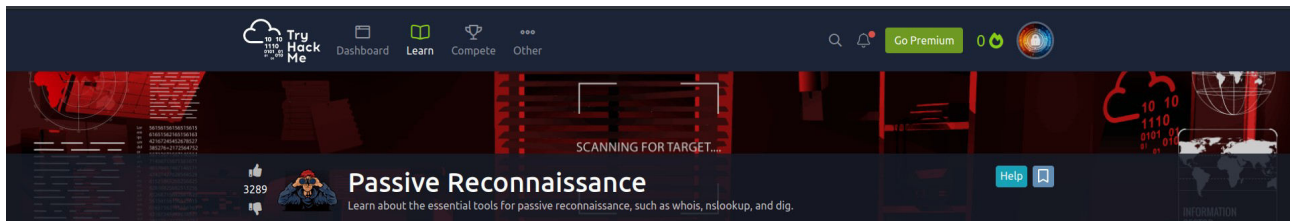




**Eric Mwenda**

**Passive Recon**

<https://tryhackme.com/p/Ericm>



## **Introduction.**

In this room we majored on Passive Reconnaissance which involves using publicly available knowledge or information to learn more about a target in other words as I learnt on the previous assignment it involves using available resources without directly engaging with the target

In this room covered three command-line tools which are:-

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

Other online tools that we took a look into were:-

- **DNSDumpster**
- **Shodan.io**

This online tools allow us to collect information about our target without directly connecting to it.

## **Passive Versus Active Recon**

In this section we started with a quote from Sun Tzu taught, in the Art of War which states:- “If you know the enemy and know yourself, your victory will not stand in doubt.”

In other words if you are planning to attack you have to gather information about your target systems.

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

1. Passive Reconnaissance
2. Active Reconnaissance.

**Passive Reconnaissance** – involves the rely on publicly available materials to gather information/knowledge about the target system without directly interacting with the target.

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** – This kind of reconnaissance cannot be achieved without directly interacting with the target.

Some examples of active reconnaissance activities may 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.

### **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? **Passive Reconnaissance**

You ping the IP address of the company webserver to check if ICMP traffic is blocked. What kind of reconnaissance activity is this? **Active Reconnaissance**

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? **Active Reconnaissance**

### **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

Correct Answer

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

Correct Answer

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

Correct Answer

## Whois

In this section we looked into WHOIS which 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 a lot of information all at once, some of this information include:-

- 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?
- 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)

Command used is:- **whois <target DN>**

Example:-

```
(coderic@kali)-[~]
$ whois amazon.com
Domain Name: AMAZON.COM
Registry Domain ID: 281209_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2023-05-16T19:03:14Z
Creation Date: 1994-11-01T05:00:00Z
Registry Expiry Date: 2024-10-31T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.AMZNDNS.CO.UK
Name Server: NS1.AMZNDNS.COM
Name Server: NS1.AMZNDNS.NET
```

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.

## Answer the questions below

When was TryHackMe.com registered? **ANS: 2018-07-05**

```
Creation Date: 2018-07-05T19:46:15.00Z
Registrar Registration Expiration Date: 2027-07-05T19:46:15.00Z
```

What is the registrar of TryHackMe.com? **ANS: namecheap.com**

```
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
```

Which company is TryHackMe.com using for name servers? **ANS: CLOUDFLARE.COM**

```
Name Server: KIP.NS.CLOUDFLARE.COM
Name Server: UMA.NS.CLOUDFLARE.COM
```

*Answer the questions below*

When was TryHackMe.com registered?

20180705

Correct Answer

Hint

What is the registrar of TryHackMe.com?

namecheap.com

Correct Answer

Hint

Which company is TryHackMe.com using for name servers?

CLOUDFLARE.COM

Correct Answer

Hint

## **nslookup and dig**

nslookup stands for for Name Server Look Up.

Command used:- **nslookup DOMAIN\_NAME** or **nslookup OPTIONS DOMAIN\_NAME SERVER**.

nslookup has 3 main parameters that are used, this 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.

