Chúng ta sẽ tập trung vào những công cụ quan trọng để thu thập thông tin bị động

* whois truy vấn đến máy chủ WHOIS
* nslookup truy vấn đến máy chủ DNS
* dig truy vấn đến máy chủ DNS

Vì đây là những thông tin công cộng nên không cảnh báo cho đối tượng

Chúng ta cũng sẽ học về hai dịch vụ trực tuyến:

* DNSDumpster
* Shodan.io

Hai công cụ cho phép chúng ta thu thập thông tin về đối tượng mà không cần kết nối trực tiếp với chúng.

Reconnaissance (recon) có thể hiểu là cuộc khảo sát sơ bộ để thu thập thông tin về đối tượng.

Passive recon là bạn thu thập thông tin về đối tượng công khai. Hãy tưởng tượng nó giống như bạn đang quan sát đối tượng từ xa mà không xâm nhập vào lãnh thổ của chúng.

Passive recon bao gồm những hoạt động sau:

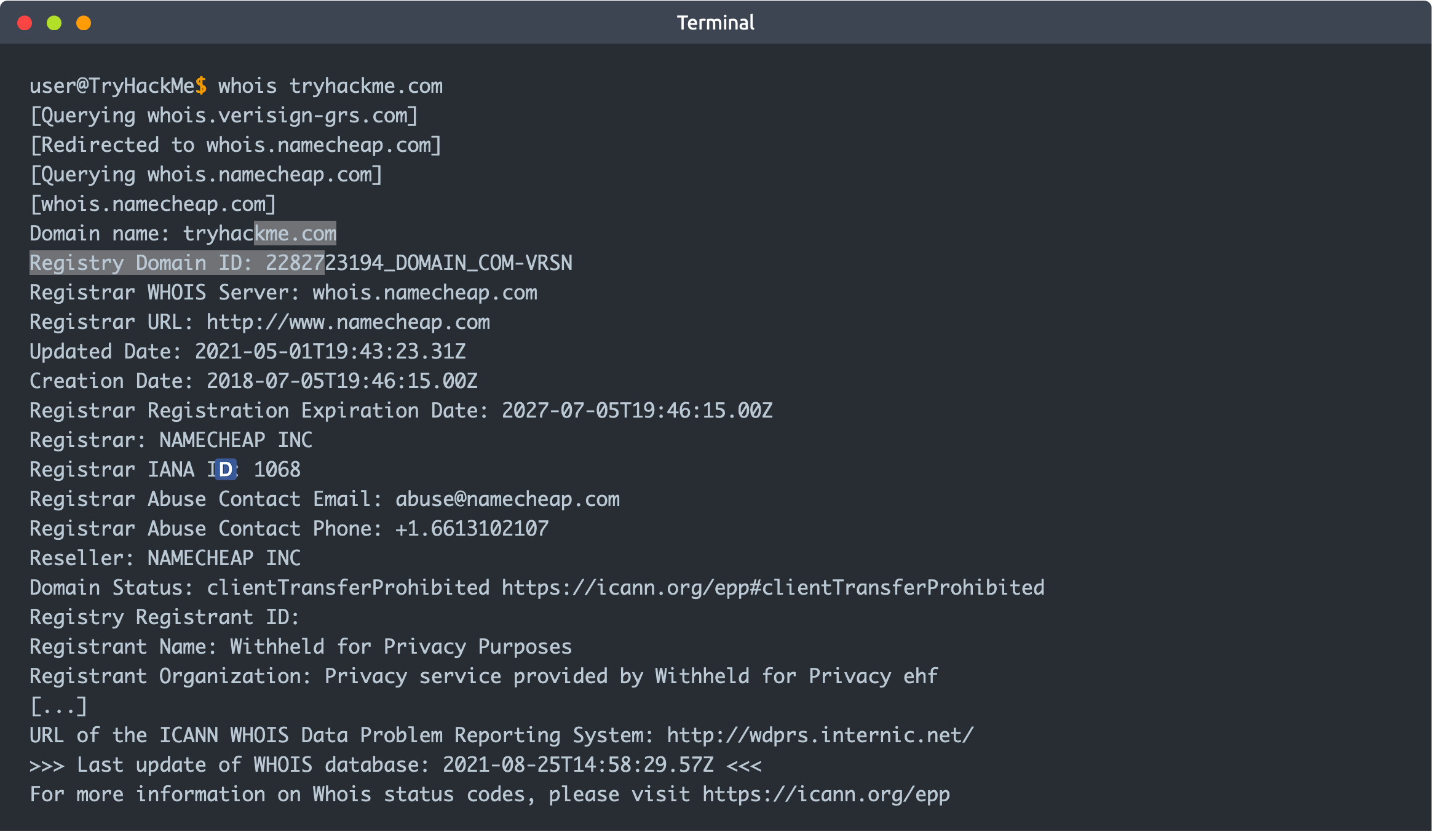
* Tra cứu tên miền từ máy chủ DNS
* Kiểm tra những quảng cáo liên quan đến mục tiêu
* Đọc những bài báo mới về đối tượng

**Whois**

WHOIS là 1 giao thức yêu cầu và phản hồi theo chỉ thị của RFC 3912. Máy chủ WHOIS lắng nghe trên cổng TCP 43. Trang bán tên miền chịu trách nhiệm duy trì những bản ghi WHOIS cho các tên miền nó đang được thuê. Máy chủ WHOIS phản hồi rất nhiều thông tin liên quan đến tên miền được yêu cầu như:

* Nhà đăng kí tên miền
* Thông tin liên lạc
* Tạo mới, chỉnh sửa và ngày hết hạn
* Tên máy chủ

Cú pháp: **whois DOMAIN\_NAME**



Đầu tiên chúng ta được chuyển hướng đến whois.namecheap.com để lấy thông tin cho chúng ta.

namecheap.com đang duy trì những bản ghi DNS cho tên miền đó. Hơn nữa, chúng ta có thể thấy ngày tạo mới, chỉnh sửa lần cuối và ngày hết hạn.

Tiếp theo chúng ta thu thập thông tin về trang bán tên miền và người đăng kí. Chúng ta có thể thấy tên và thông tin của người đăng kí nếu họ không dùng những dịch vụ riêng tư. Mặc dù không hiển thị ở trên, chúng ta vẫn có thông tin liên lạc của admin và tech.

Cuối cùng, chúng ta thấy những máy chủ tên miền để chúng ta truy vấn nếu có bản ghi DNS

Thông tin thu thập được có thể được điều tra để tìm thêm phạm vi tấn công mới. Ví dụ bạn có thể xem xét 1 cuộc tấn công chống lại máy chủ email của quản trị viên hoặc những máy chủ DNS.

Điều đáng lưu ý là những công cụ tự động lạm dụng những câu truy vấn WHOIS để thu thập địa chỉ email, rất nhiều dịch vụ WHOIS đã thực hiện các biện pháp chống lại điều này. Họ có thể xác định lại địa chỉ email. Hơn thế nữa, rất nhiều người đăng kí dùng những dịch vụ riêng tư để tránh email của mình bị tiết lộ.

**nslookup và dig**

Ở ví dụ trước, chúng ta dùng công cụ whois để có được rất nhiều thông tin và tên miền chúng ta đang tìm kiếm. Đặc biệt, chúng ta có thể lấy các máy chủ DNS từ công ty bán tên miền.

Tìm kiếm địa chỉ IP của tên miền bằng cách sử dụng nslookup.

Cú pháp : **nslookup OPTIONS DOMAIN\_NAME SERVER**

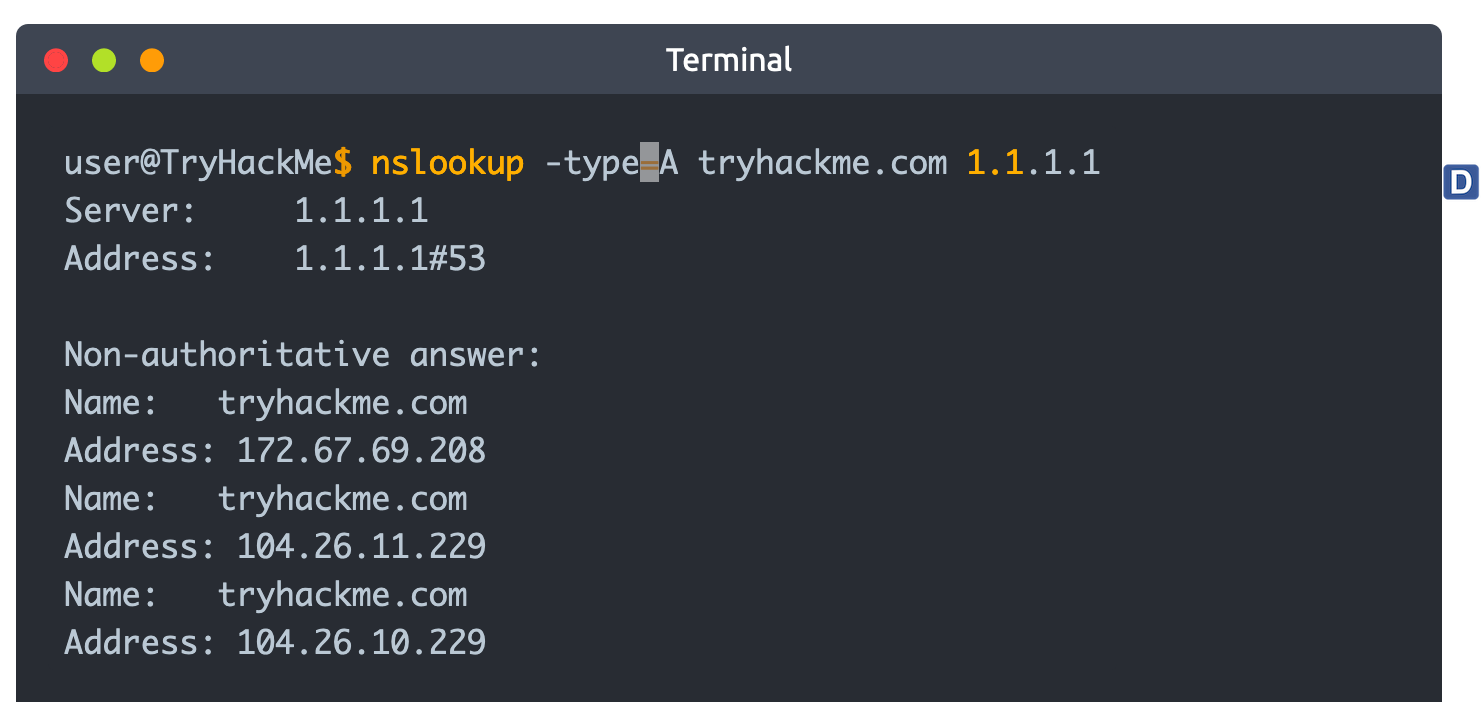
options chứa loại truy vấn. Ví dụ, bạn có thể sử dụng A để lấy địa chỉ Ipv4 và AAAA cho địa chỉ Ipv6

domain\_name là tên miền bạn đang tìm kiếm

server là máy chủ DNS bạn muốn truy vấn. Bạn có thể chọn máy chủ DNS cục bộ hay công cộng để truy vấn. Cloudflare cung cấp 1.1.1.1 và 1.0.0.1, Google cung cấp 8.8.8.8 và 8.8.4.4 và Quad9 cung cấp 9.9.9.9 và 149.112.112.112. Có rất nhiều máy chủ DNS công cộng bạn có thể chọn nếu bạn muốn thay thế những máy chủ DNS của ISP.

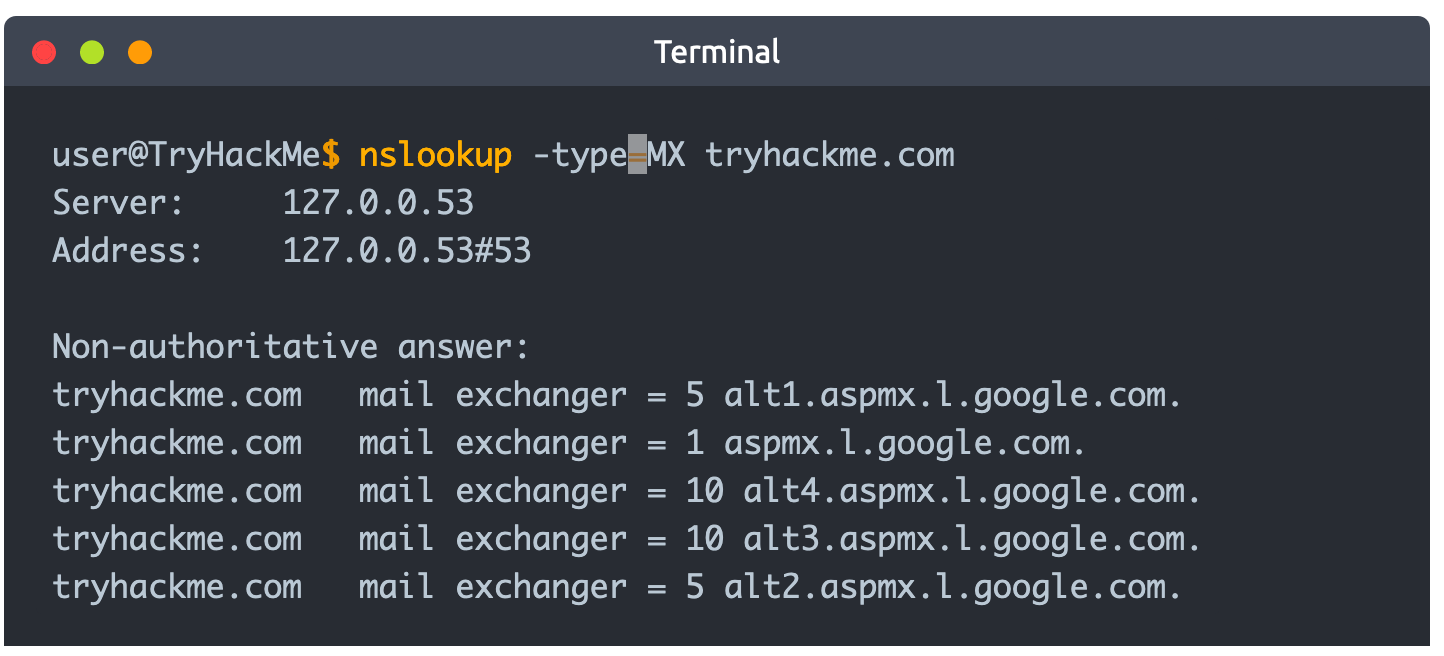
| **Query type** | **Result** |
| --- | --- |
| A | IPv4 Addresses |
| AAAA | IPv6 Addresses |
| CNAME | Canonical Name |
| MX | Mail Servers |
| SOA | Start of Authority |
| TXT | TXT Records |

Ví dụ, nslookup -type=A tryhackme.com 1.1.1.1



Việc tra cứu này rất có ích với quá trình kiểm thử. Ở ví dụ trên, chúng ta bắt đầu với 1 tên miền và nhận được 3 địa chỉ Ipv4. Mỗi địa chỉ IP có thể được kiểm tra thêm về tính bảo mật, giả sử chúng nằm trong phạm vi kiểm thử.

Nếu bạn muốn biết về những máy chủ email và cấu hình cho 1 tên miền cụ thể. Bạn có thể thực hiện lệnh sau:

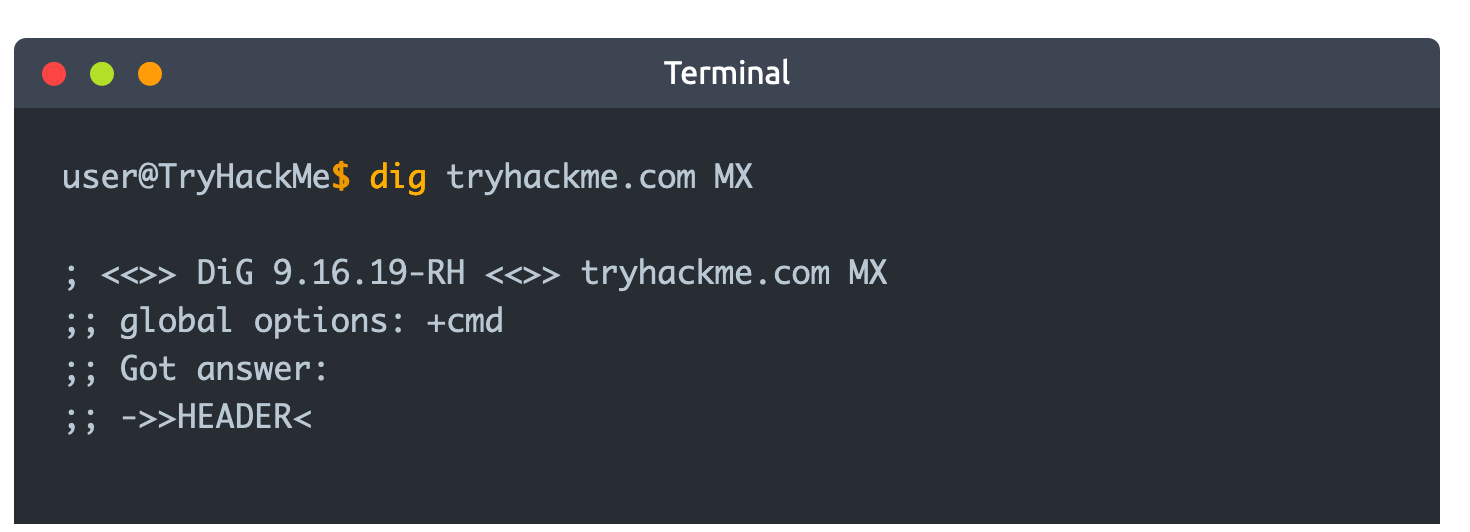


Chúng ta có thể thấy cấu hình email hiện tại của tryhackme là Google. Vì MX tra cứu những máy chủ Mail Exchange, chúng ta để ý thấy khi 1 máy chủ mail cố gắng vận chuyển thư @tryhackme.com, nó sẽ kết nối đến aspmx.l.google.com, cái có thứ tự 1. Nếu nó bận, máy chủ mail sẽ thử kết nối đến máy chủ mail thứ 2 là alt1.aspmx.l.google.com hoặc alt2.aspmx.l.google.com

Google cung cấp danh sách những máy chủ mail. Do đó, chúng ta không nên mong chờ những máy chủ mail này đang chạy 1 phiên bản có lỗ hổng. Tuy vậy, trong rất nhiều trường hợp, chúng ta có thể thấy những máy chủ mail không hoàn toàn bảo mật hay được vá.

Để truy vấn DNS nâng cao hơn, bạn có thể sử dụng dig. Dig giúp tra cứu những bản ghi MX và so sánh chúng với nslookup

Cú pháp: **dig DOMAIN\_NAME TYPE**



1 bảng so sánh nhanh giữa đầu ra của nslookup và dig cho thấy dig trả về nhiều thông tin hơn như TTL. Nếu bạn muốn truy vấn máy chủ DNS 1.1.1.1, bạn có thể thực thi câu lệnh sau: dig @1.1.1.1 tryhackme.com MX

**DNSDumpster**

Những công cụ tra cứu DNS như nslookup và dig, không thể tìm miền con.

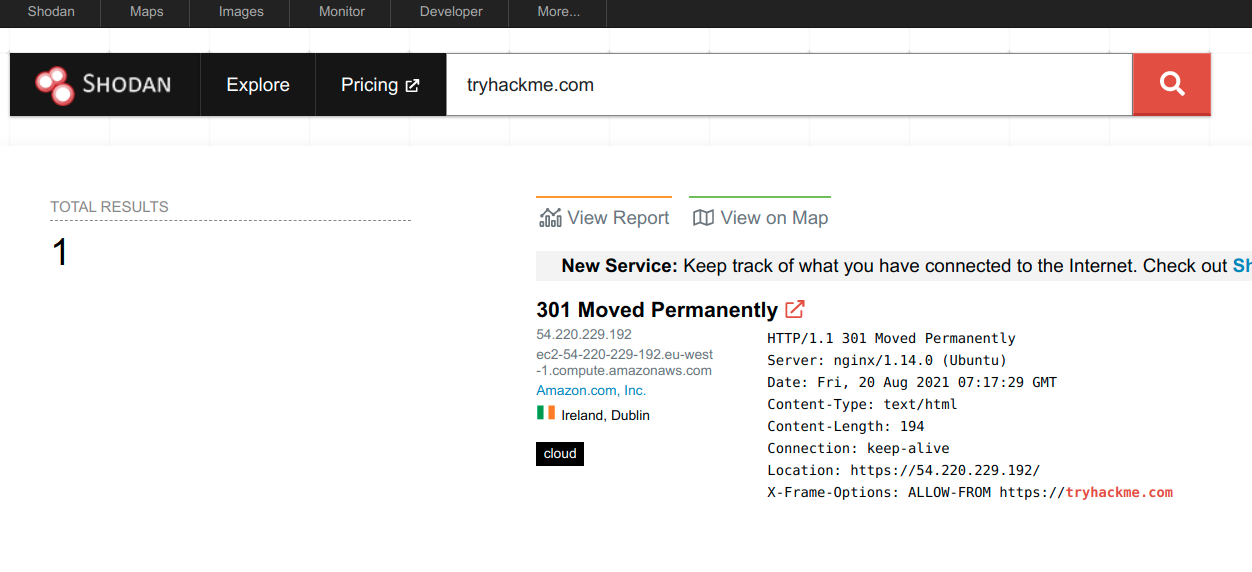
Nếu chúng ta tìm kiến tryhackme.com trên DNSDumpster, chúng ta sẽ khám phá được tên miền con như blog.tryhackme.com

**Shodan.io**

Shodan.io có thể giúp bạn biết thêm nhiều thông tin về mạng máy khách mà không cần kết nối trực tiếp với nó.

Hơn nữa, ở lĩnh vực phòng thủ, bạn có thể dùng nhiều dịch vụ khác nhau từ Shodan.io để tìm hiểu về những thiết bị được kết nối và tiếp xúc thuộc về tổ chức của bạn.

Shodan.io cố gắng kết nối mọi thiết bị trực tuyến để xây dựng 1 công cụ tìm kiếm những thứ kết nối thay vì những trang web như Google. Nó thu thập tất cả thông tin liên quan đến dịch vụ và lưu trữ nó trong cơ sở dữ liệu.



Xem xét 1 bản ghi của một trong số các máy chủ của try hack me

Bản ghi cho thấy máy chủ web; tuy nhiên, Shodan.io chỉ thu thập thông tin liên quan đến bất cứ thiết bị nào nó thấy đang kết nối trực tuyến. Qua kết quả tìm kiếm của Shodan.io, chúng ta có thể biết một vài thứ như:

* Địa chỉ IP
* Công ty lưu trữ
* Vị trí địa lý
* Loại và phiên bản máy chủ

**Summary:**

| **Purpose** | **Commandline Example** |
| --- | --- |
| Lookup WHOIS record | whois tryhackme.com |
| Lookup DNS A records | nslookup -type=A tryhackme.com |
| Lookup DNS MX records at DNS server | nslookup -type=MX tryhackme.com 1.1.1.1 |
| Lookup DNS TXT records | nslookup -type=TXT tryhackme.com |
| Lookup DNS A records | dig tryhackme.com A |
| Lookup DNS MX records at DNS server | dig @1.1.1.1 tryhackme.com MX |
| Lookup DNS TXT records | dig tryhackme.com TXT |