# Kiểm thử xâm nhập & Reconnaissance

* Pentest là gì?

Là hình thức đánh giá mức độ an toàn của một hệ thống IT bằng các cuộc tấn công mô phỏng thực tế. Hiểu đơn giản , Pentest cố gắng xâm nhập vào hệ thống để phát hiện ra những điểm yếu tiềm tàng của hệ thống mà tin tặc có thể khai thác và gây thiệt hại.

Mục tiêu để phát hiện ra các lổ hổng và khắc phục để ngăn chặn các điểm yếu này bị khai thác trong tương lai.

* Các loại Pentest.

Có 3 loại kiểm thử bảo mật là Black Box , White Box , Grey Box.

White Box: Là hình thức mà các pentester sẽ được cung cấp các thông tin về hệ thống như : user , pass , source code … Và sử dụng các thông tin đó để tiến hành kiểm tra và đánh giá bảo mật.

Gray Box: Sẽ được cung cấp một phần thông tin về hệ thống và người kiểm thử sẽ sử dụng lượng thông tin đó để tấn công hệ thống.

Black Box: là hình thức kiểm thử mà người kiểm sẽ không có bất kỳ thông tin nào về hệ thống nó giống như một người dùng trong thực tế đang tìm cách tấn công vào server.

* Quy trình kiểm thử xâm nhập.

B1: Khảo sát mục tiêu và thu thập thông tin mục đích người kiểm thử thu thập các thông tin mà họ tìm được về hệ thống chẳng hạn như với một mục tiêu là web thì các thông tin có thể là server của website là gì , mã nguồn của trang web , các domain port , các thông tin về các plugins hay các sub domain trên trang web. Từ những thông tin này kẻ tấn công có thể xác định được hướng tấn công ở các bước sau.

B2: Dò quét điểm yếu mục đích là để tìm các điểm yếu có thể bị khai thác trên hệ thống vd như một người kiểm thử thu thập thông tin rằng server đang dùng mã nguồn php và sử dụng server là apache. Lúc này kẻ tấn công sẽ sử dụng các công cụ scaning để dò tìm các lổ hổng tồn tại trên mã nguồn php hay các lổ hổng có trên apache.

B3: Xác minh lổ hổng và tấn công kiểm thử. Sau khi tìm hiểu các thông tin và scaning các lổ hổng mà có thể tồn tại trên đó. Nếu xác định được nó có tồn tại lổ hổng ta có thể tấn công vào hệ thống đó. Thường các lỗi như này sẽ tồn tại các mã khai thác trên google ta có thể tải về và sử dụng.

B4: Đánh giá mức độ nguy hiểm các lổ hổng. Việc đánh giá lổ hổng sẽ giúp ta biết đâu là các lổ hổng ảnh hưởng mạnh tới hệ thống để ta có thể ưu tiên việc fix các lổ hổng đó trước. Đồng thời cũng cho ta biết được nó ảnh hưởng như nào tới hệ thống để ta có thể tìm cách ngăn chặn.

B5: Báo cáo và khuyến nghị mục đích là để viết lại bản báo cáo quá trình một người kiểm thử trên một mục tiêu xảy ra như nào. Và đưa ra các khuyến nghị để có thể ngăn chặn các lở hổng.

B6: Tái đánh giá là sẽ kiểm tra và tấn công thử lại lần khác. Để xác minh xem lổ hổng đó còn tại không. Nếu như chưa có cách fix sẽ có những đề xuất để ngăn chặn tạm thời khai thác.

* Reconnaissance/Footprinting

Passive: Là kỹ thuật thu thập thông tin mà người thu thập sẽ không tác động đến mục tiêu. Có nghĩa là bạn sẽ không gửi các yêu cầu đến mục tiêu đo đó web sẽ không biết được là bạn đang thu thập thông tin về nó. Việc thu thập thông tin bị động thường sử dụng các nguồn tài nguyên public có chứa thông tin về mục tiêu.

* Whois lookup: là công cụ tìm kiếm tên miền trên internet để kiểm tra thông tin tên miền. Ngoài việc giúp người dùng kiểm tra một tên miền đã đăng ký chưa còn giúp tìm kiếm thông tin cá nhân của người sở hữu.

Để sử dụng công cụ ta truy cập vào đường link sau <https://vnnic.vn/whois-information> sau đó bạn điền tên trang web mà bạn muốn vào.

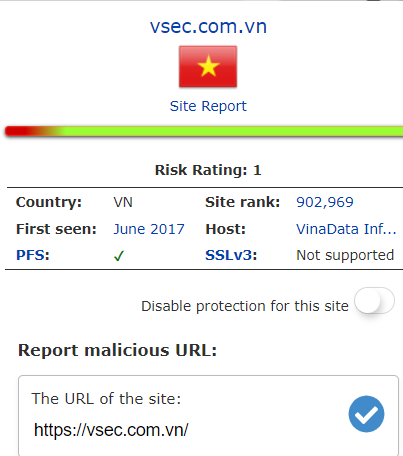
VD: kết quả trả về từ công cụ whois trên trang vnnic.vn

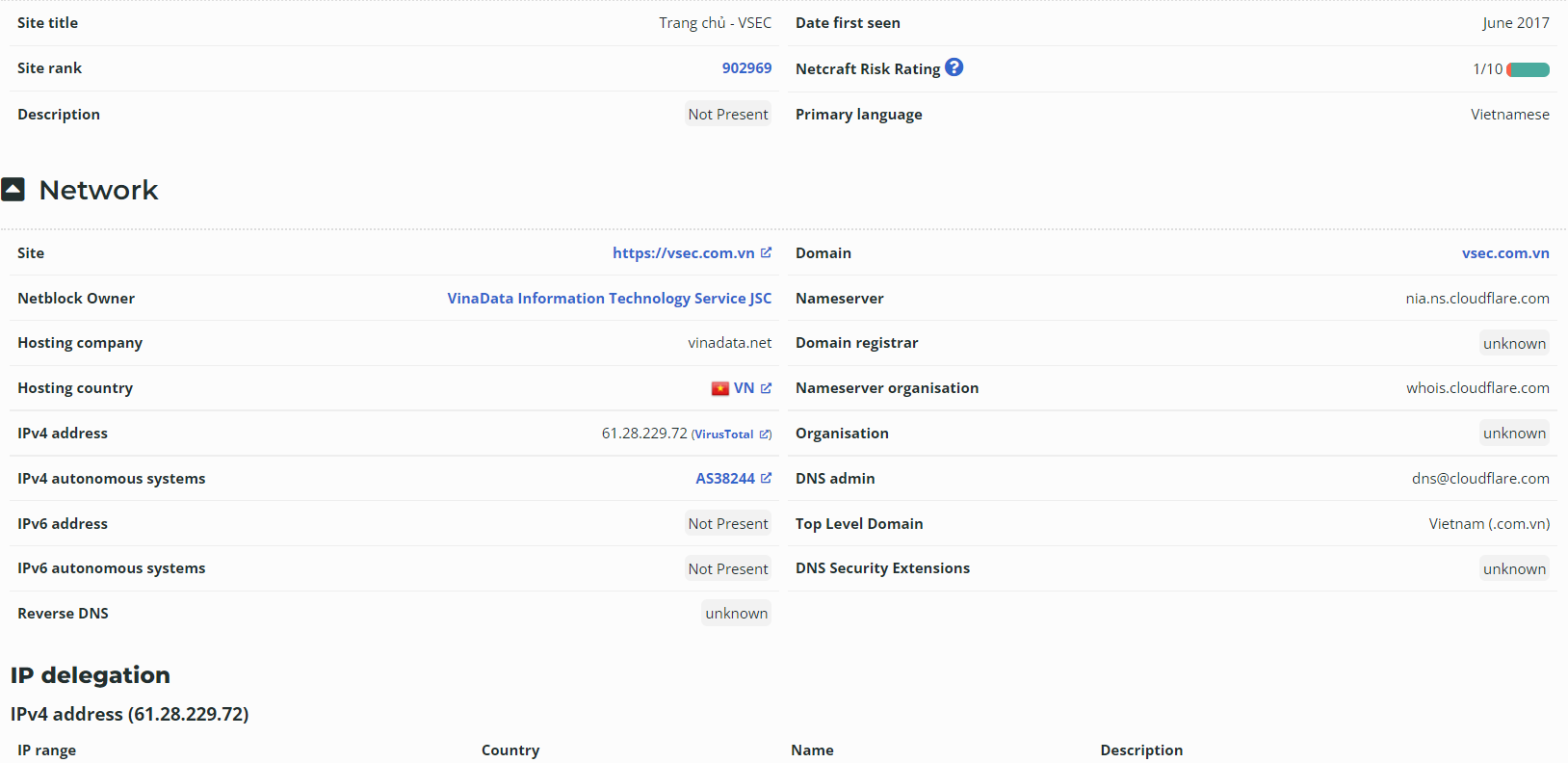


* Netcraft: Là một công cụ sử dụng để kiểm tra thông tin IP hoặc một domain nào đó. Để sử dụng công cụ này ta có 2 cách một là truy cập thẳng vào trang web cách 2 là sử dụng extension trên chrome.

B1: Để sử dụng ta truy cập vào link sau và thêm nó vào <https://chrome.google.com/webstore/detail/netcraft-extension/bmejphbfclcpmpohkggcjeibfilpamia>

B2: Ta truy cập vào website ta muốn và click vào icon netcraft sẽ show một số thông tin về trang web. Hoặc ta có thể ấn site report nó sẽ show thông tin chi tiết cho chúng ta.



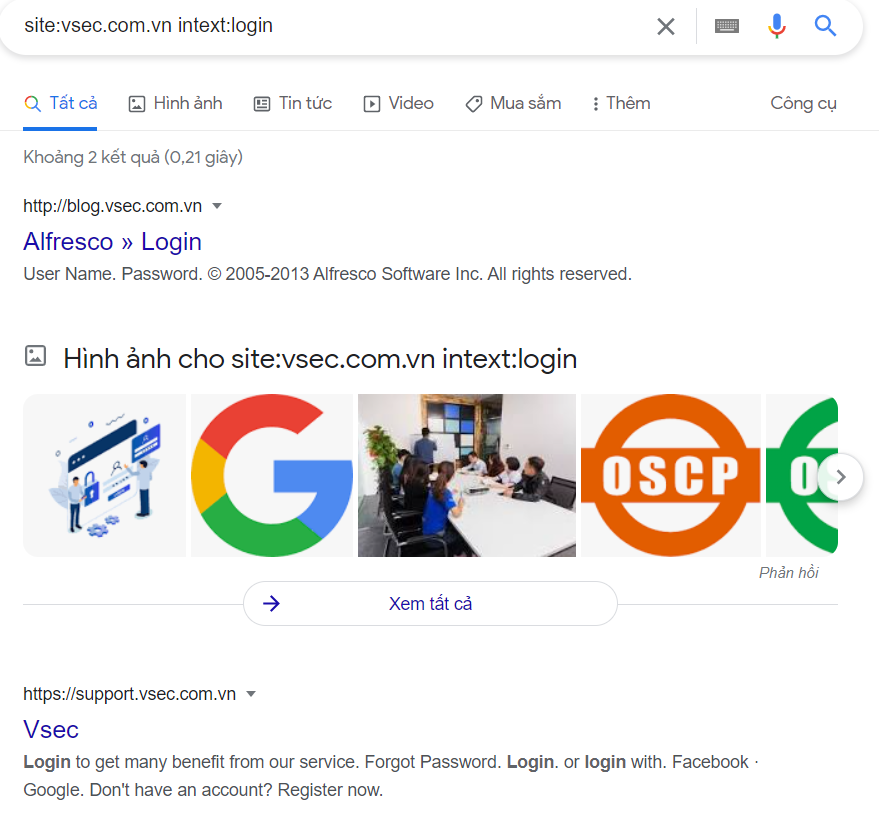


* Google Hacking(dork): Là một kỹ thuật cho phép truy vấn trên công cụ tìm kiếm Google.com , đôi khi được dùng để xác định các lổ hổng trong các ứng dụng web cụ thể. Bên cạnh việc truy vấn từ google có thể tiết lộ các lỗ hổng trong các ứng dụng web, Google Hacking cho phép bạn tìm các dữ liệu nhạy cảm. Việc truy vấn được thực hiện bằng cách kết hợp các toán tử để tìm kiếm một mục tiêu.

