

DNS in detail

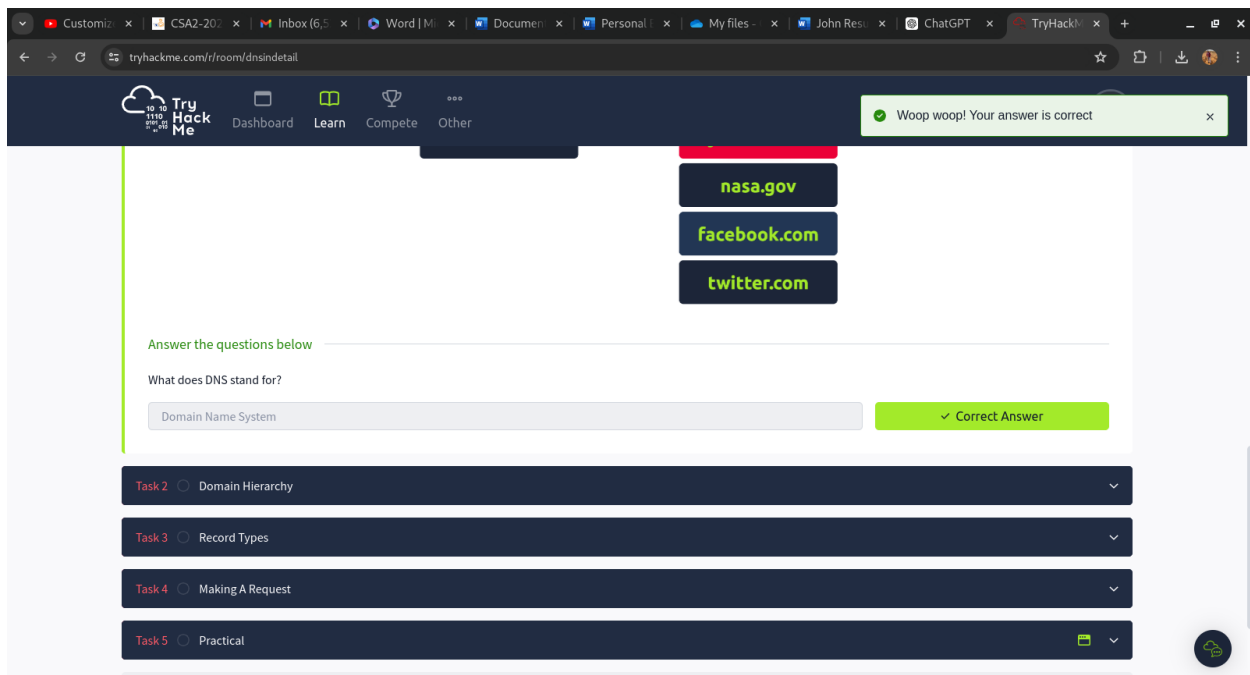
DNS (Domain Name System) provides a simple way for us to communicate with devices on the internet without remembering complex numbers.

This is 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 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.



cs-sa07-24019

John_Mbithi_Mutave

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?

MX ✓ Correct Answer

What type of record handles IPv6 addresses?

AAAA ✓ Correct Answer

Task 4 ○ Making A Request

Task 5 ○ Practical

Created by	Room Type	Users in Room	Created
...

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

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

Room progress (85%)

Answer the questions below

What is the CNAME of shop.website.thm?

shops.mysshopify.com

✓ Correct Answer

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

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

192.168.100.1

Submit

Created by

tryhackme

Room Type

Free Room. Anyone can deploy virtual machines in the room (without being subscribed!)

Users in Room

342,210

Created

1117 days ago

Copyright TryHackMe 2018-2024

[Twitter](#)[LinkedIn](#)[Discord](#)[Facebook](#)[YouTube](#)[Instagram](#)[Pinterest](#)

DNS Type

subdomain

Send DNS Request

Woop woop! Your answer is correct

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

** server can't find shop.website.thm.website.thm: NXDOMAIN
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.mysshopify.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
```

Room progress (92%)

Answer the questions below

What is the CNAME of shop.website.thm?

shops.mysshopify.com

✓ Correct Answer

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

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

192.168.100.1

Submit

Created by

tryhackme

Room Type

Free Room. Anyone can deploy virtual machines in the room (without being subscribed!)

Users in Room

342,210

Created

1117 days ago

Copyright TryHackMe 2018-2024

[Twitter](#)[LinkedIn](#)[Discord](#)[Facebook](#)[YouTube](#)[Instagram](#)[Pinterest](#)

DNS Type

subdomain

Send DNS Request

```
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.mysshopify.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
```

Custom x CSA2-2 x Inbox (6 x Word | x Docum x Person x My files x John Re x ChatGP x TryHack x DNS in Screenshot taken

tryhackme.com/r/room/dnsindetail

Room progress (78%)

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

What is the value of the TXT record of website.thm?
Answer format: ***** Submit Hint

What is the numerical priority value for the MX record?
Answer format: ** Submit

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

Created by tryhackme

Room Type Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!

Users in Room 342,210

Created 1117 days ago

Copyright TryHackMe 2018-2024

DNS Type subdomain Send DNS Request

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

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

How DNS Works

TryHackMe

DashboardLearnCompeteOther

Go Premium1

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

What is the maximum length of a domain name?

253

✓ Correct Answer

What type of TLD is .co.uk?

ccTLD

✓ Correct Answer

Task 3Record Types

Task 4Making A Request

Room completed (100%)

DNS Type

subdomain

Send DNS Request

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

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

THM[T012BBA60997F35A9516C2E16D2944FF]

✓ Correct Answer

Hint

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?

10.10.10.10

✓ Correct Answer

Created by

tryhackme

Room Type

Free Room. Anyone can deploy virtual machines in the room (without being subscribed!)

Users in Room

342,210

Created

1117 days ago

Copyright TryHackMe 2018-2024

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

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

Room progress (85%)

Answer the questions below

What is the CNAME of shop.website.thm?

shops.myshopify.com

✓ Correct Answer

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

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

192.168.100.1

Submit

Created by

tryhackme

Room Type

Free Room. Anyone can deploy virtual machines in the room (without being subscribed!)

Users in Room

342,210

Created

1117 days ago

Copyright TryHackMe 2018-2024

DNS Type

subdomain

Send DNS Request

Woop woop! Your answer is correct

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

** server can't find shop.website.thm.website.thm: NXDOMAIN
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=TEXT 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
```

Room progress (78%)

Answer the questions below

What is the CNAME of shop.website.thm?

shops.myshopify.com

✓ Correct Answer

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

Answer format: ****

Submit

Hint

What is the numerical priority value for the MX record?

Answer format: **

Submit

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

192.168.100.1

Submit

Created by

tryhackme

Room Type

Free Room. Anyone can deploy virtual machines in the room (without being subscribed!)

Users in Room

342,210

Created

1117 days ago

Copyright TryHackMe 2018-2024

DNS Type

subdomain

Send DNS Request

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

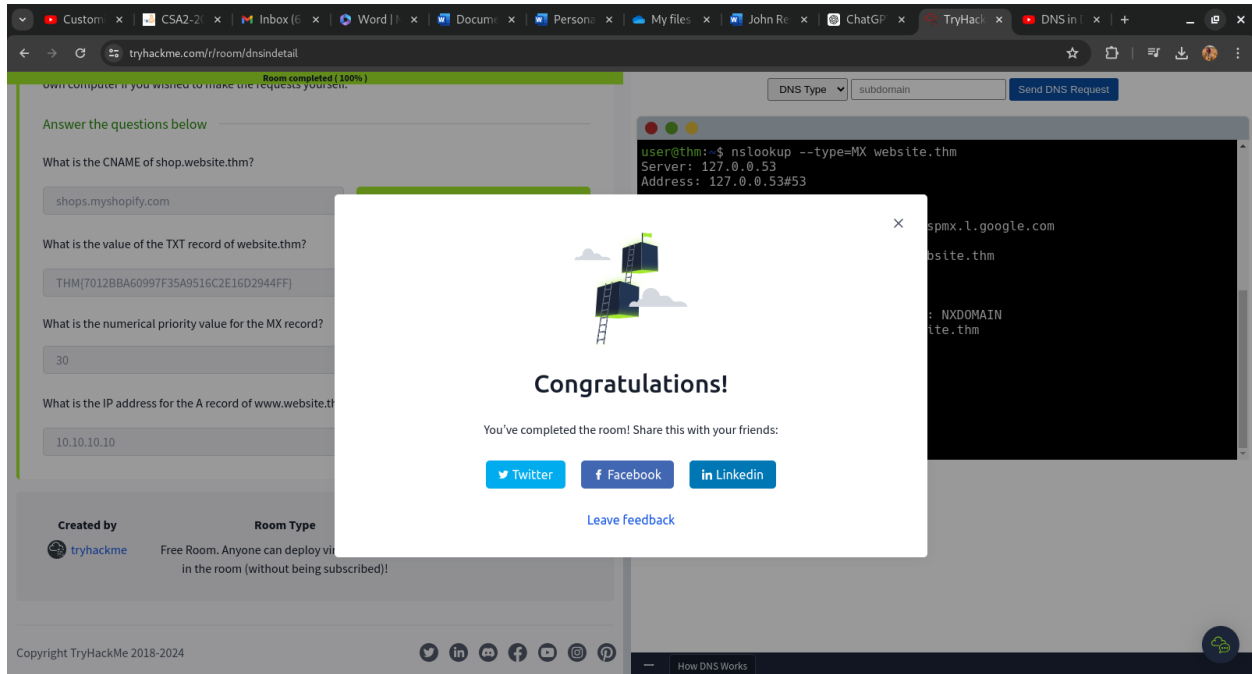
** server can't find shop.website.thm.website.thm: NXDOMAIN
user@thm:~$ nslookup --type=CNAME shop.website.thm
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
shop.website.thm canonical name = shops.myshopify.com

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

cs-sa07-24019

John_Mbithi_Mutave



Shareable link - www.tryhackme.com/r/room/dnsindetail

Conclusion

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.