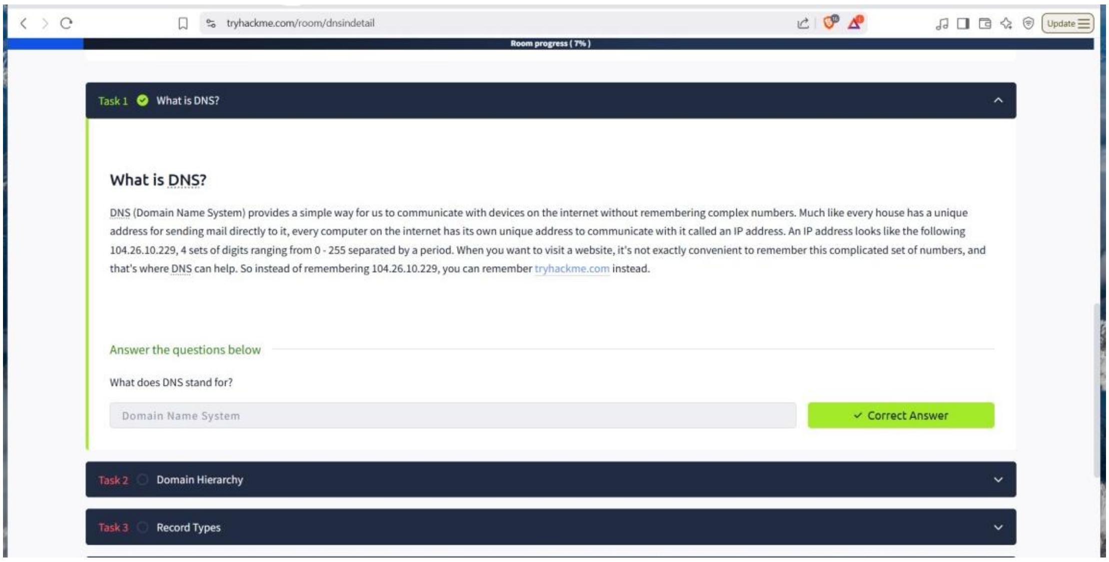
TryHackMe: DNS In Detail

Introduction

The Domain Name System (DNS) is one of the most critical components of modern networking, allowing users to interact with websites and online services using readable domain names instead of complex IP addresses. In this assignment, I explored the technical structure and operation of DNS through a TryHackMe learning module. The tasks covered everything from the DNS hierarchy and record types to how DNS queries are processed and resolved across various server levels. Practical hands-on exercises also helped reinforce theoretical knowledge by simulating real-world DNS lookups and analysis scenarios.

Task1

Covered the introduction to DNS which is 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.