Các toán tử được sử dụng trong google hacking:

* “”( dấu ngoặc kép): nó sẽ hiển thị kết quả chính xác mà ta viết vào.
* \*(dấu hoa thị): là một ký tự đại diện.
* Intitle : tìm kiếm trong phần title của trang web.
* .( dấu chấm): là ký tự đại diện cho bất kỳ kí tự nào tại vị trí đó.
* +(dấu cộng): là kí tự để xác định cụm mà mình cần tìm ví dụ như “machine gun”+uzi ta sẽ tìm thông tin về súng máy cụ thể là uzi.
* –( dấu gạch ngang): đi kèm với các điều kiện khác.
* Cache: lấy tất cả các cache mà google cho trang mình tìm kiếm.
* Info: show các thông tin liên quan đến webpage liên kết.
* Site: Chỉ định ra một site mà mình muốn tìm kiếm
* Filetype: giới hạn các loại tệp tin mà mình muốn tìm kiếm.
* Intext: Tìm kiếm các phần nội dung trong web.
* Inurl: Tìm kiếm thông tin với url.
* allintext:/allinurl:/allintitle:

VD: Ta sẽ tìm kiếm các trong site vsec.com.vn có phần nội dung là Login.



* Shodan: Là một công cụ tìm kiếm được phát triển bởi John Matherly. Shodan là một công cụ tìm kiếm các thiết bị trực tuyến trên internet như: máy tính , server , webcam , các thiết bị router…Nó hoạt động bằng cách quét các thiết bị trên internet có mở cống public ra internet và thực hiện phân tích các dấu hiệu được phản hồi về từ các thiết bị. Sử dụng thông tin đó , Shodan có thể cho biết những thứ như máy chủ web (phiên bản) phổ biến nhất hoặc có bao nhiêu máy chủ FTP ẩn danh tồn tại ở một vị trí cụ thể , hay trả về danh sách các camera có thể truy cập trực tuyến qua internet. Với shodan bạn có thể tìm kiếm bất kỳ thiết bị nào trên internet miễn là chúng kết nối internet và mở cổng public.

Cách thức hoạt động:

* + Tạo một địa chỉ IPV4 một cách ngẫu nhiên.
  + Chọn port ngẫu nhiên và gửi câu lệnh kiểm tra.
  + Xem nội dung phản hồi và từ xác định xem đó là thiết bị gì và đang chạy trên cổng nào
  + Lặp lại quá trình trên với với ip port mới.

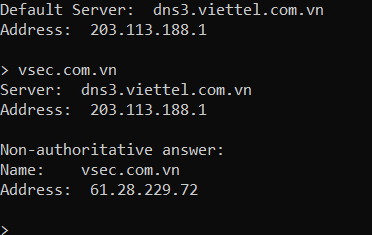
Các bộ lọc thông dụng:

* + City: Tìm các thiết bị trong phạm vi thành phố.
  + Country: Giống như city nhưng tìm trong phạm vi quốc gia.
  + Hostname: tìm theo hostname.
  + Net: Tìm kiếm bằng địa chỉ IP hoặc CIDR
  + Os: tìm theo hệ điều hành.
  + Port: Tìm theo port.
  + Before/after: Tìm kiếm trong một khoảng thời gian.

VD:

* DNS lookup: Là quá trình tìm kiếm IP phân giải tên miền mà bạn muốn. Công cụ này được tích hợp sẵn trên windows hoặc bạn có thể truy cập qua các trang web có cài đặt công cụ này.

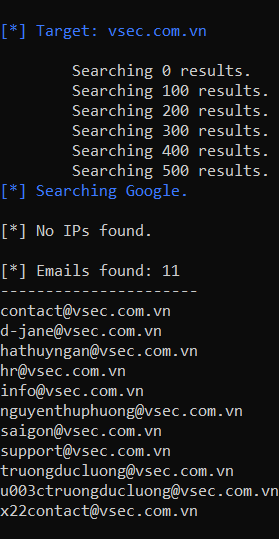
VD:Ta truy cập cmd và gõ câu lệnh nslookup sau đó chỉ cần điền domain vào nó sẽ trả về kết quả là IP của trang web đó.



* TheHarvester là một công cụ thu thập thông tin về các trang web nó được sử dụng với nhiều mục đích phổ biến nhất là thu thập email của trang web.

Cách cài đặt: sudo apt-get install theHarvester

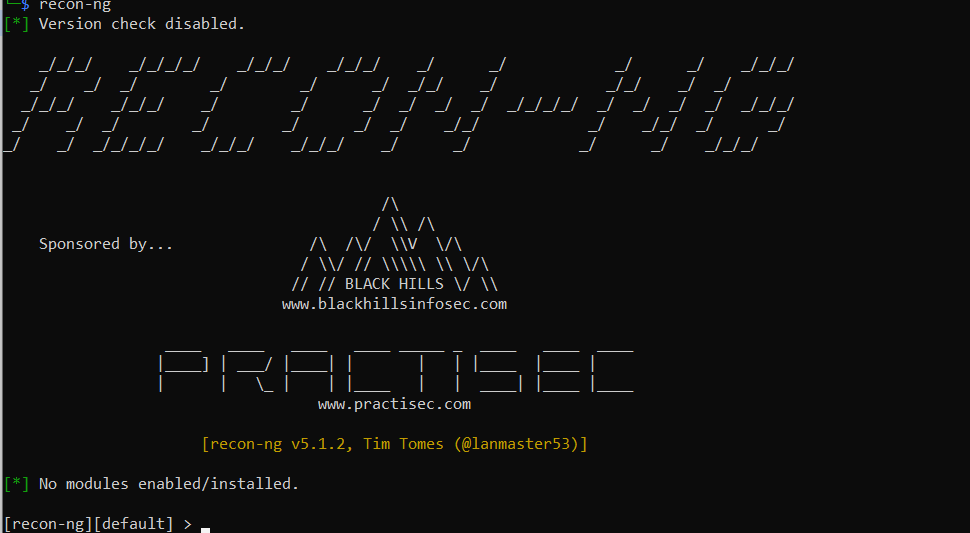
VD: Thu thập thông tin về email của một trang web



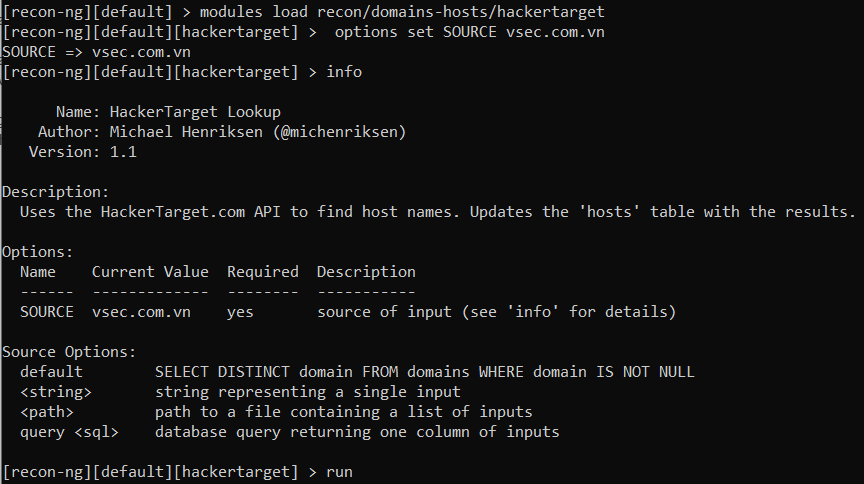
* Recon-ng: Là framework dùng để thu thập thông tin từ các web application.

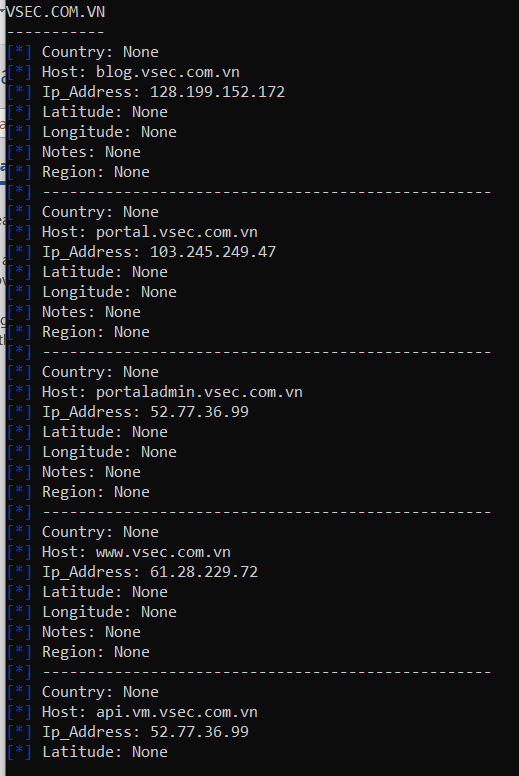
Cách cài đặt: sudo apt-get install recon-ng -y

Sau khi cài đặt xong để khởi động ta chỉ cần gõ recon-ng vào màn hình nó sẽ đưa ta vào giao diện của tool.



VD:





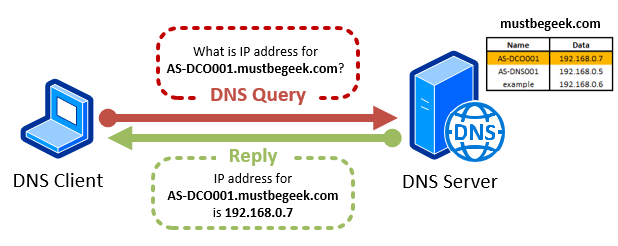
Active: là khi bạn tương tác trực tiếp với hệ thống máy tính để thu thập thông tin cụ thể của hệ thống về mục tiêu. Không giống như thu thập thông tin thụ động dựa vào thông tin có sẵn công khai, thu thập thông tin chủ động dựa vào các công cụ sẽ gửi các loại yêu cầu khác nhau đến máy tính. Mục đích là thu thập thông tin về thiết bị đó hoặc các thiết bị khác được kết nối với nó trên cùng một mạng.

* + DNS enumeration: Là quá trình tìm kiếm các thông tin có được về DNS của mục tiêu. Việc tìm kiếm này có thể tận dụng các công cụ để dễ dàng tìm kiếm được thông tin muốn có.

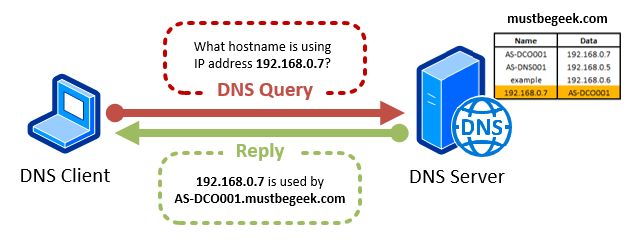
Các công cụ dns enumeration phổ biến

* + DNS forward/reverse lookup: Hai khái niệm này có mục đích khác nhau. Cái đầu tiên và được triển khai phổ biến nhất là Forward Lookup Zones , nơi thực hiện các bản dịch chuỗi tên máy chủ sang địa chỉ IP . Cái thứ hai là Reverse Lookup Zones , nơi nó làm ngược lại với cái trước.

DNS Forward: Khi truy vấn DNS đến từ máy khách, máy chủ DNS hoạt động bằng cách tra cứu giá trị chuỗi tên máy chủ trên cột “ Tên ”, sau đó trả về giá trị địa chỉ IP trên cột “ Dữ liệu ” làm câu trả lời cho truy vấn



DNS Reverse: Là quá trình tìm domain khi biết được IP.



