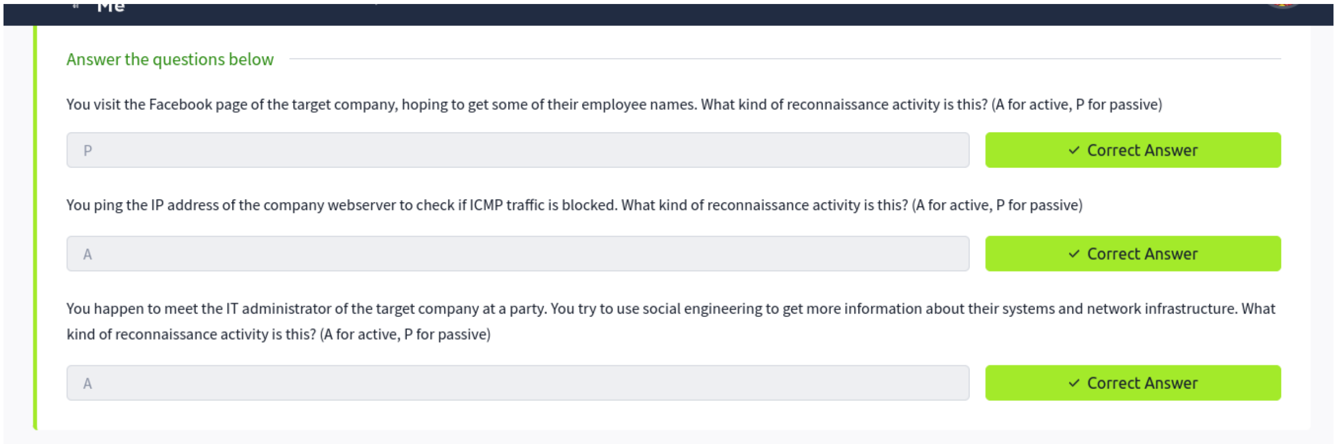
ISSACK WAITHAKA
cs-sa07-24085

Passive Versus Active Recon

- Reconnaissance is gathering information about a target.
- Passive reconnaissance rely on information that is publicly available
- Active reconnaissance requires direct engagement with the target

Questions



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)

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)

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)

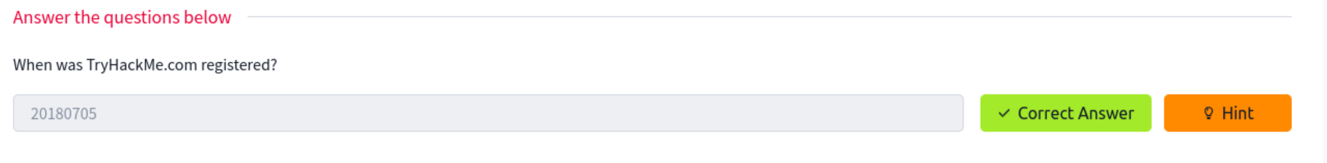
A

Whois

- Listens on port 43 for incoming requests
- Replies with various information related to the domain requested

Questions

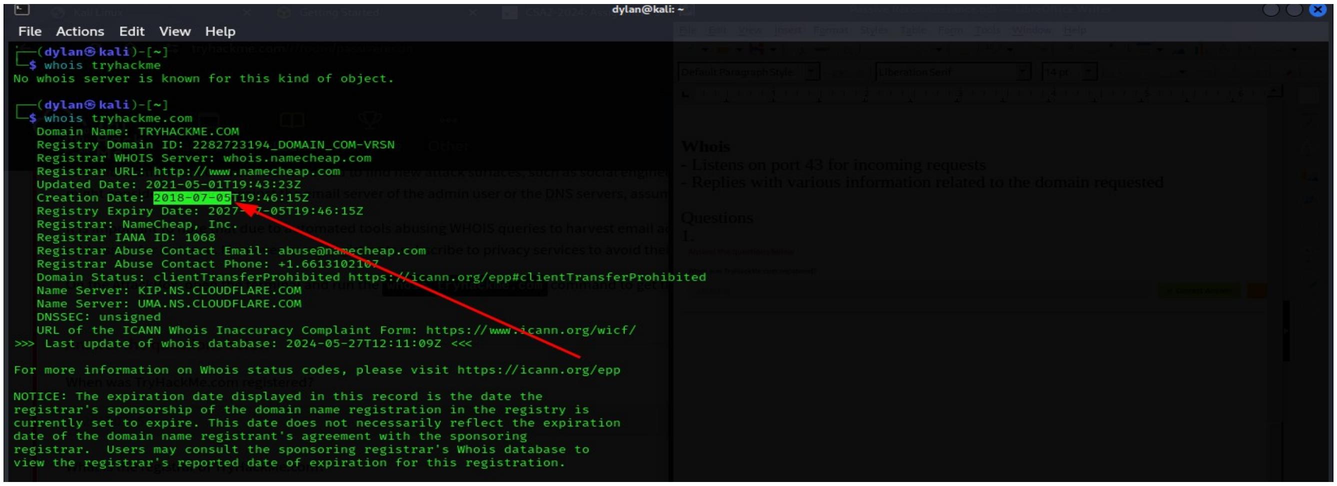
1.



