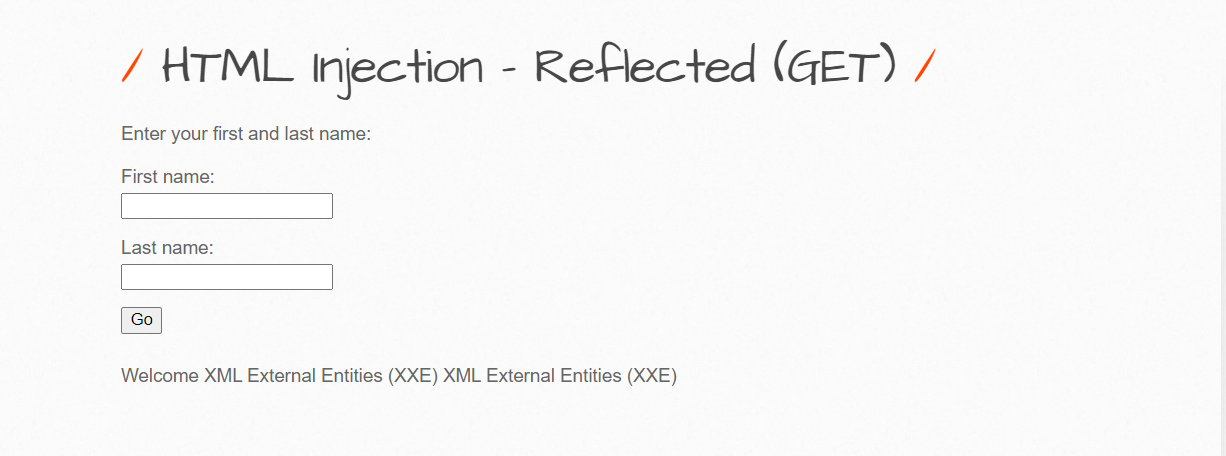
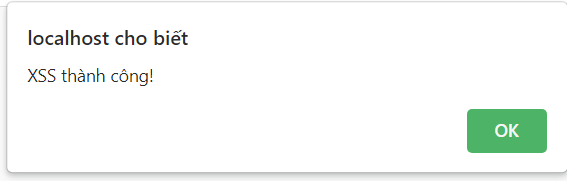
Huỳnh Gia Tuấn-HTTT2311009