Zone Transfer: có thể hiểu là việc copy zone file( bao gồm tất cả DNS name nằm trong zone) từ Master DNS server sang Slave DNS server. Chính xác hơn thì việc copy sang Slave DNS server đòi hỏi phân quyền mới được thực hiện. Tuy nhiên một số server sẽ cấu hình sai dẫn điện các Slave DNS server không được phép có thể thực hiện zone tranfer.

Để thực hiện có thể sử dụng câu lệnh

Host -l <domain name> <dns server address>

Lưu ý: Options -l tương ứng với list zone để thực hiện quá trình zone transfer.

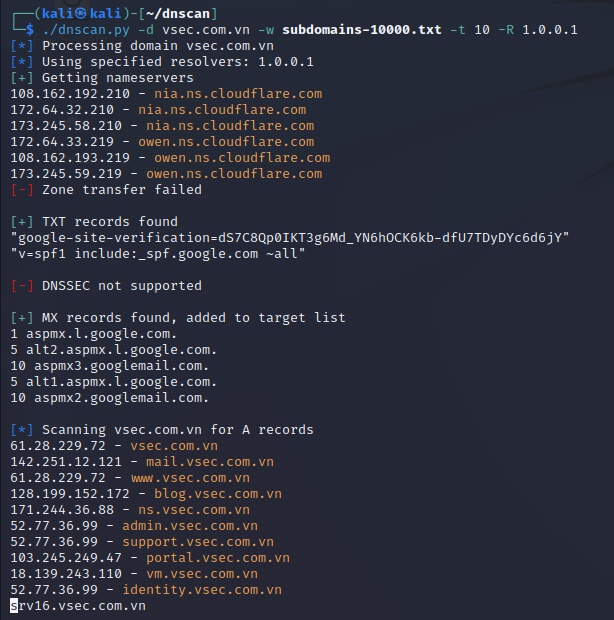
VD: với một trang web website.com sẽ có 2 dns server là ns1.website.com và ns2.website.com

host -l website.com ns1.website.com

host -l website.com ns2.website.com

Dns Brute force: Các cuộc tấn công brute force sử dụng tập lệnh hoặc các công cụ khác để tìm tất cả các sub domain và làm lộ mạng công khai của tổ chức và có thể là riêng tư.

VD: sử dụng công cụ dns để brute force dns



Amass: Là công cụ thực hiện lập bản đồ mạng và phát hiện tài nguyên bằng cách sử dụng các kỹ thuật thu thập thông tin từ các mã nguồn mở.

Cài đặt: trên terminal ta thực hiện câu lệnh: apt-get install amass -y

Giao diện



Subcommand:

* + - Amass intel: Thu thập thông tin về mục tiêu.
    - Amass enum: thu thập thông tin DNS và thiết lập bản đồ hệ thống mạng.
    - Amass viz: Tạo các h ình ảnh trực quan về quá trình thu thập.
    - Amass track: so sanh sự khác biệt giữa các kiểu enum
    - Amass db: Quản lý cơ sở dữ liệu biểu đồ lưu trữ kết quả điều tra

Ý nghĩa các flag trong subcommand tham khảo ở đây: https://github.com/OWASP/Amass/blob/master/doc/user\_guide.md

VD: Ta có thể thu thập thông tin bằng subcommand intel ở mode active với mục tiêu là các dãy ip 192.168.1.2-60 kết hợp với whois

amass intel -active -whois -addr 192.168.2.1-60

Lưu ý ta có thể sử dụng domain bằng flag -d

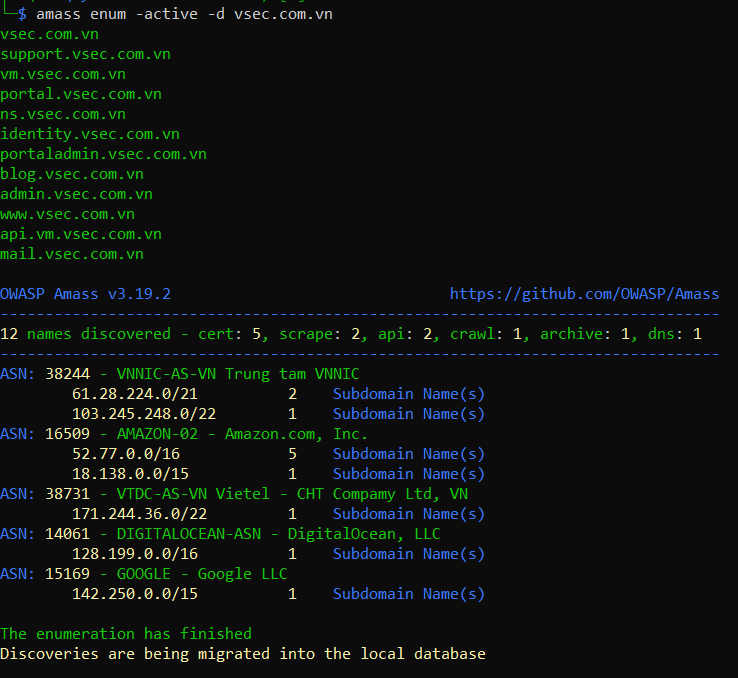
amass intel -active -d domanin.com

Ta có thể thu thập thông tin về hệ thống mạng và dns qua subcommand enum với mode active trên domain website.com và chỉ ra các blacklist subdomain không cần kết hợp brute force dns.

amass enum -active -brute -blf data/blacklist.txt -d website.com

Subfinder: Subfinder là một công cụ khám phá tên miền phụ giúp phát hiện ra các tên miền phụ hợp lệ cho các trang web bằng cách sử dụng các nguồn trực tuyến thụ động. Nó có kiến ​​trúc mô-đun đơn giản và được tối ưu hóa về tốc độ. subfinder được xây dựng để thực hiện một việc duy nhất - liệt kê tên miền phụ thụ động và nó thực hiện điều đó rất tốt.

VD:Sử dụng công cụ amass để enum về trang vsec.com.vn ta thu được mốt số 12 sub domain ,5 chứng chỉ ,2 api ,1 dns và 1 tệp

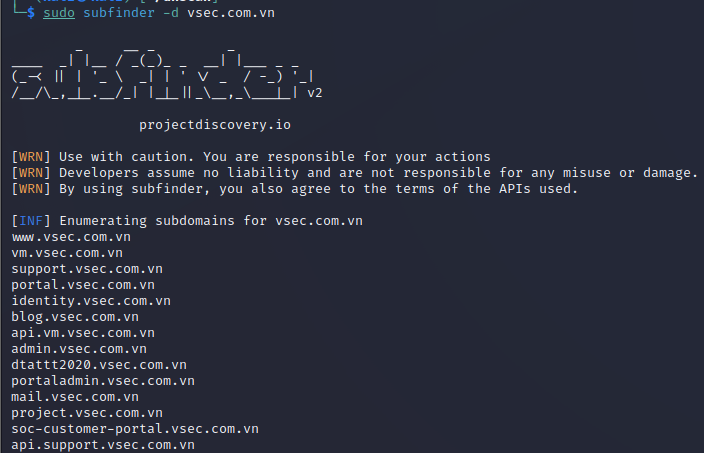


Cài đặt: apt-get install subfinder -y

Để chạy tool ta chỉ cần sử dụng câu lệnh subfinder -d website.com với -d là options chỉ ra domain muốn enum.

Ngoài ra ta có thể sử dụng một file chứa các domain bằng options -dLhay chỉ ra các source không muốn sử dụng để enum bằng options -exclude-sources string hay show kết quả các website hoạt động với options -nW.

VD:



Identify Platform/Frameworks: Là các công cụ dùng để xác định các platform hay các framework mà trang web đang được sử.

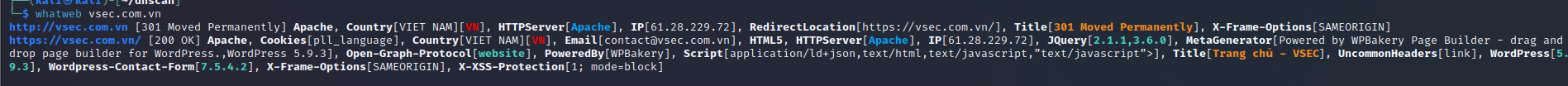
Có nhiều công cụ có thể làm được việc này. Sau đây là 2 công cụ phổ biến được sử dụng để thực hiện công việc trên.

Whatweb: xác định các trang web. Mục tiêu của nó là trả lời câu hỏi, Trang web đó là gì? WhatWeb nhận ra các công nghệ web bao gồm hệ thống quản lý nội dung (CMS), nền tảng blog, gói thống kê / phân tích, thư viện JavaScript, máy chủ web và thiết bị nhúng.

Cài đặt: apt-get install whatweb -y

Sử dụng: whatweb domain.com

VD:



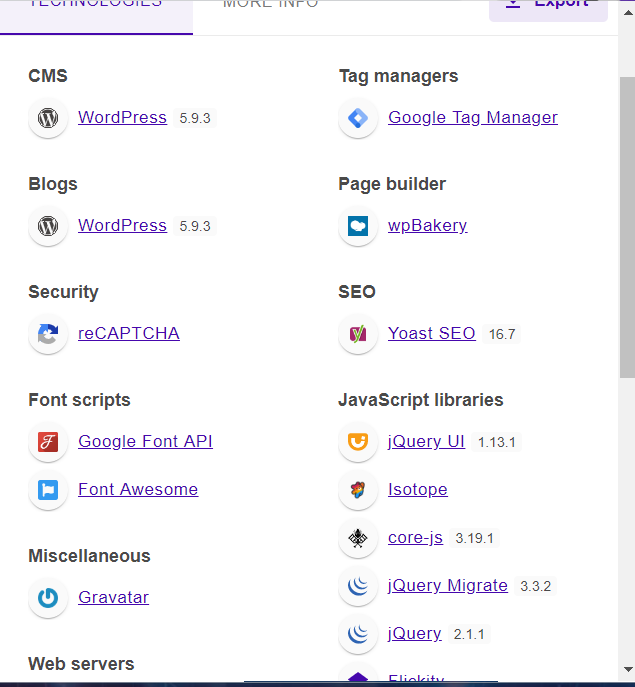
Wappalyzer: Là một extension giúp định nghĩa các công nghệ chính sử dụng trong web.

Cài đặt: <https://chrome.google.com/webstore/detail/wappalyzer-technology-pro/gppongmhjkpfnbhagpmjfkannfbllamg?hl=vi>

Truy cập vào trang web và ấn thêm.

Sử dụng: Sau khi cài đặt chỉ cần ghé vào trang web mục tiêu và click vào biểu tưởng của extension nó sẽ show ra cho ta các thông tin mà ta cần.

