Lê Ngọc Kiều Anh

MSSV: 22520047

**BÀI TẬP AN TOÀN MẠNG MÁY TÍNH BUỔI 8**

**Câu 1: Nêu các biện pháp phòng chống Trojan, sắp xếp theo thứ tự các biện pháp quan trọng từ cao đến thấp.**

**Các biện pháp phòng chống Trojan theo mức độ quan trọng từ cao đến thấp:**

1. **Cập nhật bảo mật và cài đặt bản cập nhật hệ điều hành và ứng dụng:** đảm bảo rằng các lỗ hổng bảo mật mới được khắc phục, giúp giảm thiểu nguy cơ bị tấn công.
2. **Cài đặt phần mềm diệt virus, tường lửa, và hệ thống phát hiện xâm nhập (IDS)**: đảm bảo có lớp bảo vệ chủ động để phát hiện và ngăn chặn mã độc hoặc xâm nhập trái phép.
3. **Giám sát lưu lượng mạng nội bộ để phát hiện các cổng hoặc lưu lượng mã hóa bất thường:** phát hiện sớm các hoạt động bất thường có thể giúp ngăn chặn các mối đe dọa tiềm ẩn.
4. **Hạn chế quyền truy cập khi dùng máy tính để bàn:** giới hạn quyền giúp ngăn chặn cài đặt phần mềm độc hại.
5. **Quản lý tính toàn vẹn của hệ thống thông qua kiểm tra tổng kiểm tra, kiểm tra bảo mật và quét cổng:** đảm bảo tính toàn vẹn của hệ thống giúp phát hiện thay đổi bất thường hoặc nguy cơ.
6. **Chặn các cổng không cần thiết tại máy chủ và tường lửa:** giảm khả năng xâm nhập từ bên ngoài thông qua việc giới hạn các cổng truy cập.
7. **Tăng cường cài đặt cấu hình mặc định và tắt các chức năng không sử dụng:** ngăn chặn các lỗ hổng có thể bị khai thác qua các tính năng không cần thiết.
8. **Quét đĩa CD và DVD bằng phần mềm diệt virus trước khi sử dụng:** đảm bảo các phương tiện ngoại vi không mang theo phần mềm độc hại vào hệ thống.
9. **Tránh mở các tập tin đính kèm trong email từ người gửi không xác định:** biện pháp quan trọng nhưng có thể thực hiện được nếu người dùng có kiến thức bảo mật.
10. **Tránh nhận các chương trình chuyển qua tin nhắn:** hạn chế rủi ro từ các phần mềm độc hại truyền qua các ứng dụng nhắn tin.
11. **Tránh tải và thực thi các ứng dụng từ nguồn không đáng tin cậy:** ngăn chặn các nguy cơ từ các nguồn không xác minh.
12. **Tránh chạy các chương trình hoặc tập lệnh có sẵn:** ngăn ngừa việc thực hiện mã độc từ các nguồn không đáng tin cậy.

**Câu 2: Cho biết công dụng và cách sử dụng một số công cụ sau: Netstat, Fport, TCPView, CurrPorts Tool, Process Explorer ( hoặc công cụ khác có chức năng tương tự ). So sánh sự khác biệt giữa các công cụ này.**