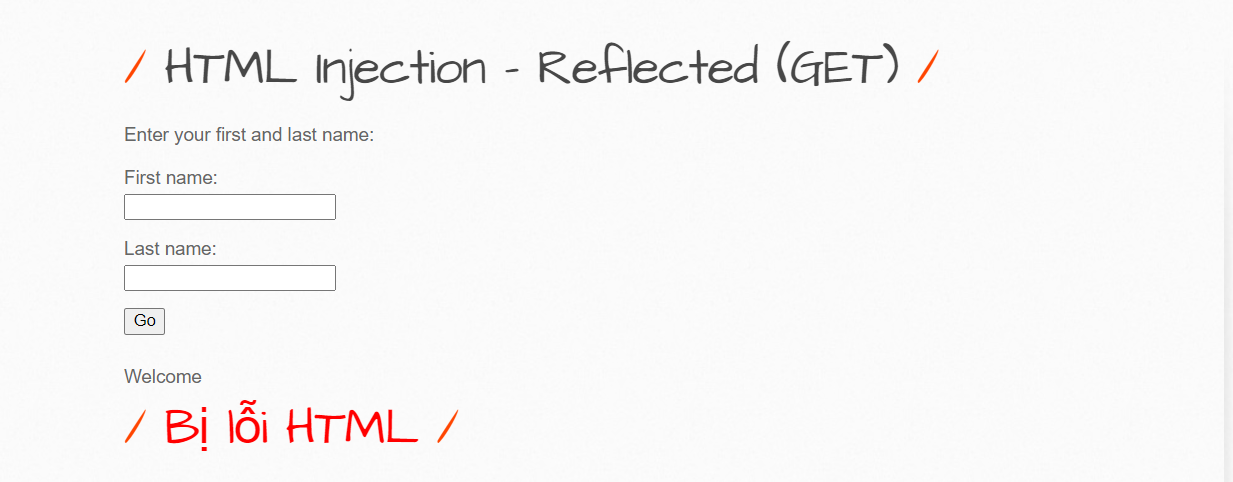




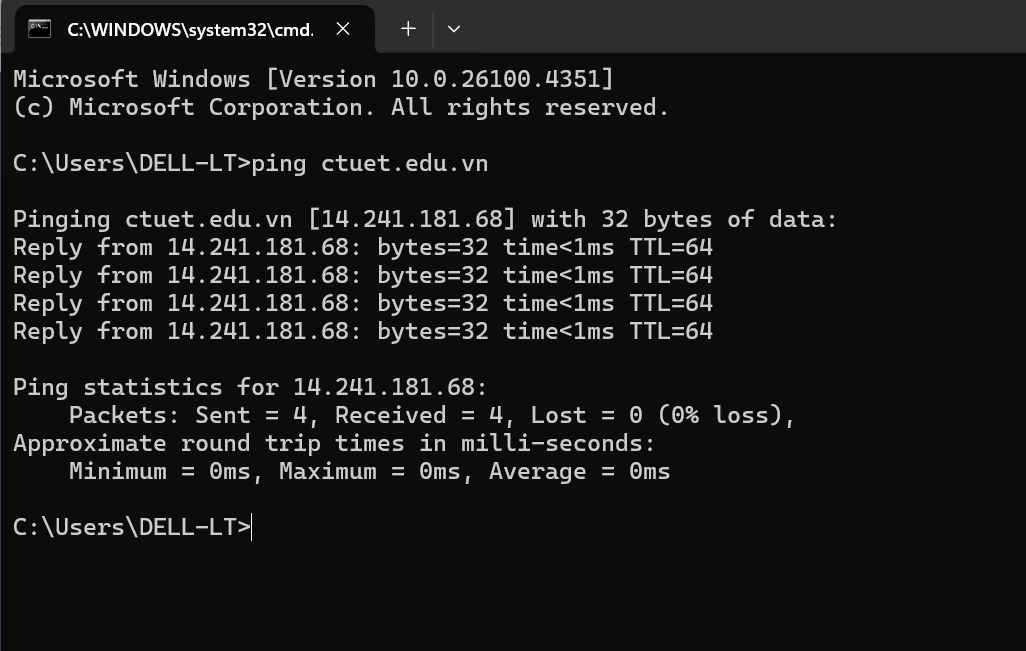




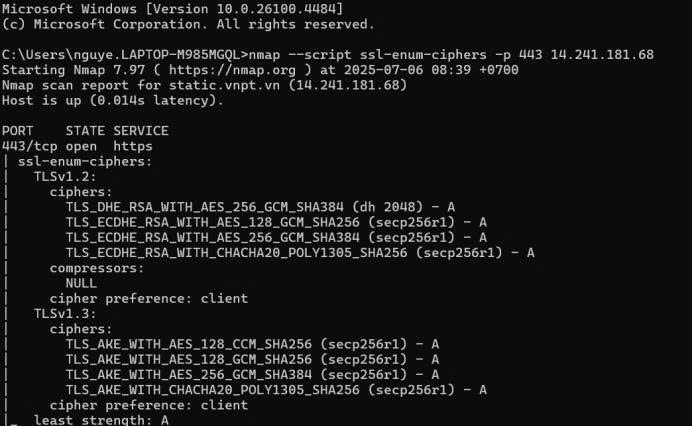




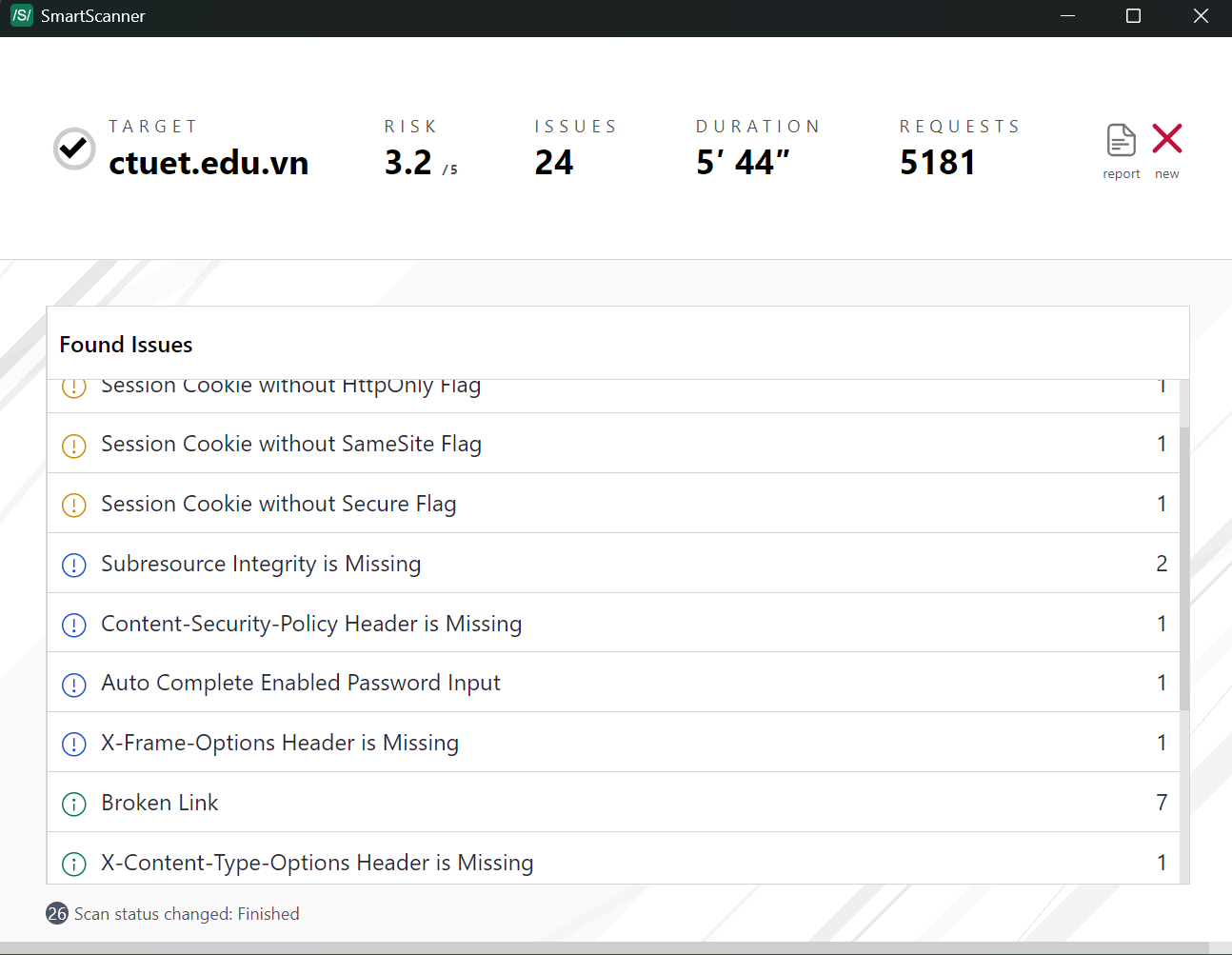
BÀI THỰC HÀNH 2



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STT** | **Điểm yếu bảo mật** | **Mô tả** | **Mức độ nghiêm trọng (Critical, High, Medium, Low)** | **Công cụ sử dụng** |
| 1 | Lộ thông tin máy chủ | Thông tin cấu hình máy chủ cho phép hacker đánh giá năng lực xử lý, từ đó đưa ra phương án tấn công. | Low | ping, nmap, shodan |
| 2 | |  | | --- | |  |  |  | | --- | | **Cổng mở dịch vụ từ xa (RDP, Winbox, SSH)** | | Các cổng như 3389 (RDP), 8291 (Winbox), 22 (SSH - filtered) đang mở ra internet có thể bị lợi dụng. | Medium | nmap -sS -sV, shodan |
| 3 | Dịch vụ UDP công khai (NTP, DHCP) | Các cổng UDP 123 (NTP), 67/68 (DHCP) mở có thể dẫn đến khai thác DDoS hoặc rò rỉ thông tin mạng nội bộ. | |  | | --- | | Medium |  |  | | --- | |  | | nmap -sUV, shodan |



