Assignment 1: TryHackMe: DNS In Detail

Report by: Tonny Odhiambo, CS-CNS06-24028

Introduction

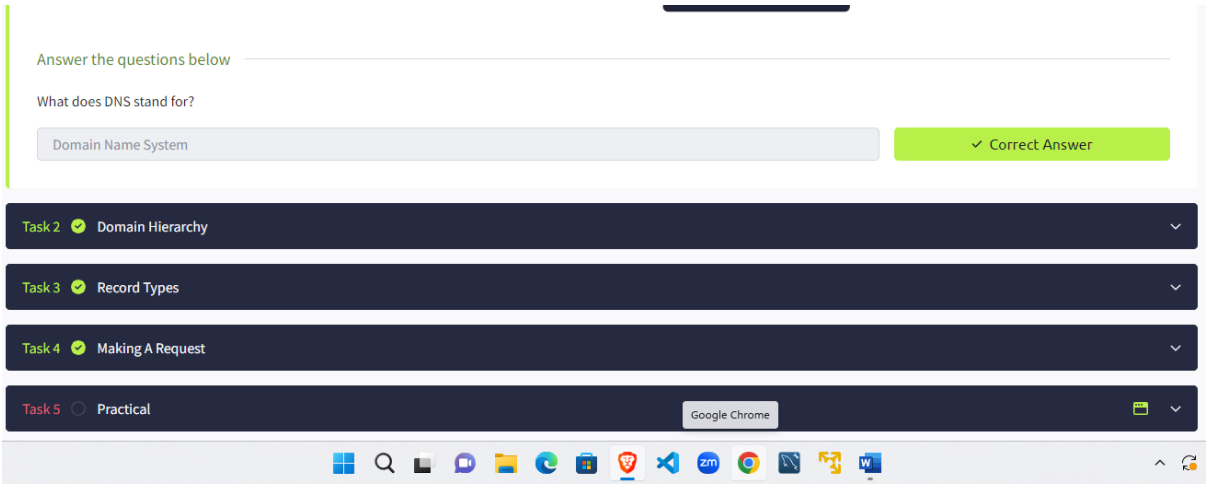
In the "DNS in Detail" module on TryHackMe, I explored the intricacies of the Domain Name System (DNS), which is a crucial component of internet functionality. This exercise provided a comprehensive overview of DNS, starting with the basics and progressing through the hierarchical structure of domain names. I examined various types of DNS records and understood how DNS requests are made and processed.

This module aimed to equip me with the knowledge necessary to comprehend how domain names are translated into IP addresses, facilitating seamless internet navigation. Through this module, I gained a deeper appreciation for the complexity and importance of DNS in our digital world.

Answers to questions:

Task 1: What does DNS stand for?

DNS stands for **Domain Name System**



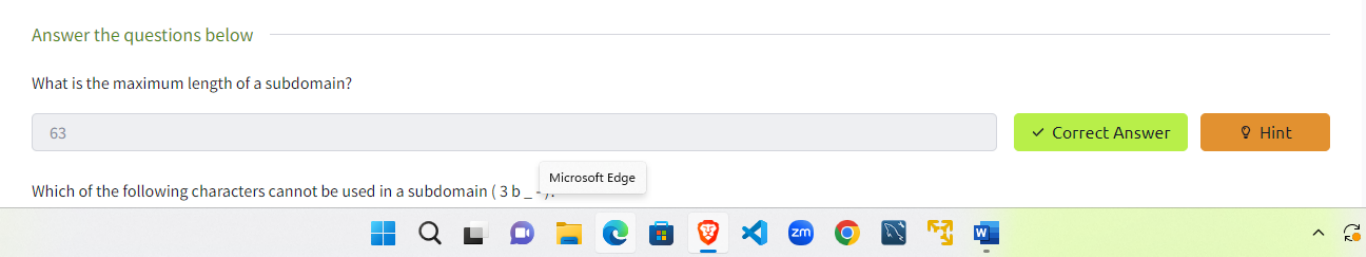
Task 2: Domain Hierarchy

There are three levels namely;

