Passive Reconnaissance

Introduction

Welcome to the first room of the Network Security Module. This module covers:

1. Passive Reconnaissance
2. Active Reconnaissance
3. Nmap Live Host Discovery
4. Nmap Basic Port Scans
5. Nmap Advanced Port Scans
6. Nmap Post Port Scans
7. Protocols and Servers
8. Protocols and Servers 2
9. Network Security Challenge

In this room, after we define passive reconnaissance and active reconnaissance, we focus on essential tools related to passive reconnaissance. We will learn three command-line tools:

- whois to query WHOIS servers
- nslookup to query DNS servers
- dig to query DNS servers

We use whois to query WHOIS records, while we use nslookup and dig to query DNS database records. These are all publicly available records and hence do not alert the target.

We will also learn the usage of two online services:

- DNSDumpster
- Shodan.io

These two online services allow us to collect information about our target without directly connecting to it.

Pre-requisites: This room requires basic networking knowledge along with basic familiarity with the command line. The modules Network Fundamentals and Linux Fundamentals provide the required knowledge if necessary.

Important Notice: Please note that if you're not subscribed, the AttackBox won't have Internet access, so you will need to use the VPN to complete the questions that require Internet access.

Passive vs Active Recon

This room expects the user to have a working knowledge of computer networks. If you like to brush up on this topic, you are encouraged to study the Network Fundamentals module first.

Before the dawn of computer systems and networks, in the Art of War, Sun Tzu taught, “If you know the enemy and know yourself, your victory will not stand in doubt.” If you are playing the role of an attacker, you need to gather information about your target systems. If you are playing the role of a defender, you need to know what your adversary will discover about your systems and networks.

Reconnaissance (recon) can be defined as a preliminary survey to gather information about a target. It is the first step in The Unified Kill Chain to gain an initial foothold on a system. We divide reconnaissance into:

1. Passive Reconnaissance
2. Active Reconnaissance

In passive reconnaissance, you rely on publicly available knowledge. It is the knowledge that you can access from publicly available resources without directly engaging with the target. Think of it like you are looking at target territory from afar without stepping foot on that territory.

Passive reconnaissance activities include many activities, for instance:

- Looking up DNS records of a domain from a public DNS server.
- Checking job ads related to the target website.
- Reading news articles about the target company.

Active reconnaissance, on the other hand, cannot be achieved so discreetly. It requires direct engagement with the target. Think of it like you check the locks on the doors and windows, among other potential entry points.

Examples of active reconnaissance activities include:

- Connecting to one of the company servers such as HTTP, FTP, and SMTP.
- Calling the company in an attempt to get information (social engineering).
- Entering company premises pretending to be a repairman.

Considering the invasive nature of active reconnaissance, one can quickly get into legal trouble unless one obtains proper legal authorization.
****

Answer the questions below:

You visit the Facebook page of the target company, hoping to get some of their employee names. What kind of reconnaissance activity is this? (A for active, P for passive)
Answer: P

You ping the IP address of the company webserver to check if ICMP traffic is blocked. What kind of reconnaissance activity is this? (A for active, P for passive)
Answer: A

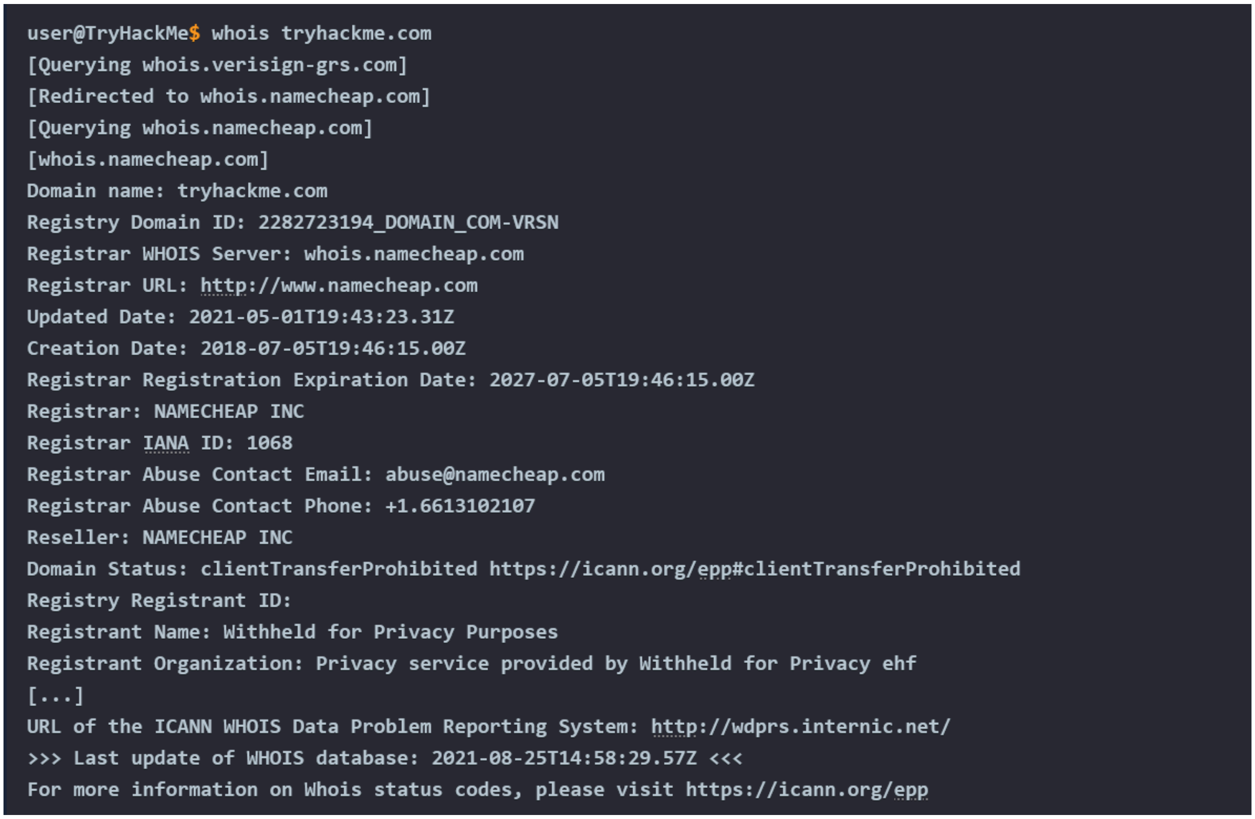
You happen to meet the IT administrator of the target company at a party. You try to use social engineering to get more information about their systems and network infrastructure. What kind of reconnaissance activity is this? (A for active, P for passive)
Answer: A
****