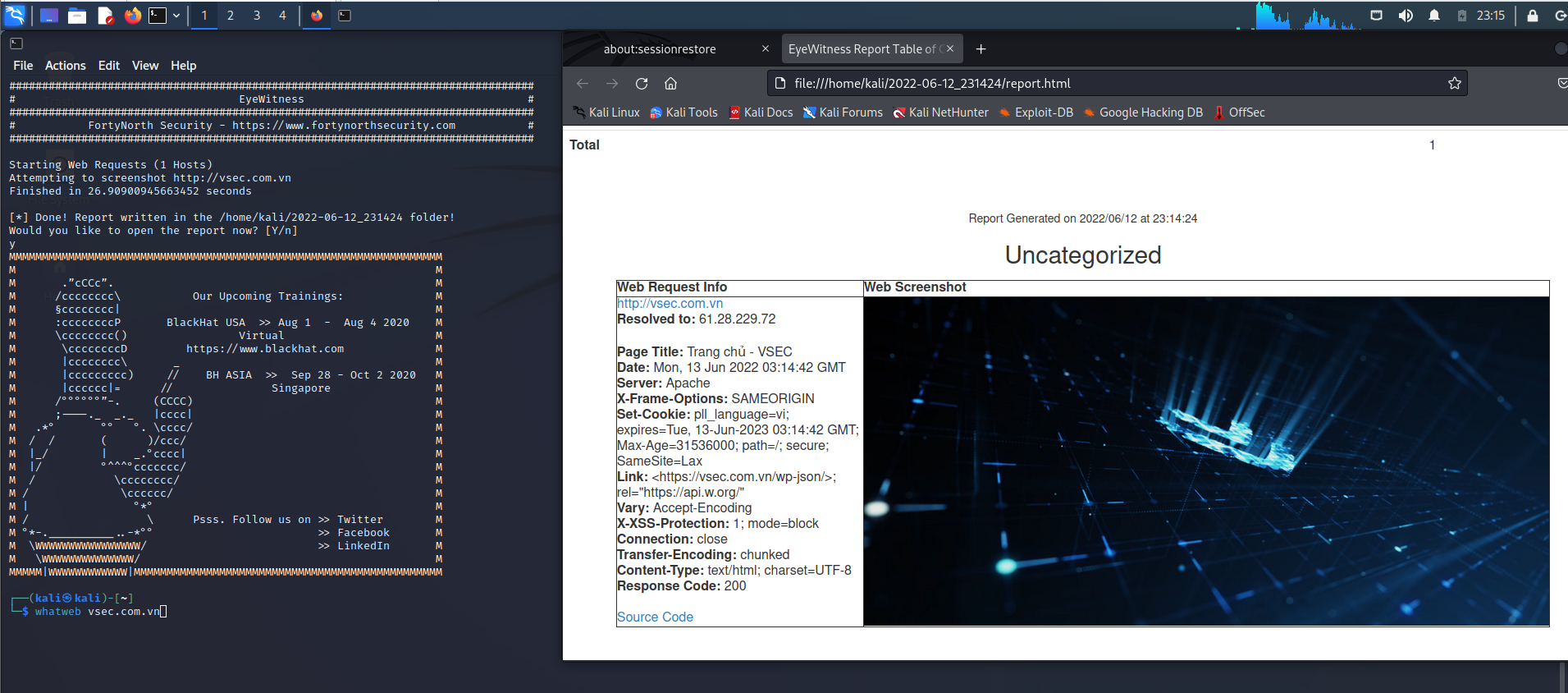
VD: sử dụng wappalyzer trên trang vsec.com.vn



Screen shot: Là các công cụ có tính năng chụp màn hình trang web và đưa kết quả cho người dùng. Ở đây ta sẽ sử dụng công cụ eyewitness được thiết kế để chụp ảnh màn hình của các trang web, cung cấp một số thông tin về tiêu đề máy chủ và xác định thông tin đăng nhập mặc định nếu có thể.

Vd: sử dụng công cụ để chụp màn hình website.

Eyewitness –web -f file.txt ( file.txt là file chứa các url ta cần quét)



* + Nmap là một công cụ được sử dụng để thực hiện các hành vi quét một mục tiêu để tìm kiếm các thông tin quan trọng. Nmap được sử dụng để scan network và port của mục tiêu. Ngoài nó ra nó còn tích hợp các script để thực hiện các quá trình khác như scan lỗi …

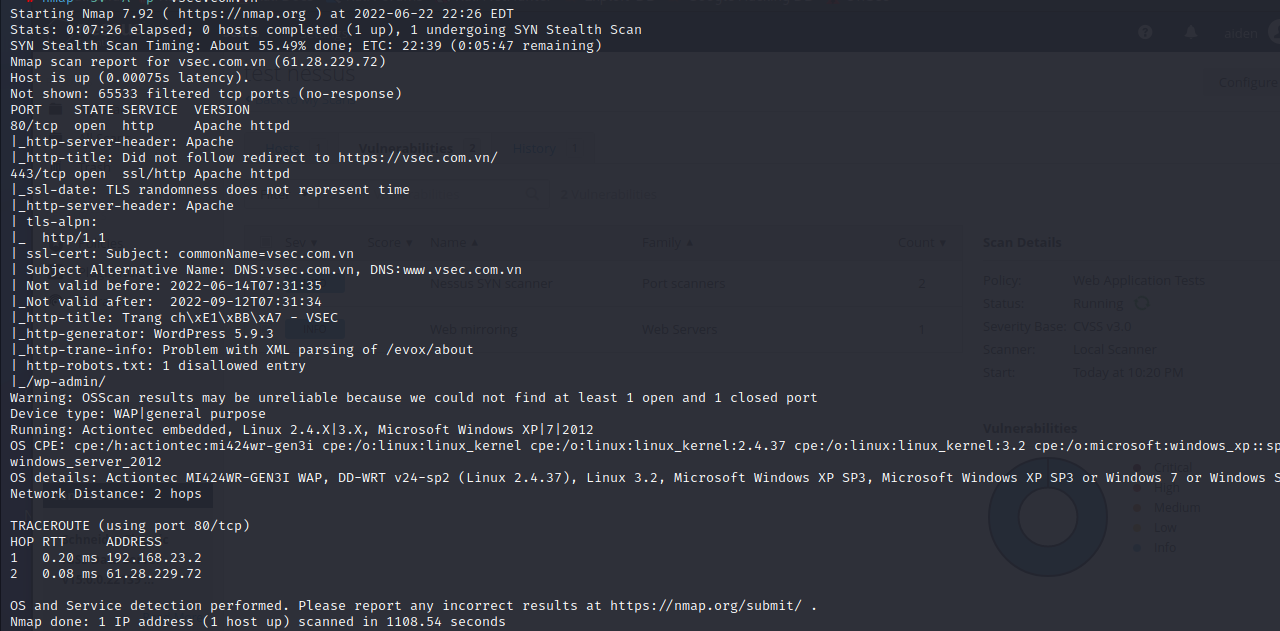
Ta có thể dùng nmap để quét một mục tiêu như sau: nmap -sV -A -p- host

-sV để thực hiện việc quét các version và các dịch vụ mục tiêu.

-A để kích hoạt detect os,version

-p- là để chỉ số port cần scan ( -p- ở đây nghĩa là scan hết port)

Sau đây là kết quả quá trình scanning



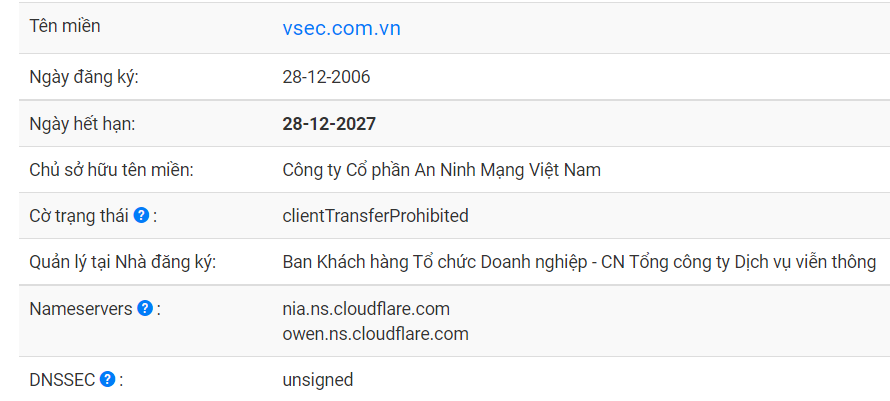
Ta phát hiện website chạy trên 2 port là 80 và 443 với 2 dịch vụ là http và https với server là apache sử dụng wordpress 5.9.3 với file robots.txt có 1 entry là /wp-admin/

Cùng với các thông tin về hệ điều hành( Ở đây do không xác dịnh rõ được server đang chạy trên OS nào nên nó sẽ để ra 2 bản là windows và linux cùng với các version trong phạm vi mà server đang xử dụng.

* Recon một mục tiêu thực tế.

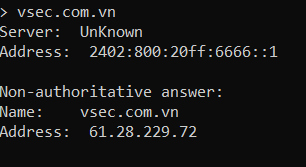
Trang web vsec.com.vn

Đầu tiên ta sử dụng công cụ whois để thu thập các thông tin về domain.



Như hình ta thu thập được domain đăng ký vào ngày 28-12-2006 và hết hạn vào 28-12-2027 thuộc sở hữu của công ty cổ phần An ninh mạng VN với 2 name server l2 nia.ns.cloudflare.com và owen.ns.cloudflare.com

Sau đó ta sử dụng công cụ nslookup để thu thập thông tin về địa chỉ IP của mục tiêu

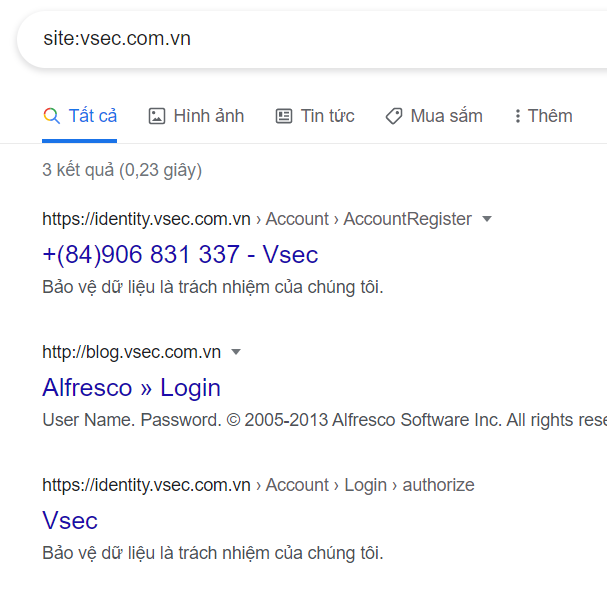


Như hình dưới ta thu về được IP là 61.28.229.72 nhưng có vẻ đây là ip khác không phải của trang vsec.com.vn

Sau đó ta sẽ sử dụng công cụ google hacking database để tìm kiếm các thông tin của web.

Site:vsec.com.vn với lệnh này ta sẽ tìm kiếm các thông tin về trang vsec.com.vn

Kết quả trả về là 3 subdomain của trang web đó.

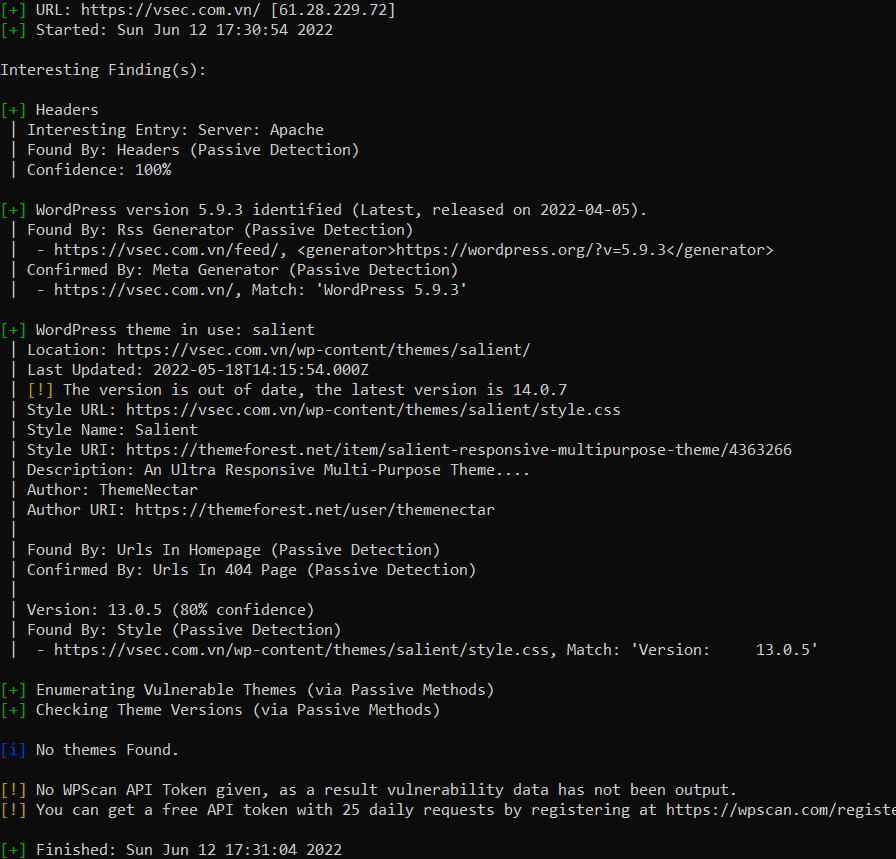


Sau đó ta thử truy cập vào trang web chính và viewsource ta phát hiện được web đang sử dụng công cụ wordpress. Ta có thể sử dụng công cụ whatweb hay Wappalyzer cho mục đích này.