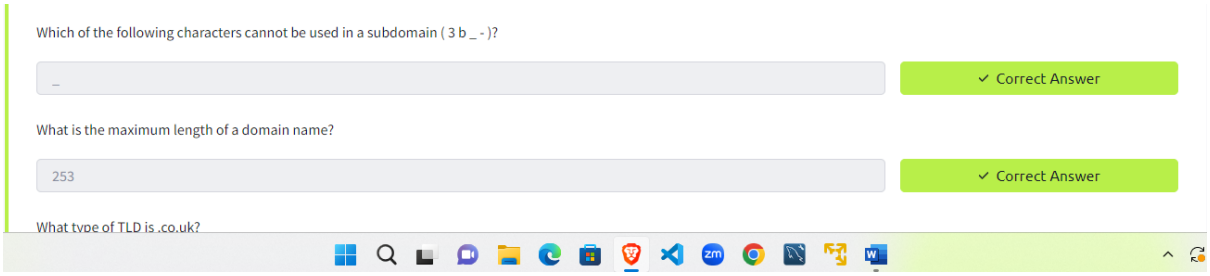
a) A Top-Level Domain (TLD) is the rightmost part of a domain name, such as .com in tryhackme.com, and includes types like gTLDs for general purposes and ccTLDs for country-specific sites.
b) A Second-Level Domain, like tryhackme in tryhackme.com, can use a-z, 0-9, and hyphens within a 63-character limit.
c) Subdomains, such as admin in admin.tryhackme.com, follow the same character rules and can be used to create longer, hierarchical names up to 253 characters in length. There is no limit to the number of subdomains that can be created for a domain.

Answers to the questions for task 2:

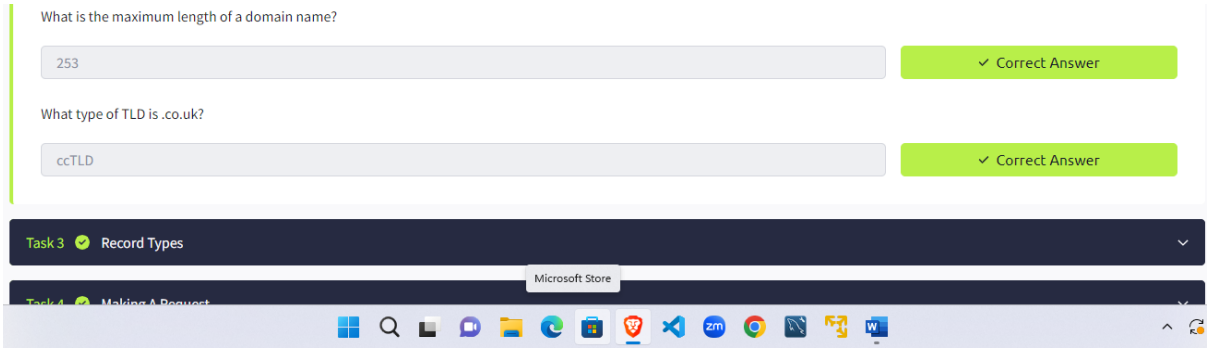
1. What is the maximum length of a subdomain? **63**



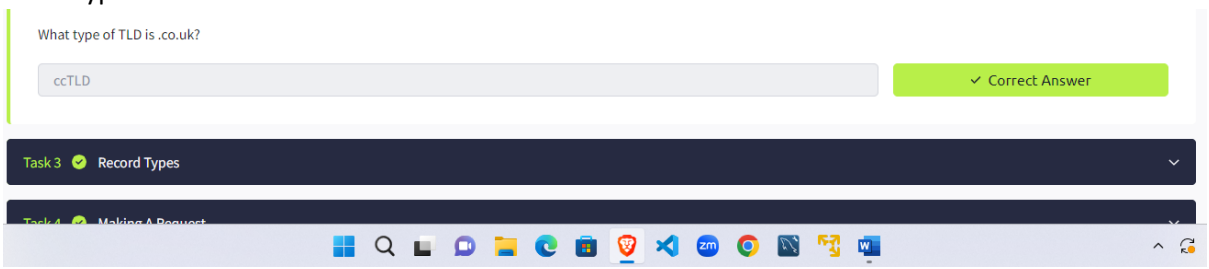
2. Which of the following characters cannot be used in a subdomain (3 b _ -)? **Answer is _**