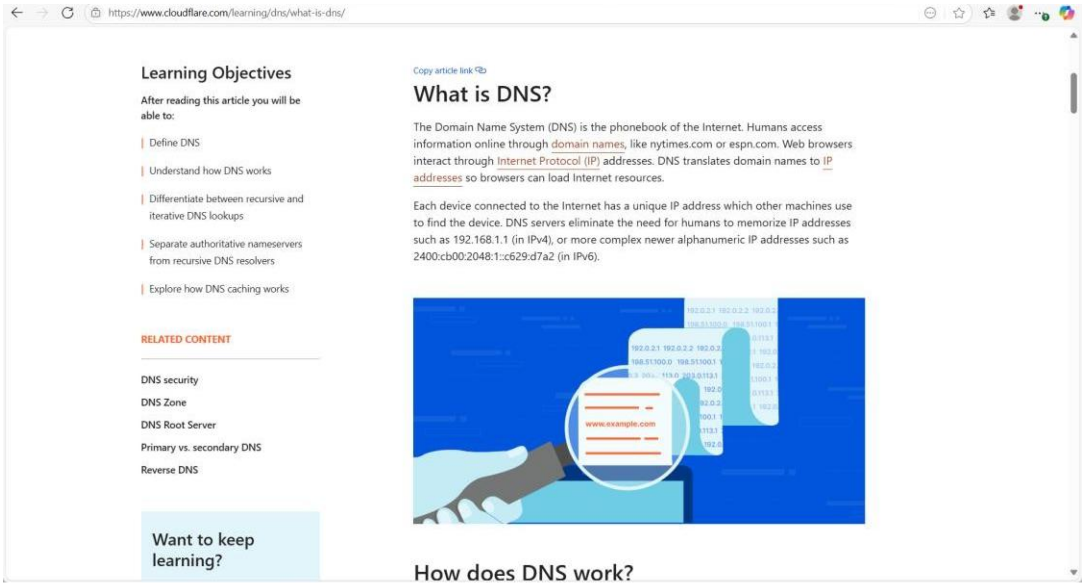
Answer the questions below

What does DNS stand for?

Domain Name System

Question

What does DNS Stand for? Domain Name system



Learning Objectives

After reading this article you will be able to:

- Define DNS
- Understand how DNS works
- Differentiate between recursive and iterative DNS lookups
- Separate authoritative nameservers from recursive DNS resolvers
- Explore how DNS caching works

RELATED CONTENT

- DNS security
- DNS Zone
- DNS Root Server
- Primary vs. secondary DNS
- Reverse DNS

Want to keep learning?

Copy article link

What is DNS?

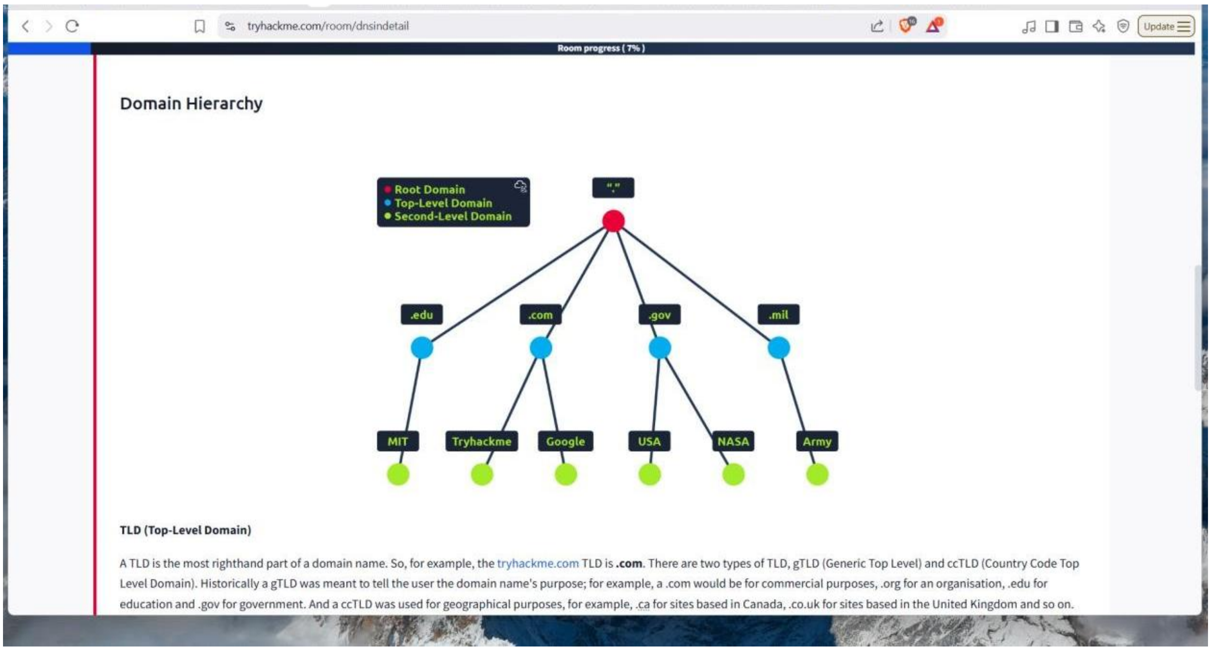
The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6).

How does DNS work?

