NETWORK SECURITY

Modules:

- Passive Reconnaissance
- Active Reconnaissance
- Nmap Live Host Discovery
- Nmap Basic Ports Scans
- Nmap Advanced Port Scans
- Protocol and Server
- Protocol and Server 2
- Network Security Challenge

1 . Passive Reconnaissance Introduction

- On here we focus on essential tools related to passive reconnaissance. We will learn three command-line tools:

- whois to query WHOIS server
- nslookup to quey DNS server
- dig to query DNS server

- Chúng tôi sử dụng **whois** để truy vấn các bản ghi WHOIS, trong khi chúng tôi sử dụng **nslookup** và **dig** để truy vấn các bản ghi cơ sở dữ liệu DNS. Đây là tất cả các bản ghi có sẵn công khai và do đó không cảnh báo cho mục tiêu.

- Chúng ta cũng sẽ học cách sử dụng hai dịch vụ trực tuyến:

1) **DNSDumpster**
2) **Shodan.io**

2. Passive Versus Active Recon

- Nếu bạn đóng vai kẻ tấn công, bạn cần thu thập thông tin về các hệ thống mục tiêu của mình. Nếu bạn đang đóng vai một người phòng thủ, bạn cần biết đối thủ của bạn sẽ phát hiện ra điều gì về hệ thống và mạng của bạn.

- Reconnaissance (recon) có thể được định nghĩa là một cuộc khảo sát sơ bộ để thu thập thông tin về một mục tiêu. Đây là bước đầu tiên trong **The Unified Kill Chain** để giành được chỗ đứng ban đầu trên một hệ thống. Chúng tôi chia recon thành:

1. **Passive Reconnaissance**
2. **Active Reconnaissance**

- Trong **passive reconnaissance** bạn dựa vào kiến thức có sẵn công khai. Đó là kiến thức mà bạn có thể truy cập từ các tài nguyên có sẵn công khai mà không cần tương tác trực tiếp với mục tiêu. Hãy nghĩ về nó giống như bạn đang nhìn vào lãnh thổ mục tiêu từ xa mà không đặt chân lên lãnh thổ đó.

- Hoạt động passive bao gồm nhiều hoạt động, ví dụ:

+Tra cứu bản ghi DNS của miền từ máy chủ DNS công cộng.

+Kiểm tra quảng cáo việc làm liên quan đến trang web mục tiêu.

+Đọc các bài báo về công ty mục tiêu.

- Mặt khác, **active reconnaissance** không thể đạt được một cách kín đáo như vậy. Nó đòi hỏi sự tham gia trực tiếp với mục tiêu. Hãy nghĩ về nó giống như bạn kiểm tra ổ khóa trên cửa ra vào và cửa sổ, trong số các điểm vào tiềm năng khác.

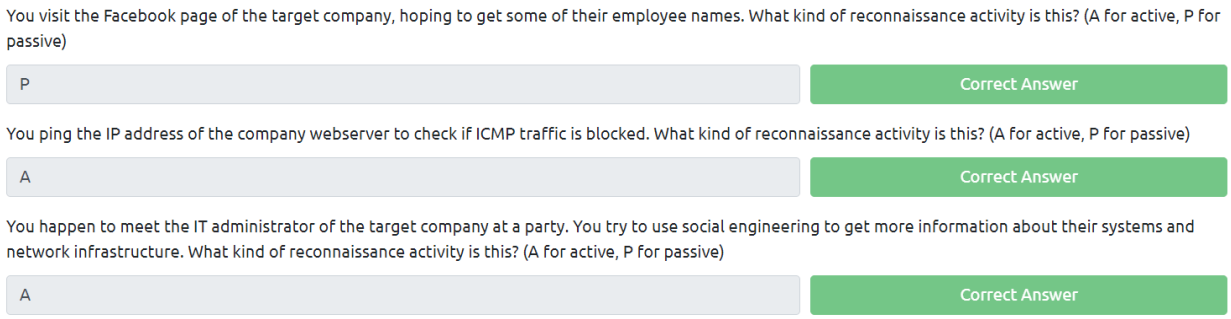
- Ví dụ về các hoạt động **passive reconnaissance** bao gồm:

+Kết nối với một trong các máy chủ của công ty như HTTP, FTP và SMTP.