Answer the questions below

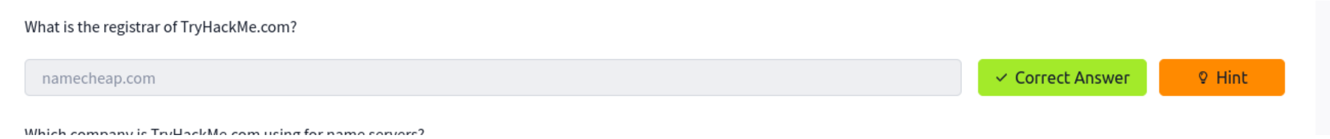
When was TryHackMe.com registered?

20180705



```
┌──(dylan㉿kali)-[~]
└─$ whois tryhackme
No whois server is known for this kind of object.

┌──(dylan㉿kali)-[~]
└─$ 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: 2021-05-01T19:43:23Z
   Creation Date: 2018-07-05T19:46:15Z
   Registry Expiry Date: 2027-07-05T19:46:15Z
   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/
>>> Last update of whois database: 2024-05-27T12:11:09Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.
```

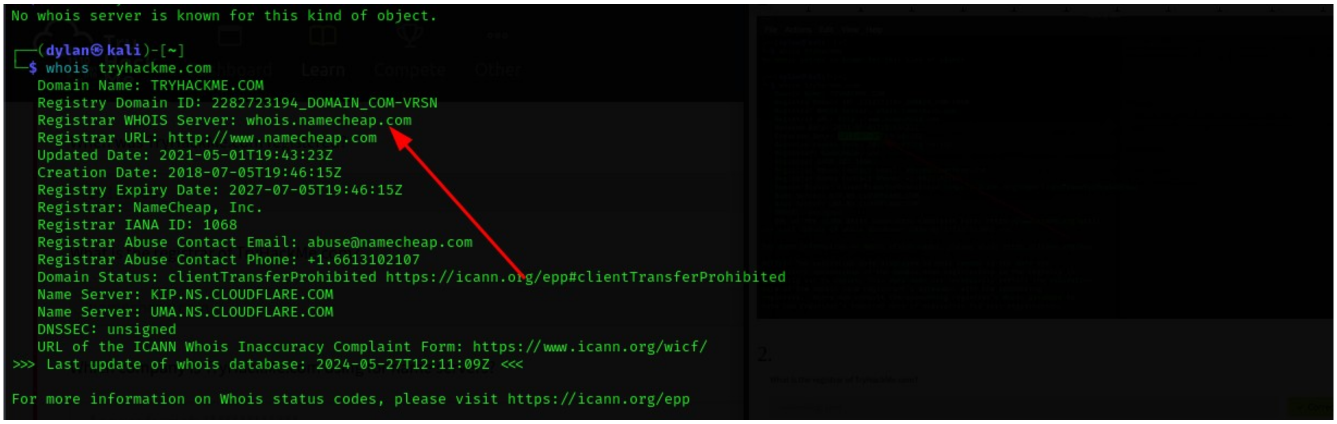
2.



What is the registrar of TryHackMe.com?