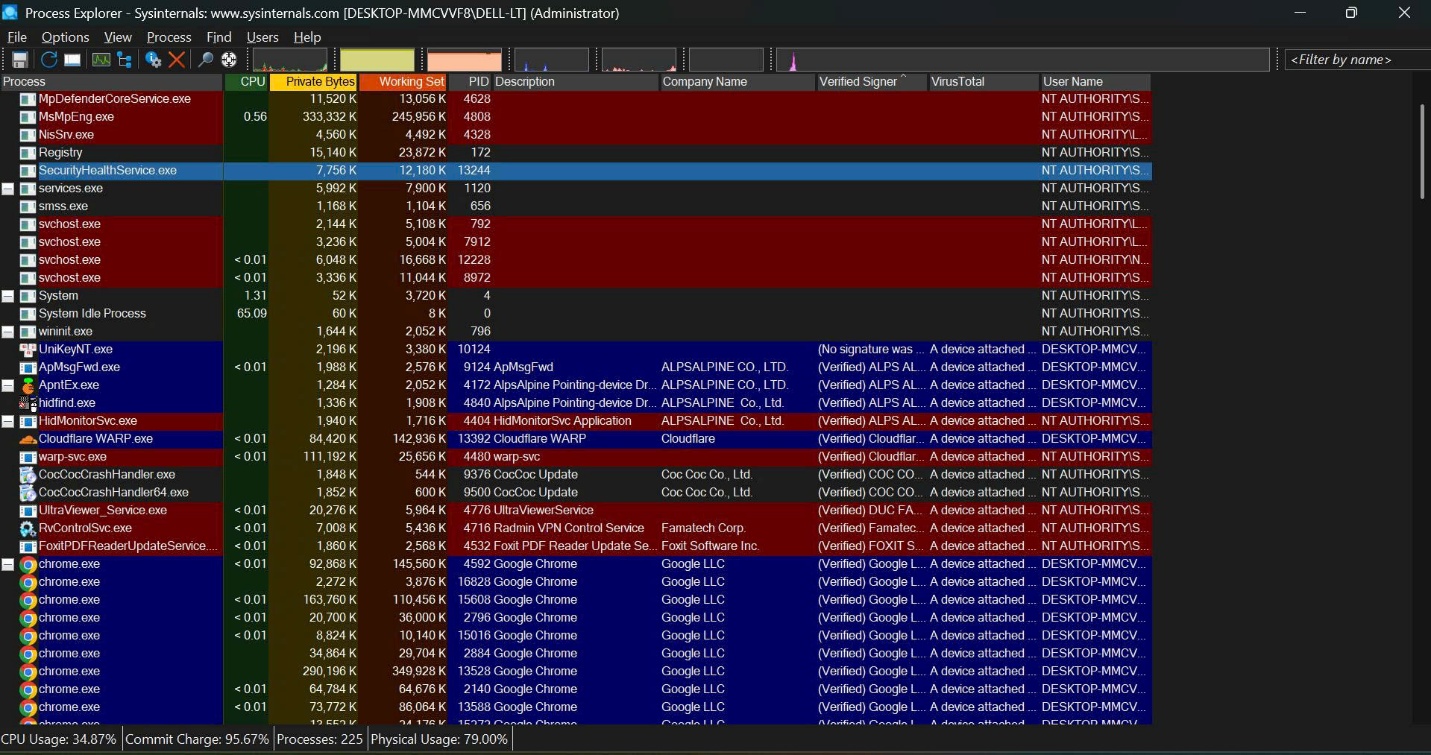
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Điểm yếu bảo mật** | **Mô tả** | **Mức độ nghiêm trọng (Critical, High, Medium, Low)** | | **Công cụ sử dụng** | | --- |  |  | | --- | |  | |
| **1** | |  | | --- | | **Cấu hình mã hóa HTTPS** |  |  | | --- | |  | | |  | | --- | | **Máy chủ hỗ trợ TLS 1.2 và TLS 1.3 với các thuật toán mã hóa mạnh (cấp độ A). Không phát hiện cipher yếu hay cấu hình rủi ro.** |  |  | | --- | |  | | **Low** | **nmap --script ssl-enum-ciphers** |

