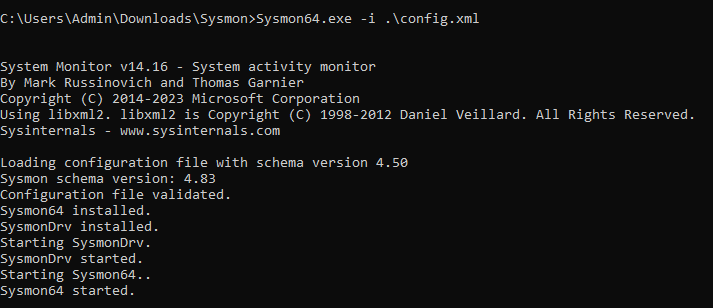
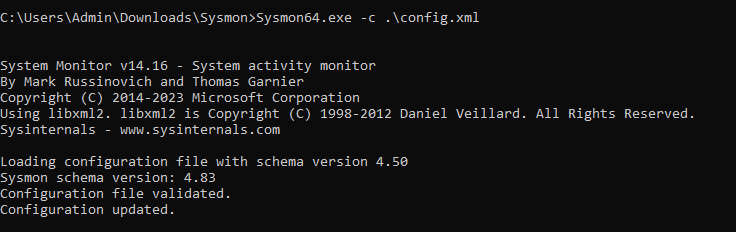
1. cài đặt sysmom

cài đặt file thực thi: https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

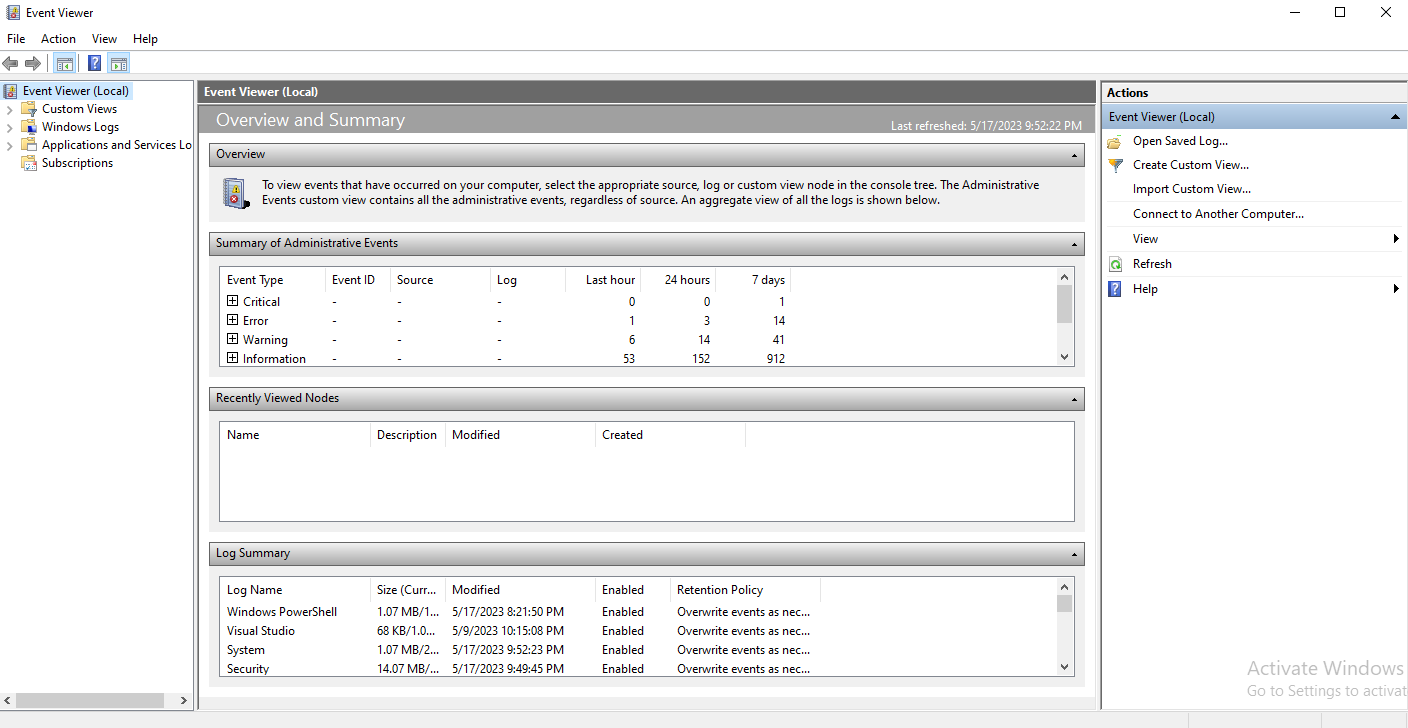
cài đặt file cấu hình: <https://github.com/SwiftOnSecurity/sysmon-config>



