

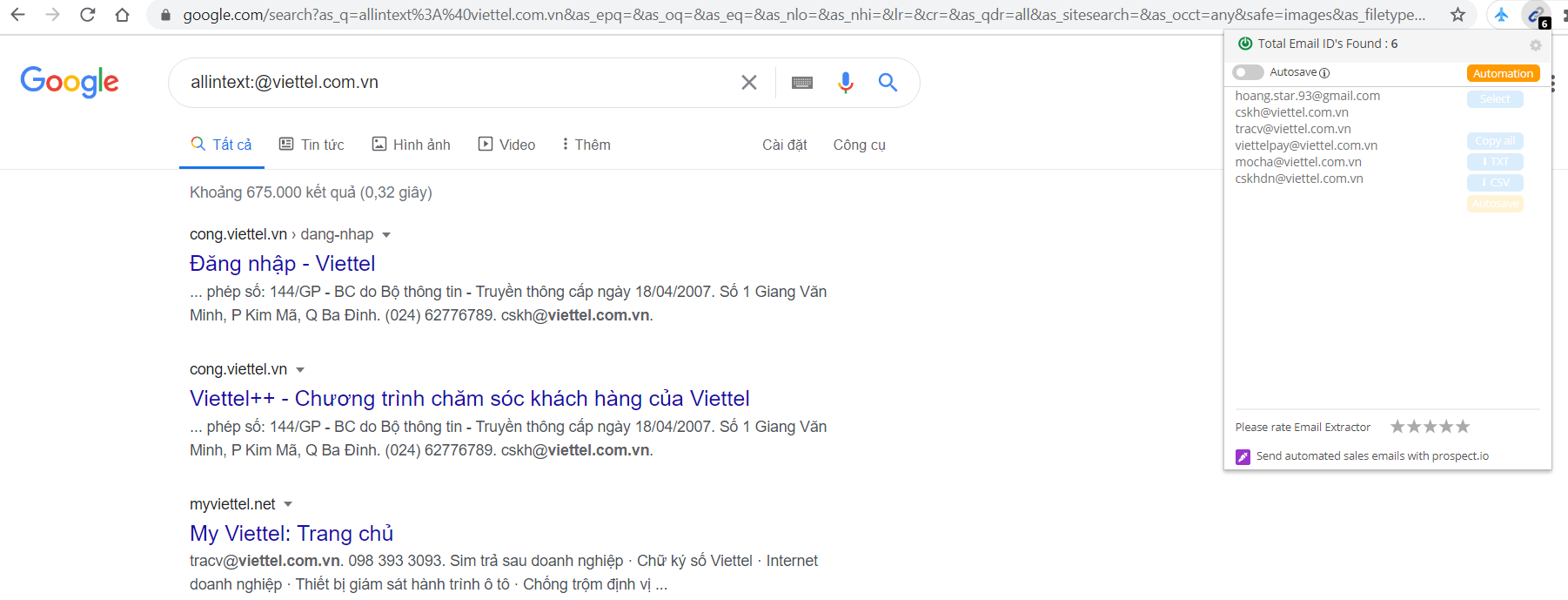
Báo Cáo LAB

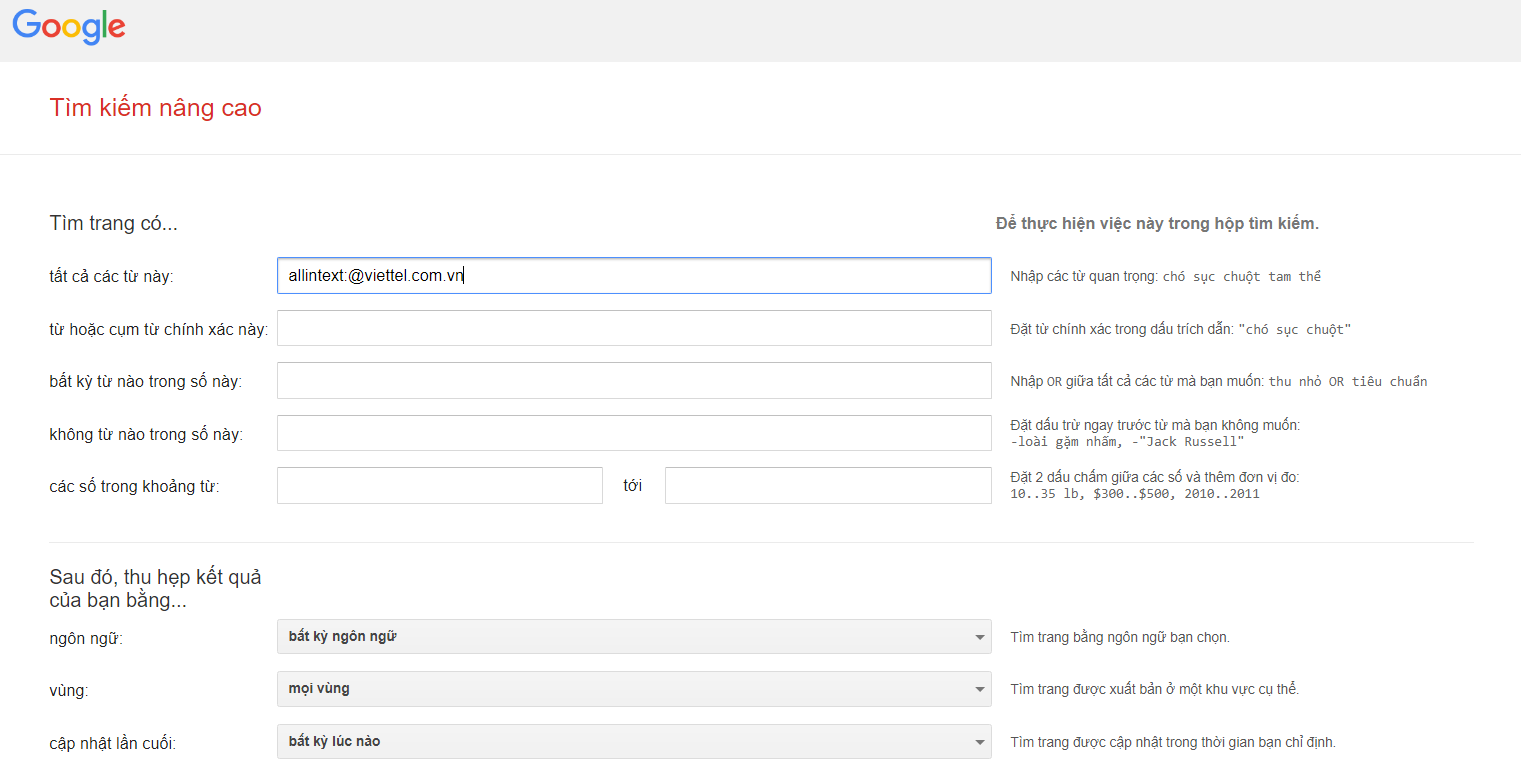
Thu Thập Thông Tin

1. **Thu thập danh sách email nhân viên Viettel (Search hoặc Tool)**
   1. Sử dụng google advanced\_search và extension Email Extrator

Dùng allintext:@viettel.com.vn để tìm kiếm email sẽ được lưu vào extension Email Extrator và được sao chép và lưu vào file excel.

Kết quả thu được sau lọc trùng 62 email.







