Course: Cloud and Network Security – C2 – 2025.

Student: Luke Mbogo

Student No: cs-cns09-25076

Wednesday, June 4th, 2025.

Week 3 Assignment 1:

DNS in Detail (Tryhackme).

Contents

Introduction.

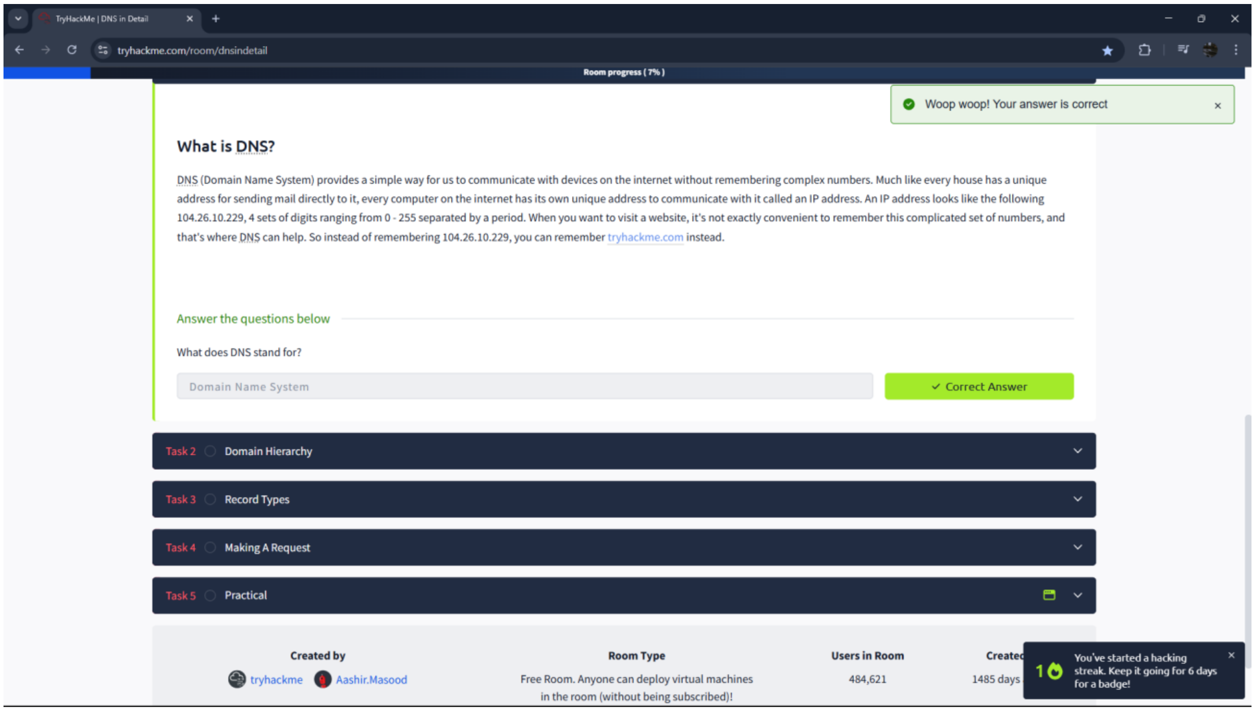
In this challenge, I got to understand the basics of DNS (Domain Name System) and its crucial role in how we interact with the internet daily. One key takeaway is how DNS makes things simpler for users — instead of having to memorize complex IP addresses like 104.26.10.229, we can just use easy-to-remember domain names like tryhackme.com.

What is DNS.

This system works a lot like a phonebook or a postal address system: every device connected to the internet has a unique IP address, much like every house has a unique address. DNS translates human-friendly domain names into those numeric IP addresses that computers use to identify each other.

Before this, I didn't fully appreciate just how fundamental DNS is in our daily browsing experience. It quietly handles the background work of connecting us to websites — making the internet more user-friendly without us even noticing.

Task 1.



Woop woop! Your answer is correct

What is DNS?

DNS (Domain Name System) provides a simple way for us to communicate with devices on the internet without remembering complex numbers. Much like every house has a unique address for sending mail directly to it, every computer on the internet has its own unique address to communicate with it called an IP address. An IP address looks like the following 104.26.10.229, 4 sets of digits ranging from 0 - 255 separated by a period. When you want to visit a website, it's not exactly convenient to remember this complicated set of numbers, and that's where DNS can help. So instead of remembering 104.26.10.229, you can remember tryhackme.com instead.