3. What is the maximum length of a domain name? **253**



4. What type of TLD is .co.uk? **ccTLD**



Task 3: DNS Record Types

There are five types of DNS record commonly encountered in DNS configurations:

1. A Record: Resolves to IPv4 addresses.

2. AAAA Record: Resolves to IPv6 addresses.

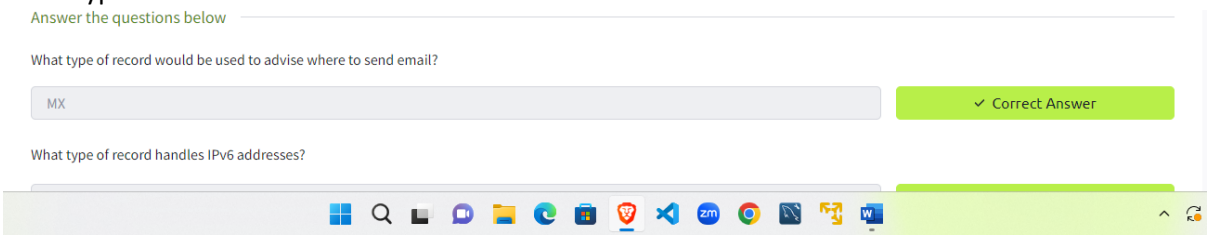
3. CNAME Record: Resolves to another domain name.

4. MX Record: Resolves to the address of email servers for the domain, with priority flags indicating server preference.

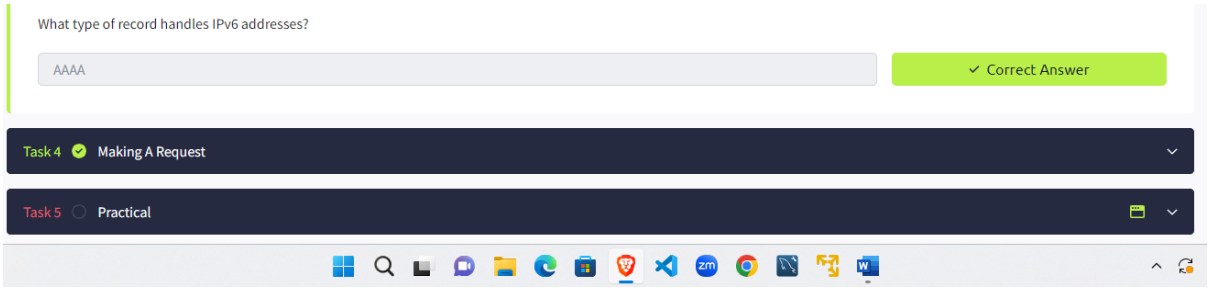
5. TXT Record: Free text fields used for various purposes, including listing authorized email servers and domain ownership verification for third-party services.

Answers to the questions for task 3:

1. What type of record would be used to advise where to send email? **MX**



2. What type of record handles IPv6 addresses? **AAAA**



Task 4: Making A Request

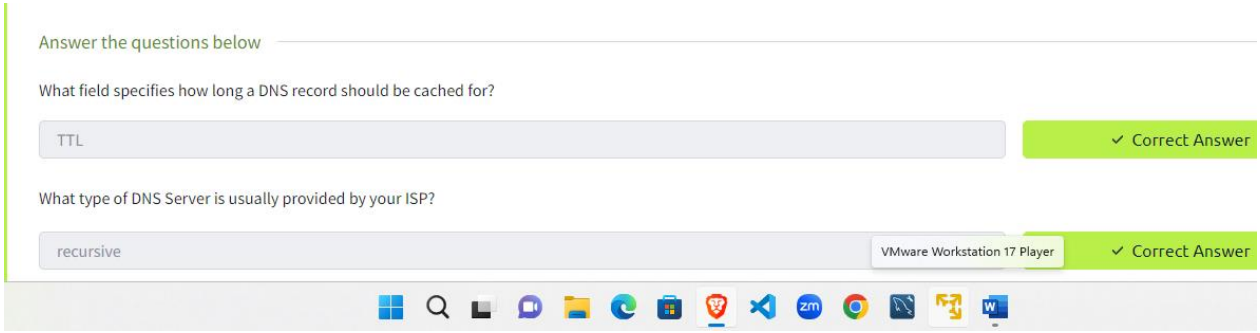
When making a DNS request, your computer first checks its local cache. If the address is not found locally, a request is sent to the Recursive DNS Server, which may have its own cache.

