LinkedIn: kelvin kimotho

PASSIVE RECONNAISSANCE MODULE ON TYHACKME

This is my shareable link. https://tryhackme.com/p/Mr.kevin

Introduction

Reconnaissance or recon involves us gathering information related to our target system.

- This might be publicly available information which we can get by using various tools.
- Reconnaissance is the first step for us to gain an initial foothold on a system.

We have two types of reconnaissance namely,

Passive reconnaissance is where we target publicly available knowledge or information about our target. It is the information we can gain access to without directly engaging with the target.

We can get the publicly available information by,

- Looking up DNS records of a domain or our target from a public DNS server.
- Checking job ads related to the target website.
- Or even by reading news articles about the target company.

For Active **reconnaissance** we need direct engagement with the target. Like, we can scan the target maybe for open ports and see services running.

The following is how we can gain information about our target through active Recon.

- 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.

Question: 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)

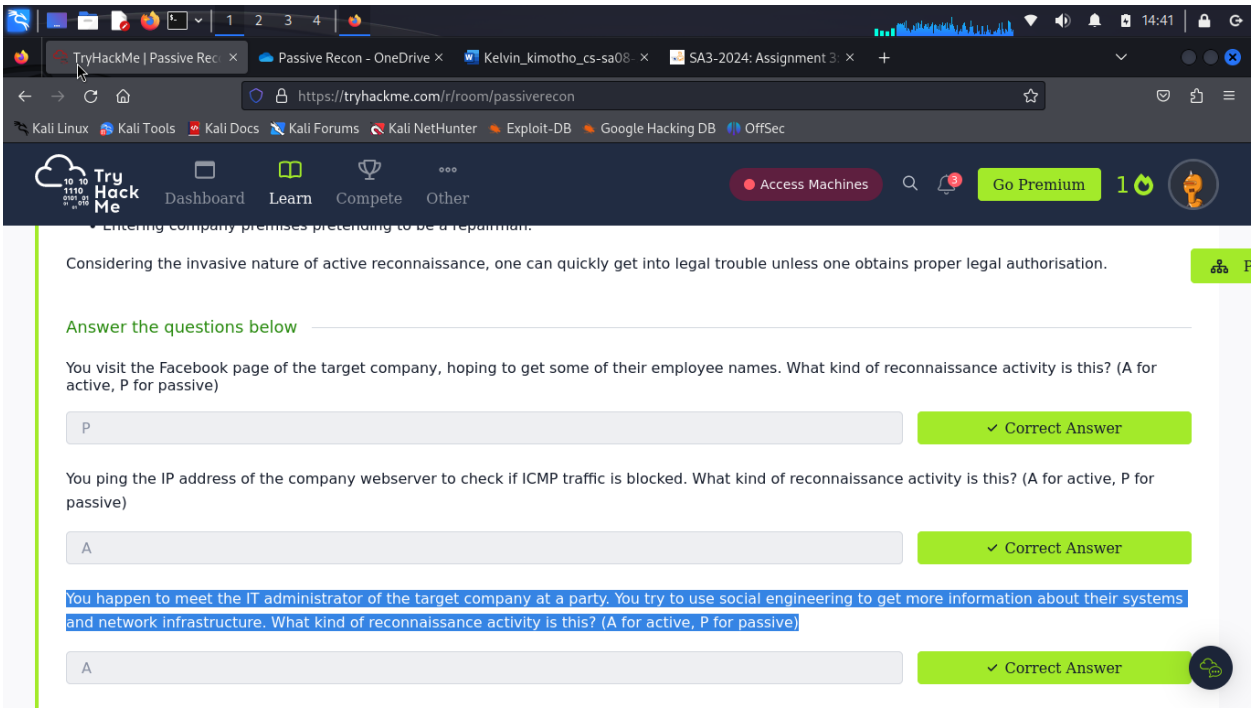
Answer: passive Recon

Question: 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: Active Recon

Question: 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: Active Recon



Whois

- It is a request and response protocol.
- 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.

we can use a **whois** client or an online service to get information about our target domain.

Information we are likely to get include,

- Registrar. This is the registrar which was used to register the domain.
- Contact info of registrant including, Name, organization, address, phone, among other things.
- Creation, update, and expiration dates. That is when was the domain name first registered? When was it last updated? And when does it need to be renewed?
- Name Server. This tells us which server to ask to resolve the domain name.

The syntax for using whois client on our terminal is “ whois domain_name”.

Question: When was TryHackMe.com registered? (creation date)

