệu phân cấp lưu trữ thông tin cấu hình và tùy chỉnh cho hệ điều hành Windows, thiết bị phần cứng, dịch vụ, tài khoản người dùng, và phần mềm cài đặt. Nhiều kỹ thuật tấn công và persistence (duy trì truy cập) lợi dụng registry để thiết lập backdoor hoặc tự động chạy mã độc. Việc theo dõi các thay đổi đáng ngờ trong registry là rất quan trọng trong giám sát an ninh hệ thống.
* **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

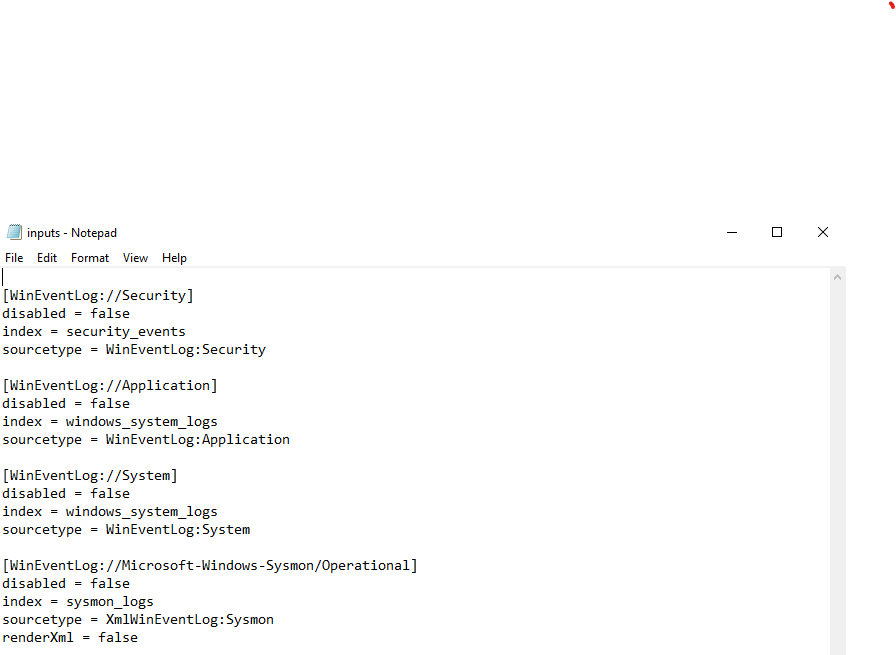
* Nếu thành công, Sysmon sẽ bắt đầu ghi lại các sự kiện vào Windows Event Log, mục **"Microsoft-Windows-Sysmon/Operational"**.
* **Kiểm tra:** Mở Event Viewer > Applications and Services Logs > Microsoft > Windows > Sysmon > Operational.