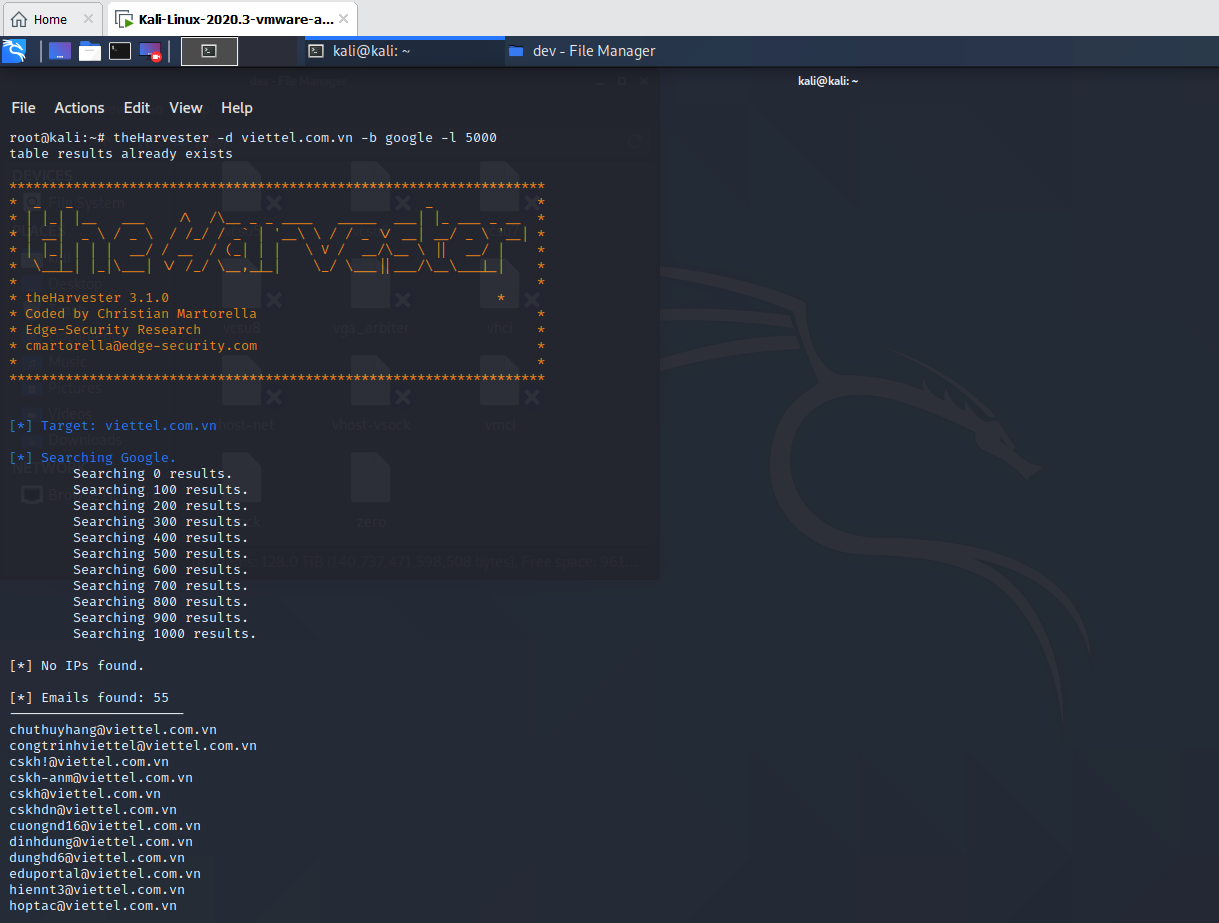
* 1. Sử dụng tool theHarvester trong máy ảo Kali-linux

Dùng câu lệnh: theHarvester -d viettel.com.vn -b google -l 5000

-d viettel.com.vn : quét domain viettel.com.vn

-b google –l 5000 : sử dụng data google tối đa 5000 data.

Kết quả thu được 55 email. Do chưa có apikey cho các phần data mở rộng khác, quét all bị lỗi chưa xác định nguyên nhân nên sử dụng dữ liệu từ google để tìm nên kết quả trùng khá nhiều với cách tìm kiếm nâng cao đạt hiệu suất không cao.



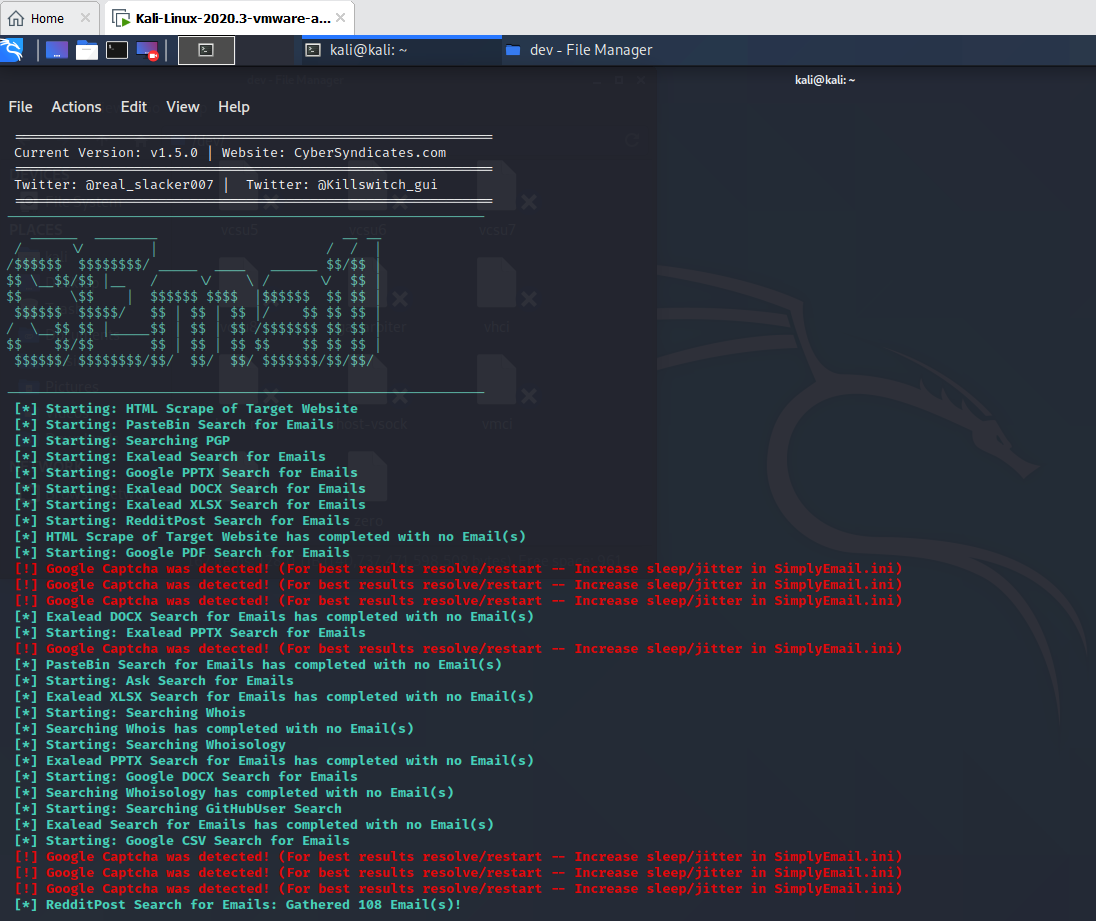
* 1. Sử dụng tool Simply Email trong máy ảo Kali-linux

Dùng câu lệnh:

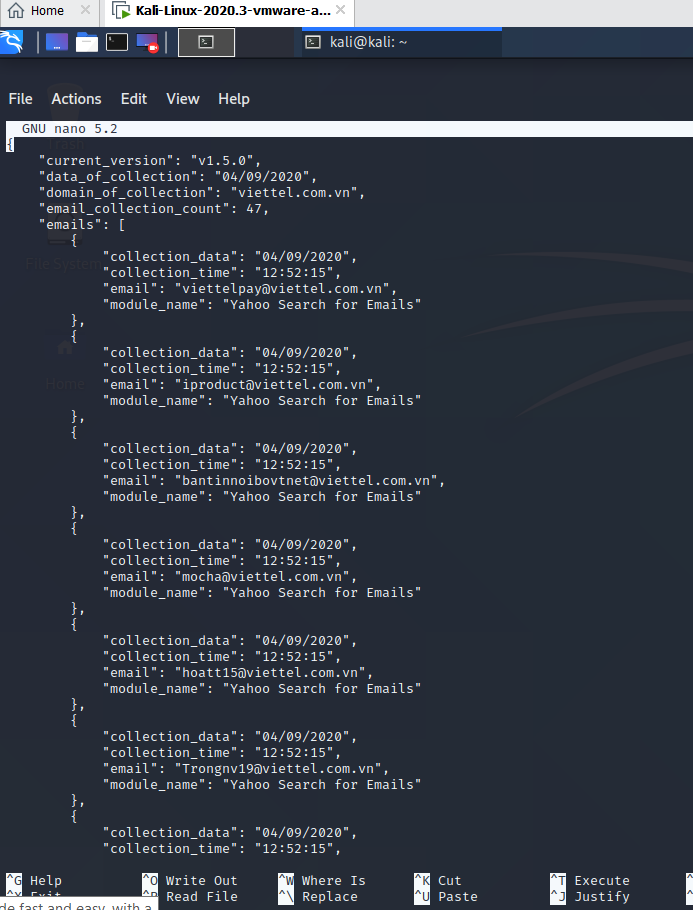
root@kali:~# curl -s https://raw.githubusercontent.com/killswitch-GUI/SimplyEmail/master/setup/oneline-setup.sh | bash

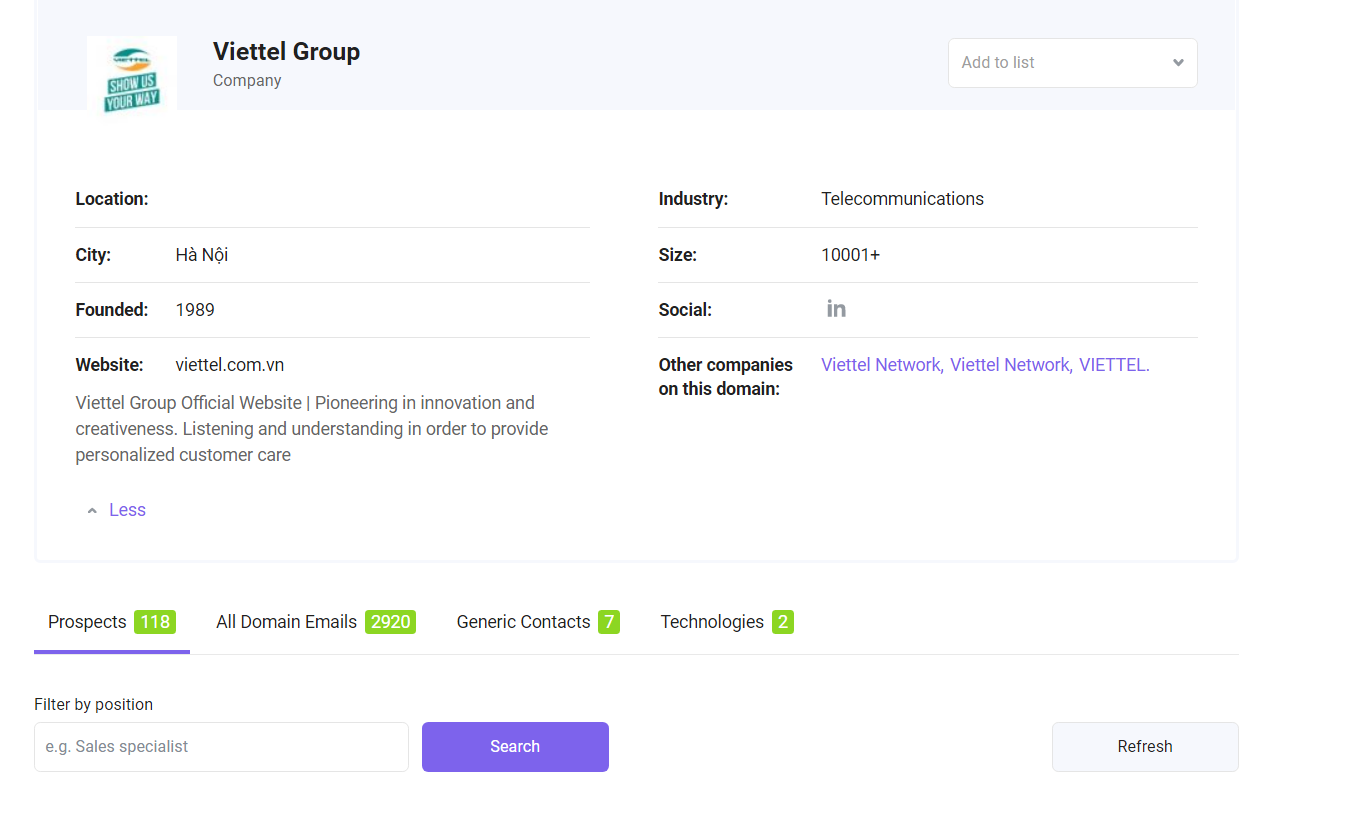
root@kali:~# cd SimplyEmail

root@kali:~/SimplyEmail# **./**SimplyEmail**.**py **-**all **-**e cybersyndicates**.**com **--**json cs**-**json**.**txt



