COURSE: CLOUD AND NETWORK SECURITY _C1_2025

STUDENT NAME: DIANA ROSE OGUDA

STUDENT NUMBER: CS-CNS09-25172

TUESDAY ,03 JUNE,2025

WEEK 3 ASSIGNMENT 1

TRYHACKME: DNS IN DETAIL- ASSIGNMENT REPORT

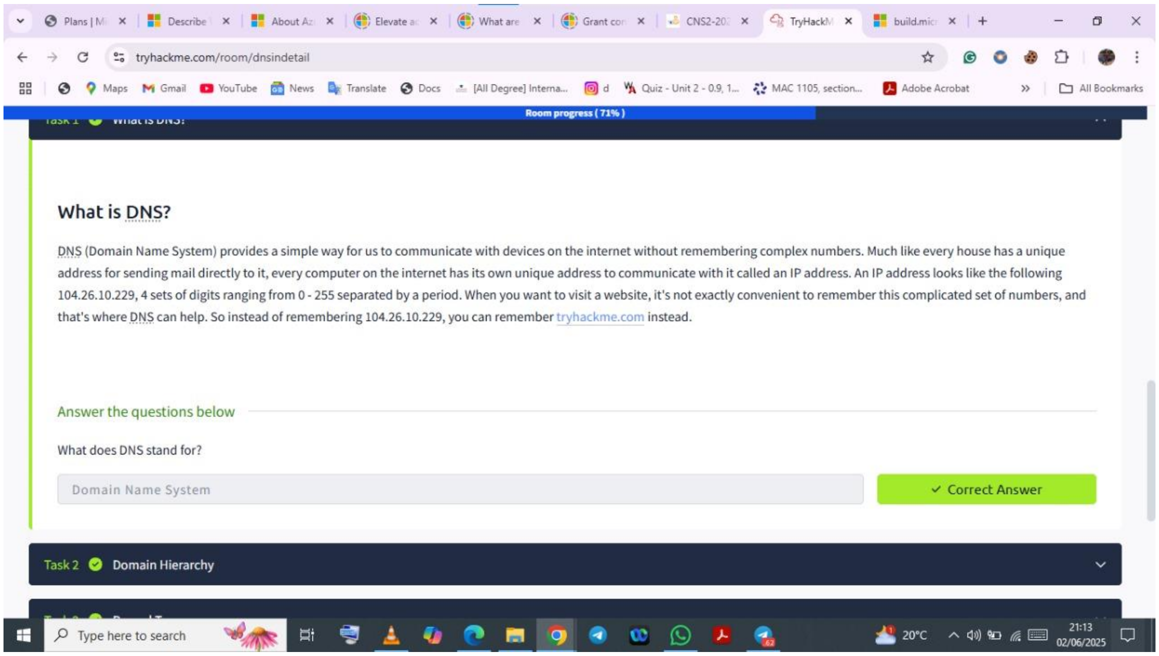
1. Introduction

The purpose of this report is to explore the 'DNS in Detail' module on TryHackMe. DNS (Domain Name System) plays a critical role in networking by translating human-readable domain names into machine-understandable IP addresses. This module aims to deepen understanding of how DNS works, its hierarchical structure, types of records used, and the process of making a DNS query. Through this learning experience, I engaged with interactive content and practical tasks to strengthen my foundational networking and cybersecurity knowledge.

2. Module Questions and Answers

Task 1: What is DNS?

Q1: What does DNS stand for?
Answer: Domain Name System



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

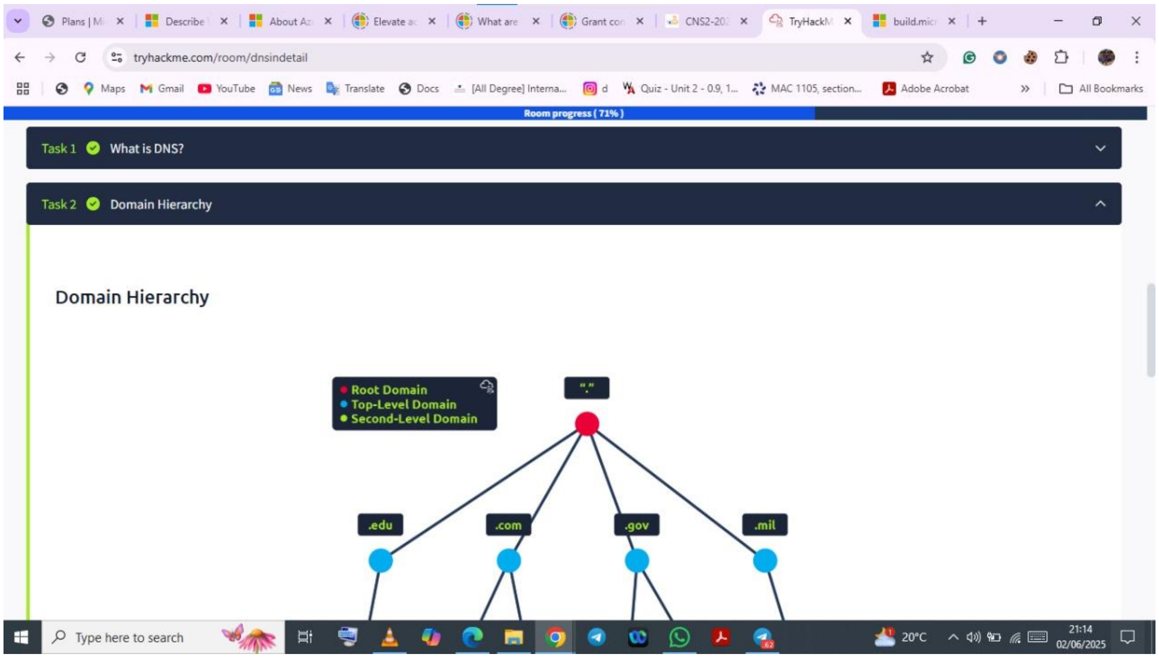
What does DNS stand for?