If the requested information is not in the Recursive DNS Server's cache, it queries the root DNS servers to determine the correct Top Level Domain (TLD) server. The TLD server then directs the request to the authoritative server for the specific domain.

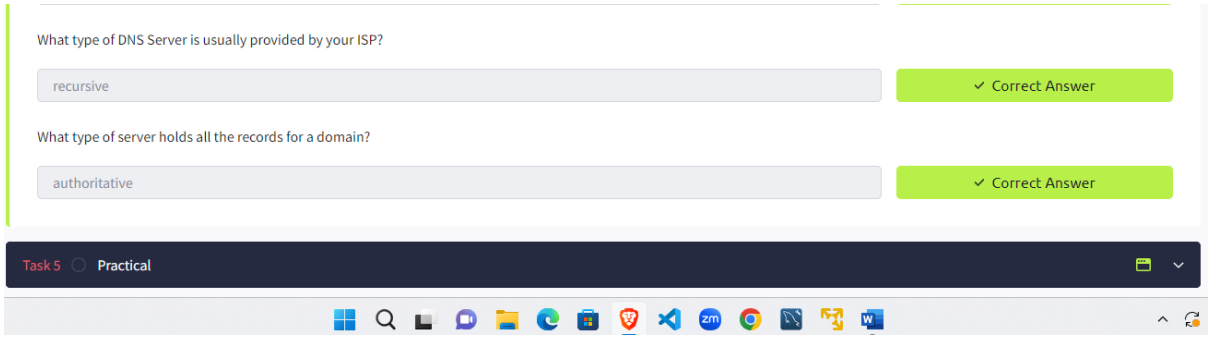
The authoritative server holds the DNS records for the domain and sends the requested information back to the Recursive DNS Server, which caches it and relays it to the original requester. DNS records have a Time To Live (TTL) value, determining how long the information should be cached.

Answers to the questions for task 4:

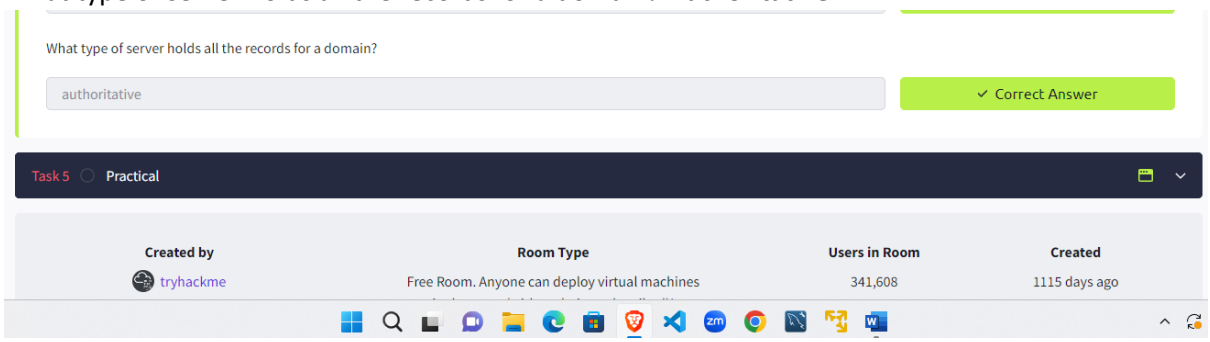
1. What field specifies how long a DNS record should be cached for? **TTL**



