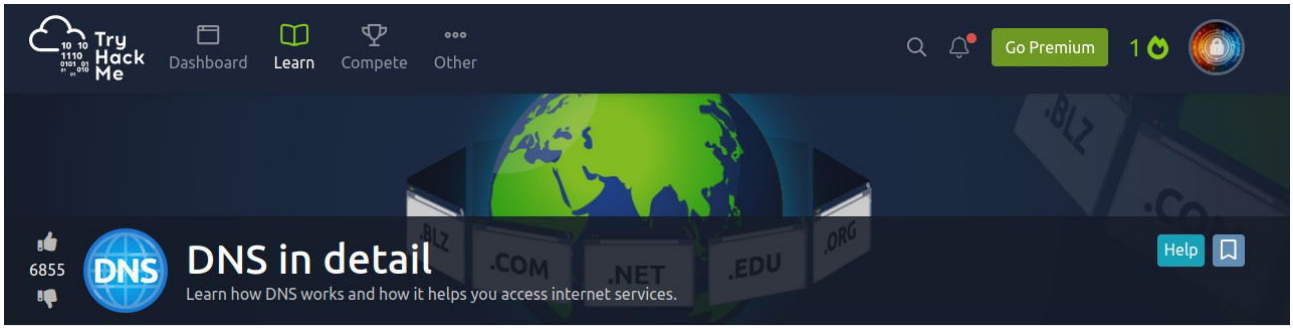
Eric Mwenda

DNS in Detail

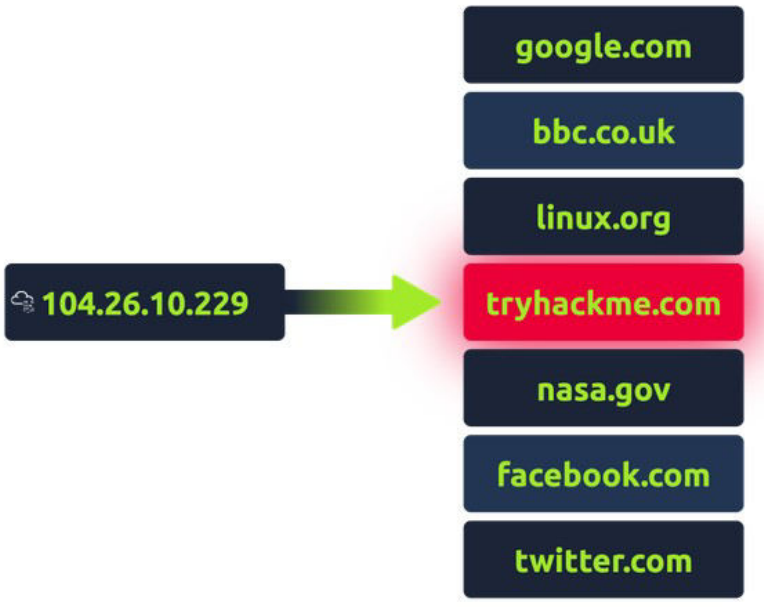
https://tryhackme.com/p/Ericm



What is DNS

In this room we began by explaining what DNS meant an what is its used.
DNS is an abbreviation foe **Domain Name System/Server**
DNS provides a simple way for us to communicate with devices on the internet without remembering complex numbers that is the IP addresses such as **10.10.23.45.**
In tryhackme they explain just as houses have unique house addresses in the case a mail needs to be sent the unique address is attaches to the mail, the same case is applied in every computer on the internet whereby each own unique address to communicate with it called an IP address.

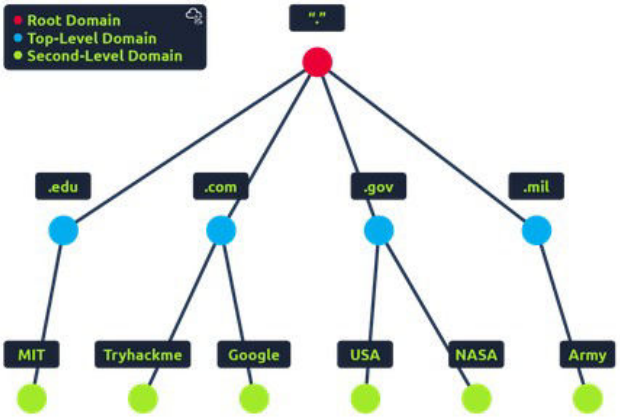
When we use DNS instead of remembering 104.26.10.229, you can remember tryhackme.com instead, which makes it more easier.