Whois

WHOIS is a request and response protocol that follows the RFC 3912 specification. A WHOIS server listens on TCP port 43 for incoming requests. The domain registrar is responsible for maintaining the WHOIS records for the domain names it is leasing. The WHOIS server replies with various information related to the domain requested. Of particular interest, we can learn:

- Registrar: Via which registrar was the domain name registered?
- Contact info of registrant: Name, organization, address, phone, among other things. (unless made hidden via a privacy service)
- Creation, update, and expiration dates: When was the domain name first registered? When was it last updated? And when does it need to be renewed?
- Name Server: Which server to ask to resolve the domain name?

To get this information, we need to use a whois client or an online service. Many online services provide whois information; however, it is generally faster and more convenient to use your local whois client. Using the AttackBox (or your local Linux machine, such as Parrot or Kali), you can easily access your whois client on the terminal. The syntax is whois DOMAIN_NAME, where DOMAIN_NAME is the domain about which you are trying to get more information. Consider the following example executing whois tryhackme.com.



```
user@TryHackMe$ whois tryhackme.com
[Querying whois.verisign-grs.com]
[Redirected to whois.namecheap.com]
[Querying whois.namecheap.com]
[whois.namecheap.com]
Domain name: tryhackme.com
Registry Domain ID: 2282723194_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2021-05-01T19:43:23.31Z
Creation Date: 2018-07-05T19:46:15.00Z
Registrar Registration Expiration Date: 2027-07-05T19:46:15.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Withheld for Privacy Purposes
Registrant Organization: Privacy service provided by Withheld for Privacy ehf
[...]
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2021-08-25T14:58:29.57Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
```

We can see plenty of information; we will inspect them in the order displayed. First, we notice that we were redirected to whois.namecheap.com to get our information. In this case and at the time being, namecheap.com is maintaining the WHOIS record for this domain name. Furthermore, we can see the creation date along with the last-update date and expiration date.

Next, we obtain information about the registrar and the registrant. We can find the registrant's name and contact information unless they are using some privacy service. Although not displayed above, we get the admin and tech contacts for this domain. Finally, we see the domain name servers that we should query if we have any DNS records to look up.

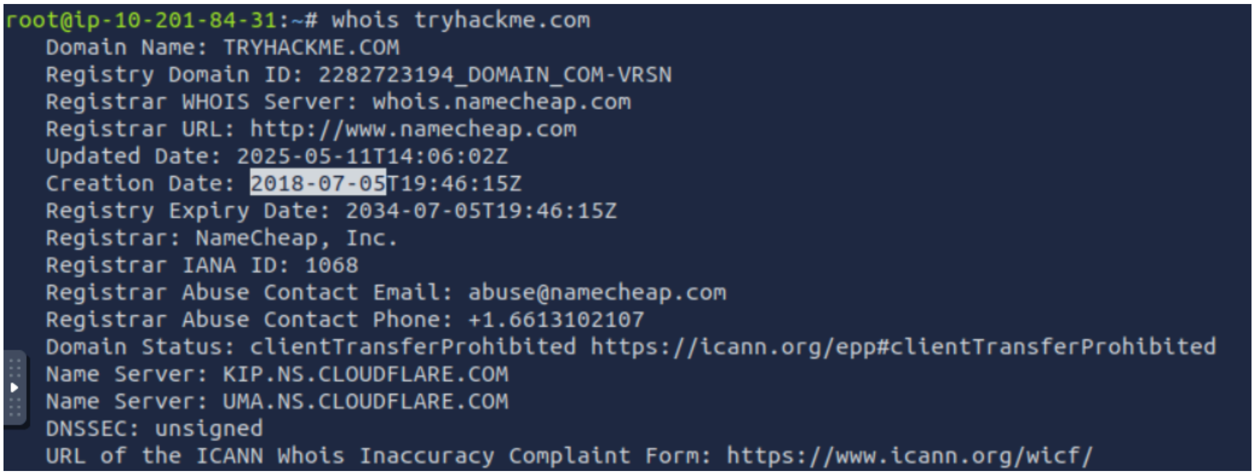
The information collected can be inspected to find new attack surfaces, such as social engineering or technical attacks. For instance, depending on the scope of the penetration test, you might consider an attack against the email server of the admin user or the DNS servers, assuming they are owned by your client and fall within the scope of the penetration test.

It is important to note that due to automated tools abusing WHOIS queries to harvest email addresses, many WHOIS services take measures against this. They might redact email addresses, for instance. Moreover, many registrants subscribe to privacy services to avoid their email addresses being harvested by spammers and keep their information private.

On the AttackBox, open the terminal and run the whois tryhackme.com command to get the information you need to answer the following questions.
****

Answer the questions below:

When was TryHackMe.com registered?



```
root@ip-10-201-84-31:~# whois tryhackme.com
   Domain Name: TRYHACKME.COM
   Registry Domain ID: 2282723194_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.namecheap.com
   Registrar URL: http://www.namecheap.com
   Updated Date: 2025-05-11T14:06:02Z
   Creation Date: 2018-07-05T19:46:15Z
   Registry Expiry Date: 2034-07-05T19:46:15Z
   Registrar: NameCheap, Inc.
   Registrar IANA ID: 1068
   Registrar Abuse Contact Email: abuse@namecheap.com
   Registrar Abuse Contact Phone: +1.6613102107
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: KIP.NS.CLOUDFLARE.COM
   Name Server: UMA.NS.CLOUDFLARE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```

Answer: 20180705

What is the registrar of TryHackMe.com?
Answer: namecheap.com

Which company is TryHackMe.com using for name servers?
Answer: cloudflare.com
****

nslookup and dig

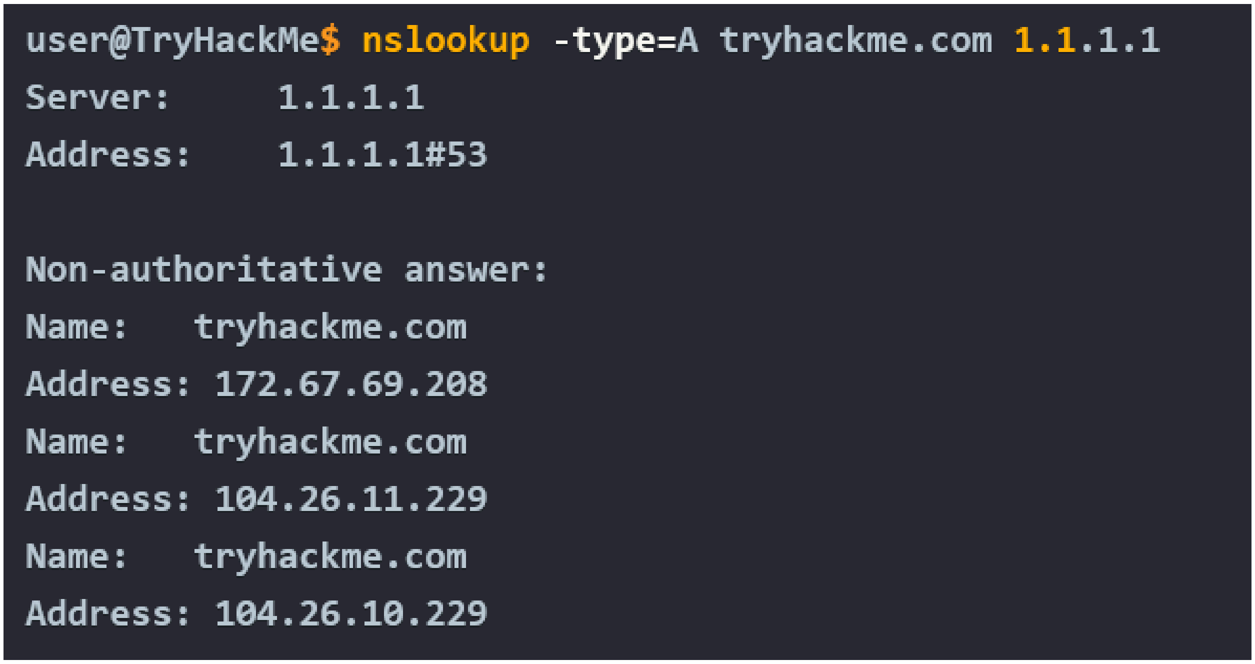
In the previous task, we used the WHOIS protocol to get various information about the domain name we were looking up. In particular, we were able to get the DNS servers from the registrar.

Find the IP address of a domain name using nslookup, which stands for Name Server Look Up. You need to issue the command nslookup DOMAIN_NAME, for example, nslookup tryhackme.com. Or, more generally, you can use nslookup OPTIONS DOMAIN_NAME SERVER. These three main parameters are:

- OPTIONS contains the query type as shown in the table below. For instance, you can use A for IPv4 addresses and AAAA for IPv6 addresses.
- DOMAIN_NAME is the domain name you are looking up.
- SERVER is the DNS server that you want to query. You can choose any local or public DNS server to query. Cloudflare offers 1.1.1.1 and 1.0.0.1, Google offers 8.8.8.8 and 8.8.4.4, and Quad9 offers 9.9.9.9 and 149.112.112.112. There are many more public DNS servers that you can choose from if you want alternatives to your ISP's DNS servers.

Query Type	**Result**
A	IPv4 Address
AAAA	IPv6 Address
CNAME	Canonical Name
MX	Mail Servers
SOA	Start of Authority
TXT	TXT Records

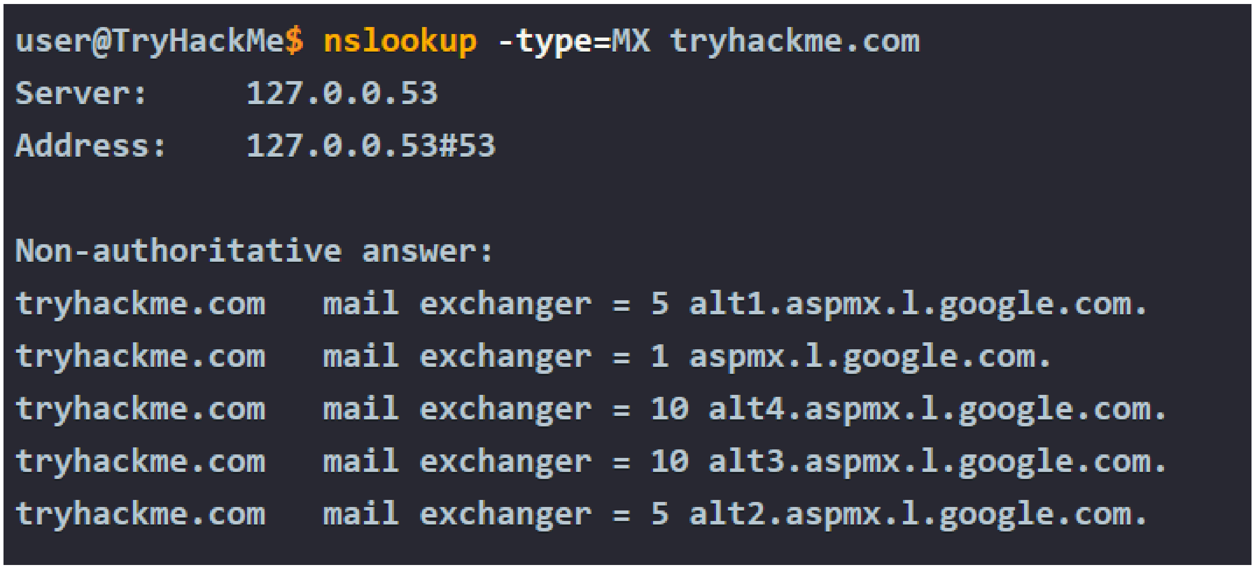
For instance, nslookup -type=A tryhackme.com 1.1.1.1 (or nslookup -type=a tryhackme.com 1.1.1.1 as it is case-insensitive) can be used to return all the IPv4 addresses used by tryhackme.com.



