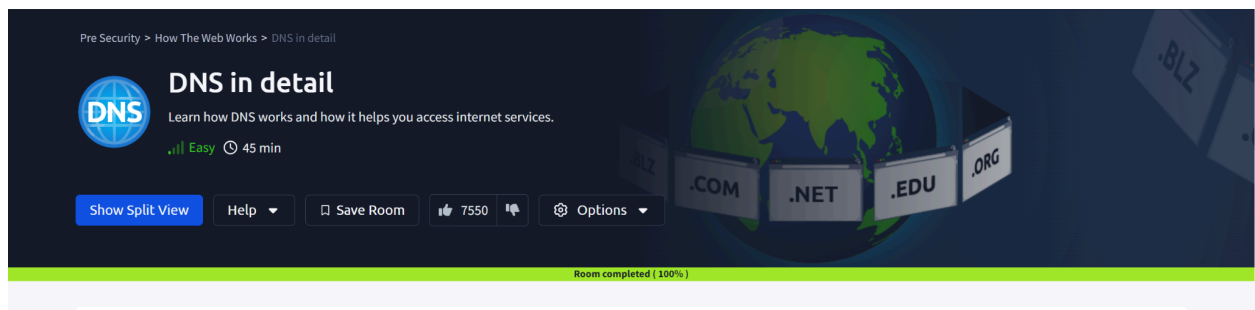


DNS IN DETAIL

ASSIGNMENT REPORT



Peter Kinyumu,
cs-sa07-24067,
May 29th, 2024

1. INTRODUCTION

This room covered how the Domain Name System(DNS) service works, including the records it encompasses and what happens under the hood when DNS requests are made.

DNS is the service that helps us access the internet by translating human-readable domain names like tryhackme.com into numerical IP addresses like **104.26.10.229**.

2. ANSWERS TO QUESTIONS

DNS

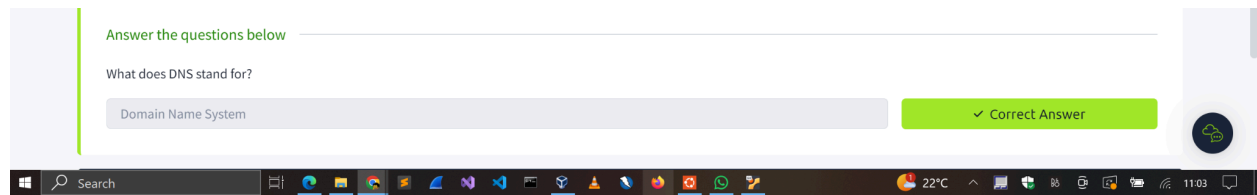
a. What does DNS stand for?

Answer the questions below

What does DNS stand for?

Domain Name System

✓ Correct Answer



Domain Hierarchy

a. What is the maximum length of a subdomain?

63 characters.

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

Subdomains cannot contain an underscore(_).

c. What is the maximum length of a domain name?

A domain name MUST not exceed 253 characters

d. What type of TLD is .co.uk?

It is a ccTLD (Country Code Top Level Domain) for the United Kingdom country in Europe.

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?