+Gọi cho công ty để cố lấy thông tin (kỹ thuật xã hội).

+Vào khuôn viên công ty giả làm thợ sửa chữa.

- Xem xét bản chất xâm lấn của **passive reconnaissance**, người ta có thể nhanh chóng gặp rắc rối pháp lý trừ khi người đó có được sự cho phép hợp pháp thích hợp.



3. Whois

- **WHOIS** là một giao thức yêu cầu và phản hồi tuân theo thông số kỹ thuật RFC 3912. Máy chủ WHOIS lắng nghe trên cổng TCP 43 đối với các yêu cầu gửi đến. Công ty đăng ký tên miền chịu trách nhiệm duy trì hồ sơ WHOIS cho các tên miền mà họ đang cho thuê. Máy chủ WHOIS trả lời với nhiều thông tin khác nhau liên quan đến miền được yêu cầu. Quan tâm đặc biệt, chúng ta có thể tìm hiểu:

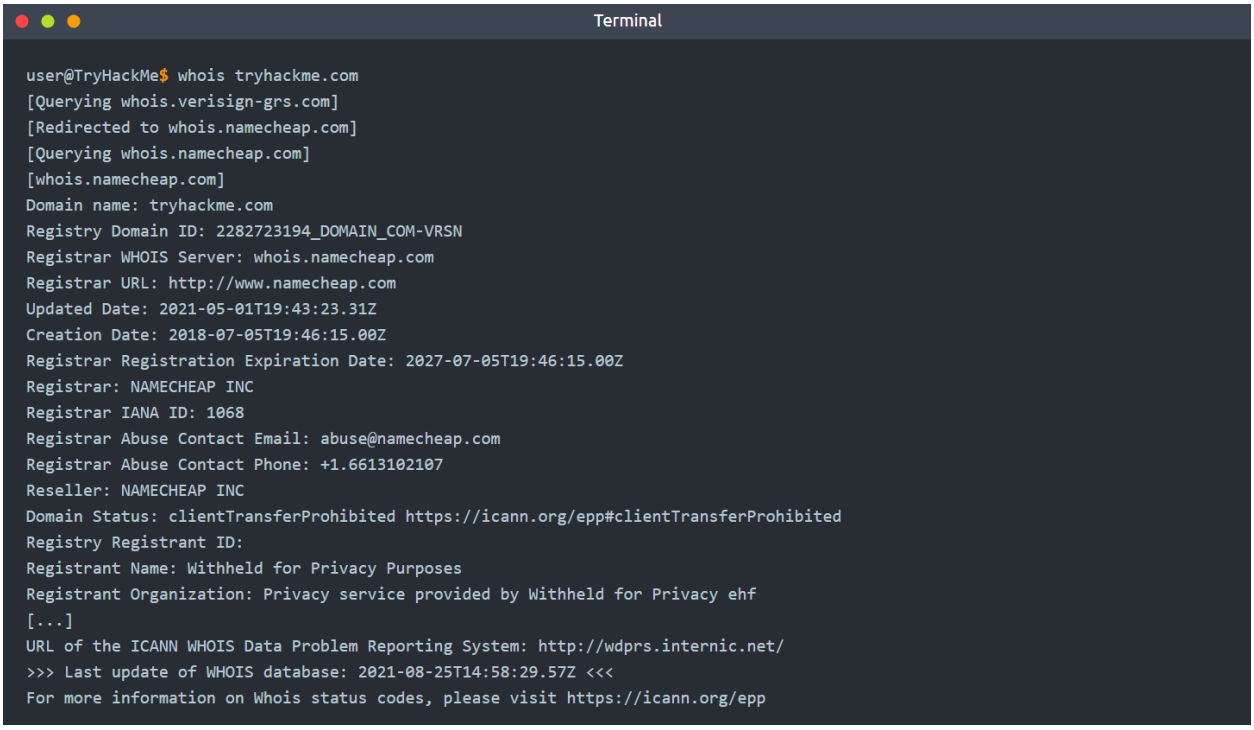
+ Công ty đăng ký: Tên miền được đăng ký qua công ty đăng ký nào?

