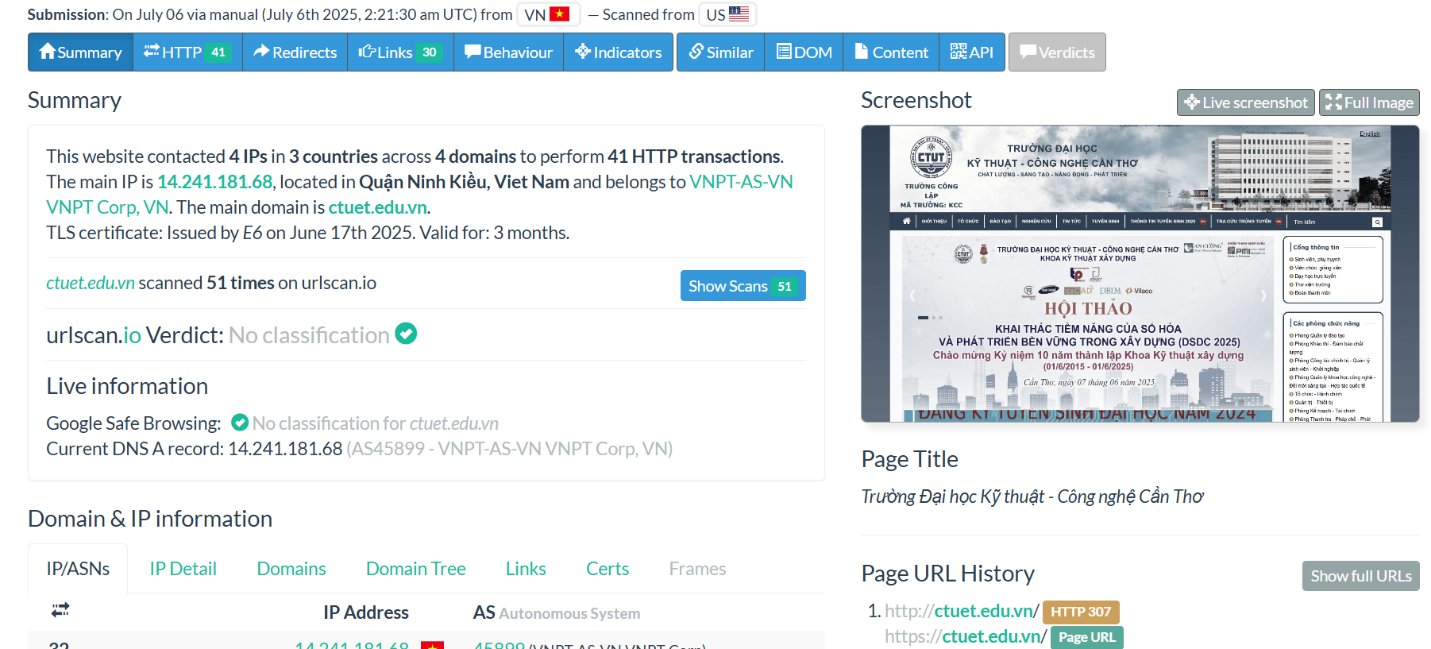
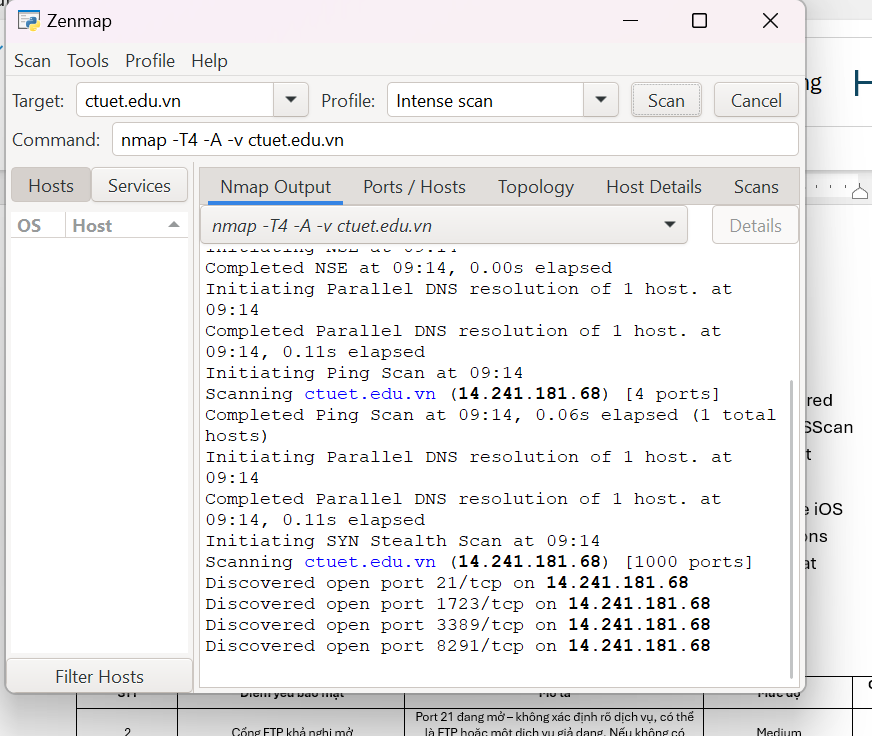