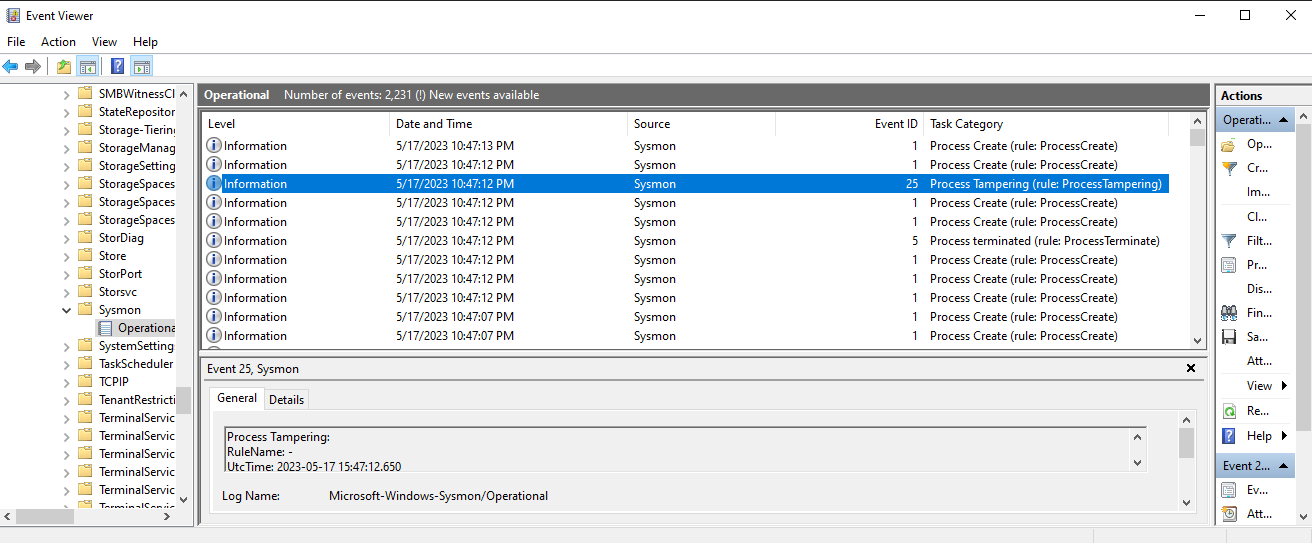


1. Sử dụng sysmon để phát hiện process injection

Open even view



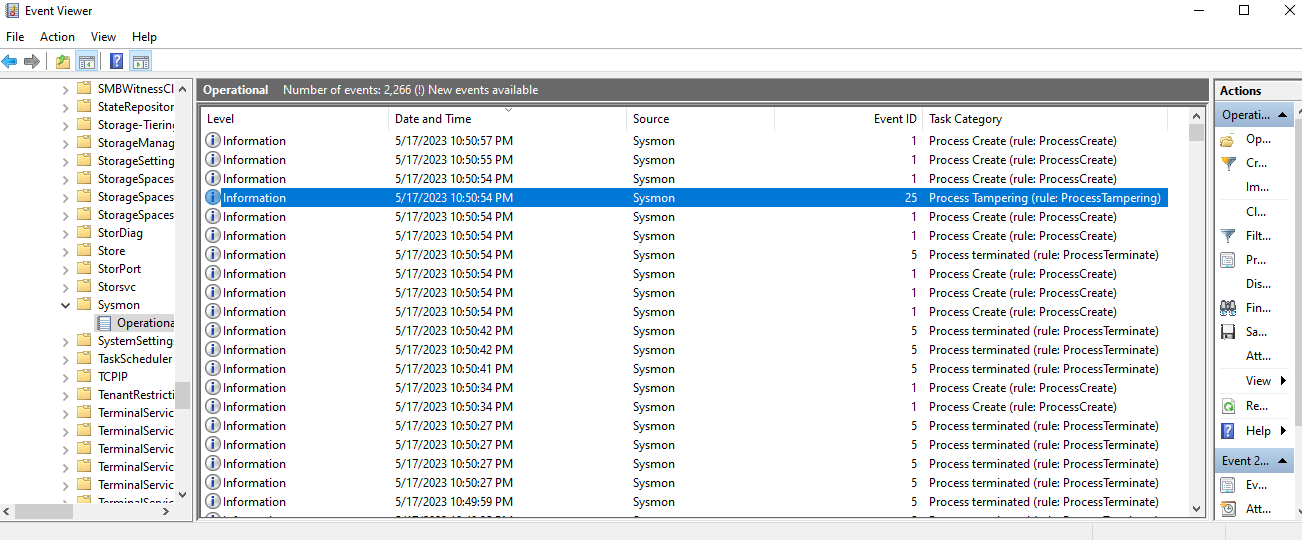
Truy cập: “Applications and Services Logs/Microsoft/Windows/Sysmon/Operational”