Thông tin liên lạc của người đăng ký: Tên, tổ chức, địa chỉ, điện thoại, trong số những thứ khác. (trừ khi được ẩn thông qua dịch vụ bảo mật)

Ngày tạo, cập nhật và ngày hết hạn: Tên miền được đăng ký lần đầu khi nào? Nó được cập nhật lần cuối khi nào? Và khi nào thì cần đổi mới?

+ Name Server: Hỏi máy chủ nào để phân giải tên miền?

Để có được thông tin này, chúng tôi cần sử dụng ứng dụng khách whois hoặc dịch vụ trực tuyến. Nhiều dịch vụ trực tuyến cung cấp thông tin whois, tuy nhiên, nhìn chung sẽ nhanh hơn và thuận tiện hơn khi sử dụng ứng dụng **client whois** cục bộ của bạn. Sử dụng AttackBox (hoặc máy Linux cục bộ của bạn, chẳng hạn như Parrot hoặc Kali), bạn có thể dễ dàng truy cập ứng dụng khách whois của mình trên thiết bị đầu cuối. Cú pháp là whois DOMAIN_NAME, trong đó DOMAIN_NAME là miền mà bạn đang cố lấy thêm thông tin. Xem xét ví dụ sau khi thực thi **whois tryhackme.com**.



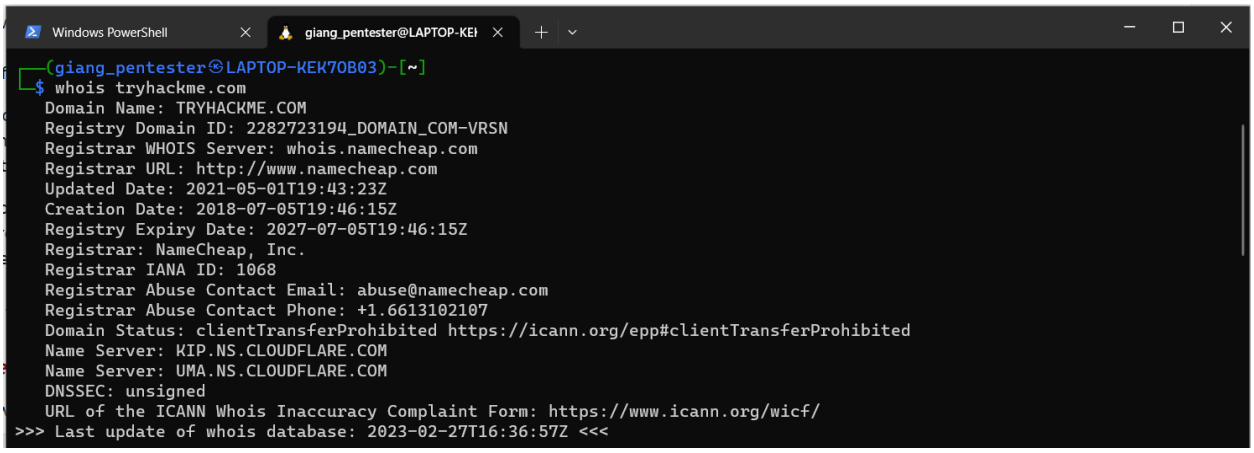
+ Chúng ta có thể thấy nhiều thông tin, chúng tôi sẽ kiểm tra chúng theo thứ tự hiển thị. Đầu tiên, chúng tôi nhận thấy rằng chúng tôi đã được chuyển hướng đến **whois.namecheap.com** để lấy thông tin của chúng tôi. Trong trường hợp này và tại thời điểm hiện tại, **namecheap.com** đang duy trì hồ sơ **WHOIS** cho tên miền này. Hơn nữa, chúng ta có thể thấy ngày tạo cùng với ngày cập nhật lần cuối và ngày hết hạn.