Answer the questions below

What does DNS stand for?

Domain Name System

Created by	Room Type	Users in Room	Created
tryhackme Aashir.Masood	Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!	484,621	1485 days

You've started a hacking streak. Keep it going for 6 days for a badge!

Domain Hierarchy.

Top-Level Domain (TLD)

I learned that the **Top-Level Domain (TLD)** is the last part of a domain name — for example, in tryhackme.com, the .com is the TLD. TLDs come in two main types: **gTLDs (Generic Top-Level Domains)** like .com, .org, and .edu, which generally reflect the nature of the website, and **ccTLDs (Country Code Top-Level Domains)** like .ke, .uk, or .ca, which are tied to specific countries or regions. Interestingly, due to high demand, a lot of new gTLDs have emerged, such as .club, .online, and .biz.

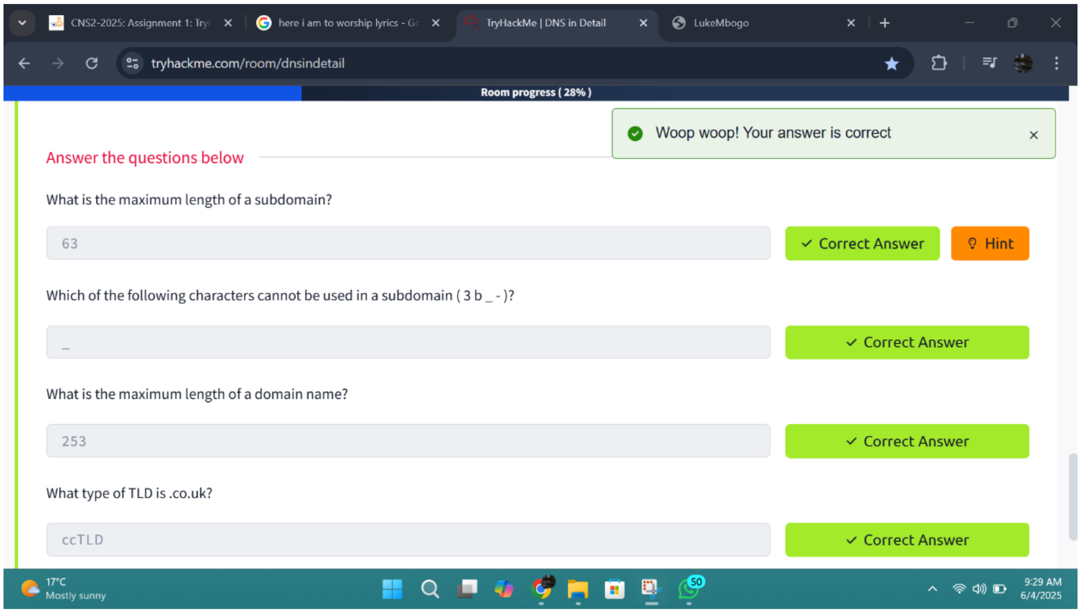
Second-Level Domain

Then there's the **Second-Level Domain**, which is the part right before the TLD — in this case, tryhackme in tryhackme.com. It's the name you actually register, and I learned it has some specific rules: it must be no longer than 63 characters, can use letters, numbers, and hyphens, but it can't start or end with a hyphen, and can't have consecutive hyphens.

Subdomains

Another interesting part was **subdomains** — these sit to the left of the Second-Level Domain and are used to organize different sections or services of a website. For example, admin.tryhackme.com uses admin as a subdomain. I also found out that you can chain subdomains like jupiter.servers.tryhackme.com, as long as the full length of the domain stays under 253 characters. Like Second-Level Domains, subdomains follow the same naming rules.

Task 2.


CNS2-2025: Assignment 1: Tryl
here i am to worship lyrics - Go
TryHackMe | DNS in Detail
LukeMbogo
tryhackme.com/room/dnsindetail
17°C
Mostly sunny
9:29 AM
6/4/2025

Room progress (28%)

Woop woop! Your answer is correct

Answer the questions below

What is the maximum length of a subdomain?

63 — ✓ Correct Answer — Hint

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

_ — ✓ Correct Answer

What is the maximum length of a domain name?