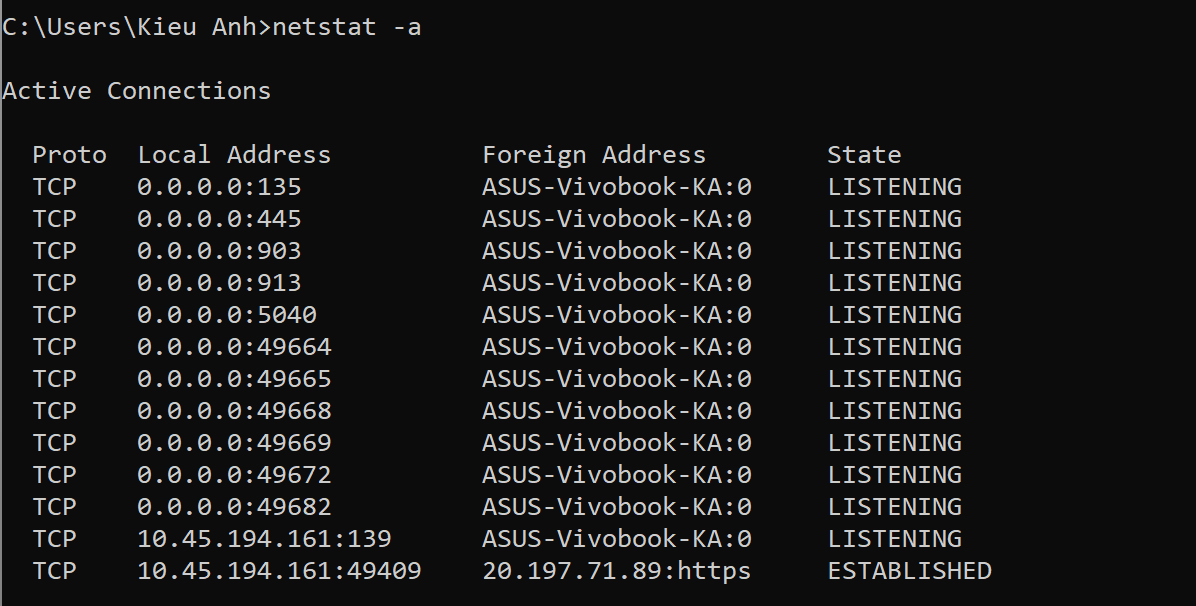
* **Netstat**

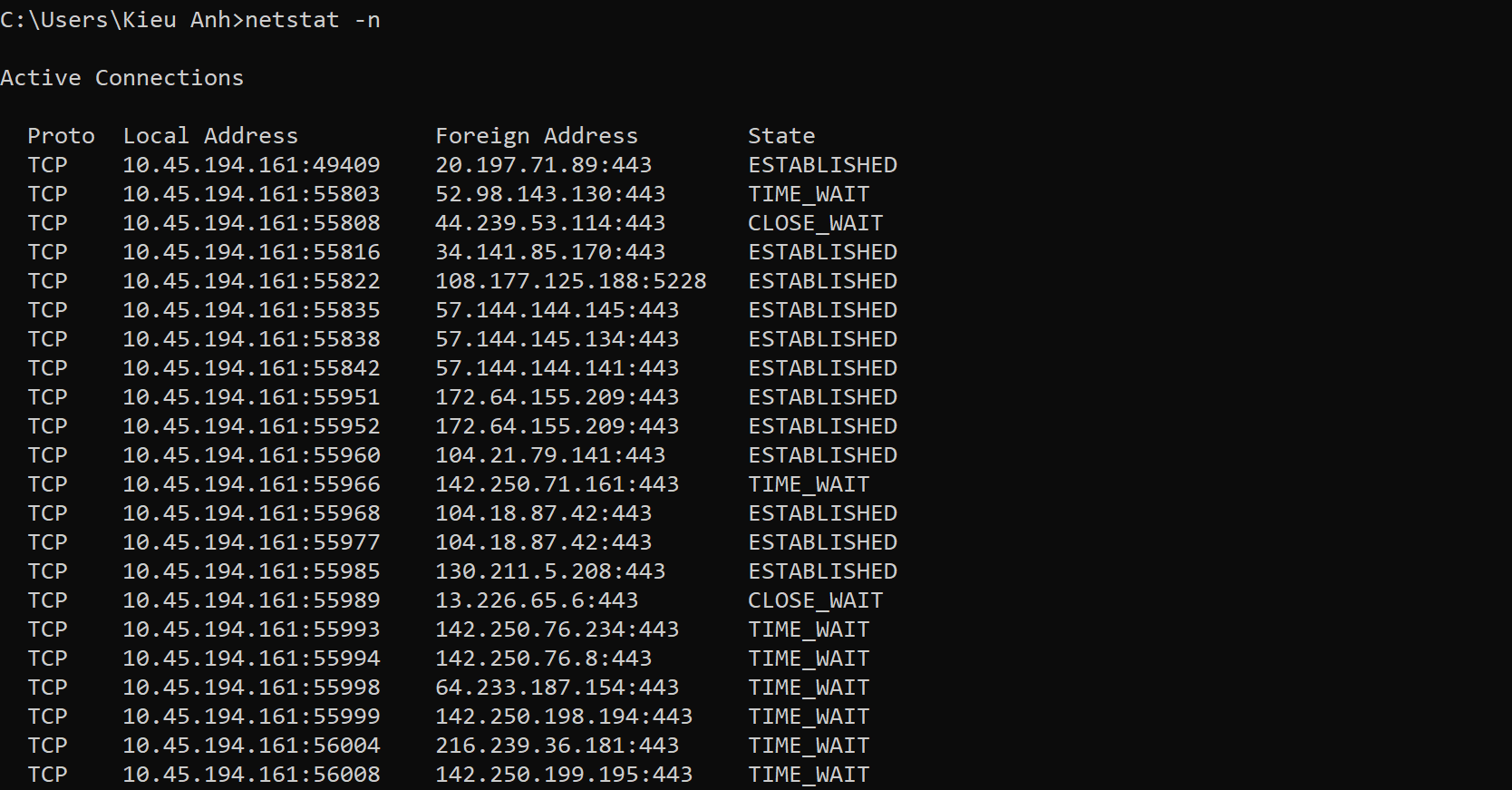
**Công dụng:** Netstat (Network Statistics) là một tiện ích dòng lệnh tích hợp sẵn trong hệ điều hành Windows, Linux, và macOS. Nó cung cấp thông tin về các kết nối mạng đang hoạt động, bao gồm địa chỉ IP, cổng kết nối, trạng thái kết nối và các dịch vụ tương ứng.