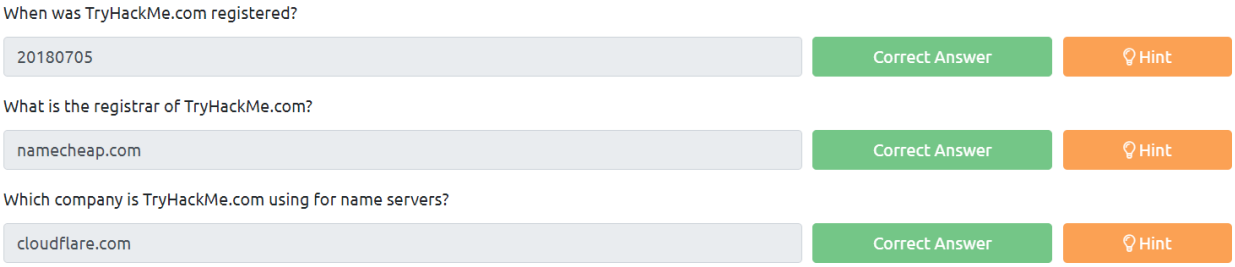
+ Tiếp theo, chúng tôi có được thông tin về công ty đăng ký và người đăng ký. Chúng tôi có thể tìm thấy tên và thông tin liên hệ của người đăng ký trừ khi họ đang sử dụng một số dịch vụ bảo mật. Mặc dù không được hiển thị ở trên, nhưng chúng tôi nhận được địa chỉ liên hệ của quản trị viên và kỹ thuật viên cho miền này. Cuối cùng, chúng tôi thấy các máy chủ tên miền mà chúng tôi nên truy vấn nếu chúng tôi có bất kỳ bản ghi DNS nào để tra cứu.

+ Thông tin được thu thập có thể được kiểm tra để tìm các bề mặt tấn công mới, chẳng hạn như tấn công kỹ thuật hoặc kỹ thuật xã hội. Chẳng hạn, tùy thuộc vào phạm vi của thử nghiệm thâm nhập, bạn có thể xem xét một cuộc tấn công nhằm vào máy chủ email của người dùng quản trị hoặc máy chủ DNS, giả sử chúng thuộc sở hữu của khách hàng của bạn và nằm trong phạm vi của thử nghiệm thâm nhập.

+ Điều quan trọng cần lưu ý là do các công cụ tự động lạm dụng truy vấn WHOIS để thu thập địa chỉ email, nhiều dịch vụ WHOIS thực hiện các biện pháp chống lại điều này. Ví dụ, họ có thể sắp xếp lại địa chỉ email. Hơn nữa, nhiều người đăng ký đăng ký các dịch vụ bảo mật để tránh địa chỉ email của họ bị những kẻ gửi thư rác thu thập và giữ thông tin của họ ở chế độ riêng tư.

Example : whois tryhackme.com





4. nslookup and dig

- Trong tác vụ trước, chúng tôi đã sử dụng giao thức WHOIS để nhận nhiều thông tin khác nhau về tên miền mà chúng tôi đang tìm kiếm. Đặc biệt, chúng tôi có thể lấy các máy chủ DNS từ công ty đăng ký.

- Tìm địa chỉ IP của một tên miền bằng cách sử dụng nslookup, viết tắt của **Name Server Look Up**. Bạn cần ra lệnh **nslookup DOMAIN_NAME**, ví dụ: nslookup tryhackme.com. Hoặc, tổng quát hơn, bạn có thể sử dụng nslookup OPTION DOMAIN_NAME SERVER. Ba tham số chính này là:

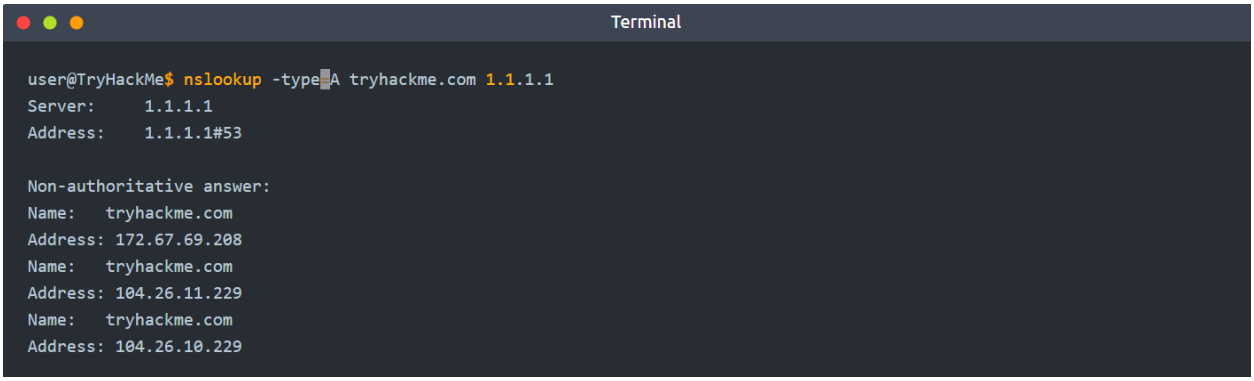
+ OPTIONS chứa loại truy vấn như trong bảng bên dưới. Chẳng hạn, bạn có thể sử dụng A cho địa chỉ IPv4 và AAAA cho địa chỉ IPv6.

+ DOMAIN_NAME là tên miền bạn đang tra cứu.

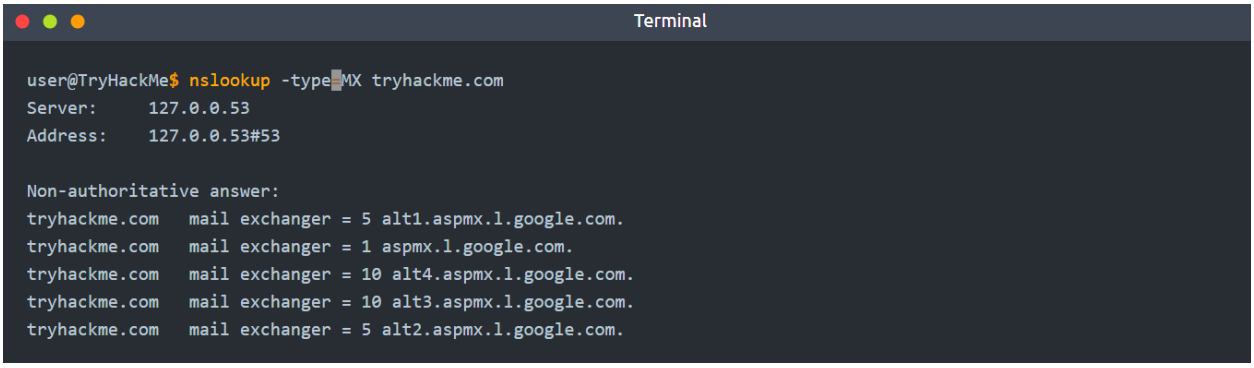
+ SERVER là máy chủ DNS mà bạn muốn truy vấn. Bạn có thể chọn bất kỳ máy chủ DNS cục bộ hoặc công cộng nào để truy vấn. **Cloudflare** cung cấp 1.1.1.1 và 1.0.0.1, **Google** cung cấp 8.8.8.8 và 8.8.4.4 và **Quad9** cung cấp 9.9.9.9 và 149.112.112.112. Có nhiều máy chủ DNS công cộng khác mà bạn có thể chọn nếu muốn có các lựa chọn thay thế cho máy chủ DNS của ISP. Bạn có thể tìm kiếm nhiều máy chủ DNS công cộng ở trang web sau đây: more public DNS Server

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

- Chẳng hạn, **nslookup -type=A tryhackme.com 1.1.1.1** (hoặc **nslookup -type=a tryhackme.com 1.1.1.1** vì nó không phân biệt chữ hoa chữ thường) có thể được sử dụng để trả về tất cả các địa chỉ IPv4 được tryhackme.com sử dụng.