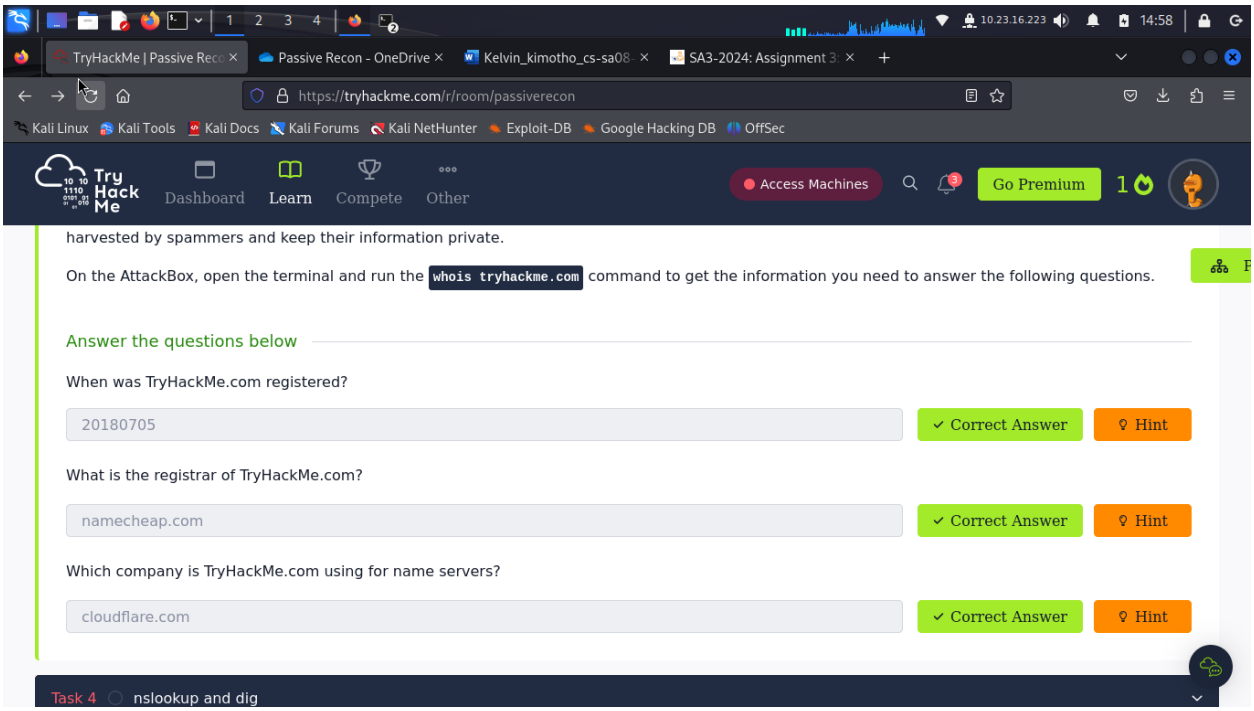
Answer: 2018-07-05

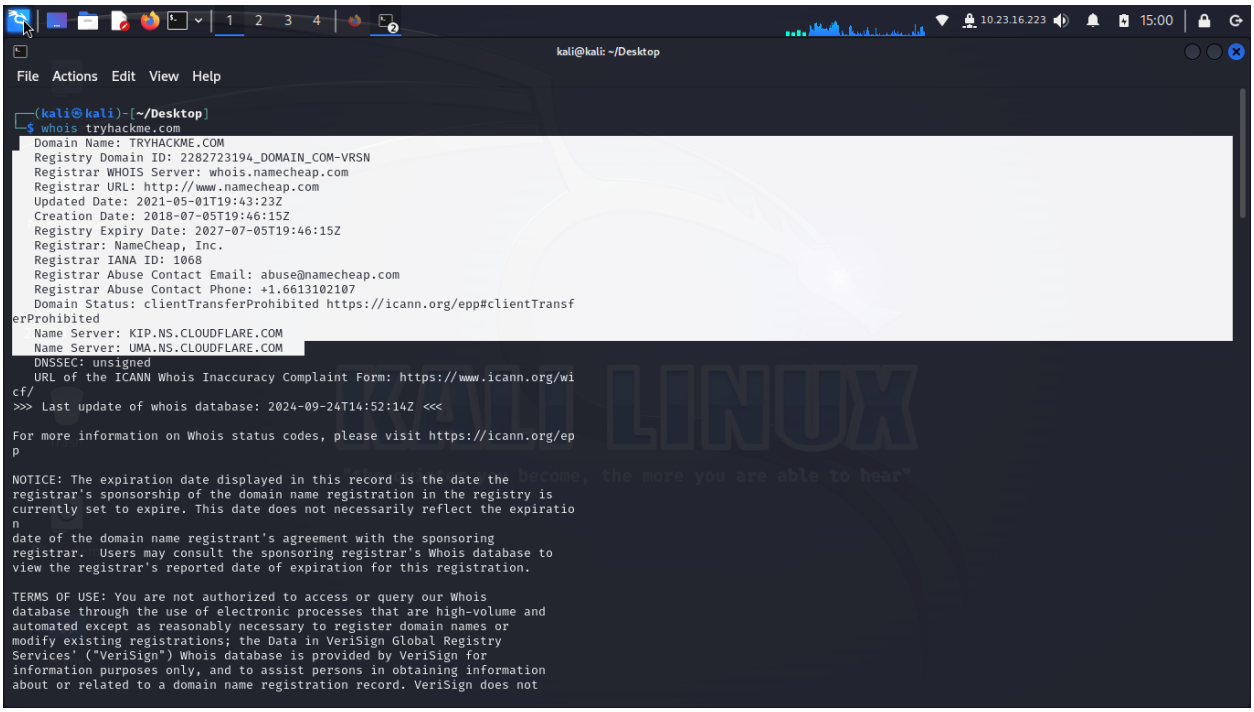
Question: What is the registrar of TryHackMe.com?

Answer: namecheap.com

Question: Which company is TryHackMe.com using for name servers?

Answer: CLOUDFLARE.COM





nslookup and dig

- We can find the IP address of a domain name using **nslookup tool.**
- Nslookup stands for Name Server Look Up.

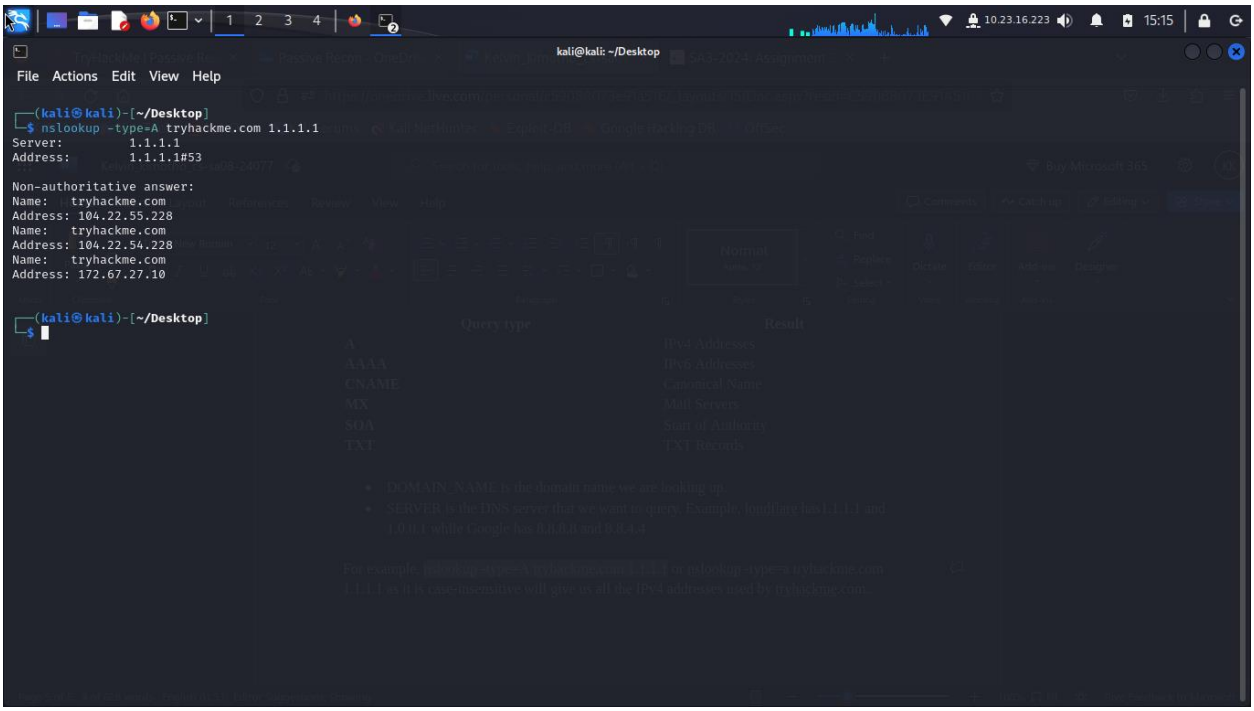
The command syntax is **nslookup DOMAIN_NAME.** We can use n**slookup OPTIONS DOMAIN_NAME SERVER where**.