Task 2: Domain Hierarchy

Covered the hierarchy of the DNS, From the root level , TLD and second level domain

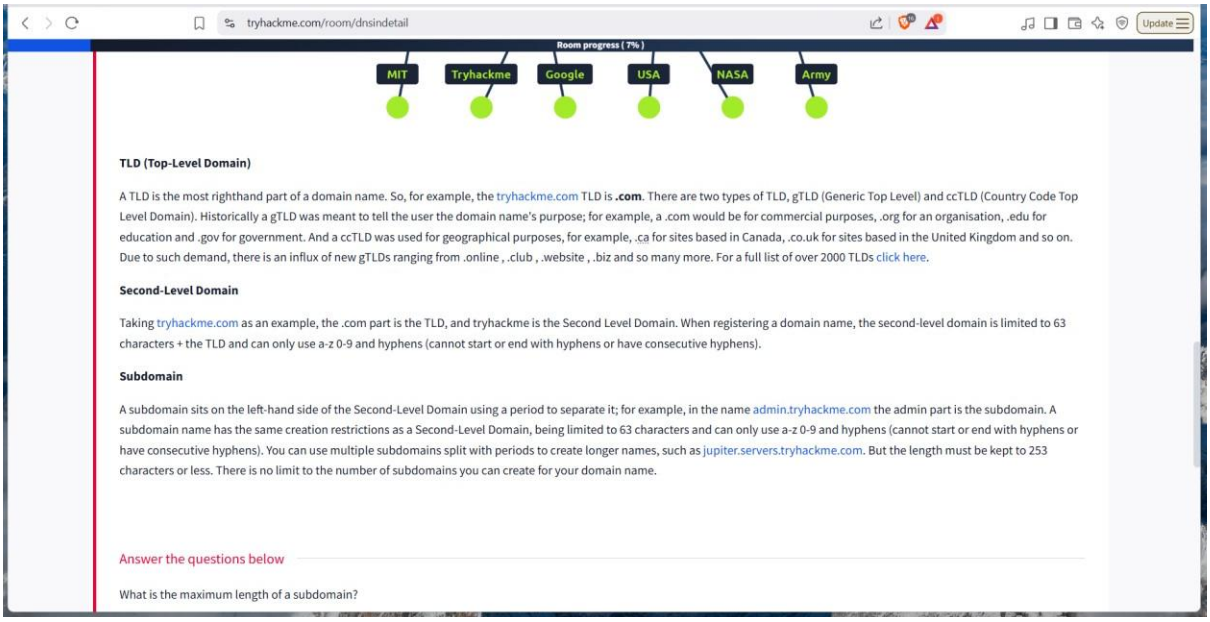


Domain Hierarchy

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.

It also covered details and length limitations of subdomains



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.

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?

Questions:

What is the maximum length of a subdomain? 63

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

subdomains cannot start or end with hyphens or have consecutive hyphens

What is the maximum length of a domain name? 253

What type of TLD is .co.uk? ccTLD

Reason: There are 2 types of TLD: gTLD(Generic TLD)eg .com, .org and ccTLD (country code TLD) eg .ke, .tz, .uk, .us