```
user@TryHackMe$ nslookup -type=A tryhackme.com 1.1.1.1
Server:     1.1.1.1
Address:    1.1.1.1#53

Non-authoritative answer:
Name:   tryhackme.com
Address: 172.67.69.208
Name:   tryhackme.com
Address: 104.26.11.229
Name:   tryhackme.com
Address: 104.26.10.229
```

The A and AAAA records are used to return IPv4 and IPv6 addresses, respectively. This lookup is helpful to know from a penetration testing perspective. In the example above, we started with one domain name, and we obtained three IPv4 addresses. Each of these IP addresses can be further checked for insecurities, assuming they lie within the scope of the penetration test.

Let's say you want to learn about the email servers and configurations for a particular domain. You can issue nslookup -type=MX tryhackme.com. Here is an example:



```
user@TryHackMe$ nslookup -type=MX tryhackme.com
Server:     127.0.0.53
Address:    127.0.0.53#53

Non-authoritative answer:
tryhackme.com   mail exchanger = 5 alt1.aspmx.l.google.com.
tryhackme.com   mail exchanger = 1 aspmx.l.google.com.
tryhackme.com   mail exchanger = 10 alt4.aspmx.l.google.com.
tryhackme.com   mail exchanger = 10 alt3.aspmx.l.google.com.
tryhackme.com   mail exchanger = 5 alt2.aspmx.l.google.com.
```

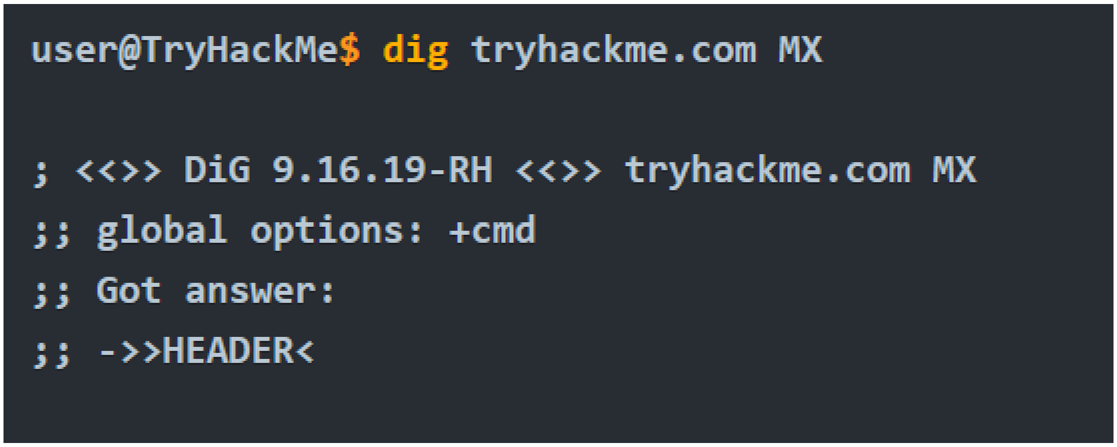
We can see that tryhackme.com's current email configuration uses Google. Since MX is looking up the Mail Exchange servers, we notice that when a mail server tries to deliver email @tryhackme.com, it will try to connect to the aspmx.l.google.com, which has order 1. If it is busy or unavailable, the mail server will attempt to connect to the next in order mail exchange servers, alt1.aspmx.l.google.com or alt2.aspmx.l.google.com.

Google provides the listed mail servers; therefore, we should not expect the mail servers to be running a vulnerable server version. However, in other cases, we might find mail servers that are not adequately secured or patched.

Such pieces of information might prove valuable as you continue the passive reconnaissance of your target. You can repeat similar queries for other domain names and try different types, such as -type=txt. Who knows what kind of information you might discover along your way!

For more advanced DNS queries and additional functionality, you can use dig, the acronym for "Domain Information Groper," if you are curious. Let's use dig to look up the MX records and compare them to nslookup. We can use dig DOMAIN_NAME, but to specify the record type, we would use dig DOMAIN_NAME TYPE. Optionally, we can select the server we want to query using dig @SERVER DOMAIN_NAME TYPE.

- SERVER is the DNS server that you want to query.
- DOMAIN_NAME is the domain name you are looking up.
- TYPE contains the DNS record type, as shown in the table provided earlier.



```
user@TryHackMe$ dig tryhackme.com MX

; <<>> DiG 9.16.19-RH <<>> tryhackme.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<
```

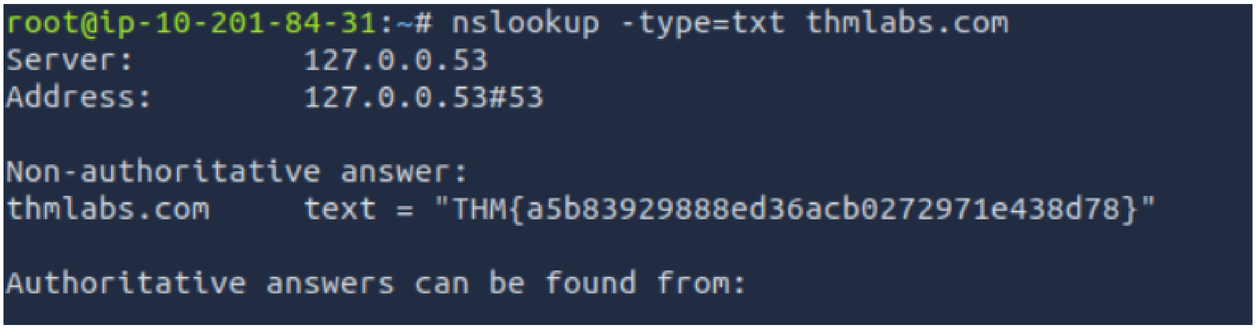
A quick comparison between the output of nslookup and dig shows that dig returned more information, such as the TTL (Time To Live) by default. If you want to query a 1.1.1.1 DNS server, you can execute dig @1.1.1.1 tryhackme.com MX.

Using the AttackBox, open the terminal and use the nslookup or dig command to get the information you need to answer the following question.

****

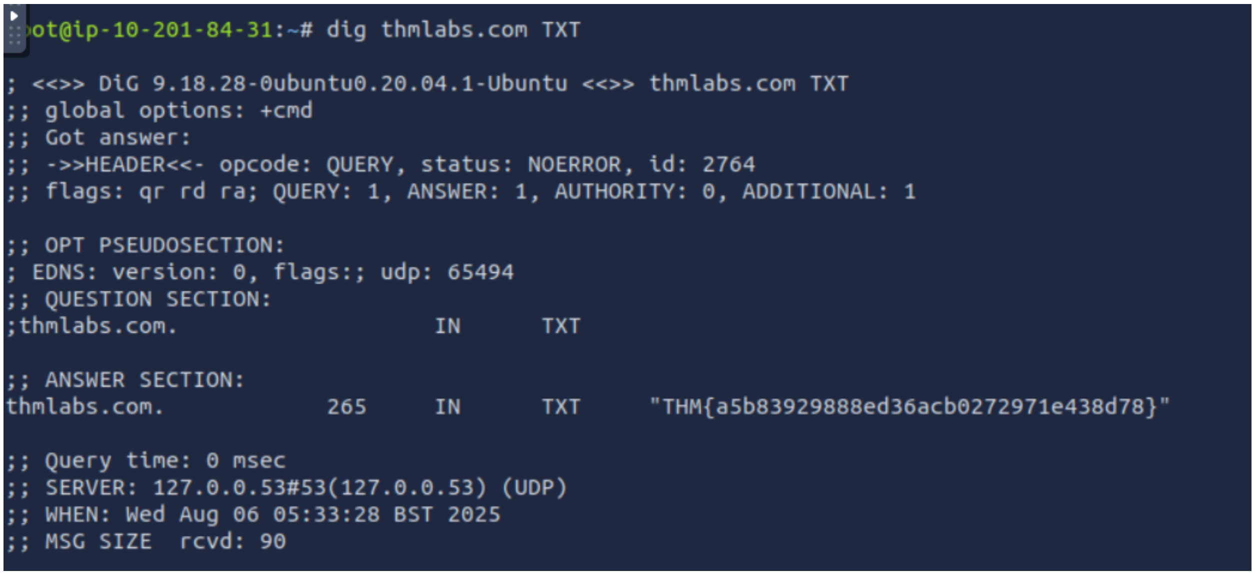
Answer the questions below:

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