2. What type of DNS Server is usually provided by your ISP? **Recursive**



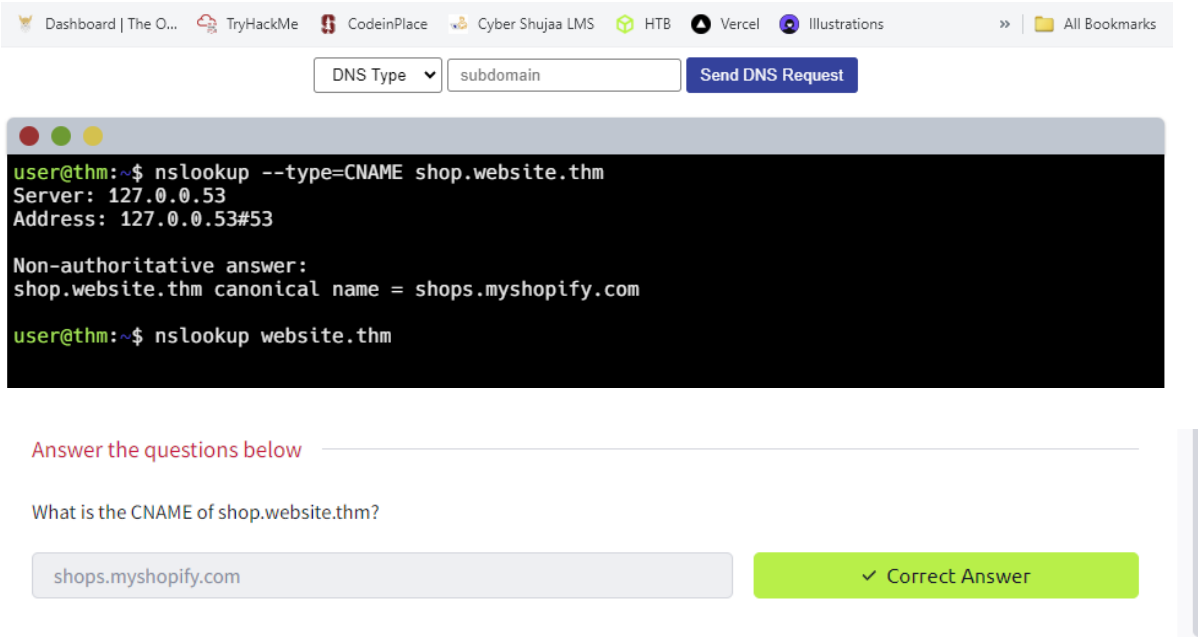
3. What type of server holds all the records for a domain? **Authoritative**



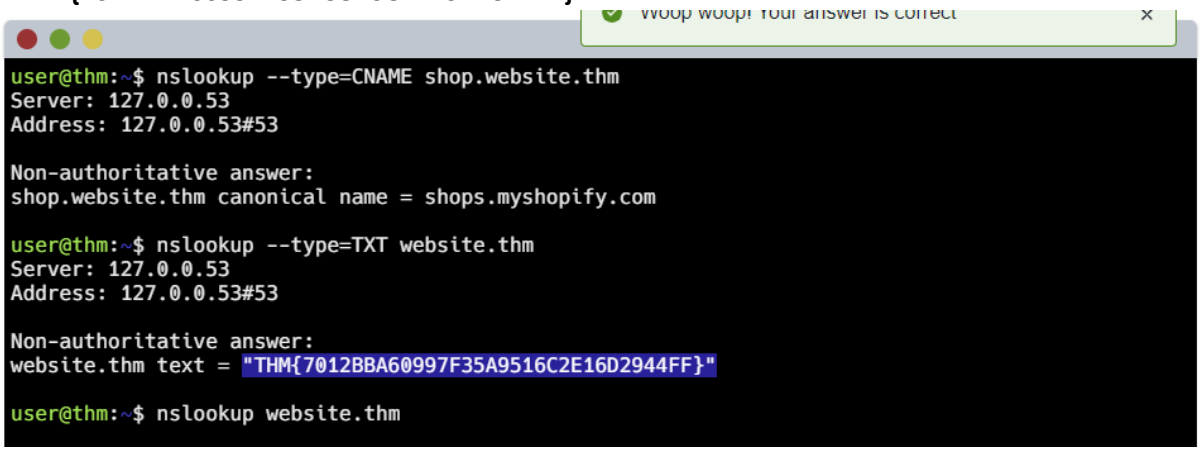
Task 5: Practical

Here, we build requests to make DNS queries and view the results.