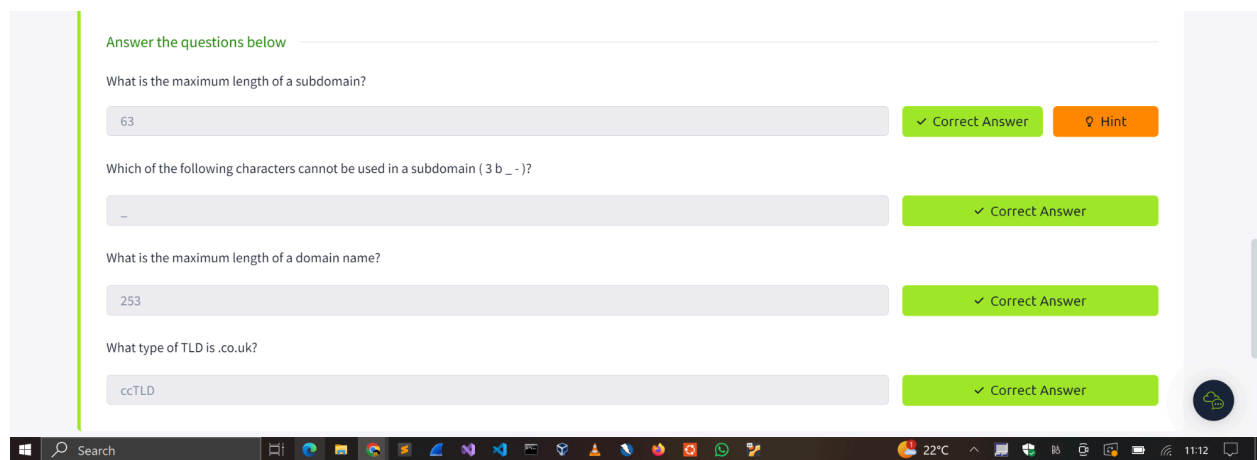
253

✓ Correct Answer

What type of TLD is .co.uk?

ccTLD

✓ Correct Answer



Record Types

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

The MX record because it resolves to the email server addresses.

b. What type of record handles IPv6 addresses?

The AAAA record resolves the IPv6 addresses.

Answer the questions below

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

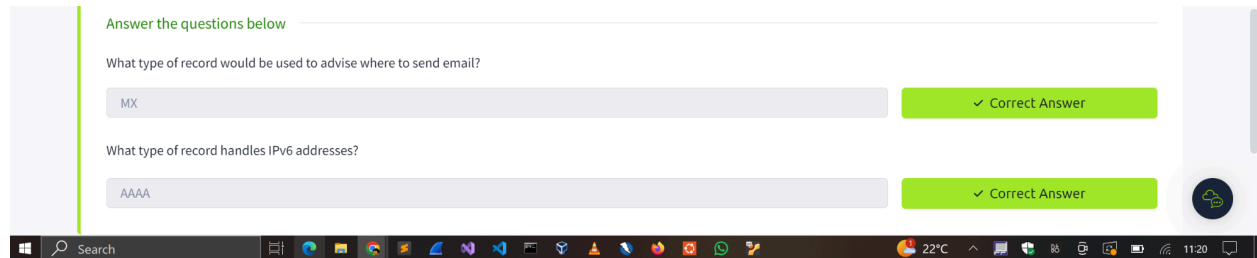
MX

✓ Correct Answer

What type of record handles IPv6 addresses?

AAAA

✓ Correct Answer



DNS Requests

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

Time To Live(TTL) indicates the duration in seconds that a DNS record should be cached.

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

Recursive DNS Server.

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

The Authoritative DNS server is responsible for storing all the DNS records.

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?

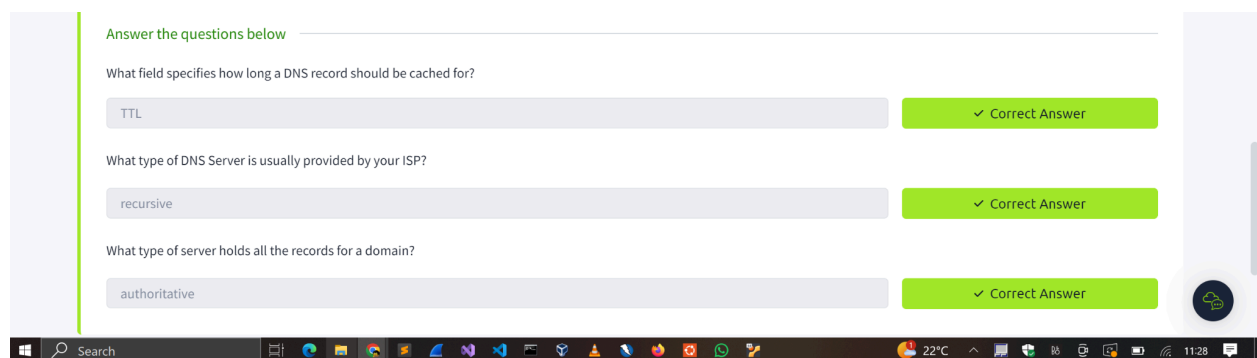
recursive

✓ Correct Answer

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

authoritative

✓ Correct Answer



Practical

- a. What is the CNAME of shop.website.thm?
shops.myshopify.com

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

```
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
```