253 — ✓ Correct Answer

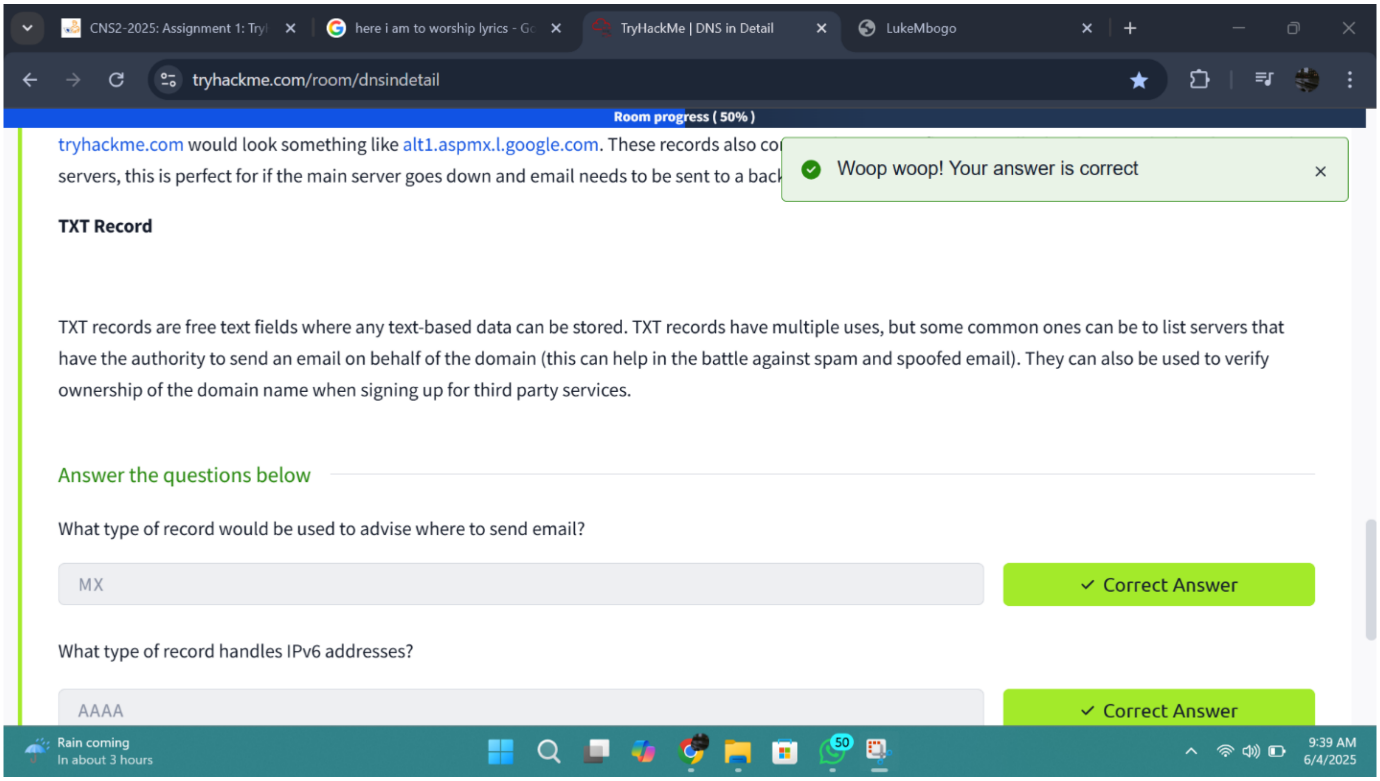
What type of TLD is .co.uk?

ccTLD — ✓ Correct Answer

DNS Record Types.

- **A and AAAA Records** - The most common type is the A Record, which maps a domain to an **IPv4 address** like 104.26.10.229. Similarly, there's the AAAA Record, which does the same but for **IPv6 addresses**, such as 2606:4700:20::681a:be5.
- **CNAME Record** - Another important one is the CNAME Record. Instead of pointing directly to an IP, it maps one domain name to another. For example, store.tryhackme.com might resolve to shops.shopify.com, and then the system will make another DNS request to find the actual IP of that second domain. This is useful when services are hosted externally.
- **MX Record** - Then there's the MX Record, which is all about handling email. These records point to the mail servers responsible for a domain. They also include a priority value, which helps email clients know which mail server to try first — super useful for backup mail routing if the main server fails.
- **TXT Records** - Lastly, I learned about TXT Records, which are basically flexible text fields attached to a domain. They're used for different purposes like verifying domain ownership, or declaring which servers are allowed to send mail on behalf of the domain a tactic used to fight email spoofing and spam.