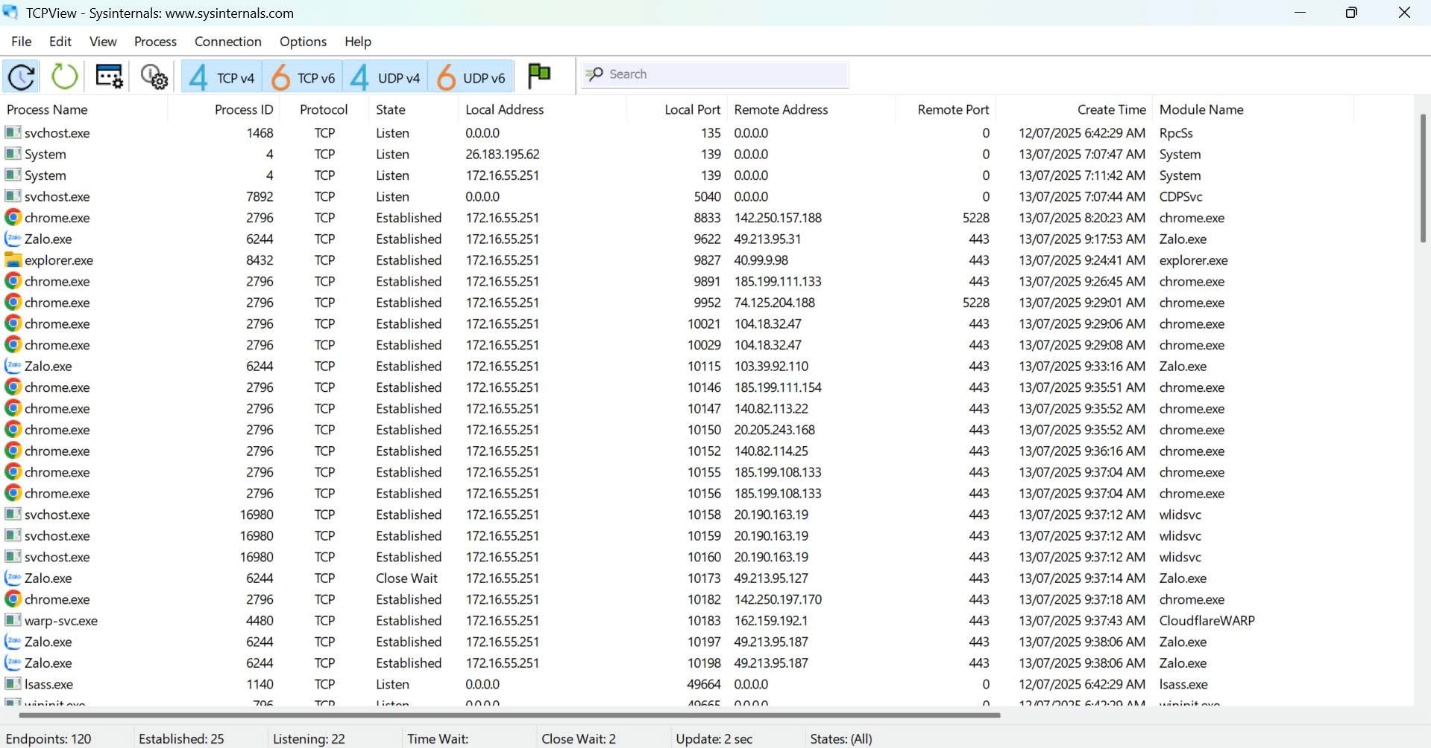


| **STT** | **Điểm yếu bảo mật** | **Mô tả** | **Mức độ nghiêm trọng** | **Công cụ sử dụng** |
| --- | --- | --- | --- | --- |
| 3 | Session Cookie thiếu HttpOnly | Cookie không có cờ HttpOnly, khiến JavaScript có thể truy cập, dễ bị tấn công XSS. | Medium | SmartScanner |
| 4 | Session Cookie thiếu SameSite | Cookie không có thuộc tính SameSite, có thể bị tấn công CSRF. | Medium | SmartScanner |
| 5 | Session Cookie thiếu Secure | Cookie không có cờ Secure, có thể bị rò rỉ nếu kết nối không mã hóa. | Medium | SmartScanner |
| 6 | Thiếu Subresource Integrity (SRI) | Các tệp từ bên thứ ba không có mã kiểm tra toàn vẹn, dễ bị thay thế script độc hại. | Low | SmartScanner |
| 7 | Thiếu Content-Security-Policy Header | Không kiểm soát nguồn tài nguyên trang web tải về, dễ bị XSS hoặc chèn nội dung độc. | High | SmartScanner |
| 8 | Tự động điền mật khẩu (autocomplete) | Trường mật khẩu cho phép trình duyệt tự động điền, tiềm ẩn nguy cơ bị khai thác khi bị chiếm quyền điều khiển trình duyệt. | Medium | SmartScanner |
| 9 | Thiếu X-Frame-Options Header | Không hạn chế iframe nhúng, dễ bị clickjacking. | Medium | SmartScanner |
| 10 | Broken Link | Có nhiều liên kết trên trang web bị hỏng (404, không tồn tại). | Low | SmartScanner |
| 11 | Thiếu X-Content-Type-Options Header | Không ngăn trình duyệt đoán kiểu nội dung, dễ bị tấn công kiểu MIME sniffing. | Low | SmartScanner |