**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

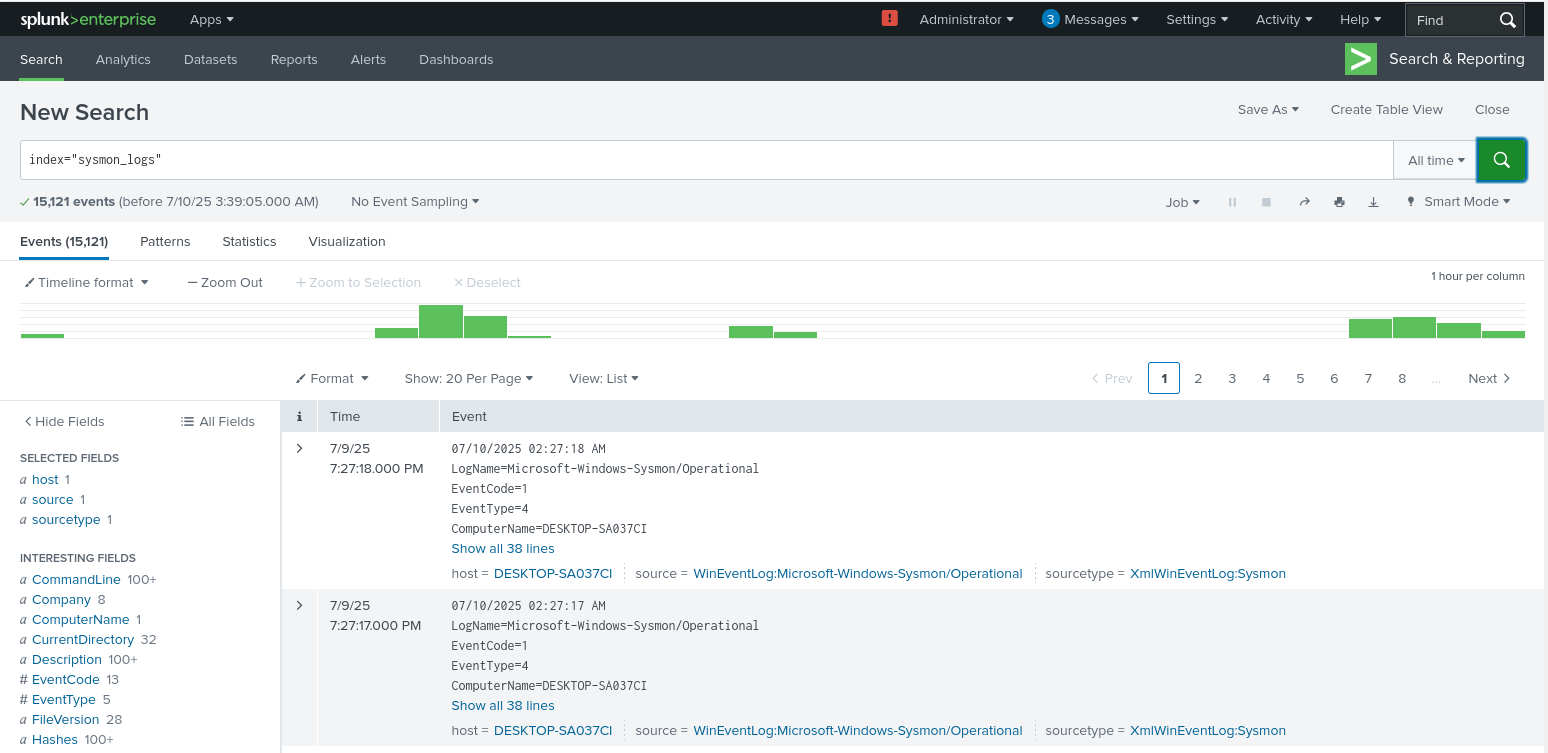
**Thêm dòng sau**



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**

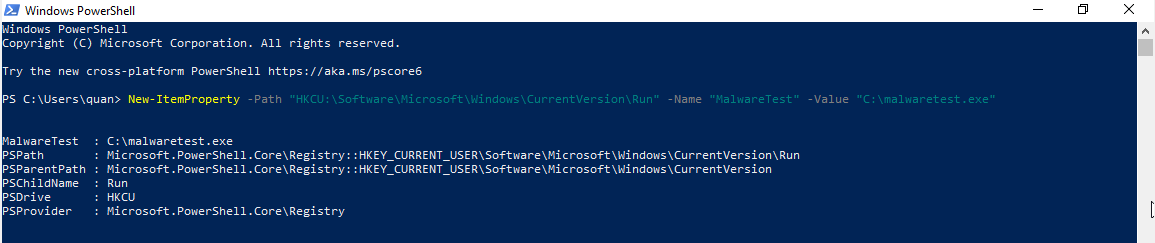


* **Lưu ý:** Nếu Splunk không nhận được log của **Sysmon** mà xem thủ công log của **Sysmon** trên máy Windows vẫn có thì khả năng là do Splunk Forwarder **không chạy bằng Local System Account** nên không đủ quyền đọc log Event Viewer ở Microsoft-Windows-Sysmon/Operational
* **Cách khắc phục:**
  + Kiểm 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 các thay đổi độc hại với Windows Registry**