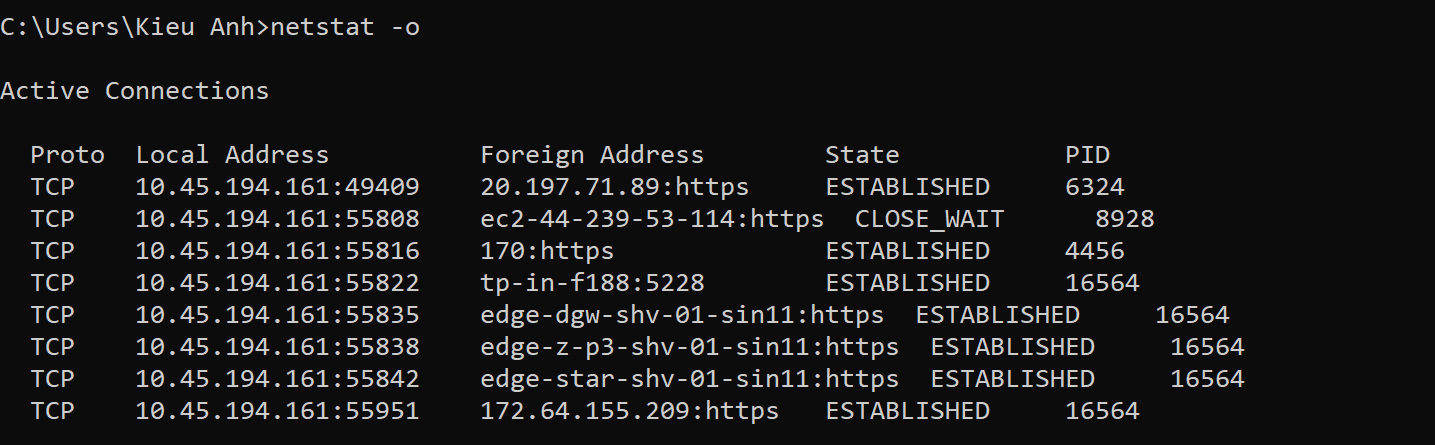
**Cách sử dụng:**

**-** Mở Command Prompt (trên Windows) hoặc Terminal (trên Linux/macOS).

- Sử dụng các lệnh như netstat -a để xem tất cả các kết nối, netstat -n để hiển thị địa chỉ IP dưới dạng số thay vì tên miền, hoặc netstat -o để hiển thị ID tiến trình (PID) tương ứng.