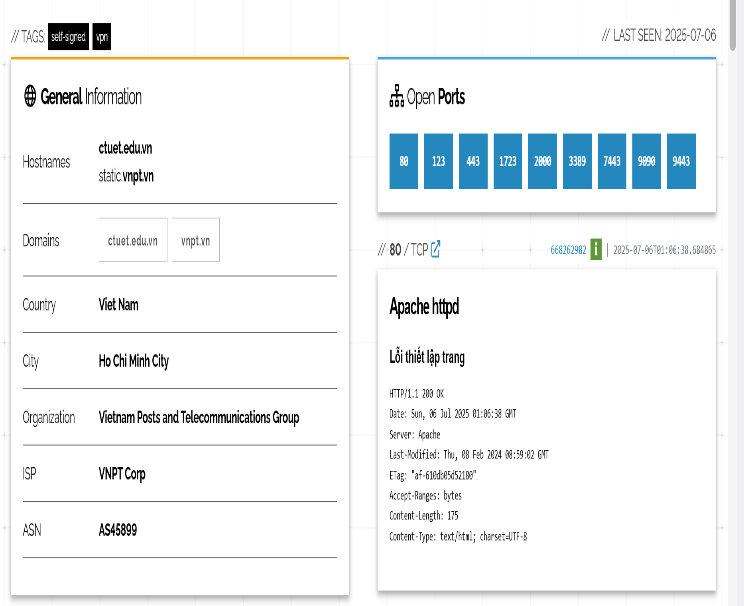
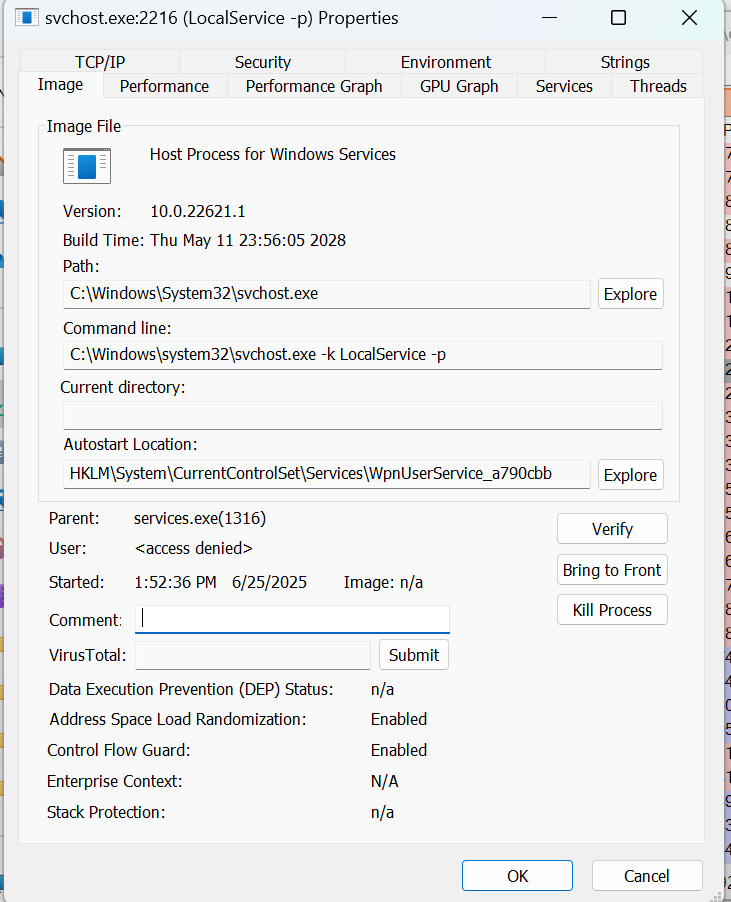
**Bài thực hành 2:**