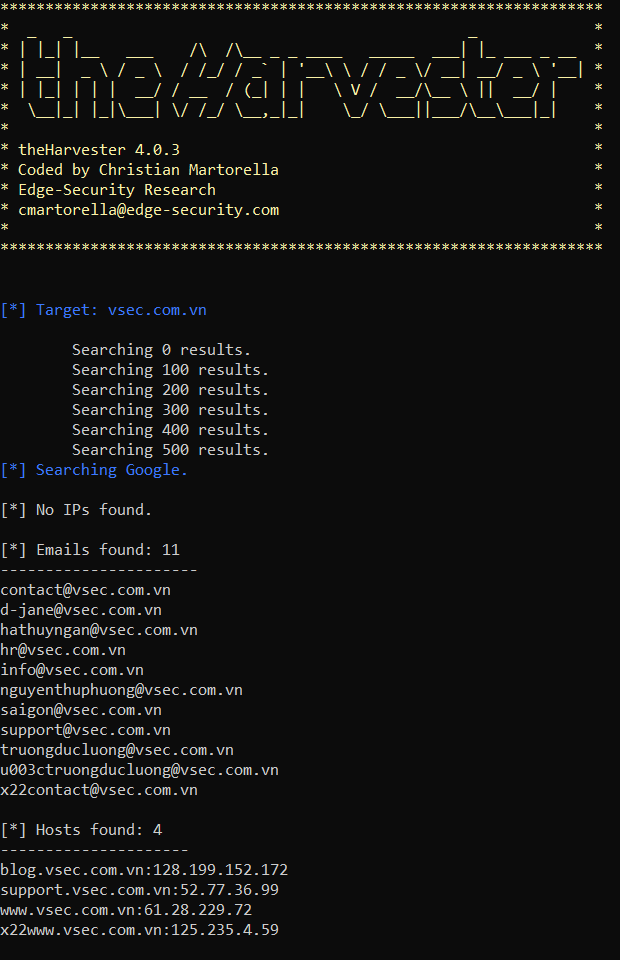


Tới đây ta có thể sử dụng công cụ wpscan để quét các thông tin về wordpress như plugins …

sudo wpscan --url vsec.com.vn -e vt --stealthy --random-user-agent --plugins-version-detection aggressive.

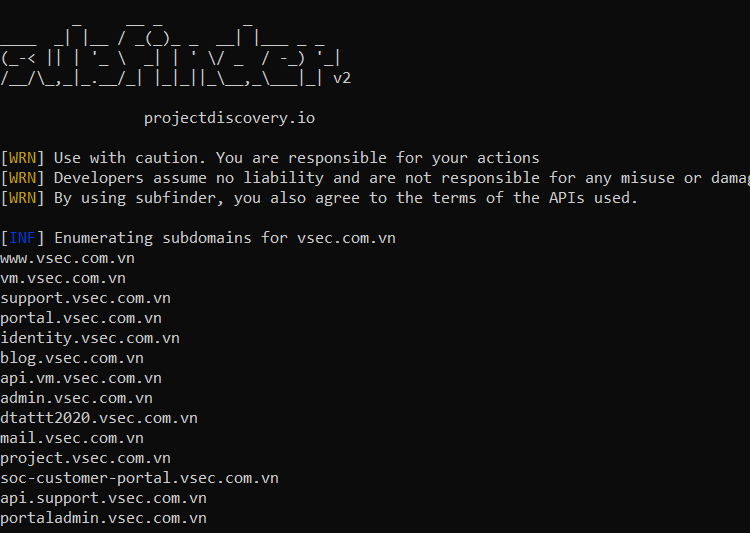


Sau đó ta tiến hành thu thập thông tin bằng công cụ theHarvester



Sau đó ta tiến hành thu thập thông tin về subdomain bằng công cụ subfinder

Subfinder -d vsec.com.vn -nW

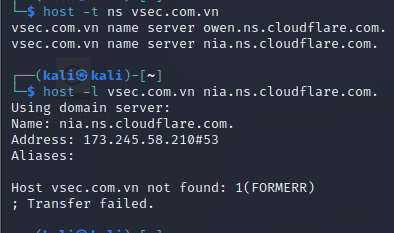


Ta tiến hành tấn công zone transfer.

Đầu tiên ta tiến hành thu thập ns server của web.

Ta có thể sử dụng câu lệnh host -t ns domain

Sau đó ta sử dụng câu lệnh host -l domain (name server vừa tìm được)



Kết quả:

Host : vsec.com.vn

Chử sở hữu: công ty Cổ phần An Ninh Mạng Việt Nam

nameserver: nia.ns.cloudflare.com , owen.ns.cloudflare.com

ip: 61.28.229.72

Wordpress 5.9.3

theme wp: salient 13.0.5(80%)

Email

contact@vsec.com.vn

d-jane@vsec.com.vn

hathuyngan@vsec.com.vn

hr@vsec.com.vn

info@vsec.com.vn

saigon@vsec.com.vn

support@vsec.com.vn

u003ctruongducluong@vsec.com.vn

x22contact@vsec.com.vn

domain

blog.vsec.com.vn:128.199.152.172

www.vsec.com.vn:61.28.229.72

x22www.vsec.com.vn:125.235.4.59

www.vsec.com.vn

vm.vsec.com.vn

support.vsec.com.vn

portal.vsec.com.vn

identity.vsec.com.vn

blog.vsec.com.vn

api.vm.vsec.com.vn

admin.vsec.com.vn

dtattt2020.vsec.com.vn

mail.vsec.com.vn

project.vsec.com.vn

portaladmin.vsec.com.vn

identity.vsec.com.vn

blog.vsec.com.vn

* Tìm hiểu môt số công cụ scan website cơ bản: wpscan, nikto, owasp zap, nessus, acunetix

Wpscan: là black box vulnerability scanner cho WordPress được viết bằng PHP chủ yếu tập trung vào các loại lỗ hổng khác nhau trong WordPress, WordPress themes, và plugins.

Những điều wpscan có thể làm:

* Phát hiện phiên bản WordPress hiện đang được cài đặt.
* Có thể phát hiện các tệp nhạy cảm như readme, robots.txt, cơ sở dữ liệu thay thế tệp,...
* Phát hiện các tính năng được kích hợt trên WordPress hiện đang được cài đặt.
* Liệt kê phiên bản và tên của theme.
* Phát hiện các plugin đã cài đặt và cho bạn biết nó đã lỗi thời chưa.
* Liệt kể tên các users.

Cách sử dụng:

Wpscan –url website.com

Ngoài ra ta có thể thêm các options khác vào như:

-e là enumeration mode

-o là xuất output ra file

--user-agent chỉ ra user-agent ta muốn dùng

--rua random user agent

--http-auth dùng để truyền user login vào

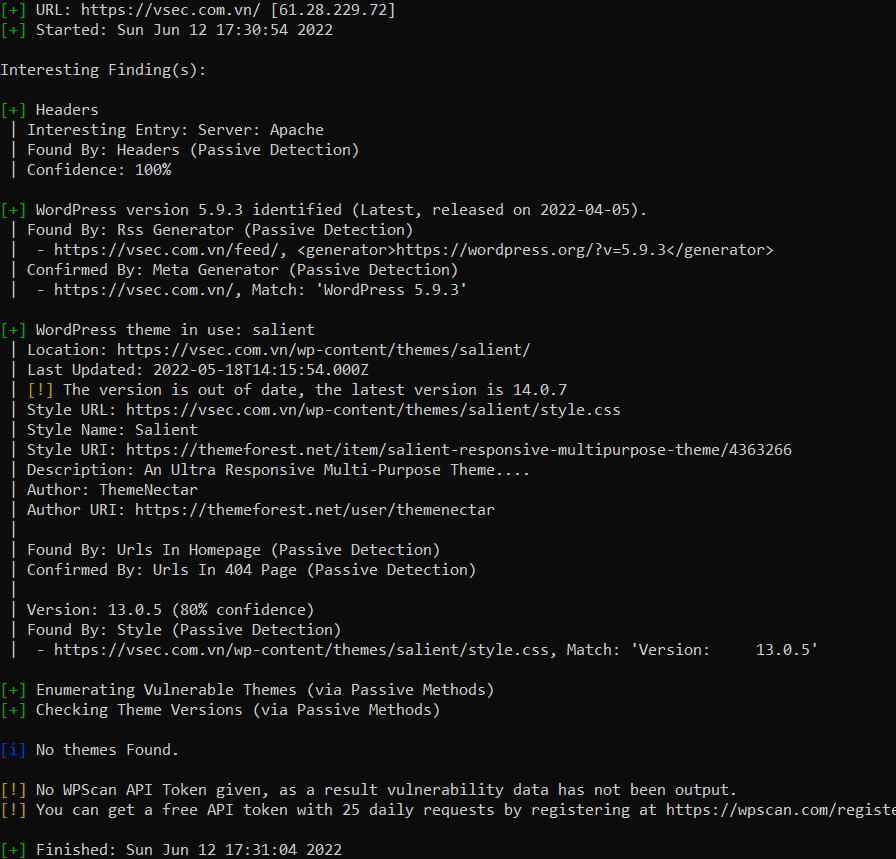
--plugins-detection phát hiện các plugins

--password-attack để brute force attack

-P trỏ đường dẫn file password

-U trỏ đường dẫn file user name.

VD: sử dụng wpscan để scan một trang wordpress



Ưu điểm: là công cụ hàng đầu trong việc thu thập các thông tin về wordpress. Hỗ trợ nhiều các tính năng quan trọng như là detect plugins version và phát hiện lỗi , brute force. Dể sử dụng

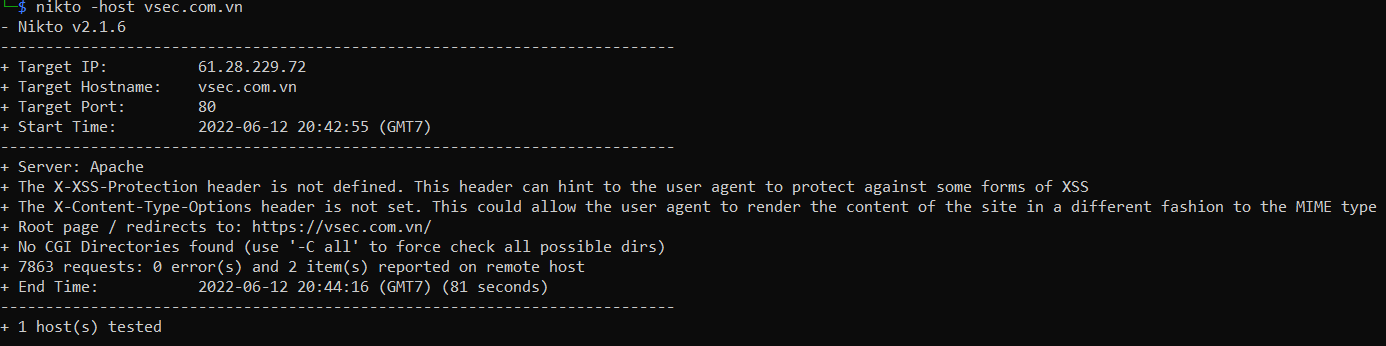
Nhược điểm: Chỉ có thể thu thập được trên các trang wordpress.