1. **Thêm một mục persistence giả**

New-ItemProperty -Path "HKCU:\\Software\\Microsoft\\Windows\\CurrentVersion\\Run" -Name "MalwareTest" -Value "C:\\malwaretest.exe"



* **Ý nghĩa:**
  + **Tạo một giá trị (registry value)** có tên là MalwareTest tại key Run trong nhánh HKCU (người dùng hiện tại).
  + Gán giá trị là "C:\\malwaretest.exe".
* **Tác dụng:**
  + Đây là **một kỹ thuật persistence**: mỗi khi người dùng **log in**, Windows sẽ **tự động chạy file C:\\malwaretest.exe**.
  + HKCU:\\Software\\Microsoft\\Windows\\CurrentVersion\\Run là một **Run Key phổ biến** dùng để auto-start chương trình khi đăng nhập.

1. **Sửa đổi một cài đặt bảo mật quan trọng**

Set-ItemProperty -Path "HKLM:\\SYSTEM\\CurrentControlSet\\Services\\Tcpip\\Parameters" -Name "DisableIPSourceRouting" -Value 1



* **Ý nghĩa:**
  + Thay đổi giá trị DisableIPSourceRouting thành 1 trong key Tcpip Parameters của HKLM (toàn bộ hệ thống).
* **Tác dụng:**
  + **Vô hiệu hóa IP source routing**, một kỹ thuật có thể bị lợi dụng để thực hiện **spoofing attack** hoặc **network reconnaissance**.
  + Đây là **một thay đổi cấu hình an ninh mạng ở cấp hệ thống**.

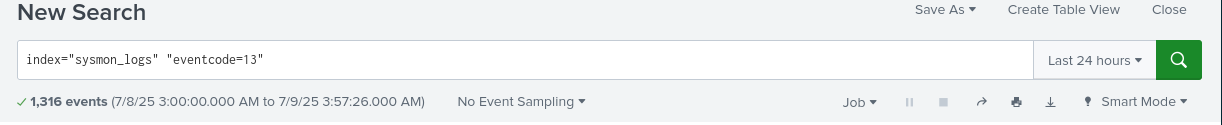
1. **Xóa một khóa registry**

Remove-Item -Path "HKCU:\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\MalwareSimulation"



* **Ý nghĩa:**
  + Xóa giá trị MalwareSimulation trong Run Key của người dùng hiện tại.
* **Tác dụng:**
  + Nếu có một malware đã tạo key này để chạy mỗi khi user đăng nhập, thì lệnh này **xóa bỏ cơ chế persistence đó**.
  + **Defender hoặc analyst** để **gỡ mã độc**
  + Hoặc ngược lại, **malware tự xóa dấu vết** để tránh phát hiện (rare)

**Bước 5: Phân tích Log trên Splunk**



05/17/2025 05:08:22 PM

LogName=Microsoft-Windows-Sysmon/Operational

EventCode=13

EventType=4

ComputerName=DESKTOP-Lab

User=NOT\_TRANSLATED

Sid=

SidType=0

SourceName=Microsoft-Windows-Sysmon

Type=Information

RecordNumber=98315

Keywords=None

TaskCategory=Registry value set (rule: RegistryEvent)

OpCode=Info

Message=Registry value set:

RuleName: T1060,RunKey

EventType: SetValue

UtcTime: 2025-05-17 10:08:22.752

ProcessGuid: {3100}

ProcessId: 3220

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

TargetObject: HKU\\S-33\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\MalwareTest

Details: C:\\malwaretest.exe

User: DESKTOP-Lab\\lab

**Sự kiện thiết lập Registry Run Key – Dấu hiệu tạo persistence**

**📌 Thời gian (UTC):** 2025-05-17 10:08:22

**📌 Thời gian (giờ địa phương):** ~17:08:22

**📌 Hostname:** DESKTOP-Lab

**📌 User thực hiện:** DESKTOP-Lab\lab

**📌 Process thực thi:**

* **Image:** C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe
* **Process ID:** 3220
* **Process GUID:** {3100}

**📌 Hành vi:**

Tiến trình PowerShell đã **tạo hoặc chỉnh sửa một giá trị trong Registry tại vị trí Run Key**, cụ thể:

HKU\\S-33\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\MalwareTest

**📌 Giá trị thiết lập:**

C:\\malwaretest.exe

Điều này đồng nghĩa với việc chương trình malwaretest.exe sẽ **tự động được khởi chạy mỗi khi người dùng đăng nhập**.

**📌 Mô tả kỹ thuật:**

Run Key là một kỹ thuật phổ biến để thiết lập **persistence** – giúp phần mềm hoặc mã độc tự động khởi chạy sau khi khởi động hoặc đăng nhập lại vào hệ thống.

**📌 Mapping MITRE ATT&CK:**

* **Technique ID:** T1060
* **Technique Name:** Registry Run Keys / Startup Folder

**📌 Mức độ nghi vấn:** Cao nếu không rõ mục đích của malwaretest.exe

**📌 Đề xuất điều tra:**

* Kiểm tra tính hợp lệ và mã hash của file C:\\malwaretest.exe.
* Phân tích hành vi của tiến trình này nếu khả nghi.
* Kiểm tra xem hành động này có phải là một phần của mô phỏng tấn công/red team hay không.
* Correlate với các sự kiện khác liên quan đến powershell.exe và registry để xác định mục tiêu hành động.

05/17/2025 08:04:26 PM

LogName=Microsoft-Windows-Sysmon/Operational

EventCode=12

EventType=4

ComputerName=DESKTOP-Lab

User=NOT\_TRANSLATED

Sid=

SidType=0

SourceName=Microsoft-Windows-Sysmon

Type=Information

RecordNumber=100038

Keywords=None

TaskCategory=Registry object added or deleted (rule: RegistryEvent)

OpCode=Info

Message=Registry object added or deleted:

RuleName: T1060,RunKey

EventType: DeleteValue

UtcTime: 2025-05-17 13:04:26.897

ProcessGuid: {3100}

ProcessId: 9440

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

TargetObject: HKU\\S-11\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\MalwareSimulation

User: DESKTOP-Lab\\lab

**Sự kiện xóa Registry Run Key – Khả năng liên quan đến hành vi xóa persistence**

**📌 Thời gian (UTC):** 2025-05-17 13:04:26

**📌 Thời gian (giờ địa phương):** ~20:04:26

**📌 Hostname:** DESKTOP-Lab

**📌 User thực hiện:** DESKTOP-Lab\lab

**📌 Process thực thi:**

* **Image:** C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe
* **Process ID:** 9440
* **Process GUID:** {3100}

**📌 Hành vi:**

Tiến trình PowerShell đã **xóa một giá trị registry tại vị trí Run Key**, cụ thể:

HKU\\S-11\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\MalwareSimulation

**📌 Mô tả kỹ thuật:**

Giá trị tại Registry key trên thường được sử dụng để **thiết lập cơ chế tự động khởi chạy chương trình mỗi khi người dùng đăng nhập vào hệ thống**. Hành vi xóa giá trị này nhiều khả năng là một nỗ lực nhằm **xóa dấu vết hoặc vô hiệu hóa persistence** đã được thiết lập trước đó.

**📌 Mapping MITRE ATT&CK:**

* **Technique ID:** T1060
* **Technique Name:** Registry Run Keys / Startup Folder

**📌 Mức độ nghi vấn:** Trung bình

**📌 Đề xuất:**

* Xác minh xem khóa MalwareSimulation trước đó có được thiết lập bởi phần mềm hợp lệ hay trong quá trình mô phỏng/malware test.
* Xem lại các sự kiện Sysmon Event ID 13 (SetValue) tương ứng để kiểm tra quá trình thiết lập giá trị này.
* Kiểm tra lịch sử hoạt động của người dùng “lab" và xác định có liên quan đến hành vi test hay không.
* Nếu không rõ mục đích, cân nhắc kiểm tra hệ thống thêm để loại trừ hành vi xóa dấu vết của phần mềm độc hại.