1. What is the CNAME of shop.website.thm? **shops.myshopify.com**



2. What is the value of the TXT record of website.thm?
"THM{7012BBA60997F35A9516C2E16D2944FF}"



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?

Answer format: **

Submit

3. What is the numerical priority value for the MX record? **30**

```
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 website.thm
```

What is the numerical priority value for the MX record?

30

✓ Correct Answer

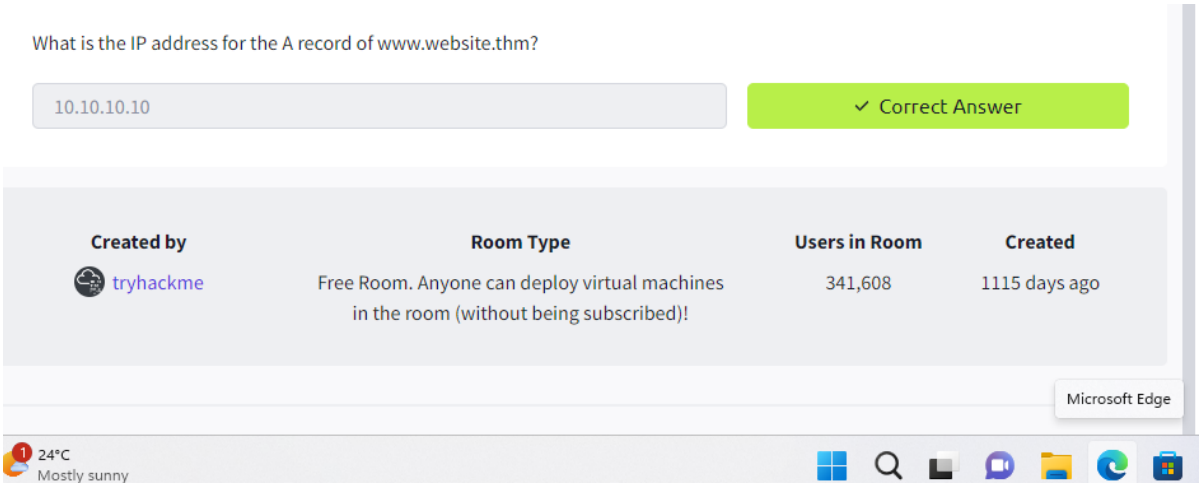
What is the IP address for the A record of www.website.thm?