```
root@ip-10-201-84-31:~# nslookup -type=txt thmlabs.com
Server:         127.0.0.53
Address:        127.0.0.53#53

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

Authoritative answers can be found from:
```

Or



```
oot@ip-10-201-84-31:~# dig thmlabs.com TXT

; <<>> DiG 9.18.28-0ubuntu0.20.04.1-Ubuntu <<>> thmlabs.com TXT
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2764
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;thmlabs.com.                   IN      TXT

;; ANSWER SECTION:
thmlabs.com.            265     IN      TXT     "THM{a5b83929888ed36acb0272971e438d78}"

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Aug 06 05:33:28 BST 2025
;; MSG SIZE  rcvd: 90
```

Answer: THM{a5b83929888ed36acb0272971e438d78}

****

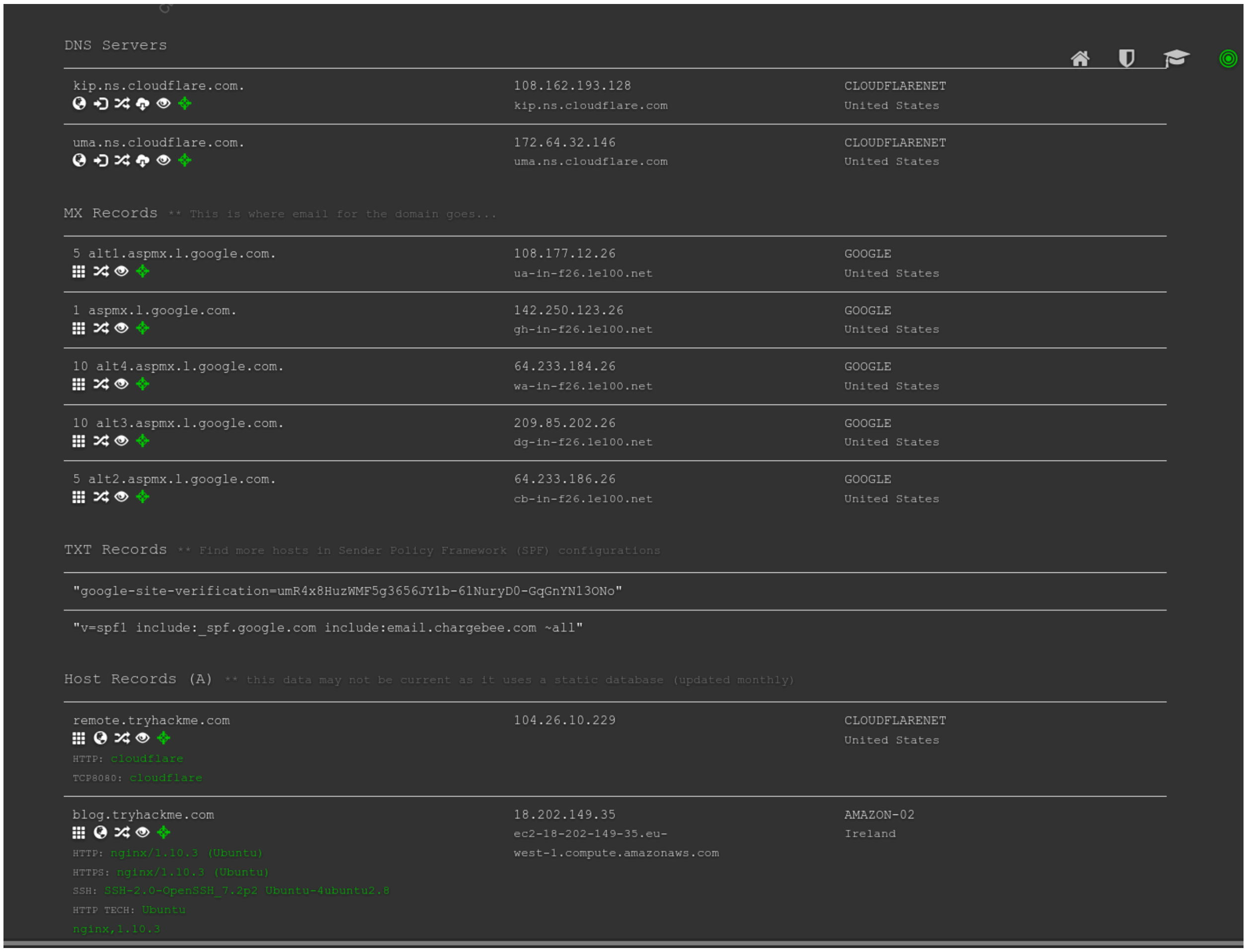
DNSDumpster

DNS lookup tools, such as nslookup and dig, cannot find subdomains on their own. The domain you are inspecting might include a different subdomain that can reveal much information about the target. For instance, if tryhackme.com has the subdomains wiki.tryhackme.com and webmail.tryhackme.com, you want to learn more about these two as they can hold a trove of information about your target. There is a possibility that one of these subdomains has been set up and is not updated regularly. Lack of proper regular updates usually leads to vulnerable services. But how can we know that such subdomains exist?