Task 3.


CNS2-2025: Assignment 1: Tryl
here i am to worship lyrics - Gc
TryHackMe | DNS in Detail
LukeMbogo
tryhackme.com/room/dnsindetail
Room progress (50%)
Rain coming
In about 3 hours
50
9:39 AM
6/4/2025

tryhackme.com would look something like alt1.aspmx.l.google.com. These records also co

servers, this is perfect for if the main server goes down and email needs to be sent to a back

Woop woop! Your answer is correct

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 ✓ Correct Answer

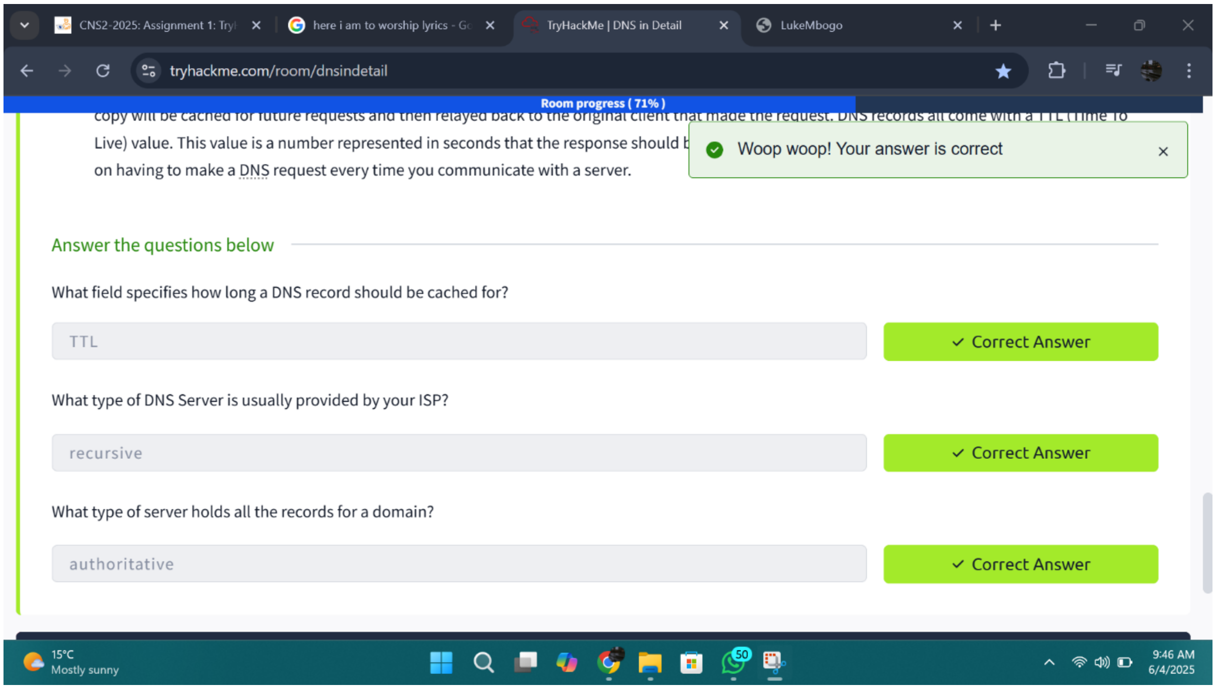
What type of record handles IPv6 addresses?

AAAA ✓ Correct Answer

DNS Request.

1. **Local Cache Check**: My computer first checks its own local DNS cache to see if the domain has been looked up recently. If it's there, it uses the cached result and ends the process immediately.
2. **Recursive DNS Server Request**: If the local cache doesn't have the answer, the request is sent to a **Recursive DNS Server** (usually from my ISP, but I can also choose others like Google DNS or Cloudflare).
3. **Recursive Server Cache Check**: The Recursive DNS Server checks its own cache. If it finds a valid result, it returns the answer to my computer.
4. **Query to Root DNS Server**: If the Recursive server has no answer, it sends the request to one of the **Root DNS Servers**, which are the backbone of the DNS system.
5. **Root to TLD Server Redirection**: The Root Server identifies the **Top-Level Domain (TLD)** in the query (like .com) and redirects the request to the relevant **TLD Server**.
6. **TLD Server Points to Authoritative Server**: The TLD Server responds with the address of the Authoritative Name Server for the domain, which actually holds the DNS records.
7. **Authoritative Server Response**: The Authoritative DNS Server returns the appropriate DNS record (A, CNAME, MX, etc.) for the domain back to the Recursive DNS Server.
8. **Caching and Final Response**: The Recursive DNS Server stores the response in its cache based on the **TTL (Time To Live)** value and then forwards it back to my computer. My machine may also cache the result for quicker access next time.