****

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **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 của máy chủ, từ đó đưa ra một số phương án tấn công | Low | thực hiện URL: |
| 2 | Dịch vụ FTP công kha |  | | Cổng 21 mở – nếu không có cấu hình xác thực bảo mật hoặc SSL thì dễ bị khai thác bằng brute force hoặc sniffing thông tin đăng nhập. | Medium | Nmap |
| 3 | Web Server |  | | Máy chủ chạy HTTP (port 80) và HTTPS (port 443) – cần kiểm tra kỹ phiên bản và các plugin để phát hiện lỗ hổng như XSS, SQLi, RCE, v.v. | Medium | Nmap |
|  | | | Tổng số lỗ hổng: 0 ;Critical: 0 ; High: 0 ; Medium: 0; Low: 1 | | | |

**Bài thực hành 3:**

1. Hiển thị thông tin các tiến trình:



| **Thuộc tính** | **Giá trị** |
| --- | --- |
| **Tên tiến trình** | **svchost.exe (Host Process for Windows Services)** |
| **Đường dẫn** | **C:\Windows\System32\svchost.exe ✅** |
| **Command Line** | **C:\Windows\System32\svchost.exe -k LocalService -p ✅** |
| **Autostart Location** | **HKLM\SYSTEM\CurrentControlSet\Services\WpnUserService\_a790cbb ✅** |
| **Parent** | **services.exe ✅** |
| **User** | **<access denied> ⚠️ (do không mở Process Explorer bằng quyền admin)** |
| **Chế độ bảo vệ** | **ASLR, Control Flow Guard đều Enabled ✅** |
| **Thời gian khởi chạy** | **1:52 PM ngày 25/6/2025** |
| **VirusTotal** | **Chưa kiểm tra (chưa submit) ❌** |

|  |  |
| --- | --- |
| **✅ Đường dẫn chuẩn** | **C:\Windows\System32\svchost.exe là chính xác, nếu không phải chỗ này thì nguy hiểm** |

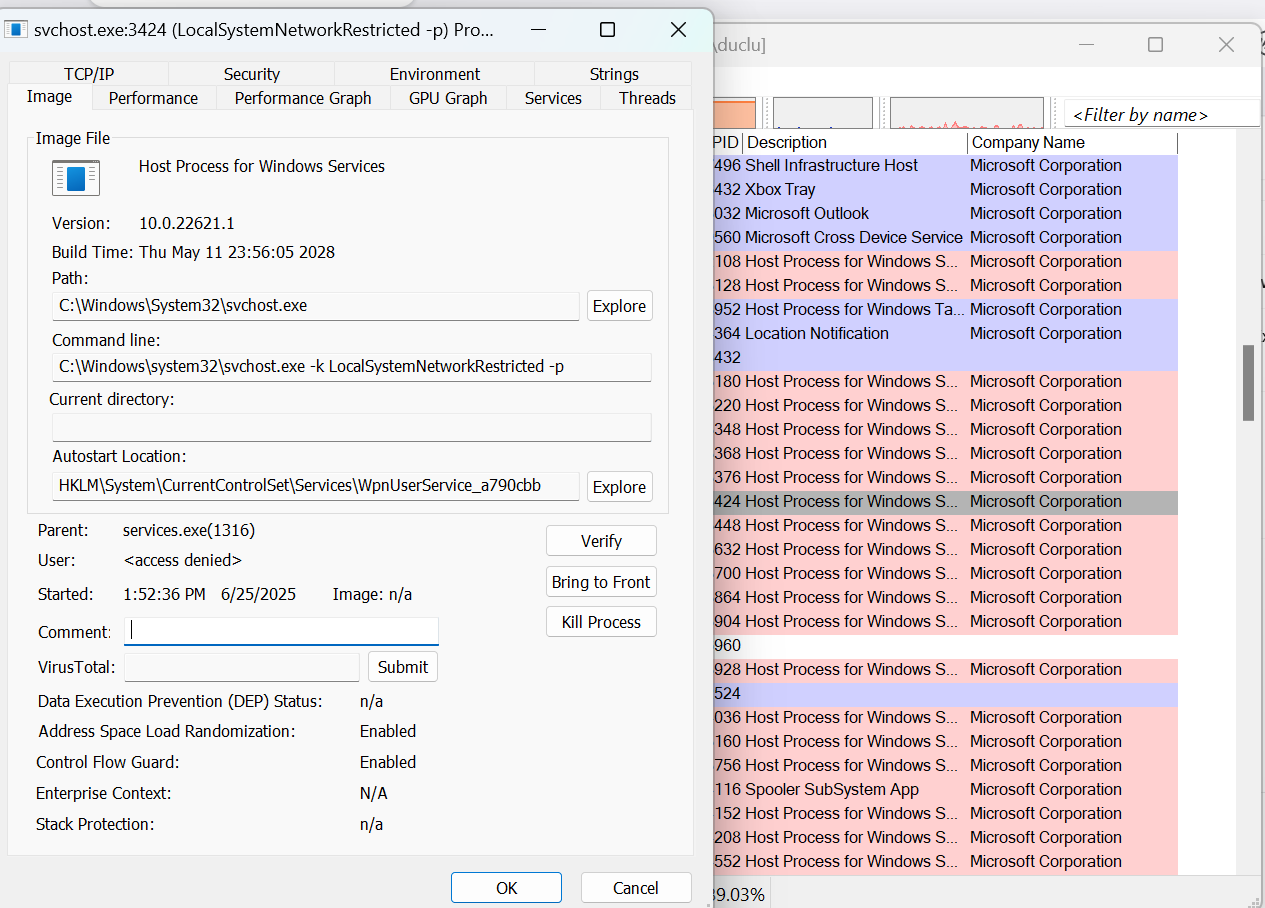
|  |  |
| --- | --- |
| **✅ Parent là services.exe** | **Phù hợp với tiến trình hệ thống** |