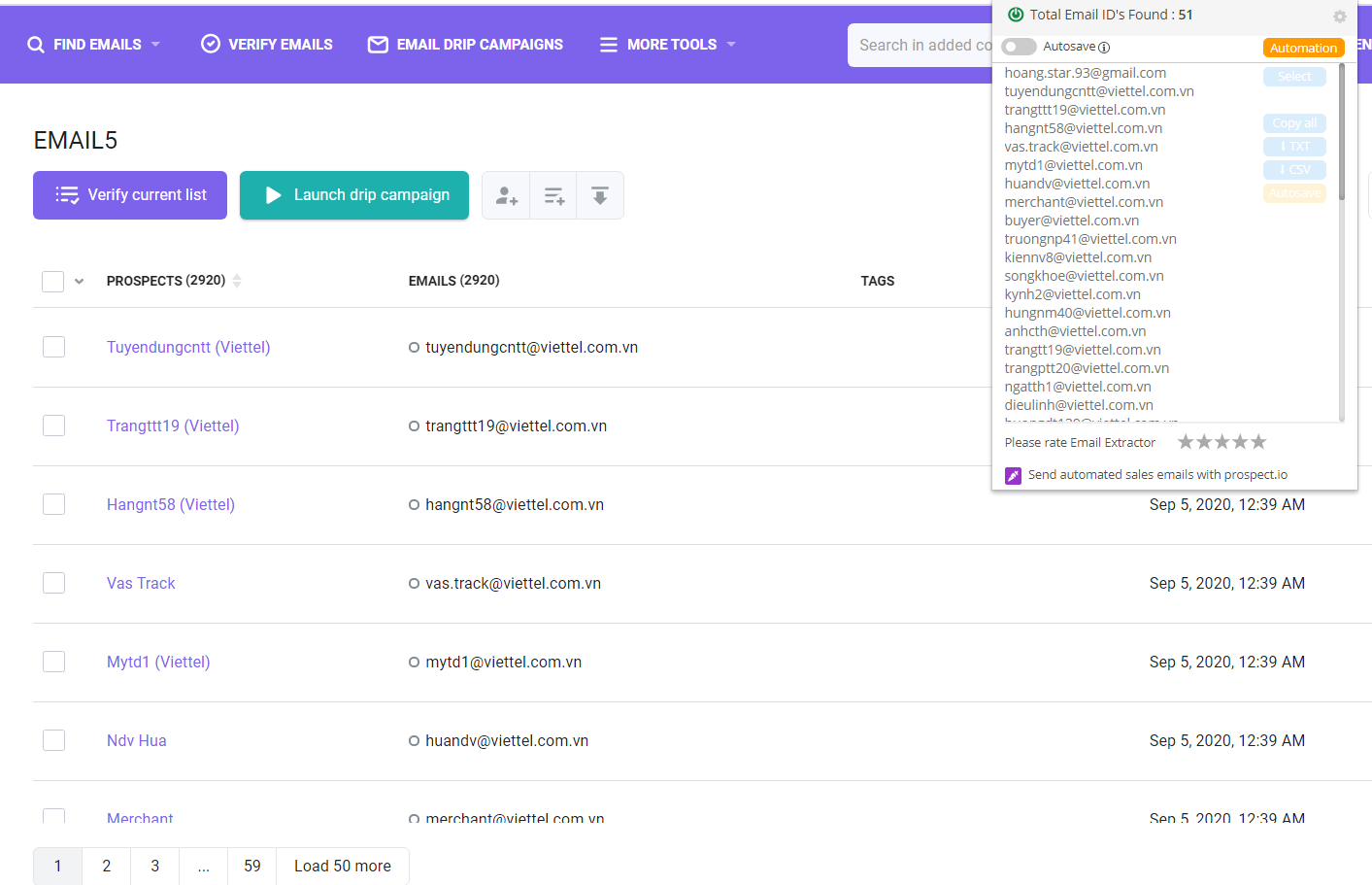
Kết quả thu được 47 email. Sử dụng Simply email do chưa có các apikey kết nối với các vùng dữ liệu khác nên vẫn tập trung quét dữ liệu trên data của google kết quả nhận được khá là ít và trùng với các trên.



* 1. Sử dụng công cụ tìm kiếm trên mạng snov.io/domain-search

Kết quả thu được 2920 email.

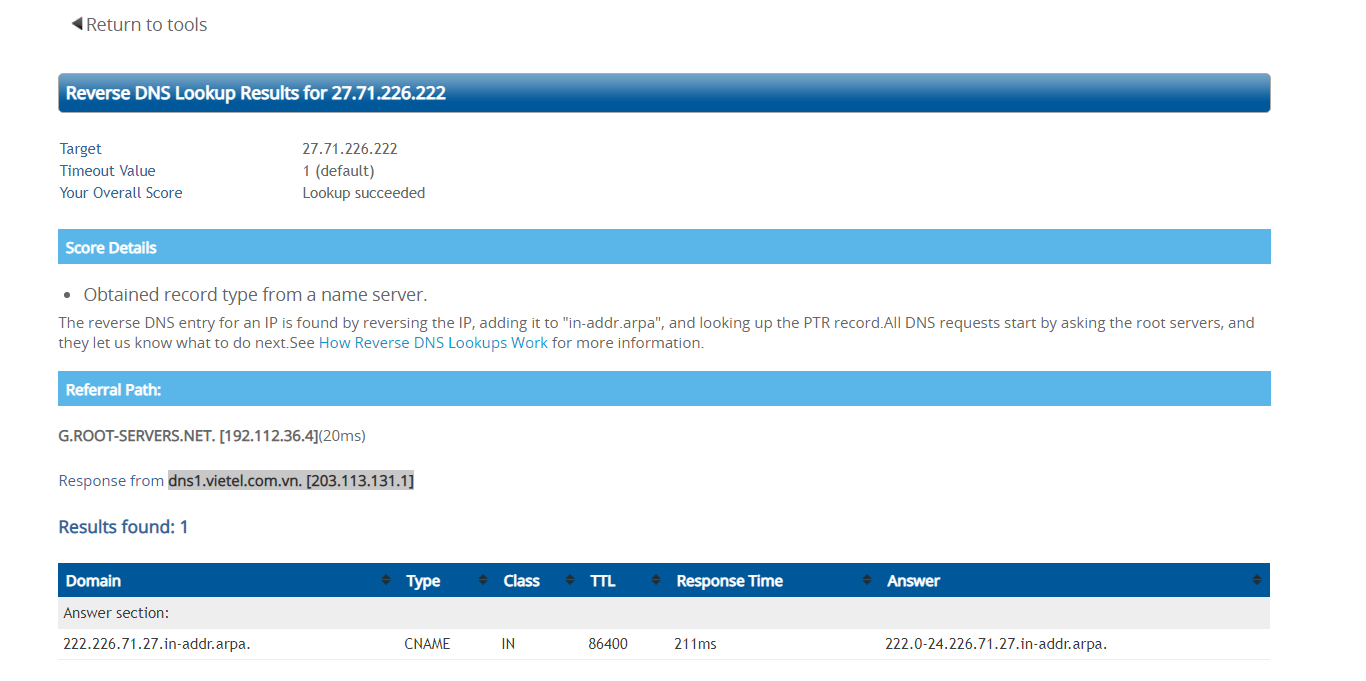
Sử dụng extension email extrator để sao chép vào file excel. Thu thập được số lượng lớn mail nhân viên chưa đảm bảo tất cả các mail còn đang hoạt động.



1. **Thu thập thông tin IP 27.71.226.222**

DNS server : **dns1.vietel.com.vn. [203.113.131.1]**

Quét trên <https://tools.dnsstuff.com/>



Open port : 80/TCP - http ,443/TCP - https

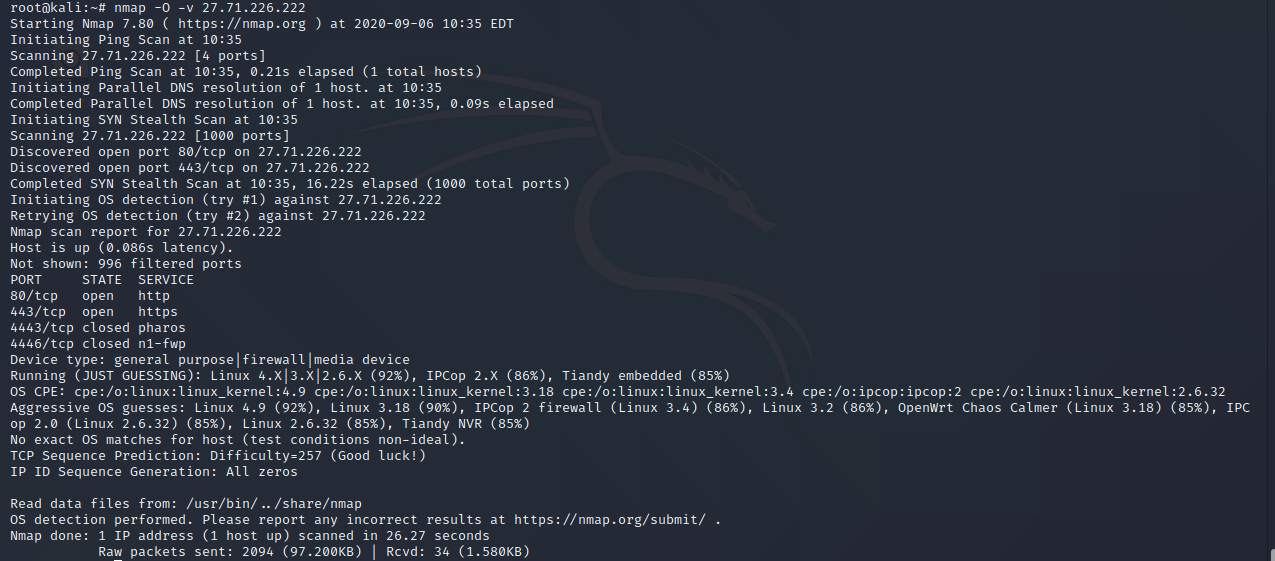
Closed port : 4443/TCP – pharos ,4446/TCP – n1-fwp