****

****

****

* **TCPView**

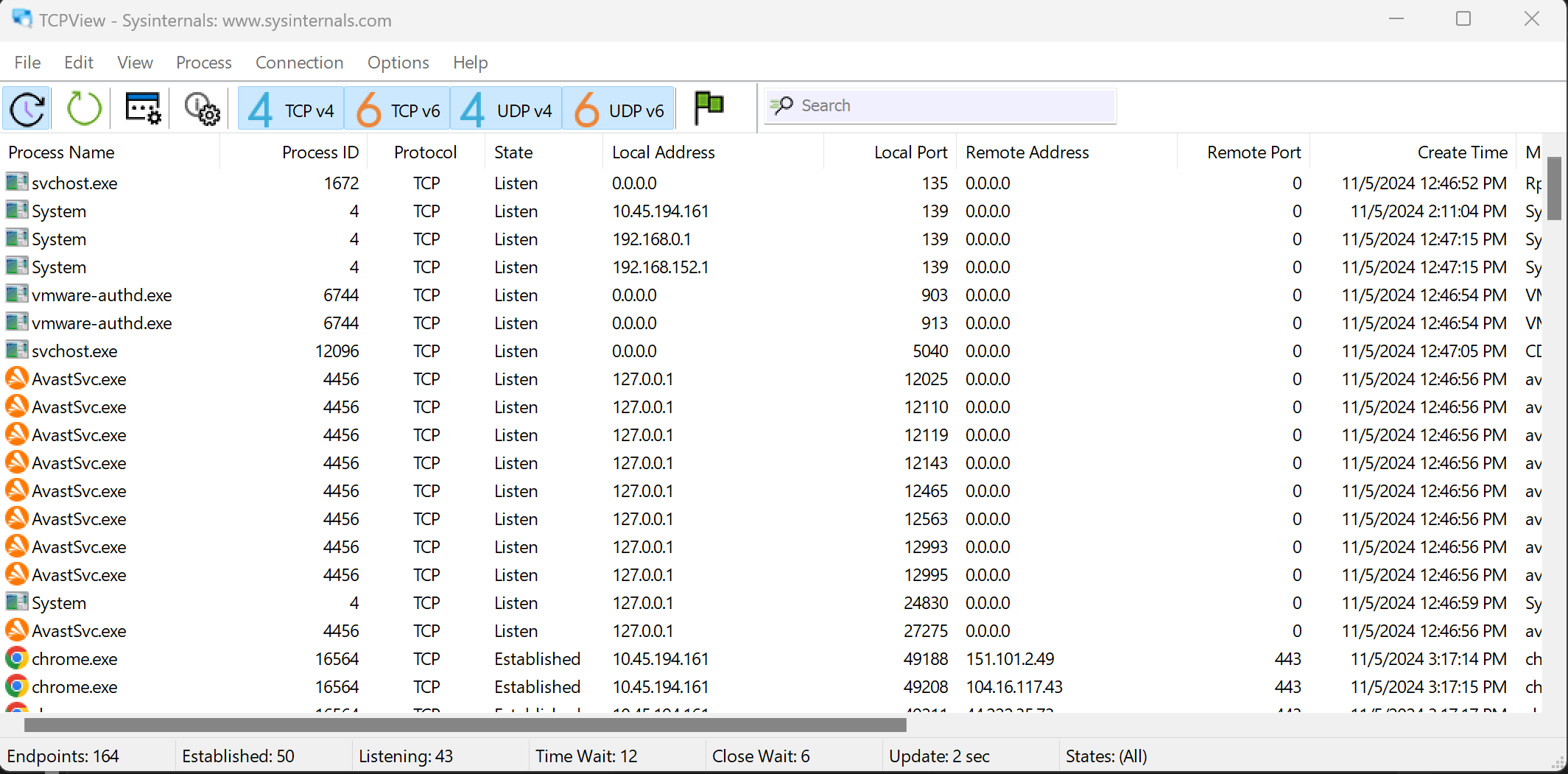
**Công dụng:** TCPView là một công cụ của Sysinternals (Microsoft), cung cấp giao diện đồ họa để giám sát các kết nối TCP và UDP đang mở. Nó hiển thị địa chỉ IP, tên quy trình, và trạng thái kết nối, giúp phát hiện các kết nối đáng ngờ dễ dàng hơn.