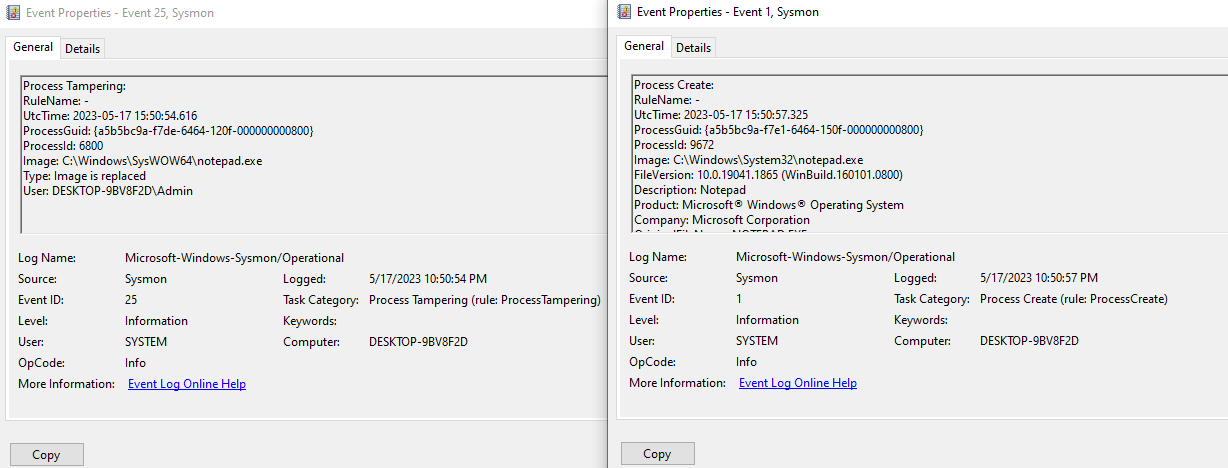


Giao diện chính của sysmon

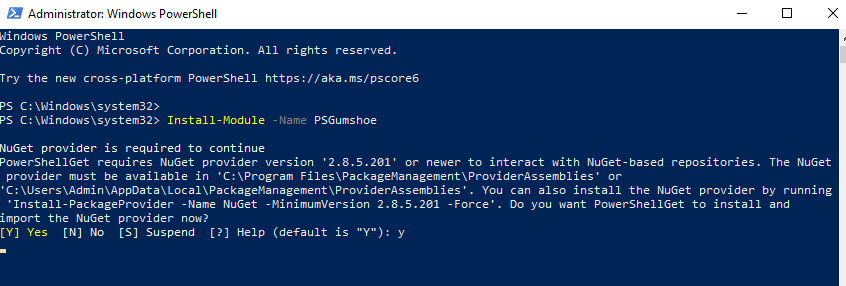
Bây giờ chạy file độc hại đã đề cập ở tuần trước ( sử dụng kĩ thuật process hollowing với file mục tiêu là notepad.exe) và mở notepad.exe bình thường

Quan sát ta thấy sysmon đã nhận diện được tiến trình giả mạo

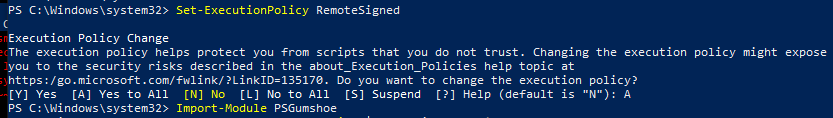


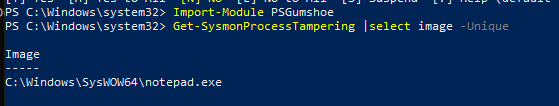


Cài đặt PowerShell Module PSGumShoe



Set policy nếu cần





<https://www.bleepingcomputer.com/news/microsoft/microsoft-sysmon-now-detects-malware-process-tampering-attempts/>

<https://pentestlaboratories.com/tag/windows-defender/>

<https://www.researchgate.net/publication/354323005_Windows_Memory-Injected_Malware_Detection_Freeware_Comparison>