HĐH : linux 4.9

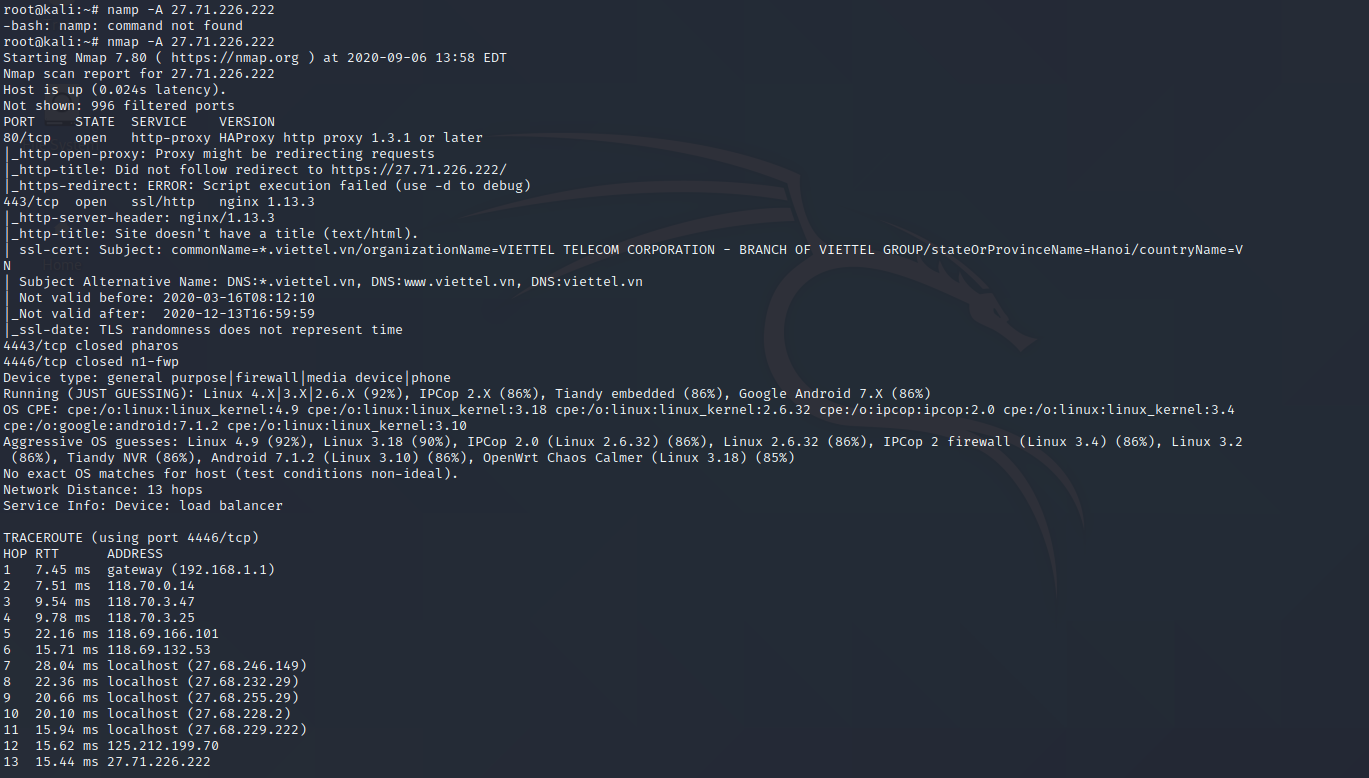
Loại thiết bị : general purpose|firewall|media device|phone

Web server : nginx 1.13.3 , HAProxy http proxy 1.3.1

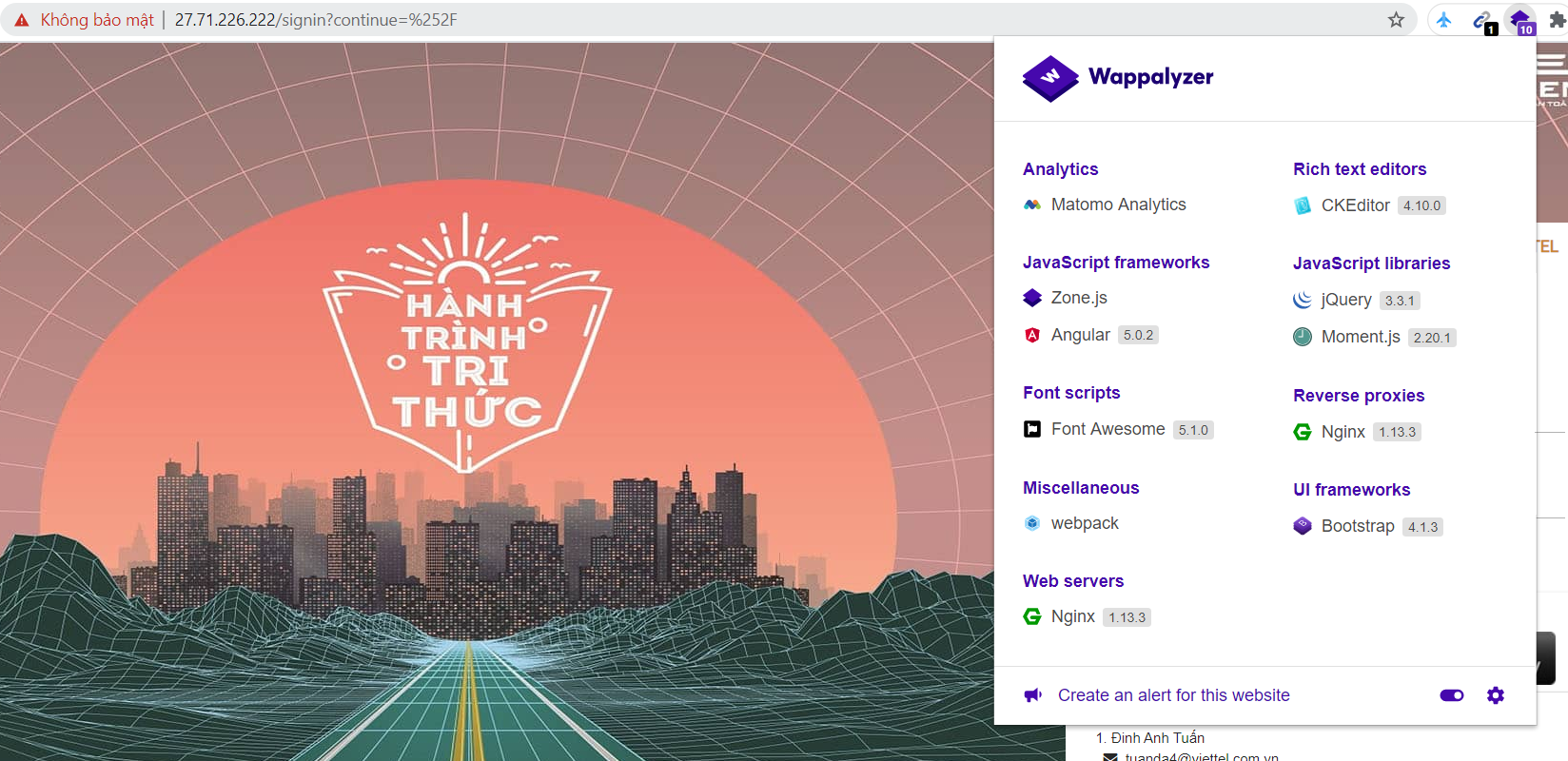
Sử dụng nmap scan : nmap -O -v 27.71.226.222