Other are a number of query types that one can use this are:-

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

Command used:- **nslookup -type=<query type> <DNS> <IP>**

**Example:**

```
Terminal

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
```

**Answer the questions below**

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

**ANS: THM{a5b83929888ed36acb0272971e438d78}**

```
File Actions Edit View Help

(coderic@kali)-[~]
$ nslookup -type=TXT thmlabs.com
Server:      10.0.2.3
Address:     10.0.2.3#53

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

Authoritative answers can be found from:
```

## Online Tools

### DNSDumpster.

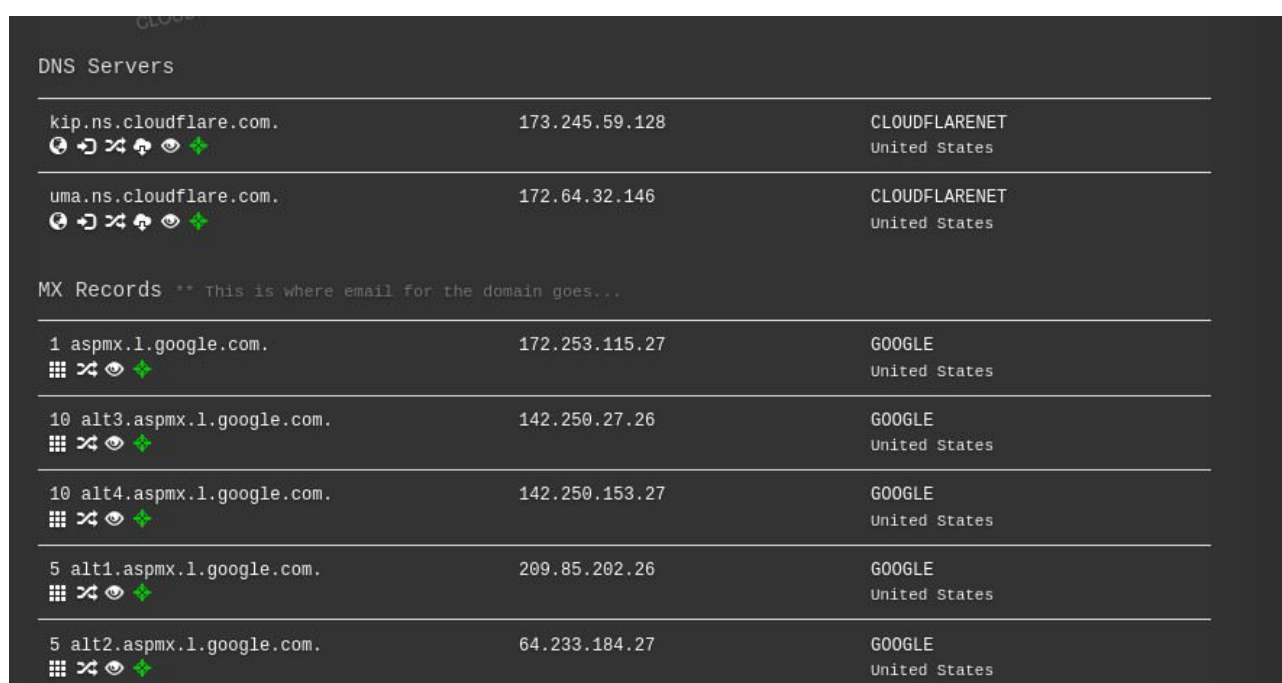
In this task, what we want to look at is on how to find those subdomains that have been set up and is not updated regularly. Lack of proper regular updates usually leads to vulnerable services.

The posed question was how can we know that such subdomains exist?











You see for one to identify such a subdomain he/she has to go through a couple of searches using different tools to find the consistent subdomain which of-course is very hard considering you have to go through a ton of information therefore to avoid this this is where **DNSDumpster** comes in.

To avoid such a time-consuming search, one can choose to use an online service that offers detailed answers to DNS queries, such as **DNSDumpster**.





















In our example we used [tryhackme.com](https://tryhackme.com) here are the results:-



The screenshot displays the output of a DNS query on a dark-themed interface. It is divided into two main sections: 'DNS Servers' and 'MX Records'. Each section contains a table of results with icons for each entry.

DNS Servers		
kip.ns.cloudflare.com.     	173.245.59.128	CLOUDFLARENET United States
uma.ns.cloudflare.com.     	172.64.32.146	CLOUDFLARENET United States

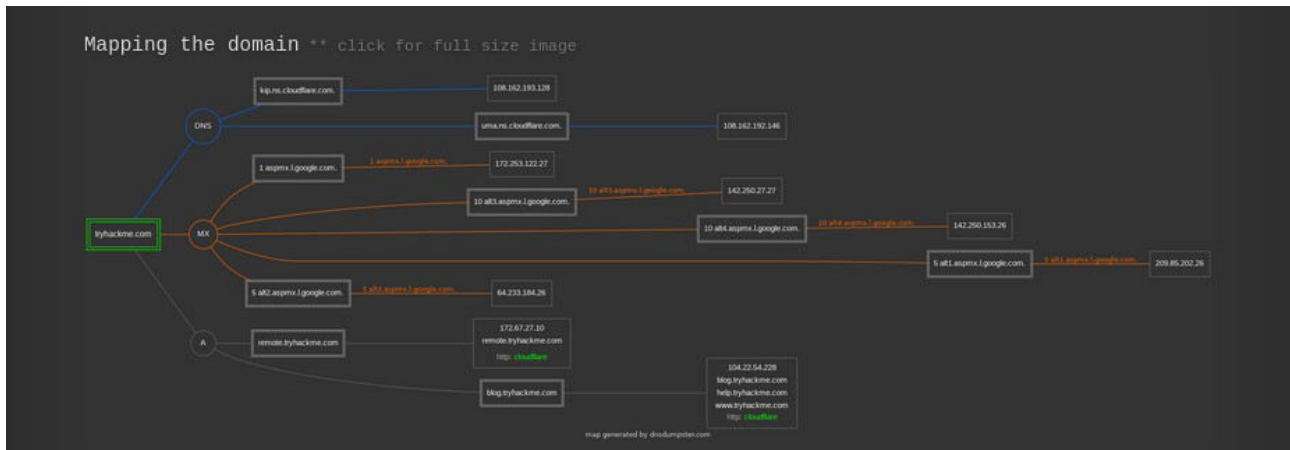
MX Records ** This is where email for the domain goes...		
1 aspmx.l.google.com.    	172.253.115.27	GOOGLE United States
10 alt3.aspmx.l.google.com.    	142.250.27.26	GOOGLE United States
10 alt4.aspmx.l.google.com.    	142.250.153.27	GOOGLE United States
5 alt1.aspmx.l.google.com.    	209.85.202.26	GOOGLE United States
5 alt2.aspmx.l.google.com.    	64.233.184.27	GOOGLE United States

From the search, a lot of information is offered all from one point

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.



DNSDumpster will also represent the information collected in a map.



TXT Records results:-

```

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"





















```

DNSDumster represents information gathered in this various ways: \_

1. Graphs
2. DNS Records
3. MX Records
4. Host Records
5. TXT Records
6. Map.

**Answer the questions below**

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

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)		
remote.tryhackme.com      HTTP: <span>cloudflare</span>	172.67.27.10	CLOUDFLARENET United States
blog.tryhackme.com      HTTP: <span>cloudflare</span>	104.22.54.228	CLOUDFLARENET unknown
help.tryhackme.com      HTTP: <span>cloudflare</span>	104.22.54.228	CLOUDFLARENET unknown
www.tryhackme.com      HTTP: <span>cloudflare</span>	104.22.54.228	CLOUDFLARENET unknown

## Shodan.io

This is also an online tool which can be used to carry out a passive reconnaissance.

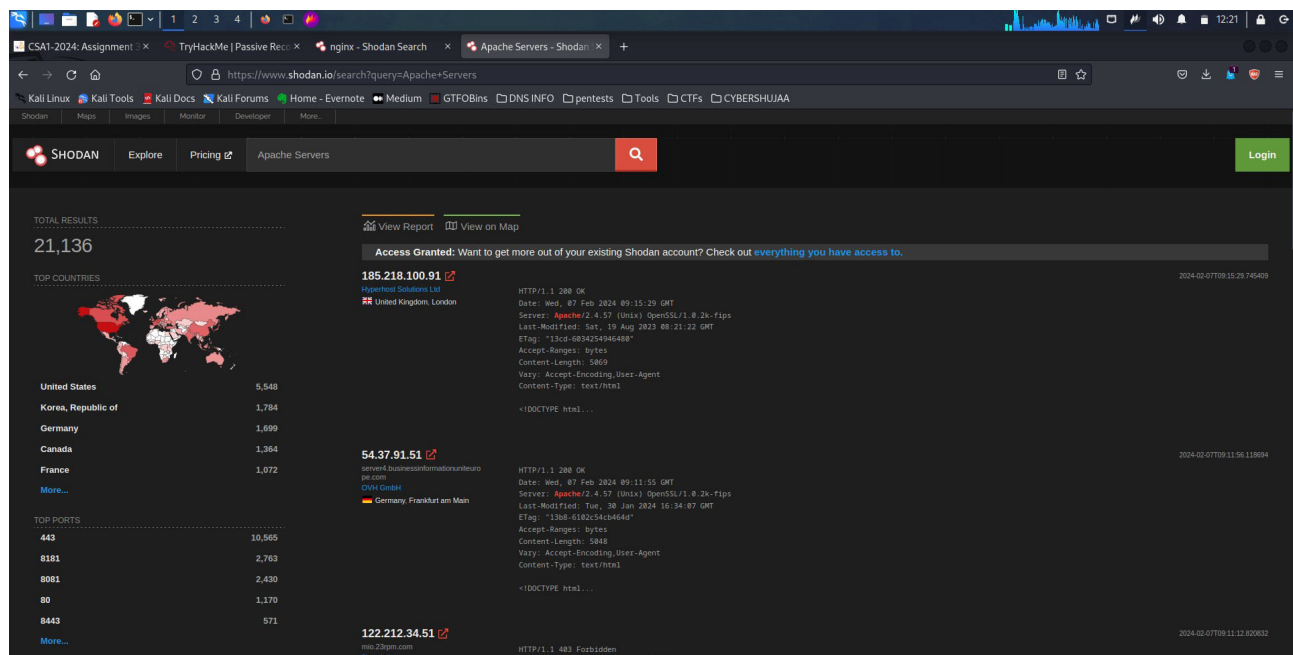
Shodan.io can be helpful to learn various pieces of information about the client's network, without actively connecting to it.

The reason why shodan is able to give the information it offers is because, 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.

### Answer the questions below

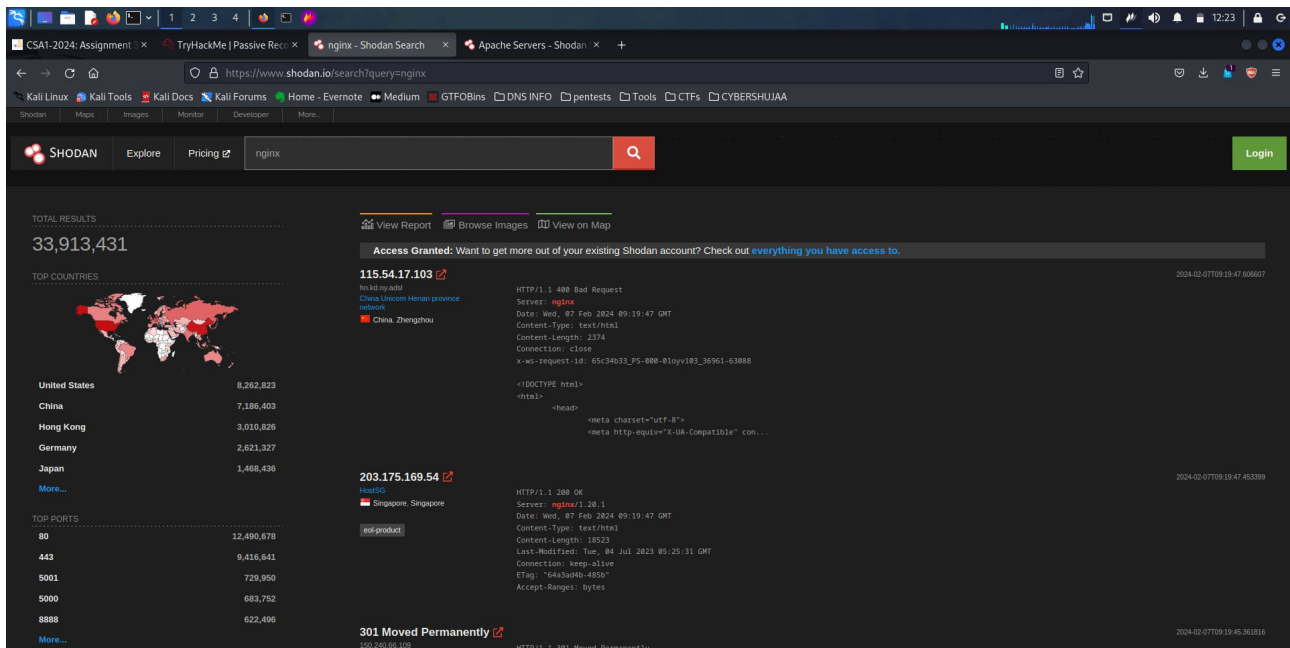
According to Shodan.io, what is the 2nd country in the world in terms of the number of publicly accessible Apache servers? **ANS: Germany**

Based on Shodan.io, what is the 3rd most common port used for Apache? **ANS: 8080**





Based on Shodan.io, what is the 3rd most common port used for nginx? ANS: 5001



## Summary

In this room we covered command-line tools which were whois, nslookup and dig. Then we looked at DNSDumpster and shodan.io as our online tools.

Here is a summarized list of how you can get the results of the following:-

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

**Conclusion.**

In conclusion, to this Room I have gained a valuable and comprehensive overview of the essential techniques and tools used in passive information gathering. By exploring the various aspects of OSINT (Open-Source Intelligence) and leveraging tools like nslookup, WHOIS, dig and online search engines such as DNS Dumpster and shodan.io my knowledge on passive recon has enlarged which I belief is useful in ethical hacking and Cybersecurity activities.

In general, Passive Reconnaissance room has offered me a good starting point to enhancing my knowledge in reconnaissance, laying up a good groundwork for more advanced penetration testing activities.

**Thank you.**