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

- c. What is the numerical priority value for the MX record?
- A priority value in the MX record refers to the order in which mail servers should be used to deliver email to a domain. A lower value indicates higher priority.
- 30 was the priority value for the mail server alt4.aspmx.l.google.com.

- d. What is the IP address for the A record of www.website.thm?
10.10.10.10

Room progress (92%)

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?

10.10.10.10

Created by tryhackme

Room Type	Users in Room	Created
Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!	341,238	1114 days ago

Copyright TryHackMe 2018-2024

```
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

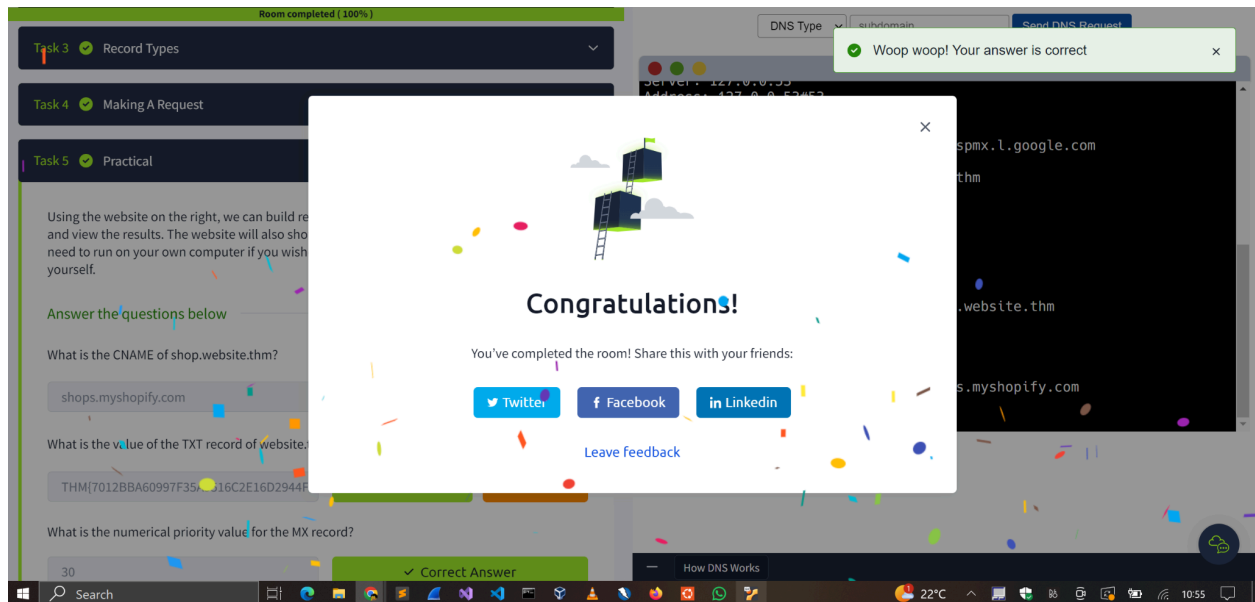
Non-authoritative answer:
website.thm mail exchanger = 30 alt4.aspmx.l.google.com

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

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

3. MODULE COMPLETION

<https://tryhackme.com/p/c1ph3rbnuk>



4. CONCLUSION

This assignment helped me learn about the different DNS records that exist, e.g., MX and A records, how DNS resolves domain names to their respective IP addresses, and the different hierarchies of a domain (Top-level domain, subdomains, etc.). It gave me a glimpse of how DNS works and as a security analyst, this is very crucial when it comes to DNS enumeration.