Answer the questions below

What does DNS stand for? **ANS: Domain Name System**

Domain Hierachy



In this room we looked into 3 domains:-
- Top-Level Domain.
- Second-Level Domain.
- Subdomain

TLD (Top-Level Domain)
A TLD is the most righthand/the furthest end to the right part of a domain name.
Example:- tryhackme.com the TLD is **.com**

There are two types of TLD:-
- gTLD (Generic Top Level)
- 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.

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.
The TLD and can only use a-z 0-9 and hyphens (cannot start or end with hyphens or have consecutive hyphens).

Second-Level Domain.

In our previous example tryhackme.com, **.com** was out **TLD,** therefore our **Second-Level Domain** will be **tryhackme.**
The second-level domain is limited to 63 characters.

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 also 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).

In this case to have a longer than 63 character subdomain, one can opt to use periods between the subdomains but not more than 253 characters.
Example:- **admin. jupiter.servers.tryhackme.com.**

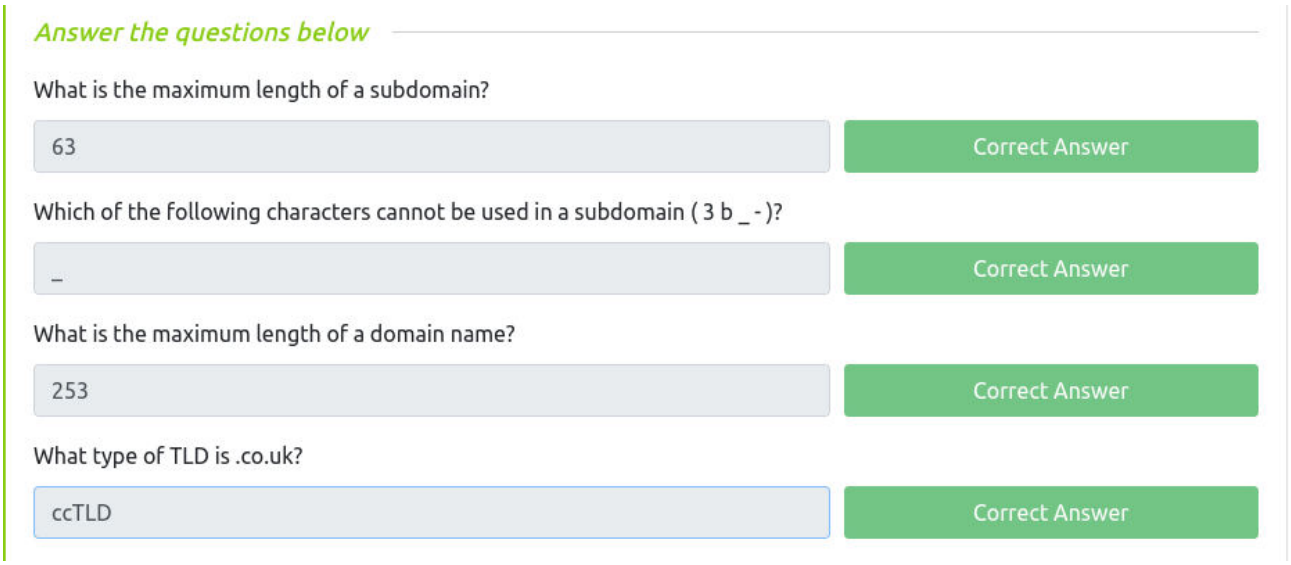
Answer the questions below

What is the maximum length of a subdomain? **ANS: 63**

Which of the following characters cannot be used in a subdomain (3 b _ -)? **ANS: _ (only a-z 0-9 and hyphens can be used)**

What is the maximum length of a domain name? **ANS: 253**

What type of TLD is .co.uk? **ANS: ccTLD**



DNS Record Types

DNS is not only for websites, DNS has multiple types of records that exist but in this room we covered a few of them.

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.

MX Record

For this record I found it interesting to the fact that it can offer other order to access the server, this can be a good vulnerability to check when attacking such targets.

MX 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.

