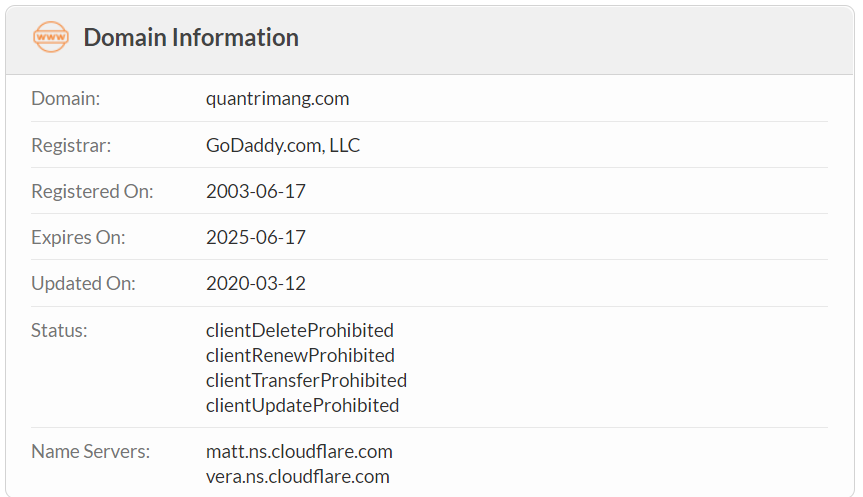
Reconnaissance

* 1. Passive

-Whois Lookup: Whois 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 whois bạn vào đường link sau: <https://www.whois.com/whois/> sau đó bạn sẽ điền website mà bạn muốn thử nó sẽ xuất ra các thông tin.

Vd: 

Registrar: Nơi cung cấp tên miền, tổ chức phân phối tên miền mà bạn đang sử dụng.

Registered On: Ngày đăng ký

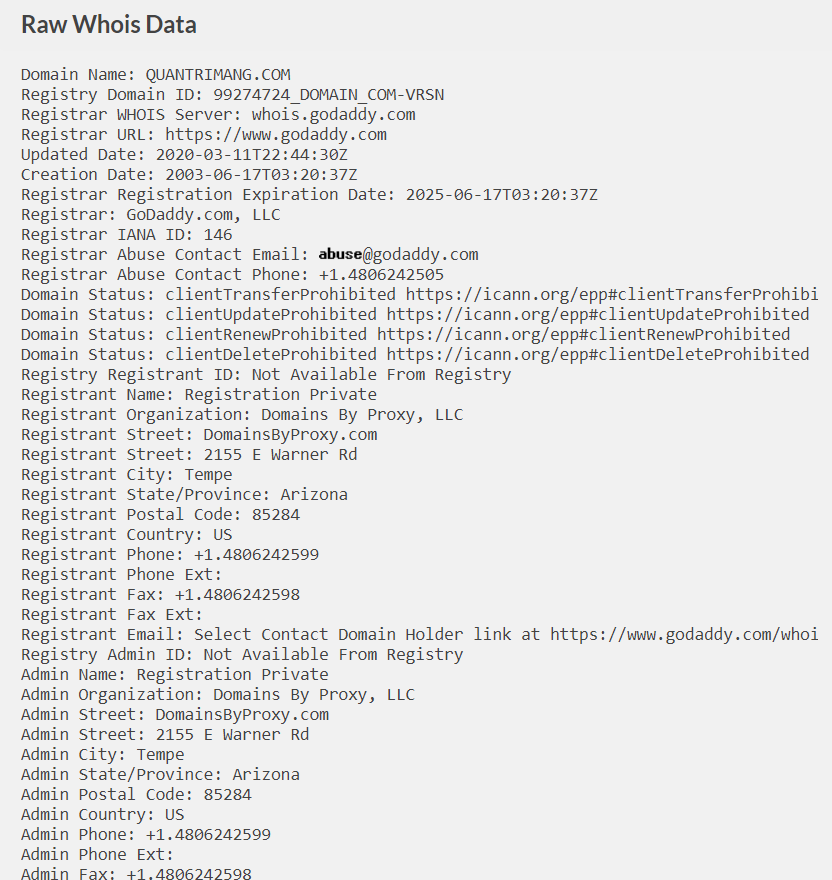
Expires On: Ngày hết hạn

Updated On: thời gian update mới nhất

Status: Tình trạng của tên miền.

Name Servers: là hệ thống điều phồi quá trình hoạt động của tên miền website , chuyển đổi tên miền sang địa chỉ ip. Như ở trên quantrimang.com sử dụng 2 Name servers là matt.ns.cldflare.com và vera.ns.cloudflare.com

Sau đây là một số thông tin tat thu thập được từ trang whois:

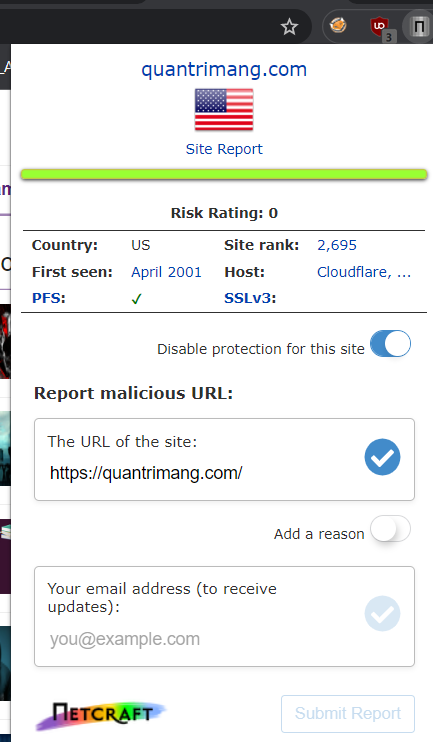


-Netcraft : Là một công củ sử dụng để kiểm tra thông tin IP hoặc một domain nào đó. Để sử dụng công ta có 2 cách một là truy cập thẳng vào trang web và cách thứ hai là sử dụng extension trên chrome.

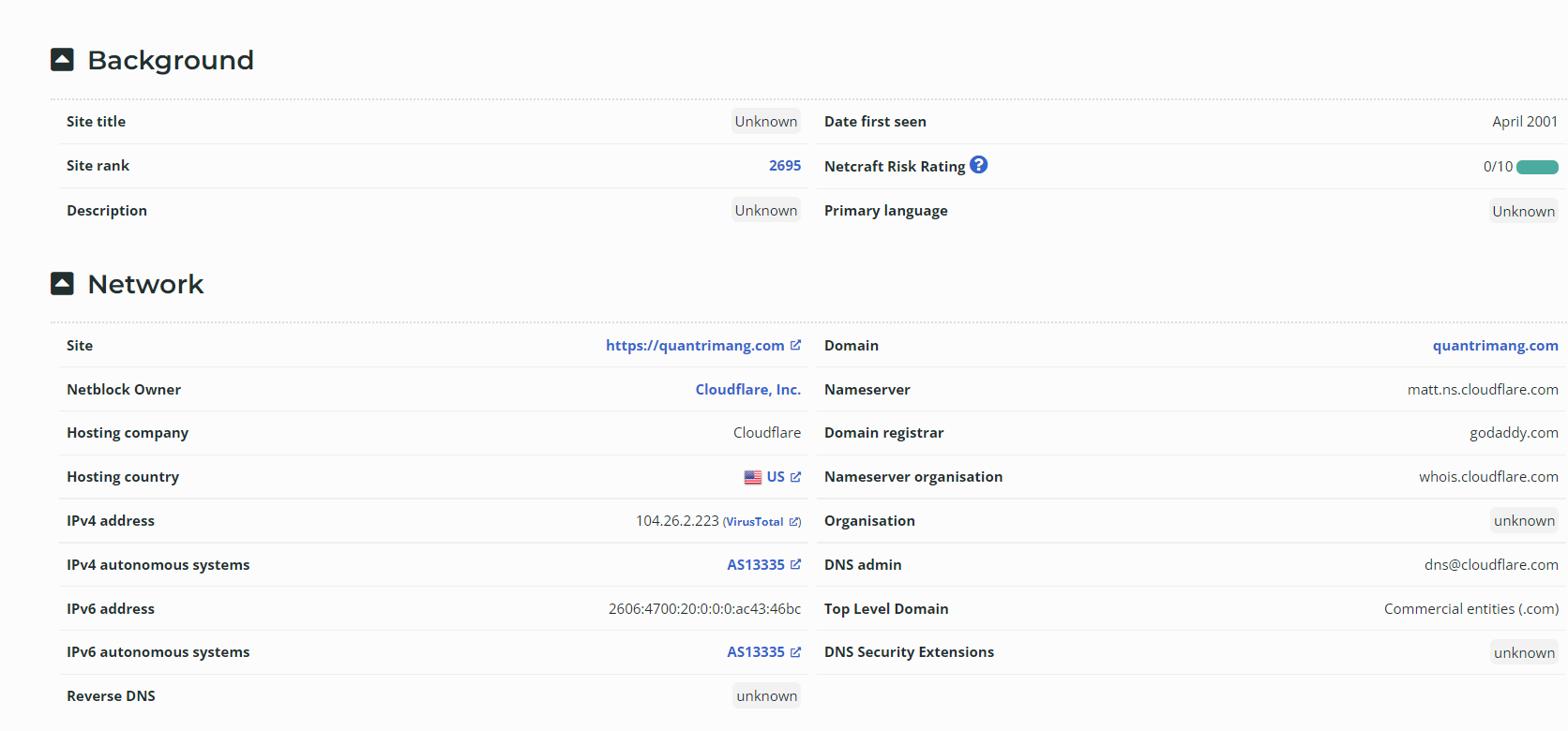
B1: Để sử dụng extension chrome đầu tiên ta sẽ truy cập vào link : <https://chrome.google.com/webstore/detail/netcraft-extension/bmejphbfclcpmpohkggcjeibfilpamia>

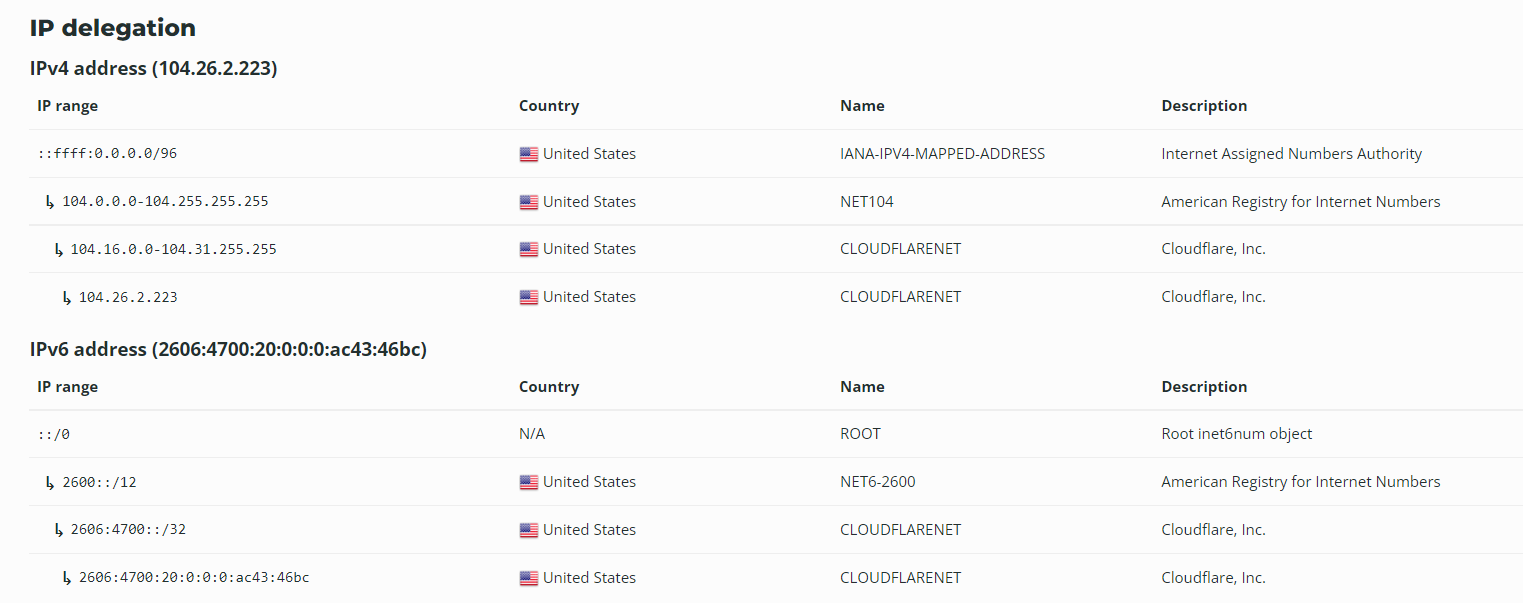
sau đó ấn nút thêm vào chrome và sẽ tự động thêm vào trình duyệt của ta.

B2: Sau đó ta truy cập vào một website nào đó ở đây ta sẽ truy cập vào trang quantrimang.com làm ví dụ và ở phía trên bên phải sẽ có icon của công cụ khi click vào đó nó sẽ show ra một số thông tin về trang web.



Hoặc ta có thể ấn Site report nó sẽ redirect ta sang trang chủ và show cho chúng ta nhiều thông tin hơn về domain.





-Google hacking(dork):

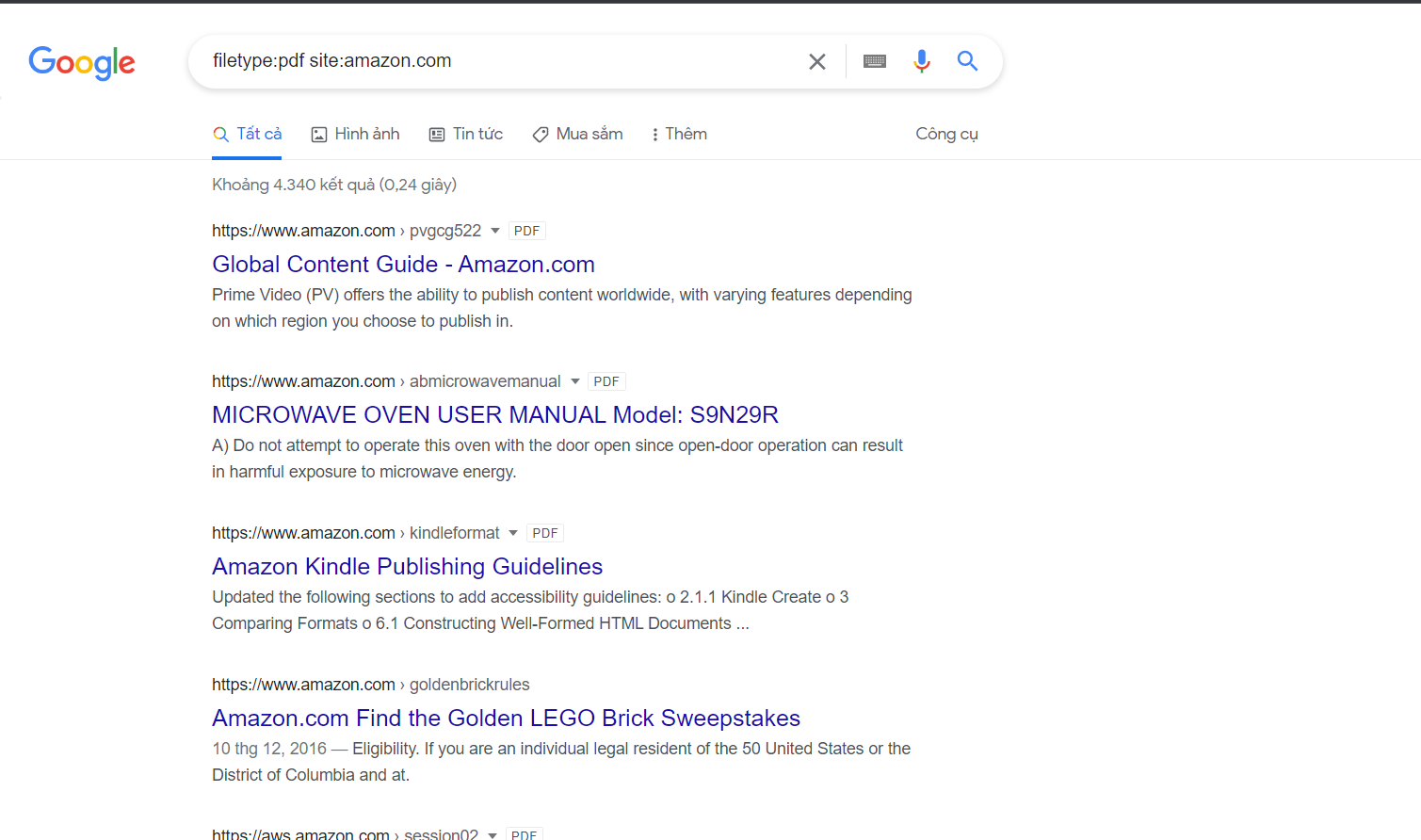
Là một kỹ thuật cho phép truy vấn trên công cụ tìm kiếm Google.com , đôi khi được dùng để xác định các lổ hổng trong các ứng dụng web cụ thể. Bên cạnh việc truy vấn từ google có thể tiết lộ các lỗ hổng trong các ứng dụng web, Google Hacking cho phép bạn tìm các dữ liệu nhạy cảm. Việc truy vấn được thực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

Các toán tử thường 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:

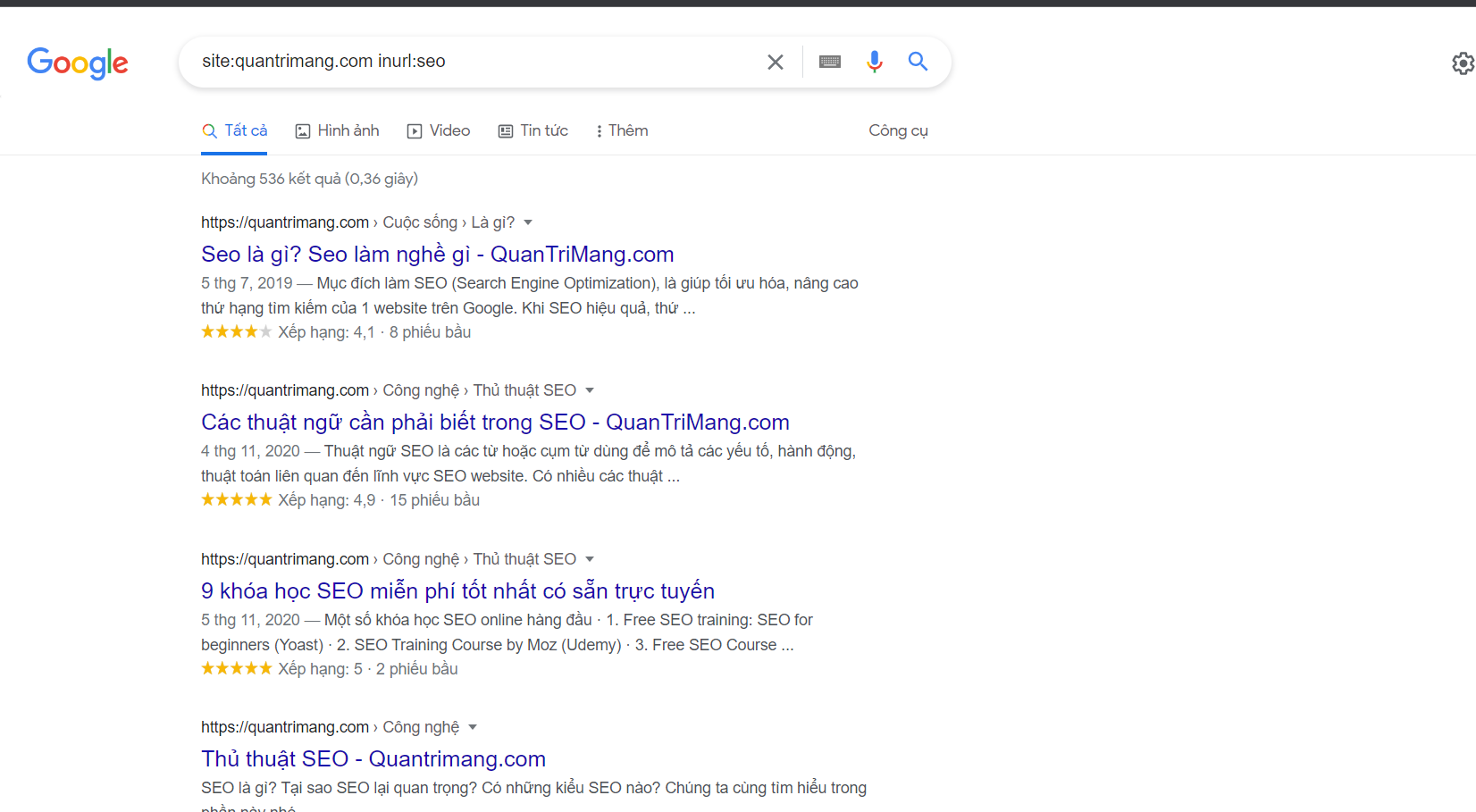
vd: Ta sẽ tìm kiếm các file pdf trên trang amazon.com

filetype:pdf site:amazon.com



vd2: Ta sẽ tìm trên site quản trị mạng với url có chừa từ khóa seo

site:quantrimang.com inurl:seo



Bằng cách sử dụng các toán tử đó ta có thể thu thập được rất nhiều thông tin về một hay nhiều website mà ta muốn , thậm chí ta có thể tìm được các file quan trọng mà người dùng không nên có quyền truy cập vào chỉ với kỹ thuật google hacking.

-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 của shodan:

Cách thức sử dụng shodan

-DNS lookup:

-TheHarvester:

Là một công cụ thu thập thông tin. Mục đích của công cụ này là thu thập email , sub-domain , port …

Cách cài đặt trên linux:

Chạy câu lệnh sau: sudo apt install theharvester -y

Các options của Harvester:

-d : Nhập vào tên domain muốn thu thập.

-b: Chọn các công cụ tìm kiếm.

-s: Dùng shodan để truy querry và phát hiện các hosts.

-l: giới hạn số lượng kết quả.

-p: Sử dụng proxy.

-S: bắt đầu bằng result thứ mấy.

-v: tìm các thông tin Virtual host của domain này.

-f: lấy output xuất ra file ở đây hỗ trợ 2 định dạng là xml và json.

-n : Truy vấn đảo ngược DNS, giống NSLOOKUP DNS tra cứu tên miền liên kết đến IP cần query

-c: Gởi lượng lớn thông tin DNS tới domain tạo sự truy vấn liên tục, để thực hiện điều này cần có 1 file dns.txt mẫu để dựa và lượng data này để truy vấn

-t: TLD(Top-level domain) có nghĩa là khi truy vấn thông tin một domain ví dụ quantrimang.vn không những truy vấn một tên miền .vn mà truy vấn các tên miên liên quan như quantrimang.com, .net .org ...

-e: Dùng DSN Server để truy vấn, trong quá trình truy vấn theHarvester sẽ dựa vào thông tin của DNS Server để thực hiện quá trình truy vấn

Demo:

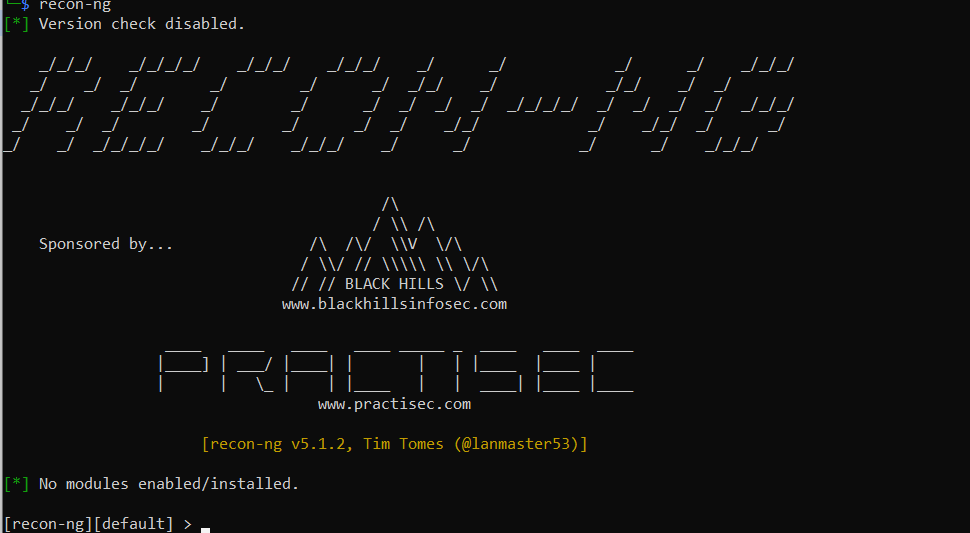
-Recon-ng:

Là framework dùng để thu thập thông tin từ các web application , hỗ trợ các tác vụ sau:

* Tìm IP của mục tiêu.
* Dò lỗi sql injection
* Tìm các file nhạy cảm như robots.txt
* Tìm các thông tin liên quan như Geo-IP lookup , Banner grabbing , DNS lookup , port scanning , sub-domain information , reverse IP với WHOIS lookup.
* Dò thông tin về CMS của web.
* Scan IOT device với Shodan search engine.

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.



3.2 Active

-DNS enumeration (note: <https://medium.com/@klockw3rk/back-to-basics-dns-enumeration-446017957aa3>)

Là quá trình định vị tất cả các máy chủ DNS và các bản ghi tương ứng của chúng cho một tổ chức. Việc liệt kê DNS sẽ mang lại tên người dùng, tên máy tính và địa chỉ IP của các hệ thống mục tiêu tiềm năng.