Course: Cloud and Network Security
Name: Neville Ngothe Iregi
Student No.: CS-CNS10-25054
Date: Tuesday, 30 September 2025

Week 3 Assignment 1: TryHackMe: DNS In Detail

Introduction

Domain Name System (DNS) is a hierarchical and distributed name service that translates human-readable domain names (e.g google.com) to machine-readable IP addresses (e.g 100.200.63.45) through a process called **DNS lookup.** It provides a naming system for computers, services, and other resources on the Internet or other Internet Protocol networks. DNS servers work together in a hierarchical manner to perform the lookups to enable access to websites and other Internet resources.

DNS operates at the Application layer (Layer 7) and utilises TCP and UDP port 53. UDP port 53 is for quick queries while TCP port 53 handles large responses, zone transfers, and DNSSEC (a suite of specifications that adds security to the Domain Name System (DNS) by providing data origin authentication and integrity protection for DNS data).

Domain Hierarchy

1. **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.
2. **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).
3. **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.

DNS Record Types

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 an alias for the domain name requested, 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.

Making a DNS request

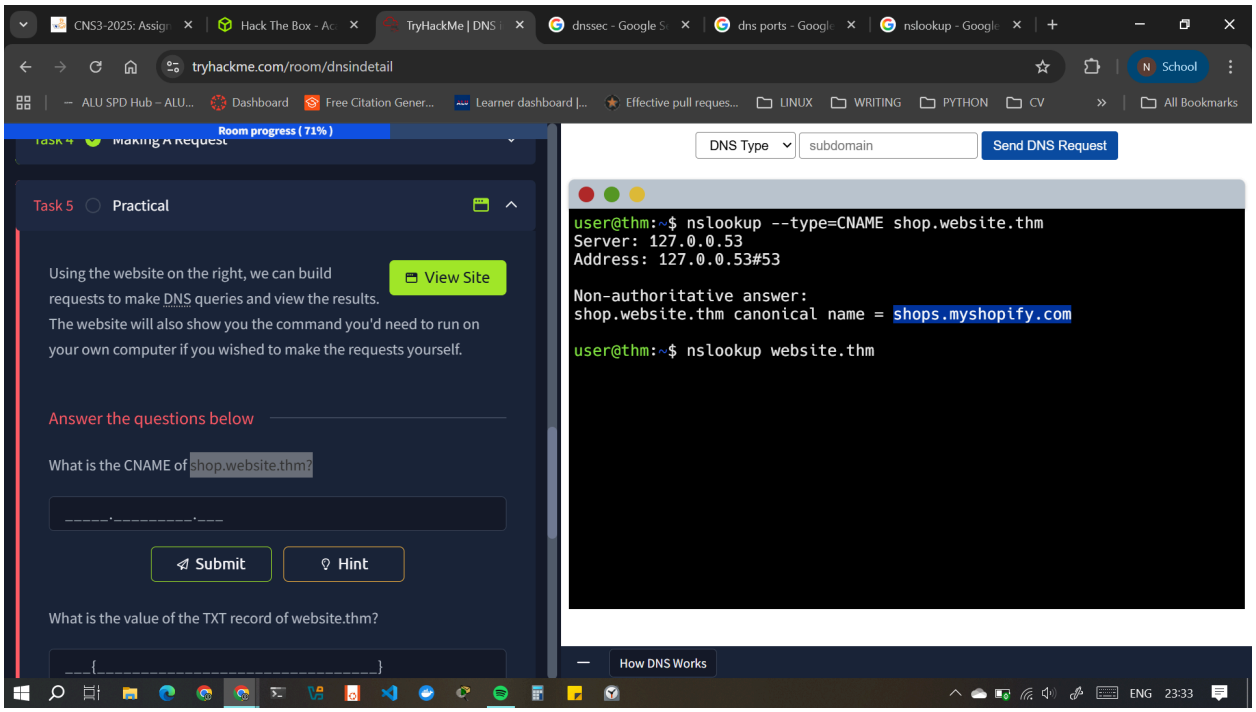
When a request is made for a domain name:

1. The computer first checks its local cache to see if you previously looked up the address recently. Otherwise, a request is made to your **Recursive DNS server**, which is usually provided by your ISP, but one can choose their own.
2. The Recursive DNS server has a local cache of recently looked up domain names and if a result is found locally, it is sent back to your computer and the request ends there. If a request is not found locally, the request is sent to the internet's **root DNS servers.**
3. The root servers 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.

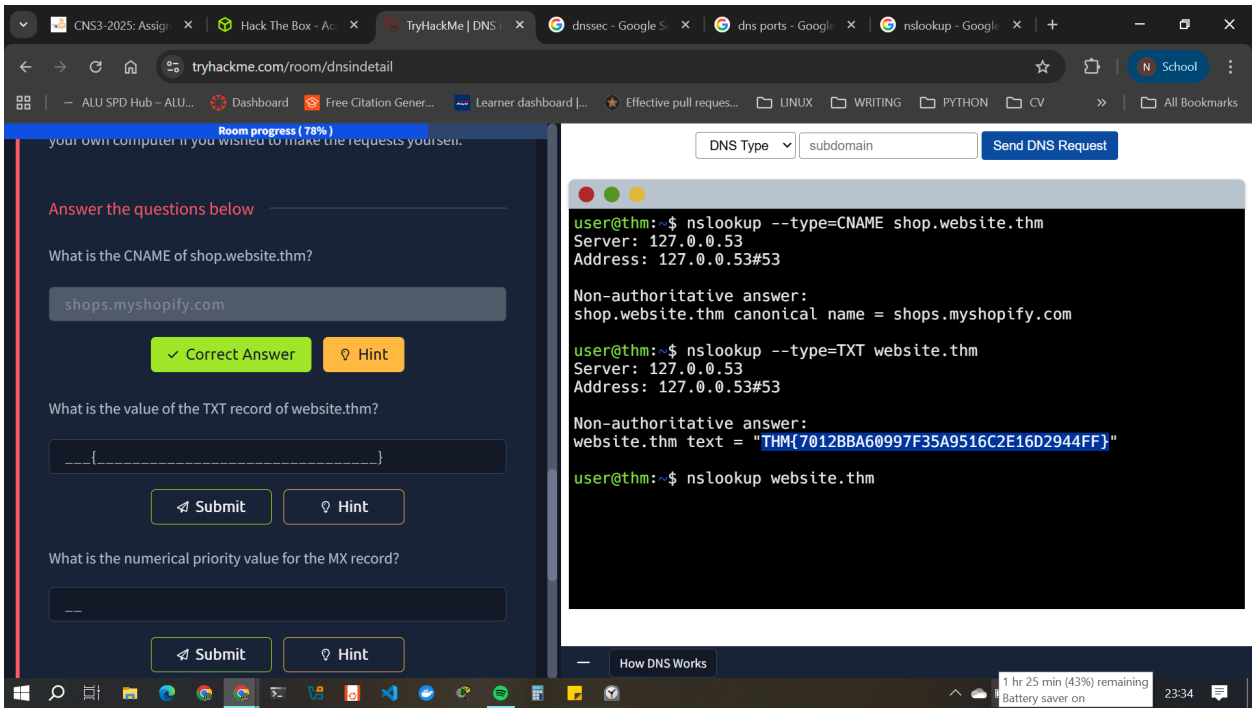
Note: DNS records all come with a **TTL (Time To Live) value**. This value is a number represented in seconds that the response should be saved for locally until you have to look it up again. Caching saves on having to make a DNS request every time you communicate with a server.

We can use **nslookup(Name Server Lookup)**, a network administration command line tool, used for querying the Domain Name System to obtain the mapping between domain name and IP addresses, or other DNS records.

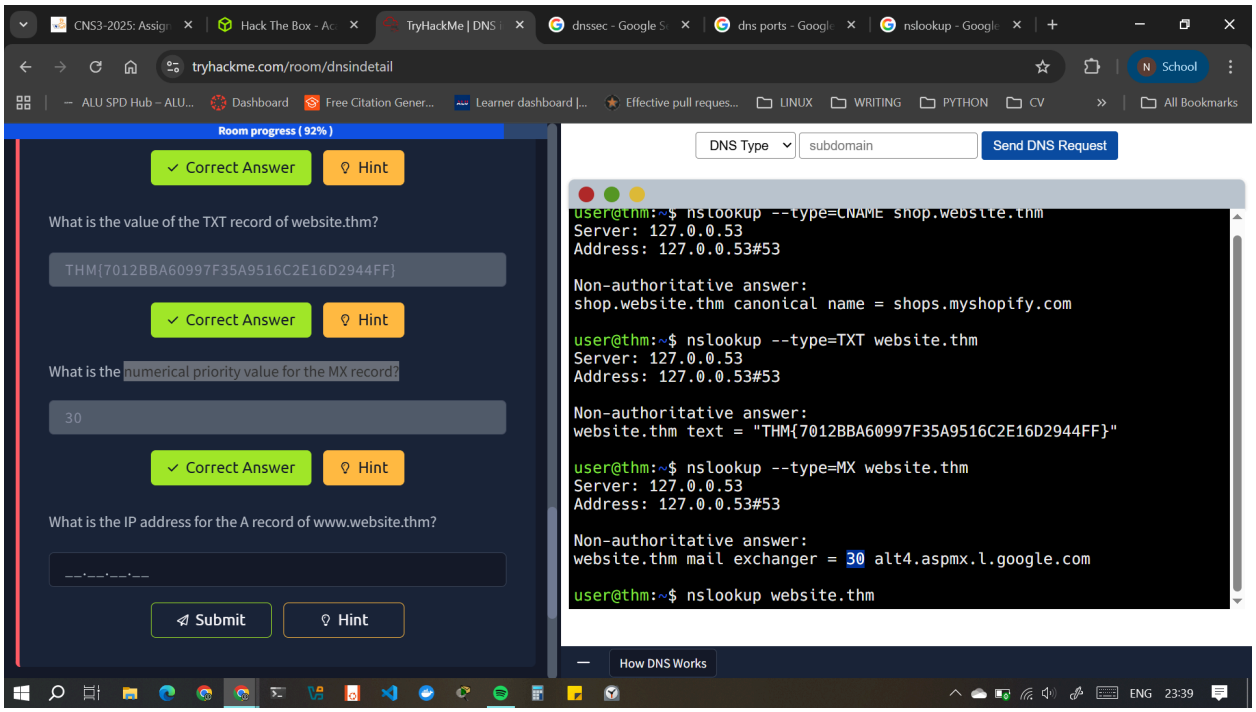
- CNAME of shop.website.thm = **shops.myshopify.com**



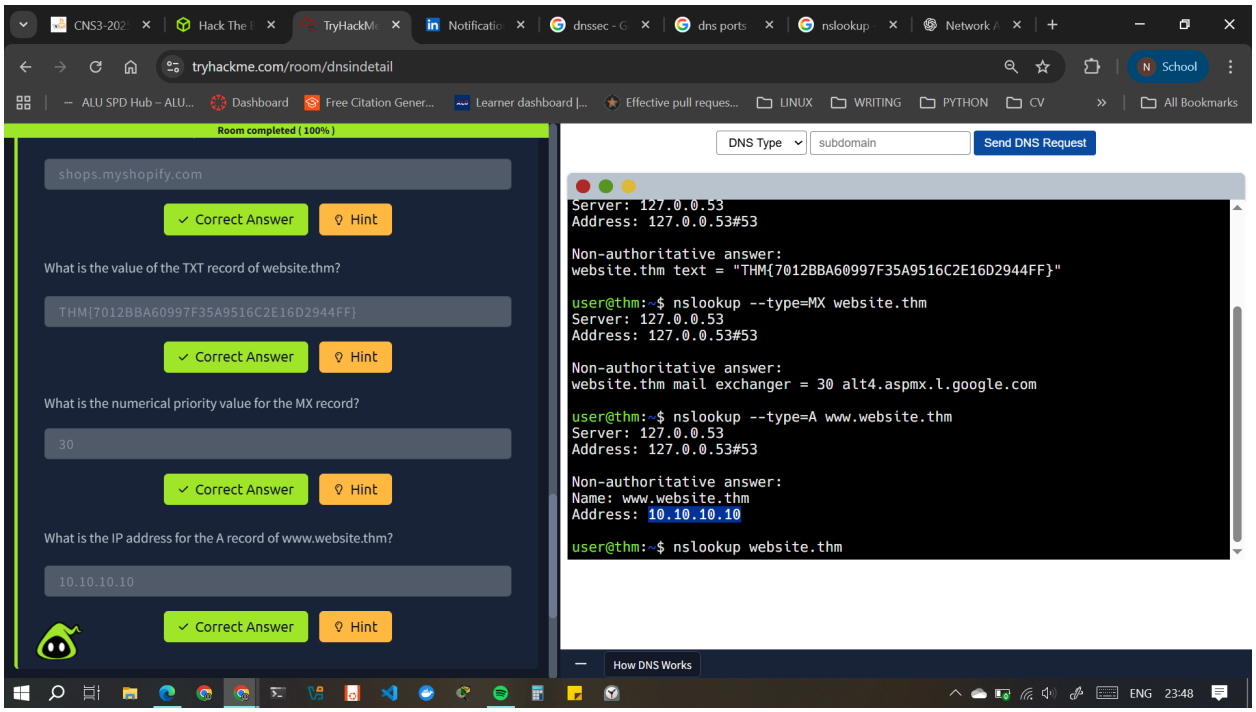
- Value of TXT record of website.thm = **THM{7012BBA60997F35A9516C2E16D2944FF}**



- numerical priority value for the MX record = **30**



- IP address for the A record of www.website.thm - **10.10.10.10**



Final screenshot showing module completion

Conclusion

This room enhanced my understanding of the Domain Name System, types of domain hierarchies, the servers involved in resolving DNS queries, and the use of the nslookup utility with –type option to find information about domains.