Nikto: Nikto là một phần mềm mã nguồn mở được sử dụng kiểm tra các vấn đề bảo mật của Web Server bằng một hệ thống cơ sở dữ liệu riêng đến khoảng 70 ngàn lỗi bảo mật thông thường được tìm thấy và cập nhật với từng phiên bản.

Cách sử dụng:

Nikto -host website.com

Nó sẽ sử dụng db của nó và scan toàn bộ kết quả và trả về cho người dùng



Kết quả cho ta thấy không tìm được lỗi nào có trong csdl của nó nhưng có môt số header không được set điều này có thể dẫn đến một số cách tấn công.

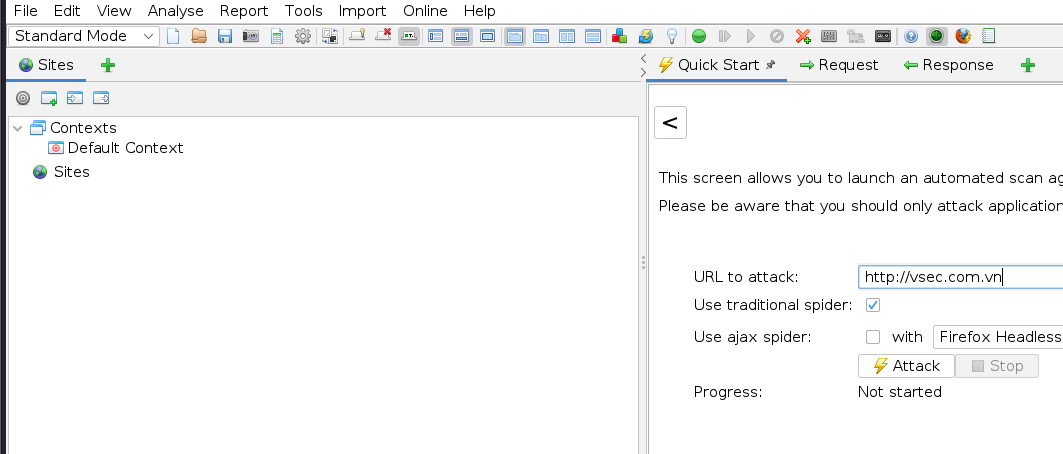
Ưu điểm: Dễ sử dụng , có tích hợp các tính năng quan trọng như là scan lỗi. Hỗ trợ scan nhiều mã nguồn khác nhau.

Nhược điểm: tool này không quá mạnh mẽ trong việc phát hiện các lổ hổng.

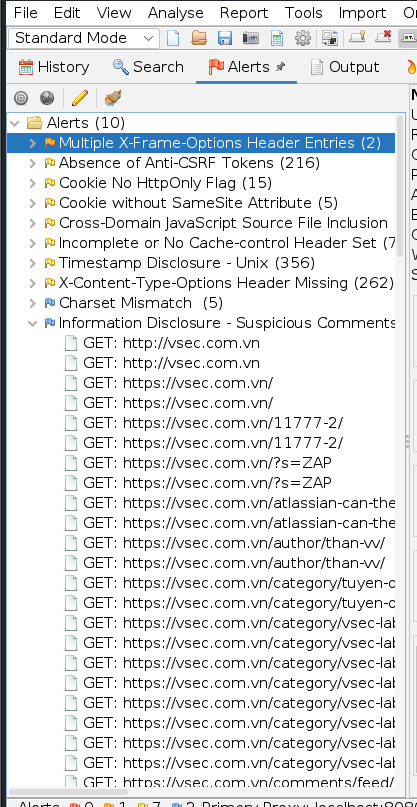
-owasp zap: Owasp Zap – The Open Web Application Security Project được hiểu là dự án mở về bảo mật ứng dụng web. Đây là một dự án được cả cộng đồng chung tay tham gia, giúp các tổ chức có thể phát triển mở hoặc bảo trì các ứng dụng ở trạng thái an toàn. Chúng được người dùng biết đến nhiều nhất với tính năng quét lỗi bảo mật của ứng dụng web, mã nguồn mở

VD:Sử dụng công cụ owasp để dò quét tìm kiếm các thông tin về website:

Đầu tiên ta sẽ điền url cần scan vào



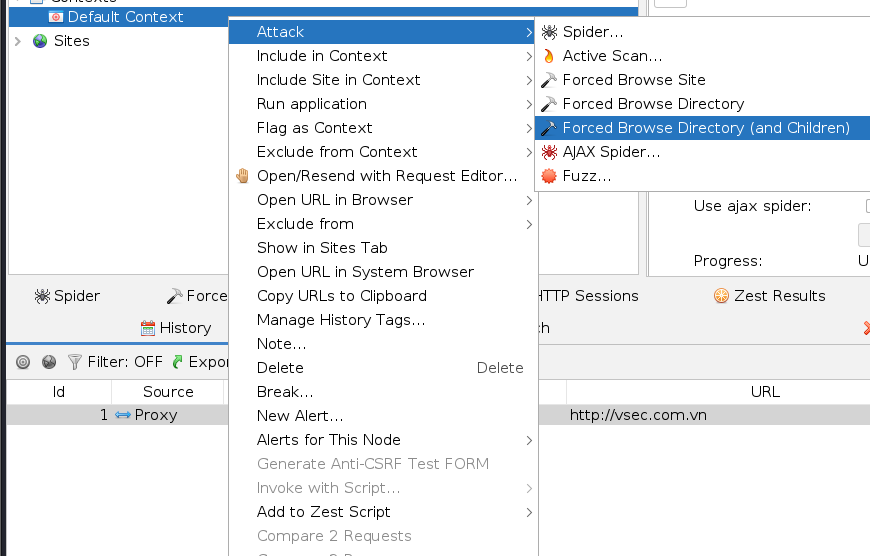
Sau đó nó sẽ spider website và trả về kết quả như hình dưới:



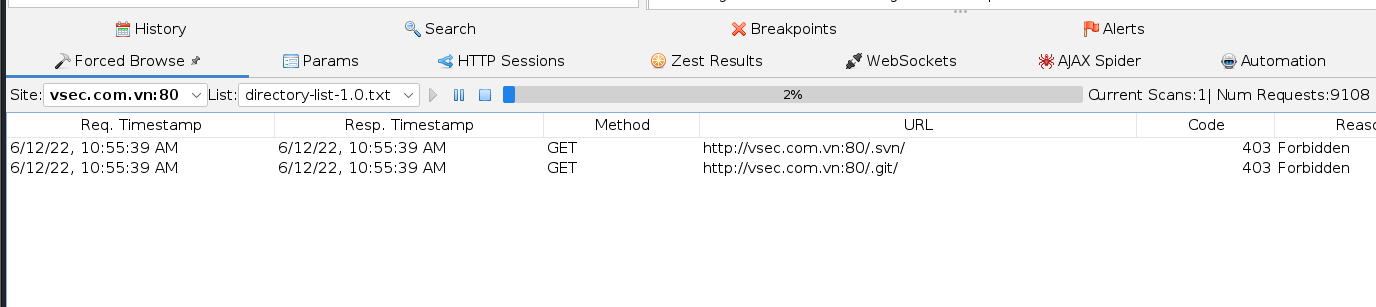
Kết quả đưa ra 10 cảnh báo và một số dường dẫn mà nó đã spider được.

Ngoài ra ta có thể scan sub directory bằng cách sau

Click phải chọn attack chọn force browse …



Sau đó nó sẽ chuyển ta đến giao diện khác ta sẽ chọn wordlist ta muốn và click scan nó sẽ scan và trả về kết quả cho ta.



Ưu điểm: Là một công cụ hỗ trợ nhiều tính năng như scan subdirectory , spider web , proxy…

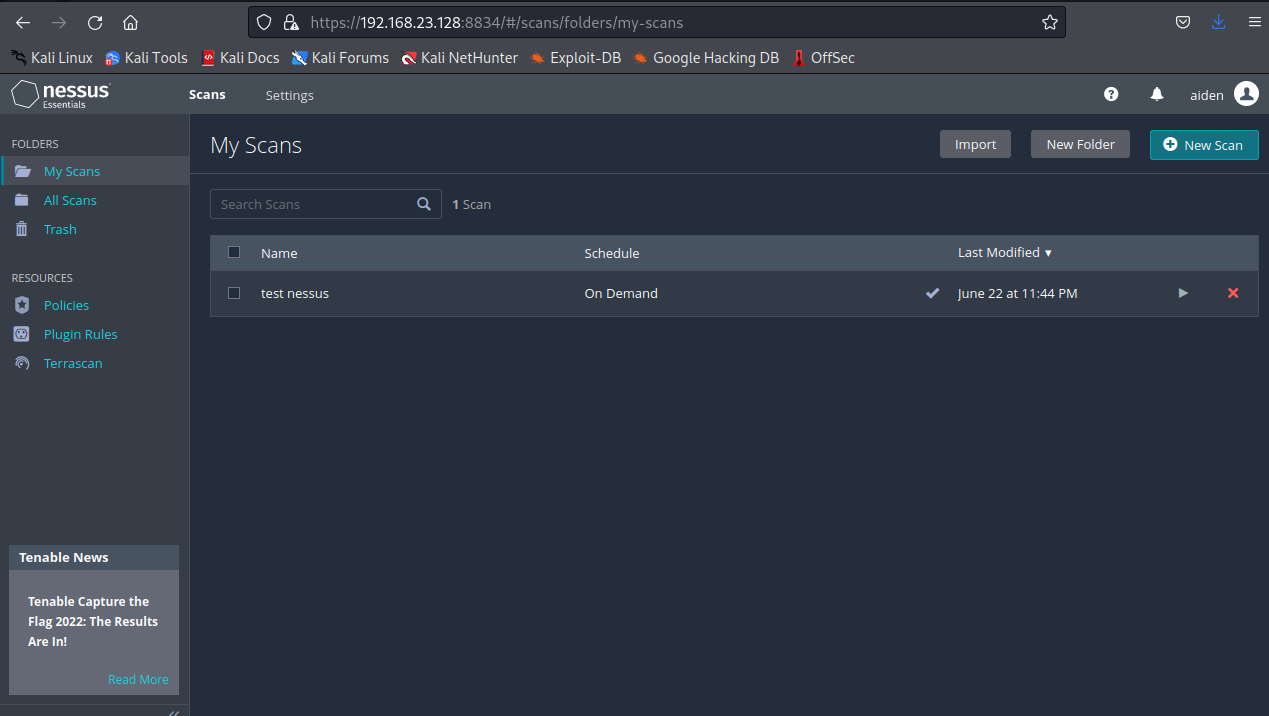
Nhược điểm: Vì là một tool nhiều tính năng nên thường các tính năng đó sẽ không mạnh bằng một số tool chuyên dụng với tính năng tương tự.