We can consider using multiple search engines to compile a list of publicly known subdomains. One search engine won't be enough; moreover, we should expect to go through at least tens of results to find interesting data. After all, you are looking for subdomains that are not explicitly advertised, and hence it is not necessary to make it to the first page of search results. Another approach to discover such subdomains would be to rely on brute-forcing queries to find which subdomains have DNS records.

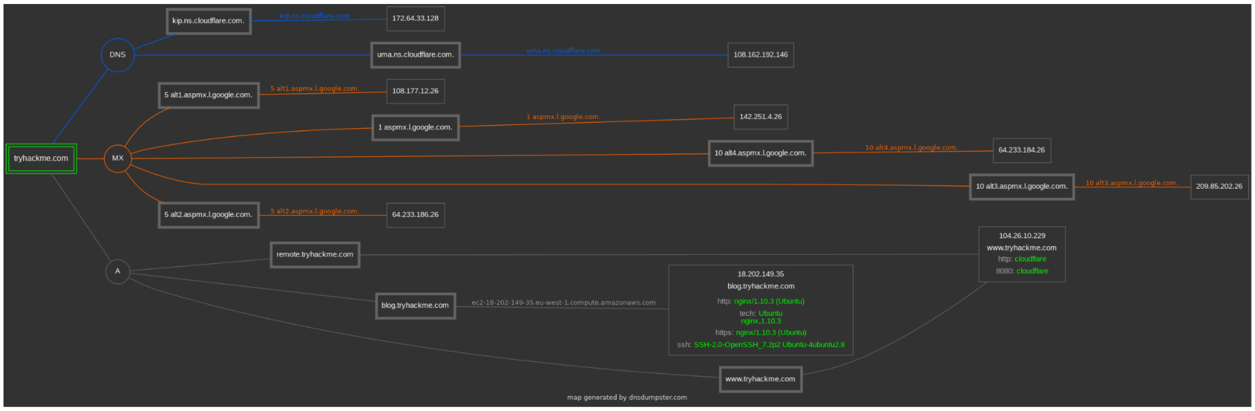
To avoid such a time-consuming search, one can use an online service that offers detailed answers to DNS queries, such as DNSDumpster. If we search DNSDumpster for tryhackme.com, we will discover the subdomain blog.tryhackme.com, which a typical DNS query cannot provide. In addition, DNSDumpster will return the collected DNS information in easy-to-read tables and a graph. DNSDumpster will also provide any collected information about listening servers.

We will search for tryhackme.com on DNSDumpster to give you a glimpse of the expected output. Among the results, we got a list of DNS servers for the domain we are looking up. DNSDumpster also resolved the domain names to IP addresses and even tried to geolocate them. We can also see the MX records; DNSDumpster resolved all five mail exchange servers to their respective IP addresses and provided more information about the owner and location. Finally, we can see TXT records. Practically a single query was enough to retrieve all this information.

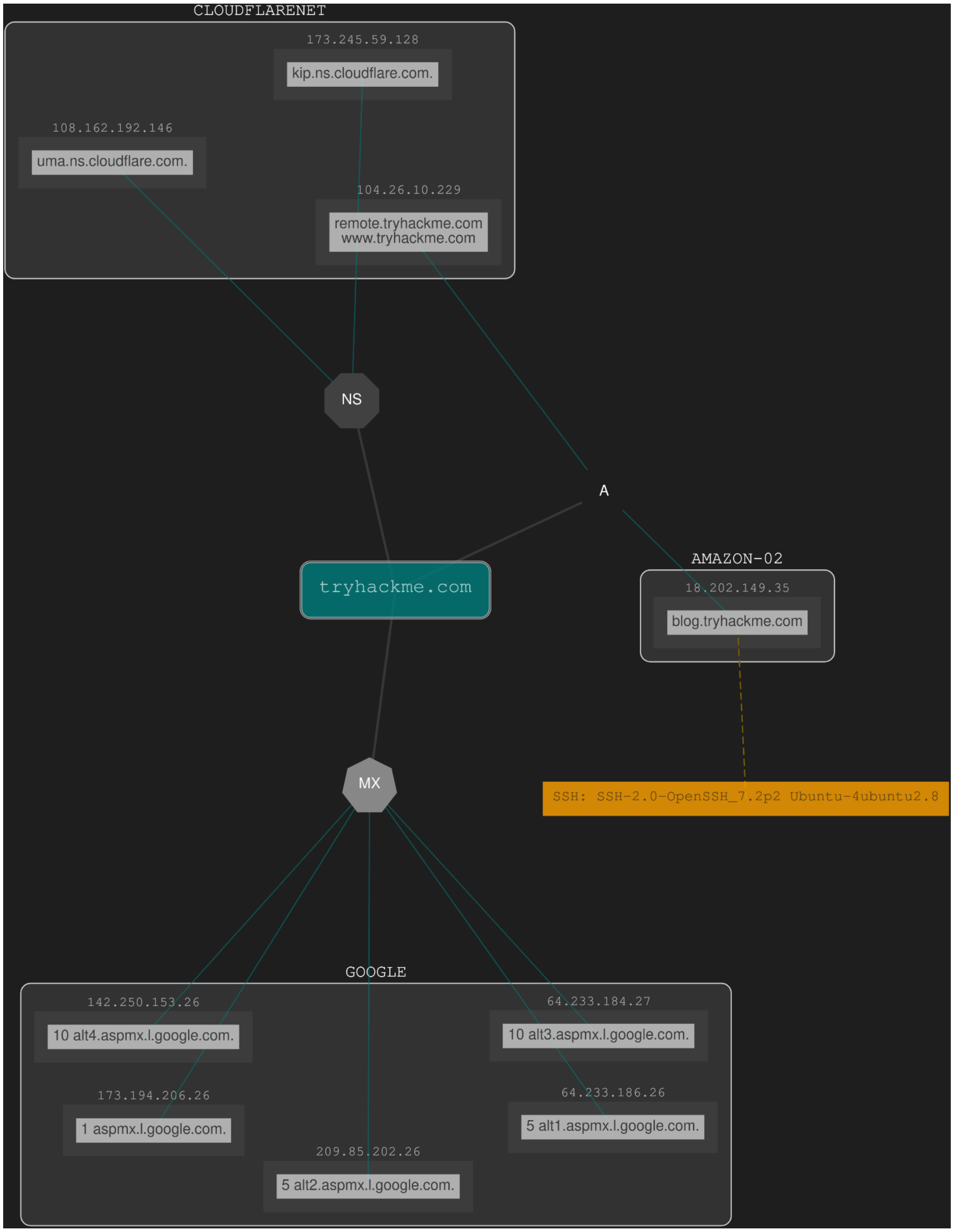


