VNCER

IR 330: SPLUNK AND SYSMON

**MỤC LỤC**

[Những gì bạn cần cho dự án này 2](#_Toc134431662)

[Mục đích 2](#_Toc134431663)

[Nhiệm vụ 1: Cài đặt Sysmon 2](#_Toc134431664)

[1.1. Sử dụng cấu hình của SwiftOnSecurity 2](#_Toc134431665)

[1.2. Cài đặt Sysmon 3](#_Toc134431666)

[1.3. Tìm hiểu về Sysmon 6](#_Toc134431667)

[1.4. Xem nhật ký Sysmon trong Trình xem Sự kiện 7](#_Toc134431668)

[1.5. Tạo tệp EXE 8](#_Toc134431669)

[1.6. Lọc sự kiện trong Trình xem sự kiện 8](#_Toc134431670)

[1.7. Mở trang quản lý Splunk 10](#_Toc134431671)

[1.8. Thêm dữ liệu Sysmon vào Splunk 12](#_Toc134431672)

[1.9. Xem Sourcetypes của dữ liệu 12](#_Toc134431673)

[Nhiệm vụ 2: Tìm khoảng thời gian tạo tệp quá mức 14](#_Toc134431674)

[2.1. Tìm kiếm sự kiện tạo tệp 14](#_Toc134431675)

[2.2. Đếm sự kiện tạo tệp mỗi phút 15](#_Toc134431676)

[2.3. Tìm kiếm tạo số tệp quá mức 16](#_Toc134431677)

[2.4. Tạo Twelve EXE 17](#_Toc134431678)

[2.5. Tìm kiếm lại để tạo tệp quá mức 17](#_Toc134431679)

[Nhiệm vụ 3: Registry Run Keys 18](#_Toc134431680)

[3.1. Thêm khóa chạy 18](#_Toc134431681)

[3.2. Tìm kiếm sự kiện Sysmon 19](#_Toc134431682)

## Những gì bạn cần cho dự án này

Một máy Windows có cài đặt Splunk, mà bạn đã chuẩn bị trong một dự án trước đó.

## Mục đích

Để giám sát hoạt động hệ thống tệp với sysmon và Splunk. Cảm ơn @rj\_chap đã cho tôi biết về điều này tại CactusCon 2017!

# Nhiệm vụ 1: Cài đặt Sysmon

## Sử dụng cấu hình của SwiftOnSecurity

Theo mặc định, sysmon không đăng nhập thay đổi đăng ký. Chúng tôi sẽ sử dụng một tệp cấu hình từ @SwiftOnSecurity nổi tiếng để khắc phục điều đó.

Trên máy tính Windows của bạn, trong trình duyệt Web, hãy mở trang này:

<https://github.com/SwiftOnSecurity/sysmon-config/blob/master/sysmonconfig-export.xml>

Nhấp chuột phải vào nút Raw, như hình dưới đây và nhấp vào "**Save Target As...**" hoặc **"Save Link As..."** Lưu tệp **sysmonconfig-export.xml** trong thư mục Tải xuống của bạn.

Ảnh chụp màn hình của máy tính

Mô tả được tạo tự động

Hình 1. 1 Sử dụng cấu hình của SwiftOnSecurity

## Cài đặt Sysmon

Mở một cửa sổ trình duyệt Web mới và đi tới

<https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>

Nhấp vào **"Download Sysmon"**. Lưu tệp **Sysmon.zip** trong thư mục **Downloads** của bạn. Ở cuối màn hình nền Windows của bạn, nhấp vào biểu tượng thư mục màu vàng để mở **Windows explorer**. Điều hướng đến **Downloads**. Nhấp chuột phải vào **Sysmon**. Nhấp vào **"Extract All... "**. Nhấp vào **Extract**. Nhấp vào **Start**. Nhập **CMD**. Nhấp chuột phải vào **"Command Prompt "** và nhấp vào **"Run as Administrator"**. Trong hộp Kiểm soát Tài khoản Người dùng, bấm **Yes**. Trong cửa sổ **Command Prompt**, thực hiện các lệnh này, thay thế "student" bằng tên đăng nhập của bạn.