Domain Name System

✓ Correct Answer

The main purpose of DNS is to translate domain names like www.google.com into IP addresses that computers use to communicate.

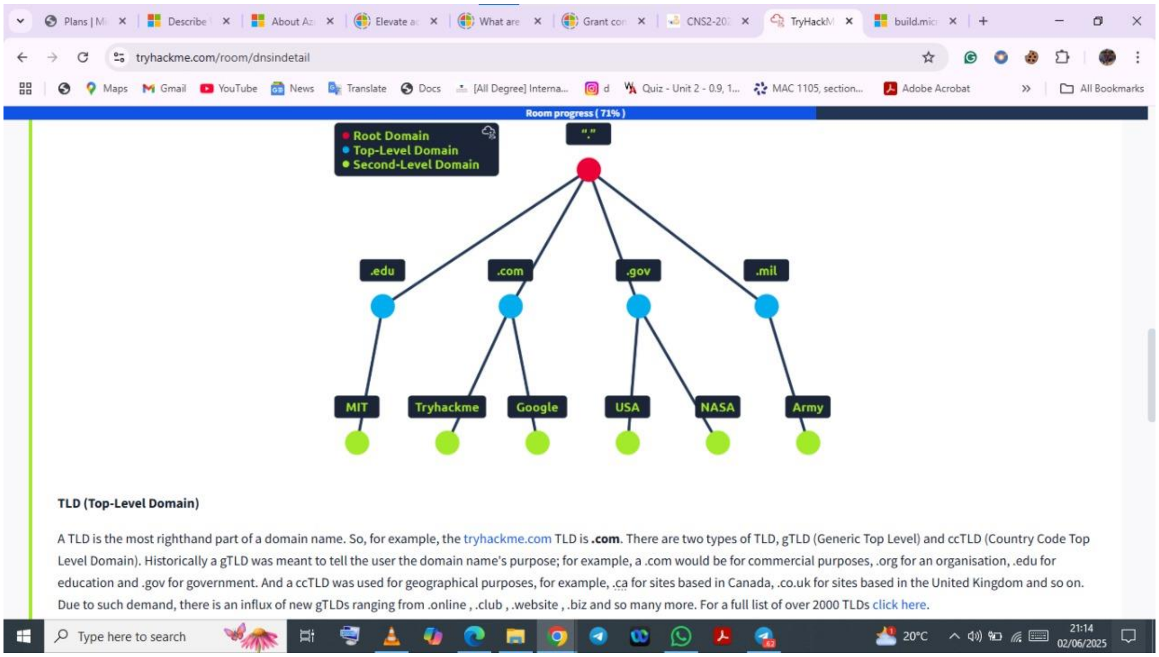
Task 2: Domain Hierarchy



Task 1 What is DNS?