- OPTIONS contains the query type. For instance, you can use A for IPv4 addresses and AAAA for IPv6 addresses.

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

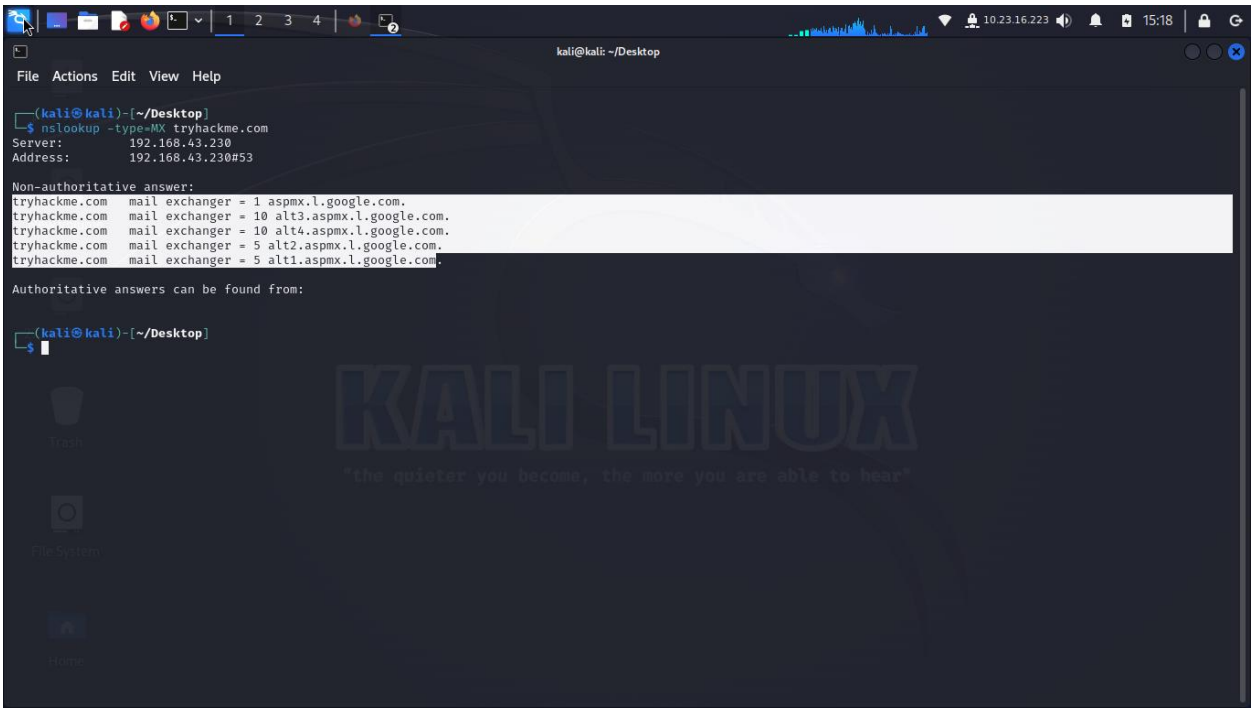
- DOMAIN_NAME is the domain name we are looking up.
- SERVER is the DNS server that we want to query. Example, cloudflare has1.1.1.1 and 1.0.0.1 while Google has 8.8.8.8 and 8.8.4.4

For example, nslookup -type=A tryhackme.com 1.1.1.1 or nslookup -type=a tryhackme.com 1.1.1.1 as it is case-insensitive will give us all the IPv4 addresses used by tryhackme.com.

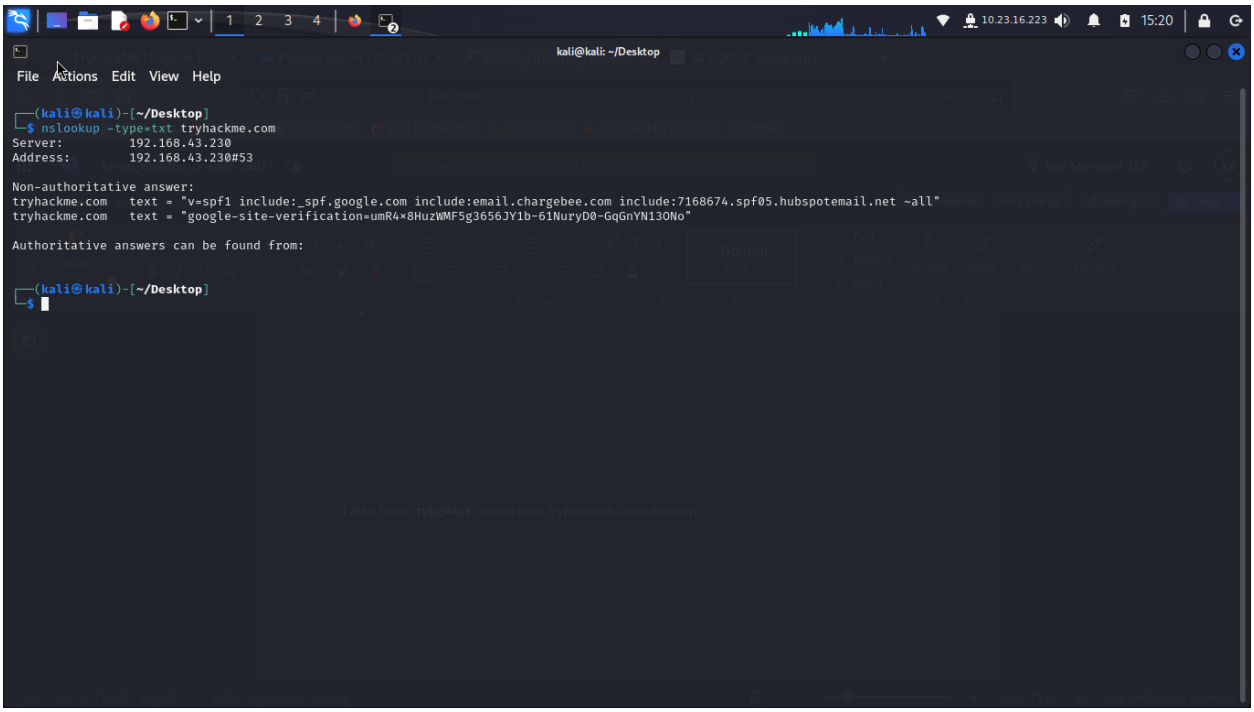


A and **AAAA** records are used to return IPv4 and IPv6 addresses, respectively.

To learn about the email servers and configurations for a particular domain. We can use the mx option type. "**nslookup -type=MX tryhackme.com"**



I also tried **-type=txt** option with tryhackme.com domain. Found some information though not sure what the information is.



