DNS in Details

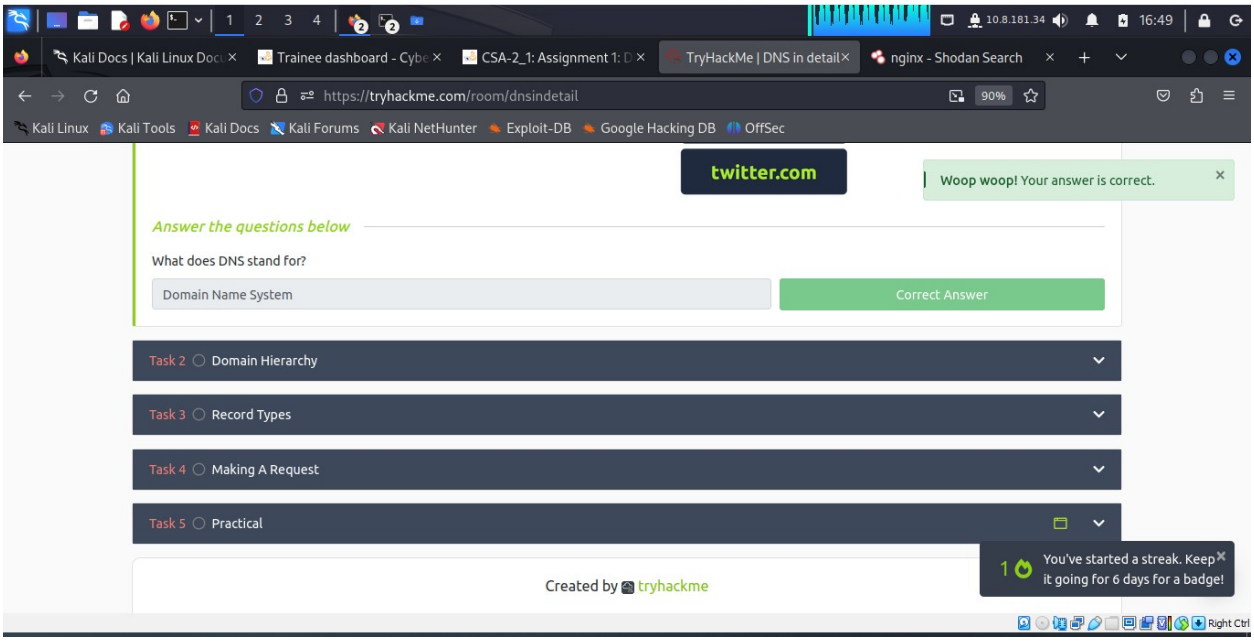
Introduction

In this section the learner will get to know what DNS is, how it is important in their world of analyzing security. Also the learner will be able to understand Domain Hierarchy, Record types making a DNS request and finally complete the module assignment with a practical related to DNS.

Activities

Task 1: What is DNS?

DNS – Domain Name System is the mean for communicating with devices on the internet without remembering complex number – like format (the *IPs*).



Task 2: Domain Hierarchy

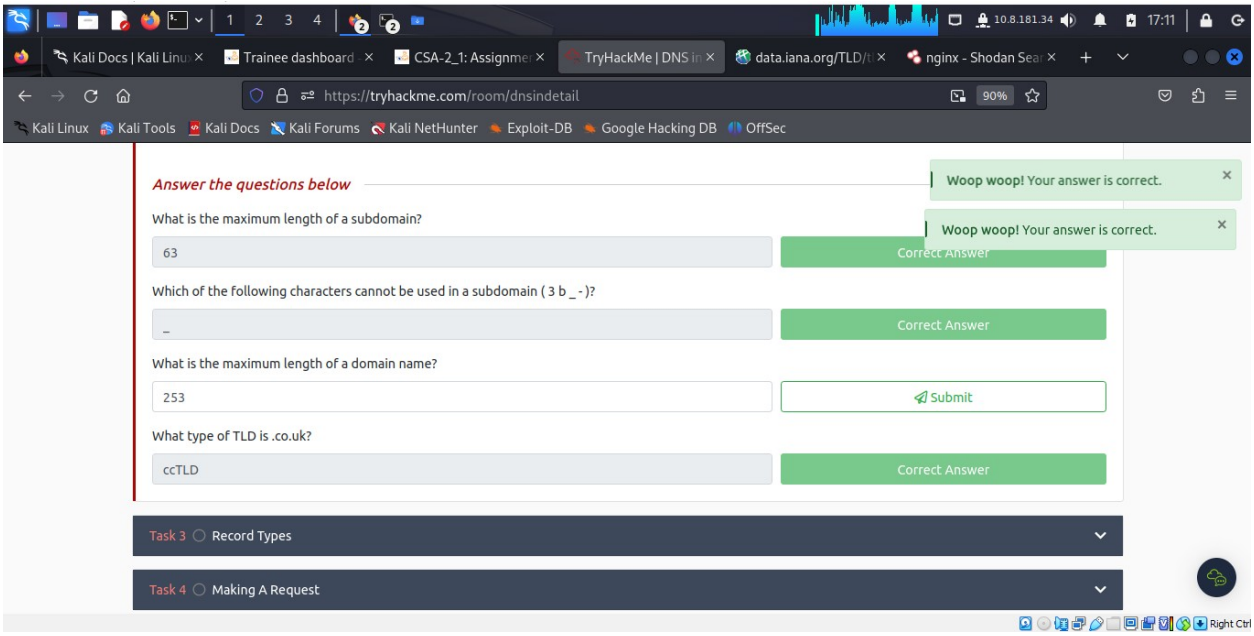
When we talk about domain hierarchy it simply implies the structure of the domain covering the TLD (Top-Level Domain) with its associated types (gTLD and ccTLD) and knowledge on subdomain.

Top-Level Domain: the most right-hand part of the domain. E.g **.com**

Types of TLD

gTLD – generic Top-level Domain: meant to tell the user the domain name's purpose. E.g., **.edu** purposed for education.

ccTLD – Country code Top – Level Domain: used for geographical purpose e.g., **.ke** for sites located in Kenya.



Task 3: Record Types

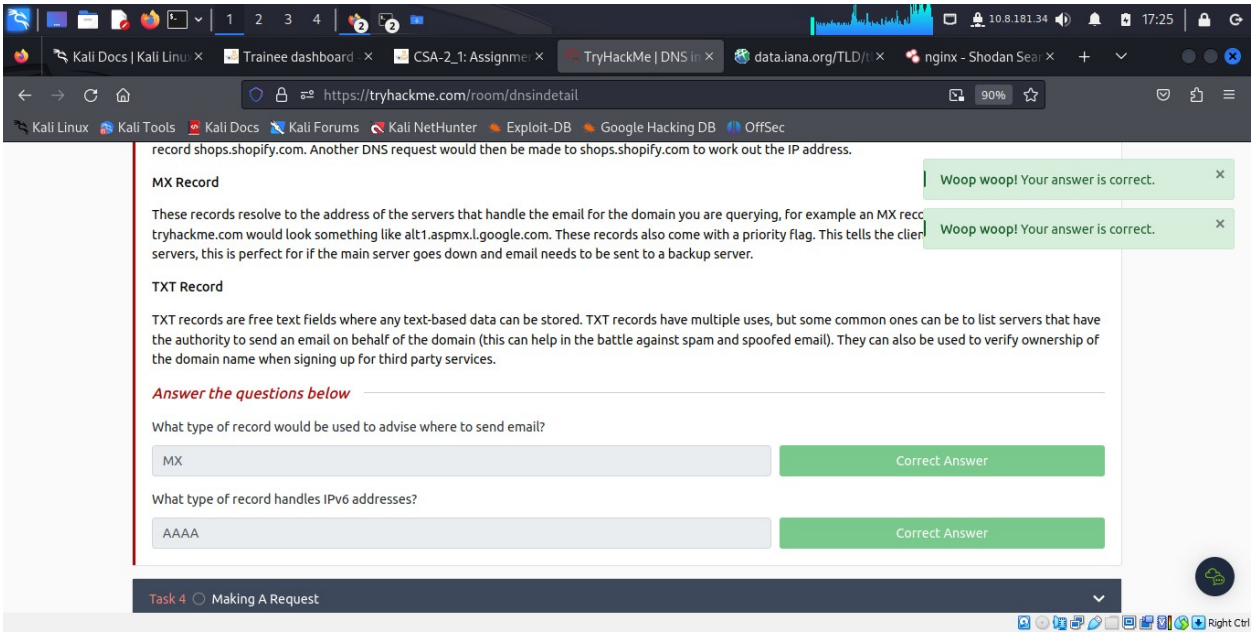
DNS record to provide important information about a domain or hostname, particularly its current IP address. The most common DNS record types are:

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.



Task 4: Making A Request

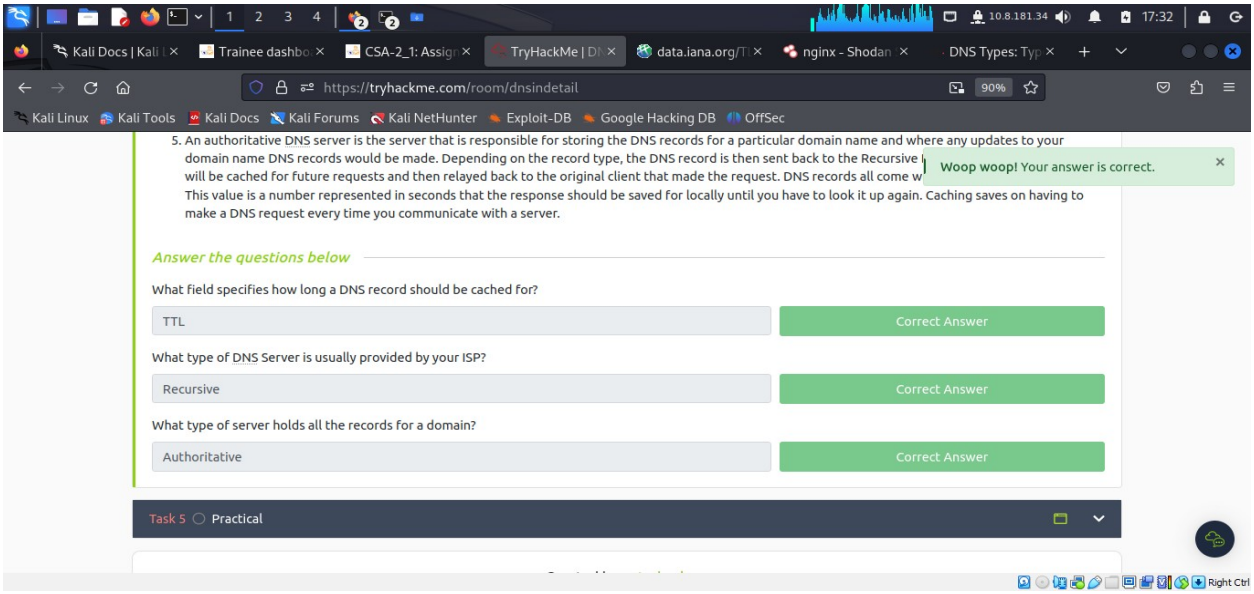
To send a DNS request, a certain procedure is followed and the learner understands the process that it entails:

Upon requesting a domain name, the computer first checks its local cache to see if previously looked up the address recently; if not, a request to Recursive DNS Server (usually provided by the ISP) will be made. to Recursive DNS Server has a local cache of recently looked up domain names. If a result is found locally, this is sent back to the computer, and the request ends here.

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.

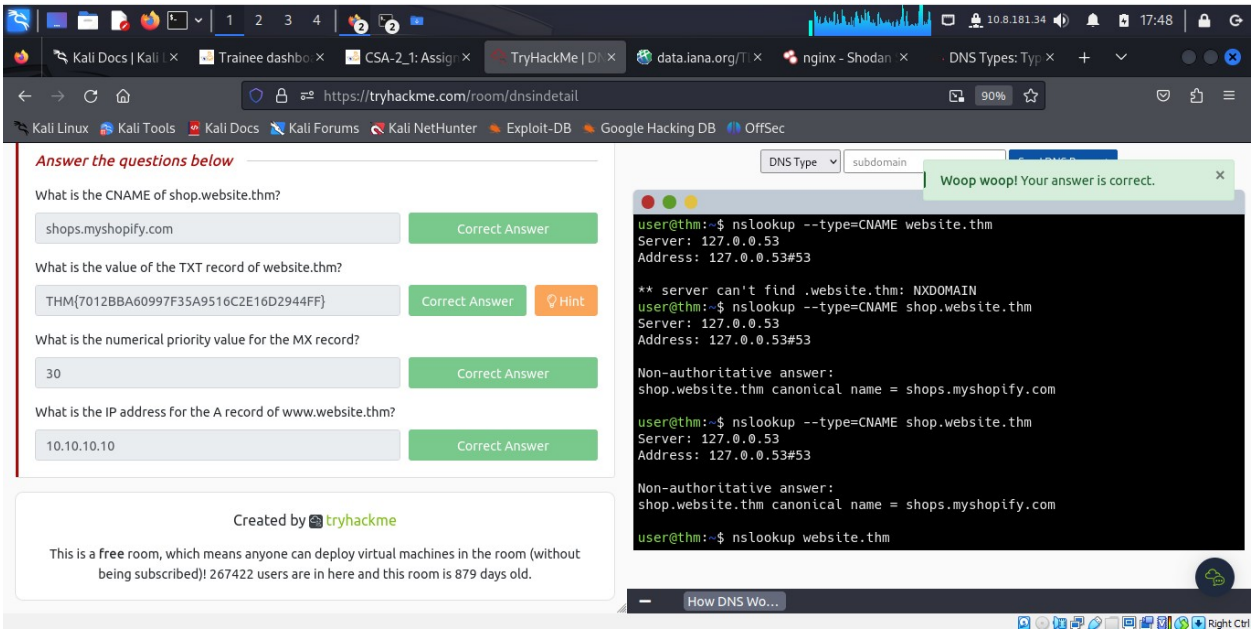
The TLD server holds records for where to find the authoritative server to answer the DNS request. The authoritative server is often also known as the nameserver for the domain.

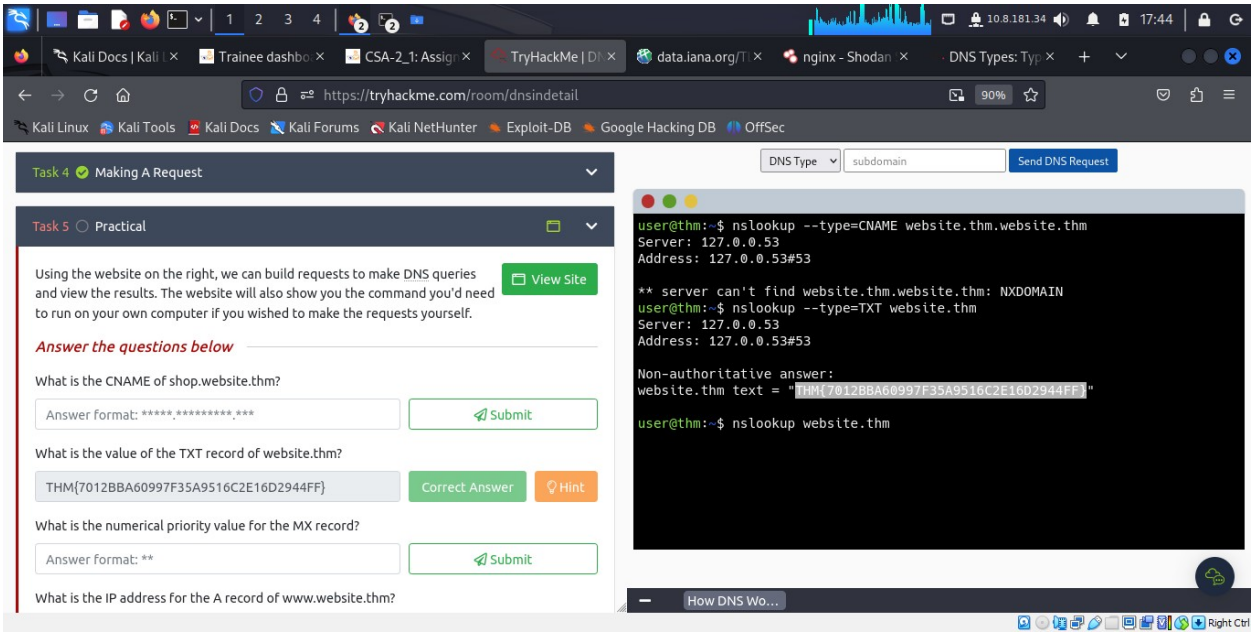
An authoritative DNS server is the server that is responsible for storing the DNS records for a particular domain name and where any updates to the domain name DNS records would be made. Depending on the record type, the DNS record is then sent back to the Recursive DNS Server, where a local copy will 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.



Task 5: Practical

This practical enables the learner to interact with theoretical concepts discussed previously. For instance, looking for CNAME, A record, AAAA record MX record and TXT record.





Conclusion

The learner completely understood the concept of Domain Name System (DNS), done a practical on the practice website **website.htm**