**Cách sử dụng:**

- Tải TCPView từ Sysinternals và khởi chạy.

- Giao diện sẽ hiển thị danh sách các kết nối mạng đang hoạt động theo thời gian thực.

Người dùng có thể chọn ngắt kết nối hoặc đóng quy trình ngay từ giao diện TCPView.

****

* **CurrPorts Tool**

**Công dụng:** CurrPorts là một công cụ của NirSoft giúp liệt kê tất cả các cổng mạng đang mở (TCP/UDP) trên hệ thống và ánh xạ chúng đến các quy trình đang chạy. Công cụ này hiển thị chi tiết về mỗi kết nối, như địa chỉ IP, tên tiến trình, và đường dẫn tiến trình.

**Cách sử dụng:**

- Tải CurrPorts từ trang web của NirSoft và khởi chạy (không cần cài đặt).

- Giao diện hiển thị các kết nối mạng đang hoạt động và các chi tiết liên quan. Có thể chọn đóng kết nối hoặc dừng quy trình nếu phát hiện hoạt động nghi ngờ.

* **Process Explorer**

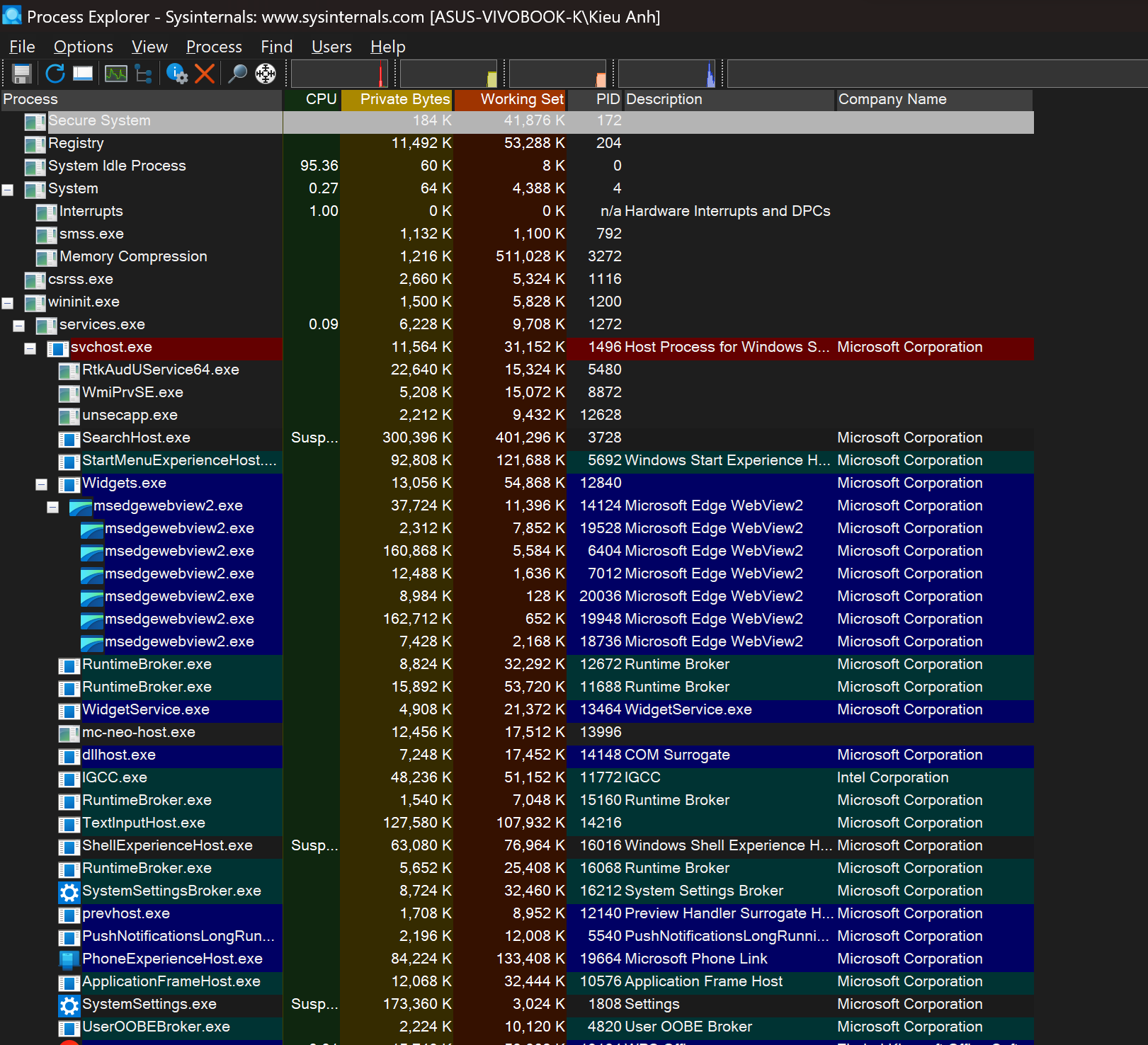
**Công dụng:** Process Explorer (cũng của Sysinternals) là một công cụ thay thế Task Manager trên Windows, hiển thị chi tiết về các quy trình đang chạy, bao gồm thông tin về cổng mạng và kết nối.