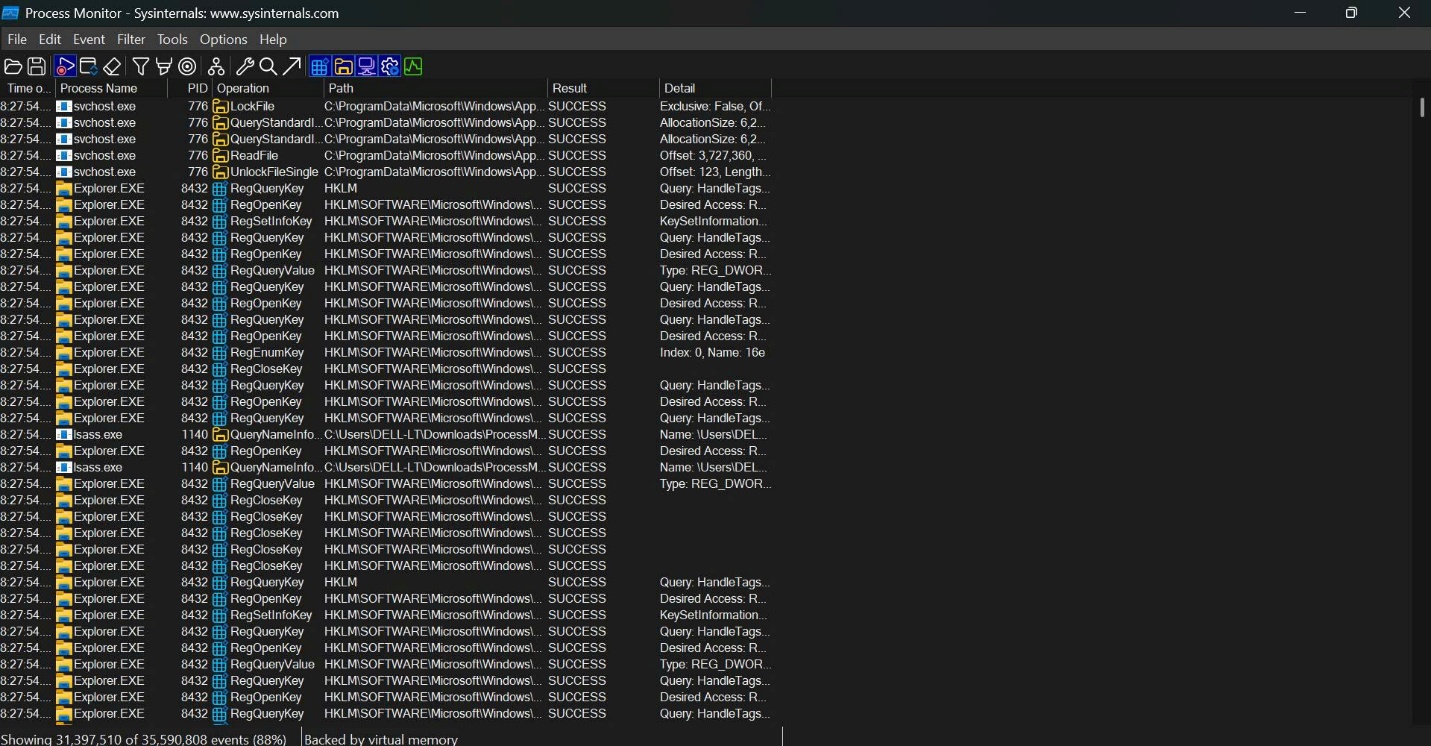
Bài thực hành 3

Process Explorer



Autoruns

Process Monitor



TCPview:

