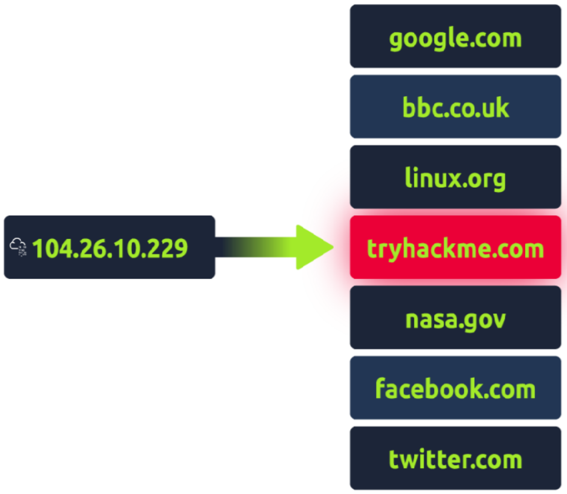
Week3: Assignment 1**:- TryHackMe: DNS In Detail**

Report by: **Aisha Khalifan, cs-cns04-23014**

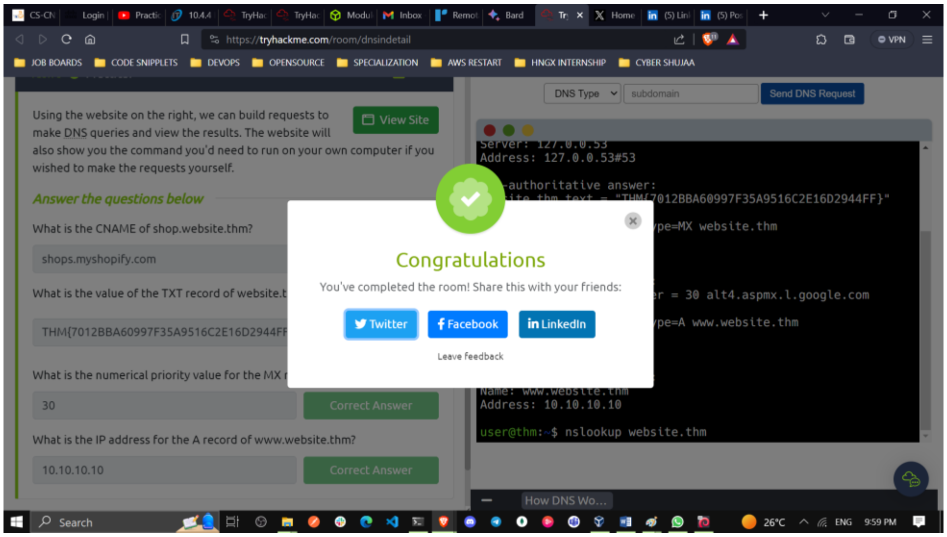
Introduction

This room walks us through an introduction to DNS (Domain Name Service). DNS is like a guide that helps us communicate with devices on the internet without needing to remember complicated numerical addresses.

Similar to how every house has a distinct address for mail, each computer on the internet has its own special address called an IP address, like 104.26.10.229, made up of four sets of numbers ranging from 0 to 255, separated by periods. Remembering these numbers can be inconvenient, especially when visiting websites. This is where DNS comes in handy. Instead of recalling long IP addresses like 104.26.10.229, we can simply remember easy-to-use names like tryhackme.com. DNS makes internet navigation much simpler.



Link: https://tryhackme.com/room/dnsindetail



Using the website on the right, we can build requests to make DNS queries and view the results. The website will also show you the command you'd need to run on your own computer if you wished to make the requests yourself.

Answer the questions below

What is the CNAME of shop.website.thm?

shops.myshopify.com

What is the value of the TXT record of website.t

THM{7012BBA60997F35A9516C2E16D2944FF

What is the numerical priority value for the MX r

30

What is the IP address for the A record of www.website.thm?

10.10.10.10

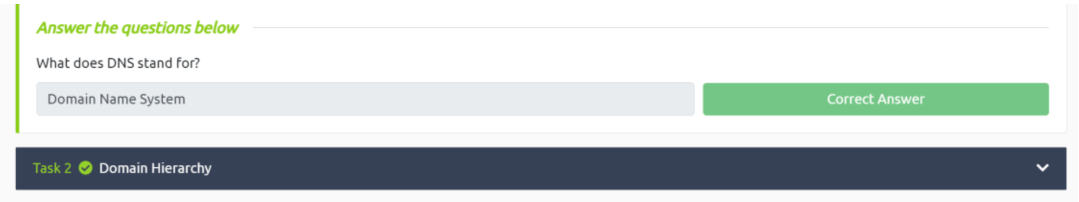
Congratulations

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

```
Server: 127.0.0.53
Address: 127.0.0.53#53

-authoritative answer:
ite.thm text = "THM{7012BBA60997F35A9516C2E16D2944FF}"

pe=MX website.thm

r = 30 alt4.aspmx.l.google.com

pe=A www.website.thm

Name: www.website.thm
Address: 10.10.10.10

user@thm:~$ nslookup website.thm
```

In this assignment, we were required to solve some five tasks and this is how our solutions looked like:

Task 1 What is DNS?

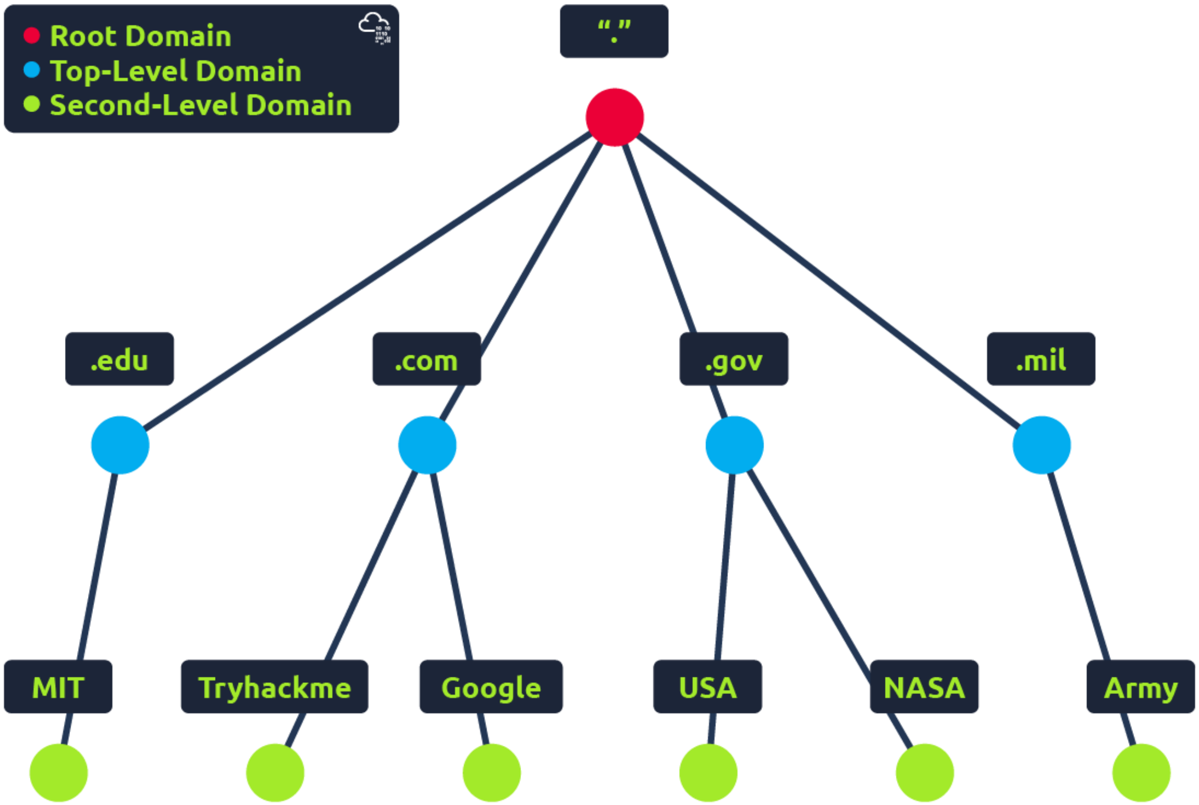


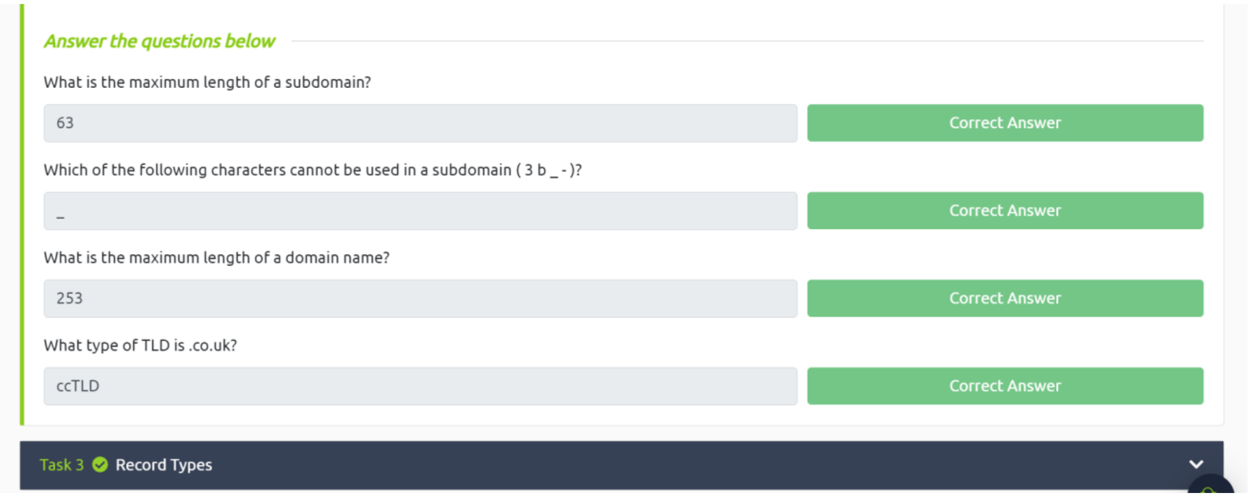
Answer the questions below

What does DNS stand for?

Domain Name System

Task 2 Domain Hierarchy





Answer the questions below

What is the maximum length of a subdomain?

63

Which of the following characters cannot be used in a subdomain (3 b _ -)?

_

What is the maximum length of a domain name?

253

What type of TLD is .co.uk?

ccTLD

Task 3 Record Types

DNS isn't just for websites though, and multiple types of DNS record exist. We'll go over some of the most common ones that you're likely to come across.

A Record

These records resolve to IPv4 addresses, for example 104.26.10.229

AAAA Record

These records resolve to IPv6 addresses, for example 2606:4700:20::681a:be5

CNAME Record

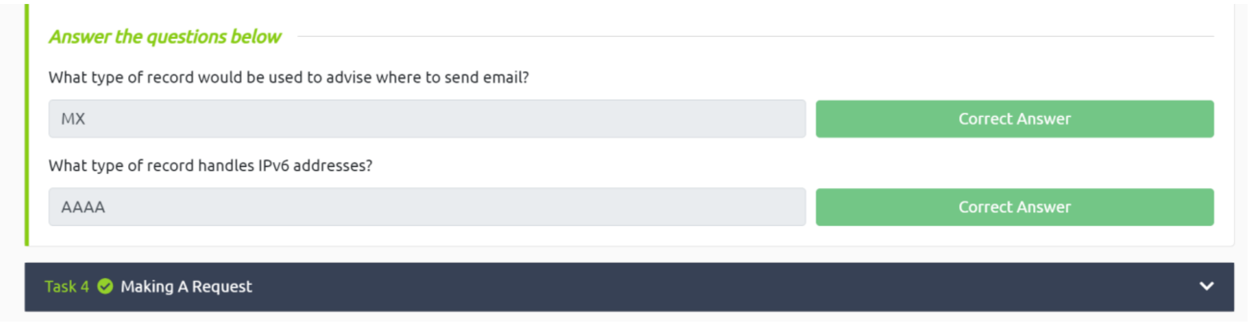
These records resolve to another domain name, for example, TryHackMe's online shop has the subdomain name store.tryhackme.com which returns a CNAME record shops.shopify.com. Another DNS request would then be made to shops.shopify.com to work out the IP address.

MX Record

These records resolve to the address of the servers that handle the email for the domain you are querying, for example an MX record response for tryhackme.com would look something like alt1.aspmx.l.google.com. These records also come with a priority flag. This tells the client in which order to try the servers, this is perfect for if the main server goes down and email needs to be sent to a backup server.

TXT Record

TXT records are free text fields where any text-based data can be stored. TXT records have multiple uses, but some common ones can be to list servers that have the authority to send an email on behalf of the domain (this can help in the battle against spam and spoofed email). They can also be used to verify ownership of the domain name when signing up for third party services.



Answer the questions below

What type of record would be used to advise where to send email?

MX

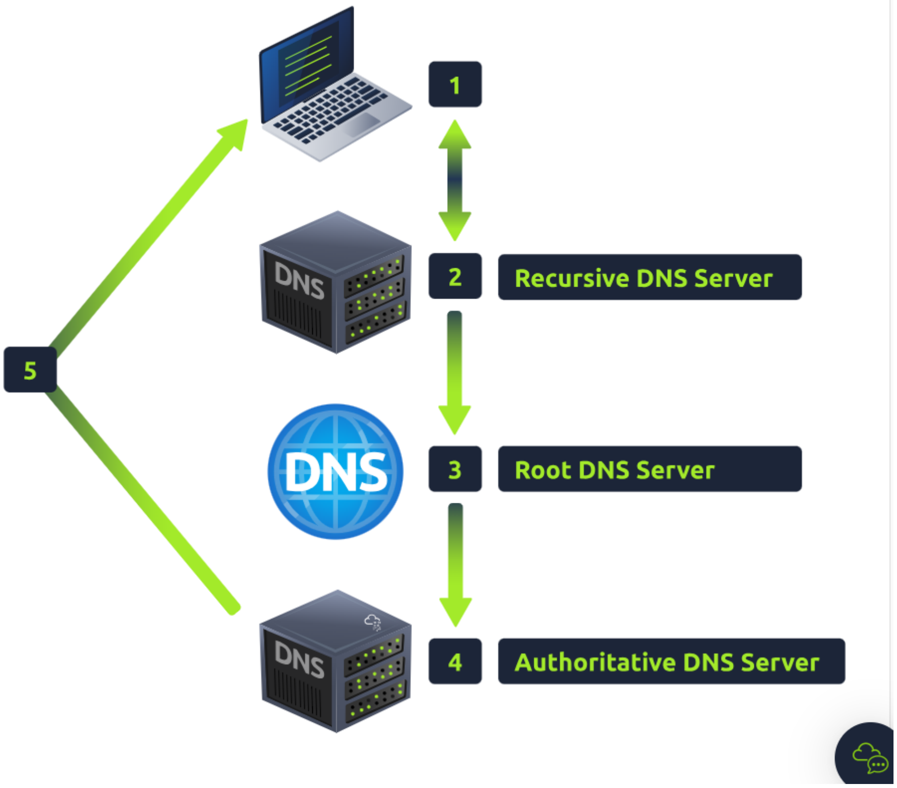
What type of record handles IPv6 addresses?

AAAA

Task 4 ✓ Making A Request

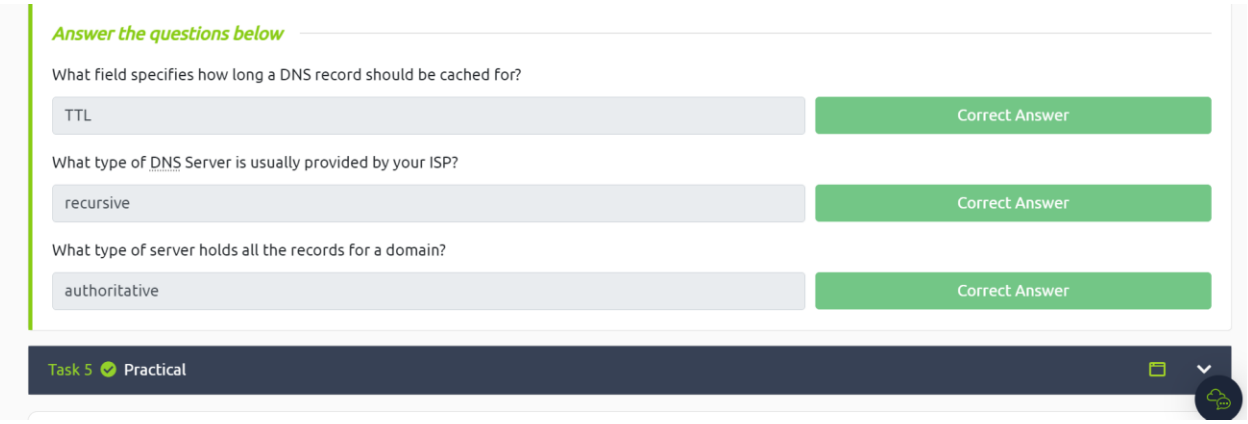
Task 4 Making A Request

When you type a domain name into your web browser, your computer needs to know the IP address of that domain in order to connect to it. It does this by making a DNS request to a series of servers, starting with the local DNS cache and ending with the authoritative DNS servers for the domain name. Once the computer has the IP address, it can connect to the domain name and load the website



When you make a DNS request:

- Your computer checks its local cache for the IP address of the domain name you requested.
- If the IP address is not in the cache, your computer sends a request to a recursive DNS server.
- The recursive DNS server checks its own cache and, if the IP address is not there, queries the root DNS servers.
- The root DNS servers redirect the recursive DNS server to the top-level domain (TLD) DNS servers.
- The TLD DNS servers redirect the recursive DNS server to the authoritative DNS servers for the domain name.
- The authoritative DNS servers send the IP address of the domain name to the recursive DNS server.
- The recursive DNS server caches the IP address and sends it to your computer.
- Your computer caches the IP address and uses it to connect to the domain name.


Answer the questions below

What field specifies how long a DNS record should be cached for?

TTL — Correct Answer

What type of DNS Server is usually provided by your ISP?

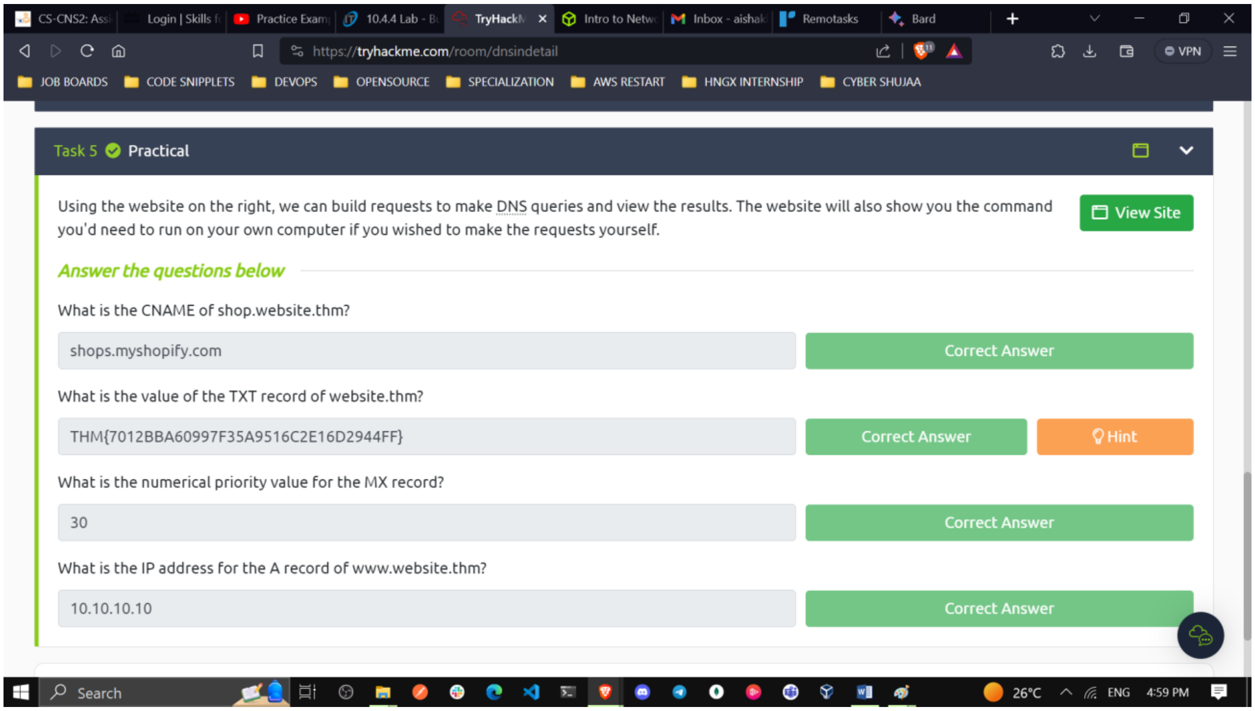
recursive — Correct Answer

What type of server holds all the records for a domain?

authoritative — Correct Answer

Task 5 Practical

Using the website on the right, we can build requests to make DNS queries and view the results. The website will also show you the command you'd need to run on your own computer if you wished to make the requests yourself.



Using the website on the right, we can build requests to make DNS queries and view the results. The website will also show you the command you'd need to run on your own computer if you wished to make the requests yourself.

Answer the questions below

What is the CNAME of shop.website.thm?

shops.myshopify.com — Correct Answer

What is the value of the TXT record of website.thm?

THM{7012BBA60997F35A9516C2E16D2944FF} — Correct Answer — Hint

What is the numerical priority value for the MX record?

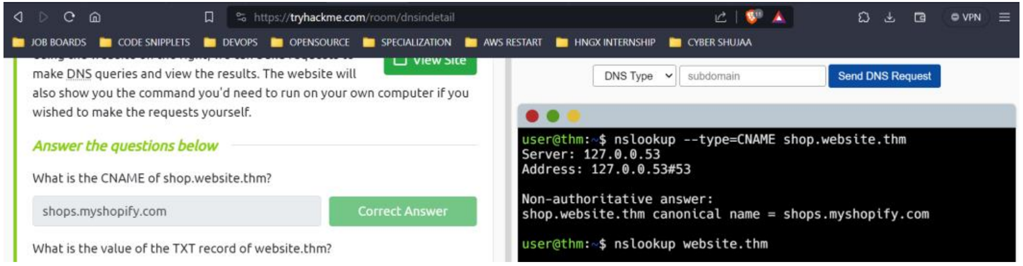
30 — Correct Answer

What is the IP address for the A record of www.website.thm?

10.10.10.10 — Correct Answer

i. What is the CNAME of shop.website.thm?

This is the code we run to check the CNAME: nslookup –type=CNAME shop.website.thm



make DNS queries and view the results. The website will also show you the command you'd need to run on your own computer if you wished to make the requests yourself.

Answer the questions below

What is the CNAME of shop.website.thm?

shops.myshopify.com — Correct Answer

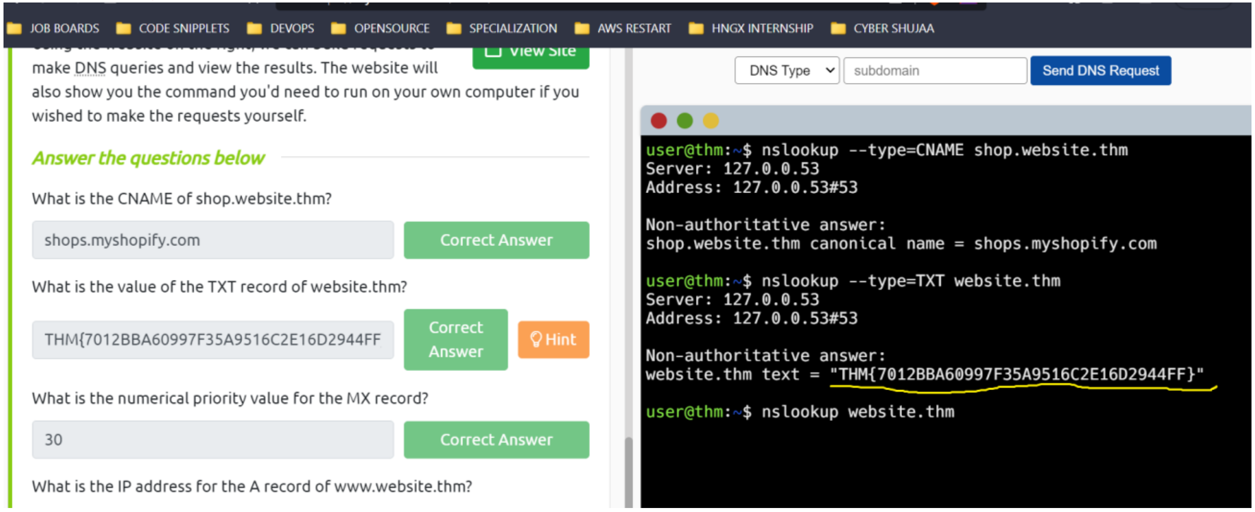
What is the value of the TXT record of website.thm?

```
user@thm:~$ nslookup --type=CNAME shop.website.thm
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
shop.website.thm canonical name = shops.myshopify.com

user@thm:~$ nslookup website.thm
```

ii. **What is the value of the TXT record of website.thm?**

To get the TXT record of website.thm this is the command that we run:

nslookup –type=TXT website.thm



make DNS queries and view the results. The website will also show you the command you'd need to run on your own computer if you wished to make the requests yourself.

Answer the questions below

What is the CNAME of shop.website.thm?

shops.myshopify.com

What is the value of the TXT record of website.thm?

THM{7012BBA60997F35A9516C2E16D2944FF

What is the numerical priority value for the MX record?

30

What is the IP address for the A record of www.website.thm?

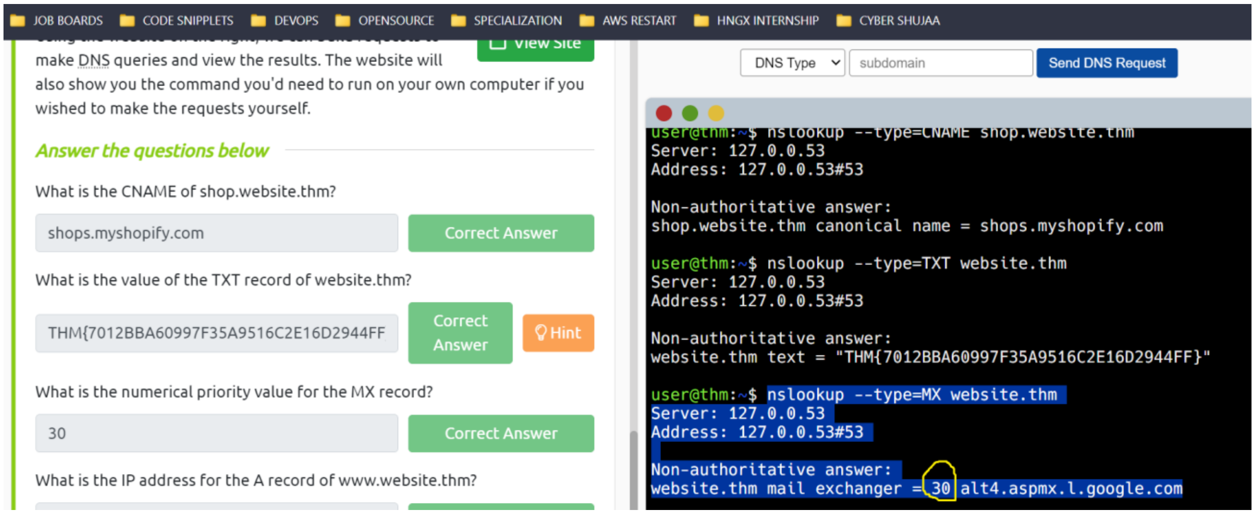
```
user@thm:~$ nslookup --type=CNAME shop.website.thm
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
shop.website.thm canonical name = shops.myshopify.com

user@thm:~$ nslookup --type=TXT website.thm
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
website.thm text = "THM{7012BBA60997F35A9516C2E16D2944FF}"

user@thm:~$ nslookup website.thm
```

iii. **What is the numerical priority value for the MX record?**

To get the numerical priority value for the MX record we run the following command:

nslookup –type=MX website.thm

30



make DNS queries and view the results. The website will also show you the command you'd need to run on your own computer if you wished to make the requests yourself.

Answer the questions below

What is the CNAME of shop.website.thm?

shops.myshopify.com

What is the value of the TXT record of website.thm?

THM{7012BBA60997F35A9516C2E16D2944FF

What is the numerical priority value for the MX record?

30

What is the IP address for the A record of www.website.thm?

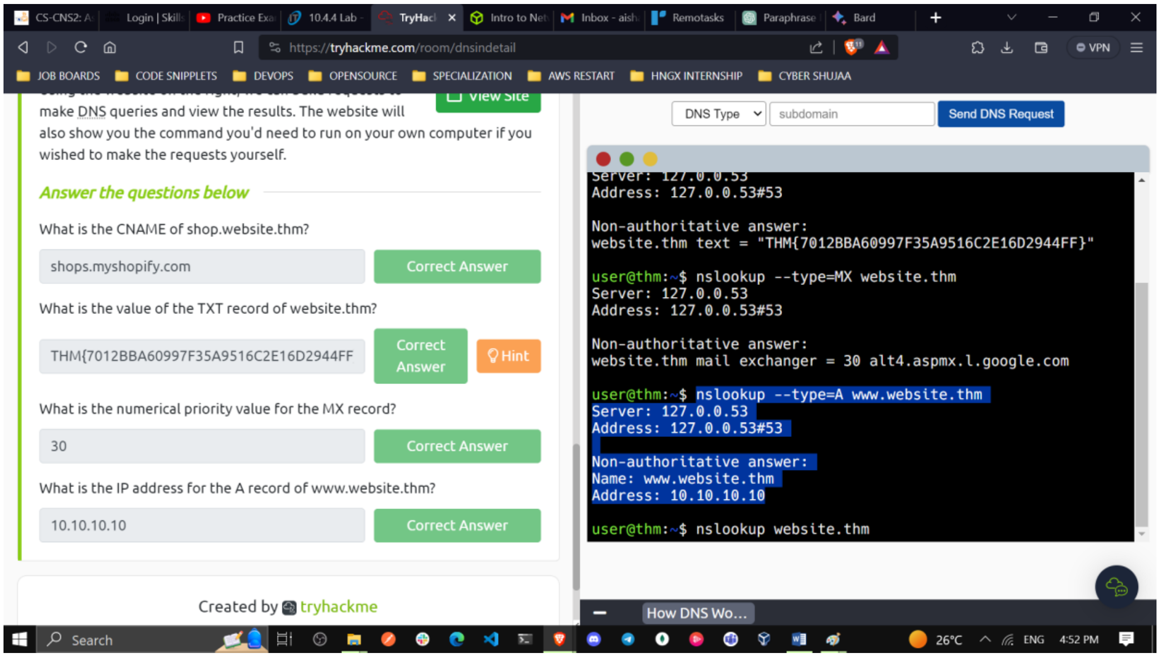
```
user@thm:~$ nslookup --type=CNAME shop.website.thm
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
shop.website.thm canonical name = shops.myshopify.com

user@thm:~$ nslookup --type=TXT website.thm
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
website.thm text = "THM{7012BBA60997F35A9516C2E16D2944FF}"

user@thm:~$ nslookup --type=MX website.thm
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
website.thm mail exchanger = 30 alt4.aspmx.l.google.com
```

iv. **What is the IP address for the A record of www.website.thm?**

To get the IP address for the A record of www.website.thm we use the following command:

nslookup –type=A website.thm

10.10.10.10



make DNS queries and view the results. The website will also show you the command you'd need to run on your own computer if you wished to make the requests yourself.

Answer the questions below

What is the CNAME of shop.website.thm?

shops.myshopify.com — Correct Answer

What is the value of the TXT record of website.thm?

THM{7012BBA60997F35A9516C2E16D2944FF — Correct Answer — Hint

What is the numerical priority value for the MX record?

30 — Correct Answer

What is the IP address for the A record of www.website.thm?

10.10.10.10 — Correct Answer

Created by tryhackme

```
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
website.thm text = "THM{7012BBA60997F35A9516C2E16D2944FF}"

user@thm:~$ nslookup --type=MX website.thm
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
website.thm mail exchanger = 30 alt4.aspmx.l.google.com

user@thm:~$ nslookup --type=A www.website.thm
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
Name: www.website.thm
Address: 10.10.10.10

user@thm:~$ nslookup website.thm
```

Conclusion

DNS is used to map domain names to IP addresses, which are the numerical addresses that computers use to communicate with each other on the Internet. When you type a domain name into your web browser, your computer sends a DNS query to a DNS server to find the IP address of the website you want to visit. Once the DNS server has found the IP address, it sends it back to your computer, which can then connect to the website.

There are many different types of DNS records, but some of the most common ones are:
A records: These records map domain names to IPv4 addresses.
AAAA records: These records map domain names to IPv6 addresses.
CNAME records: These records map domain names to other domain names.
MX records: These records map domain names to mail servers.
TXT records: These records can be used to store any type of text data.
DNS is a critical part of the Internet infrastructure, and it is essential for the smooth operation of the web. Without DNS, it would be impossible to visit websites or send emails.

nslookup is widely used by system administrators, network engineers, and developers to perform DNS-related tasks and gain insights into DNS resolution processes and find out more about the DNS records. It provides a quick and easy way to query DNS and obtain critical information necessary for troubleshooting and network management. However, newer tools like **dig** (domain information groper) and **host** are becoming more popular due to their enhanced features and functionalities.