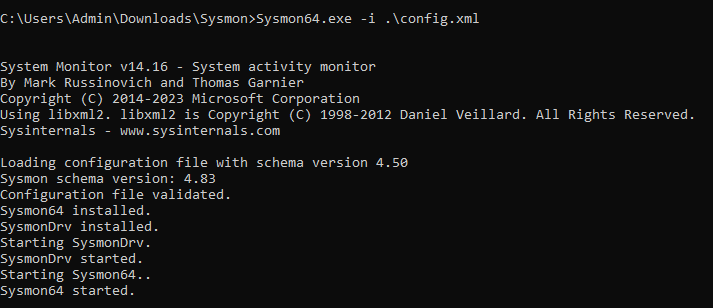
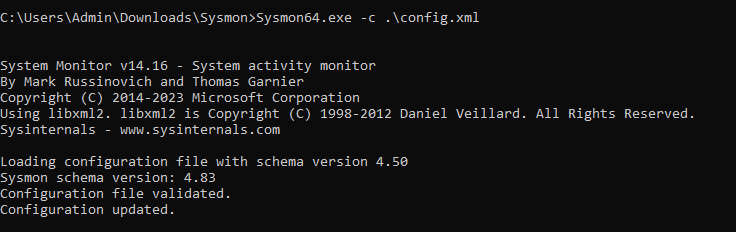
1. cài đặt sysmom

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>





<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>