Task 2 Domain Hierarchy

Domain Hierarchy

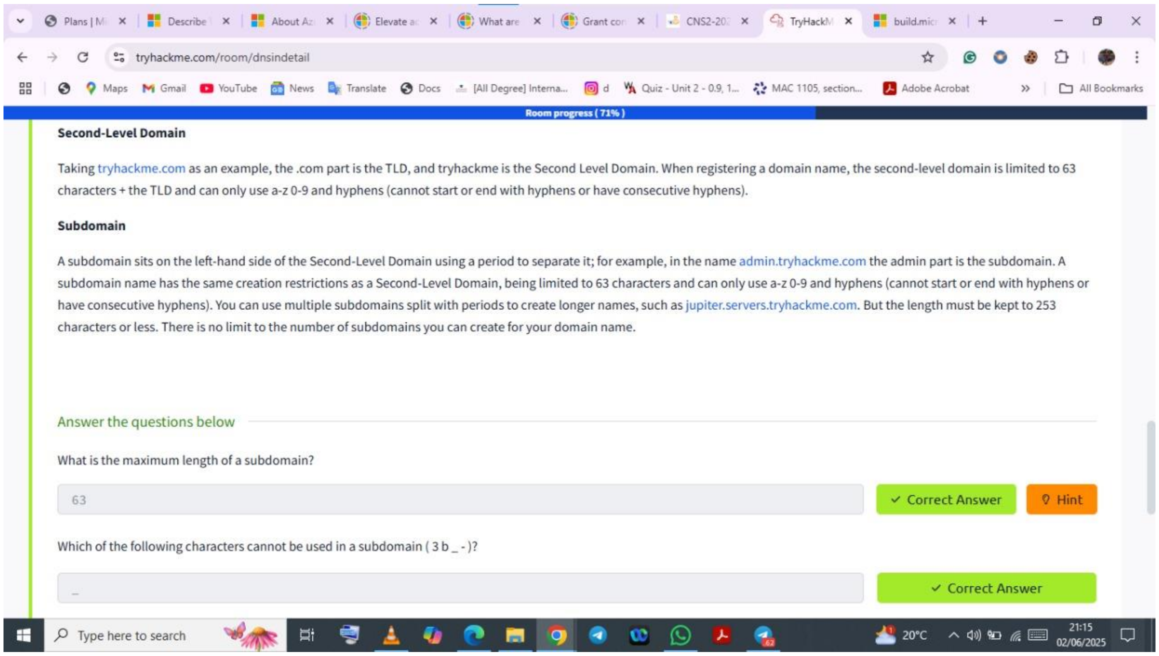


TLD (Top-Level Domain)

A TLD is the most righthand part of a domain name. So, for example, the tryhackme.com TLD is **.com**. There are two types of TLD, gTLD (Generic Top Level) and ccTLD (Country Code Top Level Domain). Historically a gTLD was meant to tell the user the domain name's purpose; for example, a .com would be for commercial purposes, .org for an organisation, .edu for education and .gov for government. And a ccTLD was used for geographical purposes, for example, .ca for sites based in Canada, .co.uk for sites based in the United Kingdom and so on. Due to such demand, there is an influx of new gTLDs ranging from .online , .club , .website , .biz and so many more. For a full list of over 2000 TLDs click here.

Q1: What is the maximum length of a subdomain?
Answer: 63

Q2: Which of the following characters cannot be used in a subdomain (3 - *)?
Answer: -



Second-Level Domain

Taking tryhackme.com as an example, the .com part is the TLD, and tryhackme is the Second Level Domain. When registering a domain name, the second-level domain is limited to 63 characters + the TLD and can only use a-z 0-9 and hyphens (cannot start or end with hyphens or have consecutive hyphens).

Subdomain

A subdomain sits on the left-hand side of the Second-Level Domain using a period to separate it; for example, in the name admin.tryhackme.com the admin part is the subdomain. A subdomain name has the same creation restrictions as a Second-Level Domain, being limited to 63 characters and can only use a-z 0-9 and hyphens (cannot start or end with hyphens or have consecutive hyphens). You can use multiple subdomains split with periods to create longer names, such as jupiter.servers.tryhackme.com. But the length must be kept to 253 characters or less. There is no limit to the number of subdomains you can create for your domain name.

Answer the questions below

What is the maximum length of a subdomain?