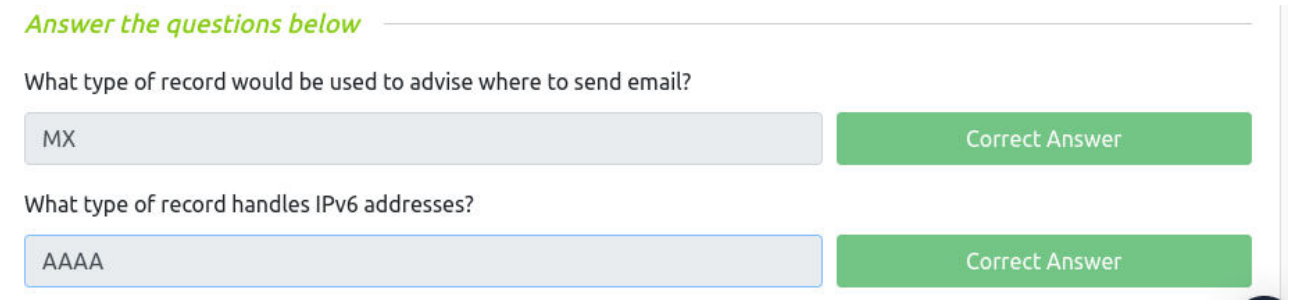
TXT Record

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.

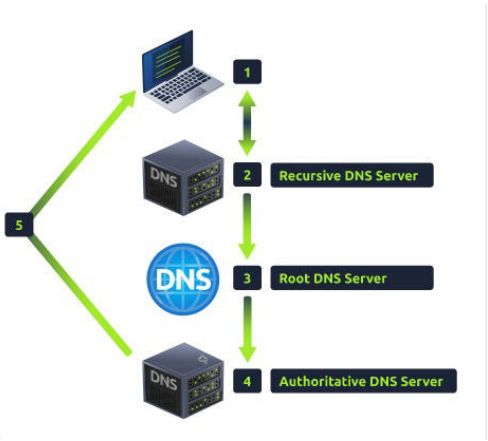
Answer the questions below

What type of record would be used to advise where to send email? **ANS: MX**

What type of record handles IPv6 addresses? **ANS: AAAA**



Making a Request.



What happens when you make a DNS request
In this section I went through the whole process that takes place from the time a DNS request is initiated and when a response is sent back.

Here is the whole process step by step:-
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.

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.

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.

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.

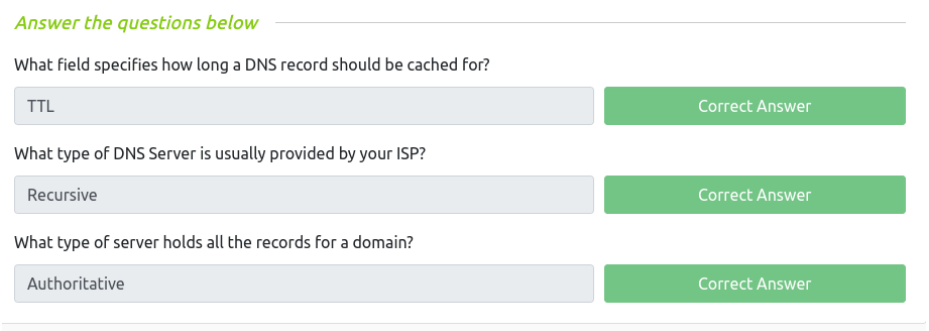
An authoritative DNS server is the server that is responsible for storing the DNS records for a particular domain name and where any updates to your domain name DNS records would be made. Depending on the record type, the DNS record is then sent back to the Recursive DNS Server, where a local copy will 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? **ANS TTL (Time To Live)**