Nessus:

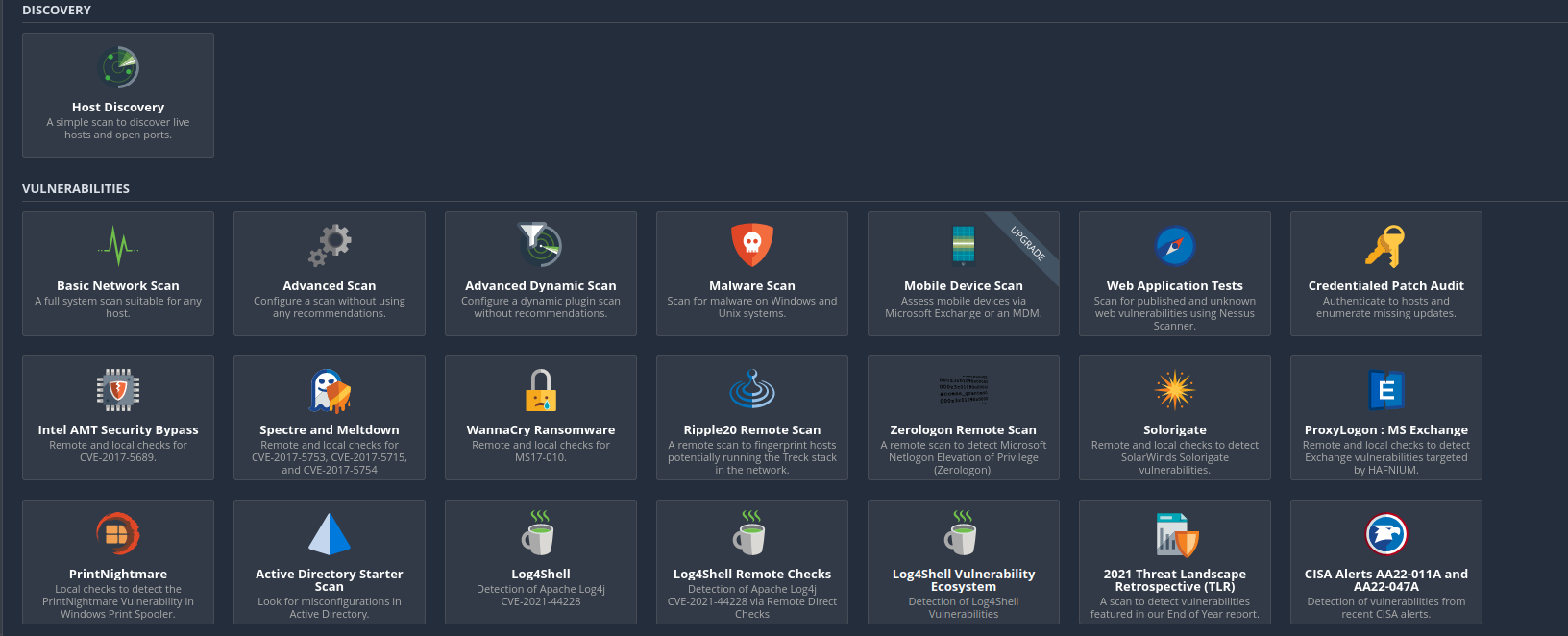
Là một công cụ được sử dụng để quét hệ thống, ứng dụng và các thiết bị mạng. Với hệ thống các plug-ins và các cơ sở dữ liệu luôn được update mới đã giúp Nessus trở thành các công cụ hang đầu.

Để sử dụng công cụ ta cần cài đặt vì nó không phải là công cụ có sẵn sau khi cài đặt ta sẽ start dịch vụ nessus bằng câu lệnh systemctl enable nessus và systemctl start nessus.

Sau đó ta truy cập vào trình duyệt với ip local của ta kèm theo số port 8834 là port mà nessus đang sử dụng để chạy.

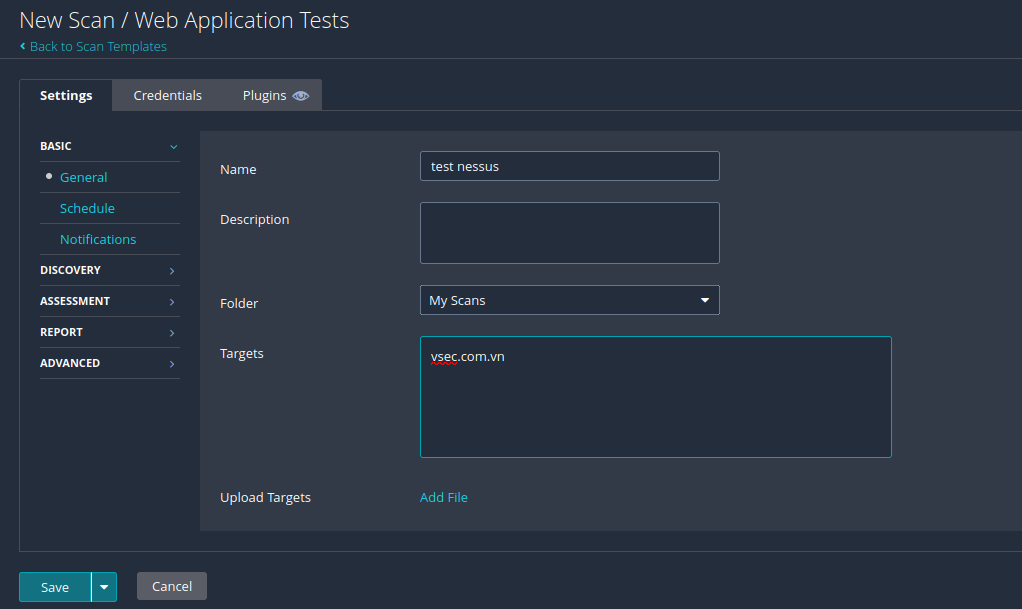


Để scan một mục tiêu ta click vào New scan nó sẽ cho ta một giao diện với các options khác nhau

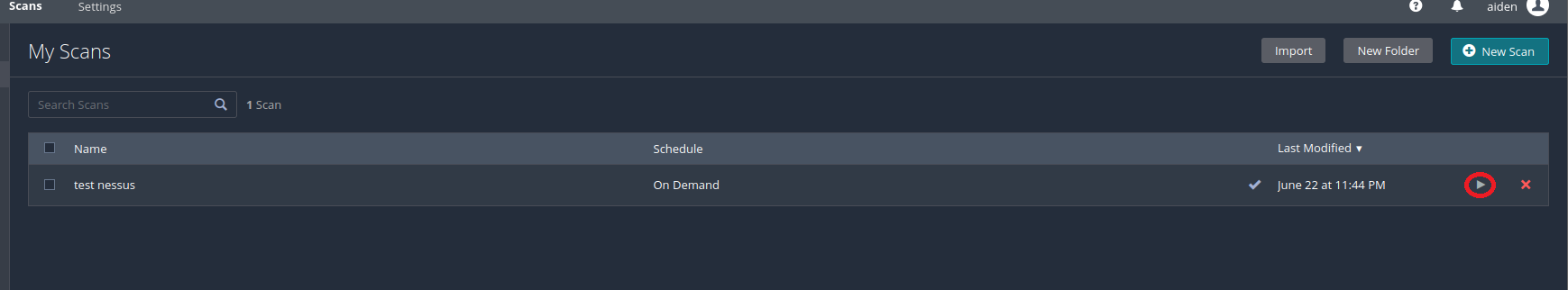


Lúc này ta sẽ chọn options mà mình muốn và click vào nó( ở đây ta sẽ dùng Web application Tests để kiểm tra và quét lỗi trang web.

Sau khi xong ta tiến hành nhập vào tên cho cái phần scan của mình và điền mục tiêu muốn scan vào và click save

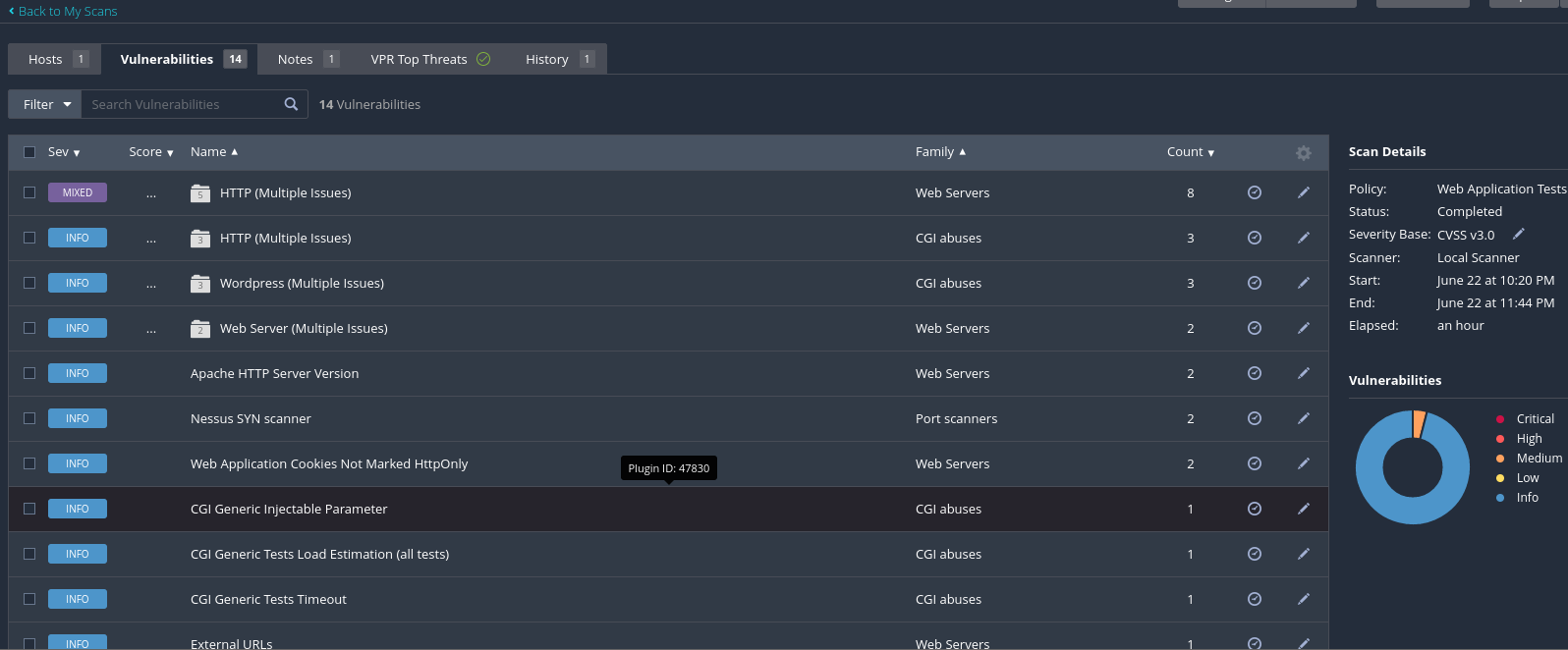


Sau khi save nó sẽ đưa ta lại giao diện đầu và sẽ tạo cho ta một nơi chưa các thông tin về mục tiêu mà ta vừa tạo.



Để scan ta chỉ cần click vào dấu được khoanh tròn đỏ là sẽ tự động scan

Sau đó nó scan và khi scan xong ta sẽ click vào để xem kết quả nó sẽ phân loại ra từng mục cho ta dễ nhìn. Muốn xem các lỗi mà nó đã scan được ta click vào phần vulnerabilities nó sẽ xuất hiện các lỗi đã phát hiện và tự phân loại theo màu sắc cho ta.



Acunetix:

là một công cụ kiểm tra bảo mật ứng dụng web tự động kiểm tra các ứng dụng web để tìm kiếm lỗ hổng bảo mật

Acunetix hoạt động như thế nào?