nmap -A 27.71.226.222



Truy cập ip 27.71.226.222 trên trình duyệt sử dụng extension Wappalyzer



IP 27.71.226.222 mở port 80,443

HTTP đang chạy trên TCP. Kết quả là máy chủ web có thể đối mặt với nhiều cuộc tấn công liên quan đến TCP. Tập trung sử dụng các kỹ thuật tấn công Từ chối Dịch vụ (DoS) như Syn floods, ACK floods, RST floods, Push-ACK floods, FIN floods.

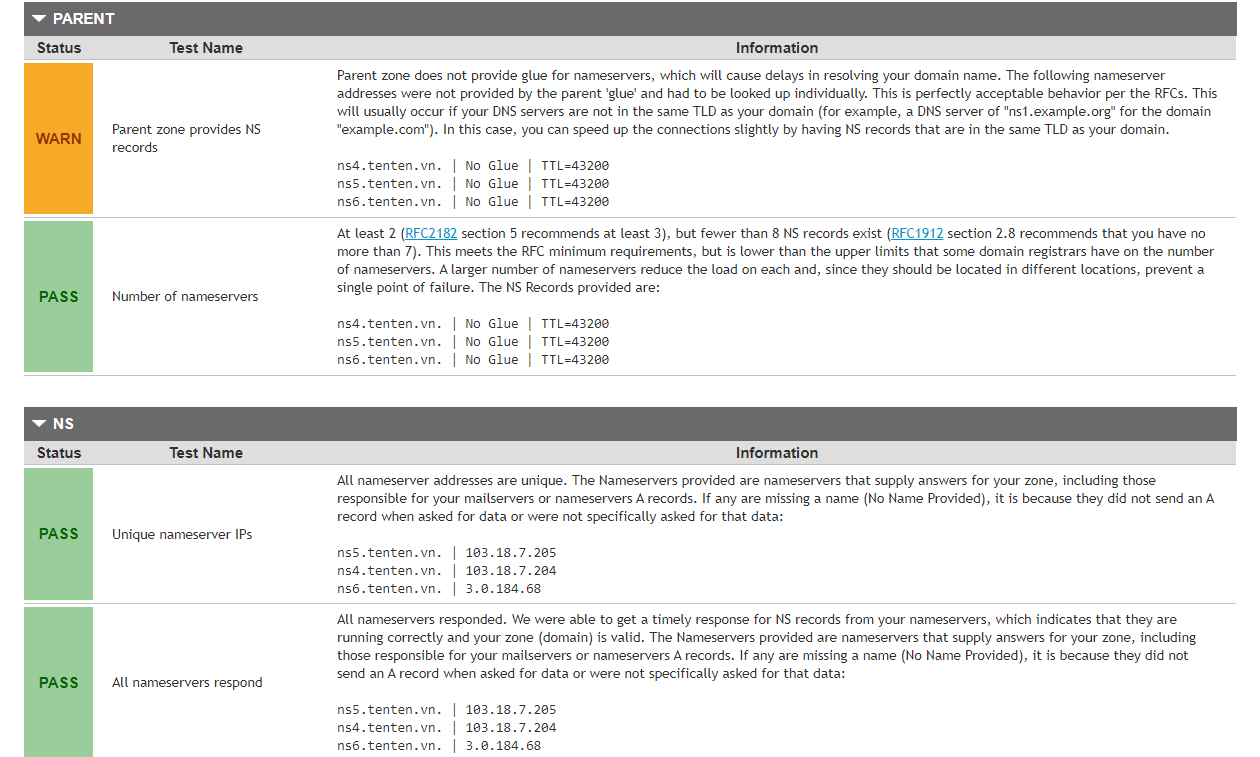
Khai thác lỗi trên frameworks web Angular 5.0.2 đang chạy trên đại chỉ ip, tìm lỗ hổng của hệ điều hành linux để thử.

1. **Thu thập thông tin songkhoe.vn**

DNS server :

ns4.tenten.vn. | 103.18.7.204  
ns6.tenten.vn. | 3.0.184.68  
ns5.tenten.vn. | 103.18.7.205