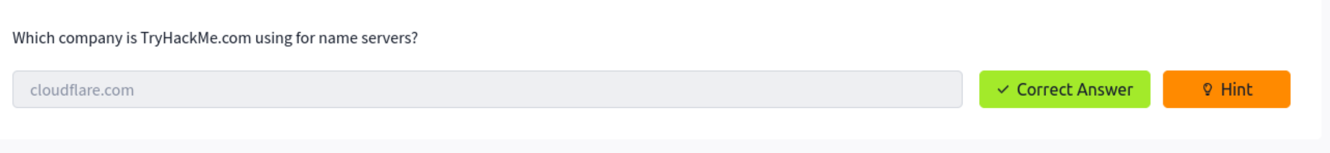
namecheap.com

Which company is TryHackMe.com using for name servers?



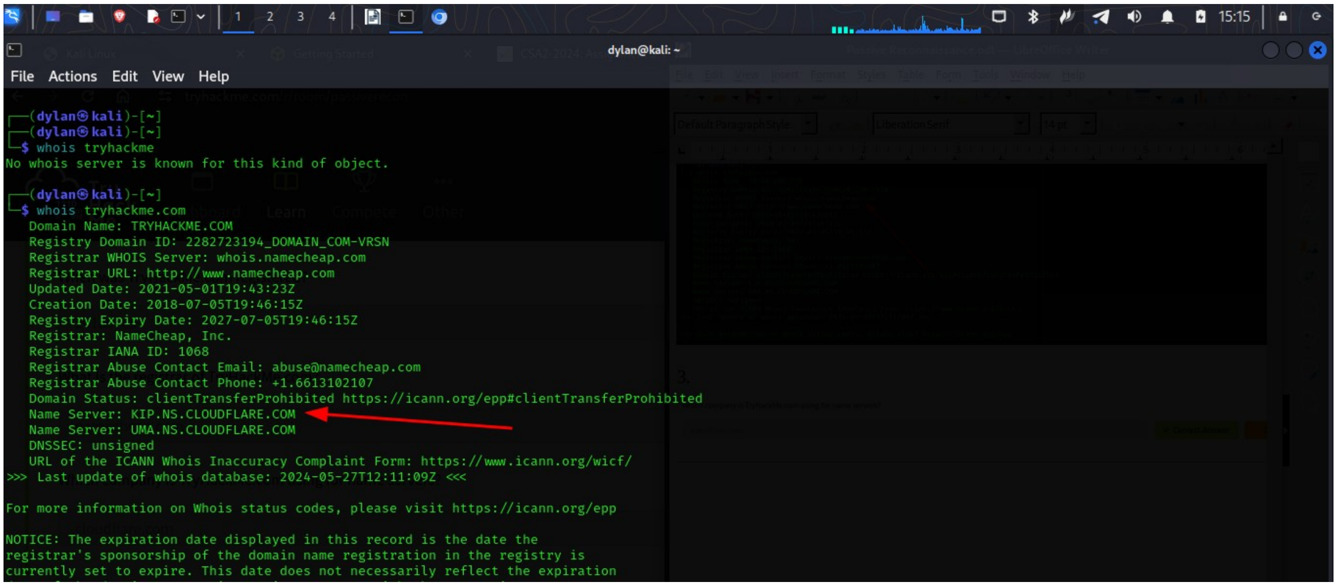
```
No whois server is known for this kind of object.

┌──(dylan㉿kali)-[~]
└─$ 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: 2021-05-01T19:43:23Z
   Creation Date: 2018-07-05T19:46:15Z
   Registry Expiry Date: 2027-07-05T19:46:15Z
   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/
>>> Last update of whois database: 2024-05-27T12:11:09Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

3.



Which company is TryHackMe.com using for name servers?

cloudflare.com



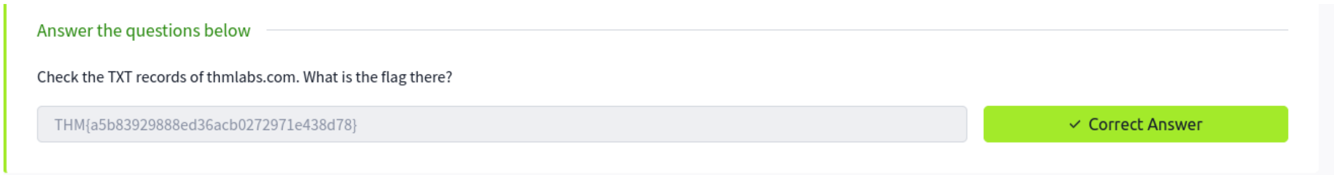
```
┌──(dylan㉿kali)-[~]
┌──(dylan㉿kali)-[~]
└─$ whois tryhackme
No whois server is known for this kind of object.

┌──(dylan㉿kali)-[~]
└─$ 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: 2021-05-01T19:43:23Z
   Creation Date: 2018-07-05T19:46:15Z
   Registry Expiry Date: 2027-07-05T19:46:15Z
   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/
>>> Last update of whois database: 2024-05-27T12:11:09Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
```

nslookup and dig

- nslookup(name server lookup) is used to find the IP address of a domain name

Questions

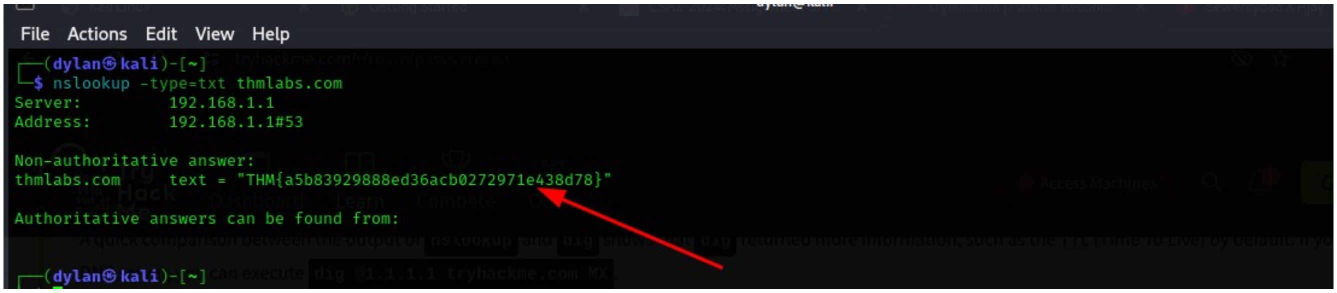
1.



Answer the questions below

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

THM{a5b83929888ed36acb0272971e438d78}



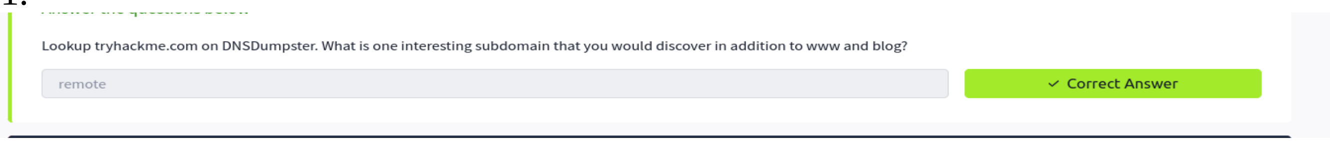
```
┌──(dylan㉿kali)-[~]
└─$ nslookup -type=txt thmlabs.com
Server:         192.168.1.1
Address:        192.168.1.1#53

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

Authoritative answers can be found from:

┌──(dylan㉿kali)-[~]
```

DNSDumpster

- It is a search engine mainly used to compile a list of publicly know subdomains
- It will also represent collected information graphically

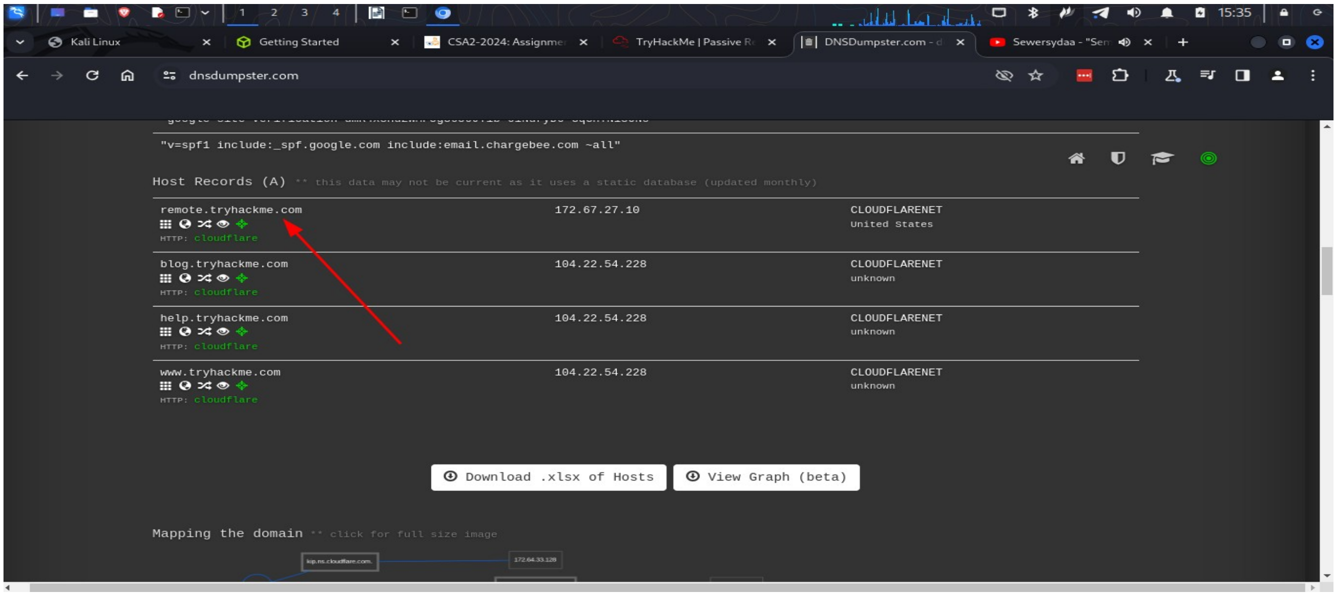
Questions

1.



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

remote



```
"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 HTTP: cloudflare	172.67.27.10	CLOUDFLARENET United States
blog.tryhackme.com HTTP: cloudflare	104.22.54.228	CLOUDFLARENET unknown
help.tryhackme.com HTTP: cloudflare	104.22.54.228	CLOUDFLARENET unknown
www.tryhackme.com HTTP: cloudflare	104.22.54.228	CLOUDFLARENET unknown

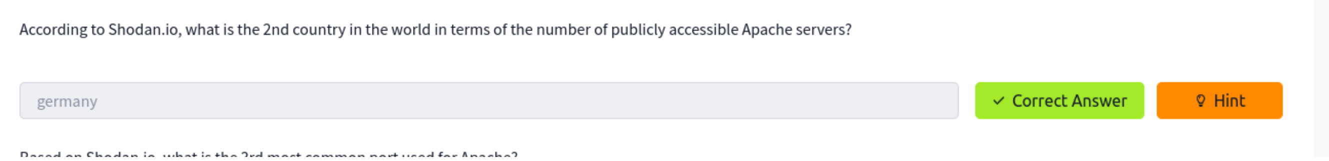
Mapping the domain ** click for full size image

Shodan.io

- Helps to learn information about a target network without actively connecting to it
- Can also learn about connected and exposed devices belonging to an organization
- It tries to connect to every device online to build a search engine of connected things.

Questions

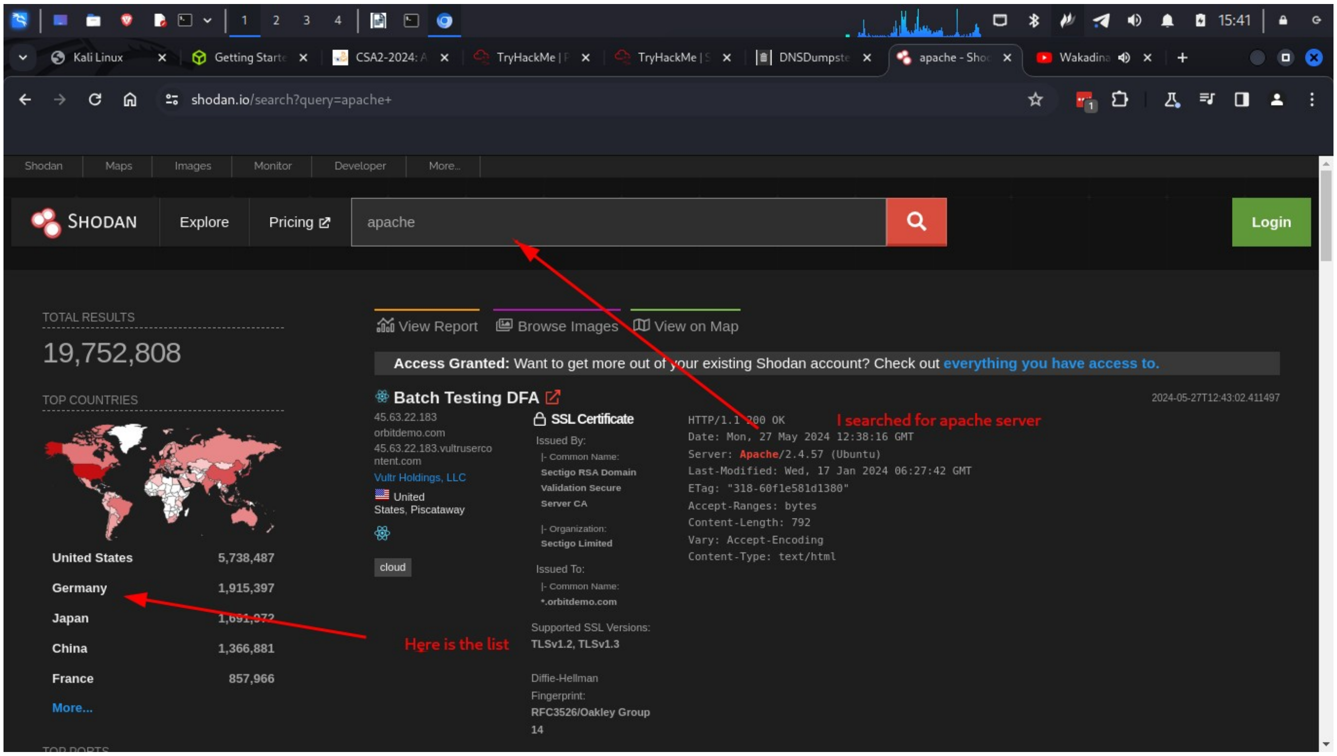
1.



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

germany

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



TOTAL RESULTS

19,752,808

TOP COUNTRIES

United States	5,738,487
Germany	1,915,397
Japan	1,691,072
China	1,366,881
France	857,966
More...	

TOP PORTS

Here is the list

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

Batch Testing DFA 2024-05-27T12:43:02.411497

45.63.22.183
orbitdemo.com
45.63.22.183.vultrusercontent.com
Vultr Holdings, LLC
United States, Piscataway

cloud

SSL Certificate

Issued By:
|- Common Name:
Sectigo RSA Domain Validation Secure Server CA

|- Organization:
Sectigo Limited

Issued To:
|- Common Name:
***.orbitdemo.com**

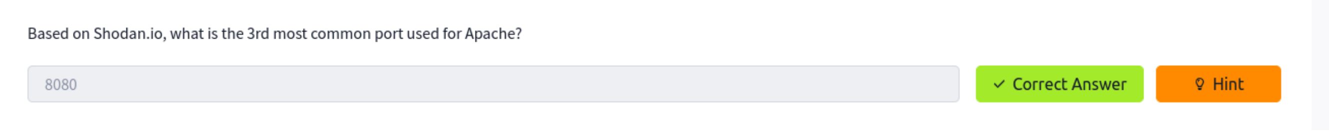
Supported SSL Versions:
TLSv1.2, TLSv1.3

Diffie-Hellman Fingerprint:
RFC3526/Oakley Group 14

```
HTTP/1.1 200 OK
Date: Mon, 27 May 2024 12:38:16 GMT
Server: Apache/2.4.57 (Ubuntu)
Last-Modified: Wed, 17 Jan 2024 06:27:42 GMT
ETag: "318-60f1e581d1380"
Accept-Ranges: bytes
Content-Length: 792
Vary: Accept-Encoding
Content-Type: text/html
```

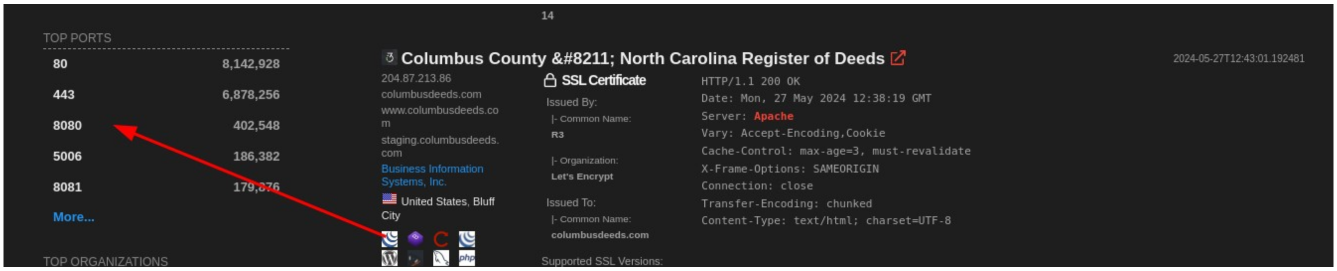
I searched for apache server

2.



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

8080



14

TOP PORTS

80	8,142,928
443	6,878,256
8080	402,548
5006	186,382
8081	179,876
More...	

TOP ORGANIZATIONS

Columbus County &#8211; North Carolina Register of Deeds 2024-05-27T12:43:01.192481

204.87.213.86
columbusdeeds.com
www.columbusdeeds.com
staging.columbusdeeds.com
Business Information Systems, Inc.
United States, Bluff City

SSL Certificate

Issued By:
|- Common Name:
R3

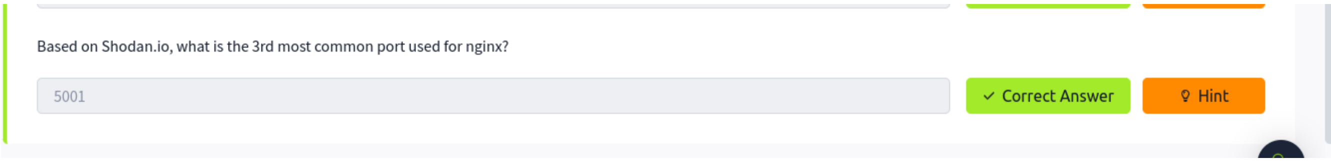
|- Organization:
Let's Encrypt

Issued To:
|- Common Name:
columbusdeeds.com

Supported SSL Versions:

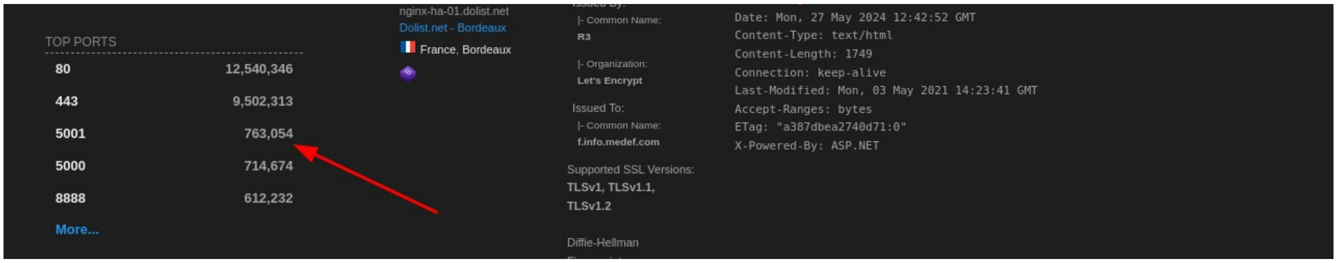
```
HTTP/1.1 200 OK
Date: Mon, 27 May 2024 12:38:19 GMT
Server: Apache
Vary: Accept-Encoding,Cookie
Cache-Control: max-age=3, must-revalidate
X-Frame-Options: SAMEORIGIN
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

3.



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

5001



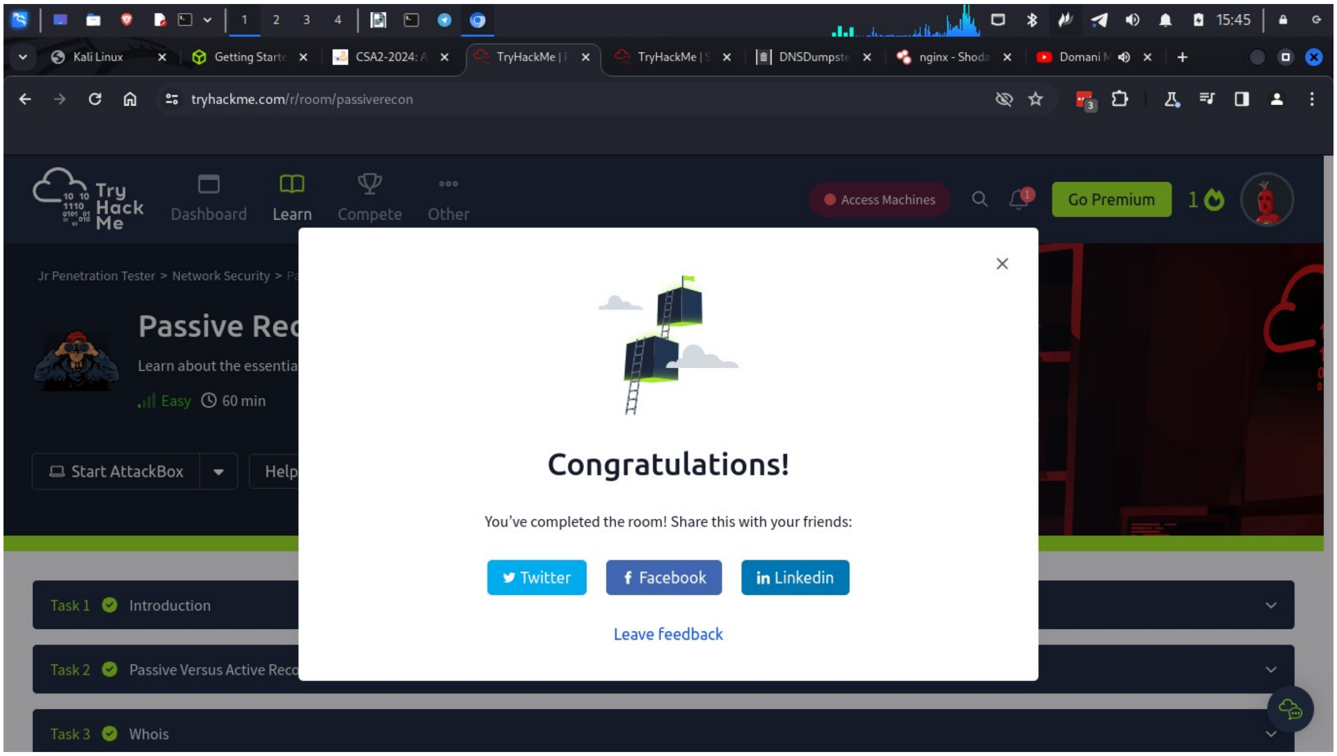
TOP PORTS	
80	12,540,346
443	9,502,313
5001	763,054
5000	714,674
8888	612,232

More...

nginx-ha-01.dolist.net
Dolist.net - Bordeaux
France, Bordeaux

```
|- Common Name:
R3
|- Organization:
Let's Encrypt
Issued To:
|- Common Name:
f.info.medef.com
Supported SSL Versions:
TLSv1, TLSv1.1,
TLSv1.2
Diffie-Hellman
```

```
Date: Mon, 27 May 2024 12:42:52 GMT
Content-Type: text/html
Content-Length: 1749
Connection: keep-alive
Last-Modified: Mon, 03 May 2021 14:23:41 GMT
Accept-Ranges: bytes
ETag: "a387dbea2740d71:0"
X-Powered-By: ASP.NET
```



Congratulations!

You've completed the room! Share this with your friends:

Conclusion

- In this room I was able to through some of the tools that make it possible to access information that is publicly available(passive reconnaissance). The tools include whois, nslookup and dig. I also learnt about shodan.io and DNSDumpster which helps in collection of information.