- Giả sử bạn muốn tìm hiểu về các máy chủ email và cấu hình cho một miền cụ thể. Bạn có thể tùy chỉnh câu lệnh nslook up như sau: **nslookup -type=MX tryhackme.com**. Đây là một ví dụ:



- Chúng ta có thể thấy rằng cấu hình email hiện tại của tryhackme.com sử dụng Google. Vì MX đang tìm kiếm các máy chủ Mail Exchange, chúng tôi nhận thấy rằng khi một máy chủ thư cố gắng gửi email @tryhackme.com, nó sẽ cố gắng kết nối với aspmx.l.google.com, có thứ tự 1. Nếu nó đang bận hoặc không khả dụng, máy chủ thư sẽ cố gắng kết nối với máy chủ trao đổi thư theo thứ tự tiếp theo, alt1.aspmx.l.google.com hoặc alt2.aspmx.l.google.com.

- Đối với các truy vấn DNS nâng cao hơn và chức năng bổ sung, bạn có thể sử dụng dig, từ viết tắt của “Domain Information Groper,” nếu bạn tò mò. Hãy sử dụng Dig để tra cứu các bản ghi MX và so sánh chúng với nslookup. Chúng tôi có thể sử dụng dig DOMAIN_NAME, nhưng để chỉ định loại bản ghi, chúng tôi sẽ sử dụng dig

DOMAIN_NAME TYPE. Theo tùy chọn, chúng tôi có thể chọn máy chủ mà chúng tôi muốn truy vấn bằng cách sử dụng dig @SERVER DOMAIN_NAME TYPE.

```
┌──(giang_pentester㉿LAPTOP-KEK7OB03)-[~]
└─$ dig tryhackme.com MX

; <<>> DiG 9.18.8-1-Debian <<>> tryhackme.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41687
;; flags: qr rd ad; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;tryhackme.com.                 IN      MX

;; ANSWER SECTION:
tryhackme.com.          0       IN      MX      1 aspmx.l.google.com.
tryhackme.com.          0       IN      MX      5 alt2.aspmx.l.google.com.
tryhackme.com.          0       IN      MX      5 alt1.aspmx.l.google.com.
tryhackme.com.          0       IN      MX      10 alt3.aspmx.l.google.com.
tryhackme.com.          0       IN      MX      10 alt4.aspmx.l.google.com.

;; Query time: 130 msec
;; SERVER: 172.26.32.1#53(172.26.32.1) (UDP)
;; WHEN: Tue Feb 28 00:08:49 +07 2023
;; MSG SIZE  rcvd: 234
```

- So sánh nhanh giữa đầu ra của nslookup và dig cho thấy rằng dig trả về nhiều thông tin hơn, chẳng hạn như TTL (Time to Live) theo mặc định. Nếu muốn truy vấn máy chủ DNS 1.1.1.1, bạn có thể thực hiện lệnh **dig @1.1.1.1 tryhackme.com MX.**

```
┌──(giang_pentester㉿LAPTOP-KEK7OB03)-[~]
└─$ nslookup -type=TXT thmlabs.com
Server:         172.26.32.1
Address:        172.26.32.1#53

Non-authoritative answer:
thmlabs.com     text = "THM{a5b83929888ed36acb0272971e438d78}"

Authoritative answers can be found from:
```

Check the TXT records of thmlabs.com. What is the flag there?

