|  |
| --- |
| 1. Hiển thị thông tin các tiến trình:   Process Explorer: <https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer> |
| 1. Xác định các chương trình chạy tự động:   Autoruns: <https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns> |

|  |
| --- |
| 1. Theo dõi hoạt động của Malware   Process Monitor: <https://learn.microsoft.com/en-us/sysinternals/downloads/procmon> |
| 1. Xác định xem tiến trình nào đang sinh ra hoạt động mạng tương ứng   TCPview: <https://learn.microsoft.com/en-us/sysinternals/downloads/tcpview> |

|  |
| --- |
| 1. Kiểm tra dữ liệu mã độc đã gửi và nhận   Wireshark: <https://www.wireshark.org/download.html> |
| 1. Báo cáo các lỗ hổng tiềm ẩn phát sinh trong cài đặt phần mềm: Chụp hệ điều hành và so sánh trước và sau khi cài đặt ứng dụng khác   Attack Surface Analyzer: <https://github.com/microsoft/attacksurfaceanalyzer> |