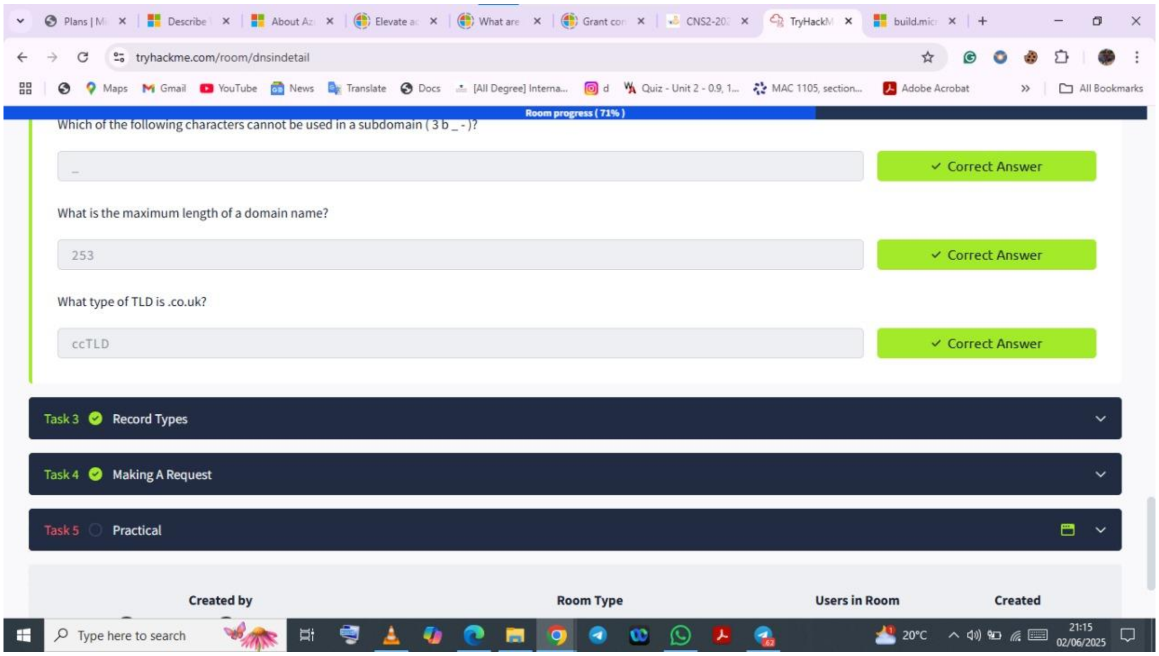
63 ✓ Correct Answer Hint

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

_ ✓ Correct Answer

Q3: What is the maximum length of a domain name?
Answer: 253

Q4: What type of TLD is .co.ke?
Answer: ccTLD



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

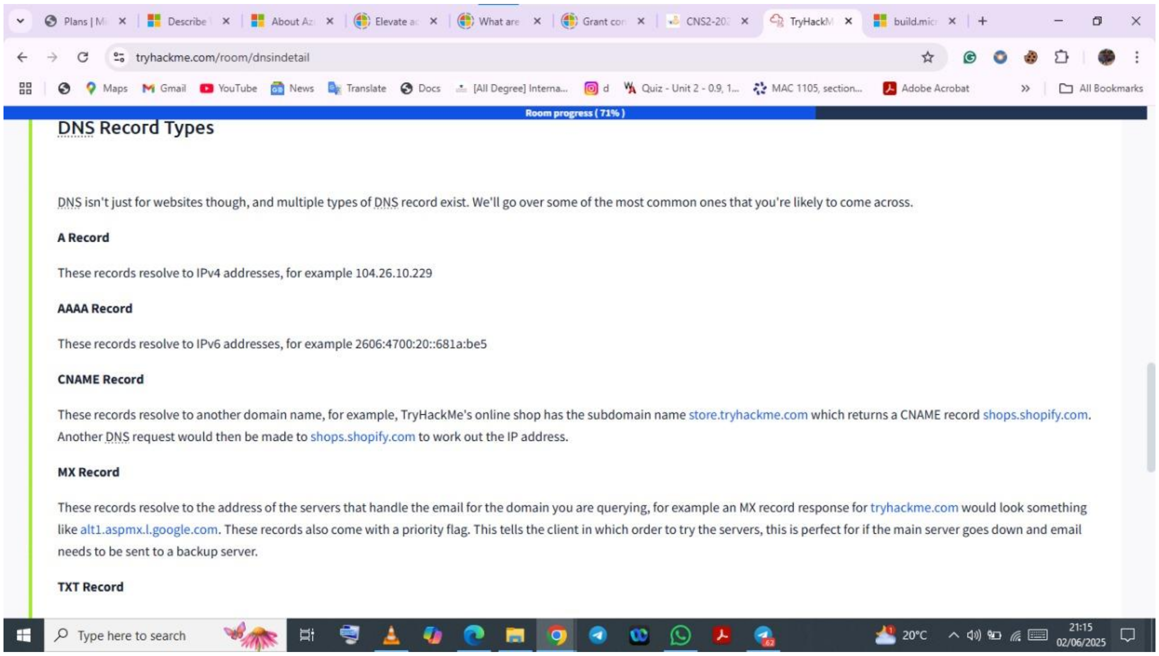
Task 3 ✓ Record Types

Task 4 ✓ Making A Request

Task 5 ○ Practical

Created by Room Type Users in Room Created

Task 3: Record Types



DNS 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.

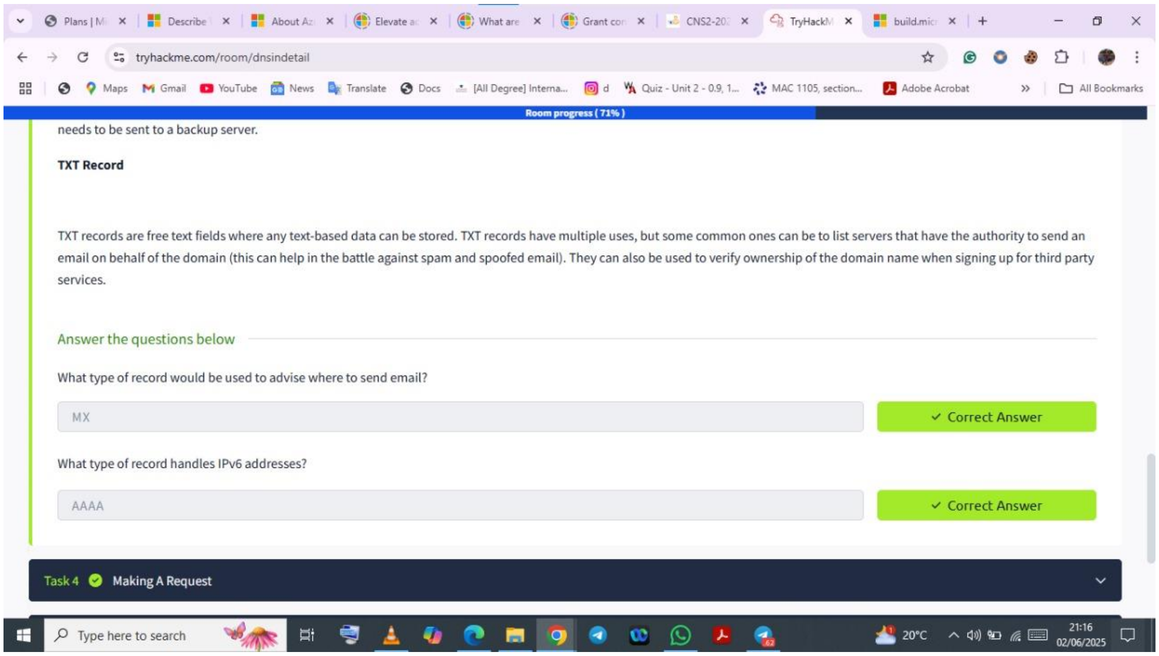
MX Record

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

Q1: What type of record would be used to advise where to send email?
Answer: MX

Q2: Which type of record handles IPv6 addresses?
Answer: AAAA Record



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?

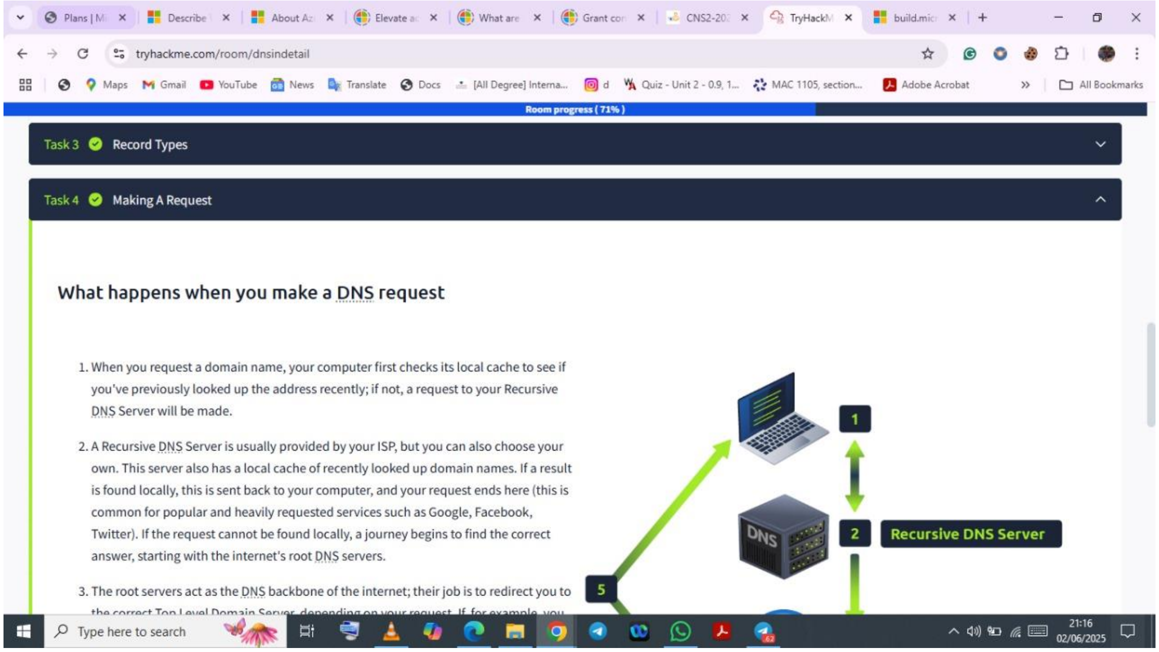
MX — ✓ Correct Answer

What type of record handles IPv6 addresses?

AAAA — ✓ Correct Answer

Task 4 ✓ Making A Request

Task 4: Making a Request

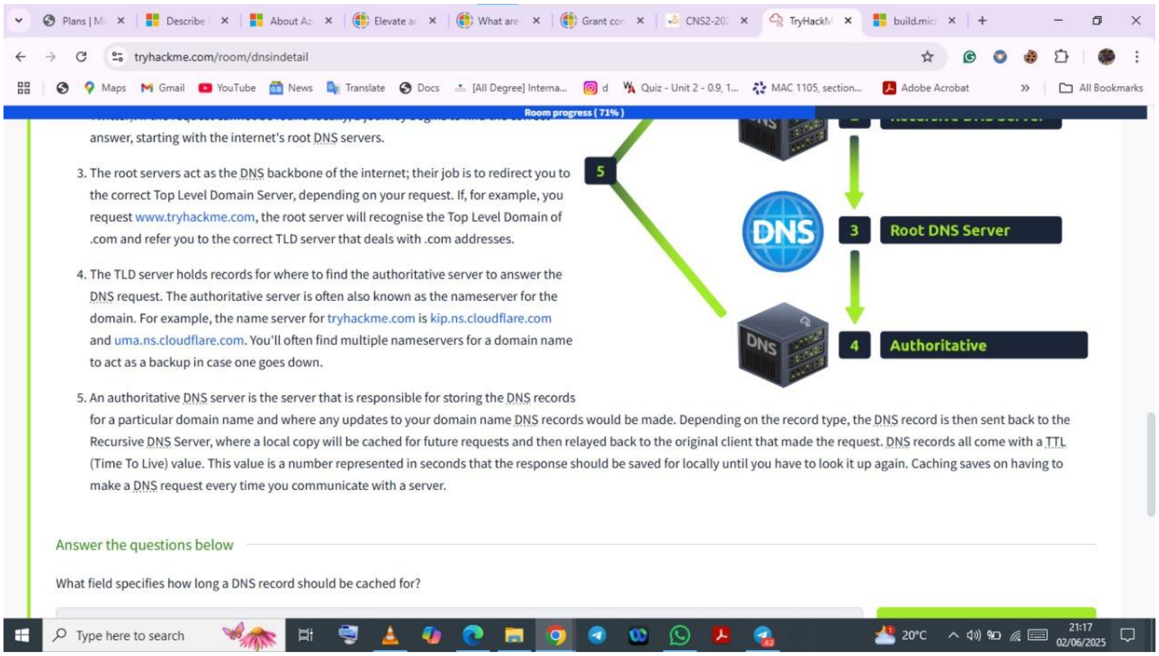


Task 3 Record Types

Task 4 Making A Request

What happens when you make a DNS request

1. When you request a domain name, your computer first checks its local cache to see if you've previously looked up the address recently; if not, a request to your Recursive DNS Server will be made.
2. A Recursive DNS Server is usually provided by your ISP, but you can also choose your own. This server also has a local cache of recently looked up domain names. If a result is found locally, this is sent back to your computer, and your request ends here (this is common for popular and heavily requested services such as Google, Facebook, Twitter). If the request cannot be found locally, a journey begins to find the correct answer, starting with the internet's root DNS servers.
3. The root servers act as the DNS backbone of the internet; their job is to redirect you to



answer, starting with the internet's root DNS servers.

3. The root servers act as the DNS backbone of the internet; their job is to redirect you to the correct Top Level Domain Server, depending on your request. If, for example, you request www.tryhackme.com, the root server will recognise the Top Level Domain of .com and refer you to the correct TLD server that deals with .com addresses.
4. The TLD server holds records for where to find the authoritative server to answer the DNS request. The authoritative server is often also known as the nameserver for the domain. For example, the name server for tryhackme.com is kip.ns.cloudflare.com and uma.ns.cloudflare.com. You'll often find multiple nameservers for a domain name to act as a backup in case one goes down.
5. An authoritative DNS server is the server that is responsible for storing the DNS records for a particular domain name and where any updates to your domain name DNS records would be made. Depending on the record type, the DNS record is then sent back to the Recursive DNS Server, where a local 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 be saved for locally until you have to look it up again. Caching saves on having to make a DNS request every time you communicate with a server.

Answer the questions below

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

Q1: What field specifies how long a DNS record should be cached for?

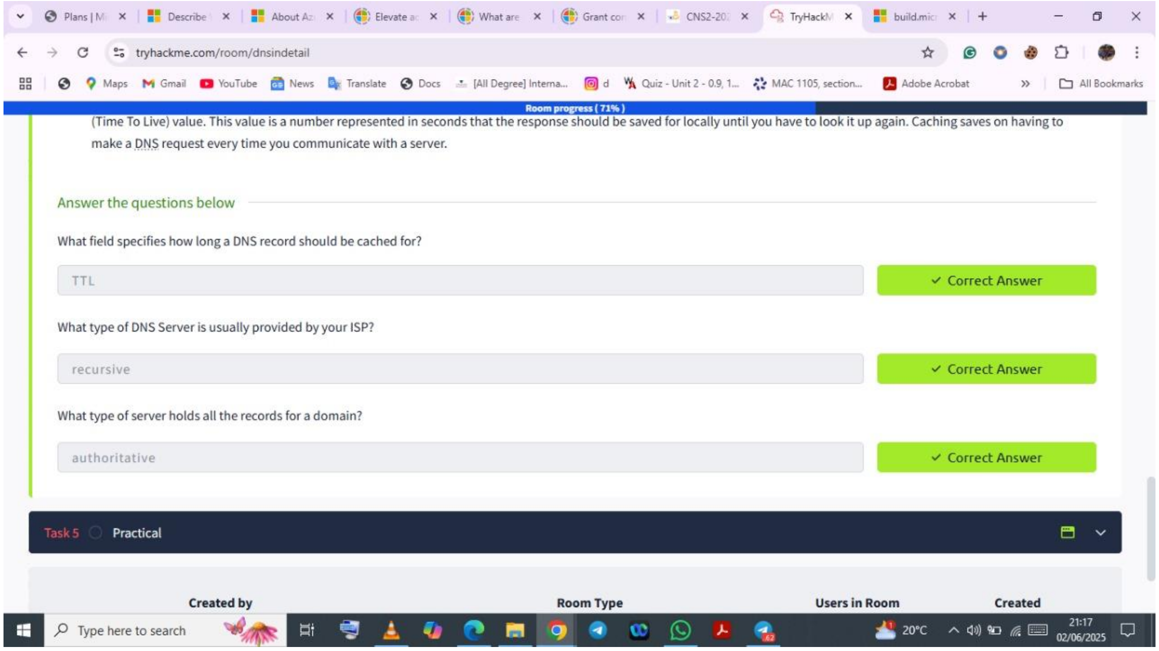
Answer: TTL

Q2: What type of DNS Server is usually provided by your ISP?

Answer: Recursive

Q3: What type of server holds all the records for a domain?

Answer: Authoritative



(Time To Live) value. This value is a number represented in seconds that the response should be saved for locally until you have to look it up again. Caching saves on having to make a DNS request every time you communicate with a server.

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?

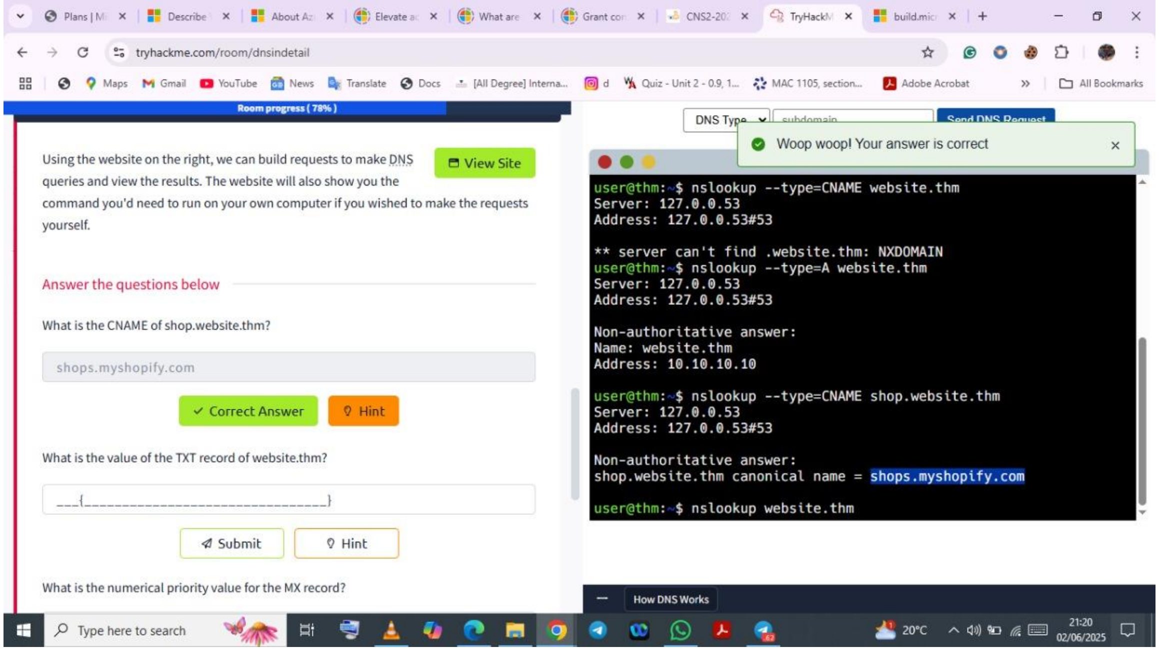
recursive ✓ Correct Answer

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

authoritative ✓ Correct Answer

Q1: What is the CNAME of shop.website.thm?

Answer: shops.myshopify.com



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.

View Site

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?

___{_______________________________}

Submit 💡 Hint

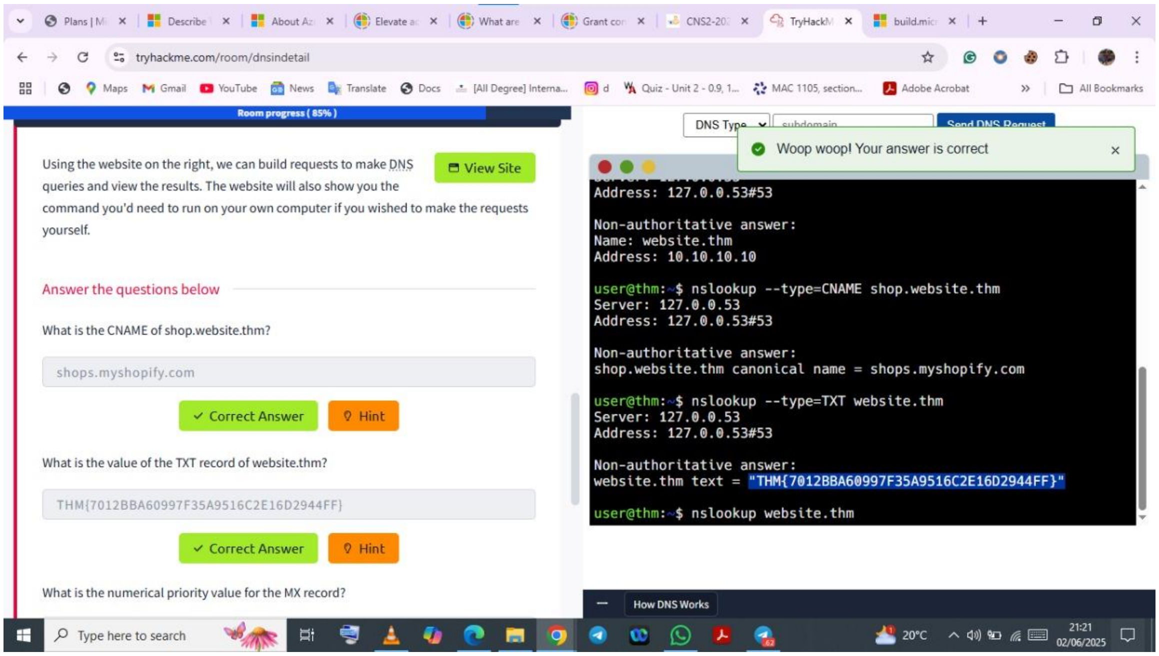
What is the numerical priority value for the MX record?

Woop woop! Your answer is correct ×

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

** server can't find .website.thm: NXDOMAIN
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

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
```

Q2: What is the value of the TXT record of website.thm?

Answer: THM{7012BBA60997F35A9516C2E16D2944FF}



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?

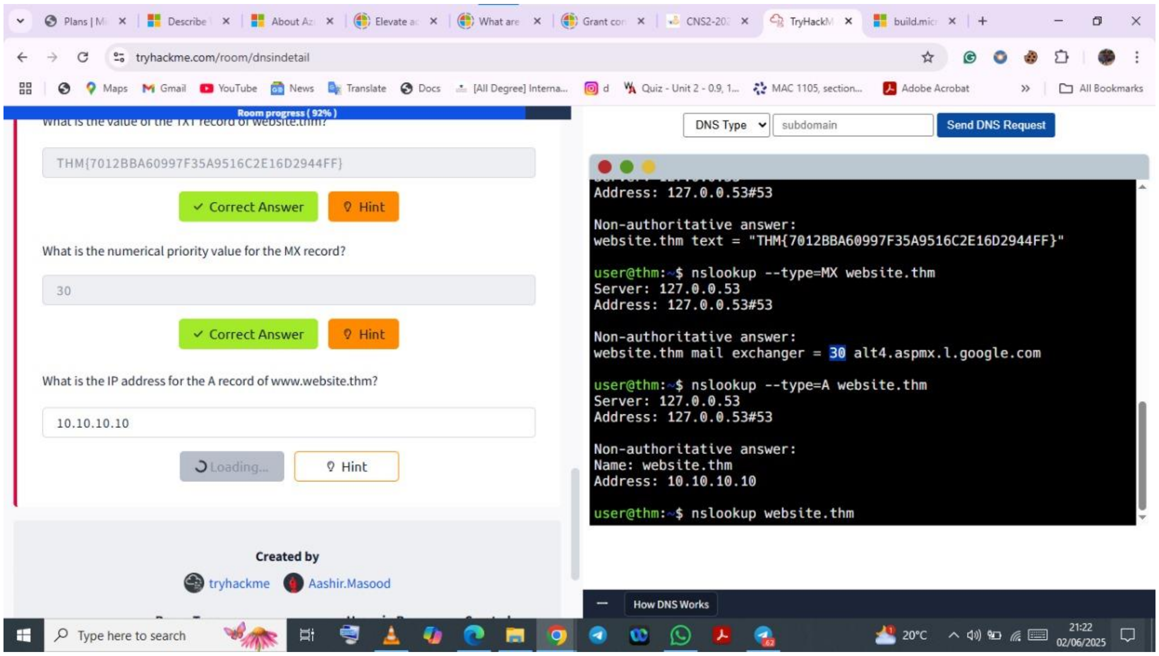
```
Address: 127.0.0.53#53

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

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
```

Q3: What is the numerical priority value for the MX record?

Answer: 30

Q4: What is the IP address for the record of www.website.thm?

Answer: 10.10.10.10



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

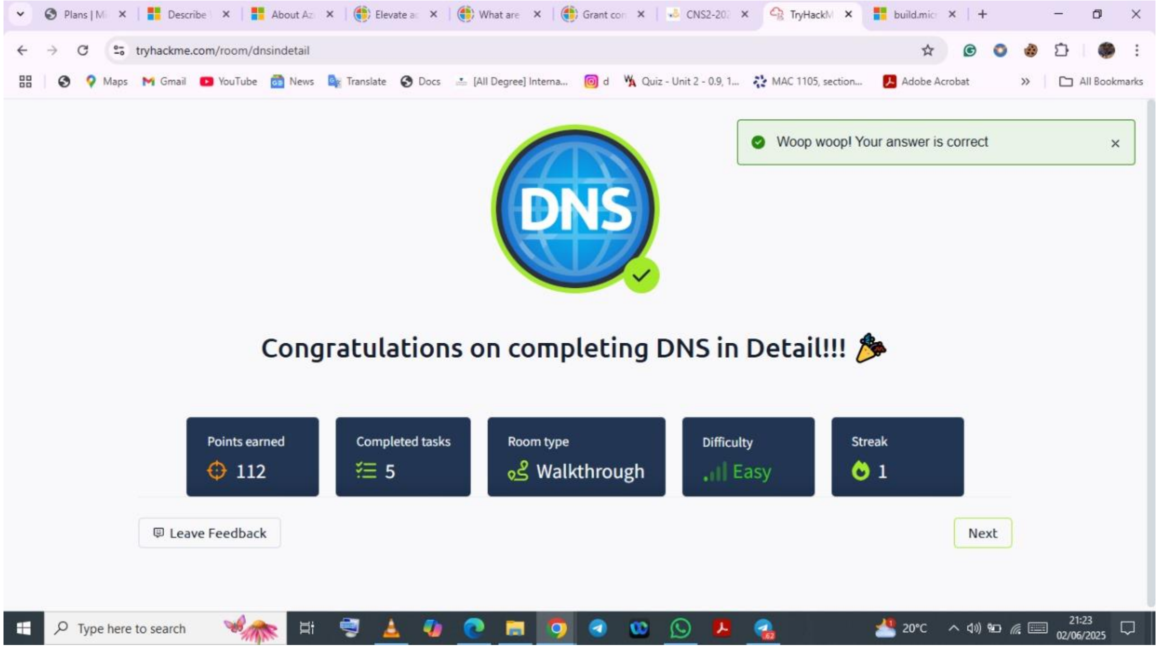
Loading... · Hint

Created by

tryhackme · Aashir.Masood

```
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

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

3. Completion Proof



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

4. Conclusion

This module provided an insightful deep dive into the Domain Name System. I learned about how DNS translates domain names to IP addresses, the structure of domain hierarchy, and the different types of DNS records and their uses. The hands-on nature of TryHackMe made learning engaging and interactive. This experience has strengthened my foundational knowledge in networking and cybersecurity.