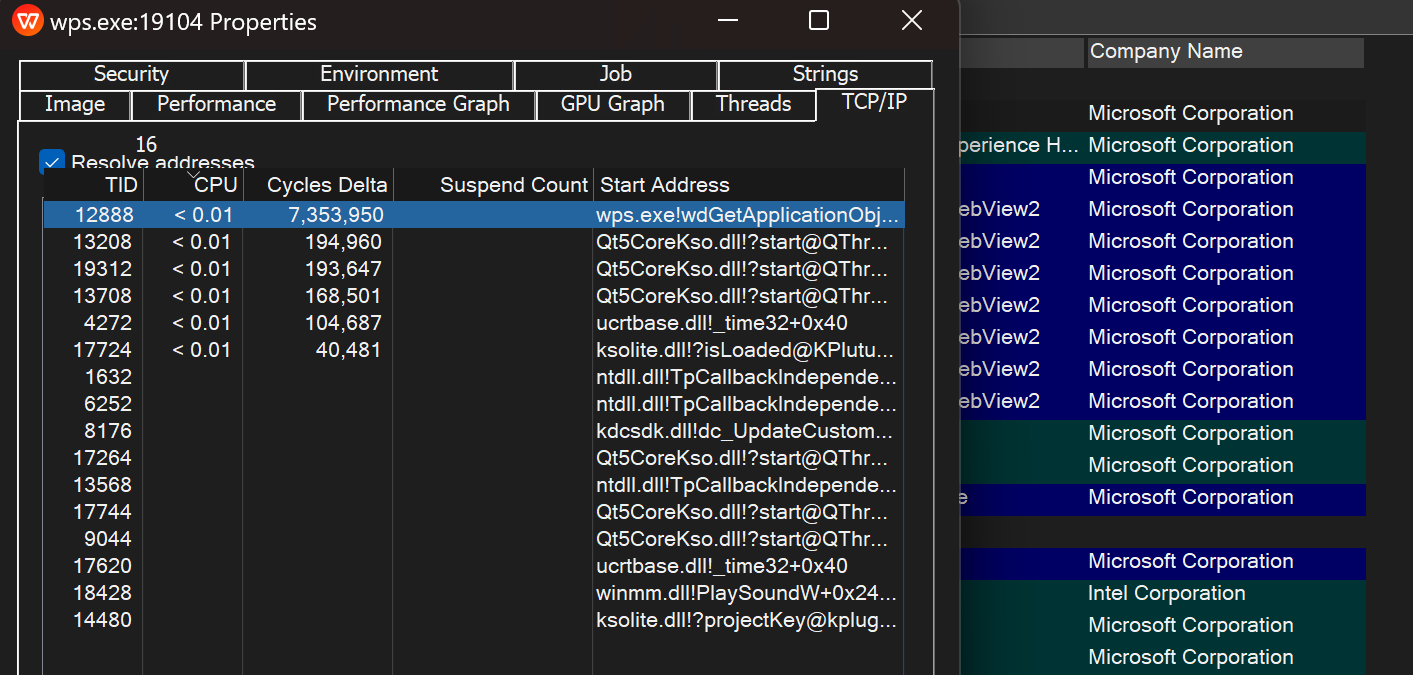
**Cách sử dụng:**

- Tải Process Explorer từ Sysinternals và mở ứng dụng.

- Giao diện hiển thị tất cả các quy trình đang chạy cùng các chi tiết như ID quy trình, mức độ sử dụng CPU và bộ nhớ, cùng các thư viện DLL liên quan.

- Người dùng có thể chọn quy trình để xem chi tiết về các cổng đang mở hoặc dừng quy trình nếu cần.

****

****

**Điểm khác nhau giữa các công cụ:**

* **Netstat:** Tích hợp sẵn, không cần cài đặt, không có giao diện đồ họa, cần lệnh để thao tác.
* **Fport:** chỉ hỗ trợ Windows cũ, tập trung vào việc hiển thị ứng dụng sử dụng các cổng.
* **TCPView:** Chỉ có trên Windows, giao diện đồ họa, trực quan hơn, cho phép ngắt kết nối hoặc dừng quy trình ngay từ giao diện.
* **CurrPorts Tool:** chỉ hỗ trợ Windows, cung cấp thông tin chi tiết và có bản portable không cần cài đặt.
* **Process Explorer:** chỉ có trên Windows, đầy đủ chức năng quản lý quy trình, hiển thị DLL và kết nối mạng, có thể thay thế Task Manager.

**Câu 3: Tìm kiếm 3-5 loại Trojan mới xuất hiện trong thời gian gần đây. Lập bảng mô tả các Trojan đó (Tên, nguồn gốc, đặc điểm, cổng xâm nhập, biện pháp phòng chống, nguồn tham khảo,…)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Tên Trojan** | **Nguồn gốc** | **Đặc điểm** | **Cổng xâm nhập** | **Biện pháp phòng chống** | **Nguồn tham khảo** |
| **Lumma** | Nga | Stealer Trojan, thu thập thông tin đăng nhập và dữ liệu nhạy cảm từ trình duyệt và phần mềm. | Email lừa đảo, mạng xã hội | Cập nhật phần mềm bảo mật, không mở liên kết không xác định. | <https://any.run/cybersecurity-blog/malware-trends-report-q3-2024/> |
| **AsyncRAT** | Chưa có thông tin | Kiểm soát từ xa hệ thống, chủ yếu qua các email lừa đảo và liên kết độc hại. | TCP (kết nối máy chủ điều khiển) | Sử dụng firewall chặn kết nối lạ, kiểm tra tính hợp pháp của email. | <https://www.bleepingcomputer.com/> |
| **Latrodectus** | Chưa có thông tin | Downloaderthực thi các lệnh từ máy chủ C2, tránh né môi trường ảo hóa. | Email lừa đảo, file độc hại | Thận trọng với email và liên kết đáng ngờ, cài đặt phần mềm diệt virus. | <https://www.proofpoint.com/us/blog/threat-insight/latrodectus-spider-byt> |
|  |