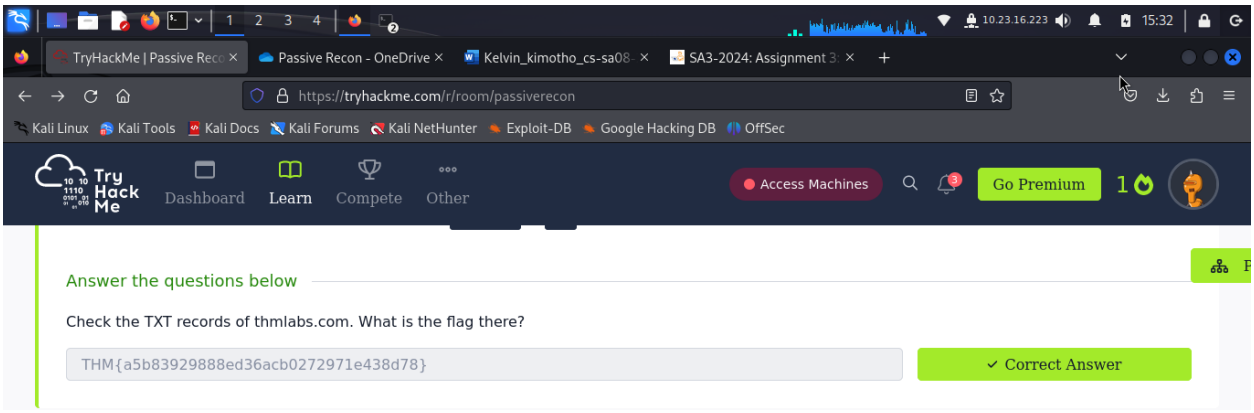
We can use **Dig (**Domain Information Groper) for more advanced DNS queries.

- The syntax to use **dig** tool is "**dig domain_name**".
- We can also use dig with the type parameter. "dig DOMAIN_NAME TYPE".
- We can also select the server we want to query using "**dig @SERVER DOMAIN_NAME TYP**E" where server is the dns server we want to query; domain name is the domain name we are gathering information about while type contains the DNS record type

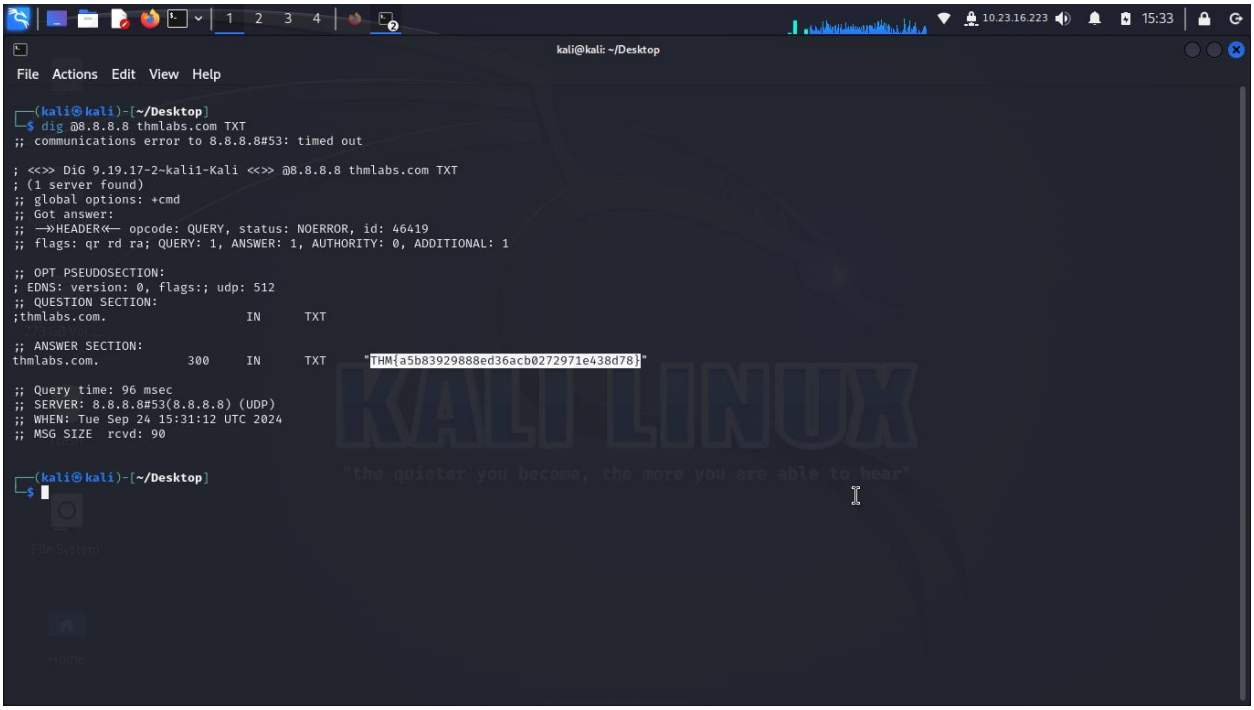
Purpose	Commandline Example
Lookup WHOIS record	`whois tryhackme.com`
Lookup DNS A records	`nslookup -type=A tryhackme.com`
Lookup DNS MX records at DNS server	`nslookup -type=MX tryhackme.com 1.1.1.1`
Lookup DNS TXT records	`nslookup -type=TXT tryhackme.com`
Lookup DNS A records	`dig tryhackme.com A`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

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

Answer: THM{a5b83929888ed36acb0272971e438d78}



I queried google dns server (8.8.8.8), I then used type TXT to gather the information.



DNSDumpster

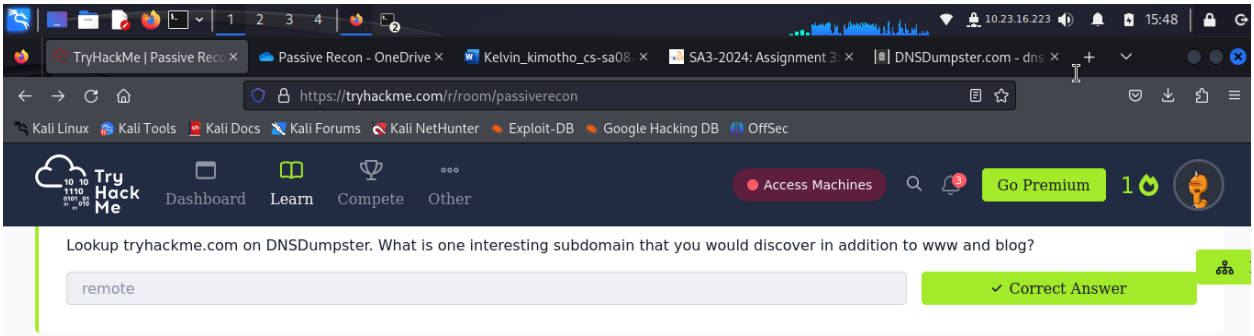
Dig and dnslookup cannot help us gain information about subdomains running on a domain.

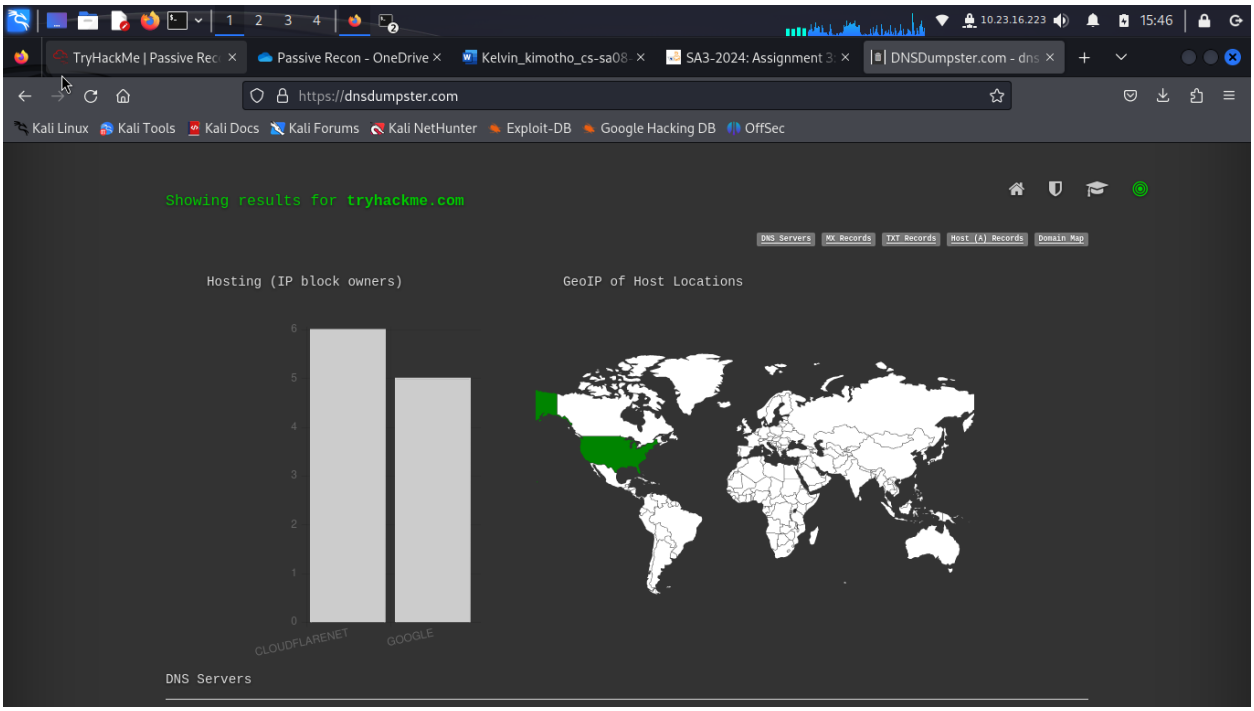
We can use **DNSDumpster**, an online service that helps find running subdomains for a given domain.

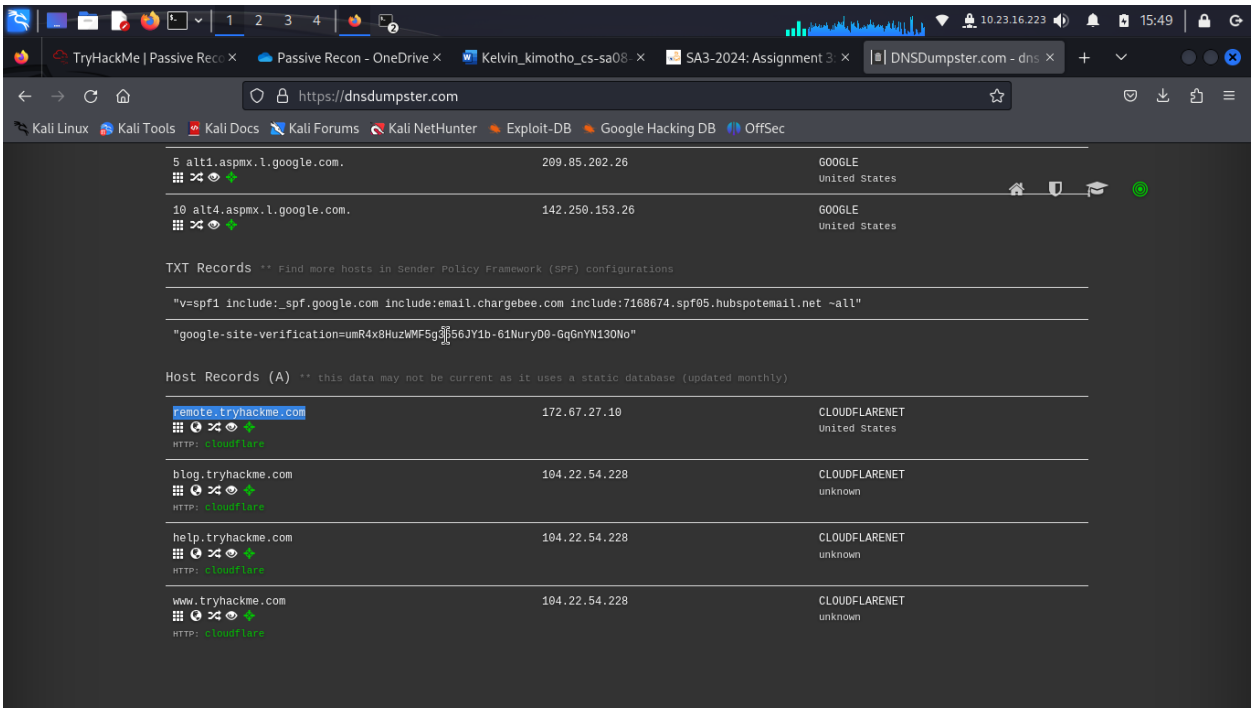
- To discover subdomains, we can brute-forcing queries to find which subdomains have DNS records but it might be time consuming and thus using DNSDumpster would save us time during our reconnaissance.
- DNSDumpster]returns the collected DNS information in easy-to-read tables and a graph.
- DNSDumpster also provides any collected information about listening servers.
- It can also resolve domain names to IP addresses and even geolocate them.
- We can also see the MX records (mail exchange servers with their respective IP addresses), information about the owner and location and also TXT records.

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

Answer: remote.







Shodan.io

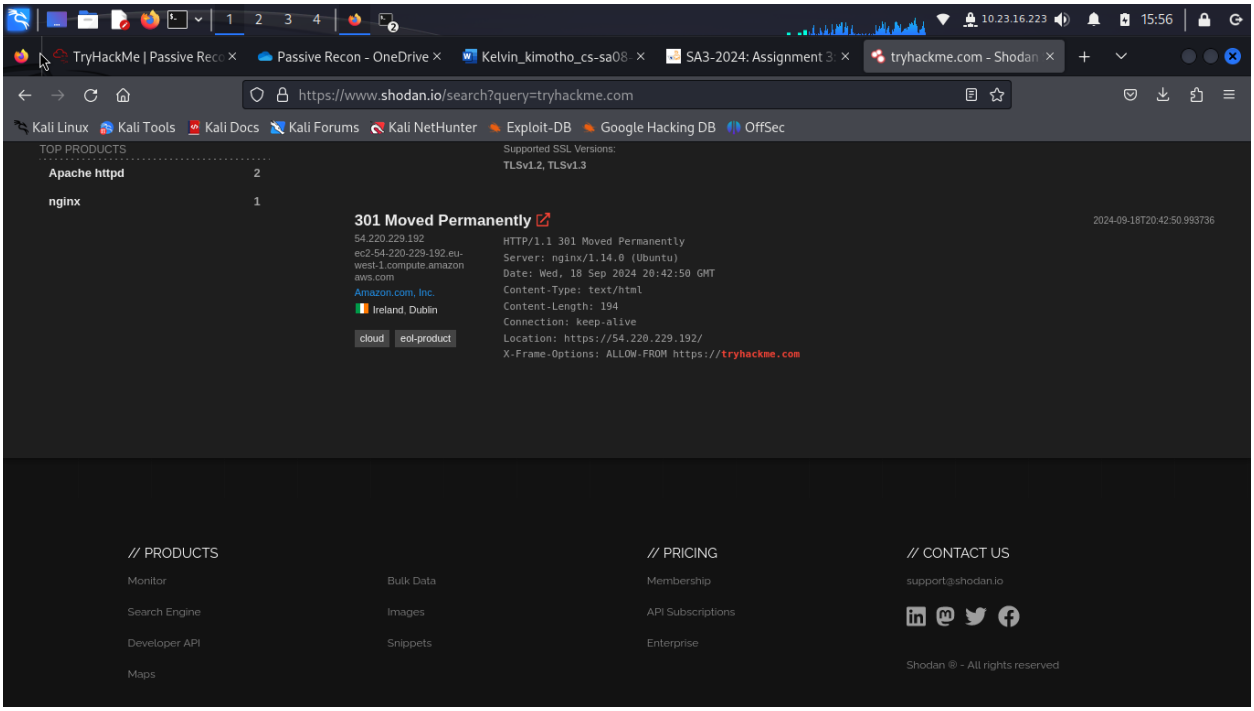
We can use a service like **Shodan.io** to discover various pieces of information about the target network without actively connecting to it as a penetration tester.

- We can also use different services from Shodan.io to learn about connected and exposed devices belonging to your organization as blue Teamers in that organization.
- Shodan.io will connect to every device reachable online to build a search engine of connected devices.
- It collects all the information related to the service and saves it in the database to make it searchable.

we can discover several things related to a search about our target such as:

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

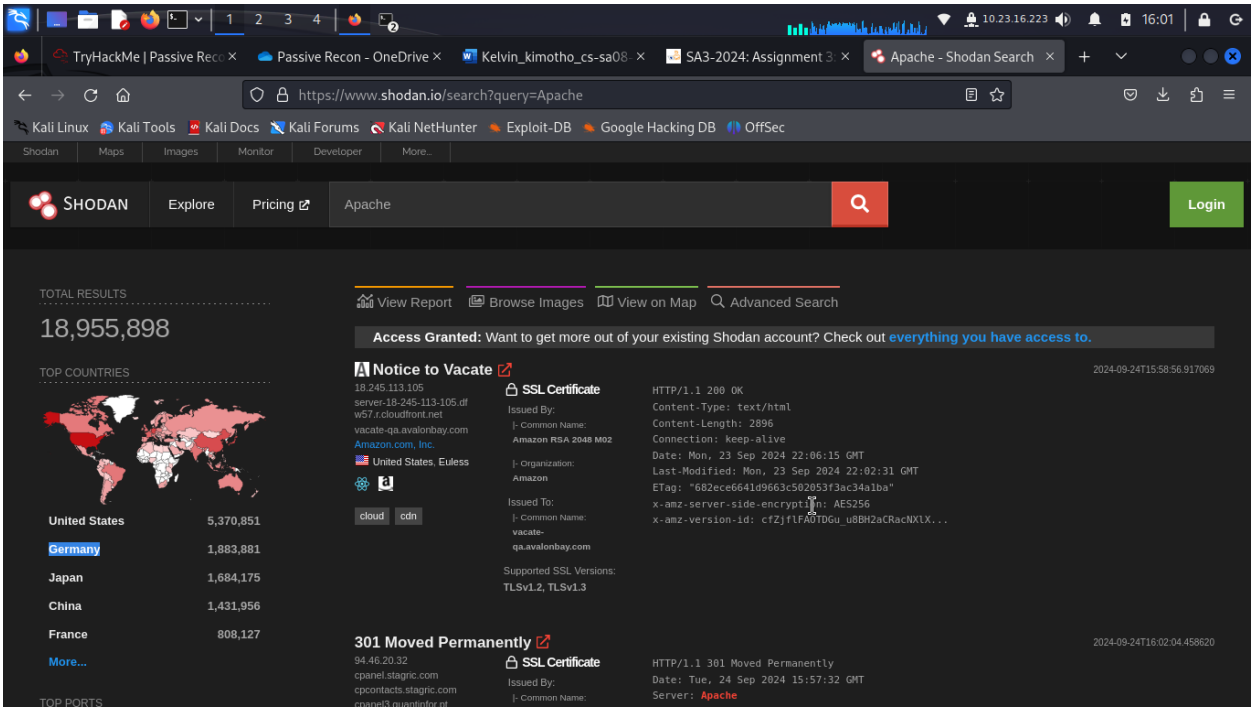
I tried searching tryhackme on shodan.io, the following were the results.



Information found included the server where it was running." Server: nginx/1.14.0 (Ubuntu)". And that it was moved lately.

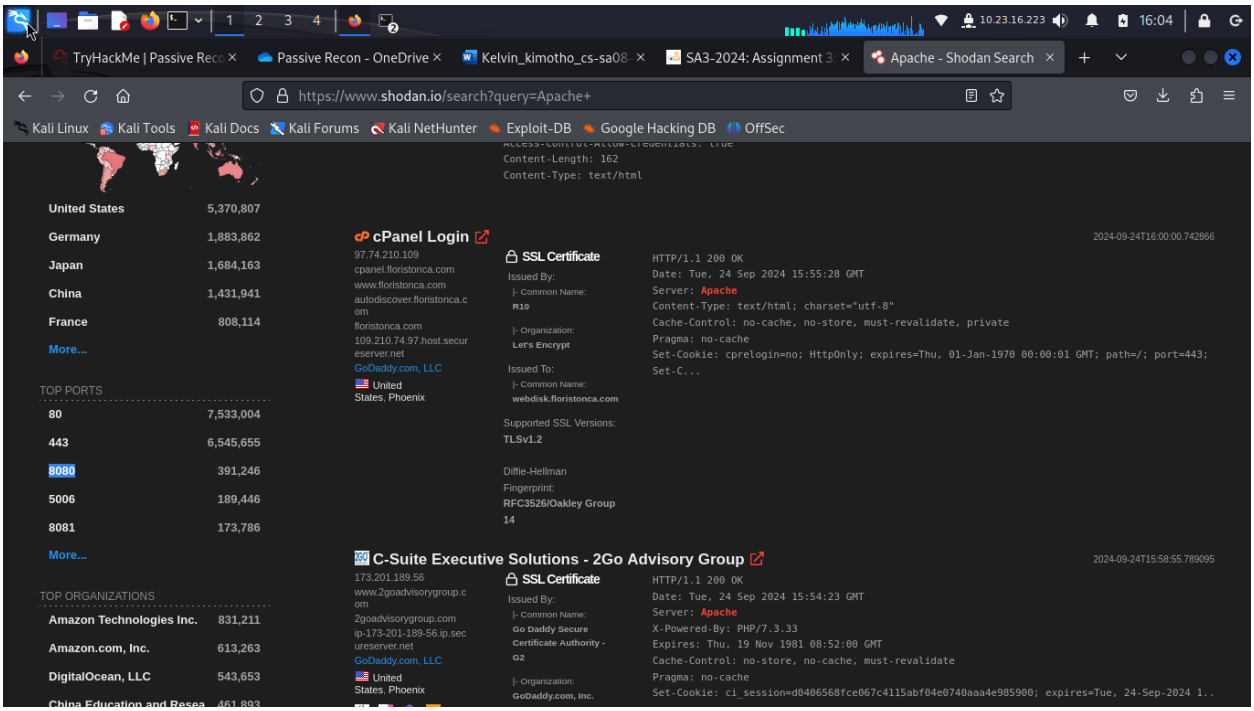
Question: According to Shodan.io, what is the 2nd country in the world in terms of the number of publicly accessible Apache servers?

Answer: Germany



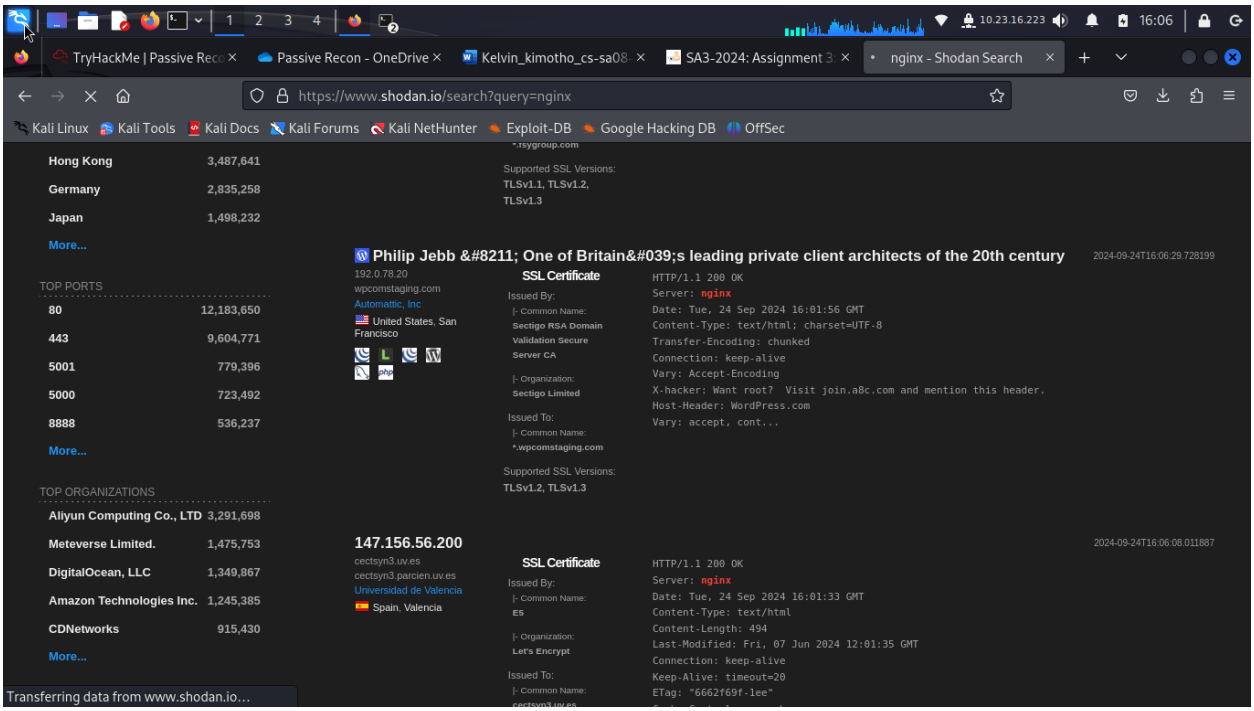
Question: Based on Shodan.io, what is the 3rd most common port used for Apache?

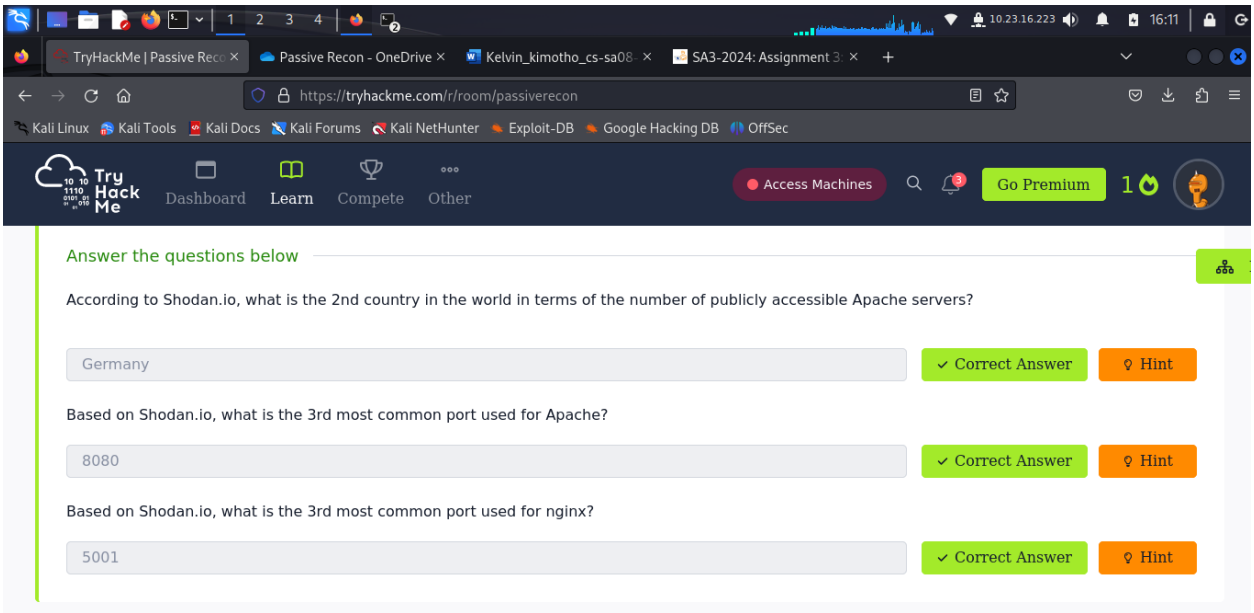
Answer: 8080

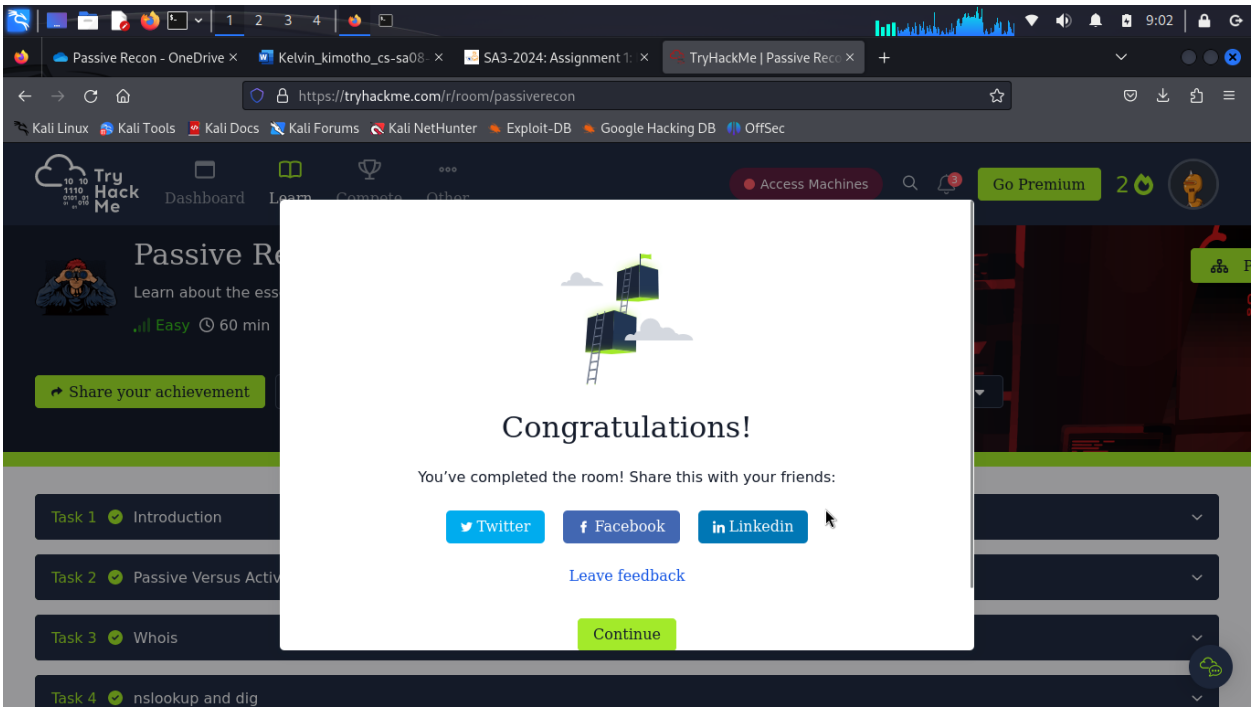


Question: Based on Shodan.io, what is the 3rd most common port used for nginx?

Answer: 5001


TryHackMe | Passive Reco
Passive Recon - OneDrive
Kelvin_kimotho_cs-sa08
SA3-2024: Assignment 3
nginx - Shodan Search
https://www.shodan.io/search?query=nginx
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Hong Kong 3,487,641
Germany 2,835,258
Japan 1,498,232
More...
TOP PORTS
80 12,183,650
443 9,604,771
5001 779,396
5000 723,492
8888 536,237
More...
TOP ORGANIZATIONS
Aliyun Computing Co., LTD 3,291,698
Meteverse Limited. 1,475,753
DigitalOcean, LLC 1,349,867
Amazon Technologies Inc. 1,245,385
CDNetworks 915,430
More...
Supported SSL Versions:
TLSv1.1, TLSv1.2, TLSv1.3
Philip Jebb – One of Britain's leading private client architects of the 20th century
2024-09-24T16:06:29.728199
192.0.78.20
wpcomstaging.com
Automattic, Inc
United States, San Francisco
SSL Certificate
Issued By:
Common Name: Sectigo RSA Domain Validation Secure Server CA
Organization: Sectigo Limited
Issued To:
Common Name: *.wpcomstaging.com
Supported SSL Versions:
TLSv1.2, TLSv1.3
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 24 Sep 2024 16:01:56 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-hacker: Want root? Visit join.a8c.com and mention this header.
Host-Header: WordPress.com
Vary: accept, cont...
147.156.56.200
2024-09-24T16:06:08.011887
cectsyn3.uv.es
cectsyn3.parcien.uv.es
Universidad de Valencia
Spain, Valencia
SSL Certificate
Issued By:
Common Name: ES
Organization: Let's Encrypt
Issued To:
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 24 Sep 2024 16:01:33 GMT
Content-Type: text/html
Content-Length: 494
Last-Modified: Fri, 07 Jun 2024 12:01:35 GMT
Connection: keep-alive
Keep-Alive: timeout=20
ETag: "6662f69f-1ee"
Transferring data from www.shodan.io...


TryHackMe | Passive Reco
Passive Recon - OneDrive
Kelvin_kimotho_cs-sa08
SA3-2024: Assignment 3
https://tryhackme.com/r/room/passiverecon
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Dashboard
Learn
Compete
Other
Access Machines
Go Premium
Answer the questions below
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
Hint
Based on Shodan.io, what is the 3rd most common port used for Apache?
8080
Correct Answer
Hint
Based on Shodan.io, what is the 3rd most common port used for nginx?
5001
Correct Answer
Hint



Conclusion

By completing thing room, I can use different tools to gather information about my target. I can now use command-line tools such as, whois, nslookup, and dig to gather very useful information about my target domain. The good thing with this tool is that i don't have to interact with my target directly and this can help me do reconnaissance without being detected. I also familiarized myself with online services like Shodan and DNSdumpster. Dumpster helps me discover subdomains associated with my target domain.