Quét trên <https://tools.dnsstuff.com/>



Open port : 80/TCP - http

Closed port : 113/TCP - ident

HĐH : Microsoft Windows Server 2012

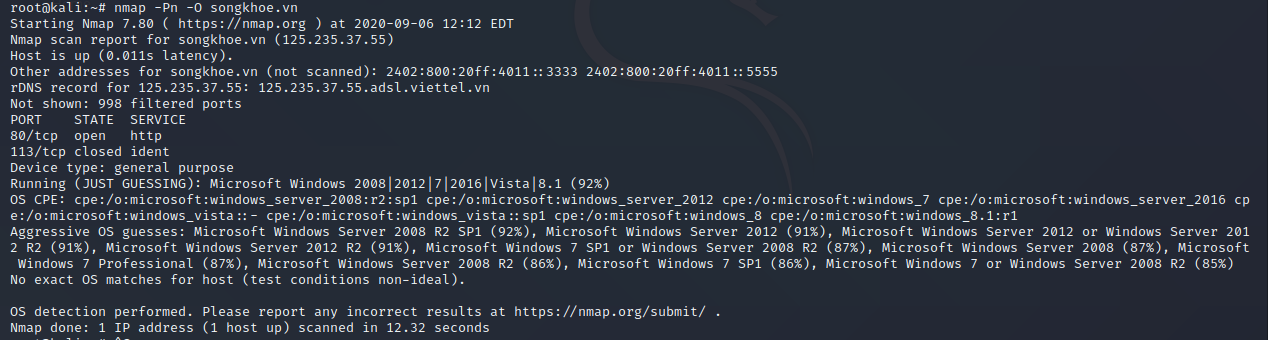
Loại thiết bị : general purpose

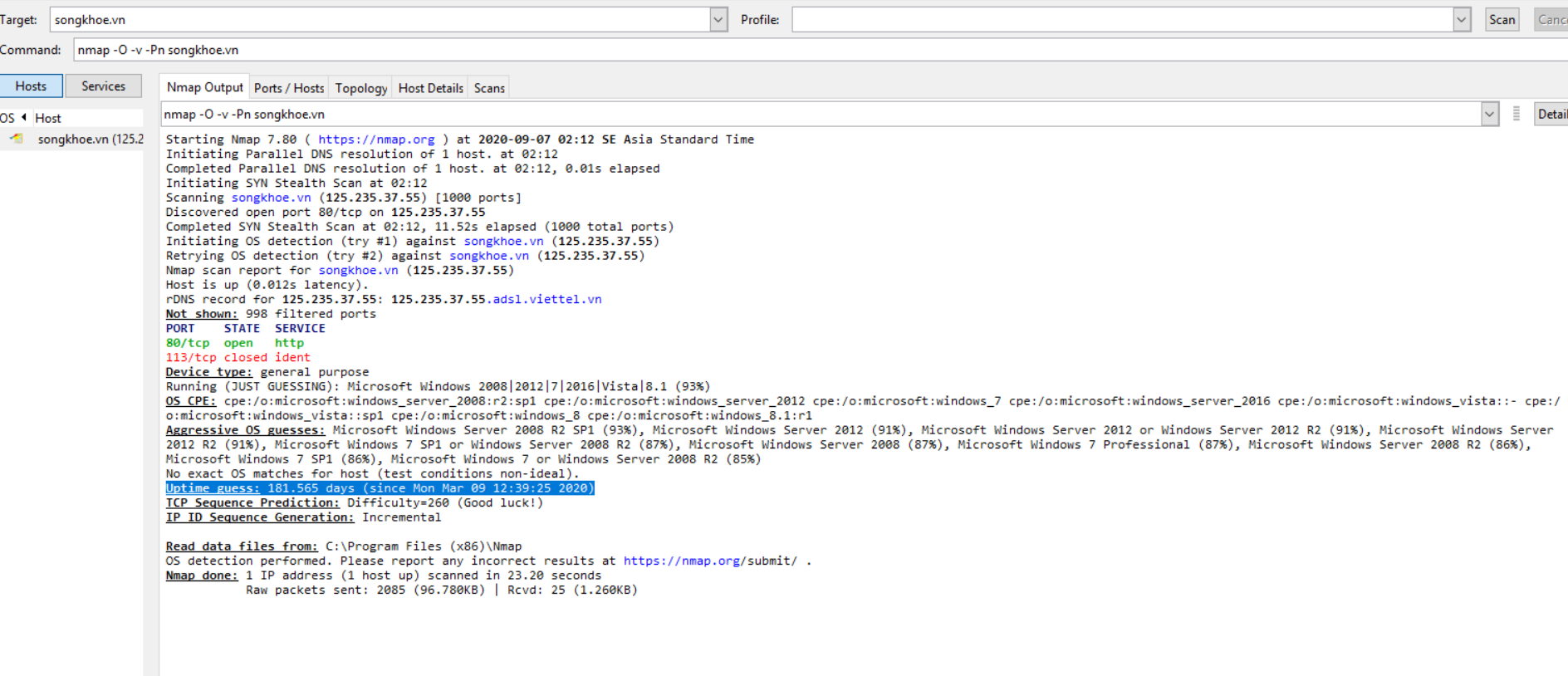
Web server : IIS 8.5

Uptime guess: 181.565 days (since Mon Mar 09 12:39:25 2020)

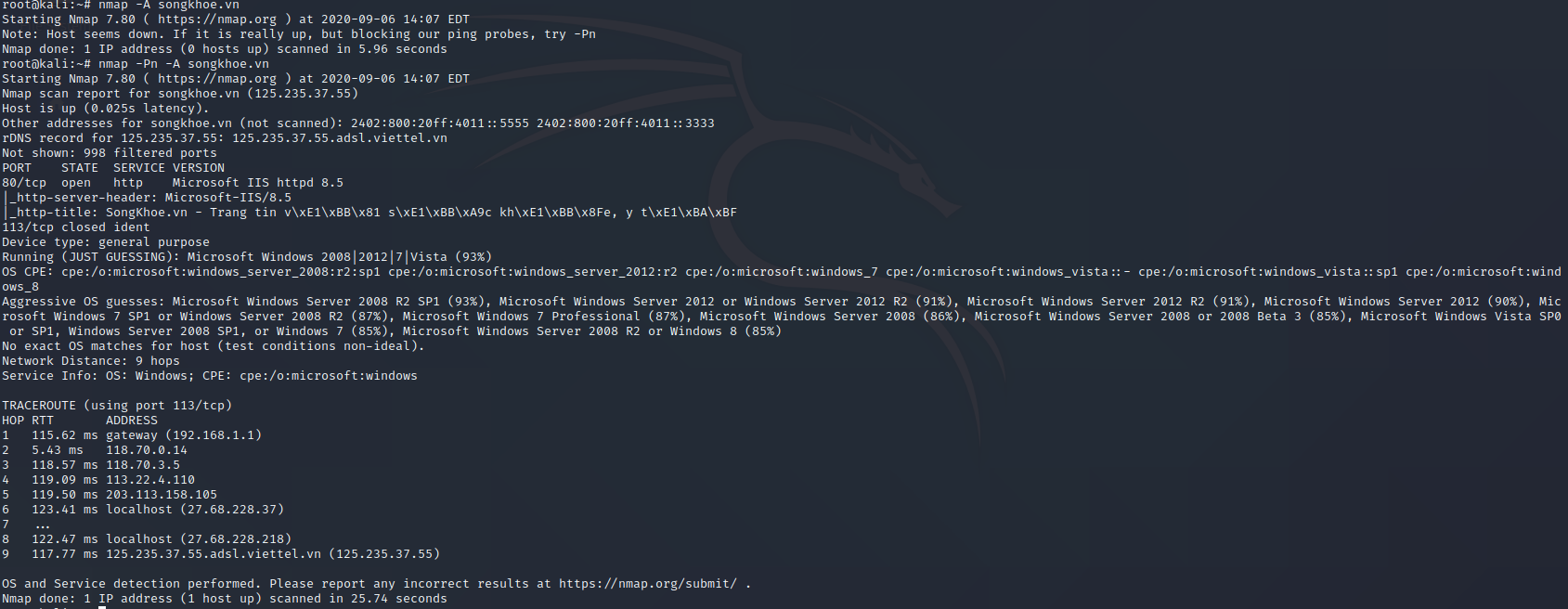
Web frameworks : Microsoft ASP.NET 2.0.50727