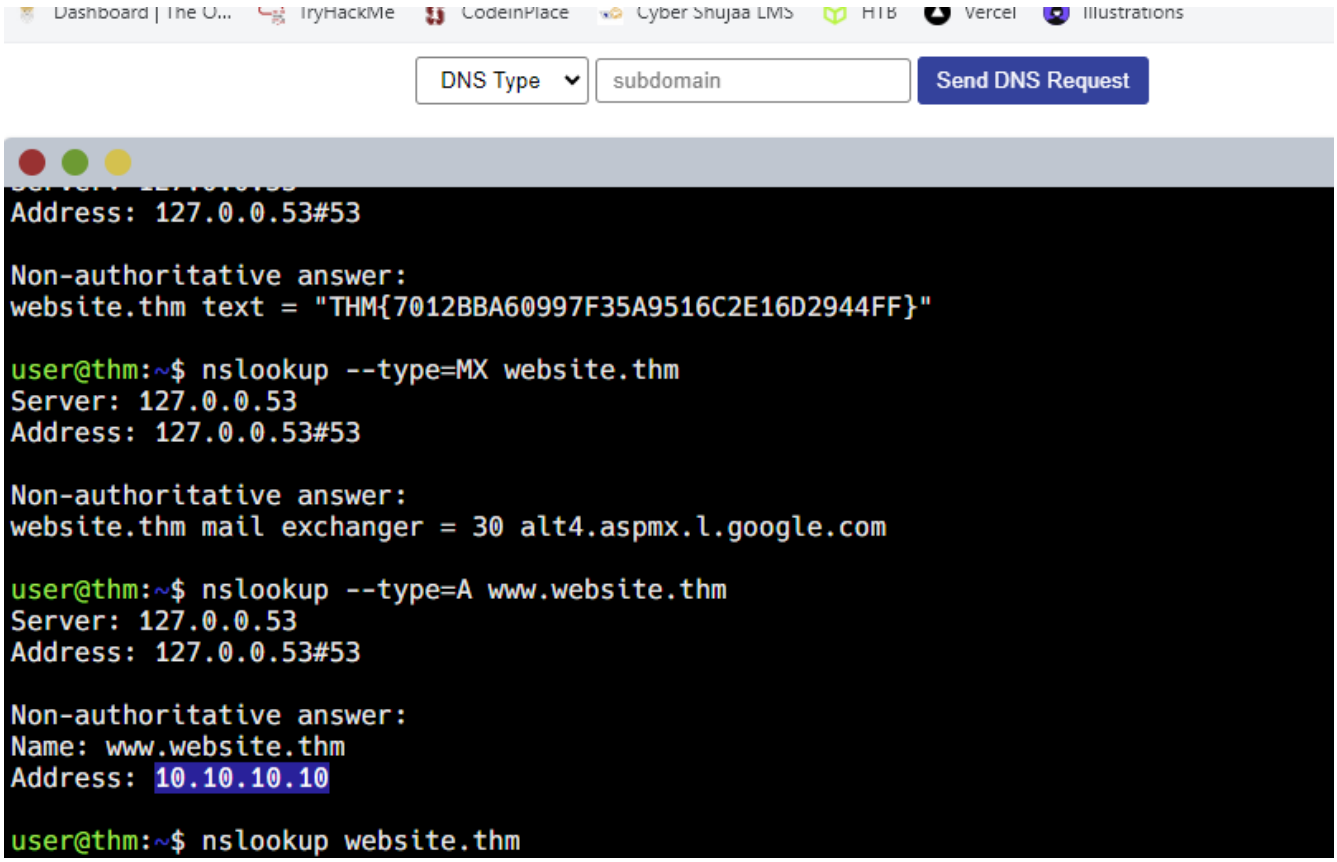
Answer format: **.**.**.**

Submit

24°C
Mostly sunny

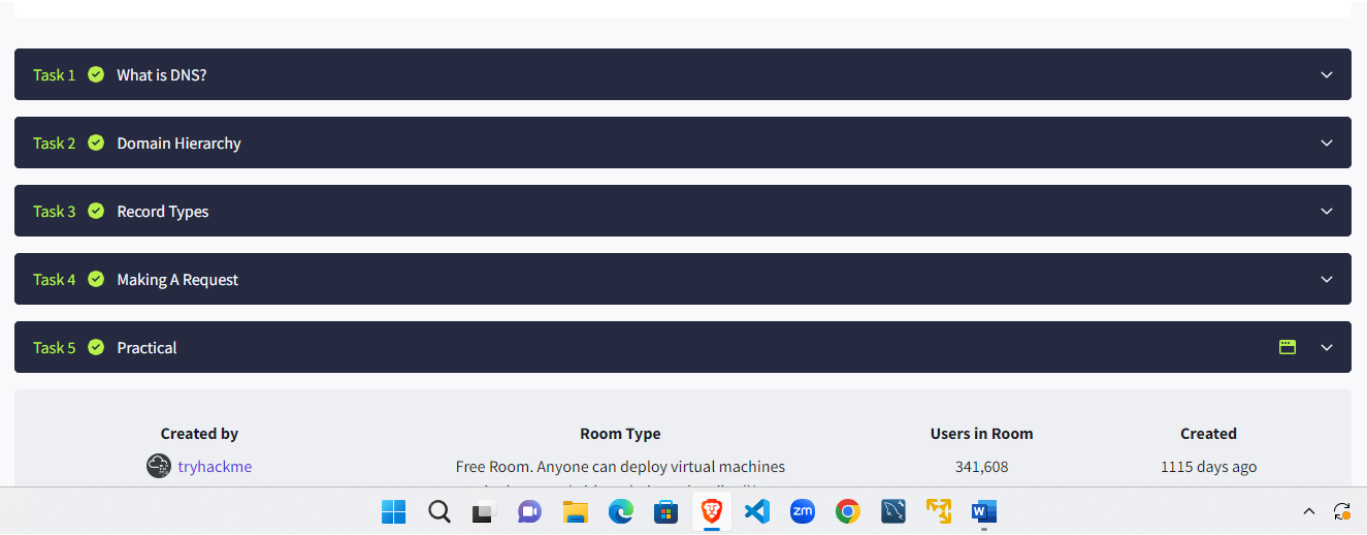
4. What is the IP address for the A record of www.website.thm? **10.10.10.10**

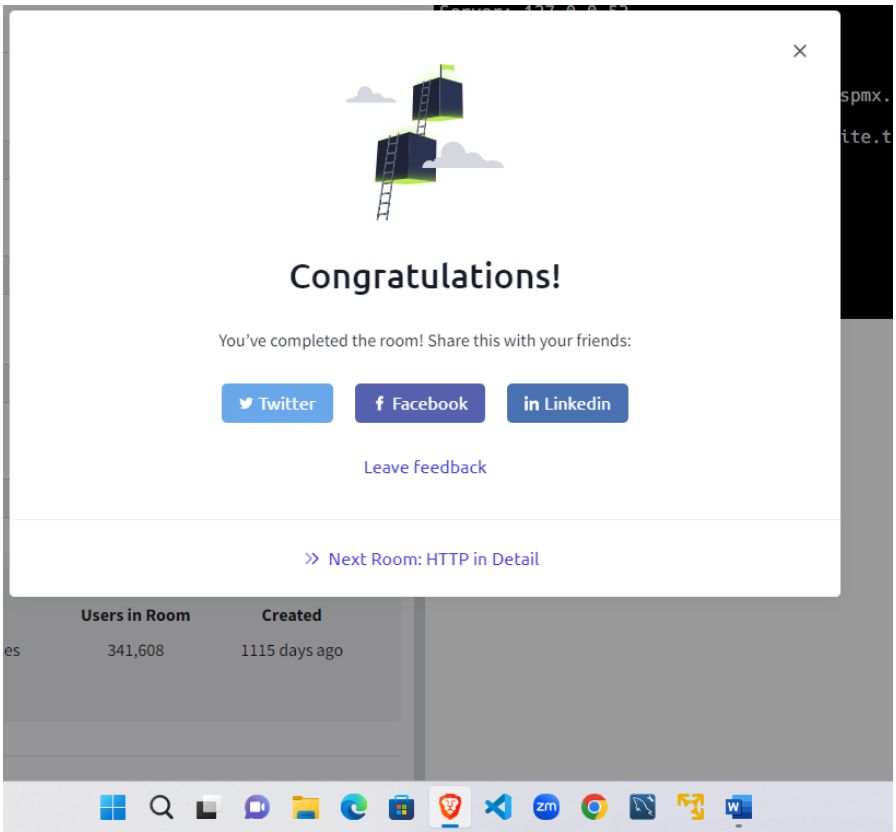




Here is a link to my TryHackMe dashboard for proof of completion.

https://tryhackme.com/jr/dnsindetail





Conclusion

Completing the "DNS in Detail" module on TryHackMe has provided me with a thorough understanding of DNS operations. From grasping the hierarchical structure of domain names to learning about various DNS record types and the process of making DNS requests, I now possess essential insights into this critical internet service.

This knowledge is essential for professionals in networking and cybersecurity, as DNS is fundamental to accessing online resources. Equipped with this understanding, I am better prepared to troubleshoot DNS-related issues and appreciate the vital role of the Domain Name System in our daily internet usage.