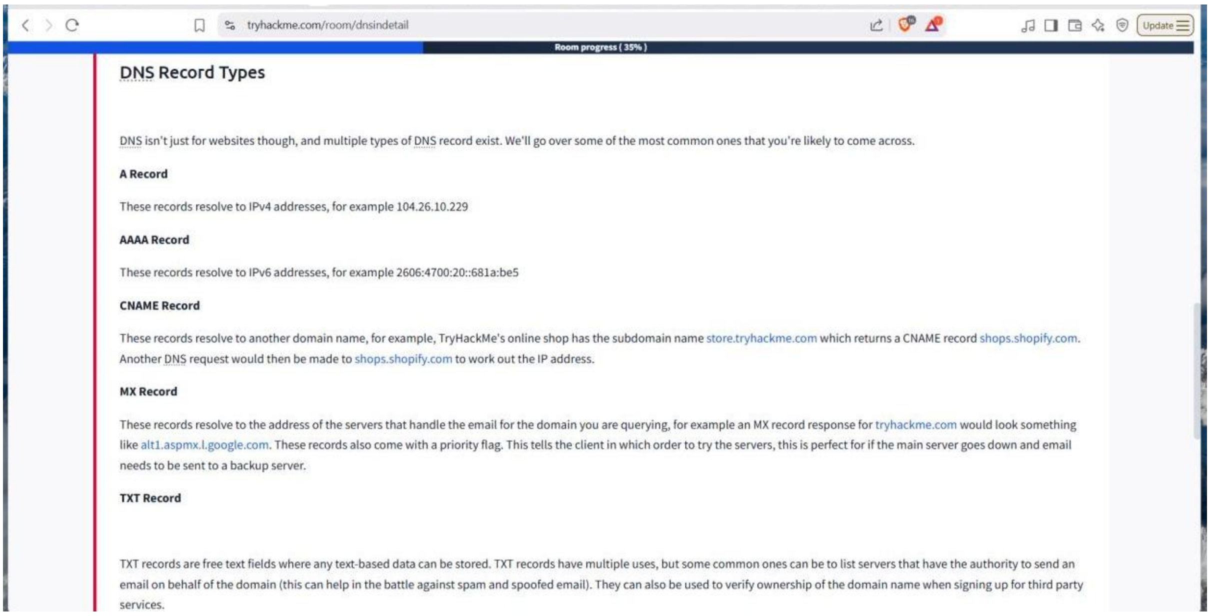
Task 3: DNS Record Types

The common DNS record types are :

1. A records: resolve to IPv4 addresses, for example 104.26.10.229
2. AAAA records: resolve to IPv6 addresses, for example 2606:4700:20::681a:be5
3. 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
4. CNAME records: resolve to another domain name, or rather show the alias of the domain being queried.

5. Txt records : 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.



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

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.

Questions

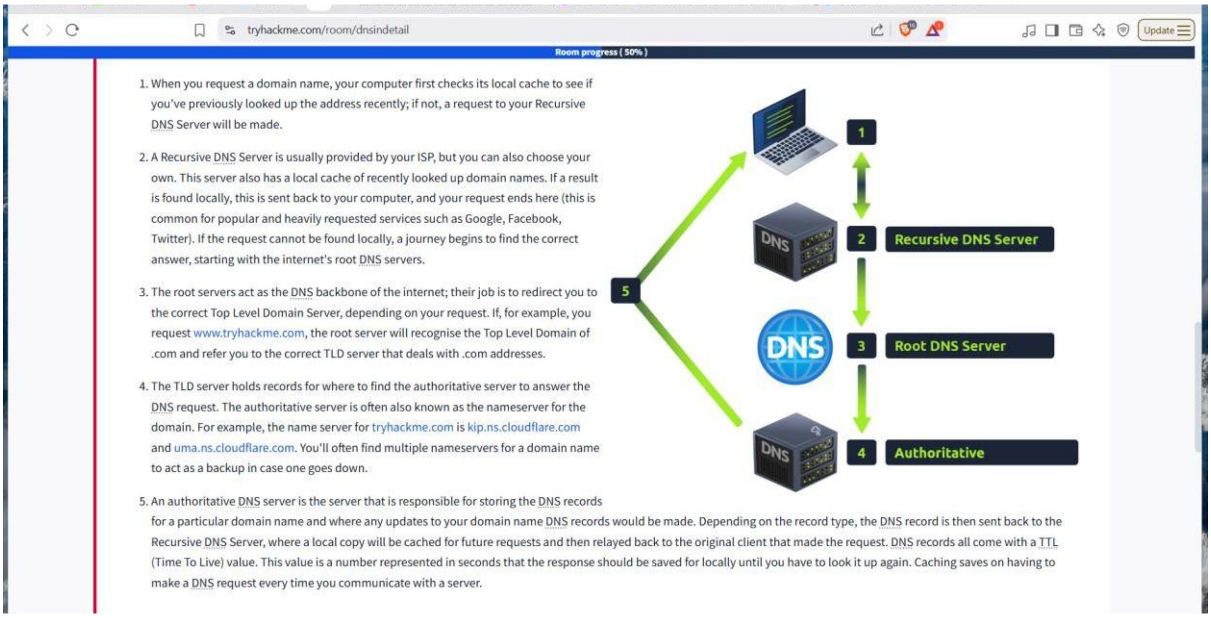
What type of record would be used to advise where to send email? Mx records What type of record handles IPv6 addresses? AAAA

Task 4: Making a Request

The root DNS acts as the backbone of the Internet.

Once a request is made, its first checked on local computer dns, if not found, it escalates to recursive dns(provided by isp) and if not found, the search now begins from the root DNS servers.

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.



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 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.

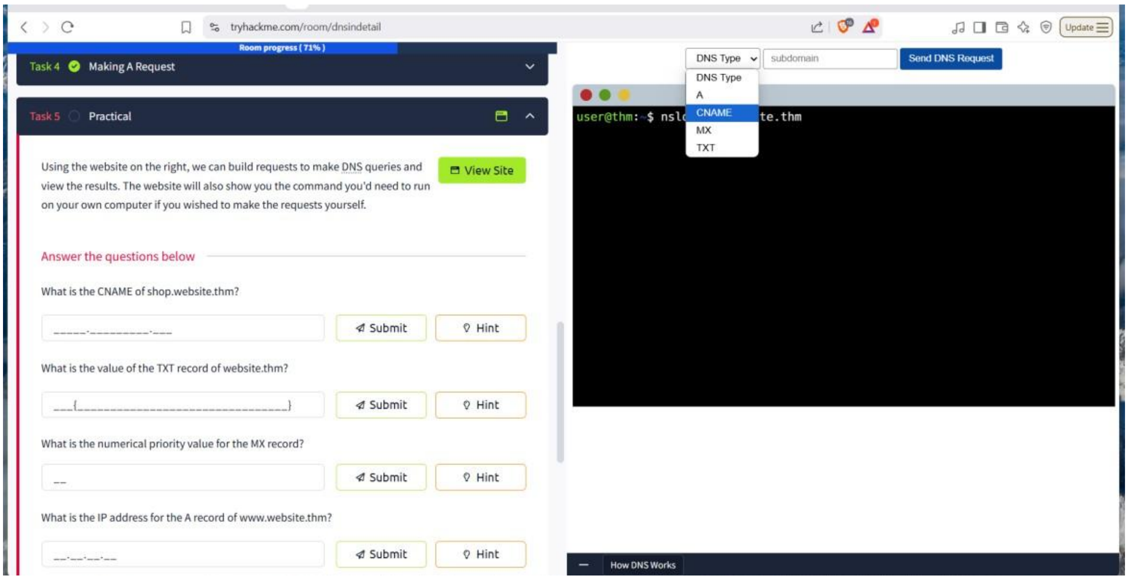
What field specifies how long a DNS record should be cached for? TTL

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

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

Task 5: Practical

Putting the theory into practice by trying to build requests to make DNS queries and view the results.



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?

_____.__________.___ Submit Hint

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

___{_______________________________} Submit Hint

What is the numerical priority value for the MX record?

__ Submit Hint

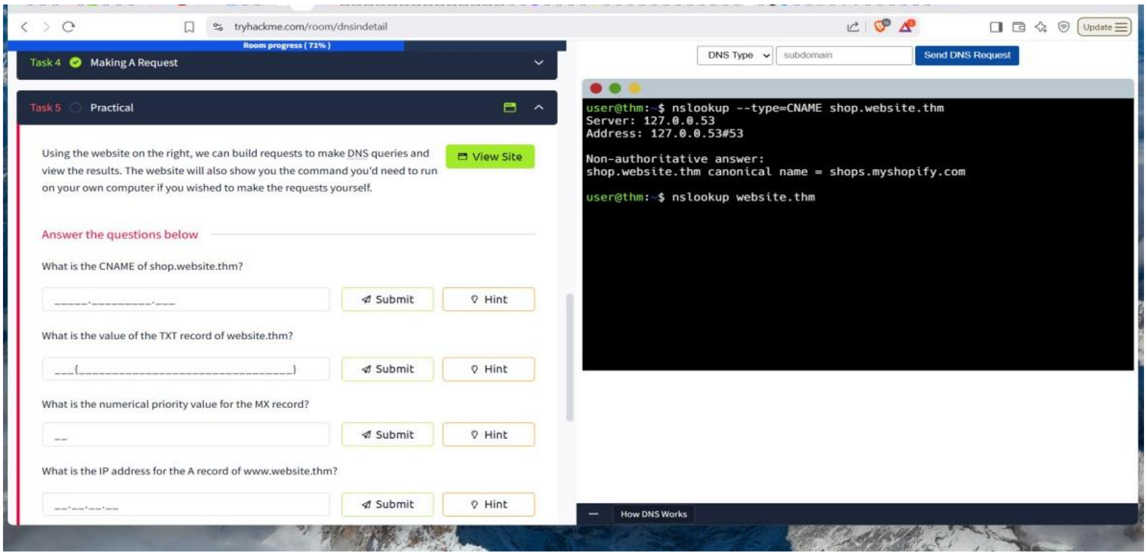
What is the IP address for the A record of www.website.thm?

__.__.__.__ Submit Hint

```
user@thm:~$ nsl      te.thm
```

Questions

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

Answer the questions below

What is the CNAME of shop.website.thm?

_____.__________.___

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

___{________________________________}

What is the numerical priority value for the MX record?

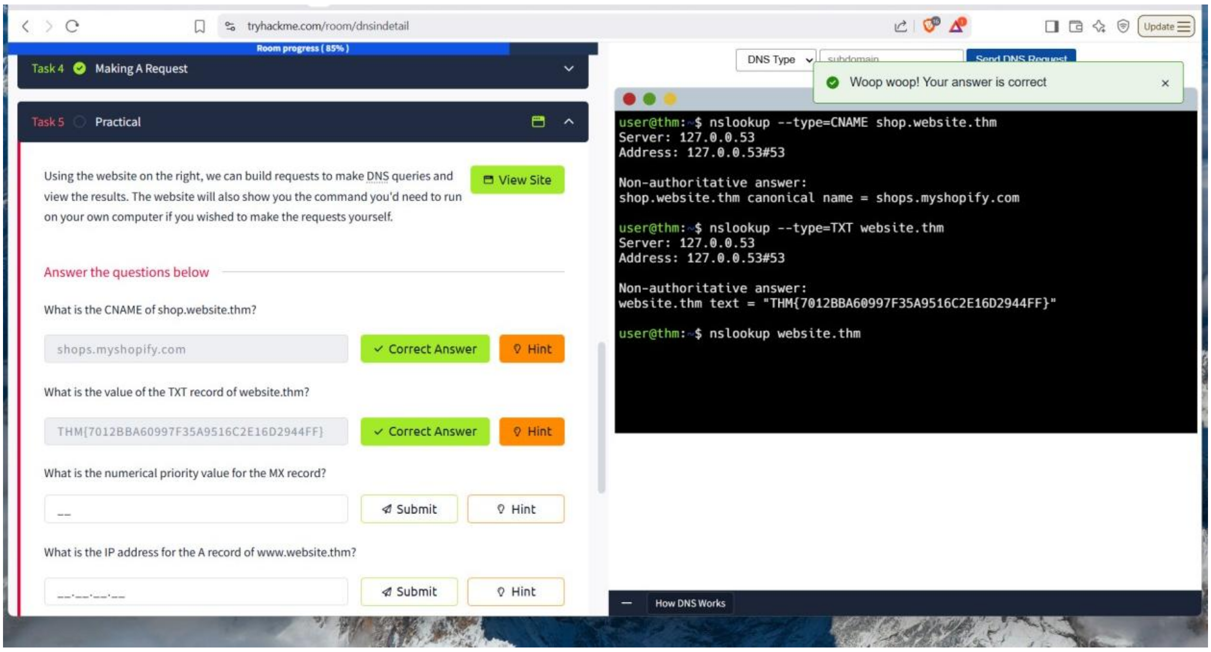
__

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

__.__.__.__

```
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
```

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



Woop woop! Your answer is correct

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

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

THM{7012BBA60997F35A9516C2E16D2944FF}

What is the numerical priority value for the MX record?

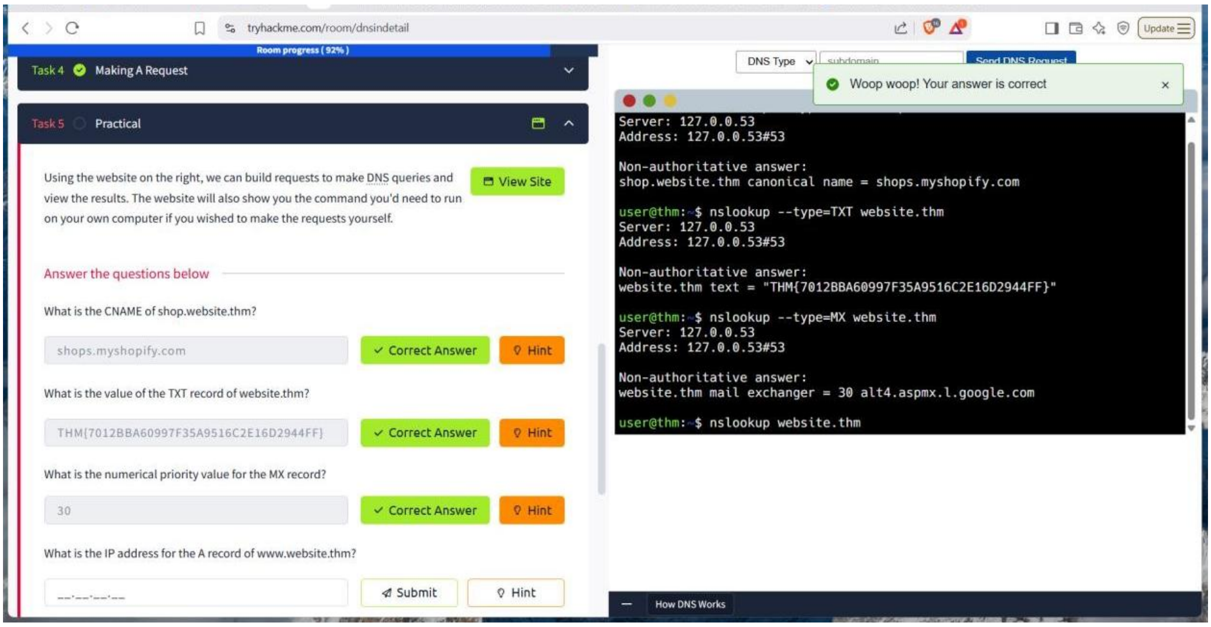
__

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

__.__.__.__

```
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
```

What is the numerical priority value for the MX record? 30



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.

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?

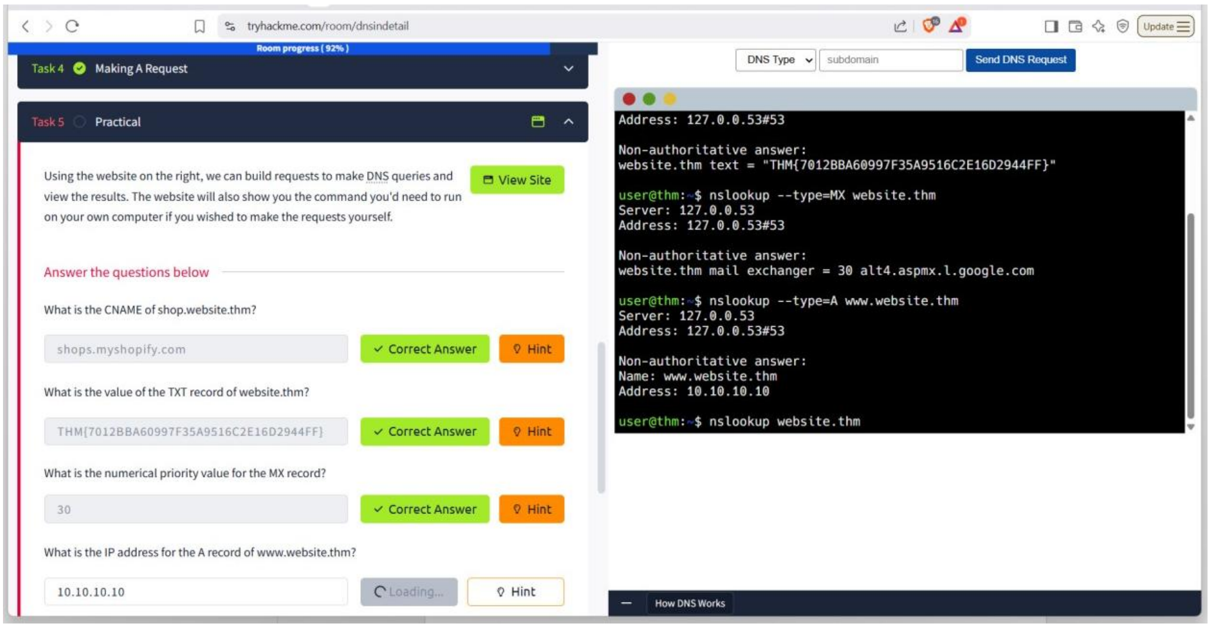
30

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

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

Since A records keep ipv4 address information



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.

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?

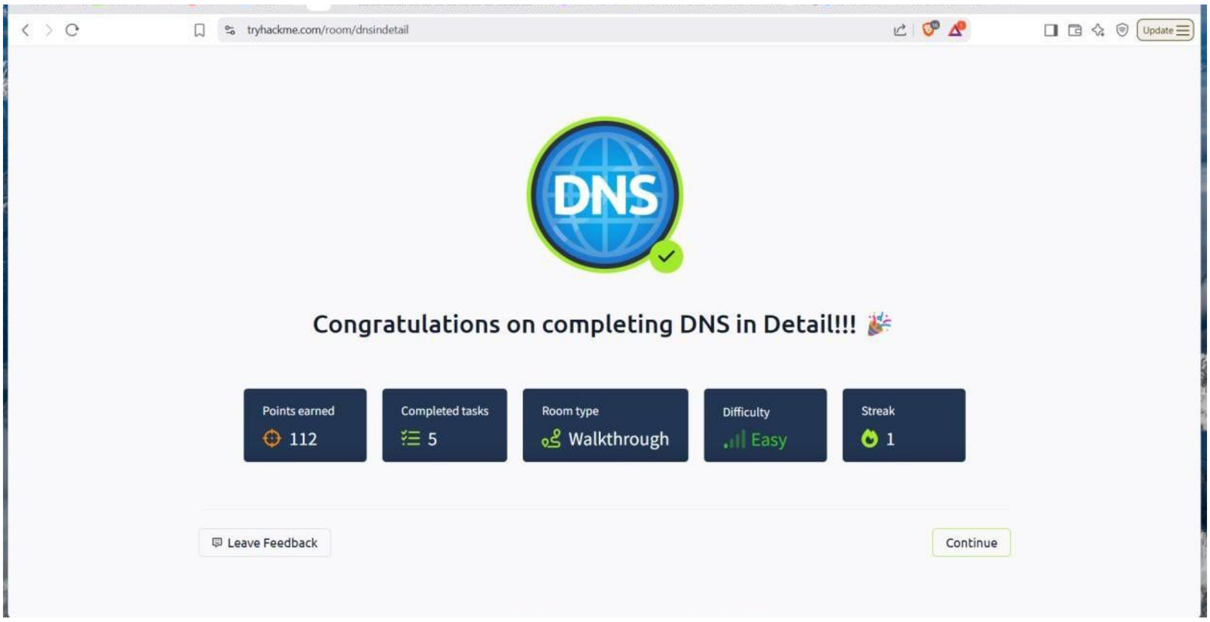
30

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

10.10.10.10

```
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 www.website.thm
Server: 127.0.0.53
Address: 127.0.0.53#53

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

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

Completion



Congratulations on completing DNS in Detail!!! 🎉

Points earned	Completed tasks	Room type	Difficulty	Streak
112	5	Walkthrough	Easy	1

Conclusion

This assignment provided valuable insight into the inner workings of DNS and its crucial role in internet communication. By progressing through both conceptual explanations and practical exercises, I now have a clearer understanding of how domains are resolved, how various record types function, and how recursive and authoritative servers interact. These concepts are foundational not just in networking but also in cybersecurity, where DNS is often used as both an investigation tool and an attack vector. The knowledge gained here builds a strong base for deeper exploration into areas like network analysis, threat detection, and secure infrastructure management.