|  |  |
| --- | --- |
| **✅ Tham số dòng lệnh** | **-k LocalService -p là thông số chuẩn** |

|  |  |
| --- | --- |
| **✅ Registry Autostart** | **WpnUserService là dịch vụ thông báo đẩy của Windows, hợp lệ** |

|  |  |
| --- | --- |
| **⚠️ Access Denied** | **Chưa mở bằng quyền admin – bạn nên chạy Process Explorer với quyền Administrator để xem hết thông tin** |

|  |  |
| --- | --- |
| **❌ Chưa kiểm tra VirusTotal** | **Bạn nên tick vào VirusTotal (Options > VirusTotal.com > Check) để thấy tỷ lệ nghi ngờ** |

****

|  |  |
| --- | --- |
| **📁 Đường dẫn** | **C:\Windows\System32\svchost.exe** |
| **🧬 Command Line** | **svchost.exe -k LocalSystemNetworkRestricted -p → Chạy theo nhóm dịch vụ LocalSystemNetworkRestricted** |
| **🧩 Tự động khởi động từ registry** | **HKLM\System\CurrentControlSet\Services\WpnUserService\_a790cbb (liên quan đến dịch vụ thông báo đẩy Windows)** |
| **🧑‍💻 Tài khoản thực thi** | **LocalSystemNetworkRestricted** |
| **🧷 Quyền truy cập** | **Có dòng "access denied" → hạn chế truy cập thông tin tài khoản từ user không đủ quyền** |
| **🧭 Thời điểm khởi chạy** | **13:52:36 ngày 25/6/2025** |
| **📌 Thuộc tính bảo mật** | **Đã bật Address Space Load Randomization và Control Flow Guard → các biện pháp chống tấn công khai thác bộ nhớ** |

Ý nghĩa và cách hiểu đơn giản

* Tiến trình này thuộc về hệ thống, không phải virus hoặc phần mềm bên thứ ba.
* Vì nó thực hiện các dịch vụ quan trọng như thông báo hệ thống, bạn không nên kết thúc tiến trình này thủ công.
* Việc "access denied" là bình thường nếu bạn không có quyền quản trị cao nhất.

1. **Xác định các chương trình chạy tự động:**

****

| **DLL** | **Đường dẫn** | **Trạng thái** |
| --- | --- | --- |
| **wow64cpu.dll** | **C:\Windows\Syswow64\...** | **❌ File not found** |
| **wowarmhw.dll** | **C:\Windows\system32\... và Syswow64** | **❌ File not found** |
| **xtajit.dll** | **C:\Windows\system32 và Syswow64** | **❌ File not found** |
| **wow64.dll, wow64base.dll, wow64con.dll, wow64win.dll** | **Syswow64** | **❌ File not found** |
| **xtajit64.dll** | **system32 và Syswow64** | **❌ File not found** |
| **Tất cả mục hiển thị đều báo “File not found” → Có nghĩa là Windows đang trỏ tới các tệp DLL không còn tồn tại trên ổ đĩa.** |  |  |