**cd %HOMEPATH%\Downloads\Sysmon**

**sysmon64 -i ..\sysmonconfig-export.xml**

Nếu hộp "Thỏa thuận cấp phép" bật lên, hãy nhấp vào **Agree**.

Sysmon bắt đầu, như hình dưới đây.

A screenshot of a computer

Description automatically generated

Hình 1. 2 Cài đặt Sysmon

Sau khi thực hiện thành công các bước được nếu ra ở trên, bạn hãy sử dụng lệnh “Sysmon.exe -i” để khởi động phần mềm.

A screenshot of a computer

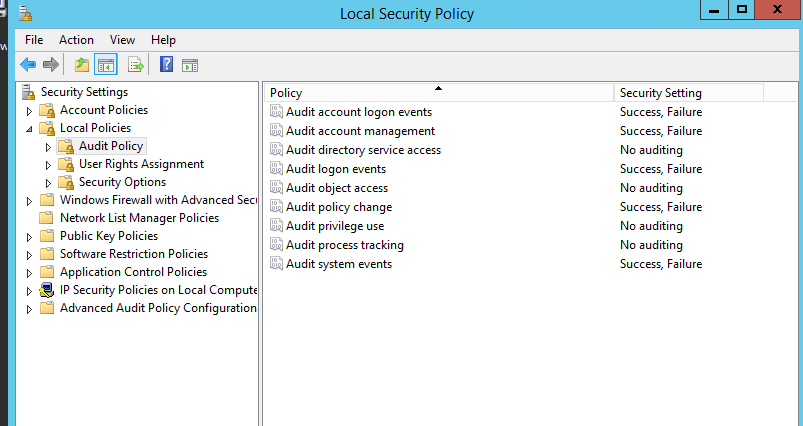
Description automatically generated with medium confidence

Hình 1. 3 Khởi động Sysmon

Tiếp theo bạn sẽ phải đẩy log, ghi log về Windows. Bật Success/Failure audit log tại Administrator Tools → Local security policy → Local Policy → Audit Policy

Audit các trường sau:

* **Audit account logon events**: Sự kiện này bao gồm việc theo dõi các hoạt động đăng nhập của người dùng vào hệ thống. Khi được bật, nó sẽ ghi lại các thông tin như tên đăng nhập, địa chỉ IP, thời gian đăng nhập, thành công hay thất bại, v.v.
* **Audit account management**: Sự kiện này bao gồm việc theo dõi các hoạt động quản lý tài khoản người dùng, chẳng hạn như tạo, xóa, đổi mật khẩu tài khoản. Khi được bật, nó sẽ ghi lại các thông tin như người dùng thực hiện hoạt động này, thời gian, tên tài khoản, v.v.
* **Audit logon events**: Sự kiện này giúp ghi lại thông tin về việc đăng nhập vào hệ thống và các thay đổi về phiên đăng nhập. Nó cũng bao gồm việc ghi lại thông tin về việc đăng nhập thành công hoặc không thành công.
* **Audit policy change**: Sự kiện này ghi lại thông tin về các thay đổi về cấu hình bảo mật hệ thống và các thay đổi liên quan đến chính sách bảo mật. Nó sẽ ghi lại thông tin về người dùng thực hiện thay đổi, thời gian, v.v.
* **Audit privilege use**: Sự kiện này bao gồm việc theo dõi các hoạt động sử dụng các quyền đặc biệt hoặc đặc quyền của người dùng trên hệ thống. Nó giúp đảm bảo rằng các hoạt động này được thực hiện theo đúng quy định và tránh được việc sử dụng đặc quyền một cách lạm dụng hoặc trái phép.
* **Audit system event**: Sự kiện này bao gồm việc ghi lại các hoạt động liên quan đến hệ thống, chẳng hạn như khởi động, tắt, sự cố hệ thống, v.v. Khi được bật, nó giúp theo dõi các sự kiện quan trọng và cung cấp thông tin cho việc phân tích hệ thống.



Hình 1. 4 Bảng Audit Policy

## Tìm hiểu về Sysmon

Sysmon ghi lại các sự kiện cho các sự kiện hệ thống quan trọng. Ba loại sự kiện đầu tiên được hiển thị dưới đây.

**ID sự kiện 1: Tạo quy trình**

Sự kiện tạo quy trình cung cấp thông tin mở rộng về một quy trình mới được tạo. Dòng lệnh đầy đủ cung cấp bối cảnh về thực thi quy trình. Trường ProcessGUID là một giá trị duy nhất cho quá trình này trên một miền để làm cho mối tương quan sự kiện dễ dàng hơn. Các băm là một hàm băm đầy đủ của tệp với các thuật toán trong trường HashType.

**ID sự kiện 2: Một quy trình đã thay đổi thời gian tạo tệp**

Sự kiện thời gian tạo tệp thay đổi được đăng ký khi thời gian tạo tệp rõ rang sửa đổi bởi một quá trình. Sự kiện này giúp theo dõi thời gian tạo thực của một tập tin. Kẻ tấn công có thể thay đổi thời gian tạo tệp của cửa hậu để làm cho nó trông giống như được cài đặt với hệ điều hành. Lưu ý rằng nhiều quy trình thay đổi hợp pháp thời gian tạo một tập tin; nó không nhất thiết chỉ ra hoạt động độc hại.

**ID sự kiện 3: Kết nối mạng**

Sự kiện kết nối mạng ghi lại các kết nối TCP/UDP trên máy. Nó bị vô hiệu hóa theo mặc định. Mỗi kết nối được liên kết với một quy trình thông qua Processld và ProcessGUID cánh đồng. Sự kiện này cũng chứa tên máy chủ nguồn và đích địa chỉ IP, cổng số và trạng thái IPv6.

*Ngoài ra còn có các sự kiện để thay đổi sổ đăng ký (registry).*

## Xem nhật ký Sysmon trong Trình xem Sự kiện

Nhấp vào **Start**. Nhập **EVENT**. Nhấp vào **"Event Viewer".** Trong ngăn bên trái, mở rộng các mục này, như hình dưới đây:

* Applications and Services Logs
* Microsoft
* Windows
* Sysmon

Nhấp vào **Operational**.

Trong ngăn trên giữa, các mục nhật ký được hiển thị, như hình dưới đây:

Ảnh chụp màn hình của máy tính

Mô tả được tạo tự động

Hình 1. 5 Các mục nhật ký

## Tạo tệp EXE

Trong cửa sổ Command Prompt, thực hiện lệnh này:

**echo 1 > ../TEST.EXE**

Trong Trình xem Sự kiện, từ thanh menu, bấm **Action, Refresh**. Nếu máy của bạn không bận lắm, bạn có thể thấy một sự kiện có ID sự kiện 11 và **Task Cetegory** của **"File created...",** như được hiển thị bên dưới:

Ảnh chụp màn hình của máy tính

Mô tả được tạo tự động

Hình 1. 6 Task Cetegory mới

## Lọc sự kiện trong Trình xem sự kiện

Trong Trình xem sự kiện, ở phía bên phải, trong ngăn Hành động, nhấp vào **"Filter Current Log...".**

Trong **"Filter Current Log"**,  ở giữa, hãy nhấp vào trường chứa "<All Event IDs>" và nhập **11** , như minh họa bên dưới.

Sau đó nhấp vào **OK.**

Ảnh chụp màn hình của máy tính

Mô tả được tạo tự động

Hình 1. 7 Hộp Filter Current Log

Nhấp vào sự kiện đầu tiên được tìm thấy. Bạn sẽ thấy chi tiết về tệp **"TEST.EXE"** mà bạn đã tạo, như được hiển thị bên dưới.

|  |
| --- |
| Cờ IR 330.1: Hình ảnh (5 điểm)  Lá cờ được bao phủ bởi một hộp màu xanh lá cây trong hình dưới đây.  Ảnh chụp màn hình của máy tính  Mô tả được tạo tự động  Hình 1. 8 Nơi lá cờ xuất hiện |

## Mở trang quản lý Splunk

Trên máy tính Windows của bạn, mở trình duyệt Web và truy cập URL này: **localhost:8000.** Một trang đăng nhập Splunk xuất hiện, như hình dưới đây.

Ảnh chụp màn hình của máy tính

Mô tả được tạo tự động với độ tin cậy trung bình

Hình 1. 9 Màn hình đăng nhập Splunk

Đăng nhập. Nếu bạn đã làm theo các bước trong dự án trước, thông tin đăng nhập của bạn **admin** và **password**. Nếu bạn bị mất mật khẩu, hãy cài lại Splunk hoặc thử ***hurricanelabs.com/splunk-tutorials/splunk-7-1-performing-a-splunk-password-reset***.

## Thêm dữ liệu Sysmon vào Splunk

Trong trang quản trị Splunk, ở trên cùng bên phải, nhấp vào **Settings**, **"Data inputs"**. Trong danh sách **"Local Inputs"**, nhấp vào **"Local event log collection"**. Trong danh sách **"Available log(s)"**, cuộn xuống và nhấp vào **Microsoft-Windows-Sysmon/Operational**, như hình dưới đây. Sau đó nhấp vào **Save**.

Ảnh chụp màn hình của máy tính

Mô tả được tạo tự động

Hình 1. 10 Thêm dữ liệu Sysmon vào Splunk

## Xem Sourcetypes của dữ liệu

Ở trên cùng bên trái của cửa sổ quản trị Splunk, nhấp vào **splunk**. Bên trên cùng bên trái, nhấp vào **"Search & Reporting".** Tại vị trí giữa bên phải, nhấp vào nút **"Data Summary",** Trong hộp **"Data Summary",** nhấp vào tab **Sourcetypes**. Bạn sẽ thấy một sourcetype của **WinEventLog:Microsoft-Windows-Sysmon/Operational** như hình dưới đây.

Ảnh chụp màn hình của máy tính

Mô tả được tạo tự động

Hình 1. 11 Xem kiểu nguồn dữ liệu

Bấm**.** **WinEventLog:Microsoft-Windows-Sysmon/Operational**

Splunk tìm kiếm và tìm thấy các sự kiện. Thêm **TEST.EXE** vào truy vấn, như được hiển thị bên dưới và nhấp vào biểu tượng kính lúp màu xanh lá cây để chạy lại tìm kiếm.

Splunk tìm thấy sự kiện bạn đã thấy trước đó trong Trình xem sự kiện, như được hiển thị bên dưới.

Ảnh chụp màn hình của máy tính

Mô tả được tạo tự động

Hình 1. 12 Sự kiện trong splunk

# Nhiệm vụ 2: Tìm khoảng thời gian tạo tệp quá mức

## Tìm kiếm sự kiện tạo tệp

Trong trang quản trị Splunk, ở trên cùng bên trái, hãy nhấp vào **splunk**. Nhấp vào **"Search & Reporting".** Nhập thông tin này vào trường "Tìm kiếm mới", như hình dưới đây.

Sau đó nhấp vào biểu tượng kính lúp ở phía bên phải.

**sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational"**

Ở phía dưới bên trái, hãy tìm **EventCode**, được viền màu đỏ trong hình ảnh bên dưới.

Ảnh chụp màn hình của máy tính

Mô tả được tạo tự động

Hình 2. 1 Dữ liệu của EventCode

Nhấp vào **EventCode**. Một hộp bật lên hiển thị các giá trị quan sát được của EventCode, như được hiển thị bên dưới.

Ảnh chụp màn hình biểu đồ

Mô tả được tạo tự động với độ tin cậy thấp

Hình 2. 2 Các giá trị của EventCode

Trong hộp EventCode, trong cột Giá trị, bấm **11**.

Các sự kiện hiển thị việc tạo tệp được tìm thấy, như được hiển thị bên dưới.

Ảnh chụp màn hình của máy tính

Mô tả được tạo tự động

Hình 2. 3 Các sự kiện liên quan đến giá trị 11

## Đếm sự kiện tạo tệp mỗi phút

Trong trường "New Search", nhấp vào cuối truy vấn và nhấn Shift+Enter để di chuyển đến dòng mới.

Sau đó thêm dòng này vào truy vấn, như hình dưới đây.

**| streamstats time\_window=1m count(EventCode)**

Nhấp vào biểu tượng kính lúp ở phía bên phải. Ở phía dưới bên trái, trong phần "Interesting Fields", nhấp vào **count(EventCode)**. Không có nhiều hơn một sự kiện như vậy mỗi phút cho đến nay, như được hiển thị bên dưới.

Ảnh chụp màn hình của máy tính

Mô tả được tạo tự động

Hình 2. 4 Kết quả khi thêm dòng truy vấn mới

## Tìm kiếm tạo số tệp quá mức

Hãy tập trung vào các sự kiện với hơn 10 tệp được tạo mỗi phút. Điều chỉnh truy vấn của bạn để trông như thế này, như được hiển thị bên dưới.

**sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=11**

**| streamstats time\_window=1m count(EventCode) as "new\_EXEs"**

**| search new\_EXEs > 10**

Chạy truy vấn. Không tìm thấy sự kiện phù hợp, như được hiển thị bên dưới.

A screenshot of a computer

Description automatically generated with medium confidence

Hình 2. 5 Không có kết quả phù hợp với lệnh truy vấn

## Tạo Twelve EXE

Trên máy tính Windows của bạn, trong trình duyệt Web, hãy truy cập <https://samsclass.info/50/proj/12EXEs.zip>. Lưu tệp trong thư mục Tải xuống của bạn.

Ở cuối màn hình nền Windows của bạn, nhấp vào biểu tượng thư mục màu vàng để mở Windows explorer. Điều hướng đến Tải xuống.

Nhấp chuột phải vào 12files và nhấp vào **"Extract All... "**. Nhấp vào **Extract.**

## Tìm kiếm lại để tạo tệp quá mức

Trong trang quản trị Splunk, nhấp vào biểu tượng kính lúp ở phía bên phải. Bây giờ các sự kiện được tìm thấy. Trong sự kiện đầu tiên, nhấp vào **"Show all 22 lines".** Thông tin đầy đủ về apears sự kiện, như hình dưới đây.

|  |
| --- |
| Cờ IR 330.2: Tên tệp mục tiêu (10 điểm)  Lá cờ được bao phủ bởi một hộp màu xanh lá cây trong hình dưới đây.  Ảnh chụp màn hình của máy tính  Mô tả được tạo tự động  Hình 2. 6 Lá cờ được dấu |

# Nhiệm vụ 3: Registry Run Keys

## Thêm khóa chạy

Trên máy tính Windows của bạn, bấm **Start**. Nhập **regedit** Trong kết quả tìm kiếm, bấm **regedit**. Trong hộp Kiểm soát Tài khoản Người dùng, bấm **Yes**.

Trong Registry Editor, trong ngăn bên trái, điều hướng đến khóa này, như được hiển thị bên dưới.

**HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run**

Trong ngăn bên phải, nhấp chuột phải vào khoảng trống và nhấp vào **New, " String Value",** như hình dưới đây.

Ảnh chụp màn hình của máy tính

Mô tả được tạo tự động

Hình 3. 1 Tạo giá trị mới

Một giá trị mới xuất hiện, với tên của nó được tô sáng. Nhập tên, nhập **BADPROG** như hình dưới đây. Nhấn phím **Enter**.

Ảnh chụp màn hình của máy tính

Mô tả được tạo tự động

Hình 3. 2 Nhập tên cho giá trị mới

Đóng Regedit.

## Tìm kiếm sự kiện Sysmon

Trong Splunk, thực hiện tìm kiếm này:

**sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" Registry**

|  |
| --- |
| Cờ IR 330.3: Tên tệp mục tiêu (5 điểm)  Tìm EventCode hiển thị tên của khóa Run mới.  Đó là lá cờ. |