Week 3 Assignment 1

Course: Cloud and Network Security - C1-2026

Student Name: Bussllus Bertrand

Student Number: CS-CNS11-26004

Tuesday, February 3, 2026

Week three Assignment one:

Class exercise: DNS in Detail

Contents

Introduction

The **Domain Name System (DNS)** acts as a critical infrastructure for internet communication, providing a streamlined method for users to connect with devices without memorizing complex numerical identifiers. Functioning similarly to a digital address book, DNS translates human-readable domain names (such as google.com) into the specific **IP addresses** (such as 104.26.10.229) required to locate computers on the internet. This report outlines the hierarchy of domain names, the specific record types used to store data, and the step-by-step process of a DNS request.

Questions and Answers

Task 1 What does DNS stand for? Domain Name System

Task 2 What is the maximum length of a subdomain? 63

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 | 💡 |

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

| _ | Check |

What is the maximum length of a domain name?

| --- | |

What type of TLD is .co.uk?

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

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.

YOU CAN ONLY USE THOSE

Answer the questions below

What is the maximum length of a subdomain?

| 63 | ✓ Correct Answer | 💡 |

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

| _ | ✓ Correct Answer |

What is the maximum length of a domain name?

What is the maximum length of a domain name? 253

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 | 💡 |

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?

| _ _ _ _ _ |

27°   Q Search   2:15 PM
                                                                   2/2/2026

What type of TLD is .co.uk? ccTLD

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.

28°   Q Search   2:17 PM
                                                                   2/2/2026

Task 3 What type of record would be used to advise where to send email? MX

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.
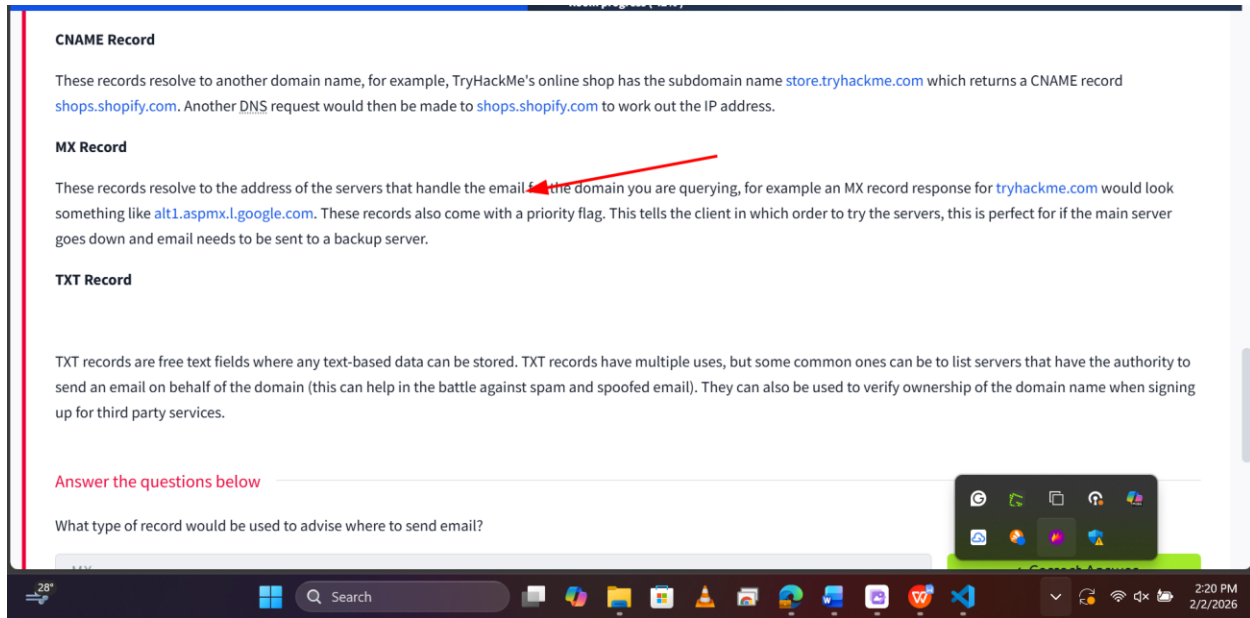
MX Record

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.

Answer the questions below

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

What type of record handles IPv6 addresses? AAAA

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
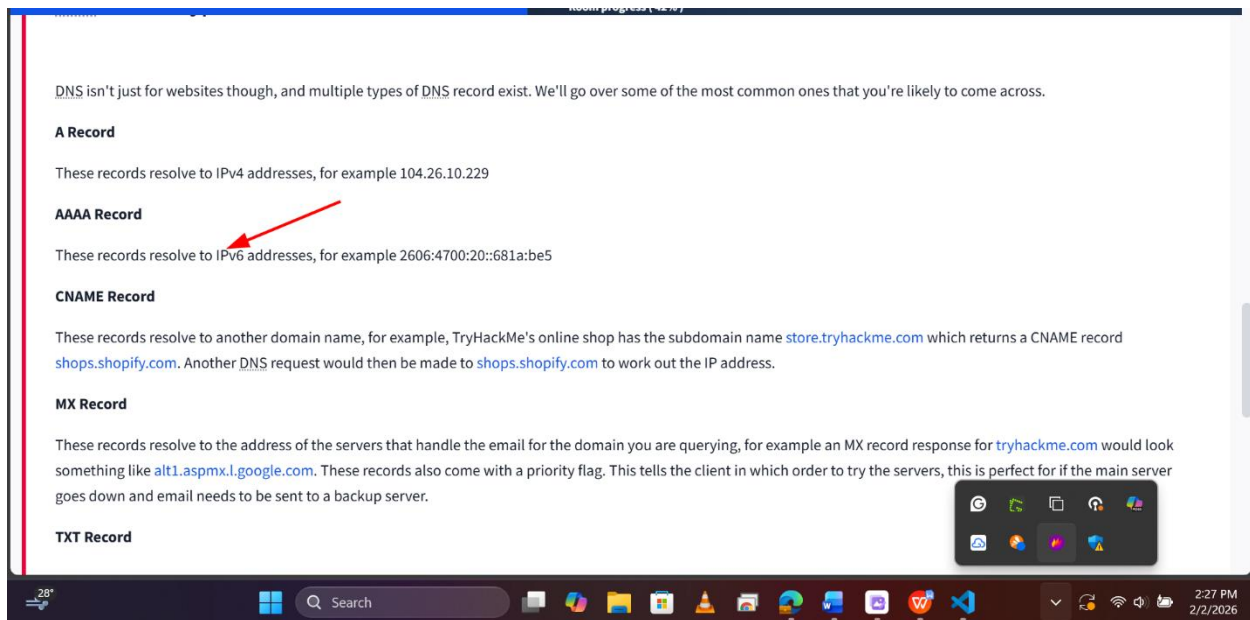
CNAME Record

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

Task 4 What field specifies how long a DNS record should be cached for? TTL

Room progress (57%)

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?

TTL

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

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

Room progress (64%)

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.

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

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?

TTL

Task 5 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
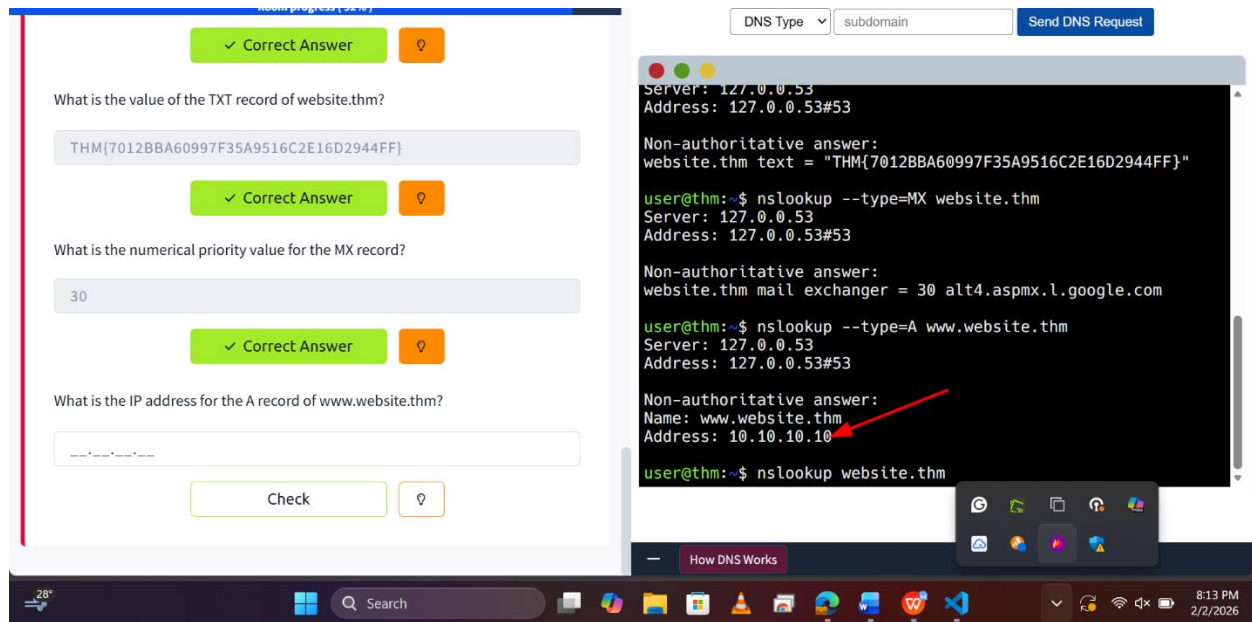
Domain Hierarchy and Structure

The structure of a domain name is hierarchical, reading from right to left.

- **Top Level Domains (TLD):** This is the rightmost segment of a domain name. TLDs are categorized into **Generic TLDs (gTLD)**, which serve specific purposes (e.g., .com for commercial use, .org for organizations), and **Country Code TLDs (ccTLD)**, which represent specific nations (e.g., .co.uk, .ar).

- **Second-Level Domains:** Located to the left of the TLD, this section is limited to a length of 63 characters. Valid characters include letters (a–z), numbers (0–9), and hyphens.

- **Subdomains:** Situated on the left-hand side of the Second-Level Domain, subdomains are separated by periods (e.g., admin.platform.google.com). While there is no limit to the number of subdomains one can create, the maximum length for a complete domain name is **253 characters**.

DNS Record Types

DNS relies on specific record types to resolve different kinds of queries. Key record types include:

- **A Record:** Resolves a hostname to an **IPv4 address**.

- **AAAA Record:** Resolves a hostname to an **IPv6 address**.

- **CNAME Record:** Resolves one domain name to another domain name (e.g., mapping a shop subdomain to shops.shopify.com) rather than directly to an IP address.

- **MX Record:** Directs traffic to the servers handling **email** for a domain. These records include a priority flag to determine the order in which servers are tried, acting as a safeguard if a primary server fails.

- **TXT Record:** Free text fields used for storing text-based data. These are commonly used to **verify domain ownership** for third-party services and to list servers authorized to send email on behalf of a domain to prevent spam.

The DNS Request Process

When a user requests a website, a specific sequence of checks occurs to locate the correct IP address:

1. **Local Cache:** The computer first checks its local history to see if the address was recently looked up.

2. **Recursive DNS Server:** If the record is not found locally, the request is sent to a Recursive DNS Server, typically provided by the **ISP (Internet Service Provider)**. This server checks its own cache and, if the record is present, returns it immediately.

3. **Root and TLD Servers:** If the Recursive Server does not have the answer, it queries the internet's **Root Servers**, which act as the backbone of the system. The Root Server redirects the inquiry to the appropriate **TLD Server** (e.g., the server managing .com addresses).

4. **Authoritative Name Server:** The TLD server points to the **Authoritative DNS Server**, which stores the actual DNS records for the specific domain and is where updates to records are made.

Once the Authoritative Server returns the correct record, it is sent back to the Recursive Server and then to the user. To improve efficiency, these records contain a **TTL (Time To Live)** value, which dictates how long the record is cached locally (in seconds) before a new lookup is required.

Verification of Completion

This completion has been shared on professional networks like Twitter to publicly document my commitment to continuous learning in cybersecurity. This section provides the official verification artifacts for the "DNS in Detail" module.
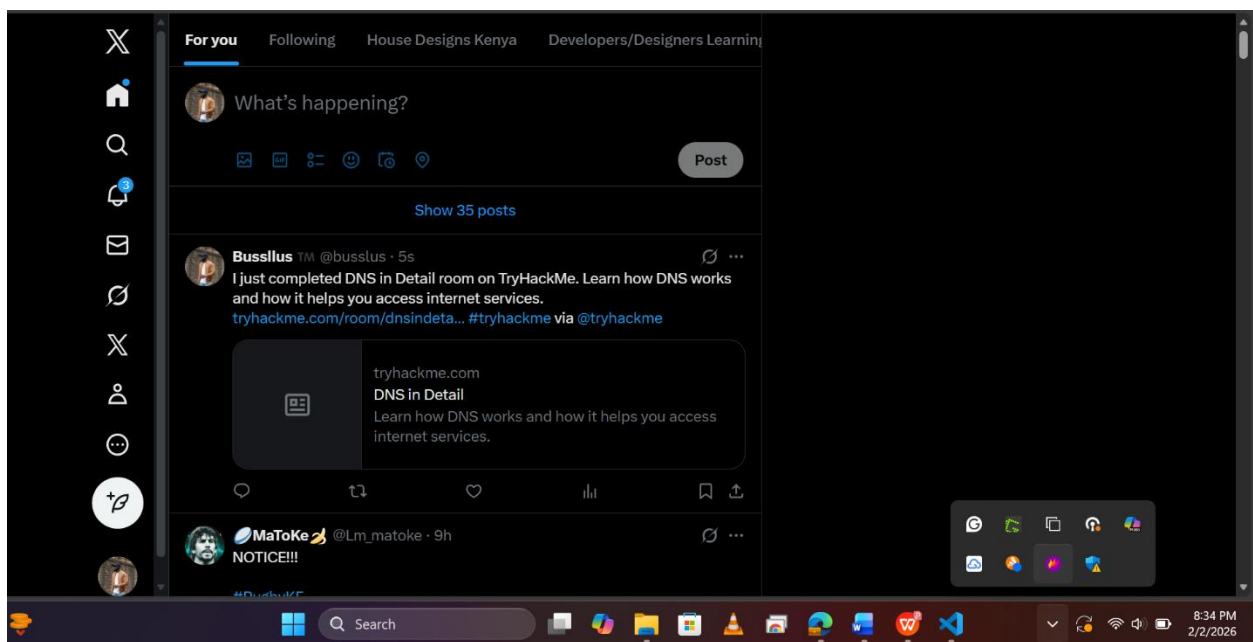
Completion Shareable Link

https://tryhackme.com/room/dnsindetail?utm_campaign=social_share&utm_medium=social &utm_content=room&utm_source=copy&sharerId=6969c8f4464c33f1983a193f

Conclusion

The Domain Name System is an essential component of internet functionality, converting user-friendly names into machine-readable addresses through a strictly defined hierarchy of TLDs,

domains, and subdomains. By utilizing a distributed network of Recursive, Root, and Authoritative servers, alongside efficient caching mechanisms dictated by TTL values, DNS ensures reliable and fast connectivity for services ranging from web browsing to email delivery. Tools such as nslookup allow administrators to query these records directly, verifying the complex infrastructure that operates behind the scenes of everyday internet use.