Task 4.


CNS2-2025: Assignment 1: Tryl
here i am to worship lyrics - Go
TryHackMe | DNS in Detail
LukeMbogo
tryhackme.com/room/dnsindetail
Room progress (71%)
15°C
Mostly sunny
9:46 AM
6/4/2025

copy will be cached for future requests and then relayed back to the original client that made the request. DNS records all come with a TTL (Time To Live) value. This value is a number represented in seconds that the response should b on having to make a DNS request every time you communicate with a server.

Woop woop! Your answer is correct

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

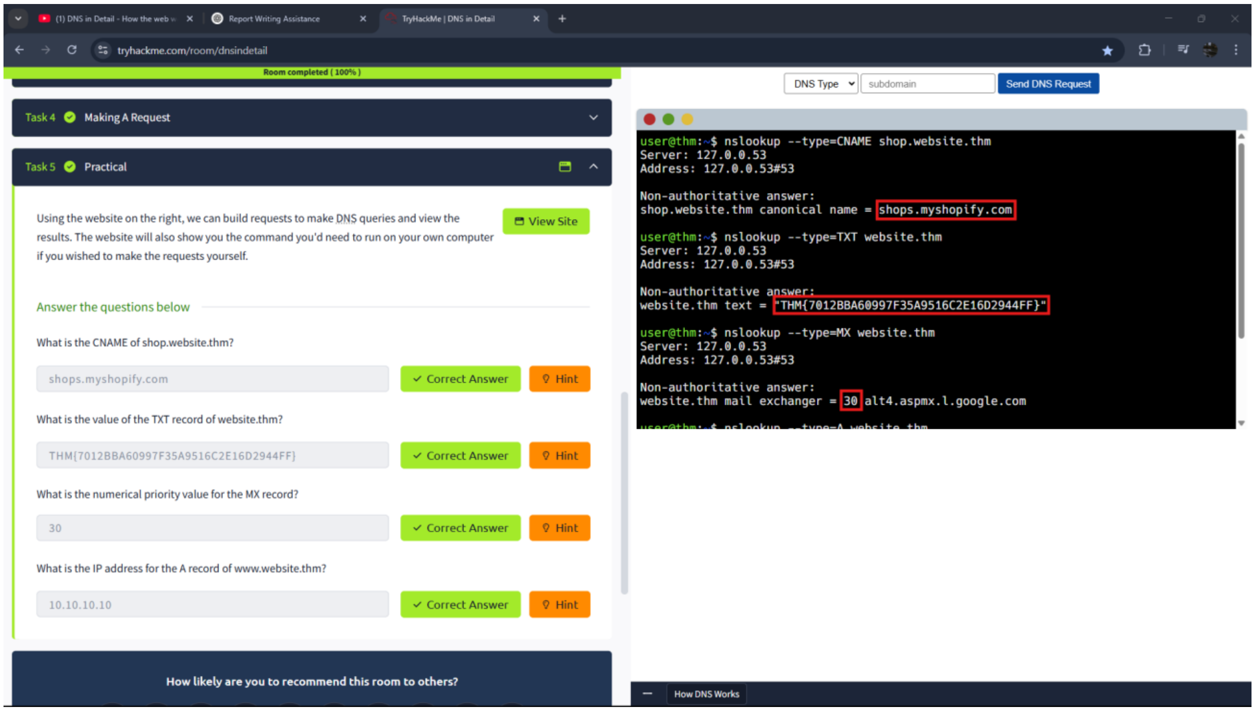
What type of server holds all the records for a domain?

authoritative

✓ Correct Answer

Practical.

Task 5.



