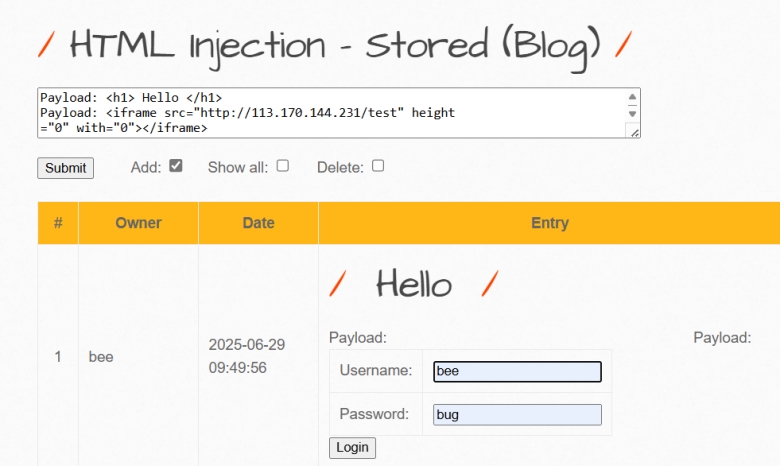
***Thực hành lab1***

***Injection***

******

***HTML injection – Stored***

******

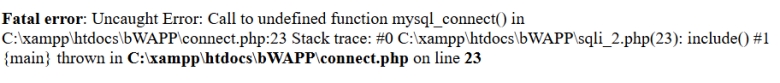
***PHP code injection***

******

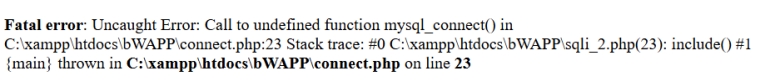
***OS Command injection***

******

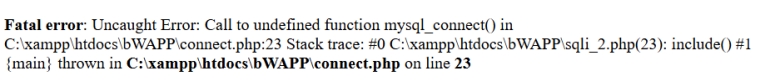
***SQL injection (Get/Search)***

******

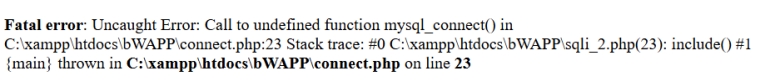
***SQL injection (Get/Select)***

******

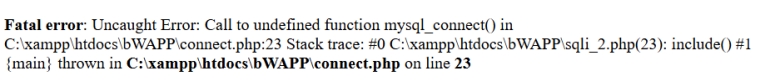
***SQL injection (Post/Search)***

******

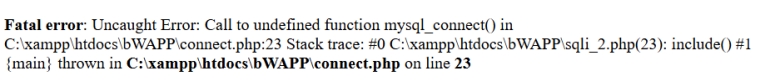
***SQL injection (Post/Select)***

******

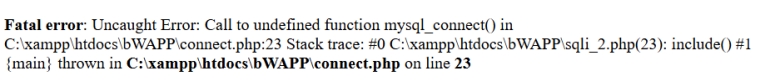
***SQL injection (Captcha)***

******

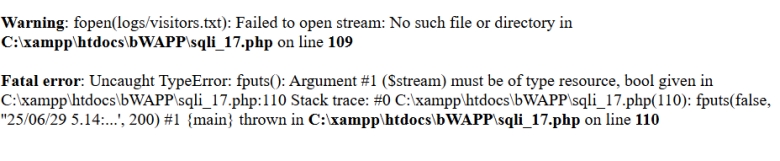
***SQL injection (Login Form/Hero)***

******

***SQL injection - Stored (Blog)***

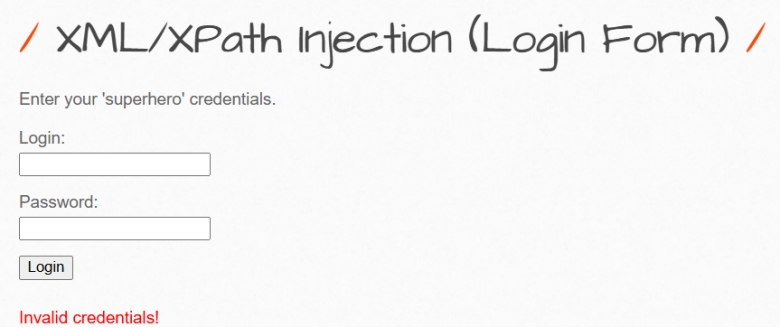
******

***SQL injection - Stored (User-Agent)***

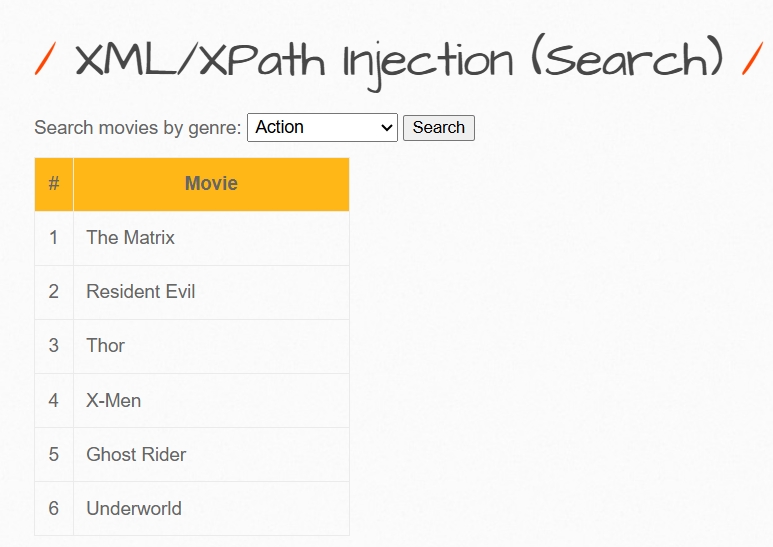
******

***SQL BỊ LỖI NÊN EM LƯỚT PHẦN SQL NHA THẦY***

***XML/XPath injection (Login Form)***

******

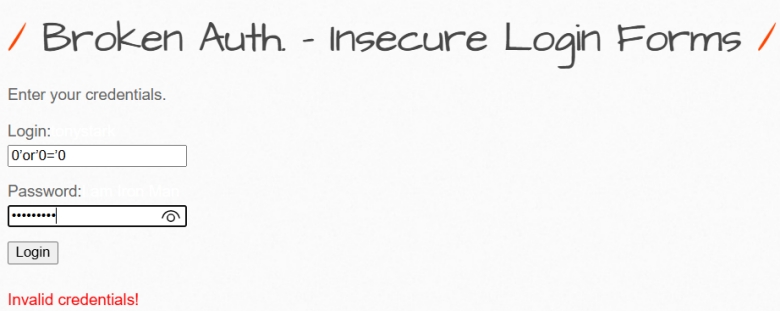
***XML/XPath injection (Search)***

******

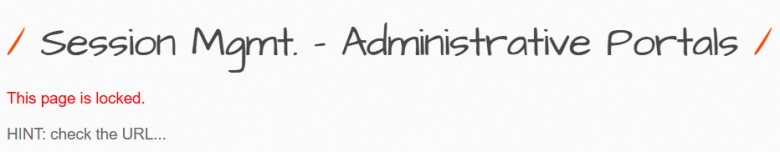
***Broken Authentication***

***“”***

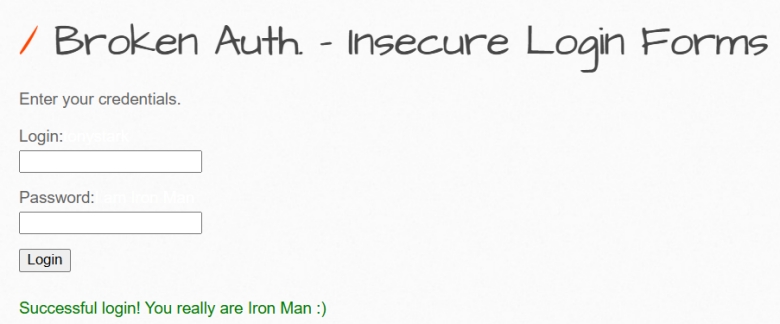
***Broken Authentication - Insecure Login Forms***

******

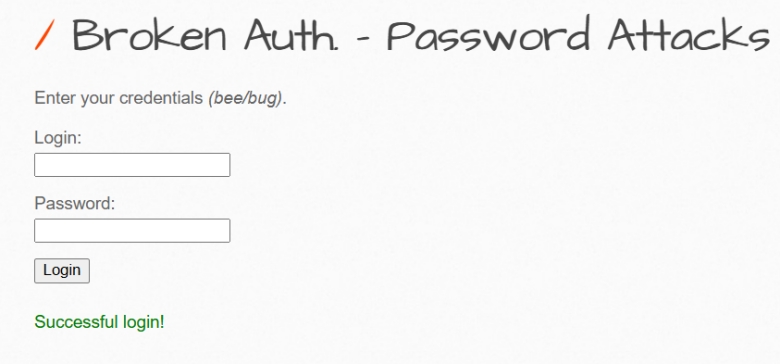
***Session Management - Administrative Portals***