What type of DNS Server is usually provided by your ISP? **ANS: Recursive**

What type of server holds all the records for a domain? **ANS: Authoritative**

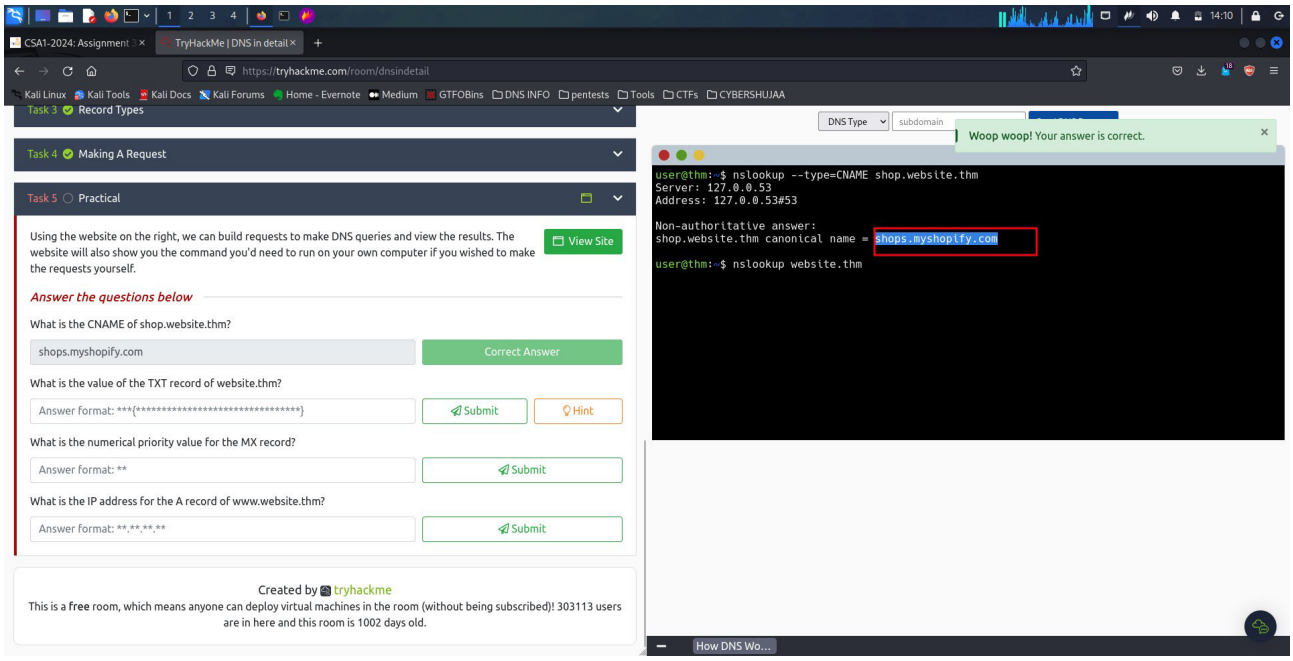


Practical.

On this section we compete with an exercise showcasing how to look at various records about a Domain Name. **ANS: shops.myshopify.com**

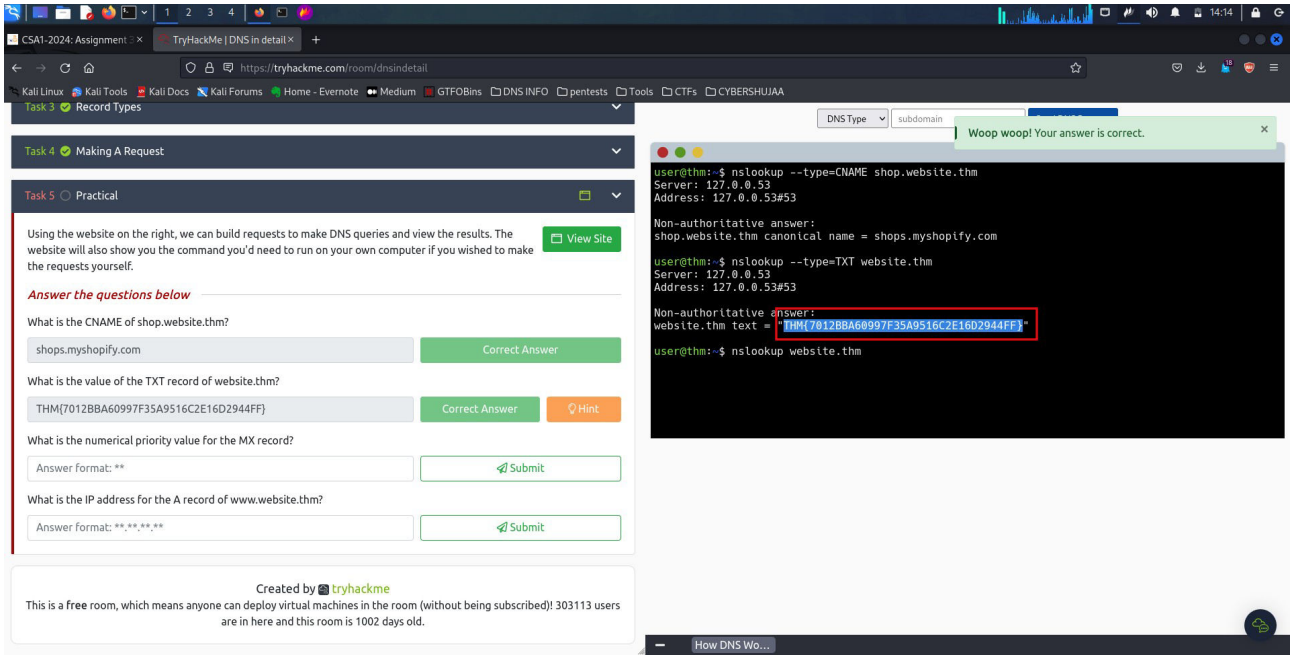
Answer the questions below

What is the CNAME of shop.website.thm? Command used:- **nslookup --type=CNAME shop.website.thm**

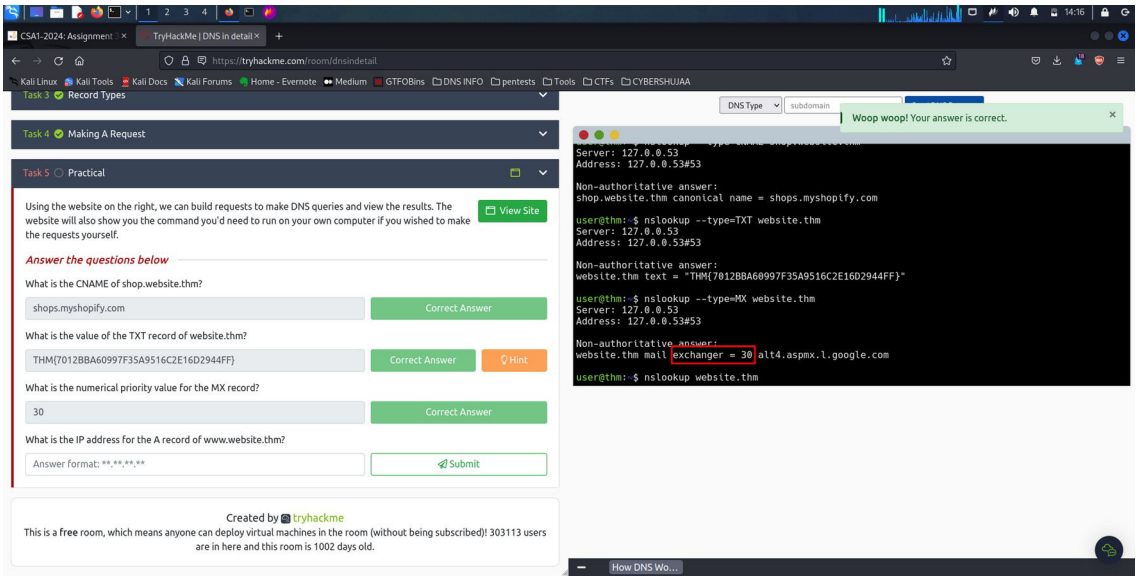


What is the value of the TXT record of website.thm? **ANS: THM{7012BBA60997F35A9516C2E16D2944FF}**

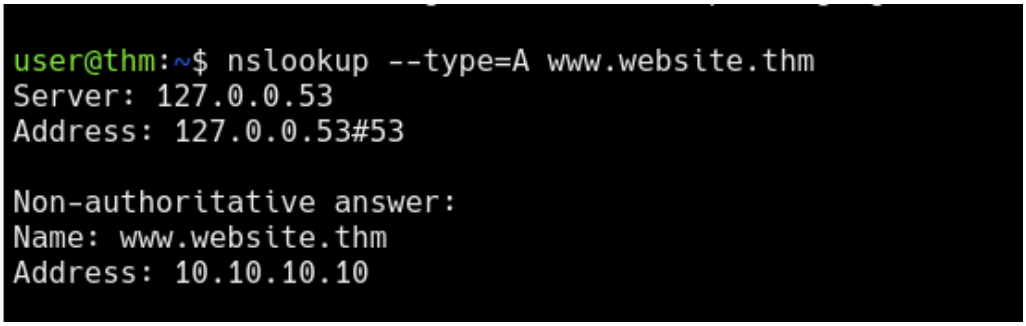
Command used:- **nslookup --type=TXT website.thm**



What is the numerical priority value for the MX record? **ANS: 30**
Command used:- **nslookup --type=MX website.thm**



What is the IP address for the A record of www.website.thm? **ANS: 10.10.10.10**
Command used:- **nslookup --type=A www.website.thm**



Conclusion.

The "DNS in Detail" room has offered me a comprehensive and insightful exploration of the Domain Name System (DNS) and its critical role in network infrastructure. With the step to step guidance into the various components of DNS, like for example the record types, I have gained the right skills I may need in the case I ever carry out a DNS assessment, with the help of this room I now know tools that I can use.
This room has also given me a deep understanding of how DNS functions and in the course of learning I was able to notice one vulnerability while checking for MX Records which may come with a priority flag to tell 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. I found this as a vulnerable point tho it has significant importance as well.

In conclusion the combination of theoretical knowledge and hands-on exercises has made it easier and faster to understand so am pleased to say I have gained something in the end.

Thank You.