```
DNS Servers

kip.ns.cloudflare.com.        108.162.193.128          CLOUDFLARENET
                              kip.ns.cloudflare.com    United States

uma.ns.cloudflare.com.        172.64.32.146            CLOUDFLARENET
                              uma.ns.cloudflare.com    United States

MX Records ** This is where email for the domain goes...

5 alt1.aspmx.l.google.com.    108.177.12.26            GOOGLE
                              ua-in-f26.1e100.net      United States

1 aspmx.l.google.com.         142.250.123.26           GOOGLE
                              gh-in-f26.1e100.net      United States

10 alt4.aspmx.l.google.com.   64.233.184.26            GOOGLE
                              wa-in-f26.1e100.net      United States

10 alt3.aspmx.l.google.com.   209.85.202.26            GOOGLE
                              dg-in-f26.1e100.net      United States

5 alt2.aspmx.l.google.com.    64.233.186.26            GOOGLE
                              cb-in-f26.1e100.net      United States

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

"google-site-verification=umR4x8HuzWMF5g3656JY1b-61NuryD0-GqGnYN13ONo"

"v=spf1 include:_spf.google.com include:email.chargebee.com ~all"

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

remote.tryhackme.com          104.26.10.229            CLOUDFLARENET
                                                       United States
HTTP: cloudflare
TCP8080: cloudflare

blog.tryhackme.com            18.202.149.35            AMAZON-02
                              ec2-18-202-149-35.eu-    Ireland
                              west-1.compute.amazonaws.com
HTTP: nginx/1.10.3 (Ubuntu)
HTTPS: nginx/1.10.3 (Ubuntu)
SSH: SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.8
HTTP TECH: Ubuntu
nginx,1.10.3
```

DNSDumpster will also represent the collected information graphically. DNSDumpster displayed the data from the table earlier as a graph. You can see the DNS and MX branching to their respective servers and also showing the IP addresses.



There is currently a beta feature that allows you to export the graph as well. You can manipulate the graph and move blocks around if needed.

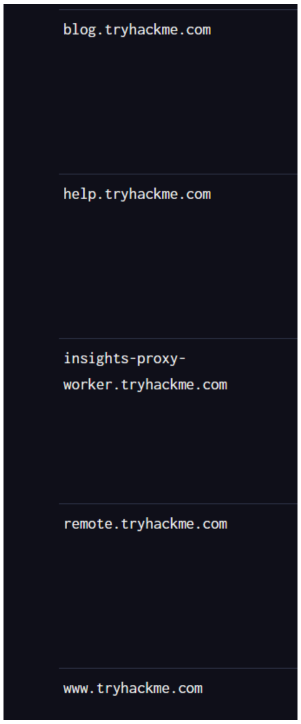


Use the web browser on the AttackBox, or your system, to answer the following question.

****

Answer the questions below:

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



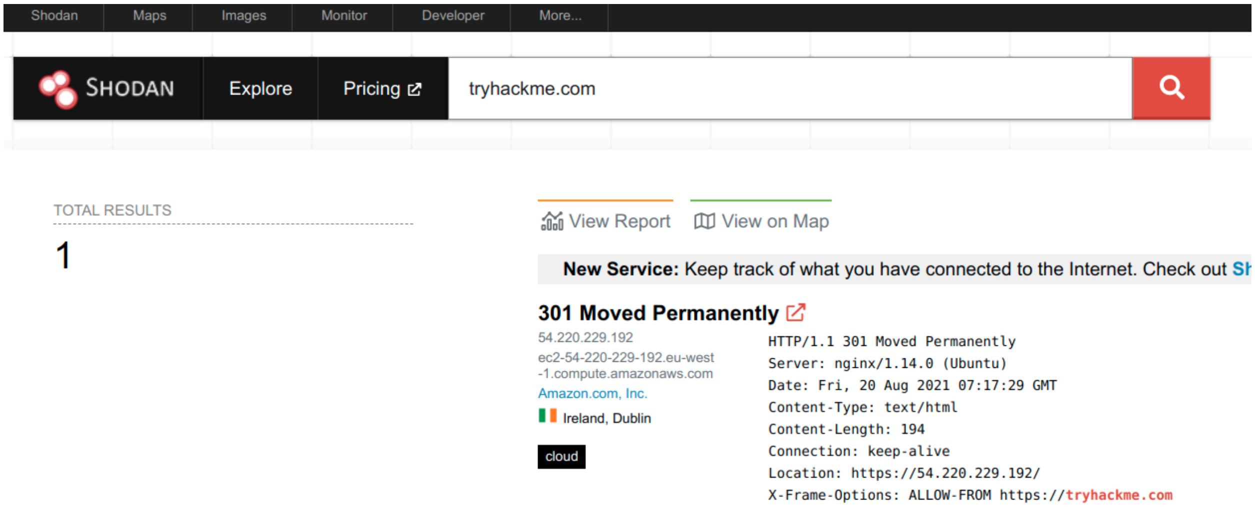
```
blog.tryhackme.com