1. Acunetix DeepScan phân tích toàn bộ trang web bằng cách truy vết tất cả các liên kết trên trang web, bao gồm các liên kết được xây dựng động bằng JavaScript và các liên kết được tìm thấy trong tệp robots.txt và sitemap.xml (nếu có). Kết quả là một bản đồ của trang web, mà Acunetix sẽ sử dụng để khởi chạy các kiểm tra được nhắm mục tiêu đối với từng phần của trang web.
2. Nếu Acunetix AcuSensor Technology (kỹ thuật hỗ trợ dò quét mã nguồn của Acunetix) được cài đặt, bộ thu thập (sensor) sẽ lấy danh sách tất cả các tệp có trong thư mục ứng dụng web và thêm các tệp mà trình thu thập thông tin không tìm thấy vào đầu ra của trình thu thập thông tin. Các tệp như vậy thường không được trình thu thập thông tin phát hiện vì chúng không thể truy cập được từ máy chủ web hoặc không được liên kết thông qua trang web chẳng hạn như web.config.
3. Sau quá trình thu thập dữ liệu, máy quét sẽ giả lập như một hacker, tự động khởi chạy một loạt các kiểm tra lỗ hổng trên mỗi trang được tìm thấy. Acunetix cũng phân tích từng trang cho những nơi có thể nhập dữ liệu và sau đó thử tất cả khả năng đầu vào độc hại. Đây là Giai đoạn quét tự động. Nếu AcuSensor Technology được bật, các mẫu kiểm tra lỗ hổng bổ sung sẽ được đưa ra đối với trang web.
4. Các lỗ hổng được xác định được hiển thị trong Scan Result. Các thông tin về lỗ hổng như data trong một request POST được sử dụng, mục bị ảnh hưởng, phản hồi HTTP của máy chủ và các thông tin khác được cung cấp chi tiết trong mỗi cảnh báo lỗ hổng. Các thông tin này trong hầu hết trường hợp có thể giúp cho người quản trị có thể dựng lại kịch bản tấn công và dễ dàng vá lỗi hơn, ví dụ như trong lỗ hổng sau của một website.’
5. Nếu AcuSensor Technology được sử dụng, các chi tiết như số dòng mã nguồn dẫn đến lỗ hổng được liệt kê. Các khuyến nghị về cách khắc phục lỗ hổng cũng được hiển thị
6. Sau khi việc dò quét hoàn tất, Acunetix có thể tạo ra các báo cáo như Executive Summary, Developer report hay các báo cáo tuân theo các tiêu chuẩn PCI DSS hoặc ISO 270001

Ưu điểm :

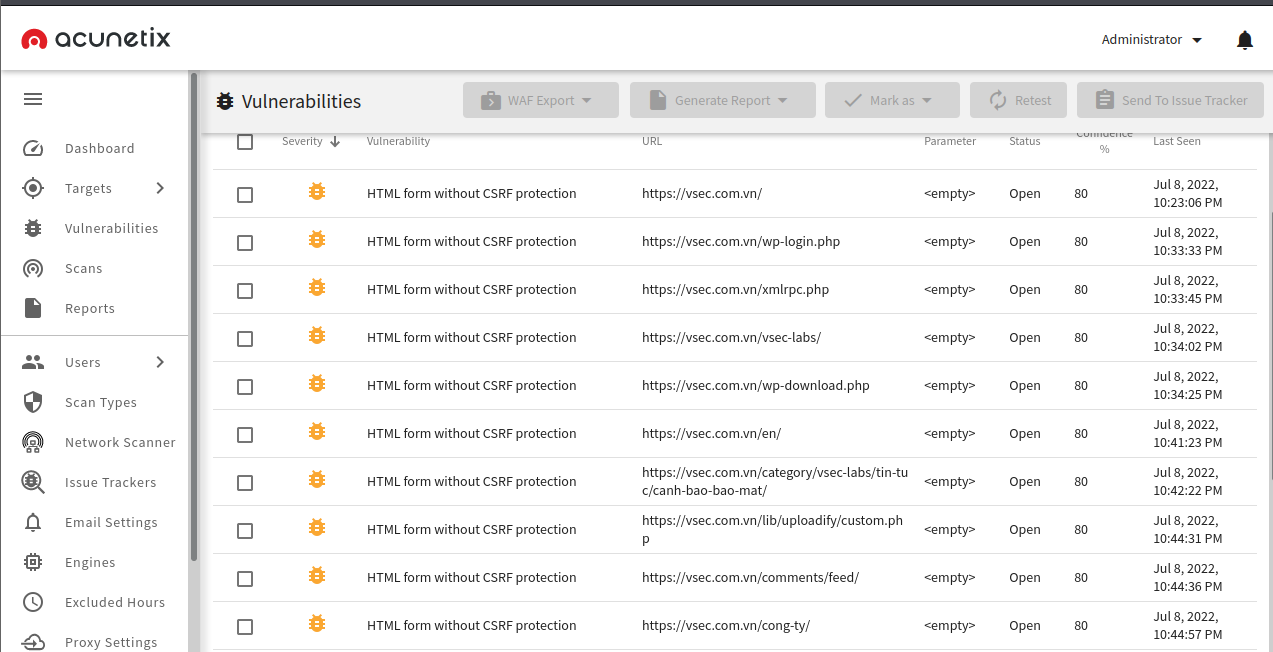
* Giao diện website trực quan, dễ sử dụng.
* Có lượng mẫu thử khổng lồ.
* Có kịch bản khai thác tốt, hỗ trợ phát hiện được hầu hết các lỗ hổng web phổ biến.
* Báo cáo cho các lỗ hổng rất chi tiết, cụ thể.
* Giữ lại lịch sử, kết quả rò quét.

Nhược điểm:

* Trong quá trình quét rất tốn RAM và bộ nhớ.
* Khi quét trang web lớn tốn nhiều thời gian, chưa hỗ trợ chức năng tạm dừng, phải chờ đến khi quét xong.
* Là công cụ có phí, không công bố mã nguồn.
* Khó để có thể nghiên cứu sâu, tận dụng nhưng module có sẵn của nó để hỗ trợ cho việc xây dựng một công cụ của bản thân.

Sử dụng Truy cập qua url <https://hostname:3443>

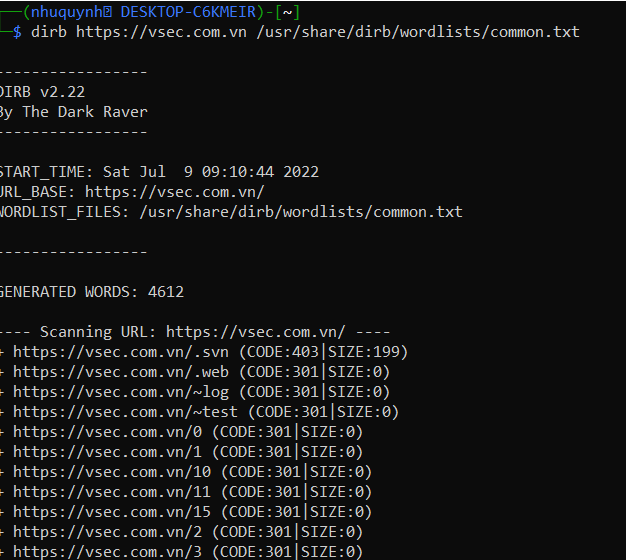
Click New target-> Add a new Target-> nhập host -> scan



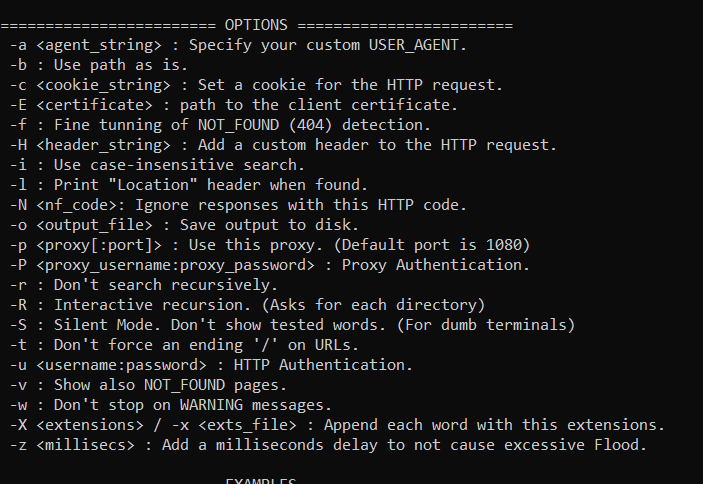
Dirb:

Là công cụ sử dụng để tìm các folder ẩn trong một trang web. Nó sẽ thực hiện liệt kê các folder đó và thông báo kết quả cho người dùng. Sử dụng kết hợp với wordlist.

Sử dụng : dirb url wordlist



Ngoài ra ta có thể kết hợp với một số options



Ưu điểm: là công cụ mạnh mẽ dò tìm các dictionary ẩn của một trang web. Hỗ trợ một số chức năng giúp người dùng dễ sử dụng và xem kết quả.

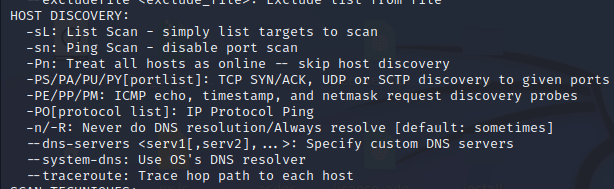
Nhược điểm: Không có cơ chế bypass khi quét quá nhanh sẽ dễ bị block.X`

Nmap

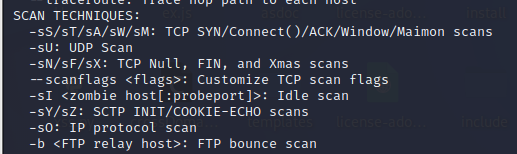
Là công cụ scanning phát hiện network – scan lỗi… Nó được sử dụng phổ biến kết hợp với nhiều kiểu scanning khác nhau.

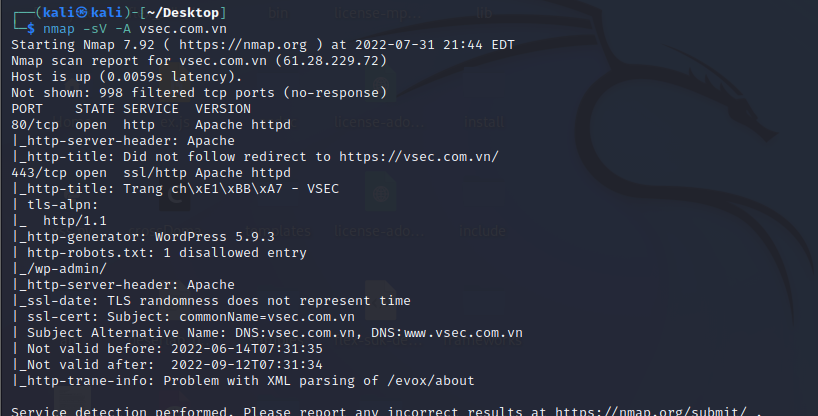
Cú pháp để scan nmap -sV -A <IP>

Câu lệnh trên dùng để scan host và hiển thị thông tin OS qua options -A và detect version qua options -sV trên 1000 port. Nếu ta muốn scan hết port có thể dùng options -p- và hoặc chỉ scan 1 số port nhất hịnh ta có thể dùng options -p và chỉ ra số port đó ví dụ: –p 80. Ngoài ra ta có thể dùng options -T(1-5) trong trường hợp để tang thời gian scan để tránh bị block vì scan quá nhiều. Ngoài ra ta có một số kiểu scan để phát hiện network như:



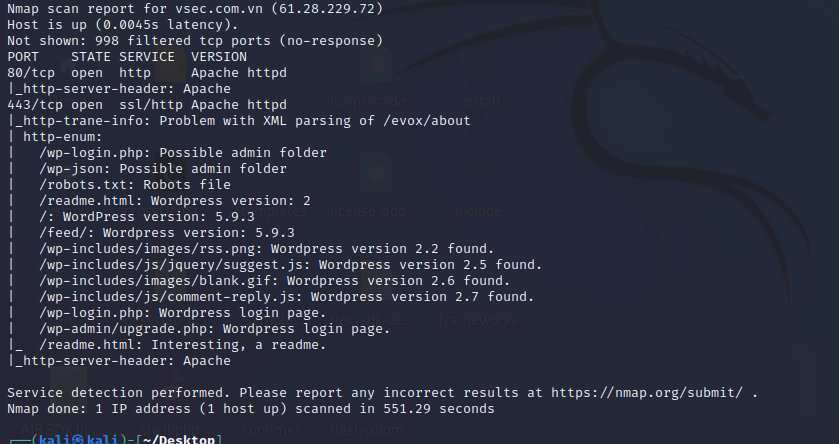
Và một số kiểu scan khác để tránh bị block khi scan kiểu thông thường.



Vd: 

NSE-script: Ngoài ra Nmap còn tích hợp các script để thực hiện từng hành động scan khác nhau

Vd:nmap -sV --script=http-enum vsec.com.vn



Ưu điểm: nhiều tính năng dể sử dụng.

Nhược điểm: Vì quá nhiều tính năng nên có một số tính năng không thực sự hữu dụng bằng các tool khác.