THM{a5b83929888ed36acb0272971e438d78} Correct Answer

5. DNSDumpster

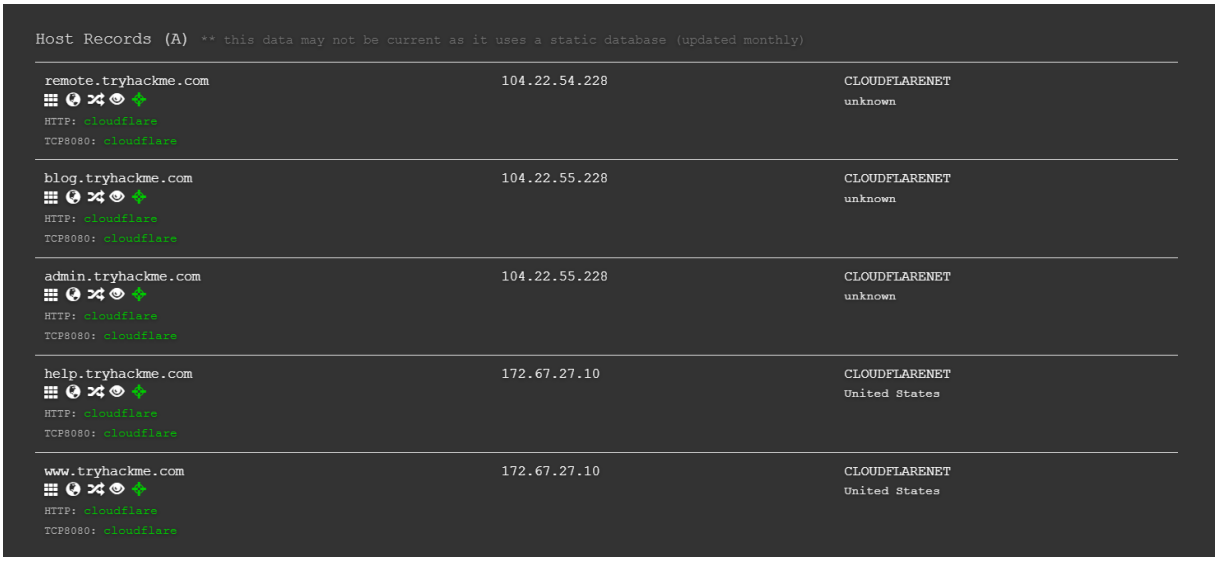
- Các công cụ tra cứu DNS, chẳng hạn như nslookup và dig, không thể tự tìm tên miền phụ. Miền bạn đang kiểm tra có thể bao gồm một miền phụ khác có thể tiết lộ nhiều thông tin về mục tiêu. Chẳng hạn, nếu tryhackme.com có các tên miền phụ wiki.tryhackme.com và webmail.tryhackme.com, bạn muốn tìm hiểu thêm về hai tên miền này vì chúng có thể chứa một kho thông tin về mục tiêu của bạn. Có khả năng một trong những tên miền phụ này đã được thiết

lập và không được cập nhật thường xuyên. Thiếu cập nhật thường xuyên thích hợp thường dẫn đến các dịch vụ dễ bị tổn thương. Nhưng làm thế nào chúng ta có thể biết rằng các tên miền phụ như vậy tồn tại?

- Chúng tôi có thể xem xét việc sử dụng nhiều công cụ tìm kiếm để biên soạn danh sách các tên miền phụ được biết đến công khai. Một công cụ tìm kiếm sẽ không đủ; hơn nữa, chúng ta nên xem qua ít nhất hàng chục kết quả để tìm ra dữ liệu thú vị. Xét cho cùng, bạn đang tìm kiếm các tên miền phụ không được quảng cáo rõ ràng và do đó không cần thiết phải đưa tên miền đó lên trang đầu tiên của kết quả tìm kiếm. Một cách tiếp cận khác để khám phá các tên miền phụ như vậy là dựa vào các truy vấn **brute-forcing** để tìm tên miền phụ nào có bản ghi DNS.

- Để tránh việc tìm kiếm tốn thời gian như vậy, người ta có thể sử dụng dịch vụ trực tuyến cung cấp câu trả lời chi tiết cho các truy vấn DNS, chẳng hạn như **DNSDumpster**. Nếu chúng tôi tìm kiếm DNSDumpster cho tryhackme.com, chúng tôi sẽ phát hiện ra tên miền phụ blog.tryhackme.com, mà một truy vấn DNS thông thường không thể cung cấp. Ngoài ra, DNSDumpster sẽ trả lại thông tin DNS đã thu thập dưới dạng bảng và biểu đồ dễ đọc. DNSDumpster cũng sẽ cung cấp mọi thông tin thu thập được về các máy chủ lắng nghe.

- Chúng tôi sẽ tìm kiếm tryhackme.com trên DNSDumpster để cung cấp cho bạn một cái nhìn thoáng qua về đầu ra dự kiến. Trong số các kết quả, chúng tôi có một danh sách các máy chủ DNS cho tên miền mà chúng tôi đang tìm kiếm. DNSDumpster cũng đã phân giải tên miền thành địa chỉ IP và thậm chí còn cố định vị trí địa lý của chúng. Chúng tôi cũng có thể xem các bản ghi MX; DNSDumpster đã giải quyết tất cả năm máy chủ trao đổi thư thành địa chỉ IP tương ứng của chúng và cung cấp thêm thông tin về chủ sở hữu và vị trí. Cuối cùng, chúng ta có thể thấy các bản ghi TXT. Thực tế, một truy vấn duy nhất là đủ để lấy tất cả thông tin này.



Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

remote.tryhackme.com HTTP: cloudflare TCP8080: cloudflare	104.22.54.228	CLOUDFLARENET unknown
blog.tryhackme.com HTTP: cloudflare TCP8080: cloudflare	104.22.55.228	CLOUDFLARENET unknown
admin.tryhackme.com HTTP: cloudflare TCP8080: cloudflare	104.22.55.228	CLOUDFLARENET unknown
help.tryhackme.com HTTP: cloudflare TCP8080: cloudflare	172.67.27.10	CLOUDFLARENET United States
www.tryhackme.com HTTP: cloudflare TCP8080: cloudflare	172.67.27.10	CLOUDFLARENET United States

Lookup tryhackme.com on DNSDumpster. What is one interesting subdomain that you would discover in addition to www and blog?

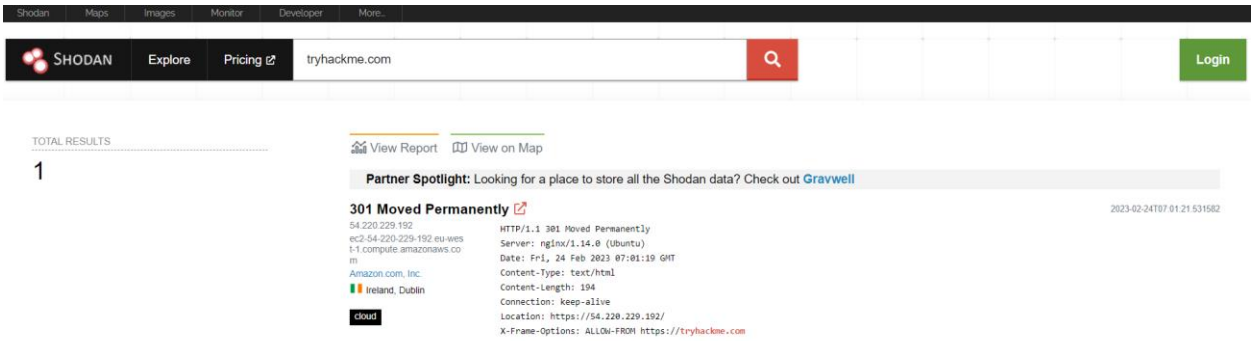
remote

Correct Answer

6. Shodan.io

- Khi bạn được giao nhiệm vụ chạy thử nghiệm thâm nhập đối với các mục tiêu cụ thể, như một phần của giai đoạn passive reconnaissance , một dịch vụ như Shodan.io có thể hữu ích để tìm hiểu nhiều thông tin khác nhau về mạng của khách hàng mà không cần chủ động kết nối với mạng đó. Hơn nữa, về mặt phòng thủ, bạn có thể sử dụng các dịch vụ khác nhau từ Shodan.io để tìm hiểu về các thiết bị được kết nối và tiếp xúc thuộc về tổ chức của bạn.

- Shodan.io cố gắng kết nối với mọi thiết bị có thể truy cập trực tuyến để xây dựng công cụ tìm kiếm các “things” được kết nối trái ngược với công cụ tìm kiếm cho các trang web. Sau khi nhận được phản hồi, nó sẽ thu thập tất cả thông tin liên quan đến dịch vụ và lưu vào cơ sở dữ liệu để có thể tìm kiếm được. Xem xét bản ghi đã lưu của một trong các máy chủ của tryhackme.com.



According to Shodan.io, what is the 2nd country in the world in terms of the number of publicly accessible Apache servers?

Germany — Correct Answer

Based on Shodan.io, what is the 3rd most common port used for Apache?

8080 — Correct Answer

Based on Shodan.io, what is the 3rd most common port used for nginx?

8888 — Correct Answer

7. 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`