help.tryhackme.com

insights-proxy-
worker.tryhackme.com

remote.tryhackme.com

www.tryhackme.com
```

Answer: Remote
****

Shodan.io

When you are tasked to run a penetration test against specific targets, as part of the passive reconnaissance phase, a service like Shodan.io can be helpful to learn various pieces of information about the client's network, without actively connecting to it. Furthermore, on the defensive side, you can use different services from Shodan.io to learn about connected and exposed devices belonging to your organization.

Shodan.io tries to connect to every device reachable online to build a search engine of connected “things” in contrast with a search engine for web pages. Once it gets a response, it collects all the information related to the service and saves it in the database to make it searchable. Consider the saved record of one of tryhackme.com's servers.



TOTAL RESULTS

1

New Service: Keep track of what you have connected to the Internet. Check out Sh

301 Moved Permanently

54.220.229.192
ec2-54-220-229-192.eu-west-1.compute.amazonaws.com
Amazon.com, Inc.
Ireland, Dublin

```
HTTP/1.1 301 Moved Permanently
Server: nginx/1.14.0 (Ubuntu)
Date: Fri, 20 Aug 2021 07:17:29 GMT
Content-Type: text/html
Content-Length: 194
Connection: keep-alive
Location: https://54.220.229.192/
X-Frame-Options: ALLOW-FROM https://tryhackme.com
```

This record shows a web server; however, as mentioned already, Shodan.io collects information related to any device it can find connected online. Searching for tryhackme.com on Shodan.io will display at least the record shown in the screenshot above. Via this Shodan.io search result, we can learn several things related to our search, such as:

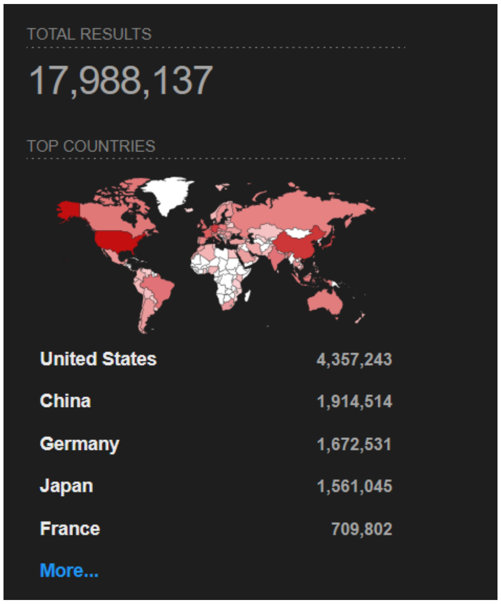
- IP address
- hosting company
- geographic location
- server type and version

You may also try searching for the IP addresses you have obtained from DNS lookups. These are, of course, more subject to change. On their help page, you can learn about all the search options available at Shodan.io, and you are encouraged to join TryHackMe's Shodan.io room.

It would be best to visit Shodan.io to answer the following questions; however, note that you can find the answers on Shodan.io without needing a premium account.
****

Answer the questions below:

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



TOTAL RESULTS

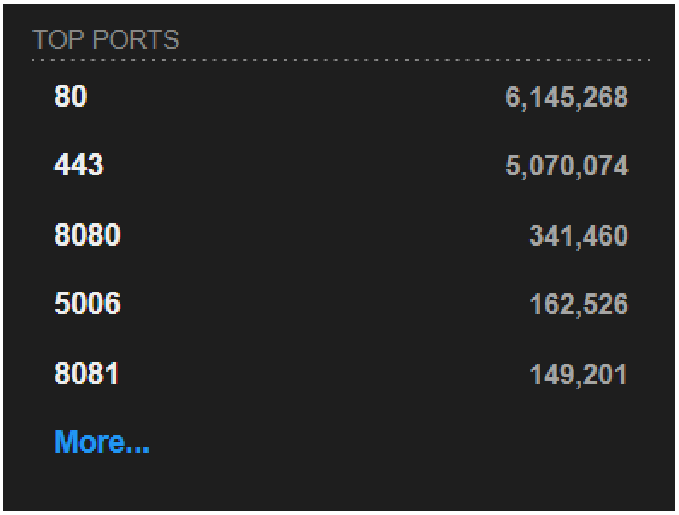
17,988,137

TOP COUNTRIES

United States	4,357,243
China	1,914,514
Germany	1,672,531
Japan	1,561,045
France	709,802
More...	

Answer: United States

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

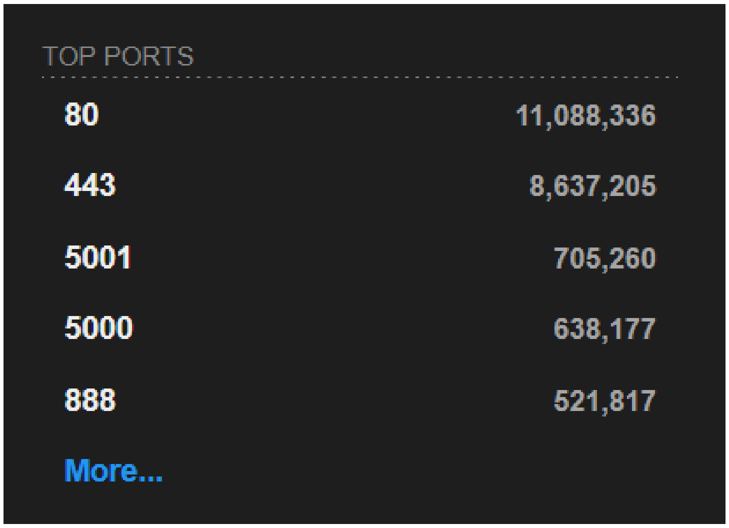


TOP PORTS

80	6,145,268
443	5,070,074
8080	341,460
5006	162,526
8081	149,201
More...	

Answer: 8080

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



TOP PORTS

80	11,088,336
443	8,637,205
5001	705,260
5000	638,177
888	521,817

More...

Answer: 5001

****

Summary

In this room, we focused on passive reconnaissance. In particular, we covered command-line tools, whois, nslookup, and dig. We also discussed two publicly available services DNSDumpster and Shodan.io. The power of such tools is that you can collect information about your targets without directly connecting to them. Moreover, the trove of information you may find using such tools can be massive once you master the search options and get used to reading the results

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*