Sử dụng nmap scan : nmap -Pn -O songkhoe.vn

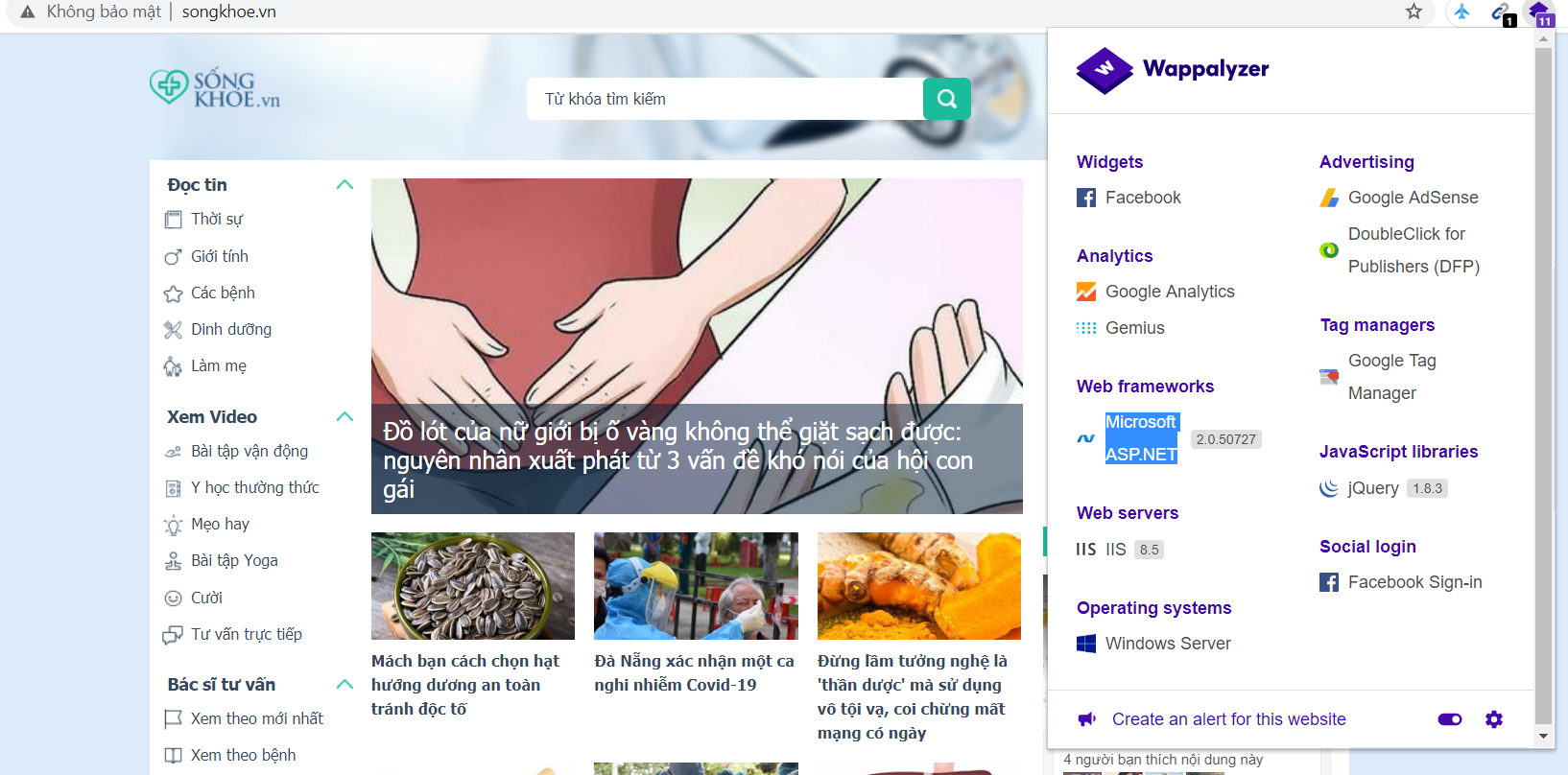




nmap -Pn -A songkhoe.vn



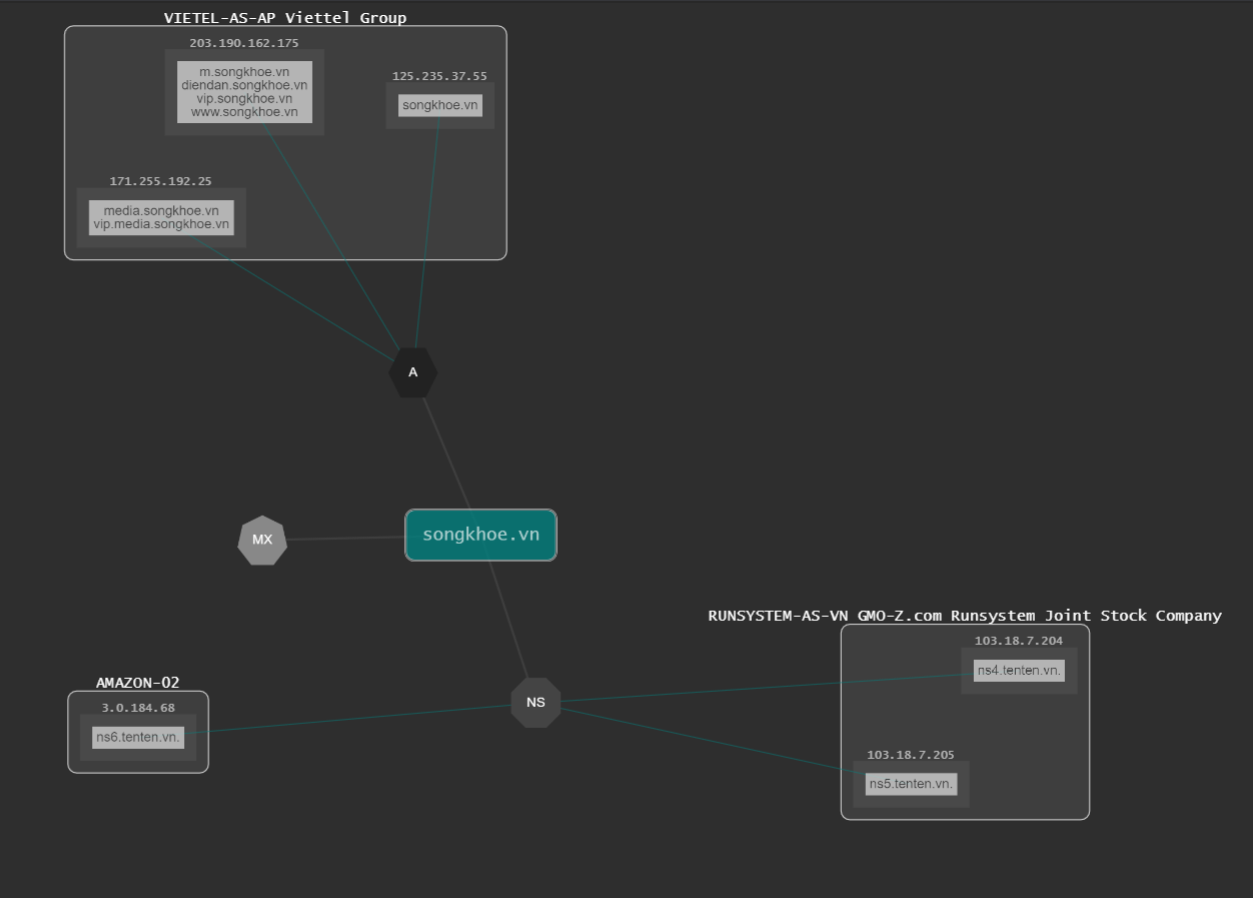
Truy cập songkhoe.vn trên trình duyệt sử dụng extension Wappalyzer



Không có bản ghi MX,TXT trên songkhoe.vn

Host Records (A):

* songkhoe.vn 125.235.37.55(125.235.37.55.adsl.viettel.vn) HTTP: Microsoft-IIS/8.5
* media.songkhoe.vn 171.255.192.25(dynamic-ip-adsl.viettel.vn) HTTP: nginx/1.10.2
* vip.media.songkhoe.vn 171.255.192.25(dynamic-ip-adsl.viettel.vn) HTTP: nginx/1.10.2
* m.songkhoe.vn 203.190.162.175 HTTP: Microsoft-IIS/8.5
* diendan.songkhoe.vn 203.190.162.175 HTTP: Microsoft-IIS/8.5
* vip.songkhoe.vn 203.190.162.175 HTTP: Microsoft-IIS/8.5
* www.songkhoe.vn 203.190.162.175 HTTP: Microsoft-IIS/8.5



Quét trên <https://dnsdumpster.com/> tên miền songkhoe.vn.

HTTP đang chạy trên TCP. Kết quả là máy chủ web có thể đối mặt với nhiều cuộc tấn công liên quan đến TCP. Tập trung sử dụng các kỹ thuật tấn công Từ chối Dịch vụ (DoS) như Syn floods, ACK floods, RST floods, Push-ACK floods, FIN floods.