******

***Broken Authentication - Insecure Login Forms***

******

***Broken Auth. - Password Attacks***

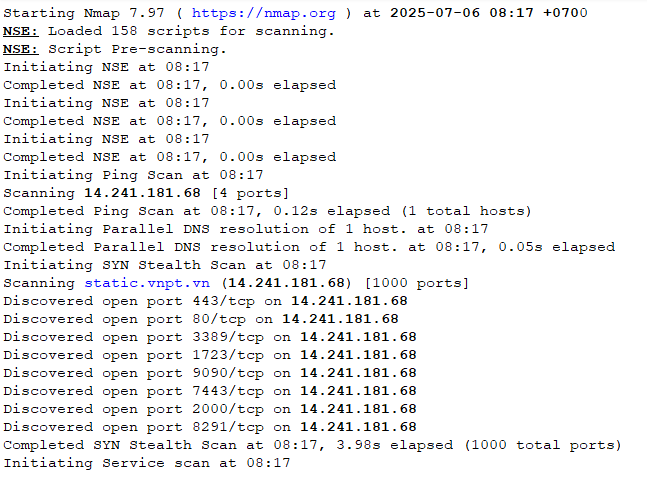
******

***HTML5 Web Storage (Secret)***

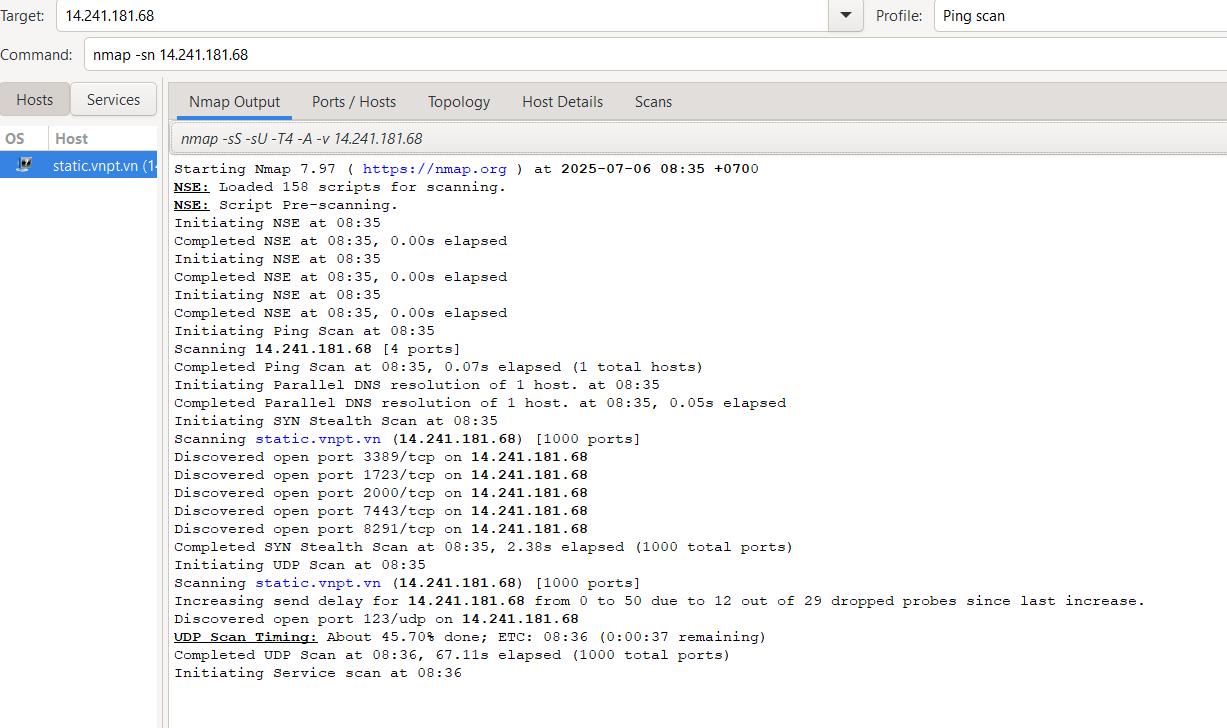
******

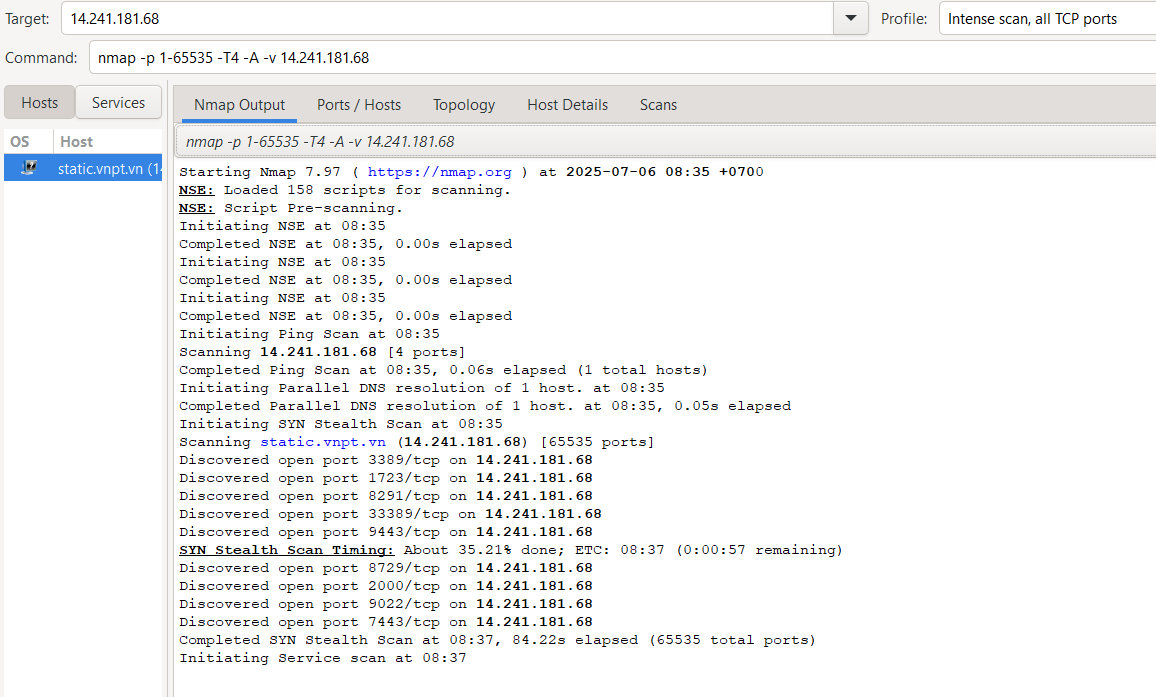
***Cross-Site Request Forgery (CSRF)***

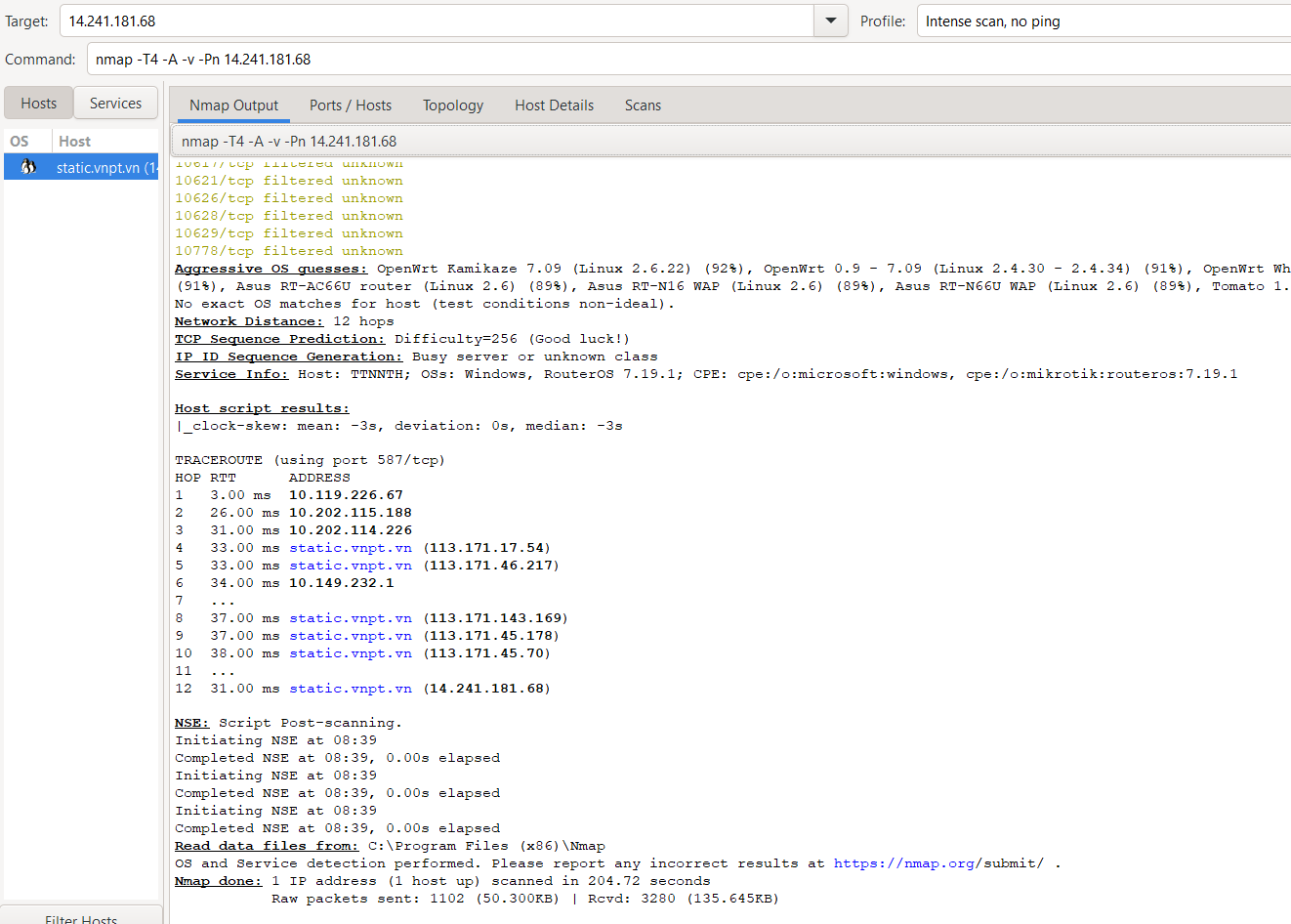
***Thực Hành Lab2***



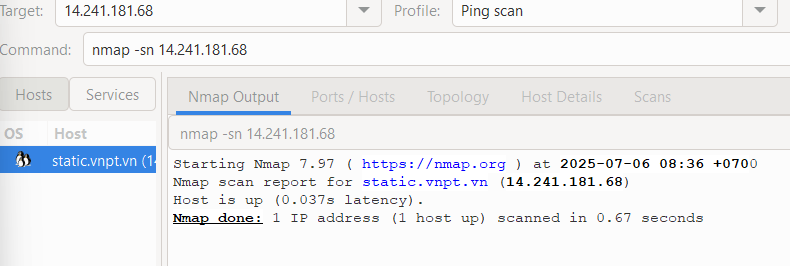
***Intense scan***

******

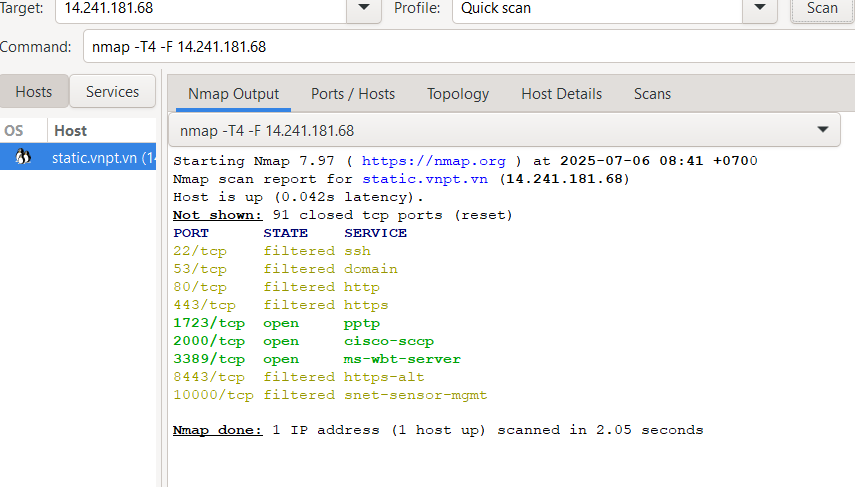
***Intense scan plus UDP***

******

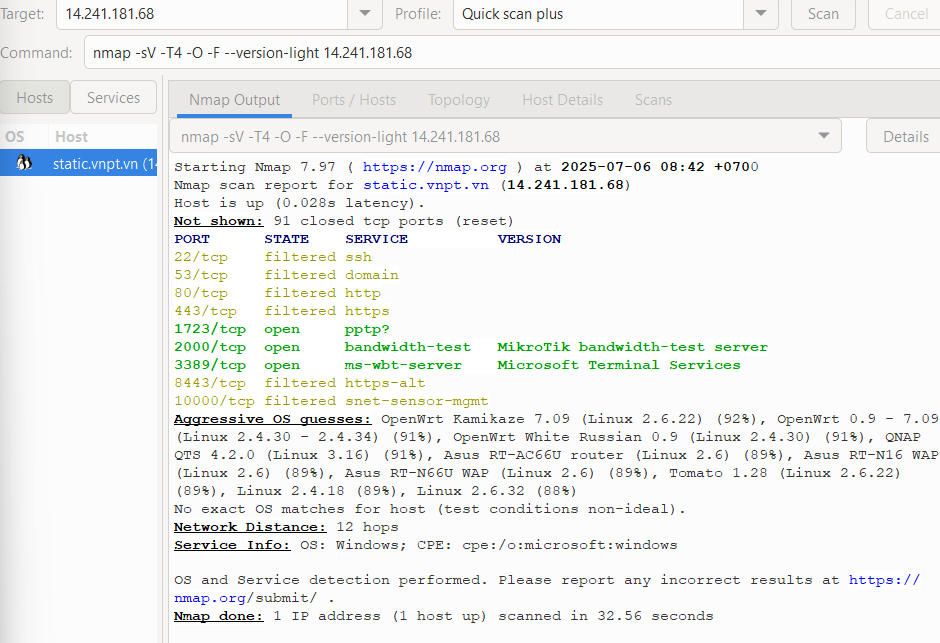
***Ping scan***

******

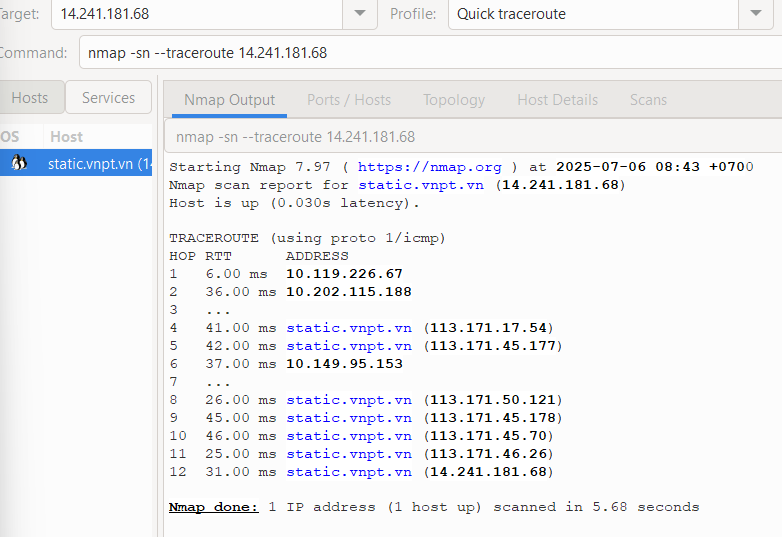
***Quick scan***

******

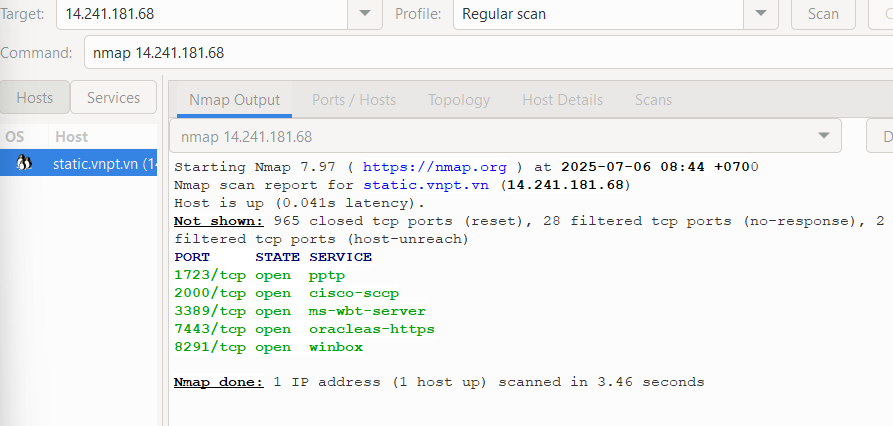
***Quick scan plus***

******

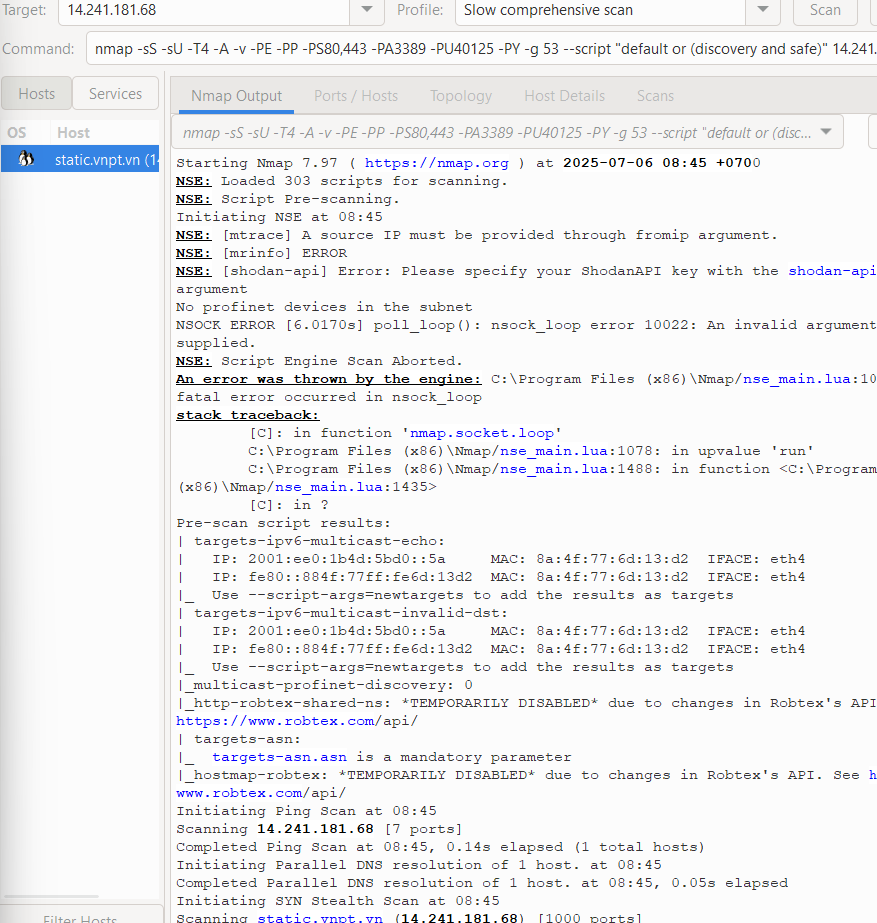
***Quick traceroute***

******

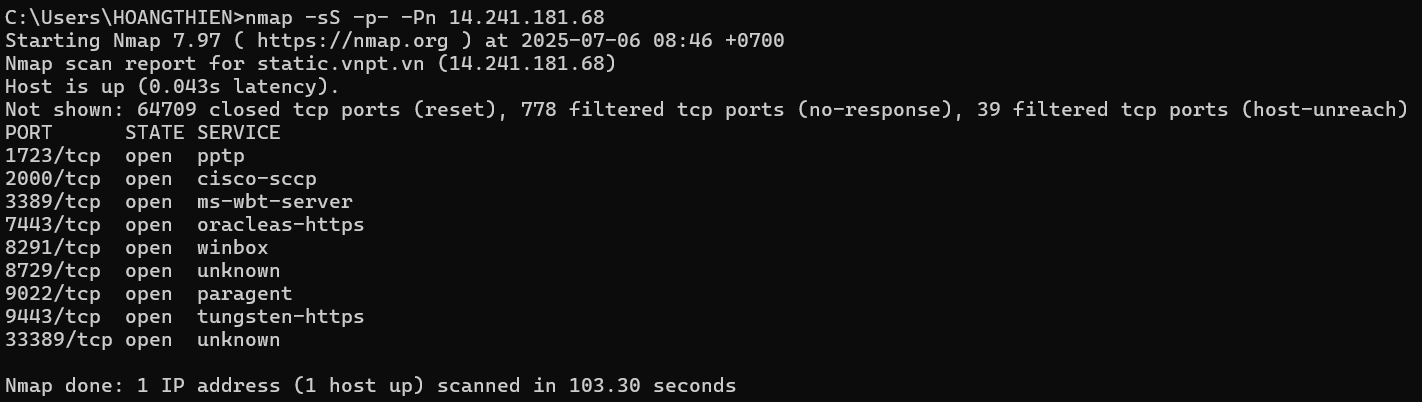
***Regular scan***

******

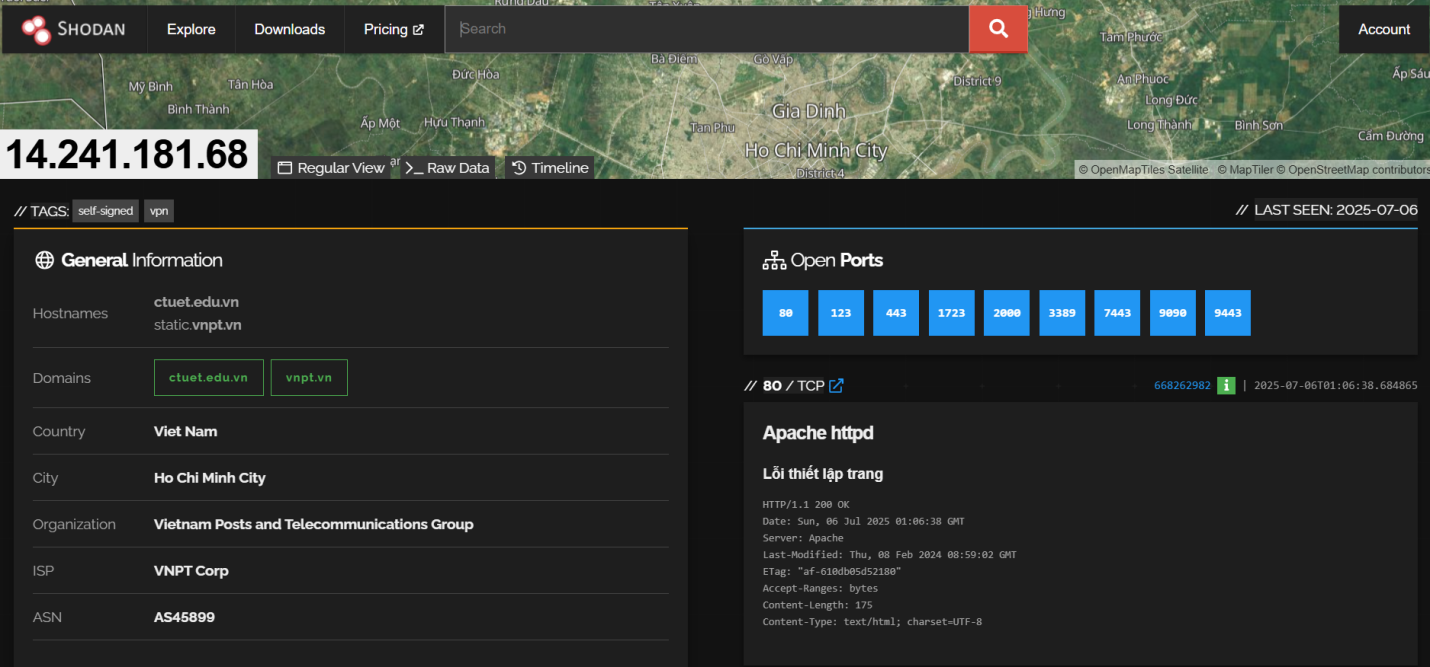
***Slow comprehensive scan***

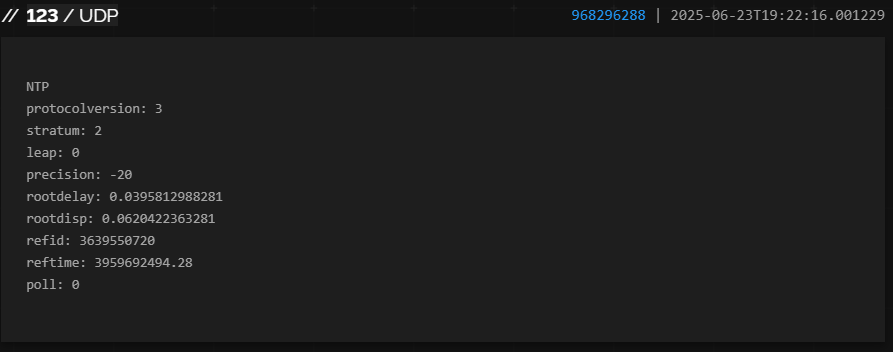
******

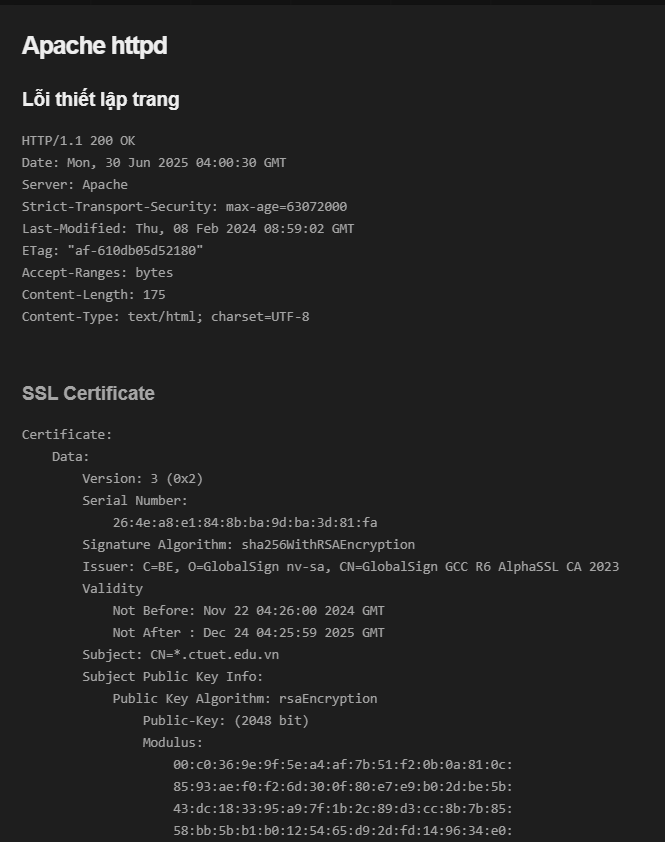
***Chạy trên cmd***

******

***Sử dụng shodan.io***

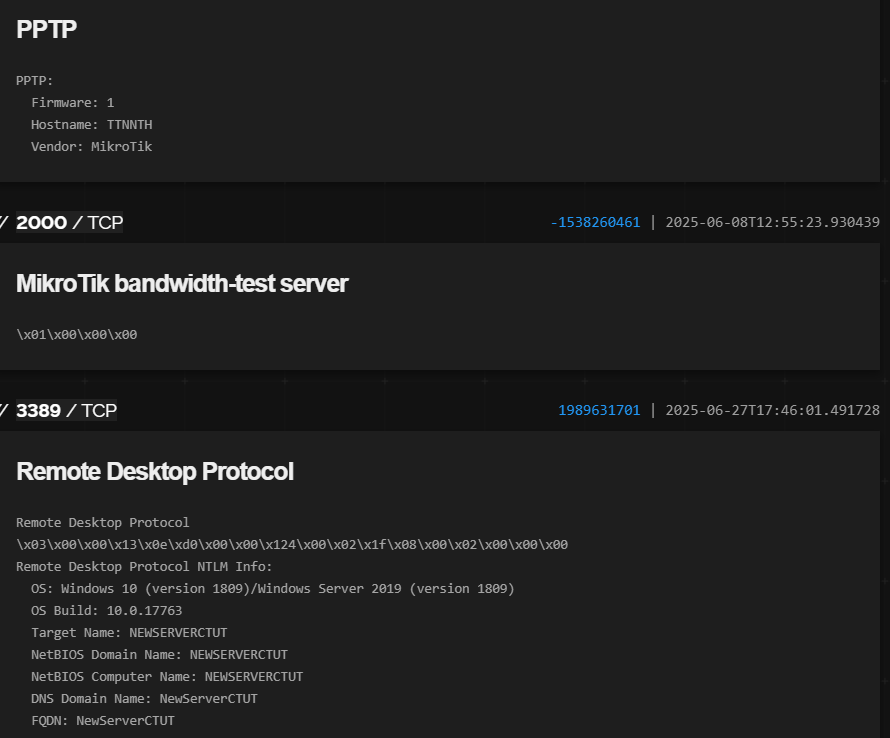
******

******

******

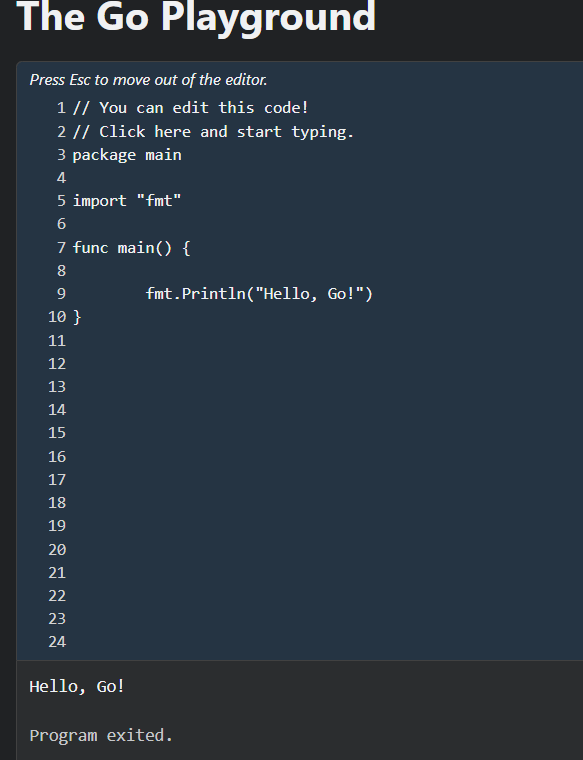
******

******

******

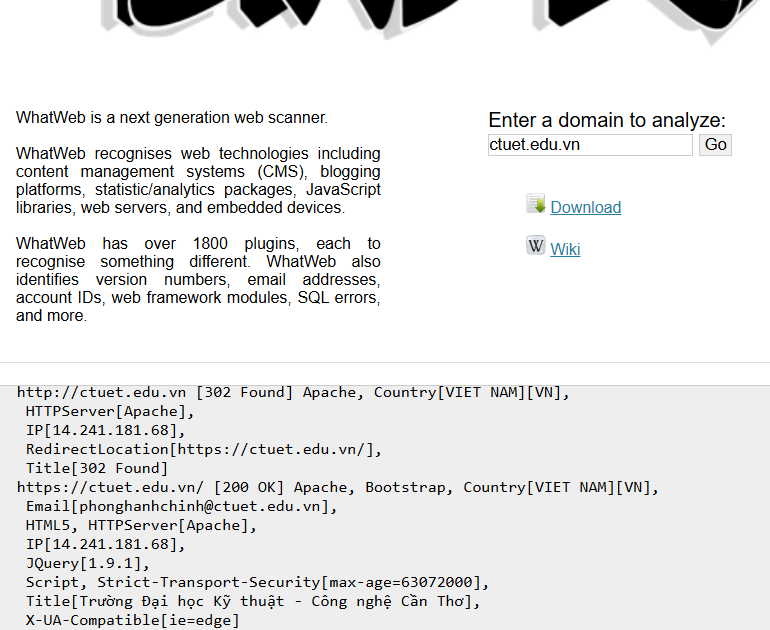
***Sử dụng Go Programming (Go Bang)***

***Em đã tải nhưng kím ko ra trên lap. Thế em sài web luôn***

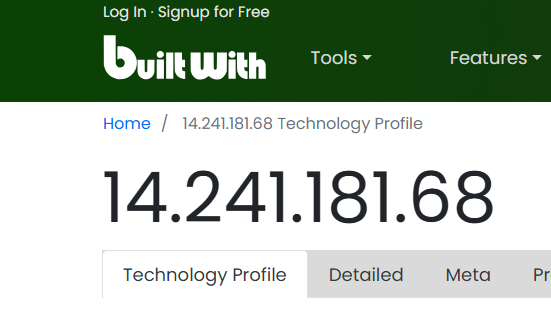
******

***Sử dụng whatweb.net***

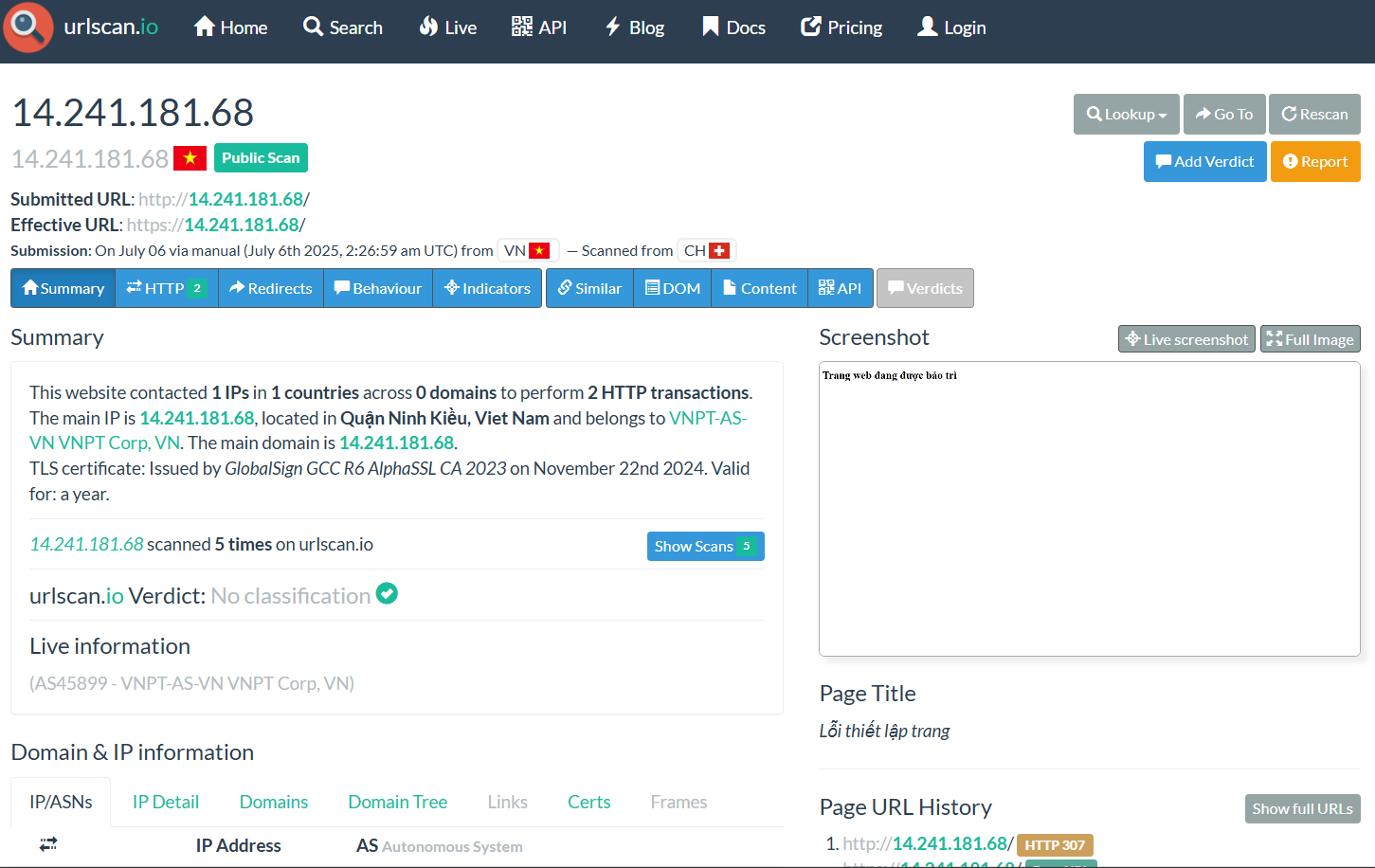
******

******

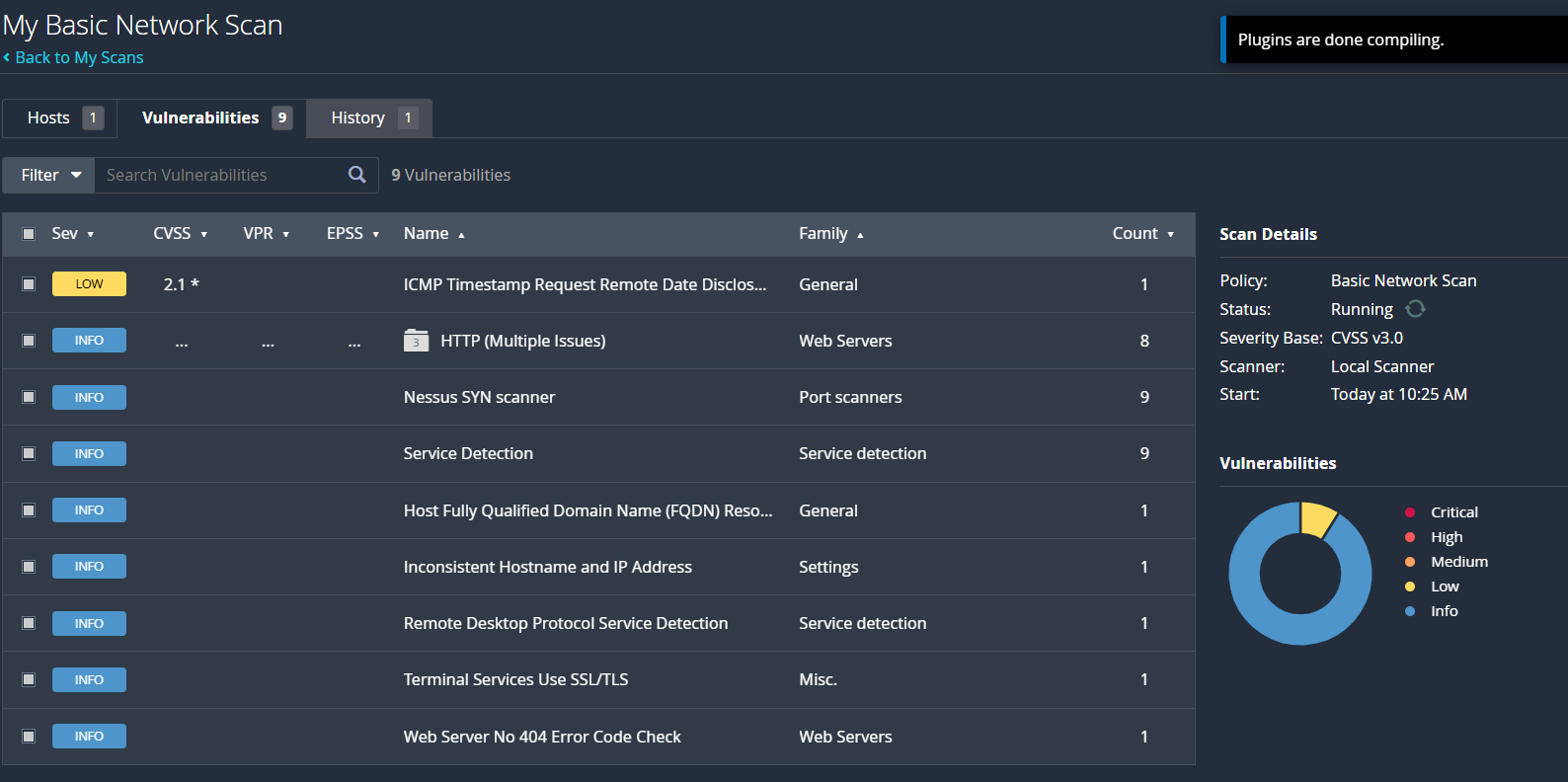
***Sử dụng builtwith.com***

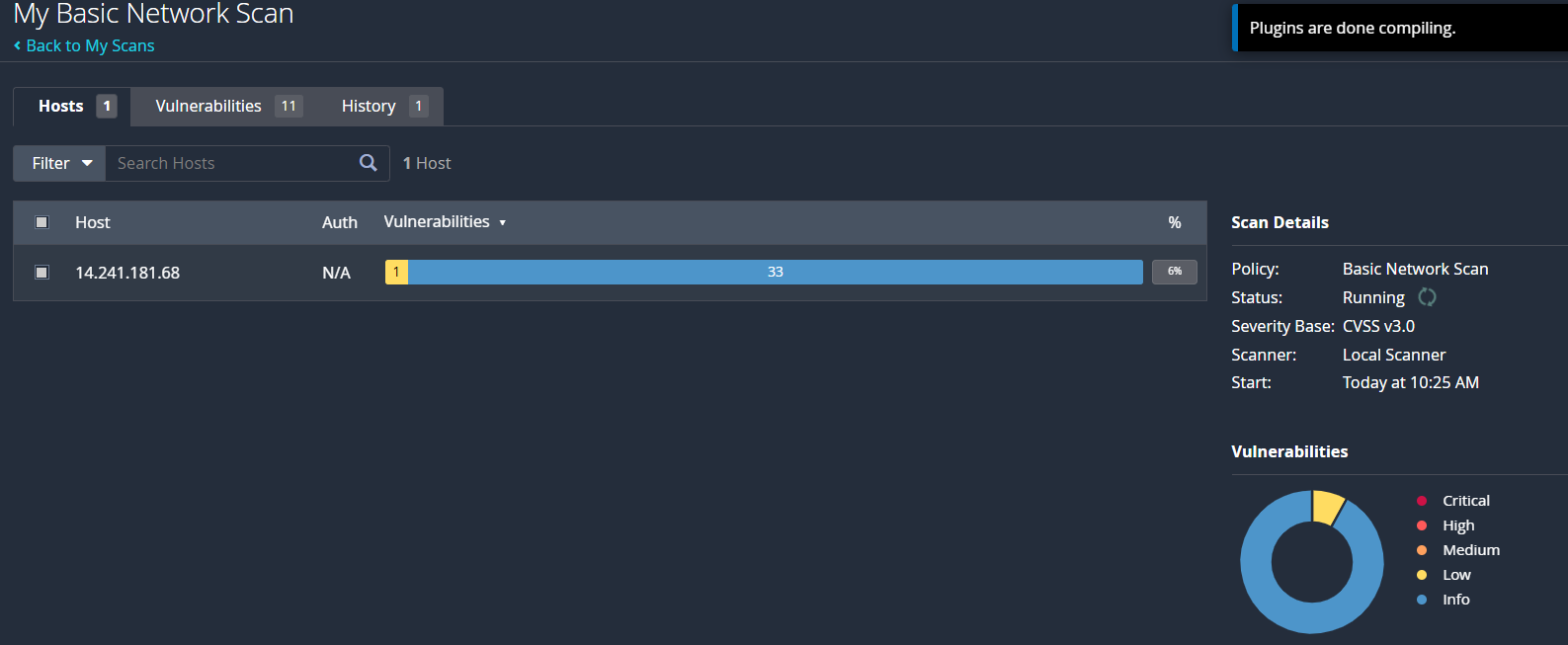
******

***Sử dụng urlscan.io***

******

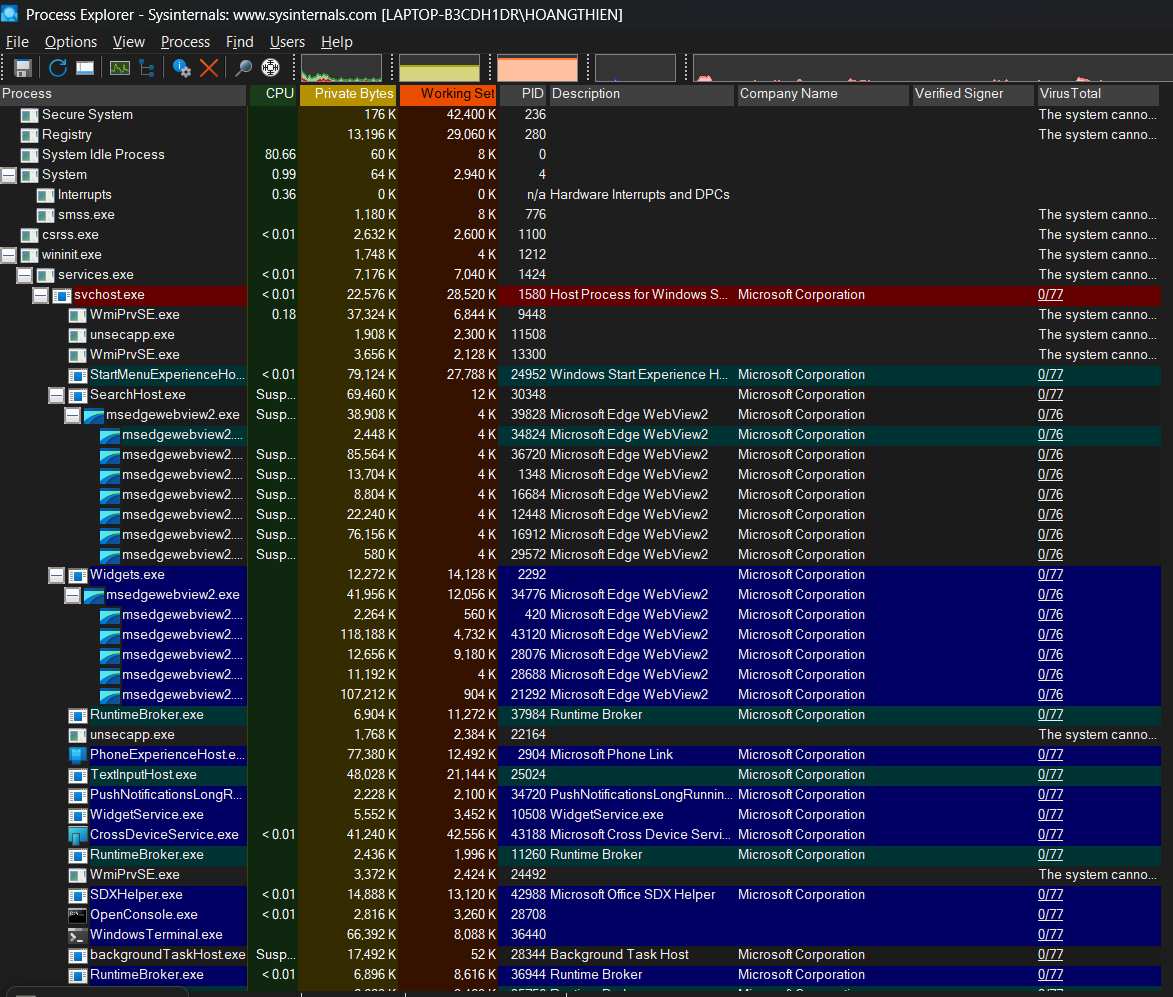
***Localhost***

******

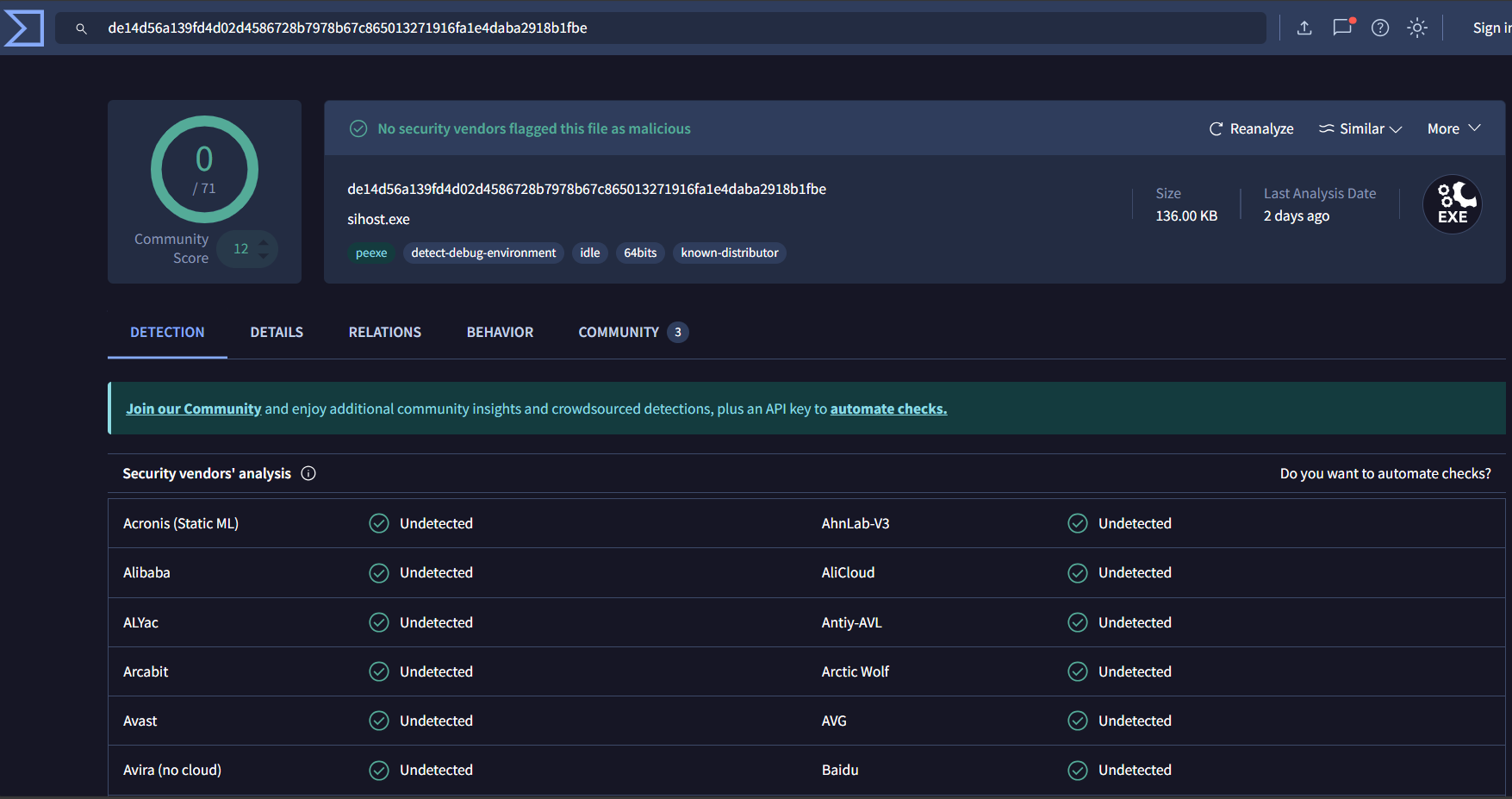
******

***Thực Hành Lab3***

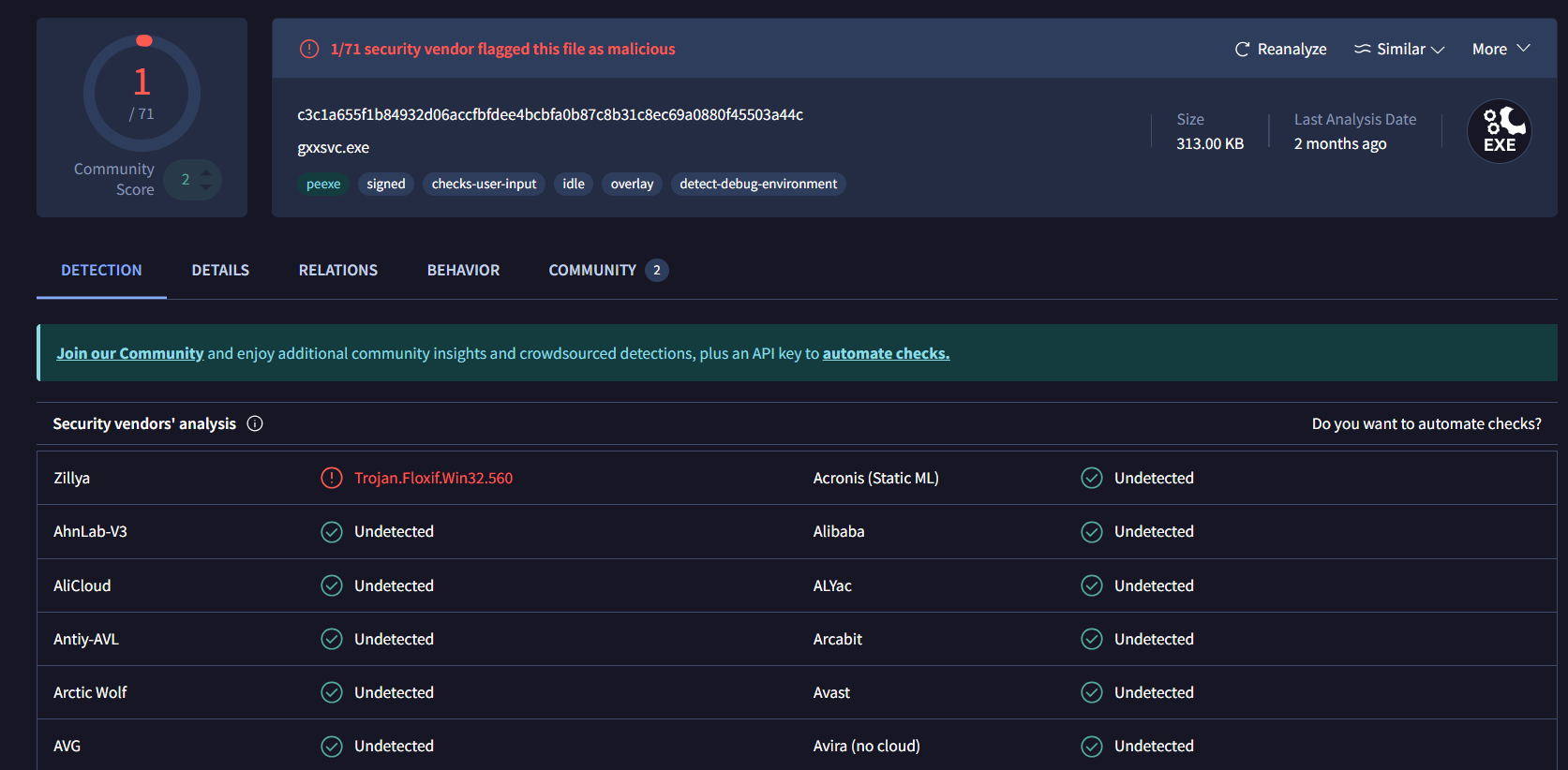
***Process Explorer***

******

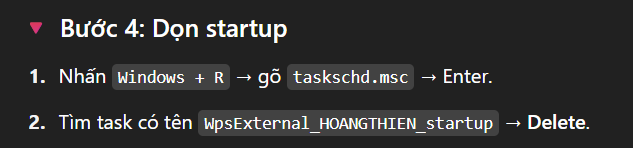
**Nếu phần mềm không dính ViruSs**

******

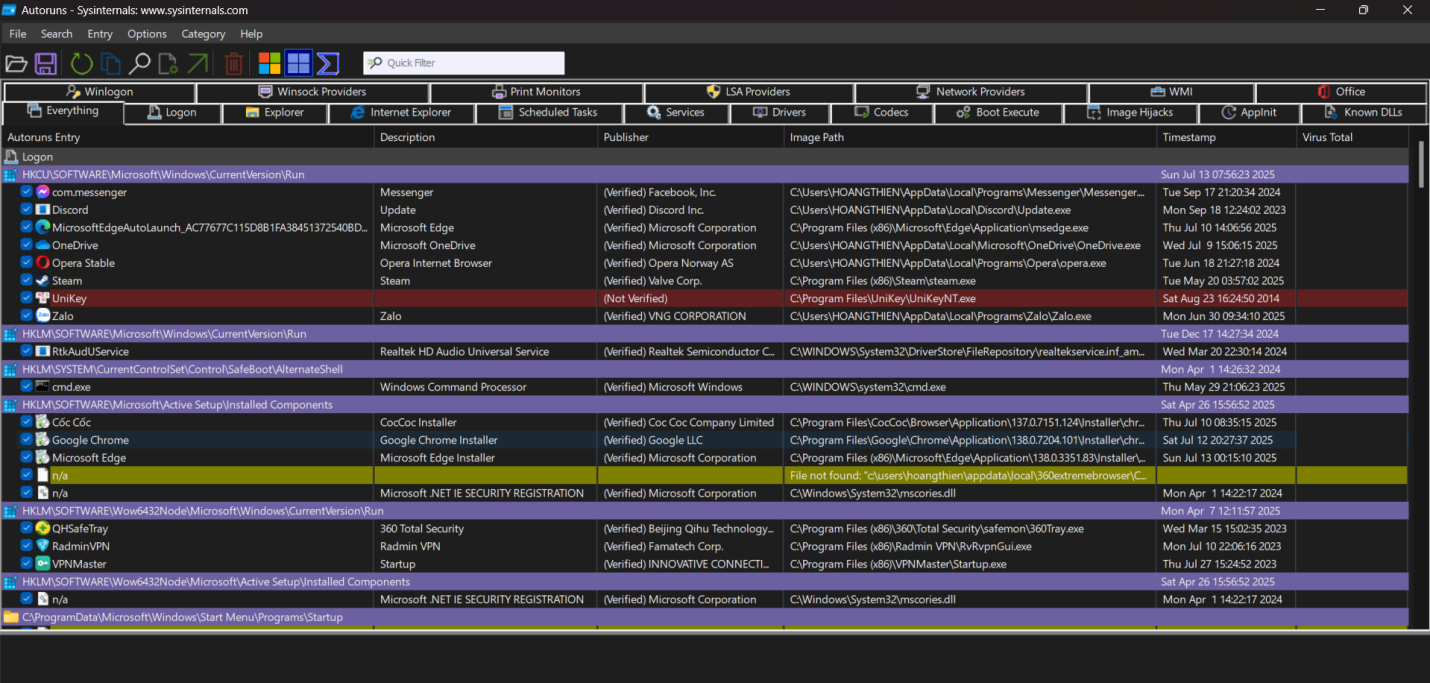
**Phần mềm dính có thể dính ViruSs**

******

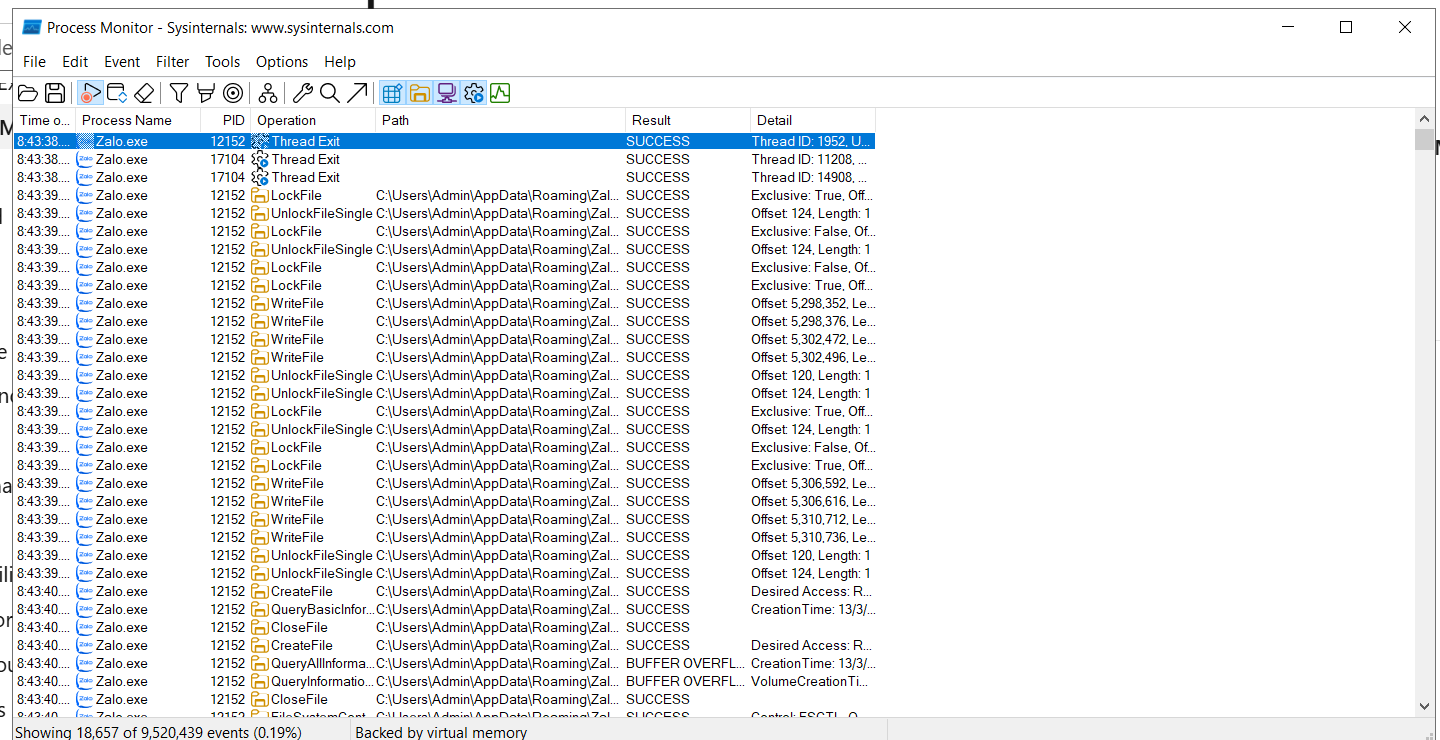
**Cách xóa**

******

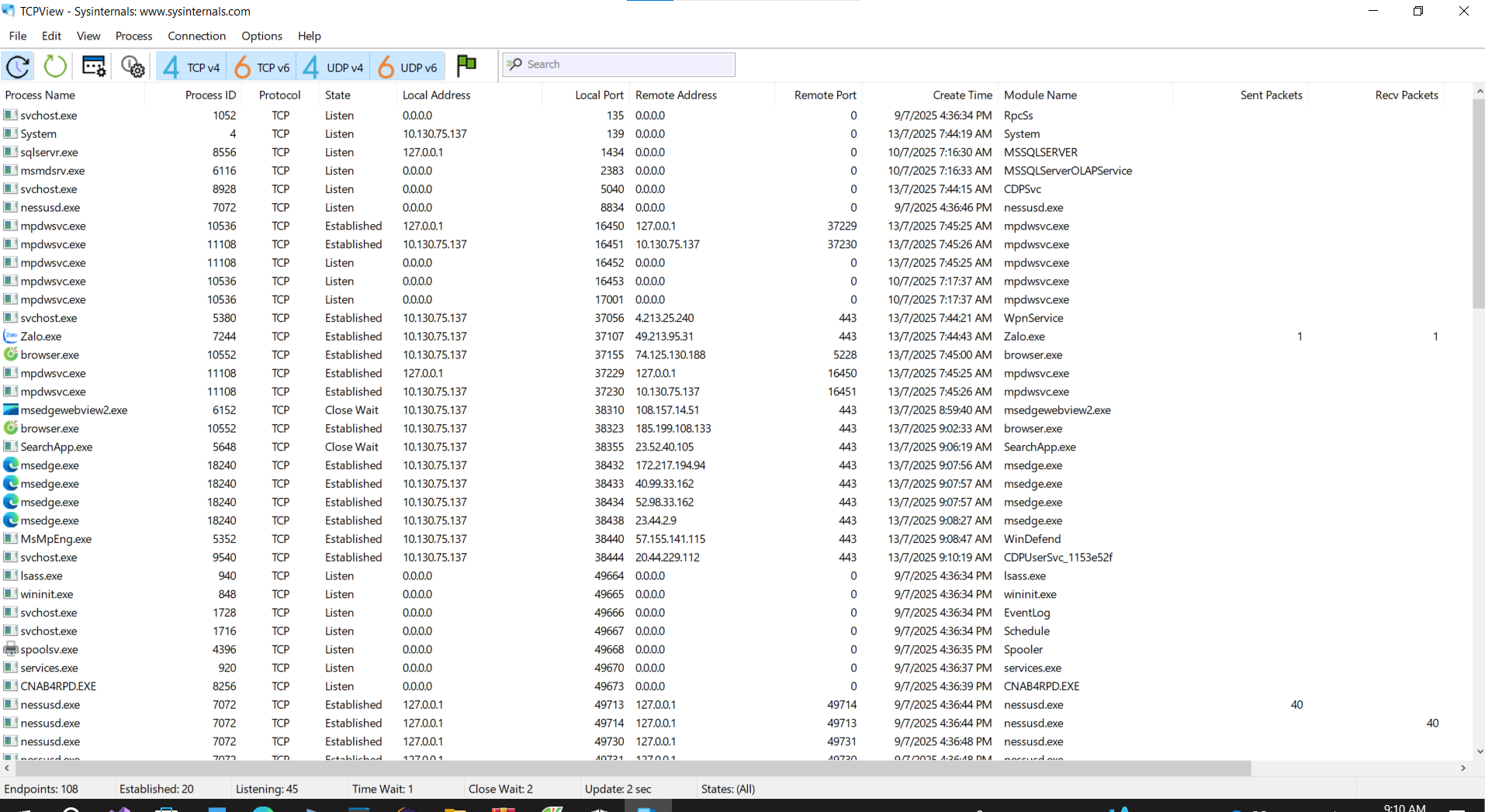
***Autoruns – Sysinternals***

******

**Theo dõi hoạt động của Malware**



**Xác định xem tiến trình nào đang sinh ra hoạt động mạng tương ứng**



**Kiểm tra dữ liệu mã độc đã gửi và nhận**