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 Hint

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 Hint

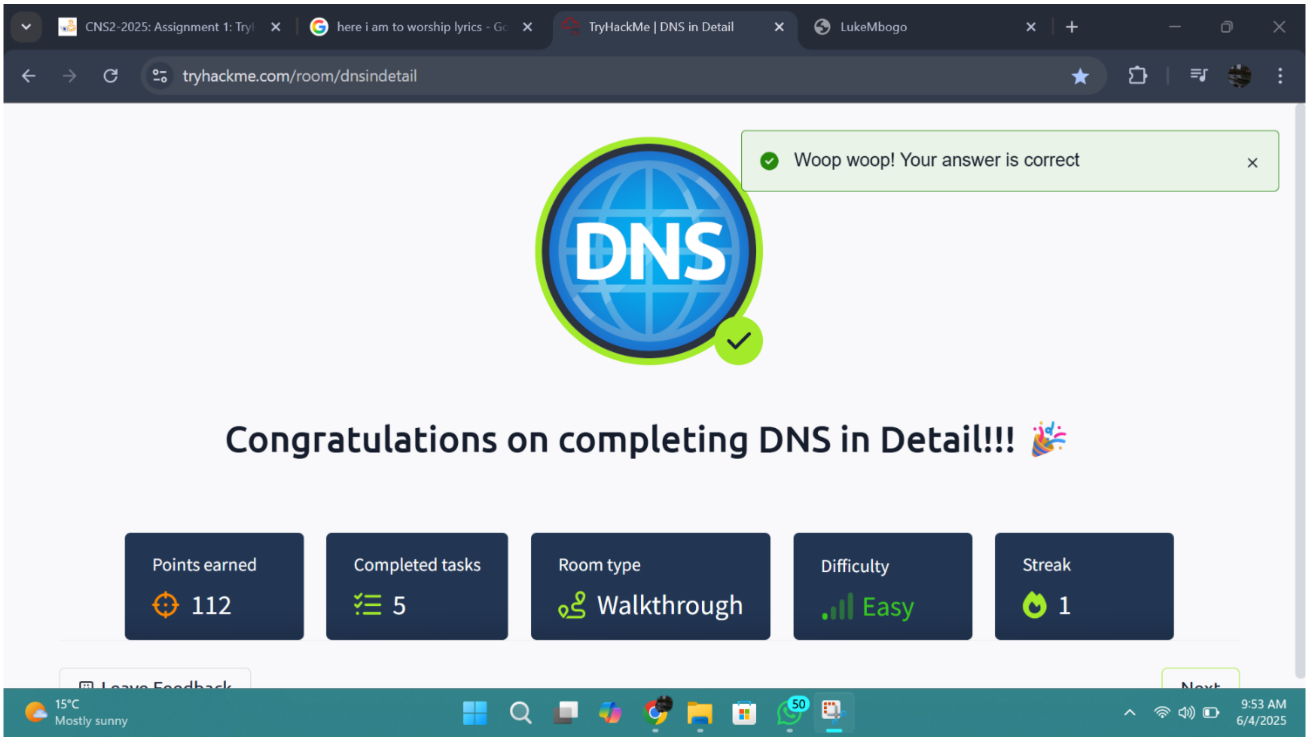
What is the IP address for the A record of www.website.thm?

10.10.10.10 ✓ Correct Answer Hint

How likely are you to recommend this room to others?

```
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

user@thm:~$ nslookup --type=A website.thm
```

Module Completion


CNS2-2025: Assignment 1: Tryl
here i am to worship lyrics - Go
TryHackMe | DNS in Detail
LukeMbogo
tryhackme.com/room/dnsindetail
DNS
Leave Feedback
Next
15°C
Mostly sunny
50
9:53 AM
6/4/2025

Woop woop! Your answer is correct

Congratulations on completing DNS in Detail!!! 🎉

Points earned 112

Completed tasks 5

Room type Walkthrough

Difficulty Easy

Streak 1

Conclusion.

Working through this TryHackMe challenge gave me a deeper understanding of how DNS works and why it's so important to how we use the internet every day. What initially seemed like a simple system for matching names to IPs turned out to be a complex, layered, and highly efficient process involving multiple servers and caching mechanisms. I learned how DNS simplifies human interaction with the web by translating domain names into IP addresses, and I explored the structure of domains — including TLDs, second-level domains, and subdomains. I also gained clarity on various DNS record types like A, AAAA, CNAME, MX, and TXT, and how each serves a specific role in directing internet traffic and services.

Finally, the detailed breakdown of the DNS resolution process helped me understand how recursive servers, root servers, TLD servers, and authoritative name servers all interact to deliver a result — often in just milliseconds. The concept of caching and TTL values showed how performance is optimized to reduce unnecessary load. Overall, this challenge not only improved my technical knowledge but also gave me a practical framework for troubleshooting and